A collaborative Approach at Internet Scale

JESSICA STEINBERGER

Distributed DDoS Defense

A collaborative Approach at Internet Scale

JESSICA STEINBERGER

UNIVERSITEIT TWENTE.

Graduation committee:

Chairman:

Prof. Dr. J. N. Kok

Supervisor:

Prof. Dr. ir. A. Pras

Co-supervisors:

Prof. Dr. rer. nat. H. Baier

Dr. A. Sperotto

Members:

Prof. Dr. rer. nat. G. Dreo Rodosek

Bundeswehr University Munich, Germany

Prof. Dr. A. K. I. Remke

Westfälische Wilhelms-Universität Münster, Germany

Prof. Dr. ir. R. N. J. Veldhuis

University of Twente, The Netherlands

Prof. Dr. ir. L. J. M. Nieuwenhuis

University of Twente, The Netherlands

Funding sources:

BMBF - Privacy-preserving Flow-based Anomaly Detection and Mitigation – 16BY1201F

BMBF - Institutional Network and Service Provider Anomaly Inspection – 03FH005PB2

Hessen Agentur GmbH - Reactive network Optimization By Using SDN Technology – 473/15-15

Center for Advanced Security Research Darmstadt (CASED)

Center for Research in Security and Privacy (CRISP)

UNIVERSITY OF TWENTE.
DIGITAL SOCIETY INSTITUTE

DSI Ph.D. Thesis Series No. 18-006

Digital Society Institute

P.O. Box 217, 7500 AE

Enschede, the Netherlands

ISBN 978-90-365-4581-5

ISSN 2589-7721 (DSI Ph.D. thesis Series No. 18-006)

DOI 10.3990/1.9789036545815

<http://dx.doi.org/10.3990/1.9789036545815>

Type set with $\LaTeX$. Printed by Gildeprint Drukkerijen, The Netherlands.

Cover design by Jessica Steinberger.

Copyright © 2018 Jessica Steinberger

This work is licensed under a Creative Commons

Attribution-NonCommercial-ShareAlike 3.0 Unported License.

<http://creativecommons.org/licenses/by-nc-sa/3.0/>

DISTRIBUTED DDOS DEFENSE: A COLLABORATIVE APPROACH AT INTERNET SCALE

PROEFSCHRIFT

ter verkrijging van
de graad van doctor aan de Universiteit Twente,
op gezag van de rector magnificus,
prof. dr. T.T.M. Palstra,
volgens besluit van het College voor Promoties,
in het openbaar te verdedigen
op woensdag 19 september 2018 om 16:45 uur

door

Jessica Steinberger

geboren op 18 juli 1983
te Mainz, Duitsland

Dit proefschrift is goedgekeurd door:

Prof. Dr. ir. A. Pras (promotor)

Prof. Dr. rer. nat. H. Baier (co-promotor)

Dr. A. Sperotto (co-promotor)

To my grandma

*To the loving memory of
my grandpa Manfred and Winfried*

Acknowledgements

Visualization of my PhD trajectory

Writing this thesis would not have been possible without the help and support of many people. Therefore I would like to say thanks to all of them.

First, I would like to express my sincere gratitude to Prof. Dr. Harald Baier for his continuous support of my PhD study and related research, for his patience, his motivation, for giving me the freedom to discover interesting research topics and providing me with everything I needed to conduct my research.

Likewise, I would like to express my gratitude to my supervisors Prof. Dr. Aiko Pras and Dr. Anna Sperotto. I am really happy that both accepted me as an external PhD student and I consider myself very lucky to work with them. I am thankful to Aiko for his continuous support of my PhD study and his to-the-point advice (professional and personal) whenever I felt lost. Many thanks go to Anna for numerous fruitful discussions, brainstorming about fresh ideas, precise sorting and ordering available research material, motivating me and providing immense knowledge. I could not have imagined having better supervisors and co-supervisors for my PhD study.

I also would like to thank my graduation committee for accepting to be in my committee and for their valuable comments on this thesis.

Special thanks go to Katharina Kuhnert, who started working with me as a student assistant in 2014. It was a pleasure to discuss and work with her on several projects and publications. She did an excellent work and provided valuable support for my research. During my PhD trajectory, I will always remember her escape reflex caused

by my most mentioned sentence: "Katharina, we have a problem" and the submission day of NOMS 2016 were we worked all night long to submit the paper and during the experiment she felt asleep while I was waiting for the results on the phone unable to wake her up. She is a really good friend and I hope we will stay in touch after this PhD trajectory.

During my research stays at the University Twente, I had the chance to meet Mozhdeh, Morteza and Ria, who soon became friends. I am especially thankful that Morteza often gave me a ride back home in the south of Enschede and thus made it possible for me to attend numerous events from the UT. I will always remember this funny night, when Mozhdeh was trying to give me back the self-made bread. Further, I really enjoyed making nice pictures with Mozhdeh in front of the UT logo. I hope to meet you both soon in Munich.

Most of the time in Enschede I stayed at Ria's house. I really appreciate our talks, her advices and her way to cook. I consider myself really lucky that I met her. I will always remember the dish washing dance evening together with Rachel. *Life is too short - sweetie* remains in my mind and always places a smile on my face in difficult moments in life.

During my PhD trajectory I have been fortunate to meet many excellent professionals and colleagues. Special thanks go to my colleagues at da/sec and DACS. In particular, I would like to say thanks to my roommates Sebastian Gärtner and Lorenz Liebler for personal and professional discussions and advices. Besides my roommates, I would like to say thanks to Marta Gómez-Barrero (*Gracias, por todas las palabras en español para evitar que olvide todo. Espero que nos veamos pronto en Munich*) and Ulrich Scherhag for their help and support during my research.

Through the project work of OpenC3S, I got to know Martin Sievers. I am grateful for his immense knowledge and invaluable advice in $\LaTeX$. There is no challenge with $\LaTeX$, I would prefer to ask anybody else. Thank you so much.

I have to thank my good friend Benedikt who played an important role that I finished my computer science studies. Learning programming was challenging and fun together with you - thank you for your patience, your teaching lessons and your advices in professional and private life. I hope you will soon find a new job, you will be happy again and we keep in touch.

Filou..., my companion, friend, protector, playmate and life-changer. She was able to free up my mind and made me smile. She was next to me, while I was finishing up exercises during my studies or writing papers all night long. Often solutions to research problems came up to my mind, while taking her out for a walk. I am thankful

for her unconditional love, her fun and her patience. If I had granted one wish, I would have wished that my best friend could have lived forever. R.I.P..

I would also like to thank Manuela & Dieter and Petra & Werner for being in my life and part of my new family. Thanks for your support and welcoming me into your family. You make my world special just being in it.

During my Phd trajectory I am pleased to say my baby girls Lia Milou and Linn Nea were born. They made me able to experience life through the eyes of a child: Everything is magical and extraordinary. Everyday they are teaching me two things: First, happiness for no reason and second, the most precious jewels you'll ever have around your neck are the arms of your children. I am thankful to be your mother.

Special thanks go to my granny for her support, her strength, doing her best to fulfill my dreams and that she has always been proud of my achievements. I would have given up, if you had not been there for me. Words can not express how much I love you.

Finally, I would like to thank my love *Honey* who gave me the courage to start a new path after so many years. The most wonderful thing I decided to do was to share my life and heart with you. Thank you for making me feel so complete and for making my life easier when it turns into complete chaos. Thank you for your support through all of my chaotic life and in finalizing this thesis. Your positive outlook on life has given me the strength to do it all. Thank you for being my reason to look forward to the next day.

Abstract

The Internet has evolved to a vital component that heavily influences our daily life. Large majorities of users rely on the Internet on a regular basis for financial services, shopping, and other customer services. In addition, the Internet has become a crucial component for millions of businesses, stock markets, public facilities and transportation hubs, power grids and water delivery systems.

In recent years, large-scale cyber attacks targeting the availability of network infrastructure and service have been constantly reported and could lead to enormous financial loss, potentially triggering sustained power outages over large portions of the electric grid and prolonged disruptions in communications, food and water supplies, and health care delivery.

One type of large-scale cyber attacks are Distributed Denial of Service (DDoS) attacks that still remain the top concern responsible for network infrastructure and service outages. The reason is that DDoS attacks are getting larger, more sophisticated (e.g. multi-vector attacks) and frequent.

At the same time it has never been easier to execute DDoS attacks, e.g., Booter services offer paying customers without any technical knowledge the possibility to perform DDoS attacks as a service via a web page. Besides Booter services, it is also possible to hire a whole botnet (e.g., hire-a-botnet-services) for a DDoS campaign at low price. Moreover, new technology trends in the development of the Internet such as Internet of Things (IoT) focus to connect billions of everyday devices. These devices are designed to be user-friendly and accessible and often do not have a stringent security standard. Currently, 4.9 billion IoT units are in use and will reach 25 billion by 2020. However, the lack of security standards, the ease of manipulation and the amount of available everyday devices encourage attackers to perform large-scale DDoS attacks.

Given the attack intensities and effects caused by DDoS attacks, we believe that Internet Service Providers (ISPs) should collaborate to optimize mitigation and their response capabilities and thus reduce potential damages caused by DDoS attacks. The main research goal of this thesis is to develop a collaborative, automated approach to mitigate the effects of DDoS attacks at Internet Scale. This thesis has the following main contributions: i) we performed a systematic and multifaceted study on mitigation of large-scale cyber attacks at ISPs in order to gain insight into current processes, structures and their mitigation capabilities. ii) We provided a detailed guidance selecting an exchange format and protocol suitable to use in an ISP network to disseminate threat information. iii) To overcome the shortcomings of missing flow-

based interoperability of current exchange formats, we developed the exchange format Flow-based Event Exchange Format (FLEX). iv) In order to perform distributed DDoS defense, we developed a communication process to facilitate the automated defense in response to ongoing network-based attacks. v) In addition to the communication process, we developed a model to select and perform a semi-automatic deployment of suitable response actions. vi) We investigate the effectiveness of the defense techniques moving-target using Software Defined Networking (SDN) and their applicability in context of large-scale cyber attacks and the networks of ISPs. Finally, we developed a trust model that determines a trust and a knowledge level of a security event in order to deploy semi-automated remediations and facilitate the dissemination of security event information using the exchange format FLEX in context of ISP networks.

Our evaluations have shown that the contributions in this thesis can be used by network administrators, network operators and networks security engineers to better limit the effects of current and future DDoS attacks and thus prevent network infrastructure and service outages.

Finally, all source code and used data that forms the basis of our research results used within this thesis has value for the research community and was made publicly available in github (<https://github.com/jesstei/MiR>) to overcome closed source and system dependency of this research domain. This provides the possibility that future research builds upon the results of this thesis.

Abstrakt

Das Internet hat sich zu einem wesentlichen Bestandteil unseres träglichen Lebens entwickelt. Die Mehrheit der Nutzer verwendet das Internet regelmäßig für Finanzdienstleistungen, Einkäufe und andere Kundendienstleistungen. Zudem ist das Internet für Millionen von Unternehmen, Börsen, öffentliche Einrichtungen und Verkehrsunternehmen, Stromnetze und Wasserversorgungssysteme ein unverzichtbarer Bestandteil der Geschäftsprozesse geworden.

In den letzten Jahren wurde zunehmend über massive Cyberangriffe berichtet, die gezielt die Verfügbarkeit von Netzwerkinfrastrukturen und -diensten angreifen. Diese massiven Cyberangriffe können unter anderem zu enormen finanziellen Verlusten führen, aber auch für möglicherweise anhaltende Stromausfälle über große Teile des Stromnetzes sowie für längere Unterbrechungen in Kommunikation, Nahrungs- und Wasserlieferungen und der Gesundheitsversorgung verantwortlich sein.

Eine Art dieser großen Cyberangriffe sind DDoS-Angriffe, die immer noch Hauptverantwortlich für Netzwerkinfrastruktur- und Dienstausfälle sind. Der Grund dafür ist, dass DDoS-Angriffe immer größer, komplexer (z. B. Multi-Vektor-Angriffe) und häufiger werden.

Neben der Größe, Komplexität und der Häufigkeit der DDoS-Angriffe war es nie einfacher diese auszuführen. Beispielsweise bieten Booter-Dienste zahlenden Kunden ohne technisches Wissen die Möglichkeit, DDoS-Angriffe als Dienst über eine Webseite auszuführen. Neben den Booter-Diensten ist es auch möglich, ein ganzes Botnet (z. B. Leih-Botnet-Dienste) für eine DDoS-Kampagne zu einem niedrigen Preis zu mieten. Zudem konzentrieren sich neue Technologietrends wie IoT auf die Verbindung von Milliarden alltäglicher Geräte. Diese Geräte sind zwar benutzerfreundlich und zugänglich, verfügen jedoch oft über einen unzureichenden bis keinen Sicherheitsstandard. Derzeit sind 4.9 Mrd. IoT-Geräte im Einsatz und deren Anzahl wird schätzungsweise bis 2020 auf 25 Mrd. ansteigen. Das Fehlen von Sicherheitsstandards, die einfache Handhabung und die Anzahl der verfügbarer IoT-Geräte ermöglichen Angreifern jedoch umfangreiche DDoS-Angriffe unter deren Verwendung durchzuführen.

In Anbetracht der Angriffsintensitäten und der dadurch verursachten Angriffseffekte von DDoS-Angriffen, sind wir überzeugt, dass ISPs zusammenarbeiten sollten, um die Schadensbegrenzung und ihre Reaktionsfähigkeit zu optimieren und so potentielle Schäden durch DDoS-Angriffe zu reduzieren. Daher ist das Hauptziel dieser Arbeit die Entwicklung eines kollaborativen, automatisierten Ansatzes zur Abmilderung der Auswirkungen von Angriffen im Netzwerk von Internet Service Providern. Die Hauptbeiträge dieser Arbeit sind: i) Wir haben eine systematische Studie zur Abschwächung

großer Cyberangriffe bei ISPs durchgeführt. Diese Studie bietet Einblicke in aktuelle Prozesse, Strukturen und die Fähigkeit mit massiven Cyberangriffen im Netzwerk von ISPs umzugehen. ii) Wir liefern eine detaillierte Übersicht zur Auswahl eines Austauschformats und eines Austauschprotokolls, welches für die Verwendung in einem ISP-Netzwerk zur Verbreitung von Bedrohungs- und Angriffsinformationen geeignet ist. iii) Um die fehlende flussbasierte Interoperabilität aktueller Austauschformate zu überwinden, haben wir das Austauschformat *FLEX* entwickelt. iv) Um eine dezentrale Verteidigung zu gewährleisten, haben wir einen Kommunikationsprozess entwickelt, um die automatisierte Abwehr als Reaktion auf laufende netzwerkbasierende Angriffe zu ermöglichen. v) Zusätzlich zum Kommunikationsprozess haben wir ein Modell entwickelt, um einen halbautomatischen Einsatz geeigneter Maßnahmen auszuwählen und durchzuführen. vi) Wir haben die Effektivität der Abwehrtechniken von *Moving Target* mit Hilfe von SDN und deren Anwendbarkeit im Kontext von massiven Cyberangriffen im Netzwerk von ISPs untersucht. Schließlich haben wir ein Vertrauensmodell entwickelt, das die Vertrauenswürdigkeit und das Wissen eines Sicherheitsereignisses ermittelt, um halbautomatisierte Fehlerbehebungsmaßnahmen zu implementieren und die Verbreitung von Sicherheitsereignisinformationen mithilfe des Austauschformats *FLEX* im Kontext von ISP Netzwerken ermöglicht.

Unsere Evaluationen haben gezeigt, dass die Beiträge dieser Arbeit von Netzwerkadministratoren, Netzbetreibern und Netzwerksicherheitsingenieuren genutzt werden können, um die Auswirkungen aktueller und zukünftiger DDoS-Angriffe besser zu begrenzen und somit Netzwerkinfrastruktur- und Serviceausfälle zu verhindern.

Weiterhin wurde der gesamte Quellcode sowie unsere verwendeten Daten, welche die Grundlage unserer Forschungsergebnisse bilden auf github (<https://github.com/jesstei/MiR>) veröffentlicht um einen Mehrwert für die Forschungsgemeinschaft zu bilden und um die geschlossene Quellen- und Systemabhängigkeit dieser Forschungsdomäne zu überwinden. Dies bietet die Möglichkeit, dass zukünftige Forschungsarbeiten auf den Ergebnissen dieser Arbeit aufbauen können.

Samenvatting

Het internet is uitgegroeid tot een onmisbaar onderdeel van ons dagelijks leven. Grote groepen gebruikers zijn afhankelijk van het internet voor toegang tot financiële diensten, online winkels en andere consumentendiensten. Daarnaast is het internet van cruciaal belang voor miljoenen bedrijven, zoals aandelenmarkten, openbare voorzieningen, transportknooppunten, en elektriciteits- en waterleidingbedrijven.

De afgelopen jaren is sprake van een stroom aan meldingen over grootschalige cyberaanvallen, gericht op de beschikbaarheid van netwerkinfrastructuur en -dienstverlening. Dit soort aanvallen kan leiden tot grote financiële verliezen, en bijvoorbeeld ook tot langdurige stroomuitval over grote delen van het elektriciteitsnet en langdurige verstoring van communicatievoorzieningen, levering van voedsel en drinkwater, en levering van gezondheidszorg.

Eén bepaald type grootschalige cyberaanval is de DDoS-aanval. Dit type aanval is nog steeds de belangrijkste reden voor uitval van netwerkdienstverlening. De reden hiervoor is dat DDoS-aanvallen nog steeds groter, geavanceerder (bijvoorbeeld multi-vectoraanvallen) en frequenter worden.

Tegelijkertijd was het nog nooit zo eenvoudig om DDoS-aanvallen uit te voeren. Zo bieden zogenaamde Booter-services aan betalende klanten zonder technische kennis de mogelijkheid om DDoS-aanvallen als dienst via een webpagina uit te voeren. Naast deze Booter-services is het ook mogelijk om voor een lage prijs een heel botnet te huren voor het uitvoeren van een DDoS-campagne (bijvoorbeeld via 'huur-een-botnet' diensten). Daar bovenop komen trends om steeds meer apparaten, zoals IoT, met het internet te verbinden. Dit type apparaten is ontworpen om laagdrempelig en gebruiksvriendelijk te zijn en voldoet vaak niet aan strenge beveiligingsnormen. Op dit moment zijn er naar schatting 4.9 miljard IoT-apparaten in gebruik, en zal de teller in 2020 al op 25 miljard staan. Het gebrek aan beveiligingsstandaarden, het gemak waarmee dit type apparaten gemanipuleerd kan worden en het aantal beschikbare IoT-apparaten moedigt aanvallers alleen maar verder aan om grootschalige DDoS-aanvallen uit te voeren.

Gezien de aanvalskracht en daaruit voortvloeiende effecten van DDoS-aanvallen, zijn wij van mening dat ISPs moeten samenwerken om de bestrijding van DDoS-aanvallen te verbeteren, en zo mogelijke schade door aanvallen te verminderen. Het belangrijkste doel van dit proefschrift is het ontwikkelen van een collaboratieve, geautomatiseerde aanpak om de effecten van DDoS-aanvallen op internetschaal te verminderen. Dit proefschrift heeft de volgende hoofdbijdragen: i) we hebben systematisch vanuit meerdere invalshoeken bestudeerd hoe ISPs DDoS-aanvallen kunnen bestrijden, om

zo inzicht te krijgen in huidige processen, structuren en de effectiviteit daarvan. ii) We geven gedetailleerde richtlijnen voor het kiezen van een uitwisselingsformaat en -protocol dat geschikt is voor een ISP om informatie over bedreigingen te verspreiden. iii) Om de tekortkomingen in interoperabiliteit van bestaande op flows gebaseerde aanpakken te verhelpen, introduceren we het FLEX uitwisselingsformaat. iv) We hebben een communicatieproces ontwikkeld om gedistribueerde en geautomatiseerde verdediging tegen lopende DDoS-aanvallen te faciliteren. v) Bovenop het communicatieproces hebben we een model ontwikkeld om semi-automatisch geschikte verdedigingsmiddelen in te zetten. vi) We onderzochten de effectiviteit van de *Moving Target* verdedigingsaanpak, met behulp van SDN, en de toepasbaarheid daarvan in de context van massale cyberaanvallen op de netwerken van ISPs. Tenslotte hebben we een model ontwikkeld om de betrouwbaarheid en het kennisniveau over een beveiligingsincident te bepalen, zodat passende semi-automatische tegenmaatregelen kunnen worden ingezet en informatie over het incident verspreid kan worden met behulp van het FLEX uitwisselingsformaat.

Ons werk laat zien dat de bijdragen van dit proefschrift daadwerkelijk kunnen worden ingezet door netwerkbeheerders, netwerkoperators en beveiligingsfunctionarissen om de effecten van huidige en toekomstige DDoS-aanvallen beter in te perken en zo uitval van netwerkinfrastructuur- en diensten te voorkomen.

Tot slot: alle broncode en alle onderzoeksgegevens die gebruikt zijn voor dit proefschrift hebben waarde voor de onderzoeksgemeenschap. Daarom zijn alle broncode en onderzoeksgegevens openbaar beschikbaar gemaakt via Github (<https://github.com/jesstei/MiR>). Hiermee leveren we een wezenlijke bijdrage aan het verminderen van de afhankelijkheid van gesloten informatiebronnen voor dit onderzoeksveld. Bovendien maakt het toekomstig werk op basis van de resultaten in dit proefschrift mogelijk.

Contents

List of Acronyms	xxiii
List of Symbols	xxvii
1. Introduction	1
1.1. Motivation	1
1.2. Research Goal, Research Questions & Approaches	5
1.2.1. Main Research Goal	5
1.2.2. Research Questions	6
1.3. Thesis Contribution	8
1.4. Thesis Organization	9
2. Current DDoS Detection & Mitigation: A Survey	15
2.1. Introduction	15
2.2. Survey Research Method	16
2.2.1. Components of the Survey	16
2.2.2. Methods of Data Collection	17
2.2.3. Nonresponse Bias	20
2.3. Survey Results	21
2.3.1. Sample	21
2.3.2. Survey 2013	25
2.3.3. Survey 2015	32
2.4. Lessons Learned	41
2.5. Concluding Remarks	43
3. Exchange of Threat Information	45
3.1. Introduction	45
3.2. Event Exchange Formats and Protocols	47
3.2.1. Terminology	47
3.2.2. Exchange Formats	48
3.2.3. Exchange Protocols	53
3.2.4. Extensible Messaging and Presence Protocol	54
3.2.5. Evaluation	55
3.2.6. Evaluation Methodology	56
3.2.7. Evaluation Results	57

3.3. Evaluation Summary	62
3.4. FLEX	63
3.4.1. Introduction	64
3.4.2. Structure of FLEX	64
3.5. Lessons Learned	68
3.6. Concluding Remarks	69
4. Collaboration Process	71
4.1. Introduction	71
4.2. Scenario, Requirements and Assumptions	72
4.2.1. Scenario	72
4.2.2. Requirements	73
4.2.3. Assumptions	74
4.3. Related Work	74
4.4. Communication Process	76
4.4.1. Components of the Communication Process	77
4.4.2. Data Flow of the Communication Process	78
4.5. Evaluation	79
4.5.1. Qualitative Evaluation	79
4.5.2. Quantitative Evaluation	80
4.6. Lessons Learned	83
4.7. Concluding Remarks	84
5. Selection of an Appropriate Response	85
5.1. Introduction	85
5.2. Scenario	86
5.3. Requirements and Assumptions	87
5.3.1. Requirements	88
5.3.2. Assumptions	89
5.4. Related Work	89
5.4.1. Evaluating the Impact of Automated Intrusion Response Mechanisms	90
5.4.2. Adaptive Intrusion Response using Attack Graph	91
5.4.3. A Framework for Cost Sensitive Assessment of Intrusion Response Selection	94
5.4.4. Topological Vulnerability Analysis	94
5.5. REASSESS - Response Effectiveness Assessment	96
5.5.1. Reaction System Concept	96
5.5.2. Calculation Methodology	97
5.5.3. Proof of Concept	99
5.6. Evaluation	104
5.6.1. Evaluation Methodology	104
5.6.2. Evaluation Results	105
5.6.3. Evaluation Summary	110
5.7. Lessons Learned	112
5.8. Concluding Remarks	113

6. DDoS Defense using MTD and SDN	115
6.1. Introduction	115
6.2. Terminology of MTD and SDN	116
6.2.1. Moving-Target Defense	117
6.2.2. Software-Defined Networking	117
6.3. Scenario, Requirements and Assumptions	118
6.3.1. Scenario	118
6.3.2. Requirements	118
6.3.3. Assumptions	120
6.4. Related Work	120
6.5. DDoS Defense Solution	122
6.6. Evaluation	122
6.6.1. Evaluation Methodology	123
6.6.2. Qualitative Evaluation Results	124
6.6.3. Quantitative Evaluation	125
6.7. Lessons Learned	130
6.8. Concluding Remarks	131
7. Trust	133
7.1. Introduction	133
7.2. Scenario and Requirements	134
7.2.1. Scenario	134
7.2.2. Requirements	135
7.3. Related Work	136
7.3.1. Terminology	136
7.3.2. Collaboration Communities	136
7.3.3. Reputation-based Trust Models	137
7.4. Trust model	138
7.5. Evaluation	142
7.5.1. Qualitative Evaluation Methodology	142
7.5.2. Quantitative Evaluation Methodology	142
7.5.3. Evaluation Results	143
7.6. Lessons Learned	145
7.7. Concluding Remarks	146
8. Conclusion & Future Research	147
8.1. Main Conclusions	147
8.2. Revising the Research Questions	148
8.3. Directions for Future research	152
A. Questionnaire of Surveys	157
A.1. Survey 2013	157
A.2. Survey 2015	168
B. Source Code Repository	181
Glossary	183

References	185
List of Figures	203
List of Tables	205
Index	207
Curriculum Vitae of the Author	211
Publications by the author	213

List of Acronyms

ACDC	Advanced Cyber Defence Centre
ADEPTS	Adaptive Intrusion Response using Attack Graph
API	Application Programming Interface
APWG	Anti-Phishing Working Group
ARF	Abuse Reporting Format
AS	Autonomous System
ASN	Autonomous System Number
ASN	Abstract Syntax Notation
BEEP	Block Extensible Exchange Protocol
BER	Basic Encoding Rules
BGP	Border Gateway Protocol
BSI	German Federal Office for Information Security
C&C	Command-and-Control
CA	Certificate Authority
CAIF	Common Announcement Interchange Format
CAPEC	Common Attack Pattern Enumeration and Classification
CEE	Common Event Expression
CER	Canonical Encoding Rules
CERT	Computer Emergency Response Team
CIDF	Common Intrusion Detection Framework
CISL	Common Intrusion Specification Language
CLI	Command-Line interface
CLS	Common Event Expression Log Syntax
CLT	Common Event Expression Log Transport
CMS	Cryptographic Message Syntax
COBIT	Control Objectives for Information and Related Technology
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposure
CYBEX	Cybersecurity Information Exchange Framework
CyBOX	Cyber Observable Expression
DAG	Directed Acyclic Graph
DARPA	Defense Advanced Research Projects Agency

DDoS	Distributed Denial of Service
DER	Distinguished Encoding Rules
DMZ	Demilitarized Zone
DNS	Domain Name System
DOTS	DDoS Open Threat Signaling
DRTBH	Destination-based Remote-Triggered Blackhole
ENISA	European Union Agency for Network and Information Security
EPTS	Event Processing Technical Society
FINE	Format for Incident Report Exchange
FIRST	Forum of Incident Response and Security Teams
FLEX	Flow-based Event Exchange Format
GÉANT	Gigabit European Academic Network
H2H	human-to-human
IAP	Intrusion Alert Protocol
IDAR	Intrusion Detection, Analysis, and Response Systems
IDMEF	Intrusion Detection Message Exchange Format
IDS	Intrusion Detection System
IDWG	Intrusion Detection Working Group
IDXP	Intrusion Detection Exchange Protocol
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
INCH	Incident Handling
IODEF	Incident Object Description Exchange Format
IoT	Internet of Things
IPFIX	Internet Protocol Flow Information Export
IPS	Intrusion Prevention System
IRS	Intrusion Response System
ISM	Information Security Management
ISP	Internet Service Provider
ITIL	Information Technology Infrastructure Library
IXP	Internet Exchange Point
JMS	Java Messaging Service
JSON	JavaScript Object Notation
M2H	machine-to-human
M2M	machine-to-machine
MAAWG	Messaging Anti-Abuse Working Group
MAEC	Malware Attribute Enumeration and Characterization
MARF	Messaging Abuse Reporting Format

MILE	Managed Incident Lightweight Exchange
MIME	Multipurpose Internet Mail Extensions
MiR	Mitigation and Response System
MIT	Massachusetts Institute of Technology
MTD	Moving Target Defense
NCC	Network Coordination Centre
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
NOC	Network Operations Center
NTP	Network Time Protocol
NVD	National Vulnerability Database
OER	Octet Encoding Rules
ONF	Open Networking Foundation
ONOS	Open Network Operating System
OS	Operating System
OSMP	Operations Security Management Process
OSVDB	Open Source Vulnerability Database
PGP	Pretty Good Privacy
PIG	Portable Intrusion Graph Generation
PKI	Public-Key infrastructure
PRI	priority value
REASSESS	Response Effectiveness Assessment
REN	Research and Education Networking
RFC	Request for Comments
RID	Real-time Inter-networking Defense
RQ	Research Question
SASL	Simple Authentication and Security Layer
SCAP	Security Content Automation Protocol
SDN	Software Defined Networking
SDX	Software Defined Exchange
SIEM	Security Information and Event Management
SIG	Special Interest Group
SLA	Service Level Agreement
SMIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SRTBH	Source-based Remote-Triggered Blackhole
STIX	Structured Threat Information Expression
STOMP	Simple (or Streaming) Text Orientated Messaging Protocol

TAXII	Trusted Automated Exchange of Indicator Information
TCP	Transmission Control Protocol
TLP	Traffic Light Protocol
TLS	Transport Layer Security
TVA	Topological Vulnerability Analysis
UDP	User Datagram Protocol
WG	Working Group
X-ARF	Extend Abuse Reporting Format
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

List of Symbols

Λ	Set of actions
Γ	Configurable system
Π	Configuration parameter type
Σ	MTD system
α	Alert (Security event)
ϵ	Entity (service)
π	Configuration parameter
τ	State transition function
S	Set of configuration states
A_n	Negative effects of a response
A_p	Positives effects of a response
$A' = \{a_0, a_1, \dots, a_m\}$	Set of alerts
D	Disruptive impact
E	Effectiveness value
$E(r)$	Effectiveness value for each response
$F_d(\epsilon)$	Capability reduction
G	Set of operational and security goals
P	Set of policies
$R = \{r_0, r_1, \dots, r_n\}$	Set of responses
$S(\epsilon)$	Importance of a service
$dps_{r_i}(a_j)$	Responses that successfully mitigate the attack
$dpt_{r_i}(a_j)$	Responses that do not successfully mitigate the attack
r	Response
s	Configuration state

*We were meant to explore this earth like children do
... unhindered by fear
.... propelled by curiosity and a sense of discovery.
Allow yourself to see the world through new eyes and
know there are amazing adventures here for you.*

UNKNOWN

Introduction

This chapter provides a short introduction to this PhD thesis and explains the motivation. Further, this chapter formulates the overall research goal and research questions. Finally, the chapter closes with an outline of this PhD thesis and a brief characterization of each individual chapter.

1.1. Motivation

Being originally described by Joseph Carl Robnett Licklider of the Massachusetts Institute of Technology (MIT) in August 1962 [M1, M2], the Internet has evolved to a vital component that heavily influences our daily life. Large majorities of users rely on the Internet on a regular basis for financial services (e.g., online banking), shopping and other customer services (e.g., access health care information, governments communication, locate jobs, watch movies) [M3]. Besides the communication and information aspect of the Internet, it has become a crucial component for millions of businesses, stock markets, public facilities and transportation hubs, power grids and water delivery systems that are controlled by networked devices [M4]. The following description of the Internet has also been published by the Internet Society in [M5]:

“ *The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location.* ”

Barry M. Leiner et al. [M5], *Internet Society*, 2012

This description primarily summarizes the benefits of the emerging technologies provided within the Internet. However, emerging technologies are also opening up new vulnerabilities that might be exploited by attackers to perform large-scale cyber attacks.

In recent years, large-scale cyber attacks targeting the availability of network infrastructure and service have been constantly reported [J1, J2, M4, M6]. These large-scale

Figure 1.1.: DDoS evolution is partially based on [J3]

cyber attacks could lead to enormous financial loss [C1, M7, M6], potentially triggering sustained power outages over large portions of the electric grid [M8] and prolonged disruptions in communications, food and water supplies, and health care delivery. An evolution of the attack intensities and related security events have been published in [J3] and are shown in Figure 1.1. However, the attack intensity of 4 Tbps was achieved by compromising software that is running on large uplinks of the Internet2 [M9, M10] network (an US research and education network) in order to calculate the total available bandwidth for an DDoS attack.

One common characteristic of these attacks is that they are referred to as large-scale cyber attacks. According to the definition of Merriam-Webster and the Tallinn Manual on the International Law Applicable to Cyber Warfare [M11] large-scale cyber attacks can be defined as follows:

“ Large-scale cyber attacks involve many devices that connote a relationship with information technology and are distributed over a large geographic area. ”

Merriam-Webster and Tallinn Manual on the International Law Applicable to Cyber Warfare [M11], 2016,

The majority of these large-scale cyber attacks are using reflection and amplification techniques while performing an attack. First, reflection is used to make publicly available network devices send attack traffic to the attack target in order to hide the attacker's identity. Usually, the attacker sets the source IP address to the target IP address and thus makes use of spoofing. As a result, the attack target receives all response packets of the publicly available network device. Second, amplification is used to increase the network packet size to overwhelm the target network. Amplification exploits the fact that response packets usually are significantly larger than the initial

Figure 1.2.: Reflection and Amplification technique of DDoS

request packet. The principles of the reflection and amplification techniques are shown in Figure 1.2.

Besides the geographic distribution and the techniques used to strengthen the attack, the attacks are either based on the two most popular transport layer protocols: Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). The majority of large-scale cyber attacks rely on UDP, because many UDP-based protocols are vulnerable to amplification due to the lack of verification of the participating communication partners [T1] and thus support spoofing. Using UDP-based protocols, an attacker can achieve network traffic up to a factor of 4670 [C2]. Even though TCP employs a three-way-handshake, it is also vulnerable for amplification as reported by Kühner et al. [C3, T1]. As reported by Kühner et al. [C4], the attacker can amplify TCP traffic by a factor of 20. Both, UDP and TCP-based attacks are volumetric attacks (floods) and are intended to reach bandwidth or connection limits of hosts or networking devices [M12].

One type of large-scale cyber attacks are DDoS attacks that still remain the top concern responsible for network infrastructure and service outages [R1]. The reason is that DDoS attacks are getting larger, more sophisticated (e.g. multi-vector attacks) and frequent as shown in Figure 1.3 (blue line). Furthermore, Figure 1.3 shows that the attack intensities on average grew by 47.24% over a time span of 43 month and will continue to grow (grey line).

At the same time it has never been easier to execute DDoS attacks, e.g., Booter services offer paying customers without any technical knowledge the possibility to perform DDoS attacks as a service via a web page [C5, M16]. Besides Booter services, it is also possible to hire a whole botnet (e.g., hire-a-botnet-services [M17]) for a DDoS campaign at low price [M18, M19]. Moreover, new technology trends in the

Figure 1.3.: Increase of attack intensities over time based on [J3, M13, M14, M15]

development of the Internet such as IoT focus to connect billions of everyday devices. These devices are designed to be user-friendly and accessible and often do not have a stringent security standard. Currently, 4.9 billion IoT units are in use [M20] and will reach 25 billion by 2020. However, the lack of missing security standards, the ease of manipulation and the amount of available everyday devices encourage attackers to perform large-scale DDoS attacks [M21].

The well-known DDoS attacks that attracted large public attention are: (i) the "SpamHaus" attack, (ii) the "NTP" attack, (iii) the attack targeting the web site of the journalist Brian Krebs and (iv) the OVH attack.

SpamHaus attack: In March 2013, SpamHaus faced a DDoS attack targeting the Spamhaus's Domain Name System (DNS) servers with traffic peaks of 300 Gbps [M14, M22, M23]. Over 30 956 unique DNS resolvers have been involved in the attack and Cloudflare was consulted to mitigate the attack. The website was unreachable and the blacklists provided by SpamHaus were not getting updated.

NTP attack: In February 2014, Cloudflare mitigated a Network Time Protocol (NTP) attack targeting one of their customers. In contrast to the SpamHaus attack, the attacker only used 4 529 NTP servers running on 1 298 different networks to create an attack traffic of 400 Gbps [M15, M24].

Brian Krebs web site attack: In September 2016, the web site of the journalist Brian Krebs faced a DNS-based DDoS with traffic peaks of 620 Gbps [M13, M25]. This attack was launched by up to 100 000 poorly secured IoT devices that have been compromised by the Mirai malware. The attack was mitigated with the help of Akamai as KrebsOnSecurity used their pro-bono arrangement. However, Akamai terminated the pro-bono arrangement and KrebsOnSecurity is now protected by a service offered by Google (Google's Project Shield) [M26]. The attack of the malicious Mirai endpoints was responsible for a nearly four days offline period of the KrebsOnSecurity web site. After analyzing the attacker and the publicly released Mirai software, Krebs found out that Mirai has been involved in other large-scale cyber attacks as well [M25, M27].

OVH: At the same time an attack was targeting the web site of the journalist Brian Krebs, the French Web hoster OVH faced a 1.1 Tbps DDoS attack. This attack was launched by a collection of hacked Internet-connected cameras and digital video recorders [M28]. Octave Klabar, the founder and CTO of OVH, suggested that his network and KrebsOnSecurity may be targeted by the same botnet.

Considering the quantity of everyday devices connected to the Internet, their mobile speed and the trend of recent attack intensities, theoretically a devastating large-scale DDoS attack might be launched [C6, M9]. To be prepared for future DDoS attacks, a new paradigm is required to mitigate their effects.

1.2. Research Goal, Research Questions & Approaches

This section presents the main research objective. In order to achieve this objective, this section introduces five research questions (RQs) that this thesis set out to explore, and it explains the used approach to answer them.

1.2.1. Main Research Goal

In the last years, DDoS evolved to one of the major causes responsible for network infrastructure and service outages. Often the amount of traffic generated by DDoS attacks is such that, although traditional security solutions as firewalls and Intrusion Prevention Systems (IPSs) are deployed, the target network will lose connectivity, because the network resources are exhausted. To optimize mitigation and response capabilities and thus reduce potential damages caused by DDoS attacks, mitigation and response should be moved as close to the source of the attack as possible. Therefore, mitigation and response should move from the target network to the networks of ISP.

1. INTRODUCTION

Additionally, ISPs should collaborate and exchange information in context of network security. Thus the main goal of this thesis is as follows:

Research Goal: *Develop a collaborative, automated approach to mitigate the effects of DDoS attacks at Internet Scale.*

1.2.2. Research Questions

The first RQ of this PhD thesis aims at gaining knowledge about established distributed and automatic mitigation in context of ISPs. Therefore, the first RQ is defined as follows:

Research Question 1: *Is distributed and automatic mitigation at ISP level performed and if yes, how?*

We analyze RQ 1 from a multi-perspective view. First, we perform a systematic review on current mitigation and response approaches, data used to detect and mitigate malicious activities and analyze the compliance to standards and frameworks. Based on these findings, we conduct a survey research as frequently used in social and psychological research [J4, B1]. We review several survey standard designs and develop two surveys - a cross-sectional and a repeated cross-sectional survey - in an interval of two years. The repeated cross-sectional survey is conducted to add additional evidence to the findings of the research results of the first survey. Both, the first and the second survey, are distributed over mailing lists of network operators and we promote the participation in the survey at the largest European research networking conference. Next, we interview experienced networking operators and networking engineers and attend the DDoS mitigation workshop offered by the Special Interest Groups (SIGs)-Information Security Management (ISM) of GÉANT¹. RQ 1 is addressed in Chapter 2 (Current DDoS Detection & Mitigation: A Survey).

Besides the aim to gain knowledge about current detection and mitigation capabilities at ISP level, we focus on collaboration among ISPs as key location for mitigation and response. Further, increasing attack intensities have shown that collaboration is required. In particular, we focus on an easy and fast form of information exchange among ISPs. Thus, we derive the following RQ:

¹<http://www.geant.org/>

Research Question 2: *How are security events currently exchanged and do they satisfy the requirements of ISPs?*

To answer RQ 2, we perform a systematic literature review [J5] on current exchange formats and protocols according to the approach described by the Cochrane Collaboration within the Cochrane Handbook for Systematic Reviews of Interventions [M29, J6]. We collate existing exchange formats and protocols in the context of intrusion detection and incident handling and take into account the results of the performed surveys. RQ 2 is addressed in Chapter 3 (Exchange of Threat Information).

In addition to the formats and protocols to exchange security information, we also focus on collaboration that supports achieving the situational awareness of the impact of an ongoing large-scale cyber attack, pools the expertise of collaborating ISPs and their resources, facilitates the automated defense in response to ongoing network-based attacks and thus lessens the time to respond. Thus, we derive the following RQs:

Research Question 3: *Is mitigation currently done in a proactive or reactive approach? If reactive, would it be possible to do it in a proactive approach?*

Research Question 4: *Is mitigation currently done manually or automatically? If manually, would it be possible to perform mitigation in an automated way?*

As the overall goal of this thesis is to develop a collaborative, automated approach to mitigate the effects of DDoS attacks at Internet Scale, the establishment of trust among collaborative partners is deemed of critical importance. Thus, we derive the following RQ:

Research Question 5: *How can trust among collaborative partners be arranged?*

To answer RQ 3 to RQ 5, we use the empirical data provided by the expertise and experience of the network administrators, network operators and networks security engineers within the surveys as a starting point of our research. The reason to use the survey as a starting point is that the provided data is based on real-world mitigation

and response capabilities and thus provides a snapshot of how things are at a specific time. We analyze the capabilities of ISPs to perform proactive and automatic mitigation, and how they arrange trust in order to satisfy their requirements to answer the remain RQs. RQ 3 is addressed in Chapter 4 (Collaboration Process), RQ 4 is addresses in Chapter 5 (Selection of an Appropriate Response) and Chapter 6 (DDoS Defense using MTD and SDN), and RQ 5 is addressed in Chapter 7 (Trust).

1.3. Thesis Contribution

The main contribution of this thesis is a systematic and multifaceted study on mitigation of large-scale cyber attacks at ISPs. By performing two surveys, we got in contact with experienced networking operators and thus gained insight into processes, structures and capabilities of ISPs to mitigate and respond to network-based attacks. Using the contact with experienced networking operators revealed potentials for improvement in their mitigation and response capabilities and it ensured that the distributed DDoS defense paradigm will be both fine-tuned and used by the intended audience. Based upon these finding, multiple aspects of a distributed DDoS defense at ISP networks were scrutinized and resulted in a multifaceted approach.

The first aspect of a distributed DDoS defense is the dissemination of threat information. We provided network operators a detailed guidance selecting an exchange format and protocol suitable to use in their network to disseminate threat information. To overcome the shortcomings of missing flow-based interoperability, we developed the exchange format FLEX.

The second aspect of distributed DDoS defense is the collaboration of ISP networks. To establish collaboration among ISP networks, a proactive and semi-automatic approach is needed and trust among collaborating partners is required.

In a first step, a communication process was developed to facilitate the automated defense in response to ongoing network-based attacks. This communication process supports the dissemination of threat information based on FLEX and helps organizations to speed up their mitigation and response capabilities without the need to modify the current network infrastructure. We demonstrated that our communication process supports achieving the situational awareness of the current threat landscape, pools expertise and resources at ISP networks, facilitates the automated defense in response to ongoing network-based attacks and thus lessens the time to respond.

In a second step, we analyze the initiation of a suitable reaction. This initiation is a process of selecting an appropriate response related to the identified network-based attack. The process of selecting a response requires to take into account the

economics of an reaction e.g., risks and benefits. We provided a response selection model that allows to mitigate network-based attacks by incorporating an intuitive response selection process that evaluates negative and positive impacts associated with each countermeasure. In addition to the process of selecting an appropriate response, the semi-automatic deployment of response actions were analyzed. Therefore, we investigate the effectiveness of the defense techniques moving-target using SDN and their applicability in context of large-scale cyber attacks and the networks of ISPs.

Besides sharing threat information and the selection of an appropriate response to ongoing network-based attacks, establishing trust among collaborative partners is deemed of critical importance to semi-automatically deploy mitigation. Therefore, we developed a trust model that determines a trust and a knowledge level of a security event in order to deploy semi-automated remediations and facilitate the dissemination of security event information using the exchange format FLEX in context of ISP networks.

The contribution in this thesis can be used by network administrators, network operators and network security engineers to better limit the effects of current and future DDoS attacks and thus prevent network infrastructure and service outages.

1.4. Thesis Organization

This section introduces the overall structure of this PhD thesis. Further, this section presents a short overview and all related publications that provide the basis for each section of the thesis.

In **Chapter 1 (Introduction)**, we have presented the motivation to this dissertation and the conceptual background of the research context, followed by the statement of the main research goal and resulting RQs. Further, Chapter 1 delineated the use-case scenario, the scope and assumptions for the thesis. Finally, the main contributions of this thesis have been addresses and the remainder structure of the thesis as a whole is presented. A use-case scenario has been published in the following publications:

- [M30]: Jessica Steinberger et al. *Real-time DDoS Defense: A collaborative Approach at Internet Scale*. Website. **Best Student Poster**. May 2014. URL: <https://tnc2014.terena.org/core/poster/21> (visited on 06/10/2018)
- [C7]: Jessica Steinberger et al. "Real-time DDoS Defense: A collaborative Approach at Internet Scale". In: *Proceedings of the 10th SPRING of the SIG Security - Intrusion Detection and Response of the German Informatics Society SIG SIDAR*. July 2015. URL: <http://www.gi-fg-sidar.de/spring/SIDAR-Reports/SIDAR-Report-SR-2015-01.pdf>

Figure 1.4.: Structure and dependence of chapters of the thesis

- [C8]: Jessica Steinberger et al. “Ludo” - Kids playing Distributed Denial of Service”. In: *Connected Communities, The Networking Conference 2016, 15-18 June, 2016, Prague, Czech Republic, Selected Papers*. Ed. by Klaas Wierenga. GÉANT Ltd, Nov. 2016. ISBN: 978-90-77559-25-3. URL: <http://www.terena.org/publications/tnc16-proceedings/>

Besides the introductory and final part of this thesis, the remainder is split up into the main parts: Chapter 2 (Current DDoS Detection & Mitigation: A Survey), Chapter 3 (Exchange of Threat Information), Chapter 4 (Collaboration Process), Chapter 5 (Selection of an Appropriate Response), Chapter 6 (DDoS Defense using MTD and SDN) and Chapter 7 (Trust) as shown in Figure 1.4.

Chapter 2 (Current DDoS Detection & Mitigation: A Survey) analyzes to what extent countermeasures are set up and which mitigation approaches are adopted by ISPs. Further, the ISP’s view on collaboration is determined. The results presented in Chapter 2 have been published in the following two publications:

- [C9]: Jessica Steinberger et al. “Anomaly Detection and Mitigation at Internet Scale: A Survey”. In: *Proceedings of the 7th IFIP International Conference on Autonomous Infr-*

structure, Management and Security (AIMS 2013): *Emerging Management Mechanisms for the Future Internet*. Ed. by Guillaume Doyen et al. Vol. 7943. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, pp. 49–60. ISBN: 978-3-642-38997-9. DOI: [10.1007/978-3-642-38998-6_7](https://doi.org/10.1007/978-3-642-38998-6_7). URL: http://dx.doi.org/10.1007/978-3-642-38998-6_7

- [C10]: Jessica Steinberger et al. “Collaborative Attack Mitigation and Response: A survey”. In: *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM 2015)*. May 2015. DOI: [10.1109/INM.2015.7140407](https://doi.org/10.1109/INM.2015.7140407)

Chapter 3 (Exchange of Threat Information) presents a structured overview of exchange formats and protocols used to share security event related information in context of intrusion detection and incident handling. Based on the results of this structured overview, this Chapter introduces the exchange format FLEX that was developed to overcome the shortcomings of missing flow-based interoperability. The results of this Chapter have been published in the following two publications and at the Internet Engineering Task Force (IETF):

- [C11]: Jessica Steinberger et al. “How to exchange security events? Overview and evaluation of formats and protocols”. In: *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. May 2015, pp. 261–269. DOI: [10.1109/INM.2015.7140300](https://doi.org/10.1109/INM.2015.7140300)
- [M31]: Jessica Steinberger et al. *Exchanging Security Events of flow-based Intrusion Detection Systems at Internet Scale*. Website. June 2015. URL: https://www.iab.org/wp-content/IAB-uploads/2015/04/CARIS_2015_submission_3.pdf (visited on 12/28/2015)
- [M32]: Jessica Steinberger. *FLEX*. Website. July 2015. URL: <https://datatracker.ietf.org/meeting/93/materials/agenda-93-mile/> (visited on 12/12/2017)

Chapter 4 (Collaboration Process) presents a communication process that facilitates the dissemination of threat information that are created in conjunction with widely adopted monitoring technologies e.g., NetFlow. The communication process uses the exchange format FLEX to exchange security event information. The results of this Chapter have been published in the following publication:

- [C12]: Jessica Steinberger et al. “Collaborative DDoS Defense using Flow-based Security Event Information”. In: *Proceedings of the 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS 2016)*. Apr. 2016. DOI: [10.1109/NOMS.2016.7502852](https://doi.org/10.1109/NOMS.2016.7502852)

Chapter 5 (Selection of an Appropriate Response) provides a process of selecting an appropriate response related to the identified network-based attack in order to initiate a suitable reaction. Therefore, Chapter 5 provides a response selection model that allows to mitigate network-based attacks by incorporating an intuitive response selection process that evaluates negative and positive impacts associated with each countermeasure. The results of this Chapter have been published in the following two publications:

- [C8]: Jessica Steinberger et al. “Ludo” - Kids playing Distributed Denial of Service”. In: *Connected Communities, The Networking Conference 2016, 15-18 June, 2016, Prague, Czech Republic, Selected Papers*. Ed. by Klaas Wierenga. GÉANT Ltd, Nov. 2016. ISBN: 978-90-77559-25-3. URL: <http://www.terena.org/publications/tnc16-proceedings/>
- [C13]: Sven Ossenbühl, Jessica Steinberger, and Harald Baier. “Towards Automated Incident Handling: How to Select an Appropriate Response against a Network-Based Attack?” In: *Proceedings of the Ninth International Conference on IT Security Incident Management IT Forensics (IMF)*. May 2015, pp. 51–67. DOI: [10.1109/IMF.2015.13](https://doi.org/10.1109/IMF.2015.13)

Chapter 6 (DDoS Defense using MTD and SDN) combines the defense techniques moving-target using Software Defined Networking to increase uncertainty due to an ever-changing attack surface and to reduce the effects of a large-scale cyber attack. The results of this Chapter have been published in the following publication:

- [C14]: Jessica Steinberger et al. “DDoS Defense using MTD and SDN”. in: *Proceedings of the 2018 IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*. May 2018. DOI: [10.1109/INM.2015.7140407](https://doi.org/10.1109/INM.2015.7140407)

Chapter 7 (Trust) presents a trust model that determines a trust and a knowledge level of a security event in order to deploy semi-automated remediations and facilitate the dissemination of security event information using the exchange format FLEX in the context of ISPs. This trust model is based on the well known Pretty Good Privacy (PGP) trust model and used to establish different levels of trust, determine the prioritization of the shared security event, sanitize the occurrence of security events and contributes to build a trust community in order to share information about cyber threats and its remediation suggestions. The results of this Chapter have been published in the following publication:

- [C15]: Jessica Steinberger et al. “In Whom Do We Trust - Sharing Security Events”. In: *Management and Security in the Age of Hyperconnectivity: 10th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2016, Munich,*

Germany, June 20-23, 2016, Proceedings. Ed. by Rémi Badonnel et al. Cham: Springer International Publishing, 2016, pp. 111–124. ISBN: 978-3-319-39814-3. DOI: [10.1007/978-3-319-39814-3_11](https://doi.org/10.1007/978-3-319-39814-3_11). URL: http://dx.doi.org/10.1007/978-3-319-39814-3_11

Chapter 8 (Conclusion & Future Research) provides an overview of the key findings of the thesis and an outlook into future work.

Current DDoS Detection & Mitigation: A Survey

2

This chapter describes the survey research method used to gather information about current detection and mitigation approaches deployed in ISP networks. In particular, the components and approaches to retrieve the data are presented and the main findings of the survey research are analyzed and discussed. This chapter is based on the two publications:

[C9]: Jessica Steinberger et al. “Anomaly Detection and Mitigation at Internet Scale: A Survey”. In: *Proceedings of the 7th IFIP International Conference on Autonomous Infrastructure, Management and Security (AIMS 2013): Emerging Management Mechanisms for the Future Internet*. Ed. by Guillaume Doyen et al. Vol. 7943. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, pp. 49–60. ISBN: 978-3-642-38997-9. DOI: [10.1007/978-3-642-38998-6_7](https://doi.org/10.1007/978-3-642-38998-6_7). URL: http://dx.doi.org/10.1007/978-3-642-38998-6_7

[C10]: Jessica Steinberger et al. “Collaborative Attack Mitigation and Response: A survey”. In: *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM 2015)*. May 2015. DOI: [10.1109/INM.2015.7140407](https://doi.org/10.1109/INM.2015.7140407)

2.1. Introduction

Motivated by the Introduction (Chapter 1) of this thesis and in accordance to a study performed by van Eeten et al. [C16], we believe that ISP networks to be key points for network-based attack detection and mitigation. Additionally, ISPs should collaborate to share and exchange information in the context of network security [M33], in order to support proactive detection, real-time and automatic mitigation of current types of attacks.

Recently the network security scientific community also discusses the advantages of network-based anomaly detection on base of NetFlow data [M34]. NetFlow is more feasible at Internet scale as e.g. raw packet data, because it is created by packet forwarding devices and preserves users’ privacy. François et al. [C17] and Bilge et al. [C18] propose a NetFlow-based detection mechanism for detecting botnets Command-and-Control (C&C) traffic at large-scale networks.

But how do ISPs currently detect and mitigate large-scale DDoS attacks in practice? Do ISPs currently collaborate? Do ISPs currently share and exchange security event/incident information with other providers in a standardized format? Will an approach relying on collaboration and the exchange of status information with third parties be adopted by ISPs? In this chapter, we investigate how network operators detect, mitigate and respond to network-based attacks in practice. In order to achieve insight into real-world processes, structures and capabilities of IT companies and their computer networks, we performed a survey research on the basis of two surveys conducted in the year 2013 and 2015.

2.2. Survey Research Method

This section introduces the used survey research method of this thesis. In particular, the design and conduction of the survey research method is presented. We describe the components of the survey, the methods of data collection, the nonresponse bias and the data cleaning process.

2.2.1. Components of the Survey

We set up our survey research according to the common procedures and standards for good practice of survey research described in Fowler [B2] and Rea and Parker [B3]. The survey research defines the survey sampling, the design of a questionnaire and nonresponse.

Sample

According to Fowler [B2] a sample represents a population that depends on the sample frame, the sample size, and the specific design of selection procedures. A set of people that have the chance to be selected constitute the sample frame. The sample size determines the minimum size of the sample frame that can be tolerated for the smallest subgroup of importance.

Design of Questionnaire

The survey was designed according to Rea and Parker [B3] and consists of introductory, sensitive and related questions. Introductory questions lead to the subject matter of the questionnaire and are easy to answer. Further, introductory questions are intended to stimulate the respondent's interest to participate in the survey. Questions related to the amount of attack traffic, established attack detection and mitigation

approaches, affiliation and own opinions regarding detection and mitigation are covered by sensitive questions. Related questions are used to gather more details on a topic and are usually placed as follow-up questions. Related questions have an impact on the sequence of questions.

The type of questions within a questionnaire are either closed-ended or open-ended questions. Closed-ended questions provide response choices or categories presented in a fixed list for selection. In contrast to closed-ended questions, open-ended questions have no preexisting response categories and are presented as a free-text field within the survey. The advantage of closed-ended questions is that they facilitate the comparison and analysis of the survey results, whereas open-ended questions might result in ambiguity.

Nonresponse

Nonresponse describes the fact of missing data. The reason of missing data is manifold. First, the survey does not reach its intended audience and thus is not answered by them. Second, the participant refuses to give an answer to a single or multiple questions or might abort the survey. Finally, the respondent was unable to answer the question. However, the sample containing nonresponses has to be identified and an approach to cope with item nonresponse has to be established.

2.2.2. Methods of Data Collection

This section describes the approach to obtain a representative sample and the question design of our questionnaire. Further, this section presents the adjustments of our sample due to nonresponse.

Sample

In order to obtain a representative sample that represents network administrators, network operators and network security engineers working in the area of detection and mitigation, we provided two web-based surveys. We distributed our survey over several relevant mailing lists of network administrators, network operators and network security engineers listed in Table 2.1 and ask for their participation. However, the mailing list of the Association of the German Internet Industry was only used to disseminate the survey among their participants during the survey performed in 2013. The selection procedures of the survey participants can be described as nonprobability sampling. As described by Rea and Parker [B3], the knowledge of the population is

Table 2.1.: Overview of mailing lists

Name, URL
European IP Networks forum RIPE, http://labs.ripe.net
German Network Operators Group DENOG , http://www.denog.de
DE-CIX competence group security, http://www.de-cix.net
Swiss Network Operators Group SwiNOG, http://www.swinog.ch
North American Network Operators Group NANOG, http://www.nanog.org
Competence Center for Applied Security Technology, http://www.cast-forum.de
Advanced Cyber Defence Centre for Europe, http://www.acdc-project.eu
Trans-European Research and Education Networking Association, http://www.terena.org
Association of the German Internet Industry, http://international.eco.de

limited and the probability of selecting any given unit of the population cannot be determined.

The answers of both, the first and second survey were collected with the aid of an online system accessible via web browser. The advantage of an online system is that participants receive the questionnaire and complete it in the privacy of their home or office.

In order to maximize the sample size and the accuracy with which the questions are answered, we promote the participation in the second survey at the largest European research networking conference. Next, we interviewed experienced networking operators and networking engineers and attend the DDoS mitigation workshop offered by the SIGs-ISM of Gigabit European Academic Network (GÉANT).

Design of Questionnaire

The surveys consist of introductory, sensitive and related questions. The introductory questions are of a basic, factual nature and covers questions related to the company and the respondent's role within the company. Sensitive questions deal with questions related to the traffic transported within the respondent's network and used attack detection and mitigation approaches. Related questions are linked to previous questions and are shown up only on certain answers (e.q., (Q9=Yes)). Therefore, the length of the survey for each respondent might vary. The questionnaire of both surveys can be found in Appendix A.

The first survey (see Appendix A.1) consists of 56 questions related to 6 categories. These categories adhere a number of questions and are listed in Table 2.2. The third column of Table 2.2 provides an aggregated overview, how many questions in each category are completely answered by all participants. The last column pair of Table 2.2 displays the number of participants on average, who answered so called level 1 and 2

Table 2.2.: Overview of the survey 2013

Category	# of ques- tions	# of complete category answer set	# of complete an- swers on average	
			1. Level	2. Level
Company and personal info	9	3 out of 9	74	17
Attacks and threats	5	2 out of 5	87	-
Data and tools	17	8 out of 17	47	26
Mitigation and reaction	11	4 out of 11	69	10
Role of ISPs and IXPs	9	2 out of 9	45	23
Contact information	5	0 out of 5	12	-

questions. Level 1 denotes questions that were available for all attendees, whereas level 2 refers to follow-up questions.

The introductory question are covered in the category 'Company and personal information'. These ask questions regarding the organizational type, location of the organizations headquarter, the working experience and the role of the survey respondents. The category 'Attacks and threats' gathers information about information sources that are used by ISPs to keep-up-to-date and to raise their security awareness. Further, this category ask questions regarding actual detected attacks and threats. The category 'Data and tools' asks the participants about the acquired data and tools to detect attacks. Within the category 'Mitigation and reaction', we collected information about the tools our respondents use to mitigate and respond to network-based attacks. Within the category 'Role of ISPs and Internet Exchange Points (IXPs)', we gathered information about their subjective view of the role of an ISP and an IXP in network attack detection and mitigation. The last category 'Contact information' covers sensitive data and collects the name and email address of the participant. The answer to the last category is optional.

The second survey (see Appendix A.2) consisted of 52 questions related to 5 categories. These categories include a number of questions that are summarized in Table 2.3. The category 'Organization and personal information' asks questions regarding the organizational type, location of the organizations headquarter, the working experience and the role of the survey respondents. Further, we ask about their ability to reconfigure border routers and the average network traffic transported over their border routers. The category 'Process and involved third parties' gathers information about internal and external parties involved in the mitigation and reaction process. Within the category 'Automatic mitigation and response systems', we collected information about the tools our respondents use to mitigate and respond to network-based

Table 2.3.: Overview of the survey 2015

Category	# of questions	# of answers
Organization and personal info	8	42
Process and involved third-parties	9	38
Automatic mitigation and response systems	11	35
Data	18	31
Exchange and Collaboration	6	28

attacks, the quantity of security events and incidents, and the attack mitigation on average. Further, we ask question regarding the accuracy of the automatic detection and mitigation systems. The category 'Data' gathers information about the use of publicly available security event data and their inclusion into the mitigation and response process. Besides the available data sources, this category also covers DDoS protection networks, the use of BCP 38 and the use of network configuration protocols. Within the last category 'Exchange and Collaboration', we asked questions regarding a collaboration between third parties and the exchange of security related information.

Within the first survey, only some questions were required. As a consequence, the result set of each question varies as questions could be skipped. To avoid different amount of answers for a single question within the questionnaire, all questions in the second survey were required. In case a respondent declined to answer one question of the second survey, the respondent had to skip the remaining questionnaire and quit the survey. As a result, the amount of collected answers decreases in case all questions are required.

The majority of questions have closed-ended response choices or categories. A couple of questions have been designed as open-ended questions, where participants have no preexisting response categories and find a free-text form field. In some cases, the questionnaire is designed to use follow-up open-ended questions to gather data that cannot be answered within the fixed-answer format of an closed-ended question.

2.2.3. Nonresponse Bias

To handle the incompletely answered questions within the first survey, we proceed as follows. If the question belongs to the first or last category of Table 2.2, no further data preparation is necessary. In case of the remaining 4 categories, we simply scale the reference point down from 135 to the number of actual answers, which yields a distinct size of these result sets. As each question could be analyzed isolated with regard to their cross-connections, there is no distortion in our results.

Within our second survey, 51 of the 93 data sets are incomplete. In particular, none of the 51 respondents completed the first question and thus do not provide any data at all. Therefore, we disregarded these data sets. The reason for incompleteness is that respondents decline to give the requested information or abort the survey before completion. Within survey 2, a total of 42 respondents submitted valuable data.

2.3. Survey Results

In this section, we present the main results of our two surveys and discuss their respective relevance. Section 2.3.2 provides information about the compliance of standards and frameworks in the context of ISPs and shows our results how ISPs rate the risk of common threats and what raises their awareness. In order to assess the feasibility of future detection approaches, section 2.3.2 identifies techniques and data that are available for detecting anomalous events. Section 2.3.2 shows that currently no mitigation with respect to third-parties is implemented and no standardized exchange formats are in use. Finally, we discuss in section 2.3.2 the self-assessment of providers about their role in network defense.

Section 2.3.3 provides information about the mitigation and response process and other involved third-parties. Further, section 2.3.3 describes which automatic mitigation and response are in place and what kind of automatic mitigation and response methods are used. Moreover, section 2.3.3 shows which external available data ISPs and network operators consider important and include into their mitigation and response process. Finally, we discuss the exchange of security events/incidents and collaboration among Internet Service Providers and network operators in section 2.3.3.

2.3.1. Sample

This section describes the approach to translate the survey data for further analysis.

As described in subsection 2.2.2, the data of both surveys were collected with the aid of an online system. This system provides the capability to download the survey results in several file formats, including as CSV, PDF, SPSS or XLS files for further analysis. We used CSV files for further analysis.

During our first survey, we collected the answers over a time period of two weeks and got 135 participants. The second survey collected answers over a time period from May to July in the year 2014 and attracted 93 participants. In the result set of our first survey, 88 of the 135 data sets are somehow incomplete. The second survey contains 51 incomplete data sets out of 93. Using the approach described in subsection 2.2.3, a total of 67 respondents have submitted valuable data concerning their geographic

Table 2.4.: Overview of the market segment and frequency of the second survey

Organization	Abbr.	Frequency
CDN/Content Delivery	CDN	2%
Cloud Service Provider	Cloud SP	2%
Educational/Research Institution	ERI	31%
Hosting/Data Center/Co-Location Services	Hosting	7%
Managed Service Provider	Managed SP	2%
National Research and Education Network provider	NREN	31%
Other	—	6%
Tier 1 Service Provider	Tier 1 SP	7%
Tier 2/3 Service Provider	Tier2/3 SP	12%

provenance and their business segment for the first survey. For the second survey, a total of 42 respondents have submitted valuable data concerning their geographic provenance and their business segment.

Both, Figure 2.1 and Figure 2.2 visualize the distribution of our anonymous participants by four characteristics in a treemap [B4]. A treemap is used to visualize multidimensional, hierarchical data and their relationships. The size of each rectangle is proportional to the number of times a certain combination occurred.

Our four characteristics are geographic region, market segment, role of employee (who answered the questionnaire) and finally the monthly average traffic transported over the respondent’s network border router (denoted as x). As shown in both, Figure 2.1 and Figure 2.2, the majority of the participants are headquartered in Europe. Within the first survey, the majority of participants classified their company as Carrier/Telco/ISP and transport on average more than 100 Gbit per second. Within the second survey, the majority classified their company as National Research and Education Network provider and the average traffic rate transported over the respondents’ routers vary between 1 – 5 and 11 – 50 Gbits per second. Besides these four characteristics, our respondents have been working in the field of IT or security with an average of 16 years. Further, they hold their current position with an average of 9 years. All of our respondents have the capability to reconfigure access or border routers. In both surveys, the majority of our participants reside in Europe and thus our results are expected to be valid for at least the European context.

Table 2.4 lists the market segment, the abbreviation of the market segment and the number of times a market segment was selected by a respondent in relation to the total number of responses for the second survey.

Figure 2.1.: Geographic and business segment information of our participants: Survey 2013

2. CURRENT DDOS DETECTION & MITIGATION: A SURVEY

Figure 2.2.: Geographic and business segment information of our participants: Survey 2015

Table 2.5.: Overview of the compliance to common standards

Standard	ITIL	COBIT	ISO 27000	German Grund- schutz	Grund-
Compliance rate	8%	1%	9%	1%	

2.3.2. Survey 2013

In this section, we present the results of our survey research performed in the year 2013.

Compliance to Security Standards and Frameworks

Being compliant to established standards and frameworks is a common approach to enhance security, however a minority of the responding ISPs actually makes use of them (see Table 2.5).

In the area of IT Service Management the best practice library called Information Technology Infrastructure Library (ITIL) is widely known and established [M35]. ITIL describes a process called ISM, which focuses on alignment of IT security with business security and ensures that information security is effectively managed in all service and management activities (e.g. with respect to the classical security goals information availability, confidentiality, integrity, authenticity). Solely 8% of 135 participants adhere ITIL.

A framework for governance and management of enterprise is called Control Objectives for Information and Related Technology (COBIT). COBIT provides a document called COBIT Security Baseline, which covers security in addition to all the other risks that can occur with the use of IT. COBIT is only implemented by 1% of our participants.

The standard series ISO/IEC 27000 [M36] provides best practice recommendations on ISM, risks and controls within the context of an overall ISM system. Like ITIL only 9% of the respondents adhere to the standards ISO/IEC 27000. Finally, the *IT-Grundschutz* from the German Federal Office for Information Security (BSI) is used by only 1% of the respondents. It uses a holistic approach in various catalogs.

To sum up, providers do not comply to common security standards. We assume that there are two main reasons for the absence of security standard compliance of ISPs. First, as shown in section 2.3.2 ISPs do not see a financial incentive to do so. Second the standards only provide a coarse-grained view of IT security related issues, which does not fit well to the segment of ISPs. Especially to the best of our knowledge there is no well-defined process model to detect and mitigate anomalous events in network

traffic. Having said that we think if such a process model existed, more ISPs would spend resources to adopt these processes to their business and therefore support the detection and mitigation of network attacks. Hence standardized network defense models at ISP level including detection and mitigation is needed.

Attacks and Threats

The results of our survey given in this section are twofold: First we show which information sources are used by ISPs to keep up-to-date and to raise their security awareness. Second we present results about actual detected attacks and threats against their networks.

With respect to awareness of common threats we are interested to know about reasons that raise the awareness of the 135 participants. As expected the most common source is an attack to the ISP's or its customers' infrastructures, respectively, namely in each case 24%. Presentations and discussions at conferences are close behind with 19%. They are followed from publications in journals, magazines, websites and mailing lists and used by 18%. Legal and regulatory requirements are an insignificant source and only used by 12%. The result shows that besides incidents in their particular networks publications at conferences or in magazines are used and an important way to raise the awareness.

Concerning information sources, the most important way to inform about new attacks and threats are websites, blogs and feeds with 28%, followed from mailing lists with 27%. Security conferences are only marginal relevant and only used by 12%. The same holds for scientific publications which are relevant for 9%. This result can be attributed to the fact that ISPs need a fast and pragmatic solution to detect and mitigate an attack. Incident information is spread much faster via non-reviewed channels such as web sites or mailing lists. We assume that there is a great challenge and a demand for close collaborations of ISPs and the security research community, so that both parties could benefit from each other's knowledge and experiences to reach expedient results in this area.

Next we turn to results about actual attacks against the ISPs infrastructures. For 49% of our 54 participants answering this question the number of detected attacks per month is at most 10 and thus rather low. On the other hand 9% detect at least 500 attacks per month to their or their customers' infrastructure. The risk assessment as shown in Figures 2.3a and 2.3b) reveals that common threats only pose a *very low* or *low* risk to ISP's or their customers' infrastructure, respectively. Denial of Service attacks pose the most common threat to the ISP's infrastructure (risk is *high* or *very*

Figure 2.3.: Risk assessment of threats

high), which accords to the result of the Arbor security report 2012 [R2]. On the other hand at their customers' infrastructure the most widespread risk is a targeted attack.

To summarize the results of this section, the awareness of threats should be raised, especially on base of scientific results. This could e.g. be achieved by dissemination activities in academic venues as well as among operators. Furthermore we see a demand for close collaborations between industry and security research community to ensure a fast exchange of experience and knowledge to gain purposeful results.

Data and Tools

As stated in the introduction the locality at an ISP node offers great possibilities for real-time detecting and correlating anomalous events. In this section, we provide the results of our survey with respect to acquired data and tools to detect attacks.

In section 2.1, we discussed different kinds of data sources for anomaly detection. We are interested, if flow data is available for anomaly detection. Once again we consider this to be important to assess the feasibility of current scientific anomalous detection approaches, especially the promising algorithms based on network flow data [C17, C18, C19]. Flow data contains statistical network information about a unidirectional data stream between two network devices in a certain time frame (e.g. source/destination IP address, source/destination port etc.). There are different network flow formats. The common ones are NetFlow [M34] developed by Cisco, its successor Internet Protocol Flow Information Export (IPFIX) [F1], and sFlow [M37].

2. CURRENT DDOS DETECTION & MITIGATION: A SURVEY

Figure 2.4.: Data used for attack detection

Figure 2.4a shows the results to the question, which kind of data the companies currently use for attack detection. The number of responses is 31. The majority of 61% actually use Simple Network Management Protocol (SNMP) data, a protocol for exchanging management information between network devices. SNMP is just like NetFlow a passive measurement technology, however, NetFlow provides the advantage of containing more detailed information. So, also shown in Figure 2.4a, SNMP data is closely followed by NetFlow data and other server logs, namely in each case 58%. Additional flow formats like sFlow and IPFIX are used by 29% and 32% of the attendees. On the other hand only a small minority of 10% make use of raw packet data for the anomaly detection.

The next questions address the technical ability to collect the three common flow data formats. The outcome is illustrated in Figure 2.4. Concerning NetFlow (version 5 or version 9) 33 of the 47 participants and hence 70% answering this question provide this possibility. The availability to collect sFlow is given by 24 of 43 responding participants, i.e. 56%. However, only 4 of 36 replying attendees (corresponding to 11%) are able to collect IPFIX data with the current company's infrastructure. But IPFIX is much newer than NetFlow, which perhaps explains this fact.

Finally we aim at comparing flow-based algorithms to the well-known deep packet inspection. We first asked for the technical ability to perform a deep packet inspection, i.e. to collect raw packet data. Although 73% of the 49 responding participants have the ability to do that, only 50% of them think that this is a feasible approach. Their main

argument against collecting raw data is the huge amount of network traffic to process. Furthermore 56% of them think, that raw packet data endangers the customers' privacy and requires too much human resources. Further mentioned disadvantages of deep packet inspection are the financial investment (44%) and a prohibition by legal or regulatory requirements (44%). To our mind flow data is privacy friendly. To support this claim we asked the participants if collecting and processing NetFlow data is superior in protecting the customers' privacy to collecting and processing raw packet data. 63% of the 41 respondents agree and 37% disagree to this statement.

In summary, flow-based data sources, such as NetFlow, are common, available and privacy-friendly data sources at network nodes. They thus present techniques for detecting anomalous events in networks. These results support our assumption that there is a demand for network-based anomaly detection systems based on NetFlow data.

Mitigation and Reaction

Although incident response requires mitigation and reaction, a significantly lower proportion of publications related to this topic is published in the last years compared to detection and correlation approaches. We aim at contributing to the current state of mitigation and reaction processes at network operators.

Our first outcome addresses the time to respond to an attack. Nearly 50% of 43 respondents are able to initially mitigate attacks within 20 minutes. To completely resolve an attack the majority requires up to one day. This is consistent to the results of [R2].

Our next question inquires about measures implemented to mitigate an attack. Figure 2.5a depicts the results if the attack targets the operator's infrastructure itself. Currently 36% of 135 attendees use access-control lists and 29% use a firewall to mitigate the attack. IPSs, Source-based Remote-Triggered Blackhole (SRTBH), and Destination-based Remote-Triggered Blackhole (DRTBH) only play a minor role. Figure 2.5b shows the distribution of the measures used to mitigate network attacks targeting the company's customer. The results are similar to the outcome of the company's infrastructure itself. Again our results are in accordance with the results reported in [R2].

Early warning systems require incident information sharing with external third parties (e.g. customers, vendors, competitors, Computer Emergency Response Team (CERTs)). However, if an attack is observed the majority of 67% of the 46 respondents do not share attack information. Additionally the 15 attendees sharing information do not use a standardized format for automated data exchange. 13 of them exchange

2. CURRENT DDOS DETECTION & MITIGATION: A SURVEY

Figure 2.5.: Measures used to mitigate network attacks

Table 2.6.: Overview of event exchange formats

Name	Abbr.	Responsible
Intrusion Detection Message Exchange Format	IDMEF	IETF
Incident Object Description Exchange Format	IODEF	IETF
Messaging Abuse Reporting Format	MARF	IETF
Extended Abuse Reporting Format	x-ARF	eco
Common Event Expression	CEE	Mitre
Malware Attribute Enumeration and Characterization	MAEC	Mitre

incident information via email, 8 via telephone and 2 automated by a proprietary detection system. Thus no early warning takes place.

A possible explanation is the absence of a well-developed and adopted standardized exchange format for security events/incidents as mentioned in [M38]. Several efforts to standardize a number of different exchange formats failed. The reasons therefore can be summarized into three main categories: lack of data of interests, difficulty to handle the information by humans and/or machines, and finally the time of development. Nevertheless effective early warning requires automated and standardized information exchange. The community came up in the past with exchange formats, which are listed in Table 2.6.

Each exchange format has its own focus and provides special possibilities to exchange attack related information. We asked if the exchange formats are known and to which extent they are used. Figure 2.6a depicts the distribution of exchange formats, currently in use or known by our participants. On average 86% of 51 respondents do not know

Figure 2.6.: Distribution of used exchange formats

about the existence of the 6 exchange formats. Furthermore Extend Abuse Reporting Format (X-ARF) is the most known or used exchange format. Figure 2.6b shows the future plans of the attendees with respect to incident exchange formats. The majority of them do not focus to establish the usage of exchange formats. In fact a few of the participants plan to use some of the mentioned exchange formats. Only the exchange format X-ARF shows an increased usage.

To sum up we suppose that exchanging attack detection data with third parties supports a faster detection and mitigation process. The approach to exchange network attack data with third parties requires a standardized and accepted exchange format, which is able to be used in conjunction with NetFlow data. Although X-ARF is a candidate for that purpose, a lot of convincing has to be done to establish an effective early warning system.

Role of ISP and IXP

In the last category we ask questions about the subjective view of the role of an ISP and an IXP in network attack detection and mitigation. 94% of 48 respondents answer that an ISP plays an important role in network attack detection and mitigation. Significantly less, namely 69% agree with this opinion related to the role of an IXP.

Even though 62% of 37 attendees think that there is a financial incentive to perform network attack detection and mitigation for ISPs, the remaining respondents are convinced that network security for an ISP is a loss center in a low margin industry. While 54% of 48 of the participants agree that the task of detection and analysis as well as coordination (46%) could be realized at IXP level, only 40% believe that mitigation / response might be a task of an IXP. We assume that the correlation of network security

Figure 2.7.: Cooperation with third parties

events at network operator level support the detection and mitigation of anomalies, but only 29% of the respondents consider IXP to be responsible for correlation.

Moreover, 42% of 45 respondents are convinced that ISPs shall protect their customers from Internet attacks and 58% agree to protect the Internet from attacks originating from its costumers. Alongside 27% added a comment that the appropriate way of thinking should include both perspectives. However, it remains the issue of accounting this security add-on. In particular, it was a widespread opinion that removing attack traffic reduces network traffic which reduces how much traffic they can charge their customers for. Hence, in their own perception there is no incentive for ISPs or IXPs to implement security measures. As addressed by [J7] we also assume that existing peering agreements might include security as an aspect of their service level agreement. Therefore the network operators should be interested in fulfilling these agreements.

2.3.3. Survey 2015

In this section, we present the results of our survey research performed in the year 2015.

Processes and Involved Third-Parties

As stated in the introduction, ISP nodes offer key opportunities for real-time mitigation of network-based attacks. In this section, we present the results of our survey with

respect to established mitigation processes and involved third parties. In this section, external companies are referred to as third party.

Although mitigation approaches using collaboration have been reported [J8] and national CERTs/Computer Security Incident Response Teams (CSIRTs) are established to assist organizations in mitigating and responding to a security event/incident, 50% of the respondents disclosed having a cooperation with an external third party (e.g., ISP or network protection service). Figure 2.7a shows the responses to the question of what best describes the third party. However, 17 of 19 replying participants (89%) cooperate with an ISP. Significantly fewer, namely 5% respondents cooperate with a forensic firm or a packet cleaning house (e.g., Cloudflare). The reasons for cooperation are visualized in Figure 2.7b. In the first place, collaboration is done to aid the respondents' Network Operations Center (NOC) (63% of the respondents). Further, 31% of the respondents use cooperation to augment the skill set and capacity of the organization's CSIRT (36% of the respondents) in daily business and during crisis situations.

Within the internal organization several functions and departments need to be involved in the mitigation and response processes (e.g., IT management, executive management, risk management, legal department). In fact, 92% of our respondents reported the involvement of the IT management. Significantly fewer, namely 32% disclosed to involve the executive management in the security response process. The departments of risk management and the legal department are considered to be important in the mitigation and response process by 8%.

Besides other functions and departments involved in the mitigation and response process, the construction of a knowledge base is important. Such a knowledge base is a centralized repository for knowledge about previous security events/incidents investigations and their solution, and is a machine-readable resource for the dissemination of information. It is used to defend the organizations from future attacks and support a faster and effective mitigation and response approach. Therefore, we asked our participants if their security event/incident investigation result in the production of threat indicators, which are then used to help defend the organization from future attacks. A knowledge base containing security event/incident investigations to defend the organizations from future attacks is used by 55%.

In our next question, we asked the participants about their communication with national CSIRTs. A national CSIRT is different from local CSIRT as a national CSIRT has been designated by a state. A national CSIRT is responsible for cyber protection of a state and supports the coordination of quick and effective mitigation and response to attacks. 65% of the participants report communicating with national CSIRTs, of

Figure 2.8.: Average number of attacks in relation to average traffic rate

which 85% uses email and 35% the telephone. Only 10% make use of an automatic mitigation and response system to communicate with national CSIRTs.

Automatic Mitigation and Response Systems

In this section, we describe which automatic detection and mitigation systems are in place and what kind of responses are performed to defend the network. Further, we describe how many security events/incidents and breaches our respondents experienced in the past 12 months. Besides the quantity of security events/incidents and breaches, we also describe how much time to initially mitigate an ongoing attack and how much time to completely resolve an attack is required.

Arbor Networks [R3] reported that the most significant operational threats are DDoS attacks. 68% of our respondents report that their organization has already been target of DDoS attacks. The majority (58%) faces 1 – 2 DDoS attacks targeting their organization’s infrastructure per month on average. Surprisingly, most of the DDoS attacks are detected in mid-size networks where the average traffic rate transported over network border router varies between 1-50 Gbits per second as shown in Figure 2.8¹. In contrast to mid-size networks, transport networks (such as Tier 1/2/3

¹ Both axes represent the answer options given by the multiple choice question and thus are discrete data scales. As a result, multiple points have exactly the same coordinates. To avoid overlapping data points, we make use of a jitter range. This jitter range is 0.2 on the x-axis and 0.1 on the y-axis.

Service Provider, Cloud Service Providers) only report a small amount of DDoS attacks per month on average. One reason might be that attackers predominantly target end users [R3]. Another reason might be that these service providers are not able to detect DDoS attacks as their effect within a high-speed network might be too small.

In our next question, we asked the participants to estimate the number of minutes to initially mitigate an ongoing DDoS attack. The majority (69%) of our respondents are able to initially mitigate an ongoing DDoS attack within 30 minutes. To resolve a DDoS-as-a-Service attack completely, 65% of our respondents require less than 24 hours. Significantly more time is needed by 35% of our respondents. They require between 1 and 5 days to completely resolve a DDoS attack. One finding is that those respondents who require more time to initially mitigate an ongoing DDoS-as-a-Service attack also require more time to completely resolve it.

Besides initial steps to mitigate an ongoing attack and a complete resolution of an attack, we asked our respondents how many security breaches they experienced within the past 12 months. 81% of our respondents reported 1 – 5 security breaches within the past 12 months. More than 6 security breaches are predominantly reported by Educational/Research Institutions.

Nowadays, automatic systems (such as Intrusion Detection System (IDS)) are in place to detect network-based attacks. In our next question, we asked our respondents how many security events/incidents are reported by automated detection mechanism per month on average. The majority (49%) report less than 10 security events/incidents raised by automated detection mechanisms per month on average. Automatic detection mechanisms that cause more than 500 security events/incidents per month are reported by 20% of our participants. The expectation, that the massive amount of events/incidents are reported from participants of high-speed network turned out to be false and is shown in Figure 2.9 (left side)¹. More than 500 security events/incidents were found in Educational/Research institutes. Subsequently, we asked our respondents how many security events/incidents raised by automated detection mechanisms (such as IDS, Security Information and Event Management (SIEM)) per month on average are real security events/incidents that need to be handled. The majority (74%) claim that a maximum of 10% of the reported security events/incidents on average are real security events as shown in Figure 2.9 (right side)¹.

In our next question, we asked our participants if their organization makes use of mitigation and response tools that perform automatic mitigation and reaction steps to defend the organization's network. Just over one third of our respondents reported to perform automatic mitigation and reaction steps. In case our respondents decline to use an automatic mitigation and response system, we asked if the use of those systems

2. CURRENT DDOS DETECTION & MITIGATION: A SURVEY

Figure 2.9.: Average security events in relation to average traffic rate and average true positives of reported security events

would speed up their organization's mitigation and response capabilities. 71% of the participants agree to this statement. Especially respondents who report a high number of security events/incidents caused by a detection mechanism and report a high false positive rate state that the use of an automatic mitigation and response tool would speed up mitigation and response capabilities. Subsequently, we asked the respondents who declined to use an automatic system if they plan to make use of it in the future. 62% of the participants plan or consider to use automatic mitigation and response tools and would like to perform the following mitigation and response actions: Change blocking or filter capabilities (71%), rerouting traffic (67%), rate limiting at ingress (62%), notification of involved function or departments within the organization (48%), exchange data with trusted partners (38%), quarantine machine (33%) and changing the target's IP address (14%).

Respondents who reported that their organization already uses automatic mitigation tools perform the following actions: Change blocking or filter capabilities (87%), notification of involved function or departments within the organization (54%), rerouting traffic (46%), rate limiting at ingress (46%), quarantine machine (31%), exchange data with trusted partners (15%) and changing the target's IP address (8%). The majority of these mitigation and response actions are performed using a self-built tool (77%). 54% of the respondents report to use open-source software to perform automatic mitigation and response and only 38% rely on commercial products. The reasons not to use commercial products are manifold. 57% of the respondents report that commercial products are too expensive. Followed by 43% of the participants

that do not use automatic mitigation and response tools due to the high risk of false positives.

Data

In this section, we describe the use of external, publicly available data sources that ISPs and network operators consider to be important and include them into their mitigation and response process. One benefit of the inclusion of external information is that the external information might contain additional information relevant for the mitigation and response process. In addition, they provide the opportunity to enhance available security event/incident information. External data sources, such as the Common Vulnerabilities and Exposure (CVE) database, Shadowserver and RIPE provide high-quality publicly available security related information. CVE provides common identifiers for publicly known information security vulnerabilities. Each CVE identifier includes a brief description of the security vulnerability or exposure and a pertinent reference. Shadowserver provides a report service that gives information about compromised servers, malicious attackers and the spread of malicious software. RIPE Network Coordination Centre (NCC) provides statistics (e.g., on specific IP prefixes and Autonomous System Number (ASNs)) and tools (e.g., network management or routing tools). Therefore, we asked our participants if they make use of these particular data sources. The CVE database is used by 52% of the participants. Information published on RIPE is used by 35% and on Shadowserver by 16%. However, 29% of the respondents answered that they do not make use of any external data source.

Other external data sources are black, white and greylists. Blacklists contain IP addresses or domain names and are used to block network traffic from the indexed systems. Conversely, whitelists contain IP addresses or domain names that produce network traffic which is allowed to bypass content or IP filters. Greylists describe a method of blocking network traffic based on the behavior of the sending server, rather than on the content of the messages. One defense mechanism described in the literature is IP filtering [J9]. IP filtering is a mechanism that decides, on the basis of the IP address within the datagram, which types of IP datagrams will be processed and which will be discarded. As IP filtering might filter out legitimate traffic, only 48% of the participants report making use of traffic filtering based on IP blacklists, whitelists or greylists. But all respondents who claim to use IP filtering report using a blacklist filtering approach, whereas only 53% of the respondents also report using whitelists and only 33% report also using greylists.

From the responses to the next question, we gathered information about the update frequency of the used black-, white- and greylists. These lists are updated once or

Figure 2.10.: Cloud-based services

more than once a day by 47% of the participants. 40% of the participants update their lists more than once per week and the remainder of our participants (13%) update their lists when necessary. In a subsequent question, we asked our respondents if they immediately include changes in the black-, white- and greylists during an update process without further review. 67% of the respondents reported to immediately include the changes in the black-, white- and greylists without further review.

Black-, white- and greylists are offered by several providers (e.g., Spamhaus, DNSWL, Spamcop). We asked our participants from which provider they obtain black, white and greylists. Those from Spamhaus are used by 60%, from Spamcop by 40% and DNSWL by 33%.

Besides the use of external data sources, a Study Group of the International Telecommunication Union's (ITU) Telecommunication Standardization Sector (ITU-T) published a framework called the Cybersecurity Information Exchange Framework (CYBEX) or X.1500 [J10]. The ITU is the United Nations specialist agency for information and communication technologies. CYBEX describes how cybersecurity information is exchanged between cybersecurity entities on a global scale and how the exchange is assured. As of September 2013, CYBEX resulted in seventeen standards within ITU-T (Recommendation ITU-T X.1500). CYBEX includes structured Information (e.g., SCAP, CVE, CVSS, CWE, Common Event Expression (CEE), Incident Object Description Exchange Format (IODEF), Malware Attribute Enumeration and Characterization (MAEC), X.gridf), an identity trust cluster (e.g., X.evcert, X.eaa) and an exchange cluster (e.g., X.cybex-beep, X.cybex-tp). Even though CYBEX is now a standard, none

of our participants makes use of CYBEX or even include parts of its framework. Our respondents point out that this framework includes seventeen standards and thus is too complex.

Another approach mitigating and responding to network-based attacks is a cloud-based approach. Cloud-based detection and mitigation solutions are offered by several companies (e.g., Cloudflare, Incapsula). These services redirect the network traffic and drop malicious network datagrams. In particular, cloud-based detection and mitigation solutions work like a network traffic "washing machine" [M39]. In our survey, we asked our participants if they would make use of a cloud-based mitigation and response solution. Figure 2.10a shows that only 26% of our respondents would make use of them. The reasons not to make use of cloud-based solutions are visualized in Figure 2.10b. The majority (64%) of our respondents claim that the data should remain in the organization's own network. Further reasons not to use cloud-based detection and mitigation is customer's privacy for 45% of the participants and an unknown impact for 54%.

In addition to external data sources and cloud-based mitigation and response, we asked our respondents if their network devices are configured according to BCP 38 (RFC 2827 or RFC 2267)[F2], because BCP 38 is a well-known standard to mitigate spoofing and thus DDoS-as-a-Service attacks. Although the attack target cannot enforce the origin ISP to implement BCP 38 and thus its intention of mitigation DDoS-as-a-Service is questionable, 77% of our participants have already implemented BCP 38.

In our next question, we ask if the respondents use network configuration protocols to configure network devices. The majority (74%) of our respondents makes use of network configuration protocols. 68% of our participants report to use the SNMP. Significantly fewer respondents use Netconf [F3], namely 19%. OpenFlow and Command-Line interface (CLI) based configuration protocols are used by only 6% of the participants.

Moving Target Defense (MTD) [C20, C21] is a use case of SDN and describes a constantly adapting environment in order to mitigate DDoS-as-a-Service attacks. Therefore, we asked our respondents about their technical ability to use OpenFlow. Currently, the majority of the respondents (71%) do not have the technical ability to use OpenFlow to configure network devices, but 69% plan or consider to have the technical ability to use OpenFlow in 3 years.

Besides BCP 38 and MTD, Border Gateway Protocol (BGP) FlowSpec [F4] introduces traffic filtering rules to mitigate DoS and DDoS attacks. To be able to use BGP FlowSpec, the routers must use BGP's Capability Advertisement facility in order to exchange the Multiprotocol Extension Capability Code [F5]. Due to this reason, we asked our

Figure 2.11.: Sharing threat indicators or security events/incidents with several entities

participants about their technical ability to use BGP FlowSpec. Currently, 52% of the respondents do not have the technical ability to use BGP FlowSpec. The majority of the participants (69%) does not even plan to use BGP FlowSpec in 3 years.

Exchange and Collaboration

In this section, we describe if our respondents report collaborating and exchanging security events/incidents. One advantage to collaborate and share information is that mitigation and response changes from a reactive to a proactive approach. Another benefit is that security events/incidents identified by the detection algorithms can be verified by trusted partners to reduce the probability of false positives.

Therefore, we asked our respondents to rate the statement, that collaboration between trusted parties would improve mitigation and response capabilities. Even though 96% of our participants strongly agreed or agreed with the statement, Figure 2.11 shows that the majority of the participants (50%) do not share threat indicators. In contrast, 69% of our participants share security events or incidents. The majority of the participants report sharing threat indicators (46%) or security events/incidents (61%) with various CERTs or CSIRTs. Significantly fewer respondents, report sharing threat indicators (21%) or security events/incidents (25%) with law enforcement or other governmental entities. In the absence of widespread collaboration between trusted partners to mitigate and respond to network-based attacks, a trusted approach

to transmit security events/incidents has not yet been established. Thus, a non-trusted approach to exchange security events/incidents is used by 54%.

To exchange security related information, several exchange protocols and formats have been published. Each exchange format has its own focus and provides facilities to exchange security related data. We asked if the exchange formats and protocols are known and to which extent they are used. Figure 2.12 shows the distribution of the exchange protocols and formats, currently in use or known by our participants. The bars from x.cybex-beep to Intrusion Detection Exchange Protocol (IDXP) represent exchange protocols. The remainder of the bars represent exchange formats. The majority of our participants had heard of the Security Content Automation Protocol (SCAP). SCAP was developed by the National Institute of Standards and Technology (NIST) and is a U.S. Government standard from 2006 for automating vulnerability management and policy compliance. But only 4% of our respondents make use of the exchange protocol SCAP and IDXP. As shown in Figure 2.12, X-ARF is the most known or used exchange format. X-ARF was developed by a competence group called "E-Mail" of eco - Association of the German Internet Industry [M40] and is a format to exchange both computer security incidents and attack data by e-mail. Besides X-ARF, IODEF is also known and used by our attendees to exchange security related data. In contrast, 79% of our respondents, on average, do not know about the existence of these particular exchange formats or protocols. These findings are in accordance with a study performed by Steinberger et al. [C9]. A possible explanation is the absence of a well-developed and adopted standardized exchange format or protocol for security events/incidents as discussed in [M38]. Several efforts to standardize the various formats and protocols failed. The reasons, why standardization efforts failed, can be summarized into three main categories: (i) lack of data of interest; (ii) difficulty in handling the information by humans and/or machines; and (iii) the time needed for development. Nevertheless, automatic mitigation and response systems require a standardized exchange protocol and format.

2.4. Lessons Learned

In this chapter, we provided a first impression about real-world processes, structures and capabilities of ISP networks. In particular, we offer an understanding of how network operators and ISPs perform attack detection and mitigation.

An important outcome is that NetFlow data is an available data source and the use of NetFlow data for attack detection is a common approach. In contrast, sampling raw packets is not considered to be a practical approach. Additionally, we reveal that

Figure 2.12.: Distribution of exchange protocols and formats

the lack of an accepted exchange format and protocol prevents to establish effective early warning systems. Our findings are that a cooperation with CERTs/CSIRTs is the most reported form of collaboration. Even though network operators regard collaboration between trusted parties as an advantage that improve mitigation and respond capabilities, our respondents do not cooperate with a third party (e.g., consulting firm, forensic firm) and therefore do not exchange security related information such as security events or incidents. As a consequence, the majority of exchange protocols and formats that were published in recent years, are unused or even unknown to our participants. SCAP and IDXP are the most known exchange protocols, whereas IODEF and X-ARF are the most known exchange formats.

Furthermore, we gained knowledge about the use of external publicly available data to mitigate and respond to a network-based attack. An important finding is that traffic filtering based on IP blacklisting is not widely adopted. A possible explanation is that blacklisting might filter out legitimate traffic. If our participants reported using traffic filtering, most of them make use of blacklists.

Moreover, we found that automatic detection systems are deployed, but might raise a massive amount of false positives. However, transport networks report significantly less security events than mid-size networks. Transport networks report a maximum of 5 attacks, on average per month. An explanation might be that transport networks are not target of network-based attacks. Another possibility is that the attack traffic is not large enough to be spotted in their aggregated traffic. In contrast to the small amount of security events reported by transport networks, mid-size networks report a

massive amount of security events raised by the automatic detection system, but only a maximum of 10% of these security events are true positives.

In contrast to automatic detection systems, automatic mitigation and response system are not widely deployed, but network operators would like to make use of them to speed up mitigation and response capabilities.

The majority of participants thinks that ISPs play an important role in detecting and mitigating anomalies. This supports our assumption to promote detection algorithms, which fit the requirements of an ISP node.

In the future there is a need for network-based anomaly detection solution based on NetFlow data. Such a solution should be published as open source and well-documented, so that ISPs could easily adapt this appliance to their special needs without investigating too much money and operational time. Appliances used in different ISP networks should be able to collect and correlate security events with each other for better detecting network anomalies.

2.5. Concluding Remarks

In this chapter, we have answered the question "*Is distributed and automatic mitigation at ISP level performed and if yes, how?*" We performed two surveys according to common procedures and standards for good practice of survey research. In our first survey, we formulated questions that addresses four specific areas: (i) Attack and threats; (ii) Data and tools; (iii) Mitigation and reaction; (iv) Role of ISPs and IXPs. In our second survey, we formulated questions that addresses four specific areas: (i) process and involved third parties; (ii) automatic mitigation and response systems; (iii) data and (iv) exchange and collaboration. Both survey formulated introductory questions addressing organizational and personal information.

Based on the results of the surveys, we indicate that future work should focus on automatic detection systems with low false positive rates that can be located in high-speed networks. Automatic mitigation and response system need to be deployed to efficiently and effectively handle the amount of security events/incidents raised by an automatic detection system. An important question for future studies is to determine the benefit of a collaborative mitigation and response approach.

Exchange of Threat Information

In this chapter, we provide a structured overview of existing exchange formats and protocols, explain their structure and their use-case scenarios. Further, we evaluate and compare existing exchange protocols and formats regarding their strength and weaknesses especially in terms of their interoperability with flow-based data and high-speed networks. Finally, the results are discussed and concluded. The results of this Chapter have been published in the following two publications and at the IETF

[C11]: Jessica Steinberger et al. “How to exchange security events? Overview and evaluation of formats and protocols”. In: *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. May 2015, pp. 261–269. DOI: [10.1109/INM.2015.7140300](https://doi.org/10.1109/INM.2015.7140300)

[M31]: Jessica Steinberger et al. *Exchanging Security Events of flow-based Intrusion Detection Systems at Internet Scale*. Website. June 2015. URL: https://www.iab.org/wp-content/uploads/2015/04/CARIS_2015_submission_3.pdf (visited on 12/28/2015)

[M32]: Jessica Steinberger. *FLEX*. Website. July 2015. URL: <https://datatracker.ietf.org/meeting/93/materials/agenda-93-mile/> (visited on 12/12/2017)

3.1. Introduction

In chapter 2, we studied how ISPs perform distributed and automatic mitigation. We found that one approach to mitigate and resolve network-based attack focus on cooperation of ISPs and their exchange of security event information. François, Aib, and Boutaba [J8] identified cooperation between ISPs as a viable solution for attack mitigation. An advantage of detection and mitigation of network-based attacks at ISP level and their cooperation is the possibility to exchange security events and thus improve timeliness and dissemination of network security information. As a consequence, the collaborating ISPs benefit from an increased security level based on shared knowledge.

For ISPs to collaborate, a common data representation to describe security-related data is important. Further, an exchange protocol to transmit security events over

network borders is also required. Several exchange formats (e.g., IODEF, ARF, x-arf) and protocols (e.g., RID, IDXP) have been published in the last years. Although a previous study that we have conducted [C9] shows that most of the exchange formats and protocols are unknown to network operators, recent network-based attacks (e.g., Spamhaus) have clearly indicated that there is a need for collaboration and therefore for exchange formats and protocols supporting it.

To the best of our knowledge, only two other publications are related to exchange formats and protocols. First, Koch et al. [J11] reviewed exchange formats and protocols used by intrusion detection and response systems, but the authors do not differentiate between a high-level description of functional requirements, an exchange format or an exchange protocol. Further, the authors do not provide information about flow-based interoperability and used security mechanisms of the exchange formats and protocols. Second, Kampanakis [J12] focuses on information sharing models and reviewed efforts driven by the US Department of Homeland Security, Mitre and the US NIST. These models cover a wide range of exchange formats shown in Figure 3.1 and thus do not focus on Intrusion Detection and Incident Management.

In this chapter, we review the exchange formats and protocols used in context of intrusion detection and incident management. We classify the exchange formats related to their use-case scenario and assign them to the different stages of the *Operations Security Management Process of The Mitre Cooperation* [M41] (Figure 3.1). We analyze both, the data representation and the use-case scenario of the exchange formats. Further, we review existing exchange protocols and explain their intended use. As we identified the key position of ISPs in detection and mitigation of cyber-criminal activities, we develop various criteria to assess the exchange formats and protocols specifically in context of high-speed networks. Moreover, we assess the exchange formats for the use in conjunction with flow-based data, because a previous study from Steinberger et al. [C9] stated that ISPs focus on detection of anomalous events based on aggregated network data (e.g. NetFlow, IPFIX). The goal of this chapter is to provide network operators a hands-on selecting an exchange format and protocol suitable to use in their network. Therefore the main contributions of this chapter are: (i) a comprehensive literature survey of 10 exchange formats and 7 exchange protocols that can be used to share security event related information in context of intrusion detection and incident handling, (ii) a structured overview that can be used by network operators when they have to decide what format and protocol should be used, (iii) an assessment of the exchange formats for the interoperability with flow-based data, (iv) a qualitative evaluation and comparison of the formats and protocols in context

Figure 3.1.: Application domains of exchange formats based on [M41]

of high-speed networks and finally an investigation of how to exchange potentially sensitive information.

3.2. Event Exchange Formats and Protocols

In this section, we introduce various formats and protocols to exchange security events as listed in Table 3.1. First, we introduce the terminology by defining an exchange format and protocol. Additionally we define security event and security incident. Second, we review existing exchange formats and protocols, explain their structure and their use-case scenarios.

3.2.1. Terminology

A *format* describes a structure for the processing, storage, or display of data. An *exchange format* defines a representation of information for sharing data. An *exchange protocol* “is a set of rules defining how to interconnect network devices and establish a channel to transmit network datagrams, representing exchange formats, across a computer network [F6, B5]”.

The analysis of the state of the art has revealed that there are various terminology used to describe the content of an exchange message. In this thesis, we adhere to the following: “A security event is defined as an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant [M42, M43].” In accordance to this definition we summarize security alert, security alarm and security warning to security event. In contrast to a security event, “a security incident is defined as single or a series of unwanted information security events that

¹Assessment Results Format

²Abuse Reporting Format

have a significant probability of compromising business operations and threatening information security [M42, M43]”.

3.2.2. Exchange Formats

In this section we introduce the security event exchange formats that focus on intrusion detection and incident handling. Therefore, we classify the exchange formats related to their use-case scenario and assign them to the different stages of the Operations Security Management Process (OSMP) of The Mitre Cooperation. This classification and assignment are shown in Figure 3.1. Next, we present the development and data representation of each exchange format. In addition, we describe what kind of communication the exchange format is intended to facilitate. Last, we describe the involved communication partners of an exchange format message.

Common Intrusion Detection Framework

In 1997 the Common Intrusion Detection Framework (CIDF) project was launched by the US governments Defense Advanced Research Projects Agency (DARPA) to construct an infrastructure that allows Intrusion Detection, Analysis, and Response Systems (IDAR) from different manufacturers to share information [M44]. CIDF provides a LISP-like structure to express information about events, attacks, and responses called Common Intrusion Specification Language (CISL) [C22]. The syntax of CISL consists of S-expressions, a list-based data structure, which are known for their use in the LISP family of programming languages. Besides S-expressions, CISL includes nouns and verbs to encode security events. Further, CISL is intended to facilitate machine-to-machine (M2M) communication. CISL is quite powerful, because a message described in CISL has no limitations related to the type of information that is communicated [C23]. Despite the fact that CISL is quite powerful, it is presently dormant [M45, M46].

Incident Object Description Exchange Format

In 2001, initial efforts towards the IODEF started. The Terena IODEF Working Group was dissolved in 2002 and further IODEF development has been transferred to IETF Incident Handling (INCH) Working Group (WG). In 2003 the IETF Extended INCH WG developed the Format for Incident Report Exchange (FINE). FINE defines a format to facilitate the exchange of security incident information between CSIRTs. In particular, FINE is a high-level description of functional requirements for a format and thus not an implementation. Referring to the requirements defined in FINE, the data model

Table 3.1.: Overview of exchange protocols and formats

Protocol	OSI layer	Format	Security
CIDF	Transport	CISL messages	symmetric cryptography
RID	Application	IODEF	TLS
XEP-0268	Application	IODEF	TLS
IDXP	Application	IDMEF	TLS
CLT	Transport	CEE	provided by syslog (RFC 5425)
SMTP	Application	CAIF ARF x-arf	None S/MIME Multipart/Signed Multipart/Encrypted
syslog (RFC 3164)	Transport	syslog (RFC 3164)	none
syslog (RFC 5425)	Transport	syslog (RFC 5424)	TLS

of IODEF was specified in RFC 5070 [F7]. In contrast to CISL, IODEF (or called INCH) focuses on a human-to-human (H2H) communication. IODEF is used to share information commonly exchanged by CSIRTs about computer security incidents. IODEF is written in Extensible Markup Language (XML) and transferred over network using Real-time Inter-networking Defense (RID) protocol. Besides RID, IODEF could be transferred using the specification XEP-0268 of the Extensible Messaging and Presence Protocol (XMPP) [C24, M47]. IODEF is compatible to the Intrusion Detection Message Exchange Format (IDMEF), but IODEF incident handling (reporting, investigations), storage, statistics and trend analysis result in a longer lifetime of IODEF messages compared to one time use of IDMEF messages.

Common Announcement Interchange Format

In 2002 the development of Common Announcement Interchange Format (CAIF) started. CAIF is an XML-based format to store and exchange security announcements developed by the Stuttgart University's Computer Emergency Response Team (RUS-CERT). CAIF is designed to describe a problem, vulnerability, or exposure that threatens the security of the IT infrastructure. Further, CAIF provides information about problems or solutions (a vendor patch or a workaround) or contains background information about one or more IT security issues. CAIF is able to address more than one security event within a single document and allows to group information for more than one target group of readers as well as multi-lingual textual descriptions within one document. Different renderings of an announcement for the intended target groups

3. EXCHANGE OF THREAT INFORMATION

addressing one, a sub-set, or all problems multi- or mono-lingual in the languages provided are supported [M48]. CAIF messages are generated by vendors or security teams and sent to users or administrators. Therefore CAIF is intended to facilitate a H2H communication. Currently, CAIF is generally considered to be inactive [M48].

Intrusion Detection Message Exchange Format

The IDMEF development is under control by the Intrusion Detection Working Group (IDWG) under the IETF. There have been numerous drafts of the IDMEF Request for Comments (RFC). In 2003 the draft RFC had been submitted to the Internet Engineering Steering Group (IESG). IDMEF has been approved by the IESG as an Informational RFC 4765 [F8]. IDMEF is intended to be a standard data format to share information of interest (alerts, alive messages etc.) with the focus on intrusion detection events for IDS/IPS systems and management systems that interact with them. Thus IDMEF is intended to facilitate M2M communication. The purpose of an alert message is to automatically inform a manager about a single or multiple detected events. Alerts occur asynchronously in response to outside events [F8], whereas heartbeat (alive) messages are sent in a regular period to indicate the analyzer's current status. Thus heartbeat messages are usually generated by network devices. IDMEF messages are written in XML and transferred over network using the IDXP.

Common Event Expression

The CEE [M49] format was developed by a community representing vendors, researchers and end users. The development of CEE was coordinated by MITRE in 2009. CEE proposes an extensible event syntax, event vocabulary, log transport information and log recommendation information to achieve consensus in event representation, communication and interpretation. CEE uses an XML and a JavaScript Object Notation (JSON) representation. The architecture of CEE consists of three parts: Requirements, which are addressed in the CEE Profile; Events, which are represented as records using the CEE Common Event Expression Log Syntax (CLS); and Records, which are shared via a CEE Common Event Expression Log Transport (CLT). At the very least, CEE event consists of 4 elements (time, level, id, and message) to formulate a valid CEE message. CEE events are generated through various devices within the network (such as firewalls, IDSs) and transported to a centralized repository that is reviewed by an administrator. Thus, CEE is intended to facilitate machine-to-human (M2H) communication. The main difference between CEE and IODEF is that IODEF is an incident-related effort and IODEF incident reports often include event logs. These

event logs may be provided in the CEE format, and a CEE-defined event may be incorporated into IODEF-defined incidents.

As both, architecture and syntax have not been finalized yet, CEE is still released as a beta version. In 2013 the U.S. Government organization, which sponsored MITRE's work on CEE has decided to stop funding development of CEE. As a result, MITRE has stopped all work on CEE, but offered to transfer all CEE-related specifications, documents and source materials to efforts willing to continue logging standards. The Project DMTF Cloud Audit and Project Lumberjack are continuing the work of CEE [M49].

Messaging Abuse Reporting Format

Yakov Shafranovich wrote the initial documentation for the Abuse Reporting Format (ARF) to report spam via e-mail. Later, a small group of members of the Messaging Anti-Abuse Working Group (MAAWG), including Yakov Shafranovich, wrote the first draft of ARF in 2005 [J13]. In the first draft of the MAAWG, an ARF message was based on email coupled with Multipurpose Internet Mail Extensions (MIME). This MIME message consists of three parts. The first MIME part provides a human-readable description of the report. The second MIME part of the message is a machine-readable format with the content type of "message/feedback-report". The third MIME part contains either the original message in its entirety or a copy of the entire header block from the original message. All MIME parts are required and thus must be included to form a valid ARF message. Following the first draft of ARF from the MAAWG, IETF chartered a working group called Messaging Abuse Reporting Format (MARF). The MARF working group updated the draft of ARF, removed unused report types [M50] and published a specification called ARF [F9] in 2007. ARF has been published as RFC 5965 and added to the library of official IETF standard documents [J13]. By 2007 ARF was already a de facto standard to report spam via e-mail [J13] and is intended to facilitate both M2M and M2H communication.

x-arf

In 2012 a competence group called "E-Mail" of eco - Association of the German Internet Industry has presented the reporting format x-arf [M40]. The main intention of X-ARF is to extend ARF. X-ARF is a format to exchange computer security incidents and attack data via e-mail and is intended to facilitate both M2M and M2H communication. X-ARF uses header fields of e-mails and two or three MIME-Parts. The content of an X-ARF message is defined by a JSON schema. An X-ARF message typically consists of

three containers, where the third one is optional. The first container conveys textual content, is human-readable and UTF-8 encoded. The second container contains a JSON object (a list of key/value pairs) represented in YAML notation. The fields within the second container of an X-ARF message depend on the type of abuse of the X-ARF message. The third container is intended to contain log data. X-ARF currently provides 5 different JSON schema: abuse, fraud, auth, info and private. In [M51] Kohlrausch and Übelacker reported the usage of X-ARF for exchanging data between national research networks. Within this use-case scenario they found that the X-ARF standard format is not able of aggregating multiple security events. Furthermore, they conclude that X-ARF messages are limited to one single destination address. Therefore they published a draft of X-ARF specification version 0.2, which enhances X-ARF in order to secure end-to-end communication for X-ARF messages and to store bulk data within the RFC 2822 container. The RFC 2822 container describes the format of an Internet message, which consists of lines of plain text. The current specification of X-ARF is version 0.2 and describes the three types of X-ARF messages: plain, unencrypted, unsigned and single abuse message (PLAIN), a signed and/or encrypted via S/MIME and PGP/MIME abuse message and a bulk e-mail abuse message. One of the main changes from specification version 0.1 to 0.2 is the change of the identifier of an X-ARF message. The identifier changed from X-ARF: YES to X-XARF: PLAIN, X-XARF: SECURE and X-XARF: BULK.

Syslog Message Format

In 2001 Eric Allmann wrote the first draft of the syslog message format that was first standardized as IETF RFC 3164 [F10]. The syslog message format is used to log messages generated by various sources e.g., an operating system, a process or an application. A syslog message consists of a priority value (PRI), a header and a free-form message part that provides information about the event (source, severity, host name, time stamp and message) and is limited to 1024 bytes. In 2009 Rainer Gerhards updated the syslog message format to remedy shortcomings of the RFC 3164 such as missing time zones or year within the time stamp. This update was published as RFC 5424 [F11] and is not backwards compatible to RFC 3164 [M52]. Besides the free-form message part in RFC 3164 and the structured data in RFC 5424, RFC 3165 [F12] defines how to encapsulate syslog messages within XML and sends them by means of TCP.

3.2.3. Exchange Protocols

In this section we introduce the security event exchange protocols. First, we describe the development and what content the exchange protocol is intended to transmit. Second, we describe to which OSI layer the exchange protocol belongs to and what kind of security mechanisms the protocol ensures.

Common Intrusion Detection Framework

The CIDF was developed by DARPA to share information of IDAR systems. CIDF messages are sent over one of four transport mechanisms, which can be negotiated depending on the needs of the components in question. The following types of transport/messaging are supported: (i) CIDF message layer without acknowledgement and re-transmission directly over UDP, (ii) CIDF message layer with reliable delivery (acknowledgment, re-transmission, and duplicate removal) over UDP, (iii) CIDF message layer directly over TCP and (iv) CIDF operations over CORBA [M53]. The default transport layer protocol for CIDF messages is reliable CIDF messaging over UDP on port 3295. The CIDF ensures privacy with the use of symmetric encryption algorithms. Besides the transport mechanism and the use of symmetric encryption algorithms, CIDF requires, that each device must possess its own certificate or certificate chain in a X.509v3 format. In 1998 the DARPA Information Assurance community decided to join forces with the IETF [C23] and stopped further development of CIDF.

Real-time Inter-Network Defense

In 2012 the Managed Incident Lightweight Exchange (MILE) WG standardized the initial work on RID. RID and its transport mechanism (RID-T) outlines a proactive inter-network communication method to facilitate sharing incident-handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident handling solution [F13]. RID adds exchange semantics to IODEF messages intended for the cooperative handling of security incidents within consortia of network operators and enterprises [F14] and provides a peer-to-peer exchange model. RID is an application-layer protocol that passes incident-handling data over HTTP/TLS. In addition, RID uses XML security features of encryption and digital signatures such as XMLencrypt and XMLsig.

3.2.4. Extensible Messaging and Presence Protocol

The XMPP is a real-time communication technology used for instant messaging collaboration and generalized routing of XML data. The specification XEP-0268: Incident Handling defines methods for incident reporting among XMPP server deployments using the IODEF format [M47]. XEP-0268 is an application-layer protocol that uses Transport Layer Security (TLS) to transmit incident messages over network. XEP-0268 was developed by the IETF's INCH WG and has been deferred [C24, M47].

Intrusion Detection Exchange Protocol

In 1998 the IETF IDWG started to develop a high-level requirements document, an intrusion detection message format and message transport protocols [C23] to define a common way to exchange Intrusion Detection Messages between intrusion detection analyzers and managers across a TCP/IP network. The Intrusion Detection Message Exchange Requirements (called IDP) were published in RFC 4766 [F15]. Out of these requirements, the Intrusion Alert Protocol (IAP) was developed [M54]. IAP was the first attempt to meet IDP [C25] and uses a request-response model of communication similar to HTTP 1.1 [M54]. In December 2000 the IDWG decided to look into using Block Extensible Exchange Protocol (BEEP) as basis of the message transport protocol to overcome security related limitation of IAP rather than completing the work on IAP.

BEEP, previously known as BXXP [F16] is an Internet Standard from the IETF and a generalized application-level protocol framework. The advantages of BEEP is that it takes care of the connections, the authentication, and the packaging up at the TCP/IP level of the messages. BEEP competes on the same level as HTTP [M55].

In a second attempt the IDWG developed the IDXP that is specified as a BEEP profile. In 2007 the application-layer protocol IDXP was published as RFC 4767 [F17]. IDXP transmits data of the following MIME types: text/xml, text/plain and application/octet-stream.

CEE Log Transport Protocol

The CEE CLT [M56] was developed by The MITRE Corporation in collaboration with the NATO Consultation, Command and Control Agency (NC3A), information technology (IT) vendors and IT administrators. The CLT defines requirements that a CLT protocol must meet to transmit CEE messages. Therefore CLT also defines transport mappings. Since Syslog is the de facto standard in log transport protocols and it is supported by numerous products, the only mapping published to transmit

CEE messages is a specification for sending JSON-encoded events over the RFC 5425 syslog protocol.

Simple Mail Transfer Protocol

In 1982 Jonathan Postel developed the Simple Mail Transfer Protocol (SMTP) that was published in RFC 821. Over the years, the RFC of SMTP was updated several times. The new Draft Standard of SMTP is published in RFC 5321 [F18]. SMTP is an application layer protocol to transfer mail messages over TCP. The content of a mail message includes a message header and a possibly structured message body. If the body of a mail message is structured, it is defined according to the MIME Part One [F19]. SMTP is inherently insecure because real mail security lies only in end-to-end methods involving the message bodies, such as digital signatures (Multipart/Signed and Multipart/Encrypted in RFC 1847, Pretty Good Privacy in RFC 4880 or Secure/Multipurpose Internet Mail Extensions (S/MIME) in RFC 3851) [F18]. SMTP is used to transmit messages of CAIF, ARF and X-ARF. The secure transmission and storage of CAIF, ARF or X-ARF messages is outside the scope of these format specifications. When creating CAIF, ARF or X-ARF messages or when interchanging the XML/JSON source of documents between sender and receiver, mechanisms such as canonical XML, digital signatures or methods for encryption have to be implemented, that assure the integrity and authenticity of the documents.

Syslog Protocol

The syslog messages defined in RFC 3164 [F10] are using the syslog protocol also published in RFC 3164. This syslog protocol uses the UDP, port 514, for communication. Therefore this syslog protocol does not guarantee a message delivery and is not encrypted. Further, the syslog protocol described in RFC 3164 is vulnerable to replay attacks. As the format of syslog was updated and the RFC 5424 was published, the syslog protocol was also updated. Unlike RFC 3164 the syslog protocol was published in a separate RFC, called RFC 5425 [F20]: Syslog over UDP and RFC 5426 [F21]: Syslog over TLS.

3.2.5. Evaluation

In this section, we evaluate the exchange formats and protocols. First, we describe the characteristics of the evaluation criteria. Furthermore, we introduce 10 evaluation criteria for the exchange formats and 7 evaluation criteria for the exchange protocols. Last, we present and summarize the results of the evaluation.

3.2.6. Evaluation Methodology

The exchange formats are evaluated based on the following ten criteria: flow-based format interoperability, extensibility, scalability, aggregability, protocol independency, machine readability, human readability, integrity & authenticity, confidentiality and practical application. These criteria were chosen to provide a means of comparison between exchange formats and to measure if and how the use of this exchange format makes a large amount of security events manageable for network operators. In this evaluation, we assess the flow-based format interoperability by using a Cisco NetFlow v5 record. The findings are also valid for other flow-based accounting technologies, e.g., IPFIX.

The ability to use the exchange format in conjunction with flow-based data is described by the criterion flow-based format 'interoperability'. 'Extensibility' defines the aptitude of the exchange format to extend its functionality. This feature refers to the use of additional information or fields, and development of particular data structure in order to fit to one's needs. The ability to handle growing data volumes is described by the 'scalability' criterion. An exchange format is called scalable when it is capable of working properly with different volumes of data. 'Aggregability' defines the aptitude to aggregate single flows within the exchange formats. 'Protocol independency' describes the ability to transport the exchange format by using a protocol already existing in the infrastructure without adaption in case of an existing complementary protocol. 'Machine readability' describes whether a format is machine readable or not, whereas the 'human readability' criterion describes the human readability of each exchange format. The use of digital signatures within a message of an exchange format is described by the criterion 'Integrity & Authenticity'. The 'Confidentiality' criterion describes the ability to encrypt a message of each exchange format. The last criterion 'practical application' indicates if there are products available that make use of the exchange formats.

The exchange protocols are evaluated based on the following seven criteria: confidentiality, integrity, authenticity, reliable message transport, interoperability, scalability and practical application. The criteria to evaluate an exchange protocol are part of the well-known model for security policy development CIA Triad.

The 'Confidentiality' criterion describes the capability to protect sensitive data from disclosure to unauthorized parties. The ability to determine whether the communication peers are, in fact who they declared to be and thus make use of authentication mechanisms is described by the 'Authenticity' criterion. The ability to protect data from modification or deletion by unauthorized parties is described by the 'Integrity' criterion.

Table 3.2.: Evaluation summary of the exchange formats

Criterion	CIDF	IODEF	CAIF	IDMEF	ARF	CEE	X-ARF		Syslog	
							v0.1	v0.2	RFC 3164	RFC 5425
Interoperability	–	–	–	–	+	+	+	+	+	+
Extensibility	+	+	+	+	+	+	+	+	+	+
Scalability	–	–	–	–	–	–	–	–	–	–
Aggregability	–	–	+	0	–	–	–	+	–	–
Protocol independency	–	0	+	0	+	0	+	+	+	+
Human readability	–	–	–	–	+	+	+	+	+	+
Machine readability	+	+	+	+	+	+	+	+	–	+
Integrity & Authenticity	–	–	–	–	–	–	–	+	–	–
Confidentiality	–	–	–	–	–	–	–	+	–	–
Practical application	–	0	0	0	0	–	0	0	+	+

Legend: high (+), medium (0) and low (–)

An exchange protocol is using 'Reliable message transport' when the transmission of a security event uses a guaranteed delivery to avoid duplicate messages and message loss. The 'Interoperability' criterion describes the ability to transmit different data representations of security events. The ability to handle different network sizes is described by the 'scalability' criterion. The last criterion 'practical application' indicates if the exchange protocol is used within the network.

3.2.7. Evaluation Results

In this section, we present and discuss the results of the evaluation of the security event exchange formats and protocols.

Evaluation of Exchange Formats

The security event exchange formats can be categorized into four groups: S-expressions, XML-based and MIMEMessage-based formats and syslog. This categorization facilitates the qualitative evaluation of the exchange formats based on common characteristics and is visualized in Figure 3.2.

Interoperability: CIDF uses nouns and verbs to encode security events, but there are no nouns and verb available to describe flow-based data. Due to this reason the interoperability of CIDF is low. To use Cisco NetFlow v5 in conjunction with XML-based formats the NetFlow record fields are passed to the structure of an appropriate XML-element. In the XML-based formats IODEF, CAIF and IDMEF, only a few NetFlow

Figure 3.2.: Classification of the exchange formats

record fields fit into the defined data representation. Therefore, the flow-based format interoperability of the XML-based formats IODEF, CAIF and IDMEF in conjunction with NetFlow is low. The XML-based exchange format CEE, the MIMEMessage based formats ARF and X-ARF, and both versions of syslog provide a free-form message part and thus result in a high interoperability.

Extensibility: The use of CIDF in conjunction with flow-based data requires a new definition of nouns and verbs and thus result in a high extensibility. The XML-based formats IODEF, CAIF and IDMEF use the <AdditionalData> structure to store all remaining NetFlow record fields. Another approach is to define an XML-schema to store flow-based data into the exchange formats IODEF, CAIF and IDMEF and thus results in a high extensibility. The MIME-based message formats, the XML-based format CEE and syslog do not have any additional fields to map NetFlow into their structure. Instead, the whole NetFlow record has to be attached as separate MIMEBodyPart or in a container of a free-form message. Thus the extensibility of the exchange formats ARF, X-ARF and syslog is high.

Scalability: It is possible to map large input files into the structure of CIDF, the XML-based formats IODEF, CAIF, IDMEF and CEE and the MIMEbased formats ARF and X-ARF. The main disadvantage of this approach is, that the output files will be as large as the input files or even larger. Thus the scalability of the exchange formats in general is low.

Aggregability: The exchange formats CIDF, IODEF, ARF, CEE, X-ARFv0.1 and both versions of syslog do not provide any field or container to enter data of more than one security event. Therefore the aggregability is considered as low. CAIF and X-ARFv0.2 address more than one security event within a single document and thus result in a high aggregability. IDMEF does not provide a field or container to enter more than one security event, but provides an XML element `CorrelationAlert` to group one or more previously sent security events together.

Protocol independency: CIDEF uses CLT and a special architecture to transmit security events. Thus, the independency of CIDEF is low. On the one hand the XML-based formats IODEF, IDMEF and CEE provide their own exchange protocol as a first choice and on the other hand these formats can be enveloped into a user-defined packet for transmission over network. Due to the reason that the designated exchange protocols are often not available in the network the independency of the XML-based formats result in a medium independency. CAIF does not define a specific protocol to exchange a CAIF message and thus can be enveloped into a user-defined packet for transmission. The protocol independency of CAIF is high. ARF and X-ARF use a MIMEMessage format and thus must use SMTP for transmission over network. Besides ARF and X-ARF, syslog also relies on an infrastructure that is available in most of the companies. The independency of the exchange formats ARF, X-ARF and syslog results in a high independency.

Human readability: The exchange formats CIDEF, IODEF, CAIF and IDMEF are hardly human readable. A parser is required to extract the requested values out of the underlying structure. Therefore the human readability of the exchange formats CIDEF, IODEF, CAIF and IDMEF is low. The exchange formats ARF, X-ARF, CEE and syslog consist of a human-readable container to store security events. Due to this container the human-readability of the exchange formats ARF, X-ARF, CEE and syslog is high.

Machine readability: Except the exchange format syslog RFC 3164, all exchange formats are machine readable. A parser is used to extract the requested values out of the underlying structure. The exchange format syslog RFC 3164 can not be parsed unambiguously. One reason is that syslog RFC 3164 does not define a structure of a syslog message and does not define the character set or encoding for syslog messages. Therefore the machine readability of syslog RFC 3164 is low.

Confidentiality, integrity and authenticity: Except the exchange format X-ARFv0.2, none of the exchange formats provide any security mechanisms to sign or encrypt a security event. X-ARFv0.2 provides the ability to use Secure/Multipurpose Internet Mail Extensions (SMIME) for public key encryption and signing the security event.

Practical application: Due to the fact that the work on CIDEF and CEE is presently stopped, no practical applications are available that make use of CIDEF or CEE. The exchange formats IODEF, CAIF, IDMEF, ARF and X-ARF are used in several applications (e. g. IODEF: DFLabs products; CAIF: RUS-CERT Stuttgart University, CERT-VW

Figure 3.3.: Classification of the exchange protocols

Volkswagen AG; IDMEF: Snort, Prelude; ARF: arffilter and X-ARF: members of the Association of the German Internet Industry (eco)). Syslog is the most used exchange format.

Evaluation of Exchange Protocols

The security event exchange protocols can be categorized into the two groups: Secured and unsecured. This categorization facilitates the qualitative evaluation of the exchange protocols based on common characteristics. Figure 3.3 shows the categorization of the security event exchange protocols, whereas the colored and bold formatted protocols make use of TLS.

Confidentiality, integrity and authenticity: CIDF provides a matchmaking service through which CIDF components use authenticated and secured communications between CIDF components. The matchmakerservice also acts as a Certificate Authority (CA). The CIDF messages can include authentication headers and can be encrypted [C26]. Therefore the authentication, the confidentiality and the integrity capabilities of the exchange protocol CIDF are high. RID uses digital signatures on a hash of the RID message with an X.509v3 certificate issued by a trusted party to authenticate the sender of an RID message. XEP-0268 is based on XMPP. As XMPP uses the Simple Authentication and Security Layer (SASL) for peer authentication, the authentication capabilities of XEP-0268 is considered as high. IDXP uses a mutual authentication of public-key certificates of the underlying BEEP security profile TLS. The syslog RFC 5425 uses mutually authenticated channels with widely deployed cryptographic algorithms and protocols. As CLT is basically syslog RFC 5424 it has the same characteristics. The authentication capability of the exchange protocol RID, IDXP, CLT and syslog RFC 5425 is high. The exchange protocols SMTP and syslog RFC 3164 do not provide the ability to verify that the declared sender is actually the peer who sent the message and thus the authentication capability of SMTP and syslog RFC 3164 is low.

RID uses XML encryption to provide confidentiality based on the `iodef: restriction` attribute in the IODEF and IODEF-RID schemes [F13]. IDXP uses the underlying

ing BEEP security profile of TLS with the TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA cipher suite to provide confidentiality and thus result in a high authentication capabilities. XMPP uses TLS to ensure the confidentiality and thus the confidentiality capability of XMPP and XEP-0268 is regarded as high. SMTP and syslog RFC 3164 do not make use of any mechanism to ensure confidentiality. Therefore the confidentiality capability is low. CLT and syslog RFC 5424 are using TLS to counter disclosure of the security events and thus the confidentiality capability is high.

The integrity of messages transmitted over the network is addressed through the use of authentication mechanisms. The TLS-based protocols RID, XEP-0268, IDXP, CLT and syslog RFC 5424 support message integrity through the use of message authentication of TLS, BEEP security profile TLS or members of the SASL profile. The capability to ensure integrity of the TLS-based exchange protocols RID, XEP-0368, IDXP, CLT and syslog RFC 5424 is high. In contrast, SMTP and syslog RFC 3164 do not provide any mechanisms to ensure integrity and thus the integrity capability is low.

Reliable-message transport: The default transport layer protocol for CIDEF messages is reliable CIDEF messaging over UDP. But CIDEF also uses (i) message layer without acknowledgment and retransmission directly over UDP, (ii) the CIDEF message layer with acknowledgement and retransmission over UDP, and (iii) the CIDEF message layer directly over TCP. RID, XEP-0268 and IDXP require the use of connection-oriented protocol and thus make use of TCP. SMTP is independent of the particular transmission protocol but requires a reliable ordered data stream channel. Most companies are using SMTP over TCP. CLT and syslog RFC 5425 transmit syslog messages over a reliable channel over UDP. Therefore capability of a reliable message transport of the exchange protocols CIDEF, RID, XEP-0268, IDXP, SMTP, CLT and syslog RFC 5425 is high. Syslog RFC 3164 relies on the simple UDP protocol and thus results in a low reliable message transport.

Interoperability: The exchange protocols RID, IDXP, SMTP and both syslog versions provide the capability to transmit various exchange messages of different formats. The ability to transmit different data representations of security events of the exchange protocols RID, IDXP, SMTP and both syslog version is high. The extension XEP-0268 was developed to transmit IODEF messages. Therefore only IODEF messages can be transmitted via XEP-0268 and thus result in a low interoperability. CIDEF and CLT can only be used to transmit CIDEF messages and CEE messages and thus result in a low interoperability.

Scalability: All exchange protocols except RID were developed to interoperate and share data. Therefore the scalability of CIDF, IDXP, XEP-0268, SMTP, CLT and both syslog versions is high. Due to the fact that RID is a point-to-point exchange protocol it does not scale well. Therefore the ability to handle different network sizes is low. Similar to CIDF, XEP:0268

Practical application: CIDF was not intended as a standard that would influence the commercial marketplace. Due to the fact that CIDF was a research project and the work on CEE and XEP-0268 is presently stopped no practical applications are available that make use of CIDF, CLT and XEP-0268. Therefore the availability of the practical application is low. There are some implementations available that make use of RID and IDXP and thus the practical application is medium. Most companies make use of SMTP and syslog in both versions and therefore the practical application is high.

3.3. Evaluation Summary

In this section, we provide an aggregated overview of the key evaluation results to support network operators to identify an exchange format/protocol that can be used in their network. We have summarized the information presented in subsection 3.2.5 in Table 3.2 and 3.3.

We found that the use of flow-based data within the XML-based exchange formats IODEF, CAIF and IDMEF requires a new XML scheme or the AdditionalData element needs to be used. The MIME-Message based formats transmit the same information multiple times without providing new knowledge.

Most of the exchange formats are machine readable. This ensures that security events can be handled automatically. In case the network operator focuses on machine readability, all exchange formats except syslog RFC 3164 are suitable. If a network operator focuses on an exchange format that is human readable and does not require an additional parser, the network operator should focus on the MIME based exchange formats ARF and X-ARF. But also CEE and syslog might be of interest, as they provide an free form message part. However, CEE has never been finalized, so actions should first be taken into this direction before the exchange format can be used in practice.

With respect to the interoperability with flow-based data, the exchange formats ARF, CEE, X-ARF and syslog are suitable to use in conjunction with flow-based data. To exchange sensitive data, however, the network operator might focus on mechanisms to sign or encrypt a security event. Except the exchange format X-ARFv0.2, none of the exchange formats provide mechanisms to sign or encrypt a security event. Finally,

Table 3.3.: Evaluation summary of the exchange protocols

Criterion	CIDF	RID	XEP-0268	IDXP	SMTP	CLT	Syslog	
							RFC 3164	RFC 5425
Confidentiality	+	+	+	+	–	+	–	+
Authenticity	+	+	+	+	–	+	–	+
Integrity	+	+	+	+	–	+	–	+
Reliable message transport	+	+	+	+	+	+	–	+
Interoperability	–	+	–	+	+	–	+	+
Scalability	+	–	+	+	+	+	+	+
Practical application	–	0	–	0	+	–	+	+

Legend: high (+), medium (0) and low (–)

we note that to establish a collaboration between exchange peers, a well-known and established format should be used. Even though, a lot of exchange formats were published in the last years, only the exchange format syslog provides a widespread use.

To transmit a security event, the network operator might focus on a high-security level. The exchange protocols CIDF, RID, XEP-0268, IDXP, CLT and syslog RFC 5425 provide a high-security level. SMTP and syslog RFC 3164 were not designed to ensure the four key aspects of information security (confidentiality, integrity, authenticity and non-repudiation). However, syslog and SMTP have the advantage that they are widely spread. Therefore we identify here a tradeoff between security level and easiness to deploy. Even though SMTP has never been updated, the use of the SMIME standard provides the ability to digitally sign messages and to encrypt message contents to overcome these missing security aspects. In case a network operator focuses on an exchange protocol that should be used in high-speed networks, all exchange protocols are suitable except RID. RID does not scale in high-speed networks because it was designed as point-to-point protocol.

3.4. FLEX

In this section, we present our new exchange format FLEX. Further, we describe its main structure and how security events are disseminated using FLEX.

3.4.1. Introduction

In recent years, network-based attacks became one of the top concerns for network infrastructure and service outage [R1]. To reduce the impact of network-based attacks (e.g. Distributed Denial of Service (DDoS)) multiple attack detection methods [C27] and countermeasures have been proposed [J14]. In detection and countermeasures, we observe two growing trends. First, flow-based solutions are becoming more and more popular. Second, collaborative approaches, especially among trusted partners, have proven to be a necessary step to counteract large attacks [J8]. However, these collaborative approaches do not take into account to exchange threat information in an interoperable, standardized format.

An *interoperable format* provides accurate, context rich, directed and actionable threat information in a timely manner [M57]. In case of an ongoing network-based attack, an interoperable format supports an automatic dissemination of threat information and thus lessens the time to respond [M58, M59]. A *standardized format* ensures the availability of detail and context information and reduces manual processing (e.g. normalization, exchanging data between different systems) [M58, M59]. In the last years, several exchange formats (e.g., IODEF, IDMEF, ARF and Extended Abuse Reporting Format (x-arf v0.1 and v0.2) have been published [C11]. However, it is still a challenge to find a standardized exchange format that is thoroughly validated and tested in full scale of industry trials. A previous study [C9] reported that exchange formats are often unknown for network operators. In addition, none of the exchange formats has been used in conjunction with flow-based data.

To overcome the shortcomings of missing flow-based interoperability, this research presents a new exchange format, which we call FLEX. FLEX is placed in high-speed networks that use links with a speed of 10 Gbps and higher [C28], and use flow export technologies (e.g. Cisco NetFlow, IPFIX) to identify, track and mitigate malicious traffic [C9]. Further, FLEX is intended to facilitate the cooperation among network operators and focus on an automated threat information exchange. The contribution that FLEX brings to the state of the art is that it allows the exchange of threat information based on flow data in a structured and unambiguous manner. In addition, since FLEX messages are disseminated using SMTP, FLEX is easy to deploy and it integrates with existing infrastructure.

3.4.2. Structure of FLEX

The FLEX is based on the x-arf specification draft v0.2 X-XARF:SECURE (henceforth referred to as x-xarf). In contrast to x-xarf, FLEX uses a generic template system.

Figure 3.4.: Components of a FLEX message

This generic template system is described by an abstract syntax denoted using the language of Abstract Syntax Notation (ASN) (ASN.1). Both, the generic template and the abstract syntax of FLEX prevent all ambiguities when being interpreted and handled by an automatic mitigation and response system. Further, FLEX ensures the interoperability with different flow-based export technologies as input source and makes use of both signature and encryption methods to prevent unauthorized access to the security event message at the application layer. FLEX consists of a mail header and an enveloped-data content type. The enveloped-data content type consists of an encrypted content of a signed multipart MIME message and encrypted content-encryption keys for one or more recipients [F22]. The enveloped-data content consists of two parts: The first part contains the FLEX container that is signed. The second part conveys the detached signature Cryptographic Message Syntax (CMS) SignedData object. Figure 3.4 visualizes the components of a FLEX message.

The FLEX container is composed of data arranged in vector form and represented by $\mathcal{F} = \{s_0, \dots, s_{n_0}, f_0, \dots, f_{n_1}, d_0, \dots, d_{n_2}, c_0, \dots, c_{n_3}\}$, where s represents the settings, f the flow fields of the flow export technology, d additional information provided by the detection engine and c security event related flow data. In addition, the FLEX container uses the Octet Encoding Rules (OER) of ASN.1. In contrast to other encoding rules (e.g., Basic Encoding Rules (BER), Canonical Encoding Rules (CER), Distinguished Encoding Rules (DER)), OER produces a compact octet-oriented encoding and increases the encoding/decoding speed. Listing 3.1 shows the ASN.1 structure of a FLEX message

3. EXCHANGE OF THREAT INFORMATION

and can be read: a FLEX message is defined as a FLEXRecord that consists of a structure (SEQUENCE) with four components: settings, flowfields, detection and correlation. These components are called identifiers. In addition, these identifiers are described by a type. For example, settings denotes data of type Settings and correlation, denotes a list (SEQUENCE OF) of data which are all of type CorrelatedFlows. Besides an identifier and a type, the FLEXRecord contains tags. A tag is a number between square brackets before a type. In order to properly decode a FLEX message and remove all ambiguities a FLEX messages uses explicitly tags.

```
FlexRecord ::= [APPLICATION 0] SEQUENCE {  
    settings      [0] Settings,  
    flowFields    [1] FlowFieldTypes,  
    detection     [2] Detection,  
    correlation   [3] SEQUENCE OF CorrelatedFlows DEFAULT {}  
}
```

Listing 3.1: ASN.1 structure of a FLEX message

The first vector stores setting information ($s_0, \dots, s_{n_0}$) on how to interpret the transmitted data. The settings vector contains a unique message identifier, a description of the event type and the type and version of the flow data. The data representation of the settings vector is described in Listing 3.2.

```
Settings ::= [APPLICATION 1] SEQUENCE {  
    id            [0] INTEGER,  
    msgType       [1] ENUMERATED{event(0), request(1), responseF(2),  
        responseNF(3), alert(4)},  
    eventType     [2] ENUMERATED{CuC(0), DDoS(1)},  
    type          [3] ENUMERATED{netflow(0), ipfix(1), sflow(2)},  
    version       [4] ENUMERATED{two(0), four(1), five(2), nine(3)}  
}
```

Listing 3.2: Settings

The flow field types of a flow format are stored in the vector ($f_0, \dots, f_{n_1}$). The quantity of the flow field types depends on the ASN.1 choice element used to enter the flow data. Thus, FLEX uses a generic template system that provides the capabilities to exchange several flow-based security events. This generic template is shown in Listing 3.3.

```
FlowFieldTypes ::= CHOICE {  
    netflow5 [0] NetFlow5,  
    netflow9 [1] NetFlow9,  
    ipfix    [2] Ipfix  
}
```

Listing 3.3: Flow field types

Next, information of a detection engine is stored in the vector $(d_0, \dots, d_{n_2})$. The detection engine provides additional data such as severity, impact, priority, NAT, reliability, correlated data flow sets and an observation ID. The data representation of the detection engine vector is presented in Listing 3.4.

```
Detection ::= [APPLICATION 2] SEQUENCE {
    severity      [0] INTEGER,
    impact        [1] INTEGER,
    priority      [2] ENUMERATED{high(0), medium(1), low(2)},
    nat           [3] ENUMERATED{true(0), false(1), na(3)},
    observationID [4] INTEGER
}
```

Listing 3.4: Additional data of the detection engine

The last vector $(c_0, \dots, c_{n_3})$ provides optional data and is composed of unique identification numbers of the correlated flow sets and an identification number of the observation point. The data representation of flows related to this security event is shown in Listing 3.6. Finally, this FLEX message is placed within the FLEX container that is signed. The encrypted data content consists of both, the FLEX container and the detached signature.

```
CorrelatedFlows ::= SEQUENCE {
    flowID          [0] INTEGER,
    observationID [1] INTEGER
}
```

Listing 3.5: Correlated flows of a FLEX message

Listing 3.6 shows an example of a FLEX message containing NetFlow version 5.

```
value FlexRecord ::=
{
    settings{
        id 25,
        type netflow,
        version five
    },
    flowFields netflow5{
        flags "0x00 Unsampled",
        size 52,
        first 1387648761,
        last 1387648762,
        msec_first 430,
        msec_last 570,
        srcaddr "10.0.2.15",
        dstaddr "65.55.162.200",
        srcport 1036,
        dstport 25,
        fwdstatus 0,
    }
}
```

3. EXCHANGE OF THREAT INFORMATION

```
    tcpflags "0x17 .A.RSF",
    proto 6,
    tos 0,
    dPkts 4,
    dOctets 186,
    input 0,
    output 0,
    src_as 0,
    dst_as 0,
    src_mask "0/0",
    dst_mask "0/0"
  },
  detection{
    severity 1,
    impact 1,
    priority high,
    nat na,
    observationID 1254
  }
}
```

Listing 3.6: Example of a FLEX message containing NetFlow version 5

The main advantage of FLEX over existing exchange formats lies in the generic template system that provides extensibility and machine readability to support automatic processing of security events. In addition, FLEX integrates with the existing infrastructure using SMTP and thus is easy to deploy. Further, FLEX constitutes a viable and more structured alternative to share threat information based on flow data.

3.5. Lessons Learned

In this chapter, we reviewed current exchange formats and protocols used in context of intrusion detection and incident management.

An important outcome is that current exchange formats and protocols are not suitable to use in conjunction with flow-based data provided by flow export technologies (e.g., Cisco NetFlow, IPFIX). As a consequence, current exchange formats and protocols do not satisfy the requirements of ISPs.

Moreover, we found that most of the exchange formats are based on XML or MIME, whereas the exchange protocols rely on SMTP. Even though the exchange of threat information often contains sensitive data (e.g., remediation suggestion), except X-ARFv0.2 none of the exchange formats provide any security mechanisms to sign or encrypt a security event. In addition, the exchange protocol SMTP has never been designed to ensure the four key aspects of information security (confidentiality, integrity, authenticity and non-repudiation). The use of the SMIME standard provides the ability to digitally sign messages and to encrypt message contents to overcome

these missing security aspects. However, SMTP has the advantage that it is widely spread. Therefore, we identify here a tradeoff between security level and easiness to deploy.

In addition, we found that several efforts to standardize current exchange formats and protocols failed and thus a standardized exchange format and protocol that is thoroughly validated and tested in full scale of industry trails is missing.

To ensure the availability of detail and context information, flow-based interoperability and the reduction of manual processing, we presented FLEX. FLEX is based on the x-arf specification draft v0.2 X-XARF: SECURE and uses a generic template system described by an abstract syntax denoted using the language of ASN (ASN.1). Therefore, FLEX is an *interoperable format* that provides accurate, context rich, directed and actionable threat information in a timely manner. FLEX supports an automatic dissemination of threat information and thus facilitates the cooperation among network operators in case of an ongoing network-based attack. In addition, since FLEX messages are disseminated using SMTP, FLEX is easy to deploy and it integrates with existing infrastructure.

3.6. Concluding Remarks

In this chapter, we have answered the question "*How are security events currently exchanged and do they satisfy the requirements of an ISP?*" We performed a systematic literature review [J5] on current exchange formats and protocols according to the approach described by the Cochrane Collaboration within the Cochrane Handbook for Systematic Reviews of Interventions [M29, J6]. We identified 10 exchange formats and 7 exchange protocols used in context of intrusion detection and incident management and assigned them to the different stages of the Operations Management Process of The Mitre Cooperation. We provided a structured overview of the exchange formats and protocols that can be used by network operators to decide what format and protocol should be used in their environment to exchange security events. We analyzed the interoperability of the exchange formats with flow-based data and evaluated and compared the formats and protocols in context of high-speed networks. As an important result, we found that despite the requirement of flow-based interoperability, none of the exchange formats has been used in conjunction with flow-based data. Therefore, we presented the new exchange format FLEX to overcome the shortcomings of missing flow-based interoperability.

Based on the findings of our systematic literature review, future work should focus on a standardized exchange format and protocol that is thoroughly validated and

3. EXCHANGE OF THREAT INFORMATION

tested in full scale of industry trials. In addition, a widespread use of these formats and protocols should be established in the community of network operators.

Collaboration Process

This chapter present a communication process that supports the dissemination of threat information based on FLEX in context of ISPs. Further, this chapter shows that this communication process helps organizations to speed up their mitigation and response capabilities without the need to modify the current network infrastructure, and hence make it viable to use for network operators. This chapter is based on the publication:

[C12]: Jessica Steinberger et al. “Collaborative DDoS Defense using Flow-based Security Event Information”. In: *Proceedings of the 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS 2016)*. Apr. 2016. DOI: [10.1109/NOMS.2016.7502852](https://doi.org/10.1109/NOMS.2016.7502852)

4.1. Introduction

In Chapter 3 (Exchange of Threat Information), we performed a systematic literature review to collate current exchange formats and protocols. Further, we introduced the exchange format FLEX to ensure flow-based data interoperability and thus its use with widely adopted monitoring technologies. However, exchanging threat information is currently done on an ad-hoc basis via email or telephone [C9]. To facilitate the exchange of security event information in conjunction with widely adopted monitoring technologies, one approach focus on collaboration among trusted partners [J8, C29]. However, these collaborative approaches do not take into account a communication process that supports the automated exchange of threat information in an interoperable format, uses unreliable and reliable transports and ensures security mechanisms.

In the last years, collaborative approaches have predominantly been published in the area of attack detection [J8], but missing to develop collaborative mitigation and response measures. To overcome the lack of a missing collaborative mitigation and response approach, this chapter presents a communication process, that uses the exchange format FLEX [M31]. The contribution that the communication process brings to the state of the art is that it supports achieving the situational awareness of the current threat landscape, pools expertise and resources, facilitates the automated defense

in response to ongoing network-based attacks and thus lessens the time to respond. In addition, since FLEX messages are disseminated using the Simple (or Streaming) Text Orientated Messaging Protocol (STOMP) ¹ or SMTP, the communication process is easy to deploy and integrates with existing infrastructure.

4.2. Scenario, Requirements and Assumptions

In this section, we describe the main focus of this work. First, we define the networks in which we are going to collaborate among trusted partners and exchange threat information. Second, we define the requirements that a communication process should fulfill, as they emerged by the scenario described in Section 4.2. In the following, we will use these requirements to evaluate the communication process. In addition, we describe our assumptions to ensure that the work is not biased by tasks related to detection technologies.

4.2.1. Scenario

The primary focus of this work are multiple high-speed networks using a link speed of 10 Gbps and higher [C28], and are using an architecture of a typical flow monitoring setup [J15] to identify, track and mitigate malicious traffic [C9]. The reason to use flow data is that flow data provides an aggregated view on network traffic passing an observation point [J16], and thus reduces the amount of traffic to analyze compared to raw packet data. Further, benefits to use flow-based data are that they are easy to deploy and satisfy the EU regulation on data retention. In addition, we focus on network operators that cooperate among trusted partners to minimize or prevent damages caused by network-based attacks and use an automated threat information exchange. The main advantage of an automated threat information exchange is to move from a reactive to a proactive network-based attack mitigation and response approach. Another benefit of a collaborative approach is that it provides insight into the current threat landscape that otherwise would not be obvious. In addition, sharing information and collaborating on network-based attacks support to enhance security expertise and speed up the mitigation and response capabilities and thus lessens the time to understand the threat for each collaborating partner.

¹<https://stomp.github.io>

4.2.2. Requirements

In this section, we introduce five requirements that a communication process among trusted partners should fulfill. These requirements are part of the operational requirements described within the IETF DDoS Open Threat Signaling (DOTS) WG [M60].

Ease of deployment: The communication process and its underlaying implementation should support platform independency. Further, the communication process should be able to handle different types of exchange formats and exchange protocols. The platform independency, the use of different exchange formats and protocols ensures that the communication process easily integrates with the existing infrastructure.

Granular access restriction policy: The communication process among trusted partners should support different detail of information tailored for its intended receivers. The reason is that the amount of provided threat information depends on the trust and sharing relationship between collaborating ISPs.

Encryption & signature: The dissemination of security event information often includes sensitive data (e.g., raw data, analyzed information of incident handling and its remediation [C30, J17, J18]). Therefore the communication process is required to use an exchange format that supports encryption to prevent unauthorized access to this threat information. Further, the exchange format used within the communication process is required to use signatures to ensure trustworthy origins, relevance and integrity of the security event.

Timeliness: The communication process among trusted partners should ensure the dissemination of security events in an appropriate amount of time. Further, the communication process should move from a reactive to a proactive network-based attack detection and mitigation approach and thus speed up detection and mitigation capabilities.

Semi-automated deployment of countermeasures: The communication process and its underlaying implementation should provide the possibility to interact with the network operator. This interaction ensures that the selection of an automated response depends on the network operator's choice and is called semi-automated. A semi-automated deployment of countermeasures is required to reduce the amount of false automated responses caused by false positives.

Figure 4.1.: Exchanging FLEX messages among trusted partners.

4.2.3. Assumptions

The detection of malicious actions are performed by monitoring technologies that classify malicious actions based on anomalies [C17, C31, C18] or signatures [B6, J19]. Both, signature and anomaly-based systems rely on information that determine what is normal behavior and what is not normal. Due to the ever-changing nature of networks, applications, and malicious actions, false positives might be raised. However, the main focus of this work is to show that collaboration among trusted partners helps organizations to speed up their mitigation and response capabilities and thus the assumptions are as follows:

Aggregation: Each alert raised by a detection engine is treated as one attack. The aggregation and fusion of alarms should be taken into account by the detection system. This assumption is in accordance to [T2, C32, T3].

Confidence: We assume 100% confidence of the alerts. A detection system might raise false alerts, but to ensure a hundred percent certainty of the alerts or a sanity check of the detection engine is out of scope of this work. This strong confidence is in accordance to [T2, C32, T3].

Scalability: We assume that the number of security events raised by the detection engine are not causing a scalability problem, because the quantity of security events that need to be handled by the network operator is low [C10].

4.3. Related Work

In this section, we present related work that has been published in the area of collaborative mitigation and response.

TAXII and STIX The Trusted Automated Exchange of Indicator Information (TAXII) is a community-driven effort, that defines concepts, protocols, and message exchanges to share cyber threat information for detection, prevention, and mitigation between trusted partners. The development of TAXII is coordinated by MITRE. The TAXII information exchanged is represented in the XML-based Structured Threat Information Expression (STIX) language [J12]. STIX describes potential cyber threat information (e.g., cyber observables, indicators, incidents, adversary tactics, exploits, and courses of action as well as cyber attack campaigns and cyber threat actors) and makes use of Cyber Observable Expression (CybOX) and Common Attack Pattern Enumeration and Classification (CAPEC).

Besides the XML-based structure of STIX, efforts are working on JSON, RDF/OWL, or other implementations. However, STIX and TAXII are complex, require much effort for processing [M61] and require extensive adoption to be used within the existing network infrastructure [J12]. Further, K. Moriarty [M62] reported that the base of TAXII is similar to RID in its use of SOAP-like messaging and thus will likely prevent it from scaling to the demands of the Internet.

Firecol Firecol [J8] is a collaborative system that detects flooding DDoS attacks at ISP level and provides a service to which customers can subscribe. This subscription forms a distributed architecture of multiple ISPs that computes and exchanges belief scores on potential attacks. In case Firecol detects an attack, the attack is blocked as close as possible to its source(s). Further, the IPS that detects the attack informs its upstream IPSs, which in turn also performs mitigation procedures. However, Firecol has not been validated in industry trails and its basic theoretic validation is founded on the DARPA'99 dataset [J20]. In addition, Firecol only uses blocking as a countermeasure and does not provide additional sophisticated mitigation and response measures.

ACDC In the year 2013, the Advanced Cyber Defence Centre (ACDC) [M63] project was launched. ACDC is an effort driven by the European Union to detect, mitigate and respond to botnets. ACDC provides one central database to collect and process data from already existing tools, sensors, sources and further unspecified components. ACDC also supports the mutual data sharing between partners (e.g., ISPs, government agencies, law enforcement, research groups, industry partners). The project finished in June 2015 and provides a web page with documents about the project deliverables. However, the possibility to join the community no longer exists, so the contribution to a collaborative mitigation and response approach remains unclear.

Exchange formats and protocols In recent years, numerous formats (e.g., IDMEF [F8], IODEF [F7], X-ARF [M64]) and protocols (e.g., IDXP, BEEP) have been published to support and facilitate the exchange of security event information [C11, J12]. Most of the exchange formats are automatically processable to reduce intensive manual processing (e.g, sorting, normalization) and support the timeliness of initial mitigation and response procedures. Moreover, these formats provide an accurate, context rich, directed and actionable data representation of threat information for its intended purpose. Further, as the most formats are based on XML-language or MIME, they ensure integrability with other security tools. Even though network operators often make use of flow-based data to identify, track and mitigate malicious traffic [C28, C18, C31, C17], the majority of the published exchange formats are not suitable to convey flow-data without extensive adoption. Besides the ability to convey flow-data, the exchange formats require encryption to prevent unauthorized access to the sensitive data (e.g., raw data, analyzed information of incident handling and its remediation [J17, J18]) of the security event. Further, signatures are required to ensure trustworthy origins, relevance and integrity of the security event. The majority of the published exchange formats, except X-ARF specification draft v0.2 X-XARF:SECURE do not provide any security mechanism.

Another important feature of the exchange format is the ability to support different detail of information tailored for its intended receivers. The reason is that the amount of provided threat information depends on the trust and sharing relationship between two collaborating ISPs.

Despite these formats and protocols are intended to facilitate sharing threat information, it is a challenge to find a standardized exchange format and protocol that is thoroughly validated and tested in full scale of industry trails, because a widespread use of these formats and protocols remain to be established in the community of network operators [C11]. A survey performed by [M65] and a presentation given by [M60] revealed that threat information is often exchanged on an ad-hoc basis via email, member calls or in personal meetings. This slows mitigation and response times and impedes mitigation and reaction efficacy.

4.4. Communication Process

In this section, we describe the main components of our proposed communication process and how these components interact with each other.

Figure 4.2.: Data flow of the communication process within MiR from the perspective of one ISP

4.4.1. Components of the Communication Process

Our communication process consists of gateways that are passed by every single security event message. A security event message is transferred among trusted partners using STOMP and the data representation uses the FLEX. The components of the communication process are illustrated in Figure 4.1.

STOMP: The STOMP is a text-based protocol that provides messaging interoperability among many languages, platforms and brokers. Therefore STOMP is language-agnostic and only uses a SEND semantic with a destination string as it does not provide its own queues or topics. STOMP supports messaging features, such as authentication, messaging models (point to point and publish and subscribe), message acknowledgment, transactions, message headers and properties.

The communication process makes use of STOMP between the gateways of the ISPs and is used to transfer FLEX messages among trusted partners. At each destination STOMP is connected to a Java Messaging Service (JMS) queue or topic.

FLEX: The FLEX [M31] is used to share security information among trusted partners based on flow data. FLEX is based on the X-ARF specification draft v0.2 X-XARF:SECURE and uses a generic template system that is described by an abstract syntax denoted using the language of ASN (ASN.1). In addition, FLEX makes use of both, signature and encryption methods to prevent unauthorized access to the security event message at the application layer.

MiR instances: Each collaborating ISP network contains a Mitigation and Response System (MiR), called MiR. MiR is aligned to the Event Processing Technical Society (EPTS) Reference Architecture [C33] and connected to both, a queue and several topics

of the MiR. MiR performs pattern matching algorithms to aggregate and consolidate security events into a smaller number of events and thus derives complex events. In addition, MiR enriches the security events through new knowledge gained through previous events or data (e.g., proposes remediations, external publicly available data sources). Besides the queue and the topic, MiR is connected to a database that stores previous security events and their remediation for a defined range of time.

4.4.2. Data Flow of the Communication Process

Our communication process consists of interconnected instances located in different ISP networks forming an overlay network. Each ISP possesses a list of directly connected collaborating ISP networks to prevent a full mesh within the network and thus ensure scalability. The data flow of the communication process is shown in Figure 4.2. The white or green rectangle represents the data entering the communication process (white=internal, green=external), whereas the gray rectangle represents a terminator symbol. The blue rectangle represents a sub-process within MiR. The diamond is used to visualize a decision or branching point and the connected lines represent different options.

At a time t the detection engine of an ISP identifies malicious activities and raises a security event of the FLEX message type Event. The security event is sent to the JMS queue of MiR via STOMP. The security event remains in the JMS queue until MiR consumes them. Next, the security event is searched within the database of previous events.

In case the security event could not be found within the database of the previous events, the MiR system initiates a detection process at collaborating neighbor ISP networks to reduce the amount of false positives of the security events. The detection process at the collaborating neighbor ISP networks is initiated by creating a FLEX message of the type Request and publishing it to the JMS topic of the adjacent ISP networks. The detection engine of the adjacent ISP network receives the FLEX message of the type Request, analyses the network traffic and tries to identify similar behavior as described within the security event. The result of the analysis is sent back to the requesting network as a FLEX message of the type Response.

In case the security event could be found within the database of the previous events, the MiR system examines whether the proposed remediation has been configured. In case the proposed remediation has not been configured yet, the ISP evaluates the feedback received in response to the FLEX message Request of the connected collaborating ISPs. In case the majority of the connected collaborating ISPs had seen similar behavior, the confidence ranking of the security event is increased, the proposed

remediation is configured and stored to the database. Subsequently, the information within the security event is preprocessed and restricted to different level of details depending on the level of trust. Finally, the tailored security events are routed based on their content to the appropriate JMS topic as a FLEX message of type Alert and thus send out to the connected collaborating ISPs.

4.5. Evaluation

In this section, we describe the qualitative and quantitative evaluation of the interaction of the main components of our collaborating MiR system. Further, we evaluate the communication process and its underlying implementation. Finally, we present and summarize the results of the evaluation.

4.5.1. Qualitative Evaluation

In this section, we perform a qualitative evaluation of the communication process. First, we describe the characteristics of the evaluation criteria. Second, we introduce three evaluation criteria for the communication process.

Evaluation Methodology

The communication process is evaluated based on the following three criteria: Ease of Deployment, access restriction and security mechanisms (e.g., encryption & signature). These criteria were derived from the requirements described in Section 4.2.

The criterion 'Ease of Deployment' describes the ability to use the communication process and its underlying implementation on different operating systems, infrastructure devices, exchange formats and protocols. The criterion 'access restriction' refers to the ability to support different detail of information within an security event tailored for its intended receivers. The 'security mechanisms' criterion describes the ability to make use of an security event exchange format that uses encryption and signature to prevent unauthorized access to the threat information and ensure trustworthy origins, relevance and integrity.

Qualitative Evaluation Results

In this paragraph, we present and discuss the results of the qualitative evaluation of the communication process.

Ease of deployment: The heterogeneity of network devices and used operating systems requires a platform independent communication process that easily integrates within the existing infrastructure. Therefore the implementation of the communication process is based on Java and thus can easily be deployed on different operating systems. Further, the MiR system was built in a modularized structure and is able to add modules that interact with various network devices. Besides the components of the communication process, the transfer of security events among trusted partners uses STOMP, a language-agnostic protocol to ensure platform independency.

Access restriction: Through the different level of trust and sharing relationship between collaborating ISPs, the communication process supports different detail of information within a security event tailored for its intended receivers. This tailored security event is sent to the appropriate JMS topic to which adjacent ISP networks subscribe and consume security event messages based on their level of trust and sharing relationship.

Security mechanisms: The dissemination of security event information often includes sensitive data (e.g., raw data, analyzed information of incident handling and its remediation [J17, J18]). Therefore the communication process uses FLEX to exchange security events among trusted partners, as FLEX supports encryption to prevent unauthorized access to the threat information and uses signatures to ensure trustworthy origins, relevance and integrity of the security event.

4.5.2. Quantitative Evaluation

In this section, we perform a quantitative evaluation of the communication process. First, we describe the setup of the testbed. Second, we present the test scenario of the communication process.

Setup of the Testbed

DeterLab [J21] is an infrastructure designed for experimentation in context of cybersecurity. We used DeterLab to evaluate our collaborative MiR system. The experiment is composed of physical machines for a limited time. DeterLab is used because it is a controlled environment in which it is possible to safely test security threats and defense measures. Our communication process consists of 5 nodes representing Internet Service Providers (ISP $A \dots E$) connected through a 500Mb link. In each

Figure 4.3.: A semantic representation of the DeterLab testbed

ISP network, MiR is installed as shown in Figure 4.1. Figure 4.3 shows a schematic representation of the DeterLab testbed.

Test Scenario

The objective of the experiments is to show that a target network with constrained resources benefits from collaborating partners during an ongoing network-based attack, because the target network has no possibility to react itself due to resource saturation. Further, we show that the network-based attack is not propagated further and that our communication process supports the automatic dissemination of threat information and thus speeds up the mitigation and response capabilities of ISP networks. In addition, we show that our communication process is lightweight in numbers of exchanged messages and fast.

To simulate a network-based attack, we performed a distributed TCP SYN flood attack from the ISP networks A and C to consume resources on the web server within ISP network E and render it unresponsive as shown in Figure 4.3. In our test scenario, ISP E is not able to effectively block the malicious traffic itself and requires collaborating partners in the stream of traffic to mitigate and respond to the TCP SYN flood attack. To create the TCP SYN flood attack, we used empty TCP packets with a TCP packet size of 40 bytes and a TCP FLAGS value of `0x02`. To ensure that our network-based attack fully utilizes the requested 500Mb link, we sent 40 000 000 TCP SYN packets in total to ensure an attack duration of 26 seconds. However, the internal function of DeterLab does not always allocate resources as requested and thus we received a link connection with 412Mb and were able to perform a TCP SYN flood attack with a duration of 42 seconds.

In our test scenario, the detection engine of the ISP network A initially identifies the malicious network traffic, creates a FLEX message of the type Event containing Cisco Netflow version 5 and starts its communication process. The MiR system of the communication process, located in each ISP network, is able to automatically deploy

Figure 4.4.: Simulation results of the attack traffic (red line) and cumulative traffic (black line)

response actions. In our test scenarios, we make use of automatic notifications via email messages including remediation suggestions that make use of `iptables`. In the initial state of the testbed networks no filtering rules are inserted to show the effects of our communication process. During the experiment within DeterLab suspicious IP addresses are identified and inserted into the packet filter ruleset to block the network traffic.

The MiR diagram of the ISP network A in Figure 4.4 shows four different types of incoming messages. First, ISP A receives two event messages at the same time containing threat information about the network-based attack from ISP network A and C targeting the web server of ISP E. Second, the adjacent collaborating networks report if they had seen similar behavior in their network. Next, ISP A adds two blocking rules to the packet filter ruleset to hit its outgoing links and starts a chain of information that is passed along to ISP C. Therefore, ISP A creates an alert and informs the adjacent collaborating networks that deploy the including remediation suggestions. The alerts shown in the MiR diagram of the ISP network A in Figure 4.4 only represent the incoming alerts and not those that are outgoing. Further, the MiR diagram of the ISP network A in Figure 4.4 shows that the attack traffic (red line) is sent over 42 seconds. Immediately, after ISP A inserted the blocking rules the effects of the attack

traffic are mitigated and the malicious traffic is not propagated further through the network of ISP A (black line). As a result, the traffic at ISP D and E dropped as shown in Figure 4.4. Next, ISP C deploys the remediation suggestion out of the alert message and as a consequence the traffic at ISP E drops. The MiR diagram of the ISP network E in Figure 4.4 shows that the collaborating partners in the stream of traffic effectively mitigate and respond to the ongoing network-based attack and thus the network of ISP E is benefiting from the collaboration and the web server recovers.

Quantitative Evaluation Results

In this paragraph, we present and discuss the results of the quantitative evaluation of the communication process.

Timeliness: The primary focus to mitigate and respond to network-based attacks is maintaining the availability of the organization's network infrastructure and services. The Message Flow diagram in Figure 4.4 shows that the overall duration until all ISP networks have a common knowledge took 6 seconds. Further, 18 messages have been sent until all participating ISP networks had a common knowledge. Even though network B has not been actively involved in the network-based attack, ISP network B has been notified by the ISP network A and thus supports a proactive and collaborative mitigation and response approach. Figure 4.4 shows that a collaboration among trusted partners facilitates a proactive network-based attack mitigation and response approach and thus contributes to ensure availability of the organization's network infrastructure.

Semi-automated deployment: Through the increasing amount of security events per day, there is a need to automatically process security events and thus lessen the time to mitigate and respond to ongoing network-based attacks. In addition, the automated dissemination of security events among collaborating partners facilitates a proactive network-based attack mitigation and response approach. In our experiment, we have shown that the dissemination of threat information including remediation suggestions exchanged with FLEX are automatically processable and deployable.

4.6. Lessons Learned

In this chapter, we found that current mitigation is done in a reactive approach and thus effects of an ongoing attack already occurred until the initial countermeasures are set up. Further, we found that collaborative mitigation is not established and as

a result the situational awareness of the current threat landscape is restricted to the view of the own network. Even though the amount of security events are increasing, current mitigation is done manually.

An important outcome is that our communication process supports proactive mitigation of network-based attacks and thus maintaining the availability of the organization's network infrastructure and services. Our communication process ensures a common knowledge of the current threat landscape even though an ISP network has not been actively involved in an ongoing attack. Through the use of FLEX within the communication process, automatic processable and deployable threat information including remediation suggestions is ensured and as a result the time to mitigate and respond to a network-based attack is reduced.

4.7. Concluding Remarks

In this chapter, we have answered the question *"Is mitigation currently done in a proactive or reactive approach? Would it be possible to do it in a proactive approach?"* We introduced a communication process that facilitates the automated defense in response to ongoing network-based attacks. We have shown that our communication process is able to proactively mitigate a network-based attack and thus reduces its effects. The main advantage of our communication process over existing approaches is that it easily integrates with the existing infrastructure and is easy to deploy. Based on our qualitative and quantitative evaluation, our communication process constitutes a viable and collaborative approach to disseminate security events among trusted ISP networks. Further, we have shown that our communication process minimizes the complexity of node interactions and will not cause a link congestion.

Selection of an Appropriate Response

This chapter introduces a new response selection model that allows to mitigate network-based attacks by incorporating an intuitive response selection process. This response selection process evaluates negative and positive impacts associated with each countermeasure. This chapter is based on the two publications:

[C8]: Jessica Steinberger et al. "Ludo" - Kids playing Distributed Denial of Service". In: *Connected Communities, The Networking Conference 2016, 15-18 June, 2016, Prague, Czech Republic, Selected Papers*. Ed. by Klaas Wierenga. GÉANT Ltd, Nov. 2016. ISBN: 978-90-77559-25-3. URL: <http://www.terena.org/publications/tnc16-proceedings/>

[C13]: Sven Ossenbühl, Jessica Steinberger, and Harald Baier. "Towards Automated Incident Handling: How to Select an Appropriate Response against a Network-Based Attack?" In: *Proceedings of the Ninth International Conference on IT Security Incident Management IT Forensics (IMF)*. May 2015, pp. 51–67. DOI: [10.1109/IMF.2015.13](https://doi.org/10.1109/IMF.2015.13)

5.1. Introduction

In Chapter 4 (Collaboration Process), we presented a communication process that supports the dissemination of threat information. This communication process constitutes one approach to counteract the proliferation of network-based attacks. However, initiating a suitable reaction is a process of selecting an appropriate response related to the identified network-based attack. The process of selecting a response requires to take into account the economics of a reaction e.g., risks and benefits.

Traditionally, automated mitigation and response processes make use of a Intrusion Response System (IRS) that provides a distinct response selection process [J22], and is able to collaborate with other security appliances, such as firewalls to block and terminate suspicious traffic [C34]. Although IRSs are promising systems, available solutions proposed by the scientific community are not widely adopted [J23]. Further, each IRS uses different metrics to select an appropriate response and some of the metrics are only applicable for specific system environments. Moreover, most of the previous work is not reproducible due to closed testing data.

Figure 5.1.: Simplified network topology of a IDS in promiscuous mode

To overcome the shortcomings of closed source and system dependency, this chapter presents a reaction strategy for response selection based on effectiveness assessment. The contribution Response Effectiveness Assessment (REASSESS) brings to the state of the art is that it evaluates negative and positive impacts associated with the responses deployment to a given attack. In addition, REASSESS is aligned to the NIST incident life cycle.

5.2. Scenario

In this section, we describe the main focus of this chapter. First, we describe the network in which we are going to place REASSESS. Second, we present how an alert occurs and initiates mitigation and response procedures within the IRS. The primary focus of this work are networks consisting of individual end hosts. Within these networks IDSs, IPSs and IRSs are often placed to protect the network against malicious traffic. The IDS sensor could be placed inline or in a promiscuous mode.

Figure 5.1 illustrates a simplified view of a network topology containing an IDS sensor in promiscuous mode. The advantage of an IDS in promiscuous mode is that it prevents forwarding delays or impacts caused by sensor failing. The traffic flow within a network with an IDS in promiscuous mode is shown in Figure 5.1. After the traffic enters the network (1) and passes the firewall, the traffic enters the Demilitarized Zone (DMZ). When the traffic arrives at the DMZ, copies of the packets are sent to the IDS sensor (2). Therefore, IDS sensors in promiscuous mode analyzes the network traffic based on copies of the original packets and raises alerts (3) in case of detected malicious traffic. However, because the original packet is already on its way towards the destination, the IDS by itself cannot prevent that the original packet makes its way onwards its destination. Hence, the IDS is detecting the attack, but not preventing.

Figure 5.2.: Simplified network topology of an IDS in inline mode (IPS)

In contrast to IDSs in a promiscuous mode, inline IDS sensors can be placed within the network as shown in Figure 5.2. Any traffic traversing the network (1) is forced to go in one physical or logical port on the sensor (2) and thus this topology adds a small delay before forwarding. In case of a benign packet, the IDS sensor forwards the packet through another logical or physical interface and continues its journey towards its destination (3). Inline IDS sensors are able to perform an automatic deployment of countermeasures e.g., drop a packet and deny that packet from reaching its final destination. Therefore inline IDSs are also called IPS. However, IPSs do not employ a distinct response selection process and thus rely on simple mappings of attacks to predefined responses [T2].

To overcome these shortcomings that just simple response actions or even no action can be taken, IRSs have been developed. IRSs provide the capability to select an appropriate response and perform both, automatic mitigation and response, to defend the network against malicious traffic. IRSs are located next to an IDS sensor as shown in Figure 5.1 and Figure 5.2. This work focuses on the reaction process deployed within an IRS. In particular, the response selection model within this reaction process that is initiated by an alert raised by IDSs. Therefore the type of IDS used within the network is not important.

5.3. Requirements and Assumptions

In this section, we define the requirements that an response selection model within an IRS should fulfill, as they emerged by the scenario described in Section Scenario and defined in [C35]. In the following, we will use these requirements to evaluate the response selection models and our proposed model REASSESS. In addition, we describe our assumptions to ensure that the work is not biased by tasks related to detection technologies.

5.3.1. Requirements

Automatic deployment: The selection of an appropriate response should be performed automatically to reduce delays caused by human interactions. Besides the reduction of delays caused by human interaction, the automatic deployment supports the timeliness of initial mitigation and response procedures, and the reduction of expert knowledge to choose an appropriate response.

Scalability: The response selection model should be able to cope with different network topologies e.g., a single network, distributed networks. Further, the response selection model should provide the capability to be placed in different network sizes and thus able to handle a different amount of alerts e.g., mid-size networks, backbone networks.

Adaptability: Due to the ever-changing nature of attacks the response selection model should have the ability to dynamically adjust the response selection and thus suit a particular type of attack identified by a IDS. The response selection model should provide automatic learning capabilities. Further, the response selection model should take into account previous responses and their effectiveness and thus make use of a knowledge base of previous responses.

System independency: The response selection model should be used within IRSs of different vendors, communities etc. It should be able to handle different sources of alerts that have been detected by IDSs that work with flow data e.g., NetFlow, IPFIX, but also IDSs that work with raw packets e.g., Snort. Further, the response selection model should ensure the integratability with other security tools. Therefore it should initiate responses that interact with other security tools e.g., firewall, router.

Calculation efficiency: A fast and efficient calculation is necessary in order to reduce the time window of an ongoing attack and thus reduce potential damages. Consequently, the identification of an appropriate response to a given alert should be calculated quickly.

Usability: The response selection model should provide a minimum number of configuration input parameters to reduce configuration efforts and the required expert knowledge to use the response model within an IRS. Network operators should be able to understand the process of selecting an appropriate response and performing the selection manually.

Security mechanisms: The selection of an appropriate response to a given attack often includes sensitive data (e.g., raw data, analyzed information of incident handling and its remediation). Due to this reason, the calculation process of the response selection model should prevent unauthorized access to this mitigation and response information to ensure that an attacker does not initiate a specific reaction with an attack. Further, the response selection model should ensure trustworthy origin, relevance and integrity of an alert.

5.3.2. Assumptions

The detection of malicious actions could be performed by monitoring technologies that classify malicious actions based on anomalies or signatures. Well-known signature based systems are Snort, Suricata [B6], STAT or NetSTAT [J19]. Current anomaly-based systems often use flow export technologies (e.g., Cisco NetFlow, IPFIX). Well-known anomaly-based systems using flow export technologies are BotTrack [C17], BotFinder [C31] and Disclosure [C18]. Both, signature and anomaly-based systems rely on information that determine what is normal behavior and what is not normal. Due to the ever-changing nature of networks, applications, and malicious actions, false positives might be raised. However, the main focus of this article is the selection of an appropriate response after a malicious action was detected and thus the assumptions are as follows:

Aggregation: Each alert raised by a detection engine is treated as one attack. The aggregation and fusion of alarms should be taken into account by the detection system. This assumption is in accordance to previous work [T2, C32, T3].

Confidence: We assume 100% confidence of the alerts. A detection system might raise false alerts but to ensure a hundred percent certainty of the alerts or a sanity check of the detection engine is out of scope of this work. This strong confidence is in accordance to [T2, C32, T3].

5.4. Related Work

In this section, we present an overview of existing response selection models. For each model we elaborate its point of view and calculation methodology. Additionally, we describe mandatory input parameters and requirements of each model. Further, we

Figure 5.3.: Dependency tree between the two users Anne and Customer of IE-IRS [C35]

analyze the response models with regard to their use-case context and to what type of attack a response is selected.

5.4.1. Evaluating the Impact of Automated Intrusion Response Mechanisms

In the year 2002 researchers of the Technical University Vienna proposed a response selection model, hereafter referred to as IE-IRS [C35]. IE-IRS is used to select different firewall configurations as a response to a given attack. These firewall configurations are evaluated with respect to their effectiveness. Therefore IE-IRS takes into account dependencies between network services offered by hosts, system users, network topologies and firewall rules [C35]. These dependencies are modeled as a dependency tree and shown in Figure 5.3.

```

DNS is service at 132.100.98.11 53 udp
{ processName="bind"; };

HTTP is service at 132.100.98.15 80,
at 132.100.101.4 80
{ processName="httpd"; };

NFS is service at 132.100.100.4 2049
{ processName="nfsd"; };

anne is user at 132.100.100.27 { cost=5000; }
requires (DNS at 132.100.98.11 53 udp 0.4)
and
(NFS at 132.100.100.4 2049 0.4
and HTTP at 132.100.101.4 80 0.2 ) ;
  
```

Listing 5.1: Dependency tree between the two users Anne and Customer of IE-IRS [C35]

Besides a dependency tree this response selection model utilizes a modeling language which is shown in Listing 5.1. This modeling language consists of a Bison¹ grammar

¹<http://www.gnu.org/software/bison>

file as input and a fast lexical analyzer generator (FLEX²) file. The final output file contains C source code. The modeling language is used to define the importance for each network service as shown in Listing 5.1. The importance for each network service has to be defined through a user or customer that uses this service. Further, the importance of a service is defined in terms of costs related with the degradation or termination of the service.

In order to select a meaningful response, the degradation of the working capability and penalty costs are determined. However, the authors declare the penalty costs as a constant value. In addition, the authors stated that IE-IRS is able to terminate processes and disable user accounts. As an example, IE-IRS has been used to mitigate and react on a Denial of Service (DoS) attack against a web server. To select a response the response selection algorithm takes into account penalty costs of a resource being unavailable and the capability of a resource. The capability is determined by using a depth-first search without a cyclic behavior. Therefore the authors introduce a capability value $c(e) \in [0..1]$ of an entity e . This capability value indicates the performance of an entity if the specified response strategy is triggered, compared to the situation when all resources are available. Let entity e be not dependent on any other entities, then the capability of $c(e) = 0$. In case of $c(e) = 0$, the entity does not provide any service to other system resources. In contrast, $c(e) = 1$ implies that the entity provides service to others. The capability reduction is defined as $cr(e) = 1 - c(e) \in [0..1]$. The penalty costs $p(e)$ for an entity e is a value representing the cost when e becomes unavailable. The penalty costs of a network service is calculated using the following equation: $p(e) = cr(e) \cdot \text{penalty}$ where the *penalty* is a user-defined constant that reflects the importance of an entity. The response with the lowest penalty cost has the least negative impact on the system and is selected to be deployed to a given intrusion.

5.4.2. Adaptive Intrusion Response using Attack Graph

The Adaptive Intrusion Response using Attack Graph (ADEPTS) [C36] approach was published by researches of Purdue University in 2005. ADEPTS mainly considers host attacks (e.g., buffer overflows or privilege escalation) and was built to show that several intermediate attack goals need to be accomplished by an adversary to achieve the attack. Thus ADEPTS employs attack graphs to identify the actions required to achieve possible attack targets in a distributed system. This attack graph of ADEPTS is an Directed Acyclic Graph (DAG) [C36] and used to show the objectives

²<http://flex.sourceforge.net>

Figure 5.4.: A sample attack graph of ADEPTS [C36]

of suitable responses. Attacker goals are expressed as end states in the attack graph with intermediate steps leading to the fulfillment of those goals. Such an attack graph is shown in Figure 5.4.

The edges in the intrusion graph are categorized into the three types: OR, AND, and QUORUM. For a node with incoming OR edges, an intruder has to achieve at least one of its child nodes. In contrast, for AND edges, all the child nodes have to be achieved. For QUORUM edges a Minimum Required Quorum (MRQ) is assigned to it. This number represents the minimum number of child nodes in which goals need to be achieved in order for the node to be accomplished. For instance, node ten in Figure 5.4 has an MRQ of two. If two database servers are successfully under attack by a DDoS attack, the database is no longer usable for the system in a satisfying manner.

The intrusion graph has to be updated when changes to the system configuration or new known vulnerabilities related to the system architecture occur. Thus vulnerability information have be obtained, preprocessed or tailored to the specific environment

in a regular manner. To update the intrusion graph, a semi automated method called Portable Intrusion Graph Generation (PIG) is employed. PIG requires the two inputs: vulnerability descriptions and system services description. Both, the vulnerability descriptions and system services description are system and environment dependent, and thus created manually.

The system service description is a directed graph, in which each node represents a service. The edges are considered as intrusion channels. These intrusion channels model how an intrusion can spread from a compromised node to the next node which is connected through the edge.

The vulnerability descriptions are obtained by querying common vulnerability databases, such as NIST's National Vulnerability Database (NVD)³, the Bugtraq security database⁴, the Open Source Vulnerability Database (OSVDB)⁵, and the CVE referencing standard. However, manually adjustments are also required in the generation algorithm. These manually adjustments cover the specification of the four characteristics: (i) name, (ii) affected services, (iii) manifestation, and (iv) dependent vulnerabilities and services.

The characteristic *Name* ensures human readability. *Affected services* represents an enumeration of services in the system service description affected by the vulnerability. The characteristic *Manifestation* describes the result of a successful exploitation. Possible outcomes are considered as leaking of information, execution of arbitrary code, incorrect behavior of service, DoS, and service termination. *Dependent vulnerabilities* denotes the dependence on other vulnerabilities and services that have to be compromised to exploit this vulnerability.

The selection of a response is based on effectiveness to that particular attack in the past. Further, the selection takes into account the disruptiveness to legitimate users and a confidence level which indicates the probability that the attack is actually taking place. ADEPTS provides response measures to block IP addresses and host specific reactions such as rebooting the web server.

After a response has been deployed the system checks if the response was successful. If a response action is deployed on an edge that can be used to reach the attackers goal the effectiveness is decreased. After a certain amount of time or when an administrator deactivates a response the response is considered as successful if no further alerts were observed.

³<https://nvd.nist.gov>

⁴<http://www.securityfocus.com/vulnerabilities>

⁵<http://osvdb.org>

5.4.3. A Framework for Cost Sensitive Assessment of Intrusion Response Selection

In 2009 researchers of the Iowa State University proposed a framework to select the most appropriate response in balance of the potential damage of an attack and the costs for mitigation [C32]. This approach is also described in several other publications of the authors [J23, M66, T2] and will be referred as CS-IRS in the following.

The basic idea of CS-IRS is that response actions lead to positive and negative effects. CS-IRS is intended to minimize the damage of the attack and the negative effects of the response deployment. To achieve this, a set of measurements are introduced to characterize potential costs associated with the intrusion handling process in terms of the risk of potential intrusion damage, effectiveness of response action, and response cost for a system. In CS-IRS, response cost and intrusion cost are evaluated based on two factors: operational cost and impact on system resources. The assessment of system resources, response cost, and potential intrusions are modeled as static values. They are based on the expert judgment and are represented as values in the range $[0, 1]$. The final step is the response selection process at the time of intrusion. To estimate the response effectiveness, they calculate a response success rate against detected intrusions and a response coverage value. A success rate parameter (response goodness) is defined for each response. If the selected response succeeds in repelling the attack, its success factor is increased by 1. Otherwise, the failure factor of the response is increased.

CS-IRS requires the input of an IDS. In particular, CS-IRS expects an alert raised by an IDS. In addition, the model requires information about the systems security policy. The systems security policy contains a value between 0 and 1 that represents the importance for the overall system with respect to the security goals confidentiality, integrity, availability. CS-IRS also requires the enumeration of system resources with their importance to the system and definitions of known intrusions [T2]. CS-IRS was designed to work as a host-based solution and thus provides response measures to reboot the system, block user accounts or restart a service. The authors of CS-IRS used attacks of the DARPA/Lincoln Lab offline evaluation data to evaluate CS-IRS and select an appropriate response to a given attack.

5.4.4. Topological Vulnerability Analysis

A preventive approach called Topological Vulnerability Analysis (TVA) was proposed by researchers of George Mason University in 2010 [C37]. TVA is a modeling and simulation approach that relies on existing security tools to gather the required information.

Figure 5.5.: Response selection process

This information includes vulnerability information and network configuration. In addition, a continual monitoring of information sources regarding reported vulnerabilities is necessary to keep pace with emerging threats.

TVA combines vulnerability information from internal sources and external sources (e.g., NIST NVD, CVE, Symantec DeepSight). TVA also takes into account the attacker perspective to discover all attack paths within a network. As internal input, potential vulnerabilities an attacker might abuse and network configurations are used for generating an attack model. Network configuration data might include vulnerability scan reports and firewall rules. The exploits in the attack model are matched against the provided vulnerability information to predict multi step attacks. Using this information, an attack graph is generated similar to ADEPTS. In contrast to ADEPTS, the attack graph of TVA guides optimal strategies for preventing attacks, such as patching critical vulnerabilities and hardening systems and services. However, there usually remain some residual attack paths within a network. At this point, the attack graph provides the necessary context for dealing with intrusion attempts. For instance, the attack graph can guide the placement of intrusion detection sensors to cover all attack paths, while minimizing sensors redundancy. Finally, this graph is used to generate recommendations for vulnerability mitigation and computation of metrics to measure the overall network security.

5.5. REASSESS - Response Effectiveness Assessment

This section introduces our response selection model REASSESS (Response Effectiveness ASSESSment). We first explain its concept and its components, and then turn to its calculation methodology. Finally, we describe the use of REASSESS within three scenarios as proof of concept.

5.5.1. Reaction System Concept

Our response selection model REASSESS is based on CS-IRS [C32] and IE-IRS [C35]. In contrast to CS-IRS, REASSESS considers the negative effects of a response as an estimation of the degree of negatively affected legitimate service requests due to the response deployment. In addition, the negative impact of an attack without taking a responsive action is modeled with the usage of the priority of an alert. In contrast to the IE-IRS, REASSESS models penalty costs as Service Level Agreement (SLA) violation costs related to the importance of a provided service.

REASSESS consists of the five stages: Input & Configuration, Alert Processing, Response selection, Response execution and Documentation, which are related to the NIST incident response cycle. The response selection process of REASSESS and its main components are shown in Figure 5.5.

Before REASSESS may be used in a productive environment, configuration steps need to be performed. These configuration steps are described within the Input & Configuration stage and the related NIST incident response cycle phase called preparation. Within this preparation phase, the importance of different system components are assessed e.g., assessment of provided services within the network. In addition, suitable responses that can be applied in the system environment are identified and defined. Besides the configuration of REASSESS, the input of an IDS is required and described within the Detection & Analysis phase. Within this phase, an IDS performs the detection and interpretation of an attack. In case the IDS detects malicious traffic, it raises an alert that initiates the alert processing within an IRS. The alert processing stage consists of an alert normalization, aggregation and correlation. The alert processing stage is not covered by REASSESS, because of its own complexity. After completion of the alert processing stage, the response selection stage is initiated. The response selection stage is related to the Detection & Analysis phase of the NIST incident response cycle. The selection of a response takes into account the benefits and risks of a reaction, but also potential damages caused by the attack in case of no reaction. In addition, the selection of a response also looks up previous reactions and their effectiveness. Finally, possible responses are identified and prioritized. After the response selection

Figure 5.6.: The reaction strategy aligned with the NIST incident response cycle

stage, the response execution is started. The response execution stage is related to the Containment, Eradication & Recovery phase of the NIST incident response cycle. Within the response execution stage, configuration changes, notifications or knowledge sharing is performed. Finally, the documentation stage starts which is related to the Post-Incident-Activity of the NIST incident response cycle. Within the documentation stage, the alert and its response are reported, the response effectiveness is calculated and all alert related data is stored for later investigations within a knowledge base. The alignment of REASSESS to the NIST incident response cycle is shown in Figure 5.6 and thus ensures both reproducible and understandable results.

5.5.2. Calculation Methodology

Traditionally, human experts are informed about the occurrence of an alert and begin to extract the necessary information. This information might include data about the targeted system component and the source of the potential attack. Afterwards the benefits and risks of each response are compared with potential damage of the attack and finally a response based on reasoning and experience is selected. The response selection model REASSESS facilitates this comparison and returns the most suitable response to a given alert.

Therefore the comparison is modeled within REASSESS with an effectiveness value E . Let $R = \{r_0, r_1, \dots, r_n\}$ be a set of appropriate responses r for the system environment, then the effectiveness for each response $E(r)$ is defined as in Equation (5.1)

$$E(r) = A_p - A_n \in [-1..1] \quad (5.1)$$

where $A_p \in [0, 1]$ are the positive effects and $A_n \in [0, 1]$ the negative effects of a response as explained in what follows. The model's aim is to select the response with the highest effectiveness E and execute it in case of a detected attack as presented in Equation (5.2).

$$\max(E) \Leftrightarrow \max(A_p - A_n) \in [-1..1] \quad (5.2)$$

In case of $E(r) = E(r')$ where $r = r'$ both responses are applicable. In the initial iteration of the response selection stage only negative effects are considered, thus $A_p = 0$. To model the negative effects of an attack or a response two factors are considered. First, the impact of the attack or response to the system and second, the importance of the attacked system component. Accordingly, the negative impact A_n can be determined as in Equation (5.3)

$$A_n = \frac{F_d(\epsilon) + S(\epsilon)}{2} \in [0..1] \quad (5.3)$$

where $S(\epsilon)$ denotes the importance of the service ϵ and $F_d(\epsilon)$ is the capability reduction. We define the capability value F to indicate the performance of an entity ϵ either due to a deployment of a response measure, or in the event of an attack. Thus, we are considering: $\exists r \in R$ that indicates no response. The capability reduction F_d is defined as in Equation (5.4)

$$F_d(\epsilon) = 1 - F(\epsilon) \in [0..1]. \quad (5.4)$$

We identified a casual loop between the priority of an incident and impact on available services. The more impact an incident has on normal services offered to users, the higher the priority assigned to the alert will be. The estimation of the alerts importance is done by IDSs. Hence, to model the case of an attack without a response, the capability reduction can be derived from the priority of the alert by dividing its priority value with the highest possible priority value. This division is performed to normalize the priority of the alert to a value $\in [0 \dots 1]$. In order to model the negative impact of a response deployment, each available response has to have a disruptive impact assigned to it. We define $D \in \{none, low, medium, high\}$ as an estimation of the disruptive impact of negatively effected legitimate service requests due to the response deployment. Whereas $none = 0.0$, $low \in [0.01 \dots 0.33]$, $medium \in [0.331 \dots 0.66]$, and $high \in [0.66 \dots 1]$. For instance, isolating a service from the network would have a

high impact and thus would have a capability reduction of $F_d(\epsilon) = 1 \in [0.661 \dots 1]$. The service importance can be derived from an SLA where penalty costs are associated with the degradation of the service. We identified a relation between the SLA defined penalty costs and the importance of the service. In theory, the higher SLA penalties have to be paid in case of unavailable services, the more important the service is in the system's context. The importance of a system component is defined by dividing the SLA costs of the incident by the highest SLA costs to normalize it to a value $S \in [0..1]$.

After a response is deployed, the positive effects are calculated. We define the positive impact A_p as in Equation (5.5)

$$A_p = rsr \in [0..1] \quad (5.5)$$

where rsr is the response success rate. Let $R = \{r_0, r_1, \dots, r_n\}$ be the set of responses and $A' = \{a_0, a_1, \dots, a_m\}$ the set of alerts, then $rsr(r_i, a_j)$ denotes the response success rate for a given response r_i and alert a_j . The rsr value is the degree of successful deployments of response r_i to counter an attack indicated by an alert a_j divided by the total number of deployments of r_i regardless of its success in countering attacks indicated by an alert a_j (cf. Equation 5.6)

$$rsr(r_i, a_j) = \frac{dps_{r_i}(a_j)}{dpt_{r_i}(a_j)} \in [0..1] \quad (5.6)$$

The number of deployments of response r_i in case of a_j that successfully mitigated the attack is denoted by $dps_{r_i}(a_j)$. The total number of deployments of response r_i in case of a_j without success in mitigating the attack is denoted by $dpt_{r_i}(a_j)$.

5.5.3. Proof of Concept

To prove the concept of the response selection model REASSESS and its calculation methodology, a testbed is set up as shown in Figure 5.7. This testbed comprises two networks interconnected by the Internet. The IRS containing REASSESS is located in network A and is able to intercept ongoing data flows. The testbed involves malicious activity originating from the attacker residing in network B targeting the victim in network A. On each relevant network interface packet capture files of the attack are recorded.

With the aid of this testbed three different test scenarios are conducted to prove the performance, the correctness and the mitigation capabilities of REASSESS and can be described as follows:

Figure 5.7.: Simplified view of the REASSESS testbed

Performance measurement: The performance of REASSESS is measured using different amounts of alerts (e.g., 125, 500, 2 000, 8 000). These alerts are passed to the IRS simultaneously in order to determine how fast REASSESS parses an alert, calculates and identifies an appropriate response and finally deploys this response.

Correctness: To verify the correctness of REASSESS, we launch a TCP SYN flooding attack that is detected by the IDS. Our response selection model REASSESS calculates, identifies and deploys the most suitable response. Afterwards the effects of this response are measured. In addition, we can evaluate if the calculation and identification of an appropriate response is fast enough to counter the attack.

Mitigation capabilities: The mitigation capabilities of REASSESS are tested using a bandwidth attack. This bandwidth attack consists of 200 000 network traffic packets with an attack duration of 13.41 seconds. The attack is launched from network B targeting network A as shown in Figure 5.7.

To perform these measurements in our three use-case scenarios, we developed an application that contains seven components as shown in Figure 5.8. The gray colored component represents the detection engine. In our application, we use the open-source IDS Snort. At a later point in time, the IDS Snort could also be replaced by other IDSs in order to keep the flexibility.

The *Preparation Module* parses the files that contain information about network services, and the disruptive impact of the response measures. This information is defined manually by a human expert within the preparation phase of REASSESS and is accessible to the *Response Selection Module* which utilize this information for its decision making process. The *Alert Parser* handles the alerts raised by the *Detection Engine* and

Figure 5.8.: Overview of the components of the REASSESS application

extracts the necessary information for the *Response Selection Module*. Afterwards, the *Response Selection Module* identifies the attacked service on the basis of the information provided by the *Alert Parser* and *Preparation Module*. In addition, it calculates the effectiveness value E for each available response measure and selects the response with the highest E . Subsequently the *Response Deployment Module* gets instructed respectively which takes the required information and deploys the selected response by means of applying firewall rules. Each response is applied with a logging prefix to identify the discarded packets later. Thus, the success of the response can be evaluated by the *Post Activity Module*. Finally, the *Documentation Module* provides an interface to a database which includes the effectiveness of previously deployed responses. Additionally, the database may include incident related information.

The testbed of REASSESS was installed on three virtual machines interconnected by two virtual networks. Each virtual machine consists of one CPU of 2.5 GHz and 1 GB of RAM. The reaction system maintains two network interfaces (internal and external), enabling it to intercept ongoing data flows as shown in Figure 5.9. The IDS and REASSESS can be installed on the same physical device, but this is not a mandatory requirement. Besides the installation and configuration, one challenge is finding a suitable dataset for testing purposes. In contrast to IDSs, replaying public available dataset is not sufficient, because an IRS requires network traffic that can be replayed bidirectional [J24]. This means that packets from the attacker should arrive on the IRS interface, and packets (and replies) from the target on another interface. In addition, configuration changes applied by the IRS need to be verified to ensure that the network components e.g., firewall are not misconfigured and still working properly. Thus, replaying recorded network data can not be used to evaluate the response deployment and mitigation capabilities of an IRS.

In our testbed, we identified and configured three suitable responses to defend the network: (i) no responsive action, (ii) rate-limiting a connection and (iii) IP traffic

Figure 5.9.: Testbed for REASSESS application

Table 5.1.: Measured runtimes for different amount of alerts.

	125 Alerts	500 Alerts	2000 Alerts	8000 Alerts
slowest runtime	13.147 sec.	50.353 sec.	195.386 sec.	838.901 sec.
fastest runtime	11.472 sec.	45.676 sec.	189.582 sec.	792.314 sec.
average runtime	11.957 sec.	48.550 sec.	192.435 sec.	804.555 sec.

filtering. The response rate-limiting and IP traffic filtering make use of `iptables`⁶ that provides the capability to throttle incoming connections and support basic firewall functionality. These responses are chosen in accordance to previous work [C36, T2, T3]. However, our evaluation also validates the correctness of the response selection.

Performance measurement: The performance of REASSESS is evaluated using the three defined suitable responses: no responsive action, rate-limiting and IP traffic filtering. In different test steps a quantity of 125, 500, 2 000, 8 000 alerts are generated and transmitted to the victims network. The IRS including REASSESS receives these alerts, calculates and identifies a suitable response. The results reveal that the runtime of the tests scale linearly as shown in Table 5.1. Furthermore, the runtime of each test depends on the available CPU and RAM resources. Other processes running on the system can slow down the selection process significantly if they are consuming a large fraction of the CPU resources.

Correctness: To verify the correctness of REASSESS, we assume that the DNS service of the victim network is target of an attack. Given $R = \{\text{none}, \text{rate-limit}, \text{blockIP}\}$, $S(\text{DNS}) = 1$, an alert α , $rsr(\text{rate-limit}, \alpha) = 0$, $rsr(\text{blockIP}, \alpha) = 0$, $D(\text{rate-limit}) = F_d(\text{rate-limit}) = 0.66$, and $D(\text{blockIP}) = F_d(\text{blockIP}) = 0.2$. Let $\#$ denote the Iteration and $p(a)$ the priority p of the alert and let $p = 1$ be the lowest and $p = 3$ the highest priority. Then REASSESS calculates values as listed in Table 5.2. The response `blockIP` was successful in every single test run. Thus, the rsr of response `blockIP` changes to 1.0 and remains at this value.

⁶<http://netfilter.org/projects/iptables/index.html>

Table 5.2.: Calculations within the Response Selection Module.

#	$p(\alpha)$	r	$D(r)$	rsr	$A_n = (F_d(r) + S)/2$	$E = A_p - A_n$
1	3	none	1.0	0.0	$2.0/2 = 1.0$	-1.0
		rate-limit	0.66	0.0	$1.66/2 = 0.83$	-0.83
		blockIP	0.2	0.0	$1.2/2 = 0.6$	-0.6
1	2	none	0.66	0.0	$1.66/2 = 0.83$	-0.83
		rate-limit	0.66	0.0	$1.66/2 = 0.83$	-0.83
		blockIP	0.2	0.0	$1.2/2 = 0.6$	-0.6
1	1	none	0.33	0.0	$1.33/2 = 0.66$	-0.66
		rate-limit	0.66	0.0	$1.66/2 = 0.83$	-0.83
		blockIP	0.2	0.0	$1.2/2 = 0.6$	-0.6
2	1	none	0.33	0.0	$1.33/2 = 0.66$	-0.66
		rate-limit	0.66	0.0	$1.66/2 = 0.83$	-0.83
		blockIP	0.2	1.0	$1.2/2 = 0.6$	0.4

Beside the identification of the most suitable response, the effectiveness of a selected response needs to be verified. After REASSESS identified blockIP as the most suitable response, the response was deployed. The deployment of the response blockIP resulted in an additional rule added to the firewall. Further, the test results show that the ninth packet and tenth packet gets dropped due to the decision of the reaction system. Blocking is considered as successful if a logging entry is found that indicates the blocking of the IP address in one second difference compared to the timestamp of the alert. The firewall log file reveals that the packets were logged and discarded.

Mitigation capabilities: The mitigation capabilities of REASSESS are evaluated by using a bandwidth attack that consists of 200 000 network traffic packets. One feasible way to verify that a replayed attack is blocked is to ensure that the packets of the attack are not received at the target [J24]. Due to capturing packets transmitted through the attackers network interface, we observed that only 157 629 of the 200 000 packets are sent out by the attack tool and transmitted further towards the victim's network. During the attack, Snort raises 17 108 alerts and 15 438 packets are blocked due to the reaction to the alerts. Even though only 10.85 % of the packets traversing the interfaces were detected as an attack, 90.23% of them were blocked due to the decision of REASSESS.

5.6. Evaluation

In this section, we evaluate the response selection models. First, we describe the characteristics of the evaluation criteria derived from the requirements presented in Section Requirements. Furthermore, we introduce eight evaluation criteria for the response selection models. Last, we present and summarize our findings.

5.6.1. Evaluation Methodology

The response selection models are evaluated based on the following eight criteria: automatic deployment, scalability, adaptability, system independency, calculation efficiency, usability, security mechanisms and evaluation methodology. These criteria were chosen to provide a means of comparison between the response selection models and to measure if and how the use of this response selection model is viable for network operators.

Each response selection model is evaluated using the following method. For each evaluation criteria one of the following scores is determined: low (-), medium (0), and high (+). All response models start with a score of 0. In case a low score is determined for a criterion, the sum will be decreased by 1, and increased by 1 in case of a high score respectively. A medium score is equal to 0 meaning that the sum will not be changed. In the best case a response model can have a sum of 8 meaning that all criteria are considered as high, in the worst case a response model will score with the sum of -8.

The ability to select and deploy an appropriate response automatically to reduce delays which result due to human intervention is described by the 'automatic deployment' criterion. This also includes the ability to evaluate the effectiveness of the deployed response. The criterion 'scalability' describes the ability handle different sizes of network topologies. An response selection model is called scalable when it is capable of working properly with small networks e.g., company networks but also large networks e.g., high-speed networks. 'Adaptability' defines the aptitude to suit different use-cases. A response selection model is called adaptable when it is capable to automatically learn from previous responses and their effectiveness and take them into account during a response selection. The ability to use the response selection model in various system environments is described by the criterion 'system independency'. The criterion 'calculation efficiency' describes how fast the calculation of an appropriate response is. The calculation of a response must be fast in order to respond in an appropriate time. 'Usability' describes whether a response selection model requires expert knowledge to provide input parameters. A response selection

model is called usable when the input parameters and their calculation process do not require a system expert. The use of security mechanisms e.g., encryption or signature, within a response selection model is described by the criterion 'security mechanisms'. The criterion 'evaluation methodology' describes the reproducibility of the evaluation of a response selection model. Further, the criterion 'evaluation methodology' focuses on real world scenarios that show the practical applicability.

5.6.2. Evaluation Results

In this section, we present and discuss the evaluation results of the response selection models according to the above described eight criteria.

Automatic deployment: IE-IRS is described to be able to automatically evaluate and re-evaluate responses in the system context and thus allows to determine the effects of different responses. IE-IRS does not describe the ability to make use of an automatic deployment of responses and thus result in low automatic deployment capability.

ADEPTS is able to automatically deploy responses. The system uses a feedback mechanism which adjusts the effectiveness of the response based on whether the response was successful in preventing further attacks or spread of the current attack. After a certain amount of time or when an administrator deactivates a response the response is considered as successful if no further alerts were observed. Therefore the capability to automatically deploy an appropriate response of ADEPTS is considered as high.

CS-IRS is also able to automatically deploy responses and thus the automatic deployment is considered as high. Even though a metric response success rate is explained, there is no explanation given how the response is evaluated to be successful or not.

In contrast to ADEPTS and CS-IRS, TVA does not provide an automatic deployment of responses and thus score low in this criterion. Instead of providing an automatic deployment of responses, TVA automatically generates graphs which show vulnerability interdependencies to guide an administrator in finding vulnerabilities and preventive measures to harden the network. REASSESS is able to automatically deploy responses and verify if they had the desired effect. The automatic deployment of responses within the REASSESS application is achieved by parsing certain log entries of the firewall for discarded packets due to the reaction decision of REASSESS. Therefore the capability to automatically deploy an appropriate response of REASSESS is considered as high.

Scalability: The calculation and descriptions of the IE-IRS dependency graph is considered as complex in mid-size or large-scale networks. The reason is that IE-IRS builds a dependency graph of network services offered by hosts, system users, network topologies and firewall rules. Therefore the scalability capability of IE-IRS is considered as low.

Similar to IE-IRS, ADEPTS creates an attack graph, but ADEPTS focuses on specific system environments, namely distributed web-based environments. Therefore the attack graph compared to IE-IRS is quite small. However, the use of ADEPTS in mid-size or large scale environments might require some adaption and thus the scalability of ADEPTS is considered as low.

Besides IE-IRS and ADEPTS, TVA also uses an attack graph. However, the graph generation of the TVA approach is quadratic in the number of hosts involved and can be reduced to $\mathcal{O}(n)$ by grouping hosts into protection domains. Therefore the scalability of TVA is considered as low. CS-IRS and REASSESS are able to handle different sizes of network topologies and thus the scalability capability is considered as high.

Adaptability: During the selection of a response, IE-IRS is capable to take into account a response history. However, the computation time to select an appropriate response increases. Further, IE-IRS only considers negative side effects of a response. Therefore the aptitude to automatically learn from previous responses and thus suit different use-cases is considered as low.

In contrast to IE-IRS, ADEPTS takes into account previous effectiveness of the response, but only considers positive effects as basis of the response selection process. The response effectiveness is a value indicating how successful the response was in mitigating the attack. ADEPTS does not consider negative side effects of the chosen response. Therefore the aptitude to automatically learn from previous responses and thus suit different use-cases is considered as medium.

The response selection model CS-IRS introduces the response success rate. This response success rate provides the aptitude to learn from previous responses. Therefore the adaptability capability of CS-IRS is considered as high. TVA takes into account several external sources (NIST NVD, CVE) to build a multi-step attack graph for the system environment. As these external sources also store the reported vulnerabilities, TVA contains both, a history and the latest reported ones. By its nature, TVA does not consider negative or positive side effects of a response to a given attack. Therefore the aptitude to automatically learn from previous responses and thus suit different use-cases is considered as medium.

Similar to CS-IRS, REASSESS stores a response success rate that represents positive effects of a response. REASSESS also provides a response history stored within a database and thus is much more efficient than IE-IRS. The aptitude to automatically learn from previous responses and thus suit different use-cases is considered as high.

System independency: The IE-IRS response model requires information about the network in terms of a list of services with their IP address and port. In addition the users or customers have to be defined along with the costs related to service degradation or termination. These definitions can be done for any network. Thus, the system independency of IE-IRS is considered as high.

The attack graph of ADEPTS can be computed for other environments as well. However, the attack graph of ADEPTS focuses on distributed web-based environments. Therefore an implicit assumption is, that the structure of the intrusion graph is fairly stable. The authors in study [J23] reported, deploying ADEPTS in a different setting might require significant modifications. Therefore the system independency of ADEPTS is considered as medium.

CS-IRS relies on measures based on expert judgment and the system security policy. The expert judgment and the system security policy could be defined in any network.

Similar to CS-IRS, TVA takes into account network scans and vulnerability information of different external sources. These external sources provide system independent vulnerability information. Therefore the system independency of CS-IRS and TVA is considered as high.

REASSESS relies on information about the services and the disruptive potential of a response. This information can be collected in any environment. Therefore the system independency of REASSESS is considered as high.

Calculation efficiency: In principle, the IE-IRS response selection model provides a fast calculation methodology to identify an appropriate response, but over time the calculation methodology has to analyze the length of the response history and the number of alternative response actions. A huge amount of alternatives in a long history of response actions lead to an explosion of the number of sequences that IE-IRS has to evaluate. The authors of IE-IRS stated that even though it is possible to optimize the algorithms used within IE-IRS, the number of possible responses increases exponentially with the length of the history of response actions. The computation time for the best response strategy of IE-IRS with 35 resources and a dependency graph of depth of up to 8 computes 34 seconds using an Pentium III with CPU of 550 MHz and 512 MB of RAM. Therefore the calculation efficiency of IE-IRS is considered as low.

ADEPTS uses a directed acyclic graph (DAG) to create an attack graph. Even so the attack graph of ADEPTS has to be updated on a regular basis, algorithms for constructing them in linear time are known. Therefore the calculation efficiency of ADEPTS is considered as high.

Similar to IE-IRS, the CS-IRS response selection model provides a fast calculation methodology to identify an appropriate response. The computation time for the best response strategy of CS-IRS in inline mode with 10 000 system resources, 100 intrusion responses available in the system and 100 suspected intrusion computes 0.015 seconds using an Intel Core 2 Duo CPU U7700 with CPU of 1.33 GHz and 1 GB of RAM. Significantly less computation time is required with 1 000 system resources, 100 intrusion responses available in the system and 100 suspected intrusion. With these settings, CS-IRS computes less than $5\mu s$. Therefore the calculation efficiency of CS-IRS is considered as high.

The graph generation of the TVA approach is quadratic in the number of hosts involved and can be reduced to $\mathcal{O}(n)$ by grouping hosts into protection domains. However, a graph for a network containing 100 subnets and 20 000 hosts computes 14 minutes using a quad-core Intel Xeon CPU at 1.86 GHz, with 4 GB RAM. Taking into account, that this approach is intended to be used for preventive measures the computation time is less important. Therefore TVA results in a medium scalability capability.

As REASSESS is based on CS-IRS, the calculation methodology is similar to CS-IRS. In contrast to CS-IRS, REASSESS was evaluated in conjunction with an IDS in promiscuous mode. Further REASSESS analyzes the impact of no reactive response, positive and negative effect of a response. Therefore the calculation methodology requires more steps to be completed in comparison with CS-IRS. The computation time for the best response strategy of REASSESS in promiscuous mode with 125 alerts computes 12 seconds using a CPU of 2.5 GHz and 1 GB of RAM. Therefore the calculation efficiency of REASSESS is considered as medium.

Usability: The IE-IRS response selection model requires a dependency tree with all available network services offered by hosts, system users, network topology and firewall rules. The importance of each network services has to be defined though a user or a customer that uses this service. As the judgment of users regarding the importance of a network service depends on subjective opinion, the importance ranking results in a diversity of interpretations. Therefore the usability of IE-IRS is considered as medium. ADEPTS uses a semi automated way to re-generate the attack graph.

As IE-IRS, ADEPTS requires a vulnerability and a system service description that are created manually. Besides the vulnerability and the system service description, adjustments are required to tailor the attack graph to the system environment. Therefore the usability of ADEPTS is considered as medium.

Similar to IE-IRS, CS-IRS the response and intrusion costs, and the system policy are modeled as static values. Further these values are based on expert judgment. Besides the a high amount of manual input, the response and intrusion costs often depend on SLAs and thus should not be modeled as static values. Therefore the usability of CS-IRS is considered as medium. TVA provides a graphical user interface (GUI) to analyze the attack graph, but the TVA attack graphs can be much too complex for easy understanding even in a small setting of 20 hosts in four subnets. To overcome this shortcoming, the GUI of TVA supports a graph navigation with high-level overviews and detail drilldowns. Due to the complexity of the attack graphs of TVA and the fact that they are not easy to understand without the GUI the usability of TVA is considered medium.

Similar to CS-IRS, REASSESS requires information about the services, SLA penalty fees, and how disruptive a response is considered in the system environment. In contrast to CS-IRS, all this information can be defined without expert judgment. In REASSESS the penalty costs are modeled in consideration of the SLA violation costs. The remaining information are either known or can be obtained by using network management tools such as SNMP. Consequently, the usability of REASSESS is considered as high.

Security mechanisms: None of the response selection models provide any mechanisms to secure the sensitive incident handling information. Moreover, none of the response selection models prevent unauthorized access to the mitigation and response information. The response selection models that take into account external sources do not ensure that the external sources is a trustworthy origin. Therefore the security mechanisms of all response selection models is considered as low.

Evaluation methodology: IE-IRS was evaluated using 13 different response actions that consists of up to ten firewall rule changes, user accounts and process status modifications. The authors of IE-IRS conclude that selecting different response actions can be done quickly, but this is only due to the fact that only crucial network services are modeled and thus the number of network services is limited. Further, the evaluation relies on optimized data structures. In addition, the authors of the IE-IRS basically measured the performance of their proposed evaluation method instead of

the calculation efficiency of IE-IRS. Therefore the evaluation methodology of IE-IRS is considered as poor. In order to evaluate ADEPTS, a metric called survivability is introduced. The value of this metric relies on two dependencies. First, the set of high level system transactions that can be achieved. Second, the set of high level system goals which are not violated in the case of an intrusion. A high level transaction depends on successfully operating services and their interactions between them. Preventing information leakage, for instance is referred as a high level system goal, thus, assuring high level system goals imply preventing certain intrusion goals from being successful. For testing, real attack scenarios were injected into the system. The survivability of the system was compared to no response mechanism, static responses only, and their system. Static responses are applied with a mapping of attacks patterns to pre-defined responses. The authors of ADEPTS have shown that ADEPTS was able to outperform the static response. The introduction of the survivability metric hinders the comparison of results and thus the evaluation methodology is considered as medium. CS-IRS was evaluate using the 1998 DARPA/Lincoln Lab offline evaluation data, in particular week 5 for days Monday, Thursday, and Friday, and week 6 on Thursday. The tcpdump data was replayed and Snort, an open source signature-based IDS, is used to generate alerts. In consideration of the outdated evaluation data and the unidirectional generated traffic that was created to analyze and evaluate IDSs, CS-IRS results in a poor evaluation methodology. The TVA publication only provides data about the runtime for the graph generation, but no further insights into its evaluation. Therefore the evaluation methodology of TVA is considered as poor. REASSESS was evaluated using a testbed and three use-case scenarios. The testbed of REASSESS was installed on three virtual machines interconnected by two virtual networks. The reaction system maintains two network interfaces (internal and external), enabling it to intercept ongoing data flows. The test data was replayed bidirectional and the effects of an response have been analyzed. Therefore the evaluation methodology of REASSESS is considered as good.

5.6.3. Evaluation Summary

In this section, we provide an aggregated overview of the key evaluation results. We have summarized the information presented in Section 5.6 in Table 5.3.

Although detecting network-based attacks and its patterns generated considerable recent research interest [C17, J25, J16], research in automated attack reaction has not yet been studied as in depth [J22]. However, methods of calculating the impact of an attack [C38] or the costs related to a response [J26] have been proposed by the scientific community.

Table 5.3.: Evaluation summary of the response selection models.

Criterion	IE-IRS	ADEPTS	CS-IRS	TVA	REASSESS
Automatic deployment	-	+	+	-	+
Scalability	-	-	+	-	+
Adaptability	-	0	+	0	+
System independency	+	0	+	+	+
Calculation efficiency	-	+	+	0	0
Usability	0	0	0	0	+
Security mechanisms	-	-	-	-	-
Evaluation	-	0	-	-	+
Sum	-5	0	3	-3	5

Legend: high (+), medium (0) and low (−)

We found that the comparison of these approaches is difficult because some approaches are only applicable for specific system environments [J23]. Another circumstance that affirm this problem is that each of the presented approaches is using different metrics, e.g the response model IE-IRS proposed by [C35] only considers negative side effects of a response deployment, while the response model ADEPTS [C36] considers the positive effects. Moreover, the majority of reviewed studies include insufficient insights in order to reproduce their approaches and results. In addition, there is no public available source code of these systems.

While each of the approaches employed reasonable metrics that aid in selecting an appropriate response, the evaluation methodology of all response selection models except REASSESS lacks in an evaluation coverage of the entire process of intrusion handling.

This isolated view is also shown in the evaluation of each response model. The majority of the tests are designed to compare the respective proposed approach to simple security measures. Other tests only measure the time which is needed to select a response. Performance measurements are reasonable since the response has to be applied in a small time window, otherwise IRSs are ineffective. However, without validating that the applied response measures are successful, we put this test criterion into question. Despite using simple response measures such as blocking IP addresses, the CS-IRS and IE-IRS studies do not provide any information on their testing to ensure if the selected response has its desired affect.

Another notable fact is that the response selection models are developed to increase the security. However, there are no security mechanisms explained in any of the publications.

While all of these approaches can be used in different environments, ADEPTS, IE-IRS and TVA require building intricate dependency graphs which hinders the scalability of these approaches. Further, the graphs of ADEPTS and TVA require vulnerability information and other data reducing the usability of the approaches.

TVA is a preventive approach and does not deploy any response measure. Neither IE-IRS, which only evaluates the response based on the negative side effects to other services and users. Both, TVA and IE-IRS do not automatically deploy a response. The residual response models are able to automatically deploy a response to a given attack. However, only ADEPTS and REASSESS describe how the feedback on the success of a deployed response is implemented.

5.7. Lessons Learned

In this chapter, we found that current mitigation is done manually and often relies on expert judgment. However, judgments of experts vary from individual to individual due to their own expertise and experience. As a consequence, performed mitigation procedures are not reproducible and thus same effects of large-scale cyber attacks do not lead to the same mitigation procedures.

To move towards an automatic mitigation, this chapter reviewed current response selection models and introduced our response selection model REASSESS. An important outcome is that current response selection models are not comparable due to the use of different metrics. Moreover, we found that the response selection models also differ in their definition of the impact of a response measure. Existing response selection models rely on building intricate dependency graphs, including vulnerability interdependencies, intrusion paths, service dependencies or response ranks based on historical data and expert judgment to express the impact of an attack.

Moreover, we found that most response selection models lack to verify their evaluation results. The reason is that the majority applied theoretical models to calculate the effectiveness of response measures or reduces the security measures to a simplistic model. Further, we observe that replaying recorded network traffic is unsuitable to evaluate the response deployment and mitigation capabilities.

Finally, we found that REASSESS is the first response selection model which considers the whole process of incident handling and is aligned with the NIST incident life cycle.

5.8. Concluding Remarks

This chapter contributes to answer the question *"Is mitigation currently done manually or automatically? Would it be possible to perform mitigation in an automated way?"*. We reviewed current existing response selection models and introduced our response selection model REASSESS. We evaluated the response selection models in regard to eight evaluation criteria and showed that REASSESS fulfills the requirements presented in Section 5.3.1. Further, we showed that REASSESS is applicable in practice and aligned to the NIST incident life cycle. In REASSESS, we consider the impact of a response as negative effects on legitimate requests to a service with relation to the service's importance. Thus, the value can be intuitively estimated with the importance of a service linked to SLA penalty fees. Further, REASSESS uses penalty costs defined in SLA to derive the importance of a system component. With the developed formulas, it is also possible to estimate the impact of an attack based on the priority of a given alert. Since the response success rate can be stored in a database and updated with every response deployed, the system is able to adapt.

Future work should elaborate a confidence metric as REASSESS intend to integrate common standards for exchanging incident related information. In addition, developing an alert correlation mechanism would aid in handling large amounts of alerts raised by the detection engine and would also allow to assess the success of applied responses in more advanced attack scenarios. The development of a secured communication channel between the IDS and the reaction system would enable the usage of multiple IDS nodes. Finally, methods of parallel programming can be applied to speed up the calculation efficiency of REASSESS.

DDoS Defense using MTD and SDN

This chapter presents a DDoS defense solution that combines the defense techniques moving-target using Software Defined Networking. This combination increases the attackers uncertainty due to an ever-changing attack surface. We enforce the implementation of moving target defense strategies using Software Defined Networks in a collaborative environment and thus focus on ISPs that cooperate among trusted partners. We found that the effects of a large-scale cyber attack can be significantly reduced using the moving-target defense and Software Defined Networking. This chapter shows that Software Defined Networking is an appropriate approach to enforce implementation of the moving target defense and thus mitigate the effects caused by large-scale cyber attacks. This chapter is based on the publication:

[C14]: Jessica Steinberger et al. “DDoS Defense using MTD and SDN”. in: *Proceedings of the 2018 IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*. May 2018. DOI: [10.1109/INM.2015.7140407](https://doi.org/10.1109/INM.2015.7140407)

6.1. Introduction

In Chapter 5 (Selection of an Appropriate Response), we presented the reaction strategy for response selection. In addition to the response selection model, this chapter provides on possible reaction to an ongoing large-scale attack. One approach to reduce the effects of a large-scale cyber attack is to leverage SDN to implement the defense techniques moving-target to increases uncertainty due to an ever-changing attack surface. Current large-scale cyber attacks are encouraged by the static configuration of the cyber systems [C39]. This static configuration supports attackers (a) to perform a reconnaissance of the target system, study and determine its potential vulnerabilities and (b) choose the best setup to perform a devastating large-scale cyber attack [C40]. Moreover, traditional mitigation solutions (e.g., firewalls, Intrusion Prevention Systems) are often not able to handle the large amount of traffic reaching the target network [M67] and the use of cloud-based or content-delivery-based mitigation solutions often cause high economic costs [M68]. One approach to handle large-scale cyber attacks is to collaborate among trusted partners. However, collaborative

approaches have predominantly focused on attack detection in the last years, but solutions for collaborative mitigation and response measures in high-speed networks are missing [C12]. At the same time, approaches using SDN and MTD have been published and are currently attracting increasing interest from research and industry. However, the use of MTD is still in its initial phase [C39, J27] and to the best of our knowledge only one publication focuses on a collaborative use of SDN in context of high-speed networks [J28].

To overcome the lack of an effective, collaborative and scalable mitigation approach, this chapter presents a collaborative DDoS defense solution using MTD and SDN in context of high-speed networks. The advantage of a collaborative DDoS defense solution is that each participating partner achieves insights into the current threat landscape that would otherwise not be obvious. Further, collaborative DDoS defense pools expertise and resources of all collaborating partners and does not propagate malicious traffic further through the network. We enhance our collaborative DDoS defense solution by means of MTD. The advantage of MTD is that it limits the attacker's knowledge of the attack target due to its ever-changing attack surface and thus increases the difficulty to launch a successful attack. Our approach of MTD is implemented using SDN. The contribution that our work brings to the state of the art is that (i) it combines the use of MTD and SDN to limit the effects caused by large-scale cyber attacks in context of high-speed networks. Further, our collaborative DDoS defense solution (ii) provides a low cost solution that easily integrated into existing infrastructure [C10]. (iii) In the evaluation of our approach, we also extend the theoretical model for determining the effectiveness of MTD systems in enterprise networks presented in Zhuang, DeLoach, and Ou [C41], which we use to determine the effectiveness of our collaborative DDoS defense solution.

6.2. Terminology of MTD and SDN

In this section, we introduce terms related to MTD and SDN that are used throughout this section and thus support better understandability of our work. In Section 6.2.1, we introduce MTD, review current MTD strategies and their applicability in context of large-scale cyber attacks and the networks of Internet Service Providers. Next, we introduce SDN and investigate its use to enforce the implementation of MTD strategies in a collaborative, high-speed environment in Section 6.2.2.

6.2.1. Moving-Target Defense

MTD is the concept of controlling changes across multiple system dimensions in order to increase uncertainty and apparent complexity for attackers, reduce their window of opportunity and increase the costs of their probing and attack efforts [M69, M70]. In the area of MTD, we adhere to the terminology defined and used in [C39] and [C40]:

A MTD system, Σ , is a tuple of (Γ, G, P) where Γ is a configurable system, G is a set of operational and security goals, and P represents a set of policies. A configuration system Γ is a tuple of (S, Λ, τ) where $S = \{s_1, s_2, \dots, s_n\}$ is a set of configuration states the MTD systems can be in, $\Lambda = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ a set of actions, and $\tau: S \times \Lambda \rightarrow S$ is the state transition function. A configuration state, s , is a unique assignment of value(s) z from a configuration parameter type Π to a configuration parameter π . A configuration parameter type Π refers to the domain of possible values that a configuration parameter π can assume. A configuration parameter π can take a value based on its configuration type Π to specify the details of the configuration. An example of a host configuration Π is shown in Equation (6.1).

$$\overbrace{\underbrace{\text{IP address}}_{\text{configuration parameter } \pi}}^{\text{configuration state } s \text{ where } s=\pi \leftarrow z} = \underbrace{192.168.0.54}_z \quad (6.1)$$

In recent years, several MTD strategies have been published which can be grouped into three main categories: (i) network-level MTD, (ii) host-level MTD and (iii) application-level MTD [M71]. The network-level MTD refers to changes of the shape of the network graph (e.g., IP-hopping, random port numbers, extra open or closed ports, fake listing hosts). The host-level MTD focuses on changes at the host and operating system (e.g., naming, configuration). Changes on application types and versioning, randomly arranging memory layout are grouped into the application-level MTD.

6.2.2. Software-Defined Networking

SDN [R4] is a network paradigm, which decouples the control and the data plane of a network device. While the data plane still resides on the device, the control plane is outsourced to a centralized controller. The control plane and the data plane communicate over a so called southbound interface. The most common southbound protocol is the OpenFlow protocol [J29], which is defined in the OpenFlow Switch Specification and published by the Open Networking Foundation (ONF) [M72]. ONF

is a consortium that was founded by software providers, content delivery networks, and networking equipment vendors. The controller also provides a centralized network overview over the northbound Application Programming Interface (API) and is responsible for high-level decisions like routing. In contrast to the southbound API, there is no definition for the northbound interface. The data plane is still responsible for packet-forwarding. Incoming packets are matched against packet header fields.

6.3. Scenario, Requirements and Assumptions

In this section, we describe the main focus of this work. First, we define the networks in which we are going to place MTD and SDN. Second, we define the requirements that MTD using SDN should fulfill, as they emerged by the scenario described in Section 6.3.1. In the following, we will use these requirements to evaluate MTD using SDN in the context of large-scale cyber attacks and the network of ISPs.

6.3.1. Scenario

The focus of this work are high-speed networks using a link speed of multiple 10 Gbps. In addition, we assume the networks in our scenario implement an architecture of a typical flow monitoring setup [J15] and provide the capability to use SDN. Besides the availability of flow data and the technical capability of SDN, we assume that network operators cooperate among trusted partners to minimize or prevent damages caused by large-scale cyber attacks. The exchange of security events is in accordance to the communication process described in Steinberger et al. [C12].

6.3.2. Requirements

In this section, we introduce nine requirements that a DDoS defense using MTD and SDN should fulfill. The requirements are part of the Theory of Moving Target Defense described in [C39], the operational requirements presented within the IETF DOTS WG [M60] and of the Software Defined Exchange (SDX) introduced in [J28]. Our requirements are:

Diversification: A DDoS defense solution using MTD within the network of Internet Service Providers should support multiple configuration choices [C39] to avoid static configurations of the high-speed networks.

Adaptations: A DDoS defense solution using MTD should support movements within the system that do not change the shape of the network graph and also support transformations that changes the size and shape of the network graph [C39].

Randomization: Configuration randomization provides the possibility to make use of the full available configuration space and thus the DDoS defense solution should have the capability to support configuration randomization and thus ensure unpredictability.

MTD entropy: The effectiveness of a DDoS defense solution using MTD should be measured by using the MTD Entropy presented by [C39].

Ease of deployment A DDoS defense solution and its underlying implementation (e.g., MTD and SDN) should support platform independence. Further, the DDoS defense solution should be able to handle different types of large-scale cyber attacks. The platform independence and the reusability with different types of large-scale cyber attacks ensures that it easily integrates with the existing infrastructure.

Timeliness: The adaptations of the DDoS defense solution should be performed in an appropriate amount of time to support a proactive network-based attack detection and mitigation.

Scalability: A collaborative DDoS defense using MTD and SDN should support hundreds of collaborating partners. As a result, conventional SDN switches should be able to handle hundreds of thousands of IP prefixes and matching rules while limiting rule-table size and computational overhead [J28].

Wide-area load balancing: In order to limit the effects and mitigate a large-scale DDoS attack, collaborating partners should bundle resources and perform wide-area load balancing in case of an ongoing large-scale attack. This wide-area load balancing should divide the attack traffic over a bundle of resources, based on packet-handling rules [C42] installed using SDX [J28].

Cost-conscious: ISPs are often geographically expansive and the use of MTD and SDN should either make use of existing hardware or the solution should avoid to be place middleboxes at every location to achieve a cost-conscious DDoS defense solution.

Figure 6.1.: A semantic representation of the testbed

6.3.3. Assumptions

The use of MTD strategies have to ensure a consistent and valid network configuration. This topic is currently under active study in literature, with focus on the effect of *Adaptation Selection* and *Timing Problem* on the transition between consistent and valid network configuration states and the creation of invalid network configuration states [C39, C43]. We consider however this topic to beyond the scope of this chapter, and for the research we conduct we always assume a consistent and valid network configuration state and thus predefine possible valid network configuration states.

6.4. Related Work

In this section, we present related work that has been published in the area of MTD, SDN and mitigation of large-scale cyber attacks.

In 2009, the Networking and Information Technology Research and Development (NITRD) Program introduced the initial concept of MTD as a new promising approach to cyber security [M69]. This concept has been formalized by Zhuang, DeLoach, and Ou [C39] in 2014. The authors presented a theory of MTD systems that defines the key concepts and their basic properties. In 2015, the authors presented a theory of cyber attacks to complement the theory of MTD systems [C40].

In [C44, J30], the authors introduced MOTAG, a moving-target defense approach against network-based flooding attacks. MOTAG relies on a hidden proxy-based shuffling approach to separate the attackers from benign clients and uses an intermediate layer with a pool of geographic distributed proxies. However, MOTAG requires client authentication and thus it is not suitable to mitigate DDoS attacks targeting network infrastructure and services used by anonymous users. In addition, MOTAG is not able to mitigate different types of large-scale cyber attacks (e.g., application-layer DDoS attacks). In [C45], Jia et al. presented a successor of MOTAG, that supports authenticated and anonymous clients and is deployed in a cloud-based environment. Both MTD approaches [C44, J30, C45] were only simulated in MATLAB and are vulnerable to the *proxy harvesting attack* [C46].

In [C47], Wright et al. presented a game-theoretic analysis of the four used MTD strategies (i) proactive server migration, (ii) use of client count signal by attacker, (iii) blocking suspected insiders, (iv) delayed attack timing) that are likely to be used in large-scale cyber attacks. This game-theoretic analysis is founded on settings in MOTAG and its successor.

MacFarland and Shue [C48] presented an MTD approach using a host-based SDN to distinguish between trustworthy and untrustworthy clients within a single network. However, the authors do not consider the use of MTD and SDN in a high-speed environment to mitigate large-scale cyber attacks.

An analytical model to analyze the effects of MTD is presented in [C41]. However, Zhuang, DeLoach, and Ou [C41] focus on enterprise networks and the propagation of compromises of nodes within this enterprise network.

In the area of SDN-enabled MTD for cloud environments, the work of Debroy et al. [C49] and Chowdhary, Pisharody, and Huang [C50] has been published. However, Steinberger et al. [C10] revealed that ISPs do not consider to make use of cloud-based mitigation.

In [J31], Ager et al. investigated the anatomy of a large European IXP. They found that the largest IXP carries petabytes of network traffic on a daily basis and are similar to large high-speed networks. Gupta et al. [J28] investigated the use of SDN in networks of IXPs and introduced SDX. They described an IXP network as a layer 2 network, consisting of layer two fabrics, in which participating networks exchange BGP routes and direct network traffic to other participants. SDX provides network operators the possibility to control the flow of network traffic entering and leaving border routers. In order to learn BGP routes, Gupta et al. [J28] used a SDX controller that integrates a route server. Further more SDX is based on Pyretic and use OpenFlow.

However, Gupta et al. [J28] did not combine SDX with MTD in order to mitigate the effects of a large-scale cyber attack.

6.5. DDoS Defense Solution

In this section, we describe the main components of our proposed DDoS Defense solution and how these components interact with each other.

Our DDoS defense solution consists of multiple ISP networks as shown in Figure 6.1 and (i) deploy the elements of a typical flow monitoring setup, (ii) establish the exchange of security events and (iii) make use of a collaboration process, (iv) implement SDX as described in Section 6.3.1.

In order to make use of a moving-target defense strategy, our DDoS defense solution combines the use of SDX and MTD. As a consequence, our approach of MTD is implemented using Open Network Operating System (ONOS), a carrier-grade SDN network operating system. The advantage of using ONOS is that it ensures scalability by design as it has been used and tested in several high-speed networks.

Our DDoS Defense solution performs network-level MTD and host-level MTD [M71]. The network-level MTD strategy is based on different BGP routes and multiple routers. The border router acts as a dispatcher while multiple routers are available on demand and are setup to change the shape of the network. The BGP routes are established and tested using Quagga¹. In addition, our DDoS defense solution performs host-level MTD and performs IP-hopping in order to set up a honeypot.

A consistent and valid network configuration is ensured by a predefined set of valid network routes. The Adaptation Selection and Timing problem is beyond the scope of this chapter as described in Section 6.2.1.

6.6. Evaluation

In this section, we describe the qualitative and quantitative evaluation of the MTD using SDN in order to limit the effects of large-scale cyber attacks. First, we describe the characteristics of the evaluation criteria. Second, we introduce nine evaluation criteria for the DDoS defense solution. Finally, we present and summarize the results of the evaluation.

¹<http://www.nongnu.org/quagga/>

Figure 6.2.: Qualitative evaluation results

6.6.1. Evaluation Methodology

The collaborative DDoS defense solution is evaluated based on the following nine criteria: Diversification, Adaptations, Randomization, MTD Entropy, Ease of Deployment, Timeliness, Scalability, Wide-area load balancing and Cost-conscious. These criteria were derived from the requirements described in Section 6.3.2.

The criterion 'Diversification' describes the ability to select and use one network configuration out of multiple network configuration choices. The criterion 'Adaptations' refers to the ability to support movements within the system that do not change the shape of the network graph and also support transformations that change the size and shape. The Unpredictability of the movements and transformations of the selected network configuration is described by the criterion 'Randomization'. The effectiveness of a chosen MTD strategy is measured by using the MTD entropy and thus as higher the MTD entropy value, the better the effectiveness of a MTD strategy. The criterion 'Ease of Deployment' describes the ability to use the DDoS defense solution and its underlying implementation on different operating systems, infrastructure devices and network protocols. The criterion 'Timeliness' refers to the ability to perform adaptations of the network configuration in an appropriate amount of time. The ability to support hundreds of collaborating partners, handle hundreds of thousands of IP prefixes and matching rules is described by the 'scalability' criterion. The 'wide-area load balancing' criterion describes the ability to divert malicious traffic into a network of collaborating partners and forward it to a scrubber or honeynet for further analysis.

The costs to run and deploy a DDoS defense solution using MTD and SDN are described by the criterion 'cost-conscious'.

6.6.2. Qualitative Evaluation Results

In this section, we present the results of a qualitative evaluation of the DDoS defense solution using MTD and SDN.

Ease of deployment: The heterogeneity of network devices and used operating systems requires a platform independent DDoS defense solution that easily integrates within the existing infrastructure. Therefore, the implementation of our DDoS defense solution is based on ONOS. ONOS is written in Java and provides a distributed SDN applications platform atop Apache Karaf OSGi container and thus can easily be deployed on different operating systems. Further, the DDoS defense solution is composed of hardware that supports the OpenFlow communications interface as a study of Steinberger et al. [C10] revealed that the majority of network operators plan or consider to have the technical ability to use OpenFlow in the near future.

Scalability: The DDoS defense solution is scalable by design as it based on ONOS and SDX. ONOS is designed for performance, high availability, scale-out and well-defined northbound and southbound abstractions and interfaces [M73]. Further, ONOS is gaining momentum around WAN use cases for service providers and is backed by AT&T, Ciena, Cisco, Ericsson, Fujitsu, Huawei, Intel, NTT, NEC, SK Telecom, and many others [M73]. Besides, ONOS and OpenFlow, we make use of SDX that ensures an appropriate rule-table size and network broadcast overhead. As a result, our DDoS defense solution interoperates with large, heterogeneous environments.

Cost-conscious: A study of Steinberger et al. [C10] investigated the technical ability to use SDN to be able to deploy a constantly adapting environment. The majority of network operators plan or consider to have the technical ability to use SDN (e.g., OpenFlow) in the near future. Therefore our approach can be easily deployed within the existing network infrastructure. Further, the costs of a DDoS defense solution depends on time-of-use of resources and bandwidth-based network resources. As our solution focuses on collaboration of trusted partners to mitigate large-scale cyber attacks, expertise and available resources are bundled and thus a smaller amount of resources and bandwidth is required to identify and mitigate ongoing attacks. As a result, our DDoS solution is cost-conscious.

Figure 6.3.: Transition model of attacker x_1 and x_2

6.6.3. Quantitative Evaluation

In this section, we perform a quantitative evaluation of the DDoS defense solution using MTD and SDN. First, we describe the setup of our testbed. Second, we present the test scenario of our DDoS defense solution.

Setup of the Testbed

Mininet [M74] is a network emulation orchestration system designed for lightweight virtualization of a complete network. We used Mininet and ONOS to evaluate our DDoS defense solution. The experiment is composed of virtual hosts, switches, links, and controllers. Mininet is used because it is a controlled environment in which it is possible to safely test security threats and defense measures. Our DDoS defense solution consists of 5 nodes representing Internet Service Providers (ISP $A - E$) connected through a link. In each ISP network, SDX is deployed and is installed as shown in Figure 6.1. In addition, the ISP networks B, D and E are collaborative partners and share security events using the communication process described [C15]. Figure 6.1 shows a schematic representation of our Mininet testbed.

Testbed Experiment

The objective of the experiments is to show that a target network with constrained resources benefits from the use of an MTD strategy during an ongoing network-based attack, because a dynamic shift of the attack surface increases the uncertainty and apparent complexity for the attacker. Further, we show that the large-scale cyber attack is not propagated further through the ISP networks and that the use of an MTD strategy combined with an collaborative approach appropriately limits their effects.

To simulate a large-scale cyber attack, we performed a distributed TCP SYN flood attack from the ISP networks A and C to consume resources on the web server within

ISP network E and render it unresponsive as shown in Figure 6.1. In our test scenario, the detection engine of the ISP network E initially identifies the malicious network traffic targeting its network and initiates an MTD strategy that changes the attack surface. Next, the ISP E informs its trusted collaborating partners about the changes and as a result the partners also start to change their networks. To create the TCP SYN flood attack, we used empty TCP packets with a TCP packet size of 40 bytes and a TCP FLAGS value of 0x02.

Based on the test scenario, we perform two experiments. The result of the experiments are shown in Figure 6.2. First, attacker x_2 who resides in ISP network C launches the TCP SYN flood attack targeting the web server within ISP network E using the network path $c \rightarrow e$. At the same time, we assume the occurrence of benign traffic in each ISP network. In particular, we placed a benign customer within ISP network D that tries to access the web server within ISP network E using the network path $d \rightarrow e$. In Figure 6.2, we show that a customer in ISP network D faces service degradation in form of less bandwidth availability as a result of the TCP SYN Flood (1). Next, attacker x_1 in ISP network A launches the TCP SYN flood attack targeting the web server in ISP network E using the network path $a \rightarrow d \rightarrow e$ (2). As a result, the customer in ISP network D faces another service degradation in form of less bandwidth availability. In the meantime, the collaborative partners exchanged security events initiated by ISP network E using the communication process described in [C15] and use MTD.

In our first experiment, ISP network D splits up the occurring network traffic into benign and malicious traffic and reroutes the malicious network traffic to the network of collaborative partners. The reason is that high-speed networks have redundant link capacities in place and their average link utilization is less than 30% [J32, C51]. Therefore, the collaborative DDoS defense solution bundles resources of all collaborating partners to handle the amount of malicious network traffic and ensure availability. As a result, the malicious network traffic from the attacker x_1 is rerouted and using the network path $a \rightarrow b \rightarrow c \rightarrow e$ (3). Further, the network path $d \rightarrow e$ recovers and provides slightly more bandwidth to the customer in ISP network D. Finally, ISP network E changes the attack surface using MTD, adds an additional network path and deploys various link capacities to the web server D . As shown in Figure 6.2, ISP E also splits up the incoming traffic into benign and malicious traffic. The malicious traffic is rerouted over a rate-limited link to the web server and thus the available bandwidth of the customer in ISP network D recovers (4).

Quantitative Evaluation Results

In this section, we present the results of a quantitative evaluation results of the DDoS defense solution using MTD and SDN.

Diversification: Within an ISP network multiple configuration choices are available. The number of configuration choices increase, as larger the ISP network. In our test scenario, we consider one virtual host (customer), multiple routers, links, link capacities and controllers available in the configuration space. ONOS provides the capability to switch between different configuration choices by using the ONOS API and enhance the functionality with a custom ONOS application.

Adaptations: Adaptations are used within the collaborative ISP network to transform the collaborative ISP network from one configuration state s into another valid configuration state s . As emerged from the test scenario, we perform three adaptations: increase uncertainty and apparent complexity through the establishment of alternative routes within α_1 the network of collaborating partners or α_2 within the network of a single ISP and α_3 change the configuration state s of the link capacity within ISP network E. The adaptations of our test scenario are deployed using ONOS. The effects of the deployment of the adaptation are visualized in Figure 6.2. In particular, adaptation α_1 was deployed in 3, adaptation α_2 and α_3 were deployed in 4. Figure 6.2 shows that the adaptations limit the effects of the TCP SYN flood and thus contribute to ensure availability of the organization's network infrastructure.

Randomization: In our experiment, the set S of the configuration states of the MTD systems consist of all possible network paths, rerouting of network traffic within the network of collaborating partners or in each ISP network and rate-limiting on all available links. Further, host configuration parameters e.g., IP addresses, operating systems, memory configurations are also part of the configuration space s . For reasons of simplicity, Figure 6.2 does not consider host configuration parameters. However, ONOS offers an API to customize the ONOS functionality. Even though ONOS does not provide configuration randomization from scratch, it provides the capability to enhance its functionality by own scripts and thus provides the capability to randomly select the next configuration state to ensure unpredictability.

MTD entropy: The attackers x_1 and x_2 try to render target D (an http web server) unresponsive. The attack is going through the network of ISP E though multiple available network paths as shown in Figure 6.3. The values p_i where $i = \{0 \leq i \leq$

$6|i \in \mathbb{N}_0\}$ represent the transition probabilities from x_1 to D that include the possibility of MTD adaptation. We adhere to the probability calculations defined in [C41] and adapt these to the scenario described in 6.3.1.

In contrast to Zhuang, DeLoach, and Ou [C41], we only consider forward transitions which represent the *hot-potato routing* [J33]. Hot-potato routing refers to the selection of the closest egress point, the router with the smallest intradomain distance, when more than one route to the destination exist.

Further, we consider that ISP network A and C are not using MTD and thus are not adapting. The ISP networks B, D and E are collaborative partners, exchange security events using a communication process as described in [C15] and make use of MTD. From the perspective of the attacker x_1 the shortest path to the target D is the network path $a \rightarrow d \rightarrow e$. As the network of ISP D, ISP E and the target D make use of MTD, we consider $2^3 = 8$ different configuration states S . From the perspective of the attacker x_2 the shortest path to the target D is the network path $c \rightarrow e$. As the network of ISP E and the target D make use of MTD, we consider $2^2 = 4$ different configuration states S . We assume the attackers x_1 and x_2 are limited to valid communication paths, know those paths, continue diligently to send traffic to the target D and try to avoid using paths of the other attacker network to not weaken the amount of attack traffic reaching the target D .

Further, we assume that the adaptations available on the nodes of the collaborative partners ensure the enlargement of constrained resources and thus the effects of a DDoS attack are limited.

$$adapted = \left(\frac{k}{n}\right)^{\frac{T_a}{T_r}}; \quad \overline{adapted} = \left(1 - \frac{k}{n}\right)^{\frac{T_a}{T_r}} \quad (6.2)$$

$$successful = \left(1 - (1 - p)\right)^{\frac{T_r}{T_a}}; \quad \overline{successful} = \left(1 - p\right)^{\frac{T_r}{T_a}} \quad (6.3)$$

Example: Based on the formula (6.2) and formula (6.3) the probability P_D of a successful DDoS attack is calculated. To calculate the probability P_D of a successful DDoS attack from attacker x_1 to the target D , the multiplication of all probabilities of all possible path to the target are used as shown in formula (6.4).

$$P_D = \prod_{i=0}^2 p_i \quad (6.4)$$

The ISP A network is not using MTD and thus is not adapted during an ongoing DDoS attack. Therefore, the probability is shown in formula (6.5).

$$p_0 = \left(1 - \frac{k}{n}\right)^{\frac{T_a}{T_r}} \quad (6.5)$$

As the network of ISP D and E are collaborative partners, and make use of MTD their networks may get adapted during an ongoing attack. In case the network of ISP D is not adapted during the ongoing attack, the DDoS attack is successful and saturates the constrained resources. This results in a probability shown in formula (6.6). In contrast, the network of ISP D is adapted during the ongoing attack and thus the effects of a DDoS attack mitigated. This results in a probability shown in formula (6.7).

$$p_{1a} = \left(1 - (1 - p)\right)^{\frac{T_r}{T_a}} \cdot \left(1 - \frac{k}{n}\right)^{\frac{T_a}{T_r}} \quad (6.6)$$

$$p_{1b} = \left(1 - p\right)^{\frac{T_r}{T_a}} \cdot \left(\frac{k}{n}\right)^{\frac{T_a}{T_r}} \quad (6.7)$$

As the network of ISP E also make use of MTD, the probabilities of p_{2a} and p_{2b} remain the same as presented in formula (6.6) and (6.7). Next, the target D within the network of ISP E also may get adapted. This results in a probability shown in formula (6.8) and (6.9).

$$p_{3a} = \left(\frac{k}{n}\right)^{\frac{T_a}{T_r}} \quad (6.8)$$

$$p_{3b} = \left(1 - \frac{k}{n}\right)^{\frac{T_a}{T_r}} \quad (6.9)$$

As reported in [R1], the average DDoS attack duration is 58 minutes and the number of attacks experienced per month is more than 21. As a consequence, we set the Attack Interval $T_a = 60$ min. In accordance to the MTD Adaptation Interval selected by [C41], the Adaptation Interval is set to $T_r = 20$ min and the number of adaptations is set to $k = 1$. The overall probability P_D of a successful DDoS attack of 8 configuration states is listed in Table 6.1. As shown in Table 6.1 the overall probability P_D of a successful DDoS attack decreases as more collaborative ISP networks process the network traffic and make use of MTD.

Table 6.1.: Overall probability P_D of a successful DDoS attack of 8 configuration states s

#	ISP D	ISP E	target D	P_D
1	<i>adapted</i>	<i>adapted</i>	<i>adapted</i>	2.2301×10^{-7}
2	<i>adapted</i>	$\overline{\text{adapted}}$	<i>adapted</i>	5.0984×10^{-6}
3	<i>adapted</i>	<i>adapted</i>	$\overline{\text{adapted}}$	6.3730×10^{-7}
4	<i>adapted</i>	$\overline{\text{adapted}}$	$\overline{\text{adapted}}$	1.4570×10^{-5}
5	$\overline{\text{adapted}}$	<i>adapted</i>	<i>adapted</i>	6.3730×10^{-7}
6	$\overline{\text{adapted}}$	$\overline{\text{adapted}}$	<i>adapted</i>	1.4570×10^{-5}
7	$\overline{\text{adapted}}$	<i>adapted</i>	$\overline{\text{adapted}}$	1.8212×10^{-6}
8	$\overline{\text{adapted}}$	$\overline{\text{adapted}}$	$\overline{\text{adapted}}$	4.1635×10^{-5}

Timeliness: The primary focus to mitigate and respond to network-based attacks is maintaining the availability of the organization's network infrastructure and services. Therefore, the DDoS defense solution performs several adaptations to increase uncertainty and apparent complexity for the attackers. As shown in Figure 6.2, the adaptations (label 3 and 4) are deployed and their effects are immediately visible (more available bandwidth for the customer located in ISP network D).

Wide-area load balancing: In [J32, C51], the authors reported that high-speed networks have redundant link capacities in place and their average link utilization is less than 30%. As a consequence, wide-area load balancing should be used to mitigate and respond to large-scale cyber attacks. In our test scenario, the collaborating partners bundle resources in order to mitigate and respond to large-scale cyber attacks. Further, the collaborating networks diversify the amount of malicious traffic among all collaborating partners to ensure availability of the organization's infrastructure. Moreover, wide-area load balancing among collaborative networks provides the possibility to analyze the attacker's behavior. ONOS provides the capability to perform wide-area load balancing.

6.7. Lessons Learned

In this chapter, we presented a DDoS defense solution that combines the defense techniques moving-target using SDN. This combination constitutes one possible reaction used by the response selection model REASSESS presented in Chapter 5 (Selection

of an Appropriate Response). As a result, it is possible to perform mitigation in an automated way.

We found that the use of MTD and SDN within the response selection model REASSESS limits the attacker's knowledge of the attack target due to its ever-changing attack surface and thus increases the difficulty to launch a successful attack. Further, we found that the effects of a large-scale cyber attack can be significantly reduced using MTD and SDN. Moreover, we showed that SDN provides a low cost solution that easily integrated into existing infrastructure [C10] and is an appropriate approach to enforce implementation of MTD.

6.8. Concluding Remarks

In this chapter, we have answered the question *"Is mitigation currently done manually or automatically? Would it be possible to perform mitigation in an automated way?"* One approach to mitigate and respond to large-scale cyber attacks is to move as close to the source of the attack as possible and thus move to the network of Internet Service Providers. In this chapter, we therefore investigated the effectiveness of the defense technique moving target using SDX in a collaborative environment in context of ISPs. In particular, we focused on the SDN Operating System (OS) called ONOS.

We have shown that the overall probability of a successful DDoS attack decreases as more collaborative partners process the network traffic and make use of MTD. Further, we found that ONOS is an appropriate SDN OS to enforce implementation of the moving target defense to mitigate the effects caused by large-scale cyber attacks. In addition, we have shown that a moving target defense strategy significantly reduces the effects of a large-scale cyber attack.

This chapter present a trust model that determines a trust and a knowledge level of a security event in order to deploy semi-automated remediations and facilitate the dissemination of security event information using the exchange format FLEX in the context of ISPs. We show that this trust model is scalable and helps to build a trust community in order to share information about threats and its remediation suggestions. This chapter is based on the publication:

[C15]: Jessica Steinberger et al. “In Whom Do We Trust - Sharing Security Events”. In: *Management and Security in the Age of Hyperconnectivity: 10th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2016, Munich, Germany, June 20-23, 2016, Proceedings*. Ed. by Rémi Badonnel et al. Cham: Springer International Publishing, 2016, pp. 111–124. ISBN: 978-3-319-39814-3. DOI: [10.1007/978-3-319-39814-3_11](https://doi.org/10.1007/978-3-319-39814-3_11). URL: http://dx.doi.org/10.1007/978-3-319-39814-3_11

7.1. Introduction

In Chapter 5 (Selection of an Appropriate Response) and Chapter 6 (DDoS Defense using MTD and SDN), we showed how to perform mitigation in an automated way. However, current collaborative cyber defense is founded on an ad-hoc basis via email, member calls or in personal meetings and thus a manual process [M75, M65]. This slows mitigation and response times and impedes mitigation and reaction efficacy [M60]. Besides the fact that collaboration and information sharing often only takes place in case participating partners are personally known to each other, some legally binding orders (e.g., Executive Order 1363 [M76, M77]) have been published recently that force owners and operators of critical infrastructures to establish procedures to increase the volume, timeliness and quality of cyber threat information sharing.

To improve the timeliness of cyber defense, support collaboration among trusted partners and facilitate the dissemination of security events, the development of trust is deemed of critical importance. Despite well-known and established trust models are used in other application contexts, the personal knowledge of each sharing partner to develop trust in order to share security events does not scale very well.

To overcome the constraint of personal knowledge of each sharing partner to develop trust in context of mitigation and response to large-scale cyber attacks and to establish an effective collaboration among trusted partners, this chapter presents a trust model, called MiRTrust. MiRTrust determines a trust and a knowledge level of a security event in order to deploy semi-automated remediations and facilitate the dissemination of security events using FLEX in the context of ISPs. MiRTrust is based on the well known PGP trust model [C52, C53] and used to establish different levels of trust, determine the prioritization of the shared security event, sanitize the occurrence of security events and contributes to build a trust community in order to share information about cyber threats and its remediation suggestions.

7.2. Scenario and Requirements

In this Section, we describe the main focus of this work. First, we define the networks in which we are going to place our trust model to facilitate the semi-automated assessment and deployment of remediation suggestions within a security event. Second, we define the requirements that a trust model should fulfill, as they emerged by the scenario described in Section 7.2.1. In the following, we will use these requirements to evaluate the trust model.

7.2.1. Scenario

The primary focus of this work are multiple high-speed networks using a link speed of 10 Gbps and higher [C28]. In addition, we focus on network operators that cooperate among trusted partners to minimize or prevent damages caused by network-based attacks and use an automated threat information exchange. The collaboration is established using an infrastructure based overlay network [J34] to prevent a full mesh within the network and to ensure scalability. Each participating partner receives security events from different origins as shown in Figure 7.1. Security events originating from a detection engine within the own network infrastructure is defined as an internal security event and shown in Figure 7.1a. Further, each participating ISP possesses a list of directly connected collaborating partners. In case of ISP *a* a directly connected collaborating partner is ISP *c* as shown in Figure 7.1b. The networks of ISP *b*, ISP *d* and ISP *e* are not directly connected to ISP *a* and thus are regarded as external non collaborating partners as shown in Figure 7.1c.

Figure 7.1.: Origin of security events

7.2.2. Requirements

In this section, we introduce five requirements that a trust model should fulfill in order to establish collaboration among trusted partners. These requirements are derived from European Union Agency for Network and Information Security (ENISA)’s position paper no. 2 [M78] and the work of [C54].

Ease of deployment: The trust model and its underlying implementation should support platform independency to ensure that they easily integrate with the existing infrastructure.

Access control: The trust model should support the use of the Traffic Light Protocol (TLP) [M79]. The reason is that the TLP provides a scheme for sharing different detail of information tailored for its intended receivers. The reason is that the amount of provided threat information depends on the trust and sharing relationship between collaborating ISPs.

Subjectivity: The trust model should provide the possibility that network operators are able to form their own trust options. These trust options represent the degree of belief about the behavior of collaborating partners.

Asymmetry: The trust model should support asymmetric levels of trust for both collaborating partners as they do not need to have similar trust in each other.

Decentralized: Each trust model within the MiR system should act as a self-contained unit and thus calculates its trust decisions locally. The MiR system should exchange these decisions in form of recommendations with its directly connected collaborating partners.

7.3. Related Work

In this section, we introduce the terminology by defining trust, review reputation-based trust models and analyze existing collaboration communities used to mitigate and response to large-scale attacks.

7.3.1. Terminology

Currently, there is no consensus in the definition of trust available. The authors of [T4] reported that there are various definitions of trust based on the use-case context. In this chapter, we adhere to the following definition of trust: "Trust is the quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee with a specific context [T4]." Besides trust, we also adhere to the following definition of distrust: "Distrust is the quantified belief by a trustor that a trustee is incompetent, dishonest, not secure or not dependable within a specific context [T4]."

7.3.2. Collaboration Communities

The majority of the collaboration communities are private communities that require a membership application and are charging an annual fee. Recent well-known collaboration communities that require a membership application and are charging an annual fee are the Anti-Phishing Working Group (APWG), the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG), the Research and Education Networking (REN) Information Sharing and Analysis Center (REN-ISAC) and the Forum of Incident Response and Security Teams (FIRST). In contrast to the fee-based collaboration communities are non-fee-based collaborations. The ACDC, the GÉANT Task Force on Computer Security Incident Response Teams¹ (TF-CSIRT) and the GÉANT Special Interest Group on Network Operations Centres² (SIG-NOC) and the DOTS³ working group within the IETF are well-known collaboration communities in context of security event sharing.

The collaboration of APWG focuses on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing [M80]. M³AAWG is working against bots, malware, spam, viruses, DoS attacks and other online exploitation [M81]. REN-ISAC is sharing sensitive information regarding cyber security threat, incidents, response, and protection located in United States, Canada and New Zealand [M82], and FIRST cooperatively handles computer security incidents and

¹http://www.geant.org/Innovation/SIG_TF/Pages/TF-CSIRT.aspx

²http://www.geant.org/Innovation/SIG_TF/Pages/SIG-NOC.aspx

³<https://datatracker.ietf.org/wg/dots/charter/>

promote incident prevention programs from around the world. ACDC focus on detection, mitigation and response of botnets. Further, ACDC also supports the mutual data sharing between partners (e.g., ISPs, government agencies, law enforcement, research groups, industry partners). TF-CSIRT and SIG-NOC facilitates knowledge exchange and collaboration in a trusted environment in order to improve cooperation and coordination. DOTS is developing a standards based approach related to DDoS detection, classification, traceback and mitigation in context of a larger collaborative system at service provider level.

All of the aforementioned collaboration communities require and provide different level of memberships, whereas the fees vary from \$250 to \$25 000 per year. In addition, each application initiates a review process which is performed by the community and decides about acceptance to join. Some communities perform collaboration following the following the Chatham House Rules⁴ (e.g., M³AAWG). The number of community members within a fee-based community vary from \$200 to \$1 800 and FIRST is mentioned to be the oldest and biggest international collaboration community for CERTs [M38].

7.3.3. Reputation-based Trust Models

e-Commerce: The trust model of e-Commerce is often a centralized reputation-based system that rely on feedback of the involved parties. This feedback system is used in eBay, AirBnB, Booking and Amazon and is a primary resource for potential buyers to determine the trustworthiness of the seller. A feedback consists of comments and five different ranking levels to evaluate several aspects (e.g., price, condition, timeliness). Further, the overall feedback score consists of a positive, neutral or negative rating. A positive feedback adds +1, a negative feedback adds -1 and a neutral feedback 0 to the overall feedback score. To calculate the overall feedback percentage, the ratio of feedback scores is computed.

Web of Trust: The trust model *web of trust* (WOT) describes a decentralized Public-Key infrastructure (PKI) relying on trust decisions of individual participants [C53]. It is used in PGP, GnuPG and OpenPGP. The basic WOT uses three levels of trust: complete, marginal and no trust. In addition, PGP, GnuPG and OpenPGP distinguish unknown trust from no trust and thus differentiate between 5 trust levels [C52, C53]. Each participating partner owns a personal collection of certificates called the key ring and is allowed to sign a key for any other participant. [C53] reported that the trust

⁴<https://www.chathamhouse.org/about/chatham-house-rule>

model accepts a given public key in the key ring as completely valid, if either i) the public key belongs to the owner of the key ring, ii) the key ring contains at least C certificates from completely trusted certificate issuer with valid public keys and iii) the key ring contains at least M certificates from marginally trusted certificate issuer with valid public keys. The default values in PGP are $C = 1$ and $M = 2$, whereas GnuPG uses $C = 1$ and $M = 3$. The calculation of the trust level is described by [C53] as follows: The key legitimacy $L = \frac{c}{C} + \frac{m}{M}$, where c and m represents the number of certificates from completely/marginally trusted certificate issuers with valid keys. A key is completely valid for $L \geq 1$, marginally valid for $0 < L < 1$, and invalid for $L = 0$.

7.4. Trust model

Our mitigation and response trust model (MiRTrust) is based on hTrust [C55], a trust management model to facilitate the construction of trust-aware mobile systems and applications and on the PGP trust model [C52, C53]. In contrast to hTrust, MiRTrust uses the four GnuPG [M83] trust levels: *unknown*, *none*, *marginal* and *full* and additionally the trust level *distrust*. Moreover, MiRTrust takes into account the EU Trusted Lists [M84] and the Alexa top 10 million websites list in order to extract the use of certification authorities using a 3 months average ranking. Unlike hTrust, MiRTrust does not consider contexts as the security events are identified in the context of ISPs and result from a large-scale attack.

MiRTrust consists of several input parameters (yellow colored) and three components: trust formation (blue colored), trust dissemination (brown colored) and trust evaluation (green colored) as shown in Figure 7.2. The component trust formation is responsible to determine the trustworthiness of a security event before a semi-automated mitigation and response action is taken. In case a security event from a new collaborating partner or an unknown source was received, the trust dissemination guarantees a minimum set of information upon the predication of trust can be calculated. The last component, trust evaluation, is responsible to continuously self-adapt the trust information kept in the ISP's local trust list.

A trusted-based collaboration relies on two participating partners exchanging security events, where trust has the following three characteristics: (i) Trust is not symmetric. If ISP a trusts ISP b , it does not follow ISP b trusts ISP a . (ii) Trust is not inherently transitive. If ISP a trusts ISP b and ISP b trusts ISP c , it does not automatically follow that ISP a trusts ISP c . (iii) Trust of own detection engines varies in a range from marginal trust to full trust, as false positives are possible. A security event

Figure 7.2.: Trust level calculation of MiRTrust

is described as the quadruple (a, b, s, t) . The quadruple can be described as follows: ISP a informs ISP b about a security event of type s occurring at time t . The sender of a security event is referred to as trustee, whereas the receiver of a security event is called trustor. ISP b is a trustor that forms a trust opinion about the trustee ISP a based on b 's previous trust experiences with a . The process to form a trust opinion about a trustee is shown in Figure 7.2. The trust experiences are stored locally at each MiR system and are described by a 6-tuple: (a, b, s, l, k, t) . The tuple can be described as follows: ISP b trusts ISP a at level l about the security event type s in context of large-scale attacks. The trust level l is denoted as $l \in [-2, 2]$, whereas -2 represents distrust, -1 represents unknown trust, 0 represents no trust, 1 represents marginal trust and 2 represents full trust. In accordance to [C55], MiRTrust also considers only partial knowledge about the trustworthiness of collaborating partner. The reason is that only directly interconnected networks are collaborating and thus their trust opinions contain a level of uncertainty. This uncertainty is expressed as knowledge k and varies from a trust based decision *do not trust* to a lack of evidence based decision *do not know*. The knowledge k is denoted as $k \in [0, 1]$, whereas 0 represents unknown and 1 perfect knowledge. Both, the trust level l and the knowledge k is retrieved from local settings and past experiences. The better the experience in the past, the higher the trust level l and the knowledge k . To relate trust and knowledge to time, MiRTrust uses the variable t to refer at which time t the trust t and knowledge k was calculated.

Local settings: In a first step, MiRTrust computes a trust range $\Upsilon[lb, ub]$ and an initial knowledge value based on the origin of the security event. In case of an internal

security event $\Upsilon[lb, ub]$ is set to $\Upsilon[1, 2]$ and the knowledge value is set to $k = 1$. The trust range of security events originating from external collaborating partners is set to $\Upsilon[0, 1]$, where as the trust range of security events originating from external non collaborating partners is set to $\Upsilon[-2, 0]$. The knowledge value of security events originating from external collaborating partners is set to $k = 0.5$ and from external non collaborating partners to $k = 0$. Next, MiRTrust takes into account several local settings ls . The basic setup of MiRTrust considers three local settings: $ls_1 = \text{check CA list}$, $ls_2 = \text{ask collaborating partners}$ and $ls_3 = \text{check previous security event database (DB)}$ that all evaluate to a boolean value. ls_1 describes if IP addresses or domains within the security event are listed on the merged CA list. This CA list combines the EU Trusted list and the used certification authorities of the Alexa top 10 million websites. ls_2 describes whether the behavior that cause the security event has also been seen in collaborating partner networks [C15]. ls_3 refers to security events with similar behavior that have been received and stored previously.

Trust formation: The trust formation enables a trustor to predict a trustee's trustworthiness before mitigation and response actions are initiated. Therefore, the function p is used to calculate a trust value as shown in Equation (7.1). p uses a weight w to emphasize the importance of a local setting ls . The importance of these values are defined by each participating ISP. The function $c(ls_i)$ is used to decide which value of the trust range $\Upsilon[lb, ub]$ is multiplied with weight w .

$$p(w_1, \dots, w_n, ls_1, \dots, ls_n, \Upsilon[lb, ub]) = \sum_{i=1}^n w_i \cdot c(ls_i), c(ls_i) = \begin{cases} \Upsilon_{lb} & \text{if } ls_i = 0 \\ \Upsilon_{ub} & \text{if } ls_i = 1 \end{cases} \quad (7.1)$$

Next, MiRTrust looks up the sender of the security event in the local trust list. In case the sender is listed within the trust list, the previous level of trust within the trust list and the current level of trust of the function p are compared. If $|\text{prev. } l - \text{curr. } l| > 1$, the sender is marked as suspicious. Otherwise, the past trust experiences v and the current trust value p are aggregated using the weighted average, as the trust experiences evolve over time. The trust level l is set to $l = \frac{v+p}{2}$. In case, the sender is not listed within the trust list and thus no aggregated trust experience tuple is available, collaborating partners are asked for recommendations r . As a recommendation is transferred over the network, it uses encryption to ensure confidentiality and a signature to prove the recommendation's authenticity. Thus, the current trust value p and the trust value of the recommendation r are aggregated depending on the quality q

of the recommendation and determined as shown in Equation (7.2). Only those recommendations are considered that provide a quality q greater than a minimum level of trust. In addition, only recommendations with a time stamp $t(p) > t(r)$ are used. The trust value rl takes into account the inherent knowledge uncertainty k of the given recommendation. T represents the time interval in which security events are observed and the total number of security events.

$$q = \max \left(l_{min}, l_i \cdot k_i \cdot \max \left(0, \frac{T - (t_n - t)}{T} \right) \right) \quad (7.2)$$

Due to the collaboration, multiple recommendations r_n are received. Therefore, a unique recommendation trust value rl is computed using a weighted average of the individual trust range of the recommendations with a quality greater than the minimum level of trust as shown in Formula (7.3) [C52].

$$rl(r_1, \dots, r_n) = \frac{1}{n} \sum_{i=1}^n l_i \cdot q_i | q_i > l_{min} \quad (7.3)$$

rl and the current trust value p are aggregated using the weighted average. The trust level l is set to $l = \frac{p+rl}{2}$.

Trust dissemination: The trust formation is used to predict the trustworthiness of an ISP. In case no aggregated tuples are available, an ISP exchanges recommendations r with its collaborating partners to guarantee a minimum set of information to decide about the trustworthiness. As a consequence, recommendations contain sensitive data that require the use of security mechanisms (e.g., encryption & signature). Therefore, the exchange format FLEX is used to disseminate the recommendations.

Trust evaluation: MiRTrust continuously updates its local settings during the occurrence of a security event and based on the received recommendations. These updates are included with equal weight to ensure that a trust opinion can not change rapidly (e.g., caused by false good recommendation). In case a recommendation r is received that conflicts with the own calculated trustworthiness, the level of trust of ISP x is not aggregated into previous trust opinions and ISP x is marked as suspicious. In case, several security events of ISP x occur with conflicting trustworthiness, the level of trust of ISP x tends to drop to -2 , that represents distrust and thus identifies x as an ISP with a suspect behavior. As a consequence, recommendations of x will be disregarded.

7.5. Evaluation

In this Section, we describe the qualitative and quantitative evaluation of our trust model MiRTrust. First, we describe the characteristics of the evaluation criteria. Second, we introduce five evaluation criteria for our trust model. Further, we evaluate MiRTrust using multi-method-modeling, describe the setup of the testbed and present the test scenario of the trust model. Finally, we present and summarize the results of the evaluation.

7.5.1. Qualitative Evaluation Methodology

The trust model MiRTrust is evaluated based on the following five criteria: Ease of deployment, authorization, subjectivity, asymmetry and decentralization. These criteria were derived from the requirements described in Section 7.2.2.

The criterion 'Ease of Deployment' describes the ability to use the trust model and its underlying implementation on different operating systems, infrastructure devices, exchange formats and protocols. The criterion 'authorization' refers to the ability to support the TLP protocol. The 'subjectivity' describes the possibility that network operators are able to form their own trust opinions. The criterion 'asymmetry' describes the possibility that two collaborating partners do not need to have the similar trust in each other. The criterion 'decentralization' refers to the ability that each participating ISP acts as a self-contained unit, calculates and stores its trust decisions locally.

7.5.2. Quantitative Evaluation Methodology

MiRTrust is evaluated using a multi-method-modeling approach consisting of an agent-based and a discrete event model using AnyLogic⁵ [B7]. The model of MiRTrust is based on a scale-free network of ISPs that share security event information and perform mitigation actions based on the trust and knowledge level of each security event. The ISPs are modeled as agents. Each ISP has an individual behavior and attitude towards the trustworthiness of a sender of a security event. The process of mitigation is modeled in a discrete event way at each single ISP.

Initially, MiRTrust models a weekly contact rate to describe the assumption that 1% of potential ISPs will want to join the MiRTrust community. Besides this contact rate, non-community members are able to join the community by using a sponsoring join process. Each community member possesses a list of directly connected collaborating partners and assigns an initial trust value range of $[0, 1]$ and a knowledge value of

⁵The model can be downloaded on <https://bitbucket.org/dasec/mirtrust>

0.5. Based on the findings in [C10], each ISP receives 5 security events per month. The sender of the security event is set using a triangular distribution. This triangular distribution is used to create security events sent from an internal detection engine of an ISP, an external collaborating ISP and an unknown ISP. Based on the sender of the security event, an ISP starts its trust formulation calculation and looks up its past trust experiences w_1 with the sender of the security event. In case no trust experiences are available and thus no previous security events have been exchanged between the sender and receiver of the security event, the receiving ISP asks its collaborating partners to send recommendation tuples about the trustworthiness of the sender. Therefore, ISPs interact and share their trust experiences. Further, MiRTrust takes into account a local created trusted CA list w_2 and if this security event has also been seen by collaborating partners w_3 . These local settings are weighted based on the formula (7.1) as follows: $w_1 = 0.5$, $w_2 = 0.15$ and $w_3 = 0.45$ with $w_1 + w_2 + w_3 = 1$, $0 \leq w_i \leq 1$. Next, the trust level and the knowledge values are calculated. Finally, mitigation and response actions are deployed, if the trust level pass a threshold of 0. The duration of the mitigation process is set using a triangular distribution with lower limit $a = 20$ and upper limit $b = 1440$ minutes. These mitigation values are derived from [C10]. Finally, the ISPs are waiting for the next occurring security event that restarts the trust formation process.

7.5.3. Evaluation Results

In this paragraph, we present and discuss the results of the qualitative and quantitative evaluation of MiRTrust.

Ease of deployment: The heterogeneity of network devices and used operating systems requires a platform independent trust model that easily integrates within the existing infrastructure. Therefore, the implementation of MiRTrust is based on Java and thus can easily be deployed on different operating systems. Further, MiRTrust encodes its recommendation tuples in FLEX. The dissemination of those tuples among trusted partners is using STOMP and thus ensures platform independency.

Access control: MiRTrust supports the semi-automated dissemination of security threat information based on the different level of trust. Therefore, MiRTrust differentiates between the following five different trust levels: distrust, unknown, none, marginal and full trust. The use of different trust levels allows to encode security event information using the TLP protocol and thus provide different detail of information within a security event tailored for its intended receivers. The trust level distrust,

7. TRUST

Figure 7.3.: Distribution of trust levels

unknown and none trust are mapped to the color red of the TLP protocol. The color amber is used to encode the trust level marginal trust and the color green is used to represent full trust.

Subjectivity: Through the different level of trust and sharing relationship between collaborating ISPs, MiRTrust supports that each collaborating partner is able to form its own trust opinion. The quantitative evaluation of MiRTrust shows the distribution of different level of trust in Figure 7.3.

Asymmetry: MiRTrust supports that two collaborating partners have different level of trust in each other as trust is not symmetric. If ISP a trusts ISP b , it does not follow ISP b trusts ISP a . Further, trust is not inherently transitive. If ISP a trusts ISP b and ISP b trusts ISP c , it does not automatically follow that ISP a trusts ISP c . Therefore,

From	To	l	k	s	t
iSPs[359]	iSPs[11]	0.98	0.6	DDoS	2016-02-08 18:27:27.103+01
iSPs[289]	iSPs[11]	-1.5	0.1	DDoS	2016-02-08 18:27:29.571+01
iSPs[168]	iSPs[11]	0.83	0.6	DDoS	2016-02-08 18:27:30.253+01

(a) Trust levels of ISP 11

From	To	l	k	s	t
iSPs[11]	iSPs[359]	0.5	0.5	I	2016-02-08 18:27:27.457+01
iSPs[11]	iSPs[289]	0.5	0.5	I	2016-02-08 18:27:29.429+01
iSPs[11]	iSPs[168]	0.5	0.5	I	2016-02-08 18:27:32.089+01

(b) Trust of other ISPs in ISP 11

Figure 7.4.: Asymmetric trust level

each single MiRTrust instance possesses a list of calculated trust level and knowledge values of each exchanged security event as shown in Figure 7.4.

Decentralization: MiRTrust is deployed at each collaborating partner and thus acts as a self-contained unit that calculates and stores trust opinions locally. Further, the recommendation tuples are transferred to collaborating partners using FLEX and thus are signed. Each ISP is able to form its own trust opinion about collaborating partners similar to the principle of web of trust.

7.6. Lessons Learned

In this chapter, we found that collaborative mitigation is done on an ad-hoc basis via email, member calls or in personal meetings only under the premise that participating partners are personally known to each other. However, the personal knowledge of each sharing partner to develop trust in order to share security events does not scale very well.

An important outcome is that that trust of network operators among collaborative partners is subjective and asymmetric. Further, we found that network operators prefer to store trust opinions locally and based on the local trust opinions share trust recommendations.

We found that the semi-automated dissemination of security threat information is based on different level of trust and encoded using the TLP protocol tailored for its intended receivers.

7.7. Concluding Remarks

In this chapter, we have answered the question "*How can trust among collaborative partners be arranged?*". We introduced our trust model MiRTrust that facilitates the semi-automated assessment and deployment of remediation suggestions within a security event. MiRTrust is used to determine different levels of trust, set the prioritization of the shared security event, sanitize the occurrence of security events and contributes to build a trust community in order to share information about cyber threats and its remediation suggestions. We showed that MiRTrust is able to support the formation of a subjective and asymmetric trust level and can be used to encode cyber threat information using TLP for dissemination.

Based on our qualitative and quantitative evaluation, MiRTrust constitutes a viable and collaborative approach to assess the trust level of collaborating ISPs and thus deploy semi-automated remediations of a security events.

Conclusion & Future Research

8

This chapter summarizes the main findings with regard to the RQs and provides a general conclusion based on the research presented in this thesis. Furthermore, the strength and limitations of this work are considered. Finally, we suggest directions for future research.

8.1. Main Conclusions

In this section, we present the main conclusions of this thesis. In Chapter 1 (Introduction), we defined the following overall research goal:

Research Goal: *Develop a collaborative, automated approach to mitigate the effects of DDoS attacks at Internet Scale.*

The key terms in the research goal were *collaboration* and *automation*. However, our research revealed that collaboration among ISPs is often not performed for three reasons. First, ISPs regard themselves as competitors in the same market segment. Second, at the time this research was started, ISPs did not see themselves responsible to perform attack detection and mitigation as they did not see financial incentives for themselves. Removing attack traffic reduces the overall network traffic in an ISP network, while ISPs are paid based on the amount of transferred traffic [M85, M86, M87]. Third, the results from our surveys showed that only a minority of ISPs adhere to established IT processes, security standards and frameworks (e.g., ITIL, COBIT, ISO/IEC 27000), even though being compliant to security standards and frameworks is known to enhance security and ensures reproducible workflow outputs.

The absence of security standard compliance of ISPs also contradicts the establishment of automated processes to detect and mitigate DDoS attacks. Moreover, the results of our surveys show that ISPs fear to face a huge amount of false positive alarms or to deploy a new attack target within their own network infrastructure and services

in case of an automated detection and mitigation approach. As a result, ISPs are afraid to lose control over their own network infrastructure and services.

Nevertheless, we consider ISPs to be key points for DDoS attack detection and mitigation. Therefore, the main contribution of this thesis is to leverage synergies and opportunities arising from the combination of the key terms to mitigate the effects of DDoS attacks at Internet scale.

8.2. Revising the Research Questions

In this section, we provide the answers for our RQs defined in Chapter 1 (Introduction) and presented how a collaborative, automated approach to mitigate the effect of DDoS attacks at Internet Scale can be deployed.

Research Question 1: *Is distributed and automatic mitigation at ISP level performed and if yes, how?*

In Chapter 2 (Current DDoS Detection & Mitigation: A Survey), we presented empirical data about current detection and mitigation approaches. This data was provided by the expertise and experience of network administrators, network operators and network security engineers gathered through a cross-sectional and a repeated cross-sectional survey. Even though survey research remains most used in applied social research, this thesis relies on those well-known empirical methods to enrich the quality and fine-tune its research results to satisfy the requirements of ISP networks. The cross-sectional survey performed in the year 2013 determined the state of the art in attack detection and mitigation in ISP networks and Figure 8.1 shows that this survey resulted in four main findings. These four main findings serve as a starting point of RQs 2 - 5. In addition, Figure 8.1 shows the link between the first and the follow-up survey. The repeated cross-sectional survey was conducted in the year 2015 with the main intention to add additional evidence to the findings of the first survey and re-evaluate the results of the first survey to ensure that our research results two years ago are still valid.

We found that current detection and mitigation approaches in ISP networks use flow-based data (e.g., NetFlow, IPFIX) and are performed primarily within single Autonomous Systems (ASs) and thus not distributed. Further, the survey revealed that in case of a large-scale cyber attack collaboration among partners is done on an ad-hoc-basis via telephone or email without the use of well-defined processes or standards for security managements (e.g., ITIL). We recognized that automatic

Figure 8.1.: Research results based on the survey research described Chapter 2 (Current DDoS Detection & Mitigation: A Survey)

mitigation to limit the effects of an ongoing large-scale attack is not a requirement of ISPs, because ISPs are afraid that automatic mitigation systems gain increasing interest to be compromised and thus perform unwanted automatic actions within the network. However, ISPs prefer semi-automatic mitigation.

In order to achieve the overall research goal of this thesis, the survey provides the following 4 main findings:

Finding 1: Many exchange formats available but unknown

For ISPs to collaborate, a common data representation to describe security-related data is important. Further, an exchange protocol to transmit security events over network borders is also required. Even though, various exchange formats and protocols have been published in context of intrusion detection and incident management, it is still a challenge to find a standardized exchange format that is thoroughly validated and tested in full scale of industry trials. In addition, exchange formats and protocols are often unknown for ISPs.

Finding 2: Collaborative mitigation is done on an ad-hoc and reactive basis

To counteract large-scale network-based attacks, ISP networks have been identified as a key position within the Internet infrastructure. Even though collaboration of trusted partners and their exchange of threat information to mitigate and respond to a network-based attack is regarded as valuable, exchanging threat information is currently done on an ad-hoc basis via email or telephone. As a consequence, mitigation is only performed in case a large-scale network-based attack occurred and already caused effects within the network and thus can be described as reactive mitigation.

Finding 3: Mitigation is done manually

Although network-based attacks are getting larger, more frequent and sophisticated and thus the number of related security events increases, network operators often manually

analyze and initiate possible countermeasures against ongoing network-based attacks to recover normal operations. Automatic mitigation and response systems to speed up mitigation and response capabilities within ISP networks are not widely deployed. Even though network operators are afraid that automatic mitigation systems gain increasing interest to be compromised, network operators prefer semi-automatic mitigation and would like to make use of it.

Finding 4: Collaboration requires the establishment of trust

Security event sharing is deemed of critical importance to counteract large-scale attacks at ISP networks. On the one hand, security event sharing is regarded to speed up organization's mitigation and response capabilities. On the other hand, it is currently done on an ad-hoc basis via email, member calls or in personal meetings only under the premise that participating partners are personally known to each other. As a consequence, mitigation and response actions are delayed and thus security events are not processed in time. However, collaboration of trusted partners to mitigate and respond to a network-based attack is regarded as valuable, but the personal knowledge of each sharing partner to develop trust in order to share security events does not scale very well.

We will now revisit each one of the RQs 2-5, which stem from the aforementioned findings.

Research Question 2: *How are security events exchanged and do they satisfy the requirements of an ISP?*

In Chapter 3 (Exchange of Threat Information), we reviewed 10 exchange formats and 7 exchange protocols used in context of intrusion detection and incident management. The security event exchange formats can be categorized into four groups: S-expressions, XML-based and MIMEMessage-based formats and syslog. The security event exchange protocols can be categorized into the two groups: Secured and unsecured. Our conclusion is that even though various exchange formats and protocols have been presented, it is still a challenge to find a standardized exchange format and protocol that is thoroughly validated and tested in full scale of industry trials. In addition, none of the exchange formats has been used in conjunction with flow-based data despite RQ 1 revealed that current detection and mitigation approaches in ISP networks rely on flow-based data.

In order to satisfy the requirement of flow-based interoperability of an ISP, we present the new exchange format FLEX in section 3.4. FLEX is suitable to carry data of

flow export technologies (e.g. Cisco NetFlow, IPFIX) that are used to identify, track and mitigate malicious traffic. Further, FLEX is intended to facilitate the cooperation among network operators and focus on an automated threat information exchange. In addition, since FLEX messages are disseminated using SMTP, FLEX is easy to deploy and it integrates with existing infrastructure.

Research Question 3: *Is mitigation currently done in a proactive or reactive approach? Would it be possible to do it in a proactive approach?*

The main findings in Chapter 2 (Current DDoS Detection & Mitigation: A Survey) revealed that current mitigation is done on an ad-hoc and reactive basis. To limit the effects of an ongoing large-scale cyber attack and to perform mitigation in a proactive approach, Chapter 4 (Collaboration Process) introduces a communication process that supports an automated dissemination of threat information based on FLEX in context of ISPs. Further, this communication process supports achieving the situational awareness of the current threat landscape, pools expertise and resources and facilitates the automated defense. Even though some collaborating partners have not been actively involved in an ongoing attack, the communication process ensures that all collaborating partners are informed about the effects of the attack. As a result, this communication process helps organizations to speed up their mitigation and response capabilities.

Research Question 4: *Is mitigation currently done manually or automatic? Would it be possible to perform mitigation in an automated way?*

In Chapter 2 (Current DDoS Detection & Mitigation: A Survey), we found that current mitigation is done manually. One approach to counteract the proliferation of network-based attacks is a generalized and automated process that initiates mitigation and response measures. Traditionally, automated mitigation and response processes make use of an IRS that provides a distinct response selection process, and is able to collaborate with other security appliances, such as firewalls to block and terminate suspicious traffic. However, available solutions proposed by the scientific community are not widely adopted. Further, each IRS uses different metrics to select an appropriate response and some of the metrics are only applicable for specific system environments. To mitigate network-based attacks by incorporating an intuitive response selection process, Chapter 5 (Selection of an Appropriate Response) introduces a new response

selection model, called REASSESS that evaluates negative and positive impacts associated with each countermeasure and selects the most appropriate response action to limit the effects of an large-scale network-based attack.

In Chapter 6 (DDoS Defense using MTD and SDN), we combined the defense techniques moving-target using Software Defined Networking. This combination increases the attackers uncertainty due to an ever-changing attack surface. We found that the effects of a large-scale cyber attack can be significantly reduced using the moving-target defense and Software Defined Networking.

Research Question 5: *How can trust among collaborative partners be arranged?*

Chapter 2 (Current DDoS Detection & Mitigation: A Survey) revealed that collaboration requires the establishment of trust. Current collaborative approaches take place under the premise that participating partners are personally known to each other. As a consequence, mitigation and response actions are delayed and thus security events are not processed in time. Therefore, Chapter 7 (Trust) presents a trust model that determines a trust and a knowledge level of a security event in order to deploy semi-automated remediations and facilitate the dissemination of security event information using the exchange format FLEX in the context collaborating ISPs. This trust model is scalable and helps to build a trust community in order to share sensitive information about threats and its remediation suggestions.

8.3. Directions for Future research

In the final section of this thesis, we provide an overview of possible directions for future research. This overview is split up into three main directions: i) standardization of the data representation and dissemination of threat information, ii) legal enforcements to incentivize DDoS mitigation at ISP level and (iii) establish collaborations among network operators.

Standardization of the Data Representation and Dissemination of Threat Information

In Chapter 3 (Exchange of Threat Information), we presented the exchange format FLEX. FLEX is intended to be an interoperable format for dissemination of threat information and was presented and discussed at the Internet Architecture Board Coordinating Attack Response at Internet Scale (CARIS) Workshop [M31]. As a result,

Kathleen Moriarty, the Area Director of the MILE WG, invited us to present FLEX at the MILE WG meeting within the IETF 93rd [M32]. As the audience within MILE WG meeting suggested, a RFC of FLEX should be written and submitted to the IETF as follow up work. In general, these efforts should resolve into a standardized format and protocol for threat information dissemination.

Besides the standardization efforts of FLEX, future research should investigate if FLEX can be used to disseminate unique characteristics of attacks (fingerprints) and if yes how. Namely, the use of FLEX to support the dissemination of fingerprints collected within the DDoSDB¹ and sharing these among law-enforcement agencies is under investigation.

Legal Enforcements to incentivize DDoS Mitigation at ISP Level

In Chapter 2 (Current DDoS Detection & Mitigation: A Survey), we found that ISP are getting paid to transfer network traffic instead of providing security services for their customers. As long as the ISP network does not face any effects of a large-scale cyber attack, there is currently no incentive to perform DDoS mitigation. Future work should focus on the misaligned financial incentives of ISPs [M88] and turn into an incentive to perform DDoS mitigation. One step into future direction are legal regulations. Currently, legal regulations [M77] are working drafts or approved and ISPs are increasingly being held accountable to contribute in mitigating DDoS attacks even the effects are only seen at their customers site.

Establish Collaboration

Chapter 2 (Current DDoS Detection & Mitigation: A Survey) revealed that collaboration requires the establishment of trust. Current collaborative approaches take place under the premise that participating partners are personally known to each other. As a consequence, mitigation and response actions are delayed and take place while effects of an ongoing attack already occurred. Future work should focus on the establishment of a trust community using a trust model in order to disseminate security events. Furthermore, future work should focus on the use of a trust model within the trust community that is well-known, tested and able to scale. The establishment of a trust community using a trust model supports a proactive mitigation approach and thus prevents effects caused by large-scale DDoS attacks.

¹<https://ddosdb.org/>

Repetition of Survey Research

We developed and conducted two surveys - a cross-sectional and a repeated cross-sectional survey that provide an overview of detection and mitigation practice in ISP networks at two points in time. We conducted the repeated cross-sectional survey to add additional evidence to the findings of the research results of the first survey. However, cross-sectional surveys should be repeated periodically to show changes over time.

Current Efforts on a Collaborative and Automated DDoS Defense

At the time this research started, DDoS had been evolved to one of the major causes responsible for network infrastructure and service outages. Therefore our main research goal was to develop a collaborative, automated approach to mitigate the effects of DDoS attacks at Internet Scale.

Today, DDoS are still the major causes responsible for network infrastructures and service outages. Exchange formats and protocols, concepts to collaborate and approaches to establish trust that have been published within this research are now getting adopted by several network operator communities [M89, M90, M91].

Questionnaire of Surveys

This chapter presents the questions and provided answers within our questionnaires.

A.1. Survey 2013

Welcome to the da/sec survey on network attack detection and mitigation. Network-based attacks pose a strong threat to the Internet landscape and academia is working towards different approaches on attack detection and mitigation. Yet, a clear understanding of possibilities and issues in commercial networks is missing. Hence, this survey aims at gaining insight in real-world processes, structures and capabilities of IT companies and the computer networks they run. This survey is conducted in context of different publicly funded research projects and work done in the combined eco e.V. and DE-CIX competence group security. Results of this survey shall frame future research and community activities in the area of Internet security. The survey targets at companies of all size and color running an own computer network. Questions within this survey address some organizational aspects, as well as processes, techniques and tools you may have employed in order to perform network attack detection and mitigation. Filling the survey should not last longer than 5 - 10 minutes. Hence, the survey can ideally be answered during a short and relaxing coffee break. The survey is completely anonymous. We will not require you to enter any personally identifiable information, neither will log IP addresses with your responses. Nevertheless, you will have the possibility to voluntarily provide us your email address and/or name. If you do so, you give us the possibility of getting in touch with you in case of any open questions. Thank you very much for taking your time to support our work! There are 56 questions in this survey

Company and personal information

The following questions will ask some general questions regarding your company and your role within your company. Answering these questions allows us to draw more fine-grained conclusions on the survey. Questions marked with asterisk (*) are required.

1. What is your role within your company?*
- Please choose only one of the following:

A. QUESTIONNAIRE OF SURVEYS

- ☐ Network operator or engineer
 - ☐ Security operator or engineer
 - ☐ Data protection officer/Information security officer
 - ☐ Management
 - ☐ Other
2. How would you classify your company?*
- Please choose only one of the following:
- ☐ Carrier/Telco/ISP
 - ☐ Hosting/Data Center/Colocation Service Provider
 - ☐ Research and Education Network
 - ☐ CDN/Content Delivery
 - ☐ Cloud Service Provider
 - ☐ Enterprise
 - ☐ Other
3. Where is your company headquartered?*
- Please choose only one of the following:
- ☐ Africa
 - ☐ America
 - ☐ Asia
 - ☐ Australia
 - ☐ Europe
4. Let x denote the monthly average traffic rate transported within your company's network. What approximates x best?
- Please choose only one of the following:
- ☐ $0 < x \leq 1$ Gbit/s
 - ☐ $1 < x \leq 5$ Gbit/s
 - ☐ $5 < x \leq 10$ Gbit/s
 - ☐ $10 < x \leq 50$ Gbit/s
 - ☐ $50 < x \leq 100$ Gbit/s
 - ☐ > 100 Gbit/s
5. Does your company have a dedicated security department that handles network security events (e.g. compromised servers, DoS attacks)?*
- Please choose only one of the following:
- ☐ Yes
 - ☐ No

6. Let x denote the size of your company's security department. What approximates x best?*

Please choose only one of the following:

- ☐ $0 < x \leq 2$
- ☐ $2 < x \leq 5$
- ☐ $5 < x \leq 10$
- ☐ $10 < x \leq 20$
- ☐ $20 < x \leq 50$
- ☐ > 50
- ☐ Do not know

7. Does your company have a dedicated department that handles customer security events (e.g. bot infected devices)?*

Please choose only one of the following:

- ☐ Yes
- ☐ No

8. Let x denote the size of your company's department that handles customer security events. What approximates x best?*

Please choose only one of the following:

- ☐ $0 < x \leq 2$
- ☐ $2 < x \leq 5$
- ☐ $5 < x \leq 10$
- ☐ $10 < x \leq 20$
- ☐ $20 < x \leq 50$
- ☐ > 50
- ☐ Do not know

9. Does your company employ measures to pro-actively detect Internet attacks?

Please choose only one of the following:

- ☐ Yes
- ☐ No

10. Does your company plan to employ measures to be able to pro-actively detect Internet attacks in future?

Please choose only one of the following:

- ☐ Yes
- ☐ No

11. Does your company employ measures to correlate security events?

Please choose only one of the following:

A. QUESTIONNAIRE OF SURVEYS

☐ Yes

☐ No

12. Does your company adhere to IT process or security frameworks and/or standards?

Please choose all that apply:

☐ Yes, ITIL

☐ Yes, COBIT

☐ Yes, ISO/IEC 27000 (e.g., 27001, 27002)

☐ Other

Attacks and threats

The following questions will cover attacks and threats that you may have faced or fear to face. Questions marked with asterisk (*) are required.

13. What raises your awareness of Internet attacks?*

Please choose all that apply:

☐ Your company's infrastructure had been under attack

☐ Your company's customers have been under attack

☐ Legal and/or regulatory requirements

☐ Publications in journals, magazines, web sites and mailing lists

☐ Presentations and discussions on conferences

☐ Other

14. How do you inform yourself and keep track of new types of attacks and threats?*

Please choose all that apply:

☐ Mailing lists

☐ Security conferences

☐ Web sites/blogs/syndication feeds

☐ Social networks

☐ Vendors

☐ Scientific publications

☐ Other

15. How would you rate the risk the following threats pose to your company's infrastructure?*

Please choose the appropriate response for each item:

	Very low	Low	Medium	High	Very high	Do not know
Misconfiguration of network equipment and servers	☐	☐	☐	☐	☐	☐
Compromised and/or bot infected devices within your network	☐	☐	☐	☐	☐	☐
Compromised and/or bot infected devices outside your network	☐	☐	☐	☐	☐	☐
Targeted attacks/zero-day exploits	☐	☐	☐	☐	☐	☐
Denial of service attacks	☐	☐	☐	☐	☐	☐
Malware	☐	☐	☐	☐	☐	☐

16. How would you rate the risk the following threats pose to your company's customers?*

Please choose the appropriate response for each item:

	Very low	Low	Medium	High	Very high	Do not know
Misconfiguration of network equipment and servers	☐	☐	☐	☐	☐	☐
Botnets	☐	☐	☐	☐	☐	☐
Drive-by-downloads	☐	☐	☐	☐	☐	☐
Targeted attacks/zero-day exploits	☐	☐	☐	☐	☐	☐
Denial of service attacks	☐	☐	☐	☐	☐	☐
Malware	☐	☐	☐	☐	☐	☐
Information theft	☐	☐	☐	☐	☐	☐

17. Let x denote the number of attacks targeting your company's infrastructure and customers per month on average. What approximates x best?

Please choose only one of the following:

- ☐ $0 < x \leq 10$
☐ $10 < x \leq 20$
☐ $20 < x \leq 50$
☐ $50 < x \leq 100$

A. QUESTIONNAIRE OF SURVEYS

- ☐ $100 < x \leq 250$
- ☐ $250 < x \leq 500$
- ☐ > 500
- ☐ Do not know

Data and tools

The following questions will cover data and tools your company uses for attack detection and mitigation. Questions marked with asterisk (*) are required.

18. Which type of tools does your company use for attack detection?*
- Please choose all that apply:
- ☐ Commercial products
 - ☐ Opensource software
 - ☐ Self-build tools
19. Which type of tools does your company use to correlate security events?*
- Please choose all that apply:
- ☐ Commercial products
 - ☐ Opensource software
 - ☐ Self-build tools
20. Does your company have the technical ability to perform network wide deep packet inspection? With 'technical ability' we mean: is it, from a technical point of view, possible to perform network wide deep packet inspection. I.e. have you the possibility to deploy tap devices? Have you the possibility to configure traffic shunts (e.g. via MPLS)? Can you configure port mirroring? If your answer to one or more of these exemplary questions is 'yes', we would call this a 'technical ability' to perform network wide deep packet inspection.
- Please choose only one of the following:
- ☐ Yes
 - ☐ No
21. Do you think it is feasible for your company to perform network wide deep packet inspection?*
- Please choose only one of the following:
- ☐ Yes
 - ☐ No
22. Why do you think network wide deep packet inspection is not feasible?*
- Please choose all that apply:
- ☐ Requires too much human resources (OPEX)
 - ☐ Financial invest too high (CAPEX)
 - ☐ Too much network traffic to process

- ☐ Want to protect our customers privacy
 - ☐ Prohibited by legal and/or regulatory requirements
 - ☐ Other
23. Does your company employ tools to visualize network security events?
Please choose only one of the following:
- ☐ Yes
 - ☐ No
24. Which tools does your company employ to visualize network security events?*
- Please choose all that apply:
- ☐ ArgSight
 - ☐ AfterGlow
 - ☐ PixlCloud
 - ☐ Self-build tools
 - ☐ Other
25. Which kind of data does your company currently use for attack detection?*
- Please choose all that apply:
- ☐ SNMP data
 - ☐ sFlow data
 - ☐ NetFlow data
 - ☐ IPFIX data
 - ☐ Raw packets
 - ☐ Darknet/backscatter
 - ☐ Mail/DNS/DHCP server logs
 - ☐ Other server logs
 - ☐ Other
26. Which kind of data does your company plan to use for attack detection in future?*
- Please choose all that apply:
- ☐ SNMP data
 - ☐ sFlow data
 - ☐ NetFlow data
 - ☐ IPFIX data
 - ☐ Raw packets
 - ☐ Darknet/backscatter
 - ☐ Mail/DNS/DHCP server logs
 - ☐ Other server logs

A. QUESTIONNAIRE OF SURVEYS

☐ Other

27. Does your company's infrastructure currently offer the availability to collect NetFlow data?

Please choose only one of the following:

☐ Yes

☐ No

28. Which NetFlow versions are supported in your company's infrastructure? Please choose all that apply:

☐ NetFlow version 5

☐ NetFlow version 7

☐ NetFlow version 8

☐ NetFlow version 9

29. Does your company's infrastructure currently offer the availability to collect sFlow data?

Please choose only one of the following:

☐ Yes

☐ No

30. Does your company's infrastructure currently offer the availability to collect IPFIX data?

Please choose only one of the following:

☐ Yes

☐ No

31. Do you think collecting and processing NetFlow data in order to perform network attack detection protects privacy rights of your customers better than collecting and processing raw packets?

Please choose only one of the following:

☐ Yes

☐ No

Mitigation and reaction

This section covers all questions related to mitigation of and reaction on detected attacks. Questions marked with asterisk (*) are required.

32. Which measures do you usually take to mitigate network attacks targeting at your company's infrastructure?*

Please choose all that apply:

☐ Access control list/packet filter

☐ Firewall

- ☐ Intrusion Prevention System
- ☐ Source-based remote-triggered blackhole
- ☐ Destination-based remote-triggered blackhole
- ☐ Other

33. Which measures do you usually take to mitigate network attacks targeting at your company's customers?*

Please choose all that apply:

- ☐ Access control list/packet filter
- ☐ Firewall
- ☐ Intrusion Prevention System
- ☐ Source-based remote-triggered blackhole
- ☐ Destination-based remote-triggered blackhole
- ☐ Other

34. Let x denote the number of minutes it takes to initially mitigate an ongoing attack on average? What approximates x best?

Please choose only one of the following:

- ☐ $0 < x \leq 10$
- ☐ $10 < x \leq 20$
- ☐ $20 < x \leq 30$
- ☐ > 30
- ☐ Do not know

35. Let x denote the number of days it takes to completely resolve attacks on average? What approximates x best?

Please choose only one of the following:

- ☐ $0 < x \leq 1$
- ☐ $1 < x \leq 3$
- ☐ $3 < x \leq 5$
- ☐ $5 < x \leq 10$
- ☐ $10 < x \leq 20$
- ☐ > 20
- ☐ Do not know

36. Does your company share attack information with 3rd parties?

Please choose only one of the following:

- ☐ Yes
- ☐ No

37. With whom does your company share attack information?*

Please choose all that apply:

A. QUESTIONNAIRE OF SURVEYS

- ☐ Customers
☐ Vendors
☐ Competitors
☐ CERTs
☐ Law enforcement
☐ Other
38. How does your company exchange attack information with 3rd parties?
Please choose all that apply:
- ☐ E-Mail
☐ Telephone
☐ Automated by detection system
☐ Other
39. Does your company use a standardized format for automated data exchange?
Please choose only one of the following:
- ☐ Yes
☐ No
40. How well do you know the following data exchange formats?*
- Please choose the appropriate response for each item:
	Do or did use	Known	Heard of	Unknown
IDMEF	☐	☐	☐	☐
IODEF	☐	☐	☐	☐
MARF	☐	☐	☐	☐
x-ARF	☐	☐	☐	☐
CEE	☐	☐	☐	☐
MAEC	☐	☐	☐	☐
SCAP	☐	☐	☐	☐
41. Would you consider using the following formats for data exchange?*
- Please choose the appropriate response for each item:
	Yes	No	Do not know
IDMEF	☐	☐	☐
IODEF	☐	☐	☐
MARF	☐	☐	☐
x-ARF	☐	☐	☐
CEE	☐	☐	☐
MAEC	☐	☐	☐
SCAP	☐	☐	☐
42. Does your company have a well-defined process for mitigation and/or information exchange?*
- Please choose only one of the following:
- ☐ Yes
☐ No

Role of ISPs and IXPs

We would like to collect your thoughts on the role of Internet Service Providers (ISPs) and Internet Exchange Points (IXPs) in detection and mitigation of network attacks targeting your own infrastructure and customers. Questions marked with asterisk (*) are required.

43. Do you think ISPs play an important role in network attack detection and mitigation?*

Please choose only one of the following:

- ☐ Yes
- ☐ No

44. What would be the appropriate way of thinking, from your point of view?*

Please choose only one of the following:

- ☐ ISPs shall protect its customers from Internet attacks
- ☐ ISPs shall protect the Internet from attack originating from its customers

45. Why do you think ISPs do not play an important role in network attack detection and mitigation?*

46. Do you think there is a financial incentive to perform network attack detection and mitigation for ISPs?

Please choose only one of the following:

- ☐ Yes
- ☐ No

47. Why do you think there is no financial incentive for ISPs to perform network attack detection and mitigation?*

48. Do you think IXPs can/could play an important role in network attack detection and mitigation?*

Please choose only one of the following:

- ☐ Yes
- ☐ No

49. Which task do you think IXPs can/could take in network attack detection and mitigation?*

Please choose all that apply:

- ☐ Detection/Analysis
- ☐ Mitigation/Response
- ☐ Correlation
- ☐ Coordination
- ☐ Other

A. QUESTIONNAIRE OF SURVEYS

50. Why do you think IXPs can/should not play an important role in network attack detection and mitigation?*

51. Do you think IXPs should implement measures to centrally and conditionally collect network traffic traces?*

Please choose only one of the following:

☐ Yes

☐ No

Contact information

The following questions are all optional. You have the possibility to give us some supplementary information that allow us to get in touch with you if we have further questions on your answers.

52. What is the name of your company?

53. What is your email address?

54. What is your name?

55. If you were to introduce new system capable to do pro-active network attack detection, event correlation and visualization as well as information exchange, what would be your requirements?

56. Is there any final information, hint or comment you want to give?

Thank you for participating in this survey, we really appreciate the time you spent! If you left your personal contact information, as a little "thank you" we will send you the results of this survey after we analyzed and concluded on all answers.

A.2. Survey 2015

Welcome to the survey on mitigation and response of network attacks. Network-based attacks pose a strong threat to the Internet landscape. In my PhD I am investigating different approaches on attack mitigation and response. Yet, a clear understanding of how mitigation and response is performed in commercial networks is missing. Hence, this survey aims at gaining insight in real-world processes, structures and capabilities of IT companies and the computer networks they run. This survey is conducted in context of different publicly funded research projects. Results of this survey shall frame future research and community activities in the area of Internet security. This survey targets all organizations that manage their own network. Questions within this survey address some organizational aspects, as well as processes, techniques and tools you may have employed in order to perform automatic attack mitigation and response. Filling the survey should not last longer than 10 minutes. Hence, the survey can ideally be answered during a short and relaxing coffee break. The survey is completely anonymous. We will not require you to enter any personally identifiable information, neither will log IP addresses with your responses. Thank you very much for taking your time to support our work! There are 52 questions in this survey. Questions marked with asterisk (*) are required.

Company and personal information

The following questions will ask some general questions regarding your company and your role within your company. Answering these questions allows us to draw more fine-grained conclusions on the survey.

1. How familiar are you with your organization's mitigation and response activities?*
- Please choose only one of the following:
 - ☐ Very familiar
 - ☐ Familiar
 - ☐ Somewhat familiar
 - ☐ Not familiar
2. Are you involved in your organization's mitigation and response activities?*
- Please choose only one of the following:
 - ☐ Significant involvement
 - ☐ Some involvement
 - ☐ No involvement
3. How would you classify your organization?*
- Please choose only one of the following:
 - ☐ Tier 2/3 Provider
 - ☐ Tier 1 Service Provider
 - ☐ Enterprise
 - ☐ Hosting/Data Center/Colocation Service Provider
 - ☐ Managed Service Provider
 - ☐ Educational/Research Institute
 - ☐ Government
 - ☐ Cloud Service Provider
 - ☐ DNS Registrar / DNS Service Provider
 - ☐ CDN / Content Delivery
 - ☐ National Research and Education Network Provider
 - ☐ Other
4. Where is your company headquartered?*
- Please choose only one of the following:
 - ☐ Africa
 - ☐ Asia
 - ☐ Australia / Oceania
 - ☐ Europe

A. QUESTIONNAIRE OF SURVEYS

- ☐ North America
 - ☐ South America
5. What organizational level best describes your current position?*
- Please choose only one of the following:
- ☐ Network operator or engineer
 - ☐ Security operator and engineer
 - ☐ Data protection officer / Information security officer
 - ☐ Other
6. How many years of relevant experience do you have?*
- Please write your answer(s) here:
- Total years of IT or security experience:
 - Total year in current position:
7. Please give an estimate of average traffic rate transported over your organization's network border routers.*
- Please choose only one of the following:
- ☐ < 1 Gbit/s
 - ☐ 1 – 5 Gbit/s
 - ☐ 6 – 10 Gbit/s
 - ☐ 11 – 50 Gbit/s
 - ☐ 51 – 100 Gbit/s
 - ☐ > 100 Gbit/s
8. Does your organization have the possibility to reconfigure access routers/border routers?*
- Please choose only one of the following:
- ☐ Yes
 - ☐ No

Processes and involved third parties

9. Is your organization target of DDoS attacks?*
- Please choose only one of the following:
- ☐ Yes
 - ☐ No
10. Please estimate the number of attacks targeting your organization's infrastructure per month on average?*
- Only answer this question if the following conditions are met: ((Q9 == YES))
- Please choose only one of the following:
- ☐ 1 – 2 attacks

- ☐ 3 – 5 attacks
- ☐ 6 – 10 attacks
- ☐ 11 – 20 attacks
- ☐ > 20 attacks

11. Please estimate the number of minutes it takes to initially mitigate an ongoing DDoS attack on average?*

Only answer this question if the following conditions are met: ((Q9 == YES))

Please choose only one of the following:

- ☐ < 15 minutes
- ☐ 15 – 30 minutes
- ☐ 31 – 60 minutes
- ☐ 61 – 120 minutes
- ☐ > 120 minutes

12. Please estimate the number of hours/days to completely resolve DDoS attacks on average?*

Only answer this question if the following conditions are met: ((Q9 == YES))

Please choose only one of the following:

- ☐ < 12 hours
- ☐ 13 – 24 hours
- ☐ 1 – 5 days
- ☐ 6 – 10 days
- ☐ 11 – 20 days
- ☐ > 20 days

13. Does your organization have a cooperation with a third party (e.g. ISP, network protection service) that can assist your organization in mitigating and responding to a security event/incident? *

Please choose only one of the following:

- ☐ Yes
- ☐ No
- ☐ Unsure

14. What best describes this third party?*

Only answer this question if the following conditions are met: ((Q13 == YES))

Please choose all that apply:

- ☐ Consulting firm
- ☐ Forensic firm
- ☐ Risk management firm
- ☐ Law firm

A. QUESTIONNAIRE OF SURVEYS

- ☐ ISP
 - ☐ Packet cleaning house (e.g., Cloudflare)
 - ☐ Other
15. What best describes how this third party is utilized by your organization?*
- Only answer this question if the following conditions are met: ((Q13 == YES))
- Please choose all that apply:
- ☐ First responder to security events
 - ☐ To augment the skill set of your CSIRT
 - ☐ To augment the capacity of your CSIRT during crisis situations
 - ☐ To aid our NOC team
 - ☐ Other
16. What functions or departments are involved in the security response process?*
- Please choose all that apply:
- ☐ IT management
 - ☐ Executive management
 - ☐ Board of directors
 - ☐ Risk management
 - ☐ Office of general counsel/legal
 - ☐ Human resources
 - ☐ Other
17. Do your organization's incident investigations result in the production of threat indicators, which are then used to defend the organization from future attacks?*
- Please choose only one of the following:
- ☐ Yes
 - ☐ No
 - ☐ Unsure

Automatic mitigation and response systems

18. Please estimate the number of security breaches experienced by your organization within the past 12 months.*
- Please choose only one of the following:
- ☐ < 1 security breach
 - ☐ 2 – 5 security breaches
 - ☐ 6 – 10 security breaches
 - ☐ > 10 security breaches
19. Please estimate the number of security events/incidents reported by automated detection mechanisms per month on average.*
- Please choose only one of the following:

- ☐ < 10 security events/incidents
 - ☐ 11 – 25 security events/incidents
 - ☐ 26 – 50 security events/incidents
 - ☐ 51 – 100 security events/incidents
 - ☐ 101 – 500 security events/incidents
 - ☐ > 500 security events/incidents
20. How many security events/incidents reported by automated detection mechanisms (e.g. Intrusion detection systems, SIEM etc) per month on average are real security events and need to be handled?*
- Please choose only one of the following:
- ☐ None
 - ☐ 1 – 10% of the reported security events/incidents
 - ☐ 11 – 25% of the reported security events/incidents
 - ☐ 26 – 50% of the reported security events/incidents
 - ☐ 51 – 100% of the reported security events/incidents
21. Does your organization make use of mitigation and response tools that perform automatic mitigation and reaction steps to defend the organization's network?*
- Please choose only one of the following:
- ☐ Yes
 - ☐ No
 - ☐ Unsure
22. Please rate the following statement: The usage of an automatic mitigation and response tool would speed up my organization's mitigation and response capabilities?*
- Only answer this question if the following conditions are met: ((Q21 == No))
- Please choose only one of the following:
- ☐ Strongly agree
 - ☐ Agree
 - ☐ Disagree
 - ☐ Strongly disagree
23. Does your organization plan to make use of mitigation and response tools, which perform automatic mitigation and reaction steps to defend the organization's network in the future?*
- Only answer this question if the following conditions are met: ((Q21 == No))
- Please choose only one of the following:
- ☐ Yes, we are planning to do it
 - ☐ We are looking into it

A. QUESTIONNAIRE OF SURVEYS

- ☐ No, we are not make use of it
- ☐ I am not aware of it

24. What kind of actions would you and your organization like to use in an automatic mitigation and response tool?*

Only answer this question if the following conditions are met: ((Q21 == No))

Please choose all that apply:

- ☐ Rerouting traffic
- ☐ Changing blocking/filter capabilities (Blacklisting etc.)
- ☐ Notification of involved functions or departments within the organization
- ☐ Rate limiting at ingress
- ☐ Exchange data with trusted partners
- ☐ Quarantine machines
- ☐ Changing the target's IP address
- ☐ Other

25. Which kind of automatic actions are performed with the aid of mitigation and response tools?*

Only answer this question if the following conditions are met: ((Q21 == No))

Please choose all that apply:

- ☐ Rerouting traffic
- ☐ Changing blocking/filter capabilities (Blacklisting etc.)
- ☐ Notification of involved functions or departments within the organization
- ☐ Rate limiting at ingress
- ☐ Exchange data with trusted partners
- ☐ Quarantine machines
- ☐ Changing the target's IP address
- ☐ Other

26. Which type of mitigation and response tools does your organization use to perform automatic mitigation?*

Only answer this question if the following conditions are met: ((Q21 == No))

Please choose all that apply:

- ☐ Commercial product
- ☐ Open source product
- ☐ Self-built tools

27. Which commercial products/service does your organization employ to perform automatic mitigation?*

Only answer this question if the following conditions are met: ((Q26.Commercial Product == Yes))

Please choose all that apply:

- ☐ Products from Arbor Networks
- ☐ Products from Prolexic
- ☐ Service from Cloudflare
- ☐ Service from Incapsula
- ☐ Others

28. What best describes the reasons of your organization not to make use of an automatic mitigation and response tool?*

Only answer this question if the following conditions are met: ((Q21 == No))

Please choose all that apply:

- ☐ Commercial solutions are too expensive
- ☐ Too high risks of false positives
- ☐ No trust in open source solutions
- ☐ No efficient support with open source solutions available
- ☐ Others

Data

29. Does your organization communicate with national CSIRTs?*

Please choose only one of the following:

- ☐ Yes
- ☐ No

30. How does your organization communicate with national CSIRTs?*

Only answer this question if the following conditions are met: ((Q29 == Yes))

Please choose all that apply:

- ☐ Telephone
- ☐ Email
- ☐ Automated by mitigation and response systems
- ☐ Others

31. Does your organization make use of databases that provide vulnerability or threat information e.g. Common Vulnerabilities and Exposures (CVE), Shadowserver or RIPE)?*

Please choose all that apply:

- ☐ Yes, we use CVE
- ☐ Yes, we use RIPE
- ☐ Yes, we use Shadowserver
- ☐ No, we do not make use of databases by external sources
- ☐ Others

A. QUESTIONNAIRE OF SURVEYS

32. Does your organization perform traffic filtering based on IP blacklisting, whitelisting or greylisting?*

Please choose only one of the following:

- ☐ Yes
- ☐ No

33. What best describes the filtering approach your organization uses?*

Only answer this question if the following conditions are met: ((Q32== Yes))

Please choose all that apply:

- ☐ Blacklists
- ☐ Whitelists
- ☐ Greylists
- ☐ Others

34. How frequently does your organization update black-, white- and greylists?*

Only answer this question if the following conditions are met: ((Q32== Yes))

Please choose only one of the following:

- ☐ Once a day
- ☐ More than once a day
- ☐ 1-2 times a week
- ☐ 3-5 times a week
- ☐ Other

35. Does your organization immediately include the changes at the black-, white- and greylist during an update process?*

Please choose only one of the following:

- ☐ Yes
- ☐ No, we review the modifications first and then include important changes
- ☐ Other

36. From which third party does your organization use black-, white- and greylists?*

Please choose all that apply:

- ☐ Spamhaus
- ☐ Shadowserver
- ☐ Spamcorp
- ☐ DNSWL
- ☐ Others

37. Does your organization configure networking devices according to BCP 38 (RFC 2827 or RFC2267)?*

Only answer this question if the following conditions are met: ((Q32== Yes))

Please choose only one of the following:

☐ Yes

☐ No

38. Does your organization use CyBex (Cybersecurity Information Exchange Framework (X.1500)) or parts of this framework?*

Please choose only one of the following:

☐ Yes

☐ No

☐ Unsure

39. Would your organization make use of a cloud-based detection and mitigation solution to perform attack detection and mitigation?*

Please choose only one of the following:

☐ Yes

☐ No

☐ Unsure

40. What best describes the filtering approach your organization uses?*

Only answer this question if the following conditions are met: ((Q39 == No))

Please choose all that apply:

☐ Impact unknown

☐ Customer's privacy

☐ Data should remain within organization

☐ Success rate unknown

☐ Others

41. Does your organization make use of network configuration protocols?*

Please choose only one of the following:

☐ Yes

☐ No

42. Which of the following network configuration protocols are used by your organization?*

Only answer this question if the following conditions are met: ((Q41 == Yes))

Please choose all that apply:

☐ Netconf

☐ SNMP

☐ OpenFlow

☐ Open vSwitch DB Management Protocol

☐ Others

43. Does your organization's infrastructure currently offer the technical ability to make use of OpenFlow (SDN)?*

Please choose only one of the following:

A. QUESTIONNAIRE OF SURVEYS

☐ Yes

☐ No

44. Does your organization plan to have the technical ability to make use of Open-Flow (SDN) in 3 years?*

Only answer this question if the following conditions are met: ((Q43== No))

Please choose only one of the following:

☐ Yes, we are planning to do it

☐ We are looking into it

☐ No, we are not make use of it

☐ I am not aware of it

45. Does your organization's infrastructure currently offer the technical ability to support BGP FlowSpec?*

Please choose only one of the following:

☐ Yes

☐ No

46. Does your organization plan to have the technical ability to make use of BGP FlowSpec in 3 years?*

Only answer this question if the following conditions are met: ((Q45== No))

Please choose only one of the following:

☐ Yes, we are planning to do it

☐ We are looking into it

☐ No, we are not make use of it

☐ I am not aware of it

Exchange and collaboration

47. Does your organization share threat indicators with the following entities?*

Please choose all that apply:

☐ None

☐ Various CERTs and CSIRTs

☐ Law enforcement or other governmental entities

☐ We receive information from sharing partners, but we do not share our information with them

☐ We neither receive nor share any information

☐ Others

48. Please rate the following statement: Collaboration between trusted parties would improve mitigation and response capabilities.*

Please choose only one of the following:

- ☐ Strongly agree
- ☐ Agree
- ☐ Disagree
- ☐ Strongly disagree

49. Does your organization share security events/incidents with the following entities?*

Please choose all that apply:

- ☐ None
- ☐ Various CERTs and CSIRTs
- ☐ Law enforcement or other governmental entities
- ☐ Industry peers
- ☐ We receive information from sharing partners, but we do not share our information with them
- ☐ We neither receive nor share any information
- ☐ Others

50. Does your organization use a trusted exchange approach to transmit security events/incidents?*

Please choose only one of the following:

- ☐ Yes
- ☐ No
- ☐ Unsure

51. How well do you know the following data exchange protocols and formats?*

Please choose the appropriate response for each item:

	Do or did use	Known	Heard of	Unknown
x.cybex-beep	☐	☐	☐	☐
x.cybex-tp	☐	☐	☐	☐
x.eaa	☐	☐	☐	☐
x.evcert	☐	☐	☐	☐
SCAP	☐	☐	☐	☐
IDXP	☐	☐	☐	☐
IDMEF	☐	☐	☐	☐
IODEF	☐	☐	☐	☐
x-ARF	☐	☐	☐	☐
PFOC	☐	☐	☐	☐

52. Please rate the following statement: Security events/incidents that are shared with third parties for collaboration must be signed and encrypted.*

Please choose only one of the following:

- ☐ Strongly agree
- ☐ Agree
- ☐ Disagree
- ☐ Strongly disagree

A. QUESTIONNAIRE OF SURVEYS

Thank you for participating in this survey, we really appreciate the time you spent! If you have any questions regarding this survey or our research projects or if you would like to further support our projects, please feel free to get in touch with jessica.steinberger@h-da.de. Thank you for completing this survey.

Source Code Repository

B

This chapter aims to overcome closed source and system dependency of this research domain. Thus, we share the test scenario scripts used within this thesis as well as the source code itself as public available data which can be downloaded from <https://github.com/jesstei/MiR>.

This chapter presents the location and the structure of the source code repository of all previous chapters of this thesis.

Glossary

Amplification

describes the disproportionate increase of a response packets compared to the initial request packet.

Cross-sectional survey

collects data to make inferences about a population of interest at one point in time.

Exchange format

defines a representation of information for sharing data.

Exchange protocol

is a set of rules defining how to interconnect network devices and establish a channel to transmit network datagrams, representing exchange formats, across a computer network.

Moving target

is the concept of controlling changes across multiple system dimensions in order to increase uncertainty and apparent complexity for attackers, reduce their window of opportunity and increase the costs of their probing and attack efforts.

NetFlow

is a network protocol developed by Cisco for collecting IP traffic information and monitoring network traffic.

OpenFlow

is a communication protocol in SDN environments that enables the SDN Controller to directly interact with the forwarding plane of network devices such as switches and routers, both physical and virtual (hypervisor-based).

Reflection

is a technique to make publicly available network devices send attack traffic to the attack target in order to hide the attacker's identity.

Security event

is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

Security incident

a single or a series of unwanted information security events that have a significant probability of compromising business operations and threatening information security.

Software defined networking

is a network paradigm, which decouples the control and the data plane of a network device.

Survey research

is a specific type of field study that involves the collection of data from a sample of elements drawn from a well-defined population through the use of a questionnaire.

References

Books

- [B1] Royce A. Singleton, Jr. and Bruce C. Straits. *Approaches to Social Research*. 5th ed. New York: Oxford University Press, 2010. ISBN: 978-0-195-37298-4 (cit. on p. 6).
- [B2] Floyd J. Fowler. *Survey Research Methods*. 5th ed. London: Sage Publications, 2013. ISBN: 978-1-483-32359-6 (cit. on p. 16).
- [B3] Louis M. Rea and Richard A. Parker. *Designing and Conducting Survey Research - A Comprehensive Guide*. 4th ed. New York: John Wiley & Sons, 2014. ISBN: 978-1-118-76703-0 (cit. on pp. 16 sq.).
- [B4] Raffael Marty. *Applied Security Visualization*. 1st ed. Westford, Massachusetts: Addison Wesley Professional, 2009. ISBN: 978-0-321-51010-5 (cit. on p. 22).
- [B5] Michael Kerrisk. *The Linux Programming Interface : A Linux and UNIX System Programming Handbook*. San Francisco: No Starch Press, 2010. ISBN: 978-1-593-27220-3 (cit. on p. 47).
- [B6] Chris Sanders and Jason Smith. *Applied Network Security Monitoring: Collection, Detection, and Analysis*. 1st. Syngress Publishing, 2013. ISBN: 978-0-124172081. URL: <http://www.sciencedirect.com/science/book/9780124172081> (cit. on pp. 74, 89).
- [B7] Ilya Grigoryev. *AnyLogic in Three Days: a Quick Course in Simulation Modeling*. 2nd ed. Grigoryev, Ilya, 2014. ISBN: 978-1-508-93374-8 (cit. on p. 142).

Conference articles

- [C1] Cas G. J. Putman, Abhishta, and Lambertus J. M. Nieuwenhuis. “Business Model of a Botnet”. In: *Proceedings of the 26th Euromicro International conference on Parallel, Distributed, and Network-Based Processing*. Vol. abs/1804.10848. PDP '18. Cambridge, United Kingdom: IEEE Press, 2018. ISBN: 978-1-5386-4976-3. URL: <http://arxiv.org/abs/1804.10848> (cit. on p. 2).
- [C2] Christian Rossow. “Amplification Hell: Revisiting Network Protocols for DDoS Abuse”. In: *Proceedings of the 2014 Network and Distributed System Security (NDSS) Symposium*. Feb. 2014. URL: <http://www.internetsociety.org/doc/amplification-hell-revisiting-network-protocols-ddos-abuse> (cit. on p. 3).

- [C3] Marc Kührer et al. “Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks”. In: *Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT 14)*. San Diego, CA: USENIX Association, Aug. 2014. URL: <https://www.usenix.org/conference/woot14/workshop-program/presentation/kuhrer> (cit. on p. 3).
- [C4] Marc Kührer et al. “Exit from Hell? Reducing the Impact of Amplification DDoS Attacks”. In: *Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA: USENIX Association, 2014, pp. 111–125. ISBN: 978-1-931971-15-7. URL: <https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/kuhrer> (cit. on p. 3).
- [C5] Jair J. Santanna et al. “Booters - An analysis of DDoS-as-a-service attacks”. In: *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. May 2015, pp. 243–251. DOI: [10.1109/INM.2015.7140298](https://doi.org/10.1109/INM.2015.7140298) (cit. on p. 3).
- [C6] Aiko Pras et al. “DDoS 3.0 - How Terrorists Bring Down the Internet”. In: *Measurement, Modelling and Evaluation of Dependable Computer and Communication Systems: 18th International GI/ITG Conference, MMB & DFT 2016, Münster, Germany, April 4-6, 2016, Proceedings*. Ed. by Anne Remke and R. Boudewijn Haverkort. Cham: Springer International Publishing, Nov. 2016, pp. 1–4. ISBN: 978-3-319-31559-1. DOI: [10.1007/978-3-319-31559-1_1](https://doi.org/10.1007/978-3-319-31559-1_1). URL: http://dx.doi.org/10.1007/978-3-319-31559-1_1 (cit. on p. 5).
- [C7] Jessica Steinberger et al. “Real-time DDoS Defense: A collaborative Approach at Internet Scale”. In: *Proceedings of the 10th SPRING of the SIG Security - Intrusion Detection and Response of the German Informatics Society SIG SIDAR*. July 2015. URL: <http://www.gi-fg-sidar.de/spring/SIDAR-Reports/SIDAR-Report-SR-2015-01.pdf> (cit. on p. 9).
- [C8] Jessica Steinberger et al. ““Ludo” - Kids playing Distributed Denial of Service”. In: *Connected Communities, The Networking Conference 2016, 15-18 June, 2016, Prague, Czech Republic, Selected Papers*. Ed. by Klaas Wierenga. GÉANT Ltd, Nov. 2016. ISBN: 978-90-77559-25-3. URL: <http://www.terena.org/publications/tnc16-proceedings/> (cit. on pp. 10, 12, 85).
- [C9] Jessica Steinberger et al. “Anomaly Detection and Mitigation at Internet Scale: A Survey”. In: *Proceedings of the 7th IFIP International Conference on Autonomous Infrastructure, Management and Security (AIMS 2013): Emerging Management Mechanisms for the Future Internet*. Ed. by Guillaume Doyen et al. Vol. 7943. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, pp. 49–60. ISBN: 978-3-642-38997-9. DOI: [10.1007/978-3-642-38998-6_7](https://doi.org/10.1007/978-3-642-38998-6_7). URL: http://dx.doi.org/10.1007/978-3-642-38998-6_7 (cit. on pp. 10, 15, 41, 46, 64, 71 sq.).
- [C10] Jessica Steinberger et al. “Collaborative Attack Mitigation and Response: A survey”. In: *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM 2015)*. May 2015. DOI: [10.1109/INM.2015.7140407](https://doi.org/10.1109/INM.2015.7140407) (cit. on pp. 11, 15, 74, 116, 121, 124, 131, 143).
- [C11] Jessica Steinberger et al. “How to exchange security events? Overview and evaluation of formats and protocols”. In: *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. May 2015, pp. 261–269. DOI: [10.1109/INM.2015.7140300](https://doi.org/10.1109/INM.2015.7140300) (cit. on pp. 11, 45, 64, 76).

-
- [C12] Jessica Steinberger et al. “Collaborative DDoS Defense using Flow-based Security Event Information”. In: *Proceedings of the 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS 2016)*. Apr. 2016. DOI: [10.1109/NOMS.2016.7502852](https://doi.org/10.1109/NOMS.2016.7502852) (cit. on pp. 11, 71, 116, 118).
- [C13] Sven Ossenbühl, Jessica Steinberger, and Harald Baier. “Towards Automated Incident Handling: How to Select an Appropriate Response against a Network-Based Attack?”. In: *Proceedings of the Ninth International Conference on IT Security Incident Management IT Forensics (IMF)*. May 2015, pp. 51–67. DOI: [10.1109/IMF.2015.13](https://doi.org/10.1109/IMF.2015.13) (cit. on pp. 12, 85).
- [C14] Jessica Steinberger et al. “DDoS Defense using MTD and SDN”. In: *Proceedings of the 2018 IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*. May 2018. DOI: [10.1109/INM.2015.7140407](https://doi.org/10.1109/INM.2015.7140407) (cit. on pp. 12, 115).
- [C15] Jessica Steinberger et al. “In Whom Do We Trust - Sharing Security Events”. In: *Management and Security in the Age of Hyperconnectivity: 10th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2016, Munich, Germany, June 20-23, 2016, Proceedings*. Ed. by Rémi Badonnel et al. Cham: Springer International Publishing, 2016, pp. 111–124. ISBN: 978-3-319-39814-3. DOI: [10.1007/978-3-319-39814-3_11](https://doi.org/10.1007/978-3-319-39814-3_11). URL: http://dx.doi.org/10.1007/978-3-319-39814-3_11 (cit. on pp. 12, 125 sq., 128, 133, 140).
- [C16] Michel van Eeten et al. “The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data”. In: *OECD Science, Technology and Industry Working Papers*. Vol. 2010/05. Freeman, Rebecca, Auriol, Laudeline, and Misu, Max, 2010. DOI: [10.1787/5km4k7m9n3vj-en](https://doi.org/10.1787/5km4k7m9n3vj-en) (cit. on p. 15).
- [C17] Jérôme François et al. “BotTrack: Tracking Botnets Using NetFlow and PageRank”. In: *NETWORKING 2011*. Ed. by Jordi Domingo-Pascual et al. Vol. 6640. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2011, pp. 1–14. ISBN: 978-3-642-20756-3. DOI: [10.1007/978-3-642-20757-0_1](https://doi.org/10.1007/978-3-642-20757-0_1) (cit. on pp. 15, 27, 74, 76, 89, 110).
- [C18] Leyla Bilge et al. “Disclosure: Detecting Botnet Command and Control Servers Through Large-scale NetFlow Analysis”. In: *Proceedings of the 28th Annual Computer Security Applications Conference. ACSAC ’12*. Orlando, Florida: ACM, 2012, pp. 129–138. ISBN: 978-1-4503-1312-4. DOI: [10.1145/2420950.2420969](https://doi.org/10.1145/2420950.2420969) (cit. on pp. 15, 27, 74, 76, 89).
- [C19] Sebastian Abt and Harald Baier. “Towards Efficient and Privacy-Preserving Netowrk-Based Botnet Detection Using NetFlow Data”. In: *Proceedings of the Ninth International Network Conference (INC 2012)*. Ed. by Reinhardt A. Botha, Paul S. Dowland, and Steven M. Furnell. Lulu.com, 2012, pp. 37–50. ISBN: 978-1-84102-315-1 (cit. on p. 27).
- [C20] David Evans, Anh Nguyen-Tuong, and John Knight. “Effectiveness of Moving Target Defenses”. English. In: *Moving Target Defense*. Ed. by Sushil Jajodia et al. Vol. 54. Advances in Information Security. Springer New York, 2011, pp. 29–48. ISBN: 978-1-4614-0976-2. DOI: [10.1007/978-1-4614-0977-9_2](https://doi.org/10.1007/978-1-4614-0977-9_2). URL: http://dx.doi.org/10.1007/978-1-4614-0977-9_2 (cit. on p. 39).
- [C21] Jafar Haadi Jafarian, Ehab Al-Shaer, and Qi Duan. “Openflow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking”. In: *Proceedings of the First Workshop on Hot Topics in Software Defined Networks. HotSDN ’12*. Helsinki, Finland: ACM, 2012, pp. 127–132. ISBN: 978-1-4503-1477-0. DOI: [10.1145/2342441.2342467](https://doi.org/10.1145/2342441.2342467) (cit. on p. 39).

- [C22] Dan Schnackenberg, Kelly Djahandari, and Dan Sterne. “Infrastructure for Intrusion Detection and Response”. In: *Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX)*. 2000, pp. 3–11. DOI: [10.1109/DISCEX.2000.821505](https://doi.org/10.1109/DISCEX.2000.821505) (cit. on p. 48).
- [C23] Joseph Betser et al. “GlobalGuard: creating the IETF-IDWG Intrusion Alert Protocol (IAP)”. In: *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX)*. 2001, pp. 22–34. DOI: [10.1109/DISCEX.2001.932189](https://doi.org/10.1109/DISCEX.2001.932189) (cit. on pp. 48, 53 sq.).
- [C24] Eric W. Burger et al. “Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies”. In: *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*. WISCS ’14. Scottsdale, Arizona, USA: ACM, 2014, pp. 51–60. ISBN: 978-1-4503-3151-7. DOI: [10.1145/2663876.2663883](https://doi.org/10.1145/2663876.2663883) (cit. on pp. 49, 54).
- [C25] Tim Buchheim et al. “Implementing the intrusion detection exchange protocol”. In: *Proceedings of the Seventeenth Annual Computer Security Applications Conference (ACSAC)*. Dec. 2001, pp. 32–41. DOI: [10.1109/ACSAC.2001.991519](https://doi.org/10.1109/ACSAC.2001.991519) (cit. on p. 54).
- [C26] Wenke Lee et al. “A Data Mining and CIDF Based Approach for Detecting Novel and Distributed Intrusions”. In: *Proceedings of the third International Workshop of Recent Advances in Intrusion Detection (RAID)*. Ed. by Hervé Debar, Ludovic Mé, and S. Felix Wu. Berlin, Heidelberg: Springer Berlin Heidelberg, Oct. 2000, pp. 49–65. ISBN: 978-3-540-39945-2. DOI: [10.1007/3-540-39945-3_4](https://doi.org/10.1007/3-540-39945-3_4). URL: http://dx.doi.org/10.1007/3-540-39945-3_4 (cit. on p. 60).
- [C27] Gerhard Munz and Georg Carle. “Real-time Analysis of Flow Data for Network Attack Detection”. In: *Proceedings of the 10th IFIP/IEEE International Symposium on Integrated Network Management (IM)*. May 2007, pp. 100–108. DOI: [10.1109/INM.2007.374774](https://doi.org/10.1109/INM.2007.374774) (cit. on p. 64).
- [C28] Mario Golling, Rick Hofstede, and Robert Koch. “Towards multi-layered Intrusion Detection in high-speed Networks”. In: *Proceedings of the 6th International Conference On Cyber Conflict (CyCon)*. June 2014, pp. 191–206. DOI: [10.1109/CYCON.2014.6916403](https://doi.org/10.1109/CYCON.2014.6916403) (cit. on pp. 64, 72, 76, 134).
- [C29] George Oikonomou et al. “A Framework for a Collaborative DDoS Defense”. In: *Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC’06)*. Dec. 2006, pp. 33–42. DOI: [10.1109/ACSAC.2006.5](https://doi.org/10.1109/ACSAC.2006.5) (cit. on p. 71).
- [C30] Tim van de Kamp et al. “Private Sharing of IOCs and Sightings”. In: *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*. WISCS ’16. Vienna, Austria: ACM, 2016, pp. 35–38. ISBN: 978-1-4503-4565-1. DOI: [10.1145/2994539.2994544](https://doi.org/10.1145/2994539.2994544) (cit. on p. 73).
- [C31] Florian Tegeler et al. “BotFinder: Finding Bots in Network Traffic Without Deep Packet Inspection”. In: *Proceedings of the 8th International Conference on Emerging Networking Experiments and Technologies*. CoNEXT ’12. Nice, France: ACM, 2012, pp. 349–360. ISBN: 978-1-4503-1775-7. DOI: [10.1145/2413176.2413217](https://doi.org/10.1145/2413176.2413217) (cit. on pp. 74, 76, 89).
- [C32] Christopher Roy Strasburg et al. “A Framework for Cost Sensitive Assessment of Intrusion Response Selection”. In: *Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference*. Vol. 1. July 2009, pp. 355–360. DOI: [10.1109/COMPSAC.2009.54](https://doi.org/10.1109/COMPSAC.2009.54) (cit. on pp. 74, 89, 94, 96).

-
- [C33] Adrian Paschke and Paul Vincent. “A Reference Architecture for Event Processing”. In: *Proceedings of the Third ACM International Conference on Distributed Event-Based Systems*. DEBS '09. Nashville, Tennessee: ACM, 2009, 25:1–25:4. ISBN: 978-1-60558-665-6. DOI: [10.1145/1619258.1619291](https://doi.org/10.1145/1619258.1619291). URL: <http://doi.acm.org/10.1145/1619258.1619291> (cit. on p. 77).
- [C34] Nor Badrul Anuar et al. “An investigation and survey of response options for Intrusion Response Systems (IRSs)”. In: *Proceedings of the 2010 Information Security for South Africa*. Aug. 2010, pp. 1–8. DOI: [10.1109/ISSA.2010.5588654](https://doi.org/10.1109/ISSA.2010.5588654) (cit. on p. 85).
- [C35] Thomas Toth and Christopher Kruegel. “Evaluating the impact of automated intrusion response mechanisms”. In: *Proceedings of the 18th Annual Computer Security Applications Conference*. Feb. 2002, pp. 301–310. DOI: [10.1109/CSAC.2002.1176302](https://doi.org/10.1109/CSAC.2002.1176302) (cit. on pp. 87, 90, 96, 111).
- [C36] Bingrui Foo et al. “ADEPTS: adaptive intrusion response using attack graphs in an e-commerce environment”. In: *Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05)*. June 2005, pp. 508–517. DOI: [10.1109/DSN.2005.17](https://doi.org/10.1109/DSN.2005.17) (cit. on pp. 91 sq., 102, 111).
- [C37] Sushil Jajodia and Steven Noel. “Topological Vulnerability Analysis”. In: *Cyber Situational Awareness: Issues and Research*. Ed. by Sushil Jajodia et al. Boston, MA: Springer US, 2010, pp. 139–154. ISBN: 978-1-4419-0140-8. DOI: [10.1007/978-1-4419-0140-8_7](https://doi.org/10.1007/978-1-4419-0140-8_7) (cit. on p. 94).
- [C38] Rangarajan Vasudevan et al. “MIDAS: An Impact Scale for DDoS attacks”. In: *Proceedings of the 15th IEEE Workshop on Local Metropolitan Area Networks*. June 2007, pp. 200–205. DOI: [10.1109/LANMAN.2007.4295999](https://doi.org/10.1109/LANMAN.2007.4295999) (cit. on p. 110).
- [C39] Rui Zhuang, Scott A. DeLoach, and Xinming Ou. “Towards a Theory of Moving Target Defense”. In: *Proceedings of the First ACM Workshop on Moving Target Defense*. MTD 14. Scottsdale, Arizona, USA: ACM, 2014, pp. 31–40. ISBN: 978-1-4503-3150-0. DOI: [10.1145/2663474.2663479](https://doi.org/10.1145/2663474.2663479) (cit. on pp. 115–120).
- [C40] Rui Zhuang et al. “A Theory of Cyber Attacks: A Step Towards Analyzing MTD Systems”. In: *Proceedings of the Second ACM Workshop on Moving Target Defense*. MTD 15. Denver, Colorado, USA: ACM, 2015, pp. 11–20. ISBN: 978-1-4503-3823-3. DOI: [10.1145/2808475.2808478](https://doi.org/10.1145/2808475.2808478) (cit. on pp. 115, 117, 120).
- [C41] Rui Zhuang, Scott A. DeLoach, and Xinming Ou. “A Model for Analyzing the Effect of Moving Target Defenses on Enterprise Networks”. In: *Proceedings of the 9th Annual Cyber and Information Security Research Conference*. CISR 14. Oak Ridge, Tennessee, USA: ACM, 2014, pp. 73–76. ISBN: 978-1-4503-2812-8. DOI: [10.1145/2602087.2602088](https://doi.org/10.1145/2602087.2602088) (cit. on pp. 116, 121, 128 sq.).
- [C42] Richard Wang, Dana Butnariu, and Jennifer Rexford. “OpenFlow-based Server Load Balancing Gone Wild”. In: *Proceedings of the 11th USENIX Conference on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services*. Hot-ICE'11. Boston, MA: USENIX Association, 2011, pp. 1–6. URL: <https://www.usenix.org/conference/hot-ice11/openflow-based-server-load-balancing-gone-wild> (cit. on p. 119).
- [C43] Huangxin Wang, Fei Li, and Songqing Chen. “Towards Cost-Effective Moving Target Defense Against DDoS and Covert Channel Attacks”. In: *Proceedings of the 2016 ACM Workshop on Moving Target Defense*. MTD 16. Vienna, Austria: ACM, 2016, pp. 15–25. ISBN: 978-1-4503-4570-5. DOI: [10.1145/2995272.2995281](https://doi.org/10.1145/2995272.2995281) (cit. on p. 120).

- [C44] Quan Jia, Kun Sun, and Angelos Stavrou. “MOTAG: Moving Target Defense against Internet Denial of Service Attacks”. In: *Proceedings of the 22nd International Conference on Computer Communication and Networks (ICCCN)*. July 2013, pp. 1–9. DOI: [10.1109/ICCCN.2013.6614155](#) (cit. on p. 121).
- [C45] Quan Jia et al. “Catch Me If You Can: A Cloud-Enabled DDoS Defense”. In: *Proceedings of the 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. June 2014, pp. 264–275. DOI: [10.1109/DSN.2014.35](#) (cit. on p. 121).
- [C46] Sridhar Venkatesan et al. “A moving target defense approach to mitigate DDoS attacks against proxy-based architectures”. In: *Proceedings of the IEEE Conference on Communications and Network Security (CNS) 2016*. Oct. 2016, pp. 198–206. DOI: [10.1109/CNS.2016.7860486](#) (cit. on p. 121).
- [C47] Mason Wright et al. “Moving Target Defense Against DDoS Attacks: An Empirical Game-Theoretic Analysis”. In: *Proceedings of the 2016 ACM Workshop on Moving Target Defense*. MTD 16. Vienna, Austria: ACM, 2016, pp. 93–104. ISBN: 978-1-4503-4570-5. DOI: [10.1145/2995272.2995279](#) (cit. on p. 121).
- [C48] Douglas C. MacFarland and Craig A. Shue. “The SDN Shuffle: Creating a Moving-Target Defense Using Host-based Software-Defined Networking”. In: *Proceedings of the Second ACM Workshop on Moving Target Defense*. MTD 15. Denver, Colorado, USA: ACM, 2015, pp. 37–41. ISBN: 978-1-4503-3823-3. DOI: [10.1145/2808475.2808485](#) (cit. on p. 121).
- [C49] Saptarshi Debroy et al. “Frequency-minimal moving target defense using software-defined networking”. In: *Proceedings of the International Conference on Computing, Networking and Communications (ICNC) 2016*. Feb. 2016, pp. 1–6. DOI: [10.1109/ICNC.2016.7440635](#) (cit. on p. 121).
- [C50] Ankur Chowdhary, Sandeep Pisharody, and Dijiang Huang. “SDN Based Scalable MTD Solution in Cloud Network”. In: *Proceedings of the 2016 ACM Workshop on Moving Target Defense*. MTD 16. Vienna, Austria: ACM, 2016, pp. 27–36. ISBN: 978-1-4503-4570-5. DOI: [10.1145/2995272.2995274](#) (cit. on p. 121).
- [C51] Avinatan Hassidim et al. “Network utilization: The flow view”. In: *Proceedings of the IEEE INFOCOM 2013*. Apr. 2013, pp. 1429–1437. DOI: [10.1109/INFOCOM.2013.6566937](#) (cit. on pp. 126, 130).
- [C52] Alfarez Abdul-Rahman and Stephen Hailes. “A Distributed Trust Model”. In: *Proceedings of the 1997 Workshop on New Security Paradigms*. NSPW '97. Langdale, Cumbria, United Kingdom: ACM, 1997, pp. 48–60. ISBN: 0-89791-986-6. DOI: [10.1145/283699.283739](#) (cit. on pp. 134, 137 sq., 141).
- [C53] Jacek Jonczyk, Markus Wüthrich, and Rolf Haenni. “A probabilistic trust model for GnuPG”. In: *Proceedings of the 23rd Chaos Communication Congress*. 23C3. Berlin, Germany, 2006, pp. 61–66 (cit. on pp. 134, 137 sq.).
- [C54] Karen K. Fullam et al. “A Specification of the Agent Reputation and Trust (ART) Testbed: Experimentation and Competition for Trust in Agent Societies”. In: *Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems*. AAMAS '05. The Netherlands: ACM, 2005, pp. 512–518. ISBN: 1-59593-093-0. DOI: [10.1145/1082473.1082551](#) (cit. on p. 135).
- [C55] Licia Capra. “Engineering Human Trust in Mobile System Collaborations”. In: *Proceedings of the 12th ACM SIGSOFT Twelfth International Symposium on Foundations of Software Engineering*. SIGSOFT '04/FSE-12. Newport Beach, CA, USA: ACM, 2004, pp. 107–116. ISBN: 1-58113-855-5. DOI: [10.1145/1029894.1029912](#) (cit. on pp. 138 sq.).

Journal articles

- [J1] Samuel Greengard. “The New Face of War”. In: *Commun. ACM* 53.12 (Dec. 2010), pp. 20–22. ISSN: 0001-0782. DOI: [10.1145/1859204.1859212](https://doi.org/10.1145/1859204.1859212) (cit. on p. 1).
- [J2] Samuel Greengard. “The War Against Botnets”. In: *Commun. ACM* 55.2 (Feb. 2012), pp. 16–18. ISSN: 0001-0782. DOI: [10.1145/2076450.2076456](https://doi.org/10.1145/2076450.2076456) (cit. on p. 1).
- [J3] Fabrice J. Ryba et al. “Amplification and DRDoS Attack Defense - A Survey and New Perspectives”. In: *CoRR* (2015). URL: <http://arxiv.org/abs/1505.07892> (cit. on pp. 2, 4).
- [J4] Kate Kelly et al. “Good practice in the conduct and reporting of survey research”. In: *International Journal for Quality in Health Care* 15.3 (2003), p. 261. DOI: [10.1093/intqhc/mzg031](https://doi.org/10.1093/intqhc/mzg031) (cit. on p. 6).
- [J5] Meike Ressing, Maria Blettner, and Stefanie J. Klug. “Systematic Literature Reviews and Meta-Analyses”. In: *Deutsches Ärzteblatt International* 106.27 (2009), pp. 456–463. DOI: [10.3238/arztebl.2009.0456](https://doi.org/10.3238/arztebl.2009.0456). URL: <http://www.aerzteblatt.de/int/article.asp?id=65283> (cit. on pp. 7, 69).
- [J6] Deborah J. Cook, David Lawrence Sackett, and Walter O. Spitzer. “Methodologic guidelines for systematic reviews of randomized control trials in health care from the potsdam consultation on meta-analysis”. In: *Journal of Clinical Epidemiology* 48.1 (1995), pp. 167–171. ISSN: 0895-4356. DOI: [http://dx.doi.org/10.1016/0895-4356\(94\)00172-M](http://dx.doi.org/10.1016/0895-4356(94)00172-M). URL: <http://www.sciencedirect.com/science/article/pii/S089543569400172M> (cit. on pp. 7, 69).
- [J7] Maurizio Molina et al. “Operational experiences with anomaly detection in backbone networks”. In: *Computers & Security* 31.3 (2012), pp. 273–285. ISSN: 0167-4048. DOI: [10.1016/j.cose.2012.01.009](https://doi.org/10.1016/j.cose.2012.01.009). URL: <http://www.sciencedirect.com/science/article/pii/S0167404812000132> (cit. on p. 32).
- [J8] Jérôme François, Issam Aib, and Raouf Boutaba. “FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks”. In: *IEEE/ACM Transactions on Networking* 20.6 (Dec. 2012), pp. 1828–1841. ISSN: 1063-6692. DOI: [10.1109/TNET.2012.2194508](https://doi.org/10.1109/TNET.2012.2194508) (cit. on pp. 33, 45, 64, 71, 75).
- [J9] Moti Geva, Amir Herzberg, and Yehoshua Gev. “Bandwidth Distributed Denial of Service: Attacks and Defenses”. In: *IEEE Security & Privacy* 12.1 (2014), pp. 54–61. ISSN: 1540-7993. DOI: [doi.ieeecomputersociety.org/10.1109/MSP.2013.55](https://doi.org/10.1109/MSP.2013.55) (cit. on p. 37).
- [J10] Anthony Rutkowski et al. “CYBEX: The Cybersecurity Information Exchange Framework (x.1500)”. In: *SIGCOMM Comput. Commun. Rev.* 40.5 (Oct. 2010), pp. 59–64. ISSN: 0146-4833. DOI: [10.1145/1880153.1880163](https://doi.org/10.1145/1880153.1880163) (cit. on p. 38).
- [J11] Robert Koch, Mario Golling, and Gabi Dreo. “Evaluation of State of the Art IDS Message Exchange Protocols”. In: *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering* 7.8 (2013), pp. 1017–1026. ISSN: PISSN:2010-376X, EISSN:2010-3778. URL: <http://waset.org/publications/16078> (cit. on p. 46).
- [J12] Panos Kampanakis. “Security Automation and Threat Information-Sharing Options”. In: *IEEE Security & Privacy* 12.5 (Sept. 2014), pp. 42–51. ISSN: 1540-7993. DOI: [10.1109/MSP.2014.99](https://doi.org/10.1109/MSP.2014.99) (cit. on pp. 46, 75 sq.).

- [J13] Jesse David Falk and Murray S. Kucherawy. "Battling Spam: The Evolution of Mail Feedback Loops". In: *IEEE Internet Computing* 14.6 (Nov. 2010), pp. 68–71. ISSN: 1089-7801. DOI: [10.1109/MIC.2010.133](https://doi.org/10.1109/MIC.2010.133) (cit. on p. 51).
- [J14] Hakem Beitollahi and Geert Deconinck. "Analyzing well-known countermeasures against Distributed Denial of Service Attacks". In: *Computer Communications* 35.11 (2012), pp. 1312–1332. ISSN: 0140-3664. DOI: [http://dx.doi.org/10.1016/j.comcom.2012.04.008](https://doi.org/10.1016/j.comcom.2012.04.008). URL: <http://www.sciencedirect.com/science/article/pii/S0140366412001211> (cit. on p. 64).
- [J15] Rick Hofstede et al. "Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX". In: *IEEE Communications Surveys Tutorials* 16.4 (2014), pp. 2037–2064. ISSN: 1553-877X. DOI: [10.1109/COMST.2014.2321898](https://doi.org/10.1109/COMST.2014.2321898) (cit. on pp. 72, 118).
- [J16] Aanna Sperotto et al. "An Overview of IP Flow-Based Intrusion Detection". In: *IEEE Communications Surveys Tutorials* 12.3 (Mar. 2010), pp. 343–356. ISSN: 1553-877X. DOI: [10.1109/SURV.2010.032210.00054](https://doi.org/10.1109/SURV.2010.032210.00054) (cit. on pp. 72, 110).
- [J17] Robin Ruefle et al. "Computer Security Incident Response Team Development and Evolution". In: *IEEE Security Privacy* 12.5 (July 2014), pp. 16–26. ISSN: 1540-7993. DOI: [10.1109/MSP.2014.89](https://doi.org/10.1109/MSP.2014.89) (cit. on pp. 73, 76, 80).
- [J18] Kathleen M. Moriarty. "Incident Coordination". In: *IEEE Security Privacy* 9.6 (Nov. 2011), pp. 71–75. ISSN: 1540-7993. DOI: [10.1109/MSP.2011.164](https://doi.org/10.1109/MSP.2011.164) (cit. on pp. 73, 76, 80).
- [J19] Mohammad A. Faysel and Syed S. Haque. "Towards Cyber Defense: Research in Intrusion Detection and Intrusion Prevention Systems". In: *IJCSNS International Journal of Computer Science and Network Security* 10.7 (2010), pp. 316–325. URL: http://paper.ijcsns.org/07_book/201007/20100741.pdf (cit. on pp. 74, 89).
- [J20] Richard Lippmann et al. "The 1999 DARPA Off-line Intrusion Detection Evaluation". In: *Comput. Netw.* 34.4 (Oct. 2000), pp. 579–595. ISSN: 1389-1286. DOI: [10.1016/S1389-1286\(00\)00139-0](https://doi.org/10.1016/S1389-1286(00)00139-0). URL: [http://dx.doi.org/10.1016/S1389-1286\(00\)00139-0](http://dx.doi.org/10.1016/S1389-1286(00)00139-0) (cit. on p. 75).
- [J21] Jelena Mirkovic and Terry Benzel. "Teaching Cybersecurity with DeterLab". In: *IEEE Security Privacy* 10.1 (Jan. 2012), pp. 73–76. ISSN: 1540-7993. DOI: [10.1109/MSP.2012.23](https://doi.org/10.1109/MSP.2012.23) (cit. on p. 80).
- [J22] Natalia Stakhanova, Samikb Basu, and Johnny S.Wong. "A taxonomy of intrusion response systems". In: *International Journal of Information and Computer Security (IJICS)* 1.1/2 (2007), pp. 169–198. DOI: [10.1504/IJICS.2007.012248](https://doi.org/10.1504/IJICS.2007.012248) (cit. on pp. 85, 110).
- [J23] Natalia Stakhanova et al. "Towards cost-sensitive assessment of intrusion response selection". In: *Journal of Computer Security* 20.2-3 (June 2012), pp. 169–198. DOI: [10.3233/JCS-2011-0436](https://doi.org/10.3233/JCS-2011-0436) (cit. on pp. 85, 94, 107, 111).
- [J24] Zhongqiang Chen, Alex Delis, and Peter Wei. "A Pragmatic Methodology for Testing Intrusion Prevention Systems". In: *The Computer Journal* 52.4 (2009), pp. 429–460. DOI: [10.1093/comjnl/bxn043](https://doi.org/10.1093/comjnl/bxn043) (cit. on pp. 101, 103).
- [J25] Sérgio dos Santos Cardoso Silva et al. "Botnets: A survey". In: *Computer Networks* 57.2 (2013), pp. 378–403. ISSN: 1389-1286. DOI: [10.1016/j.comnet.2012.07.021](https://doi.org/10.1016/j.comnet.2012.07.021). URL: <http://www.sciencedirect.com/science/article/pii/S1389128612003568> (cit. on p. 110).

-
- [J26] Wenke Lee et al. "Toward Cost-sensitive Modeling for Intrusion Detection and Response". In: *Journal of Computer Security* 10.1-2 (July 2002), pp. 5–22. ISSN: 0926-227X. URL: <http://dl.acm.org/citation.cfm?id=597917.597919> (cit. on p. 110).
- [J27] Hamed Okhravi et al. "Finding Focus in the Blur of Moving-Target Techniques". In: *IEEE Security & Privacy* 12.2 (Mar. 2014), pp. 16–26. ISSN: 1540-7993. DOI: [10.1109/MSP.2013.137](https://doi.org/10.1109/MSP.2013.137) (cit. on p. 116).
- [J28] Arpit Gupta et al. "SDX: A Software Defined Internet Exchange". In: *SIGCOMM Comput. Commun. Rev.* 44.4 (Aug. 2014), pp. 579–580. ISSN: 0146-4833. DOI: [10.1145/2740070.2631473](https://doi.org/10.1145/2740070.2631473) (cit. on pp. 116, 118 sq., 121 sq.).
- [J29] Nick McKeown et al. "OpenFlow: Enabling Innovation in Campus Networks". In: *SIGCOMM Comput. Commun. Rev.* 38.2 (Mar. 2008), pp. 69–74. DOI: [10.1145/1355734.1355746](https://doi.org/10.1145/1355734.1355746) (cit. on p. 117).
- [J30] Huangxin Wang et al. "A moving target DDoS defense mechanism". In: *Computer Communications* 46 (2014), pp. 10–21. ISSN: 0140-3664. DOI: <http://dx.doi.org/10.1016/j.comcom.2014.03.009> (cit. on p. 121).
- [J31] Bernhard Ager et al. "Anatomy of a Large European IXP". In: *ACM SIGCOMM Computer Communication Review* 42.4 (Aug. 2012), pp. 163–174. ISSN: 0146-4833. DOI: [10.1145/2377677.2377714](https://doi.org/10.1145/2377677.2377714) (cit. on p. 121).
- [J32] Tatsuya Otsuchi et al. "Traffic prediction for dynamic traffic engineering". In: *Computer Networks* 85 (2015), pp. 36–50. ISSN: 1389-1286. DOI: <http://dx.doi.org/10.1016/j.comnet.2015.05.001>. URL: <http://www.sciencedirect.com/science/article/pii/S1389128615001565> (cit. on pp. 126, 130).
- [J33] Renata Teixeira et al. "Impact of Hot-Potato Routing Changes in IP Networks". In: *IEEE/ACM Transactions on Networking* 16.6 (Dec. 2008), pp. 1295–1307. ISSN: 1063-6692. DOI: [10.1109/TNET.2008.919333](https://doi.org/10.1109/TNET.2008.919333) (cit. on p. 128).
- [J34] Christian Esposito and Mario Ciampi. "On Security in Publish/Subscribe Services: A Survey". In: *IEEE Communications Surveys & Tutorials* 17.2 (2015), pp. 966–997. ISSN: 1553-877X. DOI: [10.1109/COMST.2014.2364616](https://doi.org/10.1109/COMST.2014.2364616) (cit. on p. 134).

Miscellaneous

- [M1] Internet Hall of Fame®. *Internet Hall of Fame Pioneer - J.C.R. Licklider*. Website. 2016. URL: <https://www.internethalloffame.org/inductees/jcr-licklider> (visited on 05/06/2018) (cit. on p. 1).
- [M2] Georgi Dalakov. *Joseph Licklider*. Website. 2016. URL: <http://history-computer.com/Internet/Birth/Licklider.html> (visited on 05/06/2018) (cit. on p. 1).
- [M3] National Telecommunications and Information Administration and Economics and Statistics Administration. *Exploring the Digital Nation: America's Emerging Online Experience*. Website. 2013. URL: https://www.ntia.doc.gov/files/ntia/publications/exploring_the_digital_nation_-_americas_emerging_online_experience.pdf (visited on 12/28/2015) (cit. on p. 1).
- [M4] Caroline Baylon and David Livingstone. *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*. Website. 2015. URL: <https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks> (visited on 12/28/2015) (cit. on p. 1).

- [M5] Barry M. Leiner et al. *Brief History of the Internet*. Website. 2012. URL: <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet> (visited on 11/07/2016) (cit. on p. 1).
- [M6] Zack Whittaker. *Sony takes \$15M hit after North Korea cyberattack*. Website. 2015. URL: <http://www.zdnet.com/article/sony-hack-cost-it-15-million-so-far/> (visited on 12/30/2015) (cit. on pp. 1 sq.).
- [M7] Verizon Enterprise. *2015 Data Breach Investigations Report*. Website. 2015. URL: <http://www.verizonenterprise.com/DBIR/2015/pdf.xml> (visited on 12/29/2015) (cit. on p. 2).
- [M8] Charles Q. Choi. *Nuclear Cybersecurity Woefully Inadequate*. Website. 2015. URL: <http://spectrum.ieee.org/energywise/telecom/security/nuclear-cybersecurity-woefully-inadequate> (visited on 12/30/2015) (cit. on p. 2).
- [M9] Luke Young. *Attacking Network Infrastructure to Generate a 4 Tb/s DDoS for \$5*. Website. 2016. URL: <https://www.defcon.org/html/defcon-24/dc-24-speakers.html#Young> (visited on 01/30/2017) (cit. on pp. 2, 5).
- [M10] Internet2. *About Internet2: Accelerating research and education through community-developed technology*. Website. 2014. URL: <http://www.internet2.edu/media/medialibrary/2014/07/16/about-internet2-2014.pdf> (visited on 01/30/2017) (cit. on p. 2).
- [M11] Michael N. Schmitt. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Website. 2013. URL: <https://ccdcoe.org/tallinn-manual.html> (visited on 01/27/2017) (cit. on p. 2).
- [M12] US-CERT of the Department of Homeland Security. *DDoS Quick Guide*. Website. 2014. URL: <https://www.us-cert.gov/security-publications/DDoS-Quick-Guide> (visited on 01/30/2017) (cit. on p. 3).
- [M13] Brian Krebs. *KrebsOnSecurity Hit With Record DDoS*. Website. 2016. URL: <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/> (visited on 01/30/2017) (cit. on pp. 4 sq.).
- [M14] Matthew Prince. *The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)*. Website. 2013. URL: <https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-how/> (visited on 01/31/2017) (cit. on p. 4).
- [M15] Matthew Prince. *Technical Details Behind a 400Gbps NTP Amplification DDoS Attack*. Website. 2014. URL: <https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/> (visited on 12/31/2015) (cit. on p. 4).
- [M16] Hacker's List. *Hacker's List*. Website. 2015. URL: <https://hackerslist.com/> (visited on 12/30/2015) (cit. on p. 3).
- [M17] Tim Gallo. *Renting a Zombie Farm: Botnets and the Hacker Economy*. Website. 2014. URL: <http://www.symantec.com/connect/blogs/renting-zombie-farm-botnets-and-hacker-economy> (visited on 12/31/2015) (cit. on p. 3).
- [M18] Pierluigi Paganini. *Finding Hacking Services and More in the Deep Web*. Website. 2015. URL: <http://darkmatters.norsecorp.com/2015/06/16/finding-hacking-services-and-more-in-the-deep-web/> (visited on 12/31/2015) (cit. on p. 3).
- [M19] Max Goncharov. *Russian Underground 101*. Website. 2012. URL: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf> (visited on 12/31/2015) (cit. on p. 3).

-
- [M20] Janessa Rivera and Rob van der Meulen. *Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015*. Website. 2014. URL: <http://www.gartner.com/newsroom/id/2905717> (visited on 12/31/2015) (cit. on p. 4).
- [M21] Marek Majkowski. *Mobile Ad Networks as DDoS Vectors: A Case Study*. Website. 2015. URL: <https://blog.cloudflare.com/mobile-ad-networks-as-ddos-vectors> (visited on 12/31/2015) (cit. on p. 4).
- [M22] Quentin Jenkins. *Answers about recent DDoS attack on Spamhaus*. Website. 2013. URL: <https://www.spamhaus.org/news/article/695/answers-about-recent-ddos-attack-on-spamhaus> (visited on 01/31/2017) (cit. on p. 4).
- [M23] Matthew Prince. *The DDoS That Almost Broke the Internet*. Website. 2013. URL: <https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/> (visited on 01/31/2017) (cit. on p. 4).
- [M24] John Graham-Cumming. *Understanding and mitigating NTP-based DDoS attacks*. Website. 2014. URL: <https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/> (visited on 12/31/2015) (cit. on p. 4).
- [M25] Brian Krebs. *Who is Anna-Senpai, the Mirai Worm Author?* Website. 2017. URL: <http://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/> (visited on 01/30/2017) (cit. on p. 5).
- [M26] Brian Krebs. *Akamai on the Record KrebsOnSecurity Attack*. Website. 2016. URL: <https://krebsonsecurity.com/2016/11/akamai-on-the-record-krebsonsecurity-attack/> (visited on 01/30/2017) (cit. on p. 5).
- [M27] Scott Hilton. *Dyn Analysis Summary Of Friday October 21 Attack*. Website. 2016. URL: <http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/> (visited on 01/30/2017) (cit. on p. 5).
- [M28] Dan Goodin. *Record-breaking DDoS reportedly delivered by >145k hacked cameras*. Website. 2016. URL: <https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/> (cit. on p. 5).
- [M29] Julian PT Higgins and Sally Green. *Cochrane Handbook for Systematic Reviews of Interventions*. Website. Mar. 2011. URL: <http://handbook.cochrane.org/> (cit. on pp. 7, 69).
- [M30] Jessica Steinberger et al. *Real-time DDoS Defense: A collaborative Approach at Internet Scale*. Website. **Best Student Poster**. May 2014. URL: <https://tnc2014.terena.org/core/poster/21> (visited on 06/10/2018) (cit. on p. 9).
- [M31] Jessica Steinberger et al. *Exchanging Security Events of flow-based Intrusion Detection Systems at Internet Scale*. Website. June 2015. URL: https://www.iab.org/wp-content/uploads/2015/04/CARIS_2015_submission_3.pdf (visited on 12/28/2015) (cit. on pp. 11, 45, 71, 77, 152).
- [M32] Jessica Steinberger. *FLEX*. Website. July 2015. URL: <https://datatracker.ietf.org/meeting/93/materials/agenda-93-mile/> (visited on 12/12/2017) (cit. on pp. 11, 45, 153).
- [M33] Communications Alliance LTD. *Internet Service Providers Voluntary Code of Practice - For Industry Self-Regulation in the Area of Cyber Security*. Ed. by Communications Alliance LTD. 2014. URL: http://www.commsalliance.com.au/__data/assets/pdf_file/0019/44632/C650_2014.pdf (visited on 06/09/2017) (cit. on p. 15).

- [M34] Cisco Inc. *NetFlow Service Solution Guide*. 2001. URL: http://www.cisco.com/en/US/docs/ios/solutions_docs/netflow/nfwhite.html (visited on 01/31/2001) (cit. on pp. 15, 27).
- [M35] The German Federal Office for Information Security. *IT Infrastructure Library (ITIL) und Informationssicherheit*. Website. 2005. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITIL/itil_pdf.html (visited on 08/09/2017) (cit. on p. 25).
- [M36] International Organization for Standardization. *Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2012)*. Website. 2013. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56891 (cit. on p. 25).
- [M37] Peter Phaal and Marc Lavine. *sFlow Version 5*. Website. 2004. URL: http://www.sflow.org/sflow_version_5.txt (visited on 06/18/2017) (cit. on p. 27).
- [M38] European Union Agency for Network and Information Security. *CERT cooperation and its further facilitation by relevant stakeholders*. Ed. by European Union Agency for Network and Information Security. Website. 2010. URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing/at_download/fullReport (visited on 06/09/2017) (cit. on pp. 30, 41, 137).
- [M39] T-Systems International GmbH. *A step ahead with cloud computing and cyber security*. Ed. by T-Systems International GmbH. <http://www.t-systems.com/news-media/among-the-cebit-innovations-especially-the-cyber-security-solutions-were-of-great-interest-/1234674>. 2014. (Visited on 06/09/2017) (cit. on p. 39).
- [M40] eco — Verband der deutschen Internetwirtschaft e.V. *Network Incident Reporting: Provider verstärken Zusammenarbeit*. Website. 2012. URL: <http://www.eco.de/2012/pressemeldungen/network-incident-reporting-provider-verstaerken-zusammenarbeit.html> (cit. on pp. 41, 51).
- [M41] Robert A. Martin. *Making Security Measurable and Manageable*. Website. July 2013. URL: http://msm.mitre.org/about/Making_Security_Measurable_and_Manageable.pdf (cit. on pp. 46 sq.).
- [M42] ISO/IEC 27005:2011: *Information technology – Security techniques – Information security risk management*. Website. 2011 (cit. on pp. 47 sq.).
- [M43] Paul Cichonski et al. *Special Publication 800-61: Computer Security Incident Handling Guide*. Website. NIST, Aug. 2012 (cit. on pp. 47 sq.).
- [M44] Brian Tung. *Common Intrusion Detection Framework*. Website. 1999. URL: <http://gost.isi.edu/cidf/> (cit. on p. 48).
- [M45] Stuart Staniford-Chen. *Intrusion Detection FAQ: What open standards exist for Intrusion Detection?* Website. Feb. 2008. URL: http://www.sans.org/security-resources/idfaq/id_standards.php (cit. on p. 48).
- [M46] Larry Shields and William Heinbockel. *Common Event Expression*. Website. NIST's 5th Annual IT Security Automation Conference and Expo on October 27. 2009. URL: http://cee.mitre.org/docs/NIST_SCAP_CEE_Briefing.pdf (cit. on p. 48).
- [M47] Artur Hefczyc et al. *XEP-0268: Incident Handling*. Website. 2012. URL: <http://xmpp.org/extensions/xep-0268.html> (visited on 02/13/2017) (cit. on pp. 49, 54).

-
- [M48] RUS-CERT University of Stuttgart. *CAIF - Common Announcement Interchange Format*. Website. 2004. URL: <http://www.caif.info/> (visited on 02/13/2017) (cit. on p. 50).
- [M49] The MITRE Corporation. *Common Event Expression*. Website. May 2013. URL: <https://cee.mitre.org/> (cit. on pp. 50 sq.).
- [M50] John Levine. *ARF is Now an IETF Standard*. Website. Sept. 2010. URL: http://www.circleid.com/posts/20100901_arf_is_now_an_ietf_standard/ (cit. on p. 51).
- [M51] Jan Kohlrausch and Sven Übelacker. *X-ARF: A Reporting and Exchange Format for the Data Exchange of Netflow and Honeypot Data*. Website. 2011. URL: http://www.geant.net/Media_Centre/Media_Library/Media%20Library/xarf_geant_milestone2.pdf (cit. on p. 52).
- [M52] Assuria Ltd. *In Syslog we trust*. Website. Mar. 2012. URL: <http://www.assuria.com/uploads/In%20Syslog%20we%20trust.pdf> (cit. on p. 52).
- [M53] Clifford Kahn, Don Bolinger, and Dan Schnackenberg. *Communication in the Common Intrusion Detection Framework*. June 1998. URL: <http://gost.isi.edu/cidf/drafts/communication.txt> (cit. on p. 53).
- [M54] Dipankar Gupta et al. *IAP: Intrusion Alert Protocol Internet-Draft*. Website. IETF, Sept. 2001. URL: <http://tools.ietf.org/html/draft-ietf-idwg-iap-05> (cit. on p. 54).
- [M55] Edd Dumbill. *XML Watch: Bird's-eye BEEP*. Website. Dec. 2001. URL: <http://www.ibm.com/developerworks/webservices/library/x-beep/> (cit. on p. 54).
- [M56] The MITRE Corporation. *CEE Log Transport (CLT) Specification*. Website. Aug. 2012. URL: <https://cee.mitre.org/language/1.0-beta1/clt.html> (cit. on p. 54).
- [M57] TM Forum. *Sharing Threat Intelligence to Mitigate Cyber Attacks*. Website. 2013. URL: <http://www.tmforum.org/browse.aspx?linkid=51490%5C&docid=19968> (cit. on p. 64).
- [M58] Bret Hartman et al. *Breaking Down Barriers to Collaboration in the Fight Against Advanced Threats*. Website. 2012. URL: <http://www.emc.com/collateral/industry-overview/11652-h9084-aptbdb-brf-0212-online.pdf> (cit. on p. 64).
- [M59] Kathleen M. Moriarty. *Transforming Expectations For Threat-Intelligence Sharing*. Website. 2013. URL: <http://www.emc.com/collateral/emc-perspective/h12175-transf-expect-for-threat-intell-sharing.pdf> (cit. on p. 64).
- [M60] Chris Morrow and Roland Dobbins. *DDoS Open Threat Signaling (DOTS) Working Group Operational Requirements*. Website. July 2015. URL: <https://www.ietf.org/proceedings/93/slides/slides-93-dots-3.pdf> (cit. on pp. 73, 76, 118, 133).
- [M61] DFN-CERT Services GmbH. *D1.7.1 – Data Format Specification*. Website. July 2013. URL: http://acdc-project.eu/wp-content/uploads/2015/05/ACDC_D1.7.1_Data_Format.pdf (cit. on p. 75).
- [M62] Kathleen M. Moriarty. *CARIS Workshop Summary and Reflection*. Website. June 2015. URL: <https://www.ietf.org/blog/2015/06/caris-workshop-summary-and-reflection/> (cit. on p. 75).
- [M63] Advanced Cyber Defence Centre. *ACDC Deliverables*. Website. 2015. URL: <http://acdc-project.eu/acdc-deliverables/> (cit. on p. 75).
- [M64] abusix GmbH. *x-arf - Network Abuse Reporting 2.0*. Website. 2017. URL: <http://x-arf.org/> (visited on 02/15/2017) (cit. on p. 76).

- [M65] Internet Architecture Board and the Internet Society. *CARIS Workshop Template Submissions*. Website. June 2015. URL: <https://internetsociety2.wufoo.com/reports/caris-workshop-template-submissions/> (cit. on pp. 76, 133).
- [M66] Christopher Roy Strasburg et al. *The Methodology for Evaluating Response Cost for Intrusion Response Systems*. Website. July 2009. URL: <http://www.cs.unb.ca/~natalia/TR08-12.pdf> (cit. on p. 94).
- [M67] Brian Krebs. *New Mirai Worm Knocks 900K Germans Offline*. Website. 2016. URL: <https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/> (visited on 11/30/2016) (cit. on p. 115).
- [M68] Inc. Cloudflare. *Cloudflare Pricing*. Website. 2016. URL: <https://www.cloudflare.com/plans/> (visited on 11/30/2016) (cit. on p. 115).
- [M69] Fred Chong et al. *National Cyber Leap Year Summit 2009 Co-Chairs' Report*. Website. 2009. URL: https://www.nitrd.gov/nitrdgroups/images/b/bd/National_Cyber_Leap_Year_Summit_2009_CoChairs_Report.pdf (cit. on pp. 117, 120).
- [M70] Edward Rhyne. *Moving Target Defense*. Website. URL: <https://www.dhs.gov/science-and-technology/csd-mtd> (cit. on p. 117).
- [M71] Morphisec Ltd. *Moving Target Defense: Common Practices*. Website. 2016. URL: <http://blog.morphisec.com/moving-target-defense-common-practices> (visited on 12/19/2016) (cit. on pp. 117, 122).
- [M72] Open Networking Foundation. *OpenFlow Switch Specification Version 1.5.1 (Protocol version 0x06)*. 2015. URL: <https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf> (visited on 05/26/2015) (cit. on p. 117).
- [M73] SDNCentral LLC. *The Future of Network Virtualization and SDN Controllers*. Website. 2016. URL: <https://www.sdxcentral.com/reports/network-virtualization-sdn-controllers-2016/> (visited on 12/19/2016) (cit. on p. 124).
- [M74] Bob Lantz et al. *Introduction to Mininet*. Website. 2016. URL: <https://github.com/mininet/mininet/wiki/Introduction-to-Mininet> (visited on 12/19/2016) (cit. on p. 125).
- [M75] Philip Reiteringer. *Enabling Distributed Security in Cyberspace*. Website. 2011. URL: <https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf> (cit. on p. 133).
- [M76] The White House. *Executive Order – Improving Critical Infrastructure Cybersecurity*. Website. 2013. URL: <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity> (visited on 07/17/2017) (cit. on p. 133).
- [M77] National Parliament of the Federal Republic of Germany. *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*. Website. 2015. URL: <http://dipbt.bundestag.de/extrakt/ba/WP18/643/64396.html> (visited on 07/17/2017) (cit. on pp. 133, 153).
- [M78] European Union Agency for Network and Information Security. *Reputation-based Systems: a security analysis*. Website. Oct. 2007. URL: <https://www.enisa.europa.eu/publications/archive/reputation-based-systems-a-security-analysis> (cit. on p. 135).
- [M79] The Department of Homeland Security's United States Computer Emergency Readiness Team. *Traffic Light Protocol (TLP) Matrix and Frequently Asked Questions*. Website. 2015. URL: <https://www.us-cert.gov/tlp> (visited on 01/27/2017) (cit. on p. 135).

-
- [M80] Anti-Phishing Working Group. *Charter and Saga - Unifying the global response to cybercrime through data exchange, research and public awareness*. Website. 2015. URL: <http://apwg.org> (cit. on p. 136).
- [M81] Messaging, Malware and Mobile Anti-Abuse Working Group. *Member application*. Website. 2015. URL: <https://www.m3aawg.org/> (cit. on p. 136).
- [M82] Research and Education Networking Information Sharing and Analysis Center. *REN-ISAC Research and Education Networking Information Sharing and Analysis Center*. Website. 2015. URL: <http://www.ren-isac.net> (cit. on p. 136).
- [M83] The Free Software Foundation. *Trust in a key's owner*. Website. 1999. URL: <https://www.gnu.org/gph/en/manual.html> (cit. on p. 138).
- [M84] European Commission's Directorate General for Communications Networks, Content & Technology. *EU Trusted Lists of Certification Service Providers*. Website. 2014. URL: <https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers> (cit. on p. 138).
- [M85] Inc. Cloudflare. *The Relative Cost of Bandwidth Around the World*. Website. 2014. URL: <https://blog.cloudflare.com/the-relative-cost-of-bandwidth-around-the-world/> (visited on 06/17/2018) (cit. on p. 147).
- [M86] Tom Scholl. *Internet Routing and Traffic Engineering*. Website. 2014. URL: <https://aws.amazon.com/de/blogs/architecture/internet-routing-and-traffic-engineering/> (cit. on p. 147).
- [M87] William B. Norton. *Cloud Interconnections*. Website. 2016. URL: https://www.caida.org/workshops/wie/1612/slides/wie1612_wnorton.pdf (visited on 06/17/2018) (cit. on p. 147).
- [M88] European Union Agency for Network and Information Security. *Incentive and Challenges for Information Sharing in the Context of Network and Information Security*. Ed. by European Union Agency for Network and Information Security. Website. 2010. URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing/at_download/fullReport (visited on 01/27/2014) (cit. on p. 153).
- [M89] Dutch Continuity Board. *How we work*. Website. 2018. URL: <https://www.dcboard.nl> (visited on 06/18/2018) (cit. on p. 154).
- [M90] Nederlandse Organisatie voor Wetenschappelijk Onderzoek | dcypher. *Column: A proactive and collaborative DDoS mitigation strategy*. Website. 2018. URL: <https://www.dcypher.nl/nl/node/11690> (visited on 06/18/2018) (cit. on p. 154).
- [M91] GÉANT. *GÉANT community working groups initiate DDoS focused security collaboration*. Website. 2015. URL: https://www.geant.org/News_and_Events/Pages/DDoS-focused_collaboration.aspx (visited on 06/18/2018) (cit. on p. 154).

RFCs

- [F1] Elisa Boschi et al. *IP Flow Information Export (IPFIX) Implementation Guidelines*. RFC 5153 (Informational). Internet Engineering Task Force, Apr. 2008. URL: <http://www.ietf.org/rfc/rfc5153.txt> (cit. on p. 27).

- [F2] Paul Ferguson and Daniel Senie. *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. RFC 2827 (Best Current Practice). Updated by RFC 3704. Internet Engineering Task Force, May 2000. URL: <http://www.ietf.org/rfc/rfc2827.txt> (cit. on p. 39).
- [F3] Rob Enns et al. *Network Configuration Protocol (NETCONF)*. RFC 6241 (Proposed Standard). Updated by RFC 7803. Internet Engineering Task Force, June 2011. URL: <http://www.ietf.org/rfc/rfc6241.txt> (cit. on p. 39).
- [F4] Pedro Marques et al. *Dissemination of Flow Specification Rules*. RFC 5575 (Proposed Standard). Updated by RFC 7674. Internet Engineering Task Force, Aug. 2009. URL: <http://www.ietf.org/rfc/rfc5575.txt> (cit. on p. 39).
- [F5] Toni Bates et al. *Multiprotocol Extensions for BGP-4*. RFC 4760 (Draft Standard). Updated by RFC 7606. Internet Engineering Task Force, Jan. 2007. URL: <http://www.ietf.org/rfc/rfc4760.txt> (cit. on p. 39).
- [F6] Jon Postel. *Internet Protocol*. RFC 791 (INTERNET STANDARD). Updated by RFCs 1349, 2474, 6864. Internet Engineering Task Force, July 1981. URL: <http://www.ietf.org/rfc/rfc791.txt> (cit. on p. 47).
- [F7] Roman Danyliw, Jan Meijer, and Yuri Demchenko. *The Incident Object Description Exchange Format*. RFC 5070 (Proposed Standard). Obsoleted by RFC 7970, updated by RFC 6685. Internet Engineering Task Force, Dec. 2007. URL: <http://www.ietf.org/rfc/rfc5070.txt> (cit. on pp. 49, 76).
- [F8] Herve Debar, David A. Curry, and Benjamin S. Feinstein. *The Intrusion Detection Message Exchange Format (IDMEF)*. RFC 4765 (Experimental). Internet Engineering Task Force, Mar. 2007. URL: <http://www.ietf.org/rfc/rfc4765.txt> (cit. on pp. 50, 76).
- [F9] Yakov Shafranovich, John R. Levine, and Murray S. Kucherawy. *An Extensible Format for Email Feedback Reports*. RFC 5965 (Proposed Standard). Updated by RFC 6650. Internet Engineering Task Force, Aug. 2010. URL: <http://www.ietf.org/rfc/rfc5965.txt> (cit. on p. 51).
- [F10] Chris Lonvick. *The BSD Syslog Protocol*. RFC 3164 (Informational). Obsoleted by RFC 5424. Internet Engineering Task Force, Aug. 2001. URL: <http://www.ietf.org/rfc/rfc3164.txt> (cit. on pp. 52, 55).
- [F11] Rainer Gerhards. *The Syslog Protocol*. RFC 5424 (Proposed Standard). Internet Engineering Task Force, Mar. 2009. URL: <http://www.ietf.org/rfc/rfc5424.txt> (cit. on p. 52).
- [F12] David B. Levi and Jürgen Schönwälder. *Definitions of Managed Objects for the Delegation of Management Scripts*. RFC 3165 (Proposed Standard). Internet Engineering Task Force, Aug. 2001. URL: <http://www.ietf.org/rfc/rfc3165.txt> (cit. on p. 52).
- [F13] Kathleen M. Moriarty. *Real-time Inter-network Defense (RID)*. RFC 6545 (Proposed Standard). Internet Engineering Task Force, Apr. 2012. URL: <http://www.ietf.org/rfc/rfc6545.txt> (cit. on pp. 53, 60).
- [F14] Brian Trammell. *Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS*. RFC 6546 (Proposed Standard). Internet Engineering Task Force, Apr. 2012. URL: <http://www.ietf.org/rfc/rfc6546.txt> (cit. on p. 53).
- [F15] Mark Wood and Michael A. Erlinger. *Intrusion Detection Message Exchange Requirements*. RFC 4766 (Informational). Internet Engineering Task Force, Mar. 2007. URL: <http://www.ietf.org/rfc/rfc4766.txt> (cit. on p. 54).

-
- [F16] Marshall T. Rose. *The Blocks Extensible Exchange Protocol Core*. RFC 3080 (Proposed Standard). Internet Engineering Task Force, Mar. 2001. URL: <http://www.ietf.org/rfc/rfc3080.txt> (cit. on p. 54).
- [F17] Benjamin S. Feinstein and Gregory A. Matthews. *The Intrusion Detection Exchange Protocol (IDXP)*. RFC 4767 (Experimental). Internet Engineering Task Force, Mar. 2007. URL: <http://www.ietf.org/rfc/rfc4767.txt> (cit. on p. 54).
- [F18] John C. Klensin. *Simple Mail Transfer Protocol*. RFC 5321 (Draft Standard). Updated by RFC 7504. Internet Engineering Task Force, Oct. 2008. URL: <http://www.ietf.org/rfc/rfc5321.txt> (cit. on p. 55).
- [F19] Ned Freed and Nathaniel S. Borenstein. *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*. RFC 2045 (Draft Standard). Updated by RFCs 2184, 2231, 5335, 6532. Internet Engineering Task Force, Nov. 1996. URL: <http://www.ietf.org/rfc/rfc2045.txt> (cit. on p. 55).
- [F20] Fuyou Miao, Yuzhi Ma, and Joseph Salowey. *Transport Layer Security (TLS) Transport Mapping for Syslog*. RFC 5425 (Proposed Standard). Internet Engineering Task Force, Mar. 2009. URL: <http://www.ietf.org/rfc/rfc5425.txt> (cit. on p. 55).
- [F21] Anton Okmianski. *Transmission of Syslog Messages over UDP*. RFC 5426 (Proposed Standard). Internet Engineering Task Force, Mar. 2009. URL: <http://www.ietf.org/rfc/rfc5426.txt> (cit. on p. 55).
- [F22] Russell Housley. *Cryptographic Message Syntax (CMS)*. RFC 5652 (INTERNET STANDARD). Internet Engineering Task Force, Sept. 2009. URL: <http://www.ietf.org/rfc/rfc5652.txt> (cit. on p. 65).

Theses

- [T1] Marc Kührer. “Large-scale analysis of network-based threats and potential counter-measures”. PhD thesis. Ruhr University Bochum, 2016. URL: <http://dblp.uni-trier.de/rec/bib/phd/de/Kuhrer16> (cit. on p. 3).
- [T2] Christopher Roy Strasburg. “A framework for cost-sensitive automated selection of intrusion response”. MA thesis. Iowa State University, 2009. URL: <http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1778&context=etd> (cit. on pp. 74, 87, 89, 94, 102).
- [T3] Fred Philip Stanley. “Intrusion detection and response for system and network attacks”. MA thesis. Iowa State University, 2009. URL: <http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1730&context=etd> (cit. on pp. 74, 89, 102).
- [T4] Tyrone W. A. Grandison. “Trust Management for Internet Applications”. PhD thesis. Imperial College of Science, Technology and Medicine University of London, 2003. URL: http://www.doc.ic.ac.uk/~tgrand/PhD_Thesis.pdf (cit. on p. 136).

Technical reports

- [R1] Darren Anstee et al. *Worldwide Infrastructure Security Report*. Tech. rep. XI. Arbor Networks Inc., Jan. 2015. URL: <http://www.arbornetworks.com/resources/annual-security-report> (cit. on pp. 3, 64, 129).

- [R2] Darren Anstee et al. *Worldwide Infrastructure Security Report*. Tech. rep. VII. Arbor Networks Inc., Jan. 2012, p. 96. URL: <http://www.arbornetworks.com/research/infrastructure-security-report> (cit. on pp. 27, 29).
- [R3] Darren Anstee et al. *Worldwide Infrastructure Security Report*. Tech. rep. IX. Arbor Networks Inc., Jan. 2013, p. 88. URL: <http://www.arbornetworks.com/research/infrastructure-security-report> (cit. on pp. 34 sq.).
- [R4] Open Networking Foundation. *Software-Defined Networking: The New Norm for Networks*. Tech. rep. Open Networking Foundation, Apr. 2012. URL: <https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf> (cit. on p. 117).

List of Figures

1.1	DDoS evolution is partially based on [J3]	2
1.2	Reflection and Amplification technique of DDoS	3
1.3	Increase of attack intensities over time based on [J3, M13, M14, M15]	4
1.4	Structure and dependence of chapters of the thesis	10
2.1	Geographic and business segment information of our participants: Survey 2013	23
2.2	Geographic and business segment information of our participants: Survey 2015	24
2.3	Risk assessment of threats	27
2.4	Data used for attack detection	28
2.5	Measures used to mitigate network attacks	30
2.6	Distribution of used exchange formats	31
2.7	Cooperation with third parties	32
2.8	Average number of attacks in relation to average traffic rate	34
2.9	Average security events in relation to average traffic rate and average true positives of reported security events	36
2.10	Cloud-based services	38
2.11	Sharing threat indicators or security events/incidents with several entities	40
2.12	Distribution of exchange protocols and formats	42
3.1	Application domains of exchange formats based on [M41]	47
3.2	Classification of the exchange formats	58
3.3	Classification of the exchange protocols	60
3.4	Components of a FLEX message	65
4.1	Exchanging FLEX messages among trusted partners.	74
4.2	Data flow of the communication process within MiR from the perspective of one ISP	77
4.3	A semantic representation of the DeterLab testbed	81
4.4	Simulation results of the attack traffic (red line) and cumulative traffic (black line)	82
5.1	Simplified network topology of a IDS in promiscuous mode	86
5.2	Simplified network topology of a IDS in inline mode (IPS)	87

LIST OF FIGURES

5.3	Dependency tree between the two users Anne and Customer of IE-IRS [C35]	90
5.4	A sample attack graph of ADEPTS [C36]	92
5.5	Response selection process	95
5.6	The reaction strategy aligned with the NIST incident response cycle . .	97
5.7	Simplified view of the REASSESS testbed	100
5.8	Overview of the components of the REASSESS application	101
5.9	Testbed for REASSESS application	102
6.1	A semantic representation of the testbed	120
6.2	Qualitative evaluation results	123
6.3	Transition model of attacker x_1 and x_2	125
7.1	Origin of security events	135
7.2	Trust level calculation of MiRTrust	139
7.3	Distribution of trust levels	144
7.4	Asymmetric trust level	145
8.1	Research results based on the survey research described Chapter 2 (Current DDoS Detection & Mitigation: A Survey)	149

List of Tables

2.1	Overview of mailing lists	18
2.2	Overview of the survey 2013	19
2.3	Overview of the survey 2015	20
2.4	Overview of the market segment and frequency of the second survey .	22
2.5	Overview of the compliance to common standards	25
2.6	Overview of event exchange formats	30
3.1	Overview of exchange protocols and formats	49
3.2	Evaluation summary of the exchange formats	57
3.3	Evaluation summary of the exchange protocols	63
5.1	Measured runtimes for different amount of alerts.	102
5.2	Calculations within the response selection process.	103
5.3	Evaluation summary of the response selection models.	111
6.1	Overall probability P_D of a successful DDoS attack of 8 configuration states s	130

Index

A

Access Control List	<i>see</i> ACL
ACL	29
ADAC	136
Amplification	2
APWG	136
ARF	51, 64
ASN.1	65
Attack Detection	
DPI	<i>see</i> DPI
IDS	<i>see</i> IDS
IPFIX	<i>see</i> IPFIX
NetFlow	<i>see</i> NetFlow
sFlow	<i>see</i> sFlow
SIEM	<i>see</i> SIEM
SNMP	<i>see</i> SNMP
Attack Mitigation	
ACL	<i>see</i> ACL
DRTBH	<i>see</i> DRTBH
Firewall	<i>see</i> Firewall
IPS	<i>see</i> IPS
IRS	<i>see</i> IRS
SRTBH	<i>see</i> SRTBH

B

BCP 38	39
BEEP	54, 76
BGP FlowSpec	39
Blacklist	37

C

CAIF	49
CEE	50

CERT	29
Chatham House Rules	137
CIDF	48
Cloudflare	33, 39
CLT	54
COBIT	25
Collaboration Communities	136
ACDC	<i>see</i> ACDC
ADAC	<i>see</i> ADAC
APWG	<i>see</i> APWG
DOTS	<i>see</i> DOTS
FIRST	<i>see</i> FIRST
M ³ AAWG	<i>see</i> M ³ AAWG
SIG-NOC	<i>see</i> SIG-NOC
TF-CSIRT	<i>see</i> TF-CSIRT
Computer Emergency Response Team	
CERT	29
Computer Security Incident Response Team	
CSIRT	33
Control Objectives for Information and Related Technology	<i>see</i> COBIT
CSIRT	33

D

DDoS	
Amplification	<i>see</i> Amplification
Reflection	<i>see</i> Reflection
DDoS Protection Service	
Cloudflare	<i>see</i> Cloudflare
Incapsula	<i>see</i> Incapsula
Deep Packet Inspection	<i>see</i> DPI
Destination-based Remote-Triggered Blackhole	<i>see</i> DRTBH
DeterLab	80
DNSWL	38
DOTS	136
DPI	28
DRTBH	29

E

Exchange format 47
 ARF *see* ARF
 CAIF *see* CAIF
 CEE *see* CEE
 CIDF *see* CIDF
 FLEX *see* FLEX
 IDMEF *see* IDMEF
 IODEF *see* IODEF
 STIX *see* STIX
 Syslog *see* Syslog
 X-ARF *see* X-ARF
 Exchange protocol 47
 BEEP *see* BEEP
 CLT *see* CLT
 IAP *see* IAP
 IDXP *see* IDXP
 RID *see* RID
 SCAP *see* SCAP
 SMTP *see* SMTP
 TAXII *see* TAXII
 XMPP *see* XMPP

F

Firewall 29
 FIRST 136
 FLEX 64, 71, 77, 143

G

GnuPG 137
 Greylists 37

I

IAP 54
 IDMEF 50, 64, 76
 IDS 35
 IDXP 41, 54, 76
 Incapsula 39
 Information Technology Infrastructure Library *see* ITIL
 Intrusion Detection System *see* IDS
 Intrusion Prevention System *see* IPS
 Intrusion Response System *see* IRS
 IODEF 42, 48, 64, 76

IPFIX 27, 28
 IPS 29
 IRS 85
 ISO/IEC 27000 25
 ITIL 25

M

M³AAWG 51, 136
 Moving Target Defense *see* MTD
 MTD 117

N

Netconf 39
 NetFlow 15, 27
 NIST 41

O

ONOS 122
 OpenFlow 39, 117
 OpenPGP 137

P

PGP 137

R

Reflection 2
 Research questions 6
 RID 53
 RIPE 37

S

SCAP 41
 SDN 117
 SDX 119
 Security Information and Event Management *see* SIEM
 sFlow 27
 Shadowserver 37
 SIEM 35

SIG-NOC 136
 SMTP 55
 SNMP 28
 Software Defined Networking
 ONOS.....*see* ONOS
 OpenFlow.....*see* OpenFlow
 SDN*see* SDN
 SDX.....*see* SDX
 Source-based Remote-Triggered Blackhole...*see*
 SRTBH
 Spamcop 38
 Spamhaus 38
 SRTBH.....29
 STIX.....75
 STOMP 72, 77
 Survey research 6, 16
 Nonresponse Bias 20
 Questionnaire Design.....18
 Results21
 Sample.....17, 21
 Syslog 52

T

TAXII 75
 TF-CSIRT 136
 TLP.....144

W

Web of Trust 137
 Whitelist.....37

X

X-ARF 31, 51, 64, 76
 XMPP 54

Curriculum Vitae of the Author

Jessica Steinberger was born in Mainz, Germany in 1983. After finishing her school-based education, she started an apprenticeship at the AKZO NOBEL's subsidiary Intervet Innovation GmbH (currently operating name is Merck Animal Health (MSD Animal Health outside the USA and Canada)). MSD Animal Health Innovation is an international research and development company of vaccines, anti-infective and anti-parasitic drugs in the area of animal health. After finishing her apprenticeship, she worked at the Service Desk of MSD Animal Health Innovation as an Information System Service Officer and delivered a comprehensive and professional IT support service for researchers and veterinaries located in Schwabenheim an der Selz.

She received her Bachelor of Science (B.Sc.) degree in Computer Science in 2009 and her Master of Science (M.Sc.) in 2011 from the University of Applied Sciences Bingen (TH Bingen). In 2011, she joined the Biometrics and Internet-Security research group da/sec in Darmstadt. She was responsible to conceptualize, implement and evaluate an infrastructure to support a collaboration of Internet service providers to successfully combat network-based attacks in context of high-speed networks of the German Federal Ministry of Education and Research supported project *innovative Anomaly- and Intrusion-Detection (iAID)*. In 2014, she initiated a cooperation with the University Twente in the research area flow-based attack detection and mitigation to accomplish her PhD thesis. Therefore, she joined the Design and Analysis of Communication Systems (DACs) group as an external PhD student to work with Prof. dr. ir. Aiko Pras and Dr. Anna Sperotto.

Publications by the author

- Jessica Steinberger et al. “DDoS Defense using MTD and SDN”. In: *Proceedings of the 2018 IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*. May 2018. DOI: [10.1109/INM.2015.7140407](https://doi.org/10.1109/INM.2015.7140407) (cit. on pp. 12, 115).
- Aiko Pras et al. “DDoS 3.0 - How Terrorists Bring Down the Internet”. In: *Measurement, Modelling and Evaluation of Dependable Computer and Communication Systems: 18th International GI/ITG Conference, MMB & DFT 2016, Münster, Germany, April 4-6, 2016, Proceedings*. Ed. by Anne Remke and R. Boudewijn Haverkort. Cham: Springer International Publishing, Nov. 2016, pp. 1–4. ISBN: 978-3-319-31559-1. DOI: [10.1007/978-3-319-31559-1_1](https://doi.org/10.1007/978-3-319-31559-1_1). URL: http://dx.doi.org/10.1007/978-3-319-31559-1_1 (cit. on p. 5).
- Jessica Steinberger et al. “Collaborative DDoS Defense using Flow-based Security Event Information”. In: *Proceedings of the 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS 2016)*. Apr. 2016. DOI: [10.1109/NOMS.2016.7502852](https://doi.org/10.1109/NOMS.2016.7502852) (cit. on pp. 11, 71, 116, 118).
- Jessica Steinberger et al. “In Whom Do We Trust - Sharing Security Events”. In: *Management and Security in the Age of Hyperconnectivity: 10th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2016, Munich, Germany, June 20-23, 2016, Proceedings*. Ed. by Rémi Badonnel et al. Cham: Springer International Publishing, 2016, pp. 111–124. ISBN: 978-3-319-39814-3. DOI: [10.1007/978-3-319-39814-3_11](https://doi.org/10.1007/978-3-319-39814-3_11). URL: http://dx.doi.org/10.1007/978-3-319-39814-3_11 (cit. on pp. 12, 125 sq., 128, 133, 140).
- Jessica Steinberger et al. ““Ludo” - Kids playing Distributed Denial of Service”. In: *Connected Communities, The Networking Conference 2016, 15-18 June, 2016, Prague, Czech Republic, Selected Papers*. Ed. by Klaas Wierenga. GÉANT Ltd, Nov. 2016. ISBN: 978-90-77559-25-3. URL: <http://www.terena.org/publications/tnc16-proceedings/> (cit. on pp. 10, 12, 85).
- Sven Ossenbühl, Jessica Steinberger, and Harald Baier. “Towards Automated Incident Handling: How to Select an Appropriate Response against a Network-Based Attack?” In: *Proceedings of the Ninth International Conference on IT Security Incident Management IT Forensics (IMF)*. May 2015, pp. 51–67. DOI: [10.1109/IMF.2015.13](https://doi.org/10.1109/IMF.2015.13) (cit. on pp. 12, 85).
- Jessica Steinberger. *FLEX*. Website. July 2015. URL: <https://datatracker.ietf.org/meeting/93/materials/agenda-93-mile/> (visited on 12/12/2017) (cit. on pp. 11, 45, 153).
- Jessica Steinberger et al. “Collaborative Attack Mitigation and Response: A survey”. In: *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM 2015)*. May 2015. DOI: [10.1109/INM.2015.7140407](https://doi.org/10.1109/INM.2015.7140407) (cit. on pp. 11, 15, 74, 116, 121, 124, 131, 143).

- Jessica Steinberger et al. *Exchanging Security Events of flow-based Intrusion Detection Systems at Internet Scale*. Website. June 2015. URL: https://www.iab.org/wp-content/IAB-uploads/2015/04/CARIS_2015_submission_3.pdf (visited on 12/28/2015) (cit. on pp. 11, 45, 71, 77, 152).
- Jessica Steinberger et al. “How to exchange security events? Overview and evaluation of formats and protocols”. In: *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. May 2015, pp. 261–269. DOI: [10.1109/INM.2015.7140300](https://doi.org/10.1109/INM.2015.7140300) (cit. on pp. 11, 45, 64, 76).
- Jessica Steinberger et al. “Real-time DDoS Defense: A collaborative Approach at Internet Scale”. In: *Proceedings of the 10th SPRING of the SIG Security - Intrusion Detection and Response of the German Informatics Society SIG SIDAR*. July 2015. URL: <http://www.gi-fg-sidar.de/spring/SIDAR-Reports/SIDAR-Report-SR-2015-01.pdf> (cit. on p. 9).
- Jessica Steinberger et al. *Real-time DDoS Defense: A collaborative Approach at Internet Scale*. Website. **Best Student Poster**. May 2014. URL: <https://tnc2014.terena.org/core/poster/21> (visited on 06/10/2018) (cit. on p. 9).
- Jessica Steinberger et al. “Anomaly Detection and Mitigation at Internet Scale: A Survey”. In: *Proceedings of the 7th IFIP International Conference on Autonomous Infrastructure, Management and Security (AIMS 2013): Emerging Management Mechanisms for the Future Internet*. Ed. by Guillaume Doyen et al. Vol. 7943. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, pp. 49–60. ISBN: 978-3-642-38997-9. DOI: [10.1007/978-3-642-38998-6_7](https://doi.org/10.1007/978-3-642-38998-6_7). URL: http://dx.doi.org/10.1007/978-3-642-38998-6_7 (cit. on pp. 10, 15, 41, 46, 64, 71 sq.).