CrossMark

REPORT

Report on the 10th International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2016)

Management and Security in the Age of Hyperconnectivity

Remi Badonnel[1] · Robert Koch[2] · Martin Drasar[3] · Aiko Pras[4] · Volker Eiseler[2] · Lars Stiemert[2] · Sebastian Seeber[2] · Daphne Tuncer[5] · Marinos Charalambides[5] · Gabi Dreo Rodosek[2]

Abstract This article is a report of the IFIP AIMS 2016, which was held at Universität der Bundeswehr München, Germany from June 20 to June 23, 2016. AIMS 2016 focused on the theme "Management and Security in the Age of Hyperconnectivity". The AIMS conference positions itself in the network management community as an educational venue for young researchers and Ph.D. students. The AIMS program included keynotes, technical sessions and Ph.D. Workshop sessions, but also hands-on labs and an educational panel for training

✉ Remi Badonnel
badonnel@loria.fr

Robert Koch
robert.koch@unibw.de

Martin Drasar
drasar@ics.muni.cz

Aiko Pras
a.pras@utwente.nl

Volker Eiseler
volker.eiseler@unibw.de

Lars Stiemert
lars.stiemert@unibw.de

Sebastian Seeber
sebastian.seeber@unibw.de

Daphne Tuncer
d.tuncer@ucl.ac.uk

Marinos Charalambides
marinos.charalambides@ucl.ac.uk

Gabi Dreo Rodosek
gabi.dreo@unibw.de

young academics. The highlights on each of the parts of the AIMS 2016 program are summarized in this article.

1 Introduction

The 10th International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2016) was held at Universität der Bundeswehr München, Germany from June 20 to June 23, 2016 [1]. The 4-day AIMS 2016 conference was a single-track event integrating hands-on lab sessions, keynotes, an educational panel, technical paper sessions, and a Ph.D. student workshop into a highly interactive event. AIMS 2016 focused on management and security in the age of hyperconnectivity. This theme was addressed in the technical program with papers related to monitoring, configuration, security in multiple application areas from connected objects to cloud infrastructures and next-generation services. AIMS 2016 was co-sponsored by the IFIP WG 6.6 [2] and European FP7 NoE "FLAMINGO" (No. 318488) [3].

2 Hands-On Lab Sessions

The AIMS 2016 program contained two hands-on lab sessions on timely topics in the area of network and service management. The labs offered a balanced mix of theoretical background information and practical exercises. Between 15 and 25 participants attended every hands-on lab.

1 Telecom Nancy, University of Lorraine, LORIA - INRIA, Campus Scientifique, 54600 Villers Lès Nancy, France

2 Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, 85579 Neubiberg, Germany

3 Institute of Computer Science, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic

4 Faculty for Electrical Engineering, Mathematics, and Computer Science, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands

5 Department of Electronic and Electrical Engineering, University College London, Torrington Place, London WC1E 7JE, UK

The first lab session, dedicated to Big Data Analysis for DNS,[1] was delivered by Mattijs Jonker (University of Twente, The Netherlands) and Christian Dietz (Universität der Bundeswehr München, Germany). The presenters provided the participants with a general introduction to the DNS measurement including a few example use cases, and introduced them to a virtualized lab environment in which they can experiment with the data themselves. This big data environment, hosted by the University of Twente, consisted of 14 Hadoop nodes, to which the participants were granted remote access to. A Jupyter notebook was prepared for each participant, which contained examples for interfacing the Hadoop cluster with Python via Ibis and Impala. Impala provides an SQL[2] like syntax for querying information from big datasets, and includes background caching and query optimization technologies. Furthermore, the lab environment contained one month of real data captures for the Alexa Top 1 Million domains. These captures were made on the root level of DNS by using an active-passive measurement environment. The participants learned how to formulate queries to derive the relevant information, post process it with python and display it in an interactive Notebook with python and matplotlib.

The second lab session, related to Flow-based Traffic Mining, was presented by Stefan Burschka and Benoit Dupasquier (RUAG, Switzerland). The participants played the role of analysts trying to find anomalies in real IP traffic. In particular, they experimented Tranalyzer, a lightweight flow generator and packet analyzer. It provides an extension of the Cisco NetFlow functionality and helps analysists in processing ultra large packet dumps. It supports the drill down process to the very flow of interest, which can then be analyzed in depth by regular tools such as tcpdump, wireshark, or by its inbuild text based packet mode. Tranalyzer provides functionality to analyze and generate key parameters and statistics from IP traces either being live-captured from ethernet interfaces or pcap files.

These hands-on labs have highlighted the benefits of analytics methods for addressing the large volume and velocity of datasets generated by networks and services. The MapReduce big data architectural pattern enables to distribute and bring a processing close to data (instead of requiring their migration), while filtering and flow-based approaches permit to minimize the quantity of collected data. These methods provide a large variety of usage in network and service management, from security detection [4] to troubleshooting [5], and may also be supported by management techniques, such as in [6].

3 Keynotes

The conference also included two keynote sessions related to cyber security.

The first session, entitled "Today's Cyber Security Threats and Challenges for Telco Providers" was given by Dr. Bernd Eßer, head of the Deutsche Telekoms Cyber Defense Center and member of the board of the German CERT association.

---

[1] Domain Name System.

[2] Structured Query Language.

His keynote presented the threat landscape and its evolution as seen from a Tier-1 operator's perspective, and gave some strategic and operational options to manage security attacks. The recommendations focused on the application of a risk-based preventive approach to threats, complemented by capabilities to react (damage control techniques) and to detect incidents (early detection methods). The talk also highlighted the limits of security standards, that should further take into account the complexity of current infrastructures, as well as the capabilities of new attackers that are highly skilled, resourceful and motivated. It concluded with the growing role of telecommunication operators with respect to cyber security. Through the variety of their activities, they become privileged points of contact to perform holistic security management, and to share security information through their cyber defense centers.

The second session, entitled "Cyber Resilience of Complex Interdependent Infrastructures" was given by Dr. Tobias Kiesling (IABG), a Program Manager for Cyber Defense at IABG. His keynote addressed the huge challenge of understanding and addressing risks induced by critical infrastructures that we utilize in our daily life. These infrastructures are quite complex and interdependent on one another. It focused on the case of air traffic systems at large, seen as an attractive target for cyber attacks due to its importance and prominence. The current system is already vulnerable and the advent of more automation and pervasion of standard IT in the wake of future approaches leads to ever more complex and interconnected systems with an increasing attack surface. To cope with this situation, the talk argued in favor of a resilience-oriented view and the usage of suitable methods and tools to achieve understanding of the consequences in potential cyber threat situations.

For additional information on the keynote speakers and accessing their presentation, we point the reader to the AIMS 2016 website [1]. Note that cyber defense also relies on the development of dedicated training/educational programs (that can be provided online) to increase the security awareness of users.

4 Educational Panel

Massive Open Online Courses (MOOCs) are open access and scalable online higher education courses. They have been gaining increasing popularity in recent years mainly due to their extended outreach and lack of entry requirements as well as tuition fees. Given their initial success and the interest from the higher education community, they have the potential of becoming an essential part of the education system. However, due to their online nature, they do not follow the traditional teaching paradigm that requires classroom presence and direct interactions.

A panel session on Experiences with MOOCs was organized and moderated by Daphne Tuncer and Marinos Charalambides (University College London) and gathered four Ph.D. researchers working in the area of Network and Service Management who shared their experience of using MOOCs with the audience and debated possible changes in current practices to make learning more effective: Jessica Steinberger from Hochschule Darmstadt (Germany) and University of Twente (The Netherlands), Wouter de Vries from University of Twente (The

Netherlands), Sebastian Seeber from Universität der Bundeswehr München (Germany) and Gioacchino Tangari from University College London (UK).

Discussions were focused on MOOC structure and position with respect to course integration, interactions with other students/instructor, MOOC format, course customisation, grading systems. The panel was a positive experience, with both the panellists and the audience actively involved in the debate. In particular, it pointed out: (1) the importance of organizing MOOCs in short sequences enabling learners to easily stop and continue lessons, (2) the need for efficient dashboards and indicators for evaluating learner progressions, and (3) the development of cloud-based solutions for virtual practical exercises.

5 Technical Paper Sessions

The three technical sessions of AIMS 2016—covering "Autonomic and Smart Management", "Methods for Management and Security", and finally, "Security Attacks and Defenses"—included 7 full papers, which were selected after a thorough reviewing process out of a total of 22 submissions. All papers received at least three independent reviews. A significant part of the submissions targeted security aspects of emerging networks and services, as shown in the technical program and emphasized by the two keynote speeches.

The already established tradition of an unsually vivid and interactive conference series has been confirmed with an important richness and variety of papers. The program included papers with a high technical expertise, such as "Analysis and Evaluation of OpenFlow Message Usage for Security Applications" by Sebastian Seeber [7], which describes mitigation and defense mechanisms that are currently used in SDN[3] environments, analyzes their dependencies with respect to OpenFlow messages, and quantifies their performances with different implementations. It also covered papers related to high level methodologies, such as "In Whom Do We Trust—Sharing Security Events" by Jessica Steinberger [8], which specifies a trust model for security events in order to deploy semi-automated remediations and facilitate the dissemination of security event information, using the exchange format FLEX[4] in the context of ISPs.[5]

The best paper award went to "Cloud Flat Rates Enabled via Fair Multi-resource Consumption" by Patrick Poullie and Burkhard Stiller (University of Zürich—Switzerland) [9], which proposes a fair multi-resource cloud sharing approach, and shows its enforcement to enable cloud flat rates. Based on a questionnaire among more than 600 individuals, a new Greediness Metric (GM) was designed, which formalizes an intuitive understanding of multi-resource fairness without access to consumers' utility functions. By simulating the GM's application to adapt resource allocations of cloud hosts, it was shown how fairness between cloud customers can be achieved, and thereby attractive cloud flat rates be offered.

---

[3] Software-Defined Networking.

[4] Flow-based Event Exchange Format.

[5] Internet Service Providers.

The conference proceedings [10] include the papers presented at AIMS 2016 and the overall final program. The proceedings demonstrate again the European scope of this conference series since most of accepted papers are from European research groups.

6 Ph.D. Workshop

The Ph.D. workshop is a venue for early-stage doctoral students to present and to discuss their research ideas and, more importantly, to obtain valuable feedback from the AIMS audience about their planned Ph.D. research work. A total of 9 Ph.D. papers and 2 Ph.D. short papers were selected for presentation, out of 21 submissions, after a rigorous review process that provided at least 3 independent reviews for each paper. The workshop was structured into two technical sessions.

The first session on management of future networks featured four papers, and the accompanying short paper session on the same topic featured another two. While each paper focused on a different topic, two main themes emerged—ensuring reliability of next-generation virtualized networks and a proliferation of future networking technologies to different areas of human endeavour. New approaches to network monitoring, QoS and SLA[6] maintenance, and 5G efficiency were discussed. Also, applications of networking in the electric grid environment and intra-vehicular communication were explored.

The second session on security management covered a large number of topics in just five presented papers. It started with a game-theoretic approach to modelling attacker-attacked interaction, was followed by evaluation of entities' reputation, continued with detection methods for advanced attacks and botnets, and concluded with practical approach to DDoS[7] mitigation. The diversity of presented papers highlighted how interwoven the security is into the current and future networking.

7 Evaluation and Conclusions

Beyond the richness of technical sessions, AIMS 2016 conference has pursued several complementary activities dedicated to the academic training of young researchers and Ph.D. students. Since AIMS 2013, the organization committee and the steering committee have worked together to better define AIMS' DNA and its position within the network and service management community [11]. In that context, this year edition included an educational panel dedicated to MOOCs, and two hands-on lab sessions. The feedback on these activities was again very positive, with interactive discussions during the educational panel, and a high attendance to the labs. As previously mentioned, the authors of the second hands-on lab even proposed one additional third open-end session on the last conference day. AIMS 2016 conference was attended by 45 people, a number that conforms with the trend

---

[6] Service-Level Agreement.

[7] Distributed Denial of Service.

for the previous editions [12]. The majority of the attendees came from universities and research centers within Europe. We achieved highly interactive discussions in a relaxed environment. The event confirmed one of the key goals of AIMS to provide young researchers and Ph.D. students with a constructive feedback by senior scientists and give them the possibility of growing in the research community.

References

1. IFIP AIMS 2016 Conference Web Site. http://www.aims-conference.org/2016/. Accessed July 2016
2. IFIP TC6 Working Group 6: Management of Networks and Distributed Systems. http://www.simpleweb.org/ifip/. Accessed July 2016
3. Flamingo European (ICT-FP7) Network of Excellence. http://www.fp7-flamingo.eu/. Accessed July 2016
4. Sperotto, A., van der Toorn, O., van Rijswijk-Deij, R.: TIDE: threat identification using active DNS measurements. In: Proceedings of the SIGCOMM Posters and Demos (SIGCOMM 2017), pp. 65–67 (2017)
5. Liotta, A., Di Fatta, G.: Special issue on data mining for monitoring and managing systems and networks. J. Netw. Syst. Manag. **22**(2) (2014)
6. Zhao, S., Medhi, D.: Application-aware network design for hadoop mapreduce optimization using software-defined networking. IEEE Trans. Netw. Serv. Manag. **14**(4), 804–816 (2017)
7. Seeber S., Dreo Rodosek G., Hurel G., Badonnel R.: Analysis and evaluation of OpenFlow message usage for security applications. In: Proceedings of the 10th IFIP International Conference on Autonomous Infrastructure, Management and Security (AIMS), June 2016, Munich, Germany. Lecture Notes in Computer Science, LNCS 9701. Springer International Publishing (2016)
8. Steinberger J., Kuhnert B., Sperotto A., Baier H., Pras A.: In whom do we trust—sharing security events. In: Proceedings of the 10th IFIP International Conference on Autonomous Infrastructure, Management and Security (AIMS), June 2016, Munich, Germany. Lecture Notes in Computer Science, LNCS 9701. Springer International Publishing (2016)
9. Poullie O., Stiller B.: Cloud flat rates enabled via fair multi-resource consumption. In: Proceedings of the 10th IFIP International Conference on Autonomous Infrastructure, Management and Security (AIMS), June 2016, Munich, Germany. Lecture Notes in Computer Science, LNCS 9701. Springer International Publishing (2016)
10. Badonnel, R., Koch, R., Pras, A., Drasar, M., Stiller, B. (eds.): Proceedings of the 10th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2016)—Management and Security in the Age of Hyperconnectivity. Lecture Notes in Computer Science (LNCS), vol. 9701. Springer (2016)
11. Sperotto, A., Doyen, G., Latre, S., Charalambides, M., Famaey, J., Velan, P., Celeda, P.: Report on the 8th international conference on autonomous infrastructure, management, and security (AIMS 2014): monitoring and securing virtualized networks and services. J. Netw. Syst. Manag. **23**(3), 794–802 (2015)
12. Almeroth, K.: Networking Conferences Statistics. http://www.cs.ucsb.edu/~almeroth/conf/stats/#aims. Accessed July 2016

Remi Badonnel is an Associate Professor of Computer Science with the TELECOM Nancy Engineering School, University of Lorraine, France. He is a Permanent Research Staff Member within the MADYNES Team, LORIA–INRIA Nancy Grand Est, France. He worked on change management methods and algorithms for data centers with IBM T. J. Watson, USA and on autonomous smart systems with the University College of Oslo, Norway. His research interests are mainly focused on network and service management, smart and autonomic environments, security and defense techniques, orchestration and chaining of services, cloud infrastructures, and Internet of Things.

Robert Koch is an IT Staff Officer of the Federal Armed Forces and a research assistant in the Department of Computer Science at Universität der Bundeswehr München and member of the university's Research Institute for Cyber Defense (CODE). He received his Ph.D. in 2011 and is now a senior research assistant and lecturer for Computer Science. His main areas of research are network and system security with focus on intrusion and extrusion detection in encrypted networks, security of COTS products, security visualization and the application of artificial intelligence. He has several years of experience in the operation of high security networks and systems. His research papers were published in various international conferences and journals. Additionally, he serves as program chair and member of the technical program chair for numerous conferences.

Martin Drasar is a Security Researcher at Masaryk University, Czech Republic and a head of the Proactive Security Group at the accredited security team CSIRT-MU. Martin has received his Ph.D. on the topic of behavioral detection of distributed dictionary attacks and is currently focusing on the topic of adaptable attack strategies for large-scale attacks and on general usage of machine learning in network security.

Aiko Pras is Professor in the area of Network Operations and Management at the University of Twente, the Netherlands and member of the Design and Analysis of Communication Systems Group. He received a Ph.D. degree for his thesis titled "Network Management Architectures". His research interests include network management technologies, network monitoring, measurements and security. He is chairing the IFIP Technical Committee on "Communications Systems", and is Coordinator of the European Network of Excellence on "Management of the Future Internet" (FLAMINGO). He is steering committee member of several conferences, including IM/NOMS and CNSM, and series/associate editor of ComMag, IJNM and TNSM.

Volker Eiseler studied Computer Sciences at the Technical University of Munich an received his diploma in 2007. Since 2007 he worked as a Research Assistant at the Univerität der Bundeswehr München. Since 2014 he is also a Ph.D. student at Chair of Prof. Gabi Dreo. His research fields are network security and security of computing centers (security visualization). Since 2017 Volker Eiseler is the Manager of the new Research Institute CODE (Cyber Defense and Smart Data) at the Universität der Bundeswehr München.

Lars Stiemert is a Research Assistant at the Universität der Bundeswehr München, since 2013. His main fields of interest are geolocation, traffic analysis and IT security. He is well educated in system and network administration and has several years of experience in running operational networks.

Sebastian Seeber is a Ph.D. Candidate at the Chair for Communication Systems and Network Security at the Universität der Bundeswehr München, pursuing his Ph.D. in the area of IT security aspects and of software defined networking. Previously he worked as IT manager at Leipzig Trade Fair taking care of network security, wifi deployment, virtualization technology and customer support. He holds a M.Sc. in Computer Science (2011) from the Faculty of Mathematics, Science and Computer Science of the Hochschule Mittweida, University of Applied Sciences, Germany. He also holds a B.Sc. in Computer Science (2009) from the same university.

Daphne Tuncer is a Research Associate in the Communications and Information Systems Group, Electronic and Electrical Engineering Department, University College London (UCL), UK. She obtained her Ph.D. in Electronic and Electrical Engineering from UCL in November 2013. Before joining UCL, she received a "Diplome d'ingenieur de Telecom SudParis", France, in 2009. Her research interests are in the area of software-defined networks, cache/content management and more generally in distributed and adaptive resource management.

Marinos Charalambides is a Senior Researcher at the Department of Electronic and Electrical Engineering, UCL. He received a B.E. (First Class Hons.) in Electronic and Electrical Engineering, an M.Sc. (Distinction) in Communications Networks and Software, and a Ph.D. in Policy-based Management, all from the University of Surrey, UK, in 2001, 2002 and 2009, respectively. He has been working on a number of European and UK national projects since 2005 and his research interests include network programmability, content distribution, network monitoring, and online traffic engineering. He has been the technical program chair of several conferences and in 2016 he received the Young Professional Award for "outstanding research contributions and leadership in the field of network and service management".

Gabi Dreo Rodosek studied computer science at the University of Maribor, Slovenia. She obtained her Ph.D. and habilitation degree from the Ludwig Maximilians University in Munich in 1995 and 2002, respectively. Since 2004 she holds the Chair for Communication Systems and Network Security at the Universität der Bundeswehr München. Since 2017 she is the Leading Director of the Research Institute CODE (Cyber Defense and Smart Data) at the Universität der Bundeswehr München. She is member of the Supervisory and Advisory Board of Giesecke and Devrient GmbH, member of the Supervisory and Advisory Board of BWI IT GmbH and BWI Systeme GmbH, and member of the Governing Board of the German Research Network (DFN). Furthermore she is member of the Editorial Advisory Board of the International Journal of Network Management, and of several other national and international advisory councils and committees. She was member of the Executive Committee of the EU NoE Project FLAMINGO.