Estimating Impact and Frequency of Risks to Safety and Mission Critical Systems Using CVSS

Siv Hilde Houmb[1], Virginia N. L. Franqueira[1] and Erlend A. Engum[2]
[1]*University of Twente, The Netherlands*
{s.h.houmb, franqueirav} (at) ewi.utwente.nl
[2]*iTexion, The Netherlands*
E.Engum (at) itexion.nl

Abstract

Many safety and mission critical systems depend on the correct and secure operation of both supportive and core software systems. E.g., both the safety of personnel and the effective execution of core missions on an oil platform depend on the correct recording storing, transfer and interpretation of data, such as that for the Logging While Drilling (LWD) and Measurement While Drilling (MWD) subsystems. Here, data is recorded on site, packaged and then transferred to an on-shore operational centre. Today, the data is transferred on dedicated communication channels to ensure a secure and safe transfer, free from deliberately and accidental faults.

However, as the cost control is ever more important some of the transfer will be over remotely accessible infrastructure in the future. Thus, communication will be prone to known security vulnerabilities exploitable by outsiders. This paper presents a model that estimates risk level of known vulnerabilities as a combination of frequency and impact estimates derived from the Common Vulnerability Scoring System (CVSS). The model is implemented as a Bayesian Belief Network (BBN).

1. Introduction

Safety and mission critical systems need to ensure both the safety of personnel and the profitable execution of their core missions. These systems are relying on software systems both in their core mission and in supportive tasks, such as Logging While Drilling (LWD) and Measurement While Drilling (MWD) support subsystems to offshore oil installations. Log files are large and complex and requires experts for a correct and safe assessment. However, increasing cost demands makes it non-profitable to have the necessary expertise on-site. Experts are therefore moved to on-shore operational support centres. This means that log data are recorded and packaged offshore and transferred to other, sometimes multiple, locations on-shore. For data to be correctly processed it is crucial that all steps involved are executed in a secure and safe manner free from deliberately and accidental fault introduction. Due to this, data is usually transferred on dedicated communication channels either owned by the oil or service company themselves or leased from trusted third parties. As dedicated communication links are expensive and as cost control is ever more important it is likely that some of the data transfer will be over infrastructure that is remotely accessible. This increases the risks of intentionally and accidentally fault introduction.

Executing mission (including safety missions) and ensuring sustainable profit is both important, although maybe not always equally important. This involves trade-offs and the trade-offs relevant for LWD and MWD subsystems is whether it is reasonably safe to use less expensive communication infrastructure. In this paper, we assume the use of remotely accessibility communication infrastructure prone to inherent or accidental fault introduction of known vulnerabilities and show how to use existing experience data to estimate the frequency of potential fault introduction and the magnitude of impact that these may have. In particular, we use the Common Vulnerability Scoring System (CVSS) and the paper describes a model developed to estimate risk level from frequency and impact estimates derived using CVSS data. The model is implemented as a BBN to allow for multiple frequency and impact estimation sources and to allow for combining CVSS [3,14] with expert opinions; that is, supporting disparate information sources.

The paper is structured as following. Section 2 points to related work on controlling security risks to place the paper into context. Section 3 introduces the risk level estimation model. Section 4 discusses CVSS and Section 5 discusses how to use CVSS as an information source for frequency and impact estimation. Section 5 also introduces the concept of BBN and discusses the risk level estimation model BBN. Section 6 gives an example, while Section 7 summarises the main contributions of the paper and points to future work.

2. Related work

Our work is mainly related to controlling security risks and in particular quantifying security risks; that is, quantitative risk analysis. The current strategies for controlling security risks are: (i) penetration and patch, (ii) standards, (iii) risk management/assessment and (iv) “wait and see” approaches. The latter is similar to the first, only different in the fact that penetration and patch often includes authorised penetration and patch activities such as tiger-team activity. ``Wait and see'' is a passive security strategy where problems are fixed only after the fact and if budget allows.

Standards provide tools for evaluating the security and safety controls of systems. Examples of such are ISO 15408:2007 Common Criteria for Information Technology Security Evaluation [8] within the security domain and IEC 61508:1998 Functional safety of electrical/electronic/program-mable electronic safety-related systems [7] within the safety domain. However, most evaluations, even though they follow a standard, are a qualitative and subjective activity biased by the evaluator.

Risk assessment was initially developed within the safety domain, but has later been adapted to security critical systems as security risk assessment. The two most relevant approaches are CCTA Risk Analysis and Management Methodology (CRAMM) [2] and the CORAS framework [15]. CRAMM targets health care information systems and is asset-driven. The CORAS framework is inspired by CRAMM and has adapted the asset-driven strategy of CRAMM.

The main deficiency of the above approaches is that the risk level is not under control, meaning that there has not been a prior activity on deciding which risk to accept and not to accept based on a cost-benefit strategy. These are the challenges of the research domain of quantifying security or operational security.

An initial model towards quantitative estimation of security risk, also referred to as operational security, was discussed in Littlewood et al. (1993) [12]. The model derives quantitative operational measures such as mean time and effort to security breach. This idea was further explored in [4,5,13,16].

This paper extends the availability prediction model from [5] and uses CVSS to estimate frequency and impact of remotely exploitable vulnerabilities.

3. Risk level estimation model

To estimate risk level we need to specify not only the expected behaviour and services that the safety and mission critical system offers, but also the ability of the system to resist external faults and in particular intentional faults [10]. The latter is usually referred to as the ability of the system to withstand security attacks or attack resistance capabilities. For these systems, security attacks might be the cause of reduction of either/or the system's safety level or its core mission execution abilities. This means that security interchange with safety and mission criticality in that preserving security becomes one of the core missions of the system. Figure 1 gives an overview of the potential fault introduction sources and how these may affect the risk level.

The risk level estimation model is based on work by Laprie (1992/2004) [1,11] and Jonsson (1992) [10].

Definition *A fault* occurs when authorised user, unauthorised user (attacker) or system internal input causes an error in the system.

Definition *A failure* is an undesirable system state. A failure may lead to degradation of safety and/or core mission level and thereby increase the risk level.

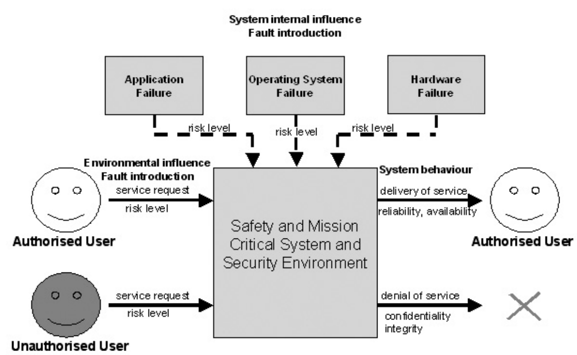

Figure 1. Fault introduction and risk level

3.1. Computational procedure for deriving risk level

The risk level model is supported by a three step computational procedure: (1) Identify vulnerabilities, (2) Estimate frequency and impact of vulnerabilities using CVSS and (3) Derive risk level from frequency and impact estimates.

Step 1 is performed by examining the CVSS and/or by running a vulnerability scanner to derive a list of vulnerabilities in the system. However, the latter is not always possible in practise. The risk levels of a vulnerability defines its severity. This does not always mean that two vulnerabilities having the same risk level pose the same severity in terms of reducing the service level (safety and mission level) of a system. Also, risk is perceived differently by different stakeholders and has only meaning within a context.

Step 2 estimates the frequency and impact of the vulnerabilities using the experience information in the CVSS. Details are given in the following.

Step 3 takes the resulting frequency and impact estimations and combines them into a risk level. As the model is implemented as a BBN this is done using the computational means of BBN.

4. Common Vulnerability Scoring System (CVSS)

The CVSS, launched in 2004, is an effort to provide a universal and vender-independent score of known vulnerabilities. CVSS has already been adopted by big hardware and software development companies, like IBM, HP and Cisco as a reporting metric in vulnerability bulletins, by scanning tools vendor like Nessus and Qualys and by the NIST (National Institute of Standards and Vulnerabilities), which maintains the National Vulnerability Database (NVD); the main repository of known vulnerabilities worldwide.

The CVSS score, a decimal number on a scale 0.0-10.0, is composed of three metrics groups: base, temporal and environmental [14]. The **base metrics group** quantifies the intrinsic characteristics of a vulnerability in terms of two sub-scores: (i) *exploitability_subscore*; composed of *access required (B_AR)*, *access complexity (B_AC)* and *authentication instances (B_AU)*, and (ii) *impact_subscore* to confidentiality *(B_C)*, integrity *(B_I)* and availability *(B_A)* in terms of *none*, *partial* or *complete*. The **temporal metrics group** quantifies dynamic aspects of a vulnerability in terms of three attributes: (i) *exploitability tools & techniques (T_E)*, (ii) *remediation level (T_RL)* and (iii) *report confidence (T_RC)*. The exploitability attribute refers to the availability of code or technique for exploiting a vulnerability and is evaluated in terms of: *unproved*, *proof-of-concept*, *functional* or high. The remediation level attribute refers to the type of remediation available for the vulnerability in terms of *official fix*, *temporary fix*, *workaround* or *unavailable*. The report confidence attribute refers to the certainty of information about the existence of the vulnerability. It is evaluated as *unconfirmed*, *uncorroborated* (conflicting sources of information) or *confirmed*. For all three attributes the list of options reflects increasing levels of exploitability. The **environmental metrics group** quantifies two relevant aspects of a vulnerability that are dependent on the environment and on stakeholders' values: (i) *collateral damage potential (E_CDP)* and (ii) *security requirements*. The collateral damage potential measures the potential damage to life loss, physical asset loss, loss of revenue and loss of productivity in terms of the qualitative scale *none*, *low*, *low-medium*, *medium-high* or *high*. The security requirements refer to the desired level of *confidentiality (E_CR)*, *integrity (E_IR)* and *availability (E_AR)* of the system and are measured in terms of *low*, *medium* or *high*.

More information on CVSS in general and the CVSS formulas in particular are in the CVSS guide [3,14].

5. Estimating frequency and impact using CVSS

We use the CVSS to estimate the two variables frequency and impact. In fact, we rearrange the CVSS attributes to calculate frequency and impact instead of base, temporal and environmental scores. I.e., the more exploitable is a vulnerability, the more likely it will be exploitable by attackers, and the higher should be its frequency. By considering the exploitability factors intrinsic to the vulnerability itself (i.e. the base metrics related to exploitability) and the temporal factors we are able to calculate the frequency for all vulnerabilities present in the system. The same rationale applies to impact. The impact potential of a vulnerability (i.e. the base metrics related to impact) depends on the security requirements to the system and the collateral damage potential of the vulnerability (i.e. the environmental metrics related to impact).

5.1. Obtaining temporal and environmental data

Unlike the base metrics, which are available for all vulnerability in the CVSS, the temporal and environmental metrics are obtained elsewhere.

The temporal metrics used for the calculation of frequency refer to the availability of fixes, the availability of exploitation tools & techniques and the availability of evidences that confirm the vulnerability. Although the CVSS does not provide the temporal and environmental metrics, because they are dynamic, it

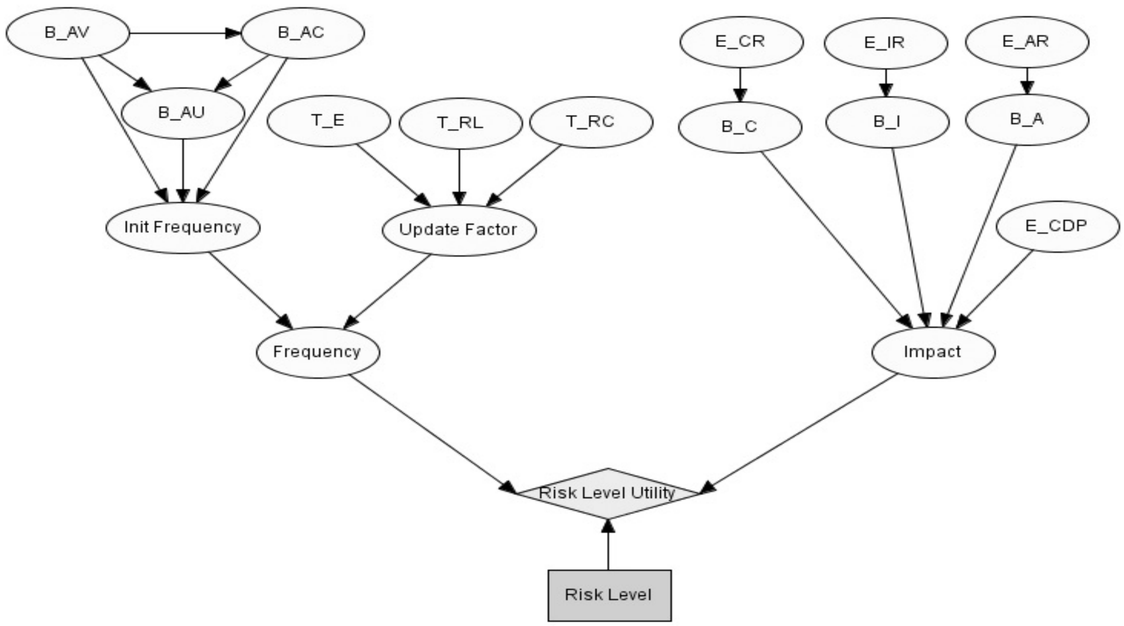

Figure 2. Risk level estimation model BBN

provides external links (http://www.securityfocus.com, http://xforce.iss.net, http://www.readhat.com) and references to vendors' sites that contain relevant information. Additional information can be collected from specialised forums (http://isc.sans.org/, http://www.modsecurity.org/blog) and media (http://www.darkreading.com/). Furthermore, the CVSS guide [14] supplies some guidelines for assigning qualitative values to the temporal metrics. Thus, temporal metrics are dependent on expert judgment of public information about a specific vulnerability.

The environmental metrics used for the calculation of impact refer to the system security requirements (C I A) and collateral damage. Security requirements are given by stakeholders on a system basis (as they are system specific). Collateral damage is specific to an organisation and depend on a coherent and agreed upon definition of the inherent meaning of *low*, *low-medium*, *medium-high* and *high* loss. This means that the underlying CDP qualitative value scale must be defined per organisation.

5.2. Estimating frequency from base and temporal data

Frequency is a value in the range *[0,1]*, where the value *0* means that the vulnerability will never be exploited and the value *1* means that the vulnerability will for certain be exploited. Values in the range *<0,0.5>* means low possibility for the vulnerability to be exploited and values in the range *<0.5,1.0>* means high possibility for the vulnerability to be exploited. The value *0.5* should be interpreted as that it is just as likely that the vulnerability will be exploited as that it will not.

The risk level estimation model is implemented as a BBN. BBN is a directed acyclic graph (DAG) together with an associated set of probability tables. A DAG consists of nodes representing the variables involved and arcs representing the dependencies between these variables. Nodes are defined as stochastic or decision variables and multiple variables may be used to determine the state of a node. Each state of a node is expressed using probability density functions. Probability density expresses the confidence in the various outcomes of the set of variables connected to a node and depends conditionally on the status of the parent nodes at the incoming edges.

There are three types of nodes in a DAG: (1) target node(s), (2) intermediate nodes and (3) observable nodes. Target nodes are nodes about which the objective of the network is to make an assessment (the question that needs an answer). The directed arcs between the nodes denote the causal relationship between the underlying variables. Evidence or information is entered at the observable nodes and propagated through the network using the causal relationships and a propagation algorithm based on the underlying computational model of BBN [9]. Our model is implemented using the BBN tool HUGIN [6] and this introduces the additional semantics of: stochastic variables are modelled as ovals, decision variables are modelled as rectangles and the associated utility functions supporting the decision variables are modelled as diamonds.

Figure 2 shows the risk level estimation model BBN. The frequency part is on the left side of the figure.

The frequency estimate is derived by inserting the values for the base metrics sub variables first and from those derive the initial frequency. As can be seen in Figure 2, there is a dependency between the sub variables *B_AC* and *B_AR*. That is, the attack complexity is dependent on the access required. This points to that it is easier to exploit a vulnerability in cases where only network access is required. If local access is required it becomes substantially more difficult both to launch and to carry out an attack without being discovered. Furthermore, authentication instances is both dependent on the attack complexity and the access required (*B_AU|(B_AR,B_AC)*), as it is likely that one need several authentication instances if the exploit is complex and if it requires local access. There might also be dependency in the other direction (that is attack complexity dependent on authentication instances), but this is not specified in the CVSS.

The temporal metrics sub variables is used to derive the update factor and covers the indirect circumstances of an attack. Exploitability tools & techniques points to the availability of automated tools to exploit the vulnerability. Remediation level refers to the effectiveness of the existing security measures and report confidence describes the trust level one should have towards the values provided for the base metric sub variables.

5.3. Estimating impact from base and environmental data

As for frequency, the base metrics are used to establish the initial impact value. However, for impact it is the environmental metrics that are used to update the initial value. The environmental metrics are context specific; that is, they put the confidentiality, integrity and availability impacts into perspective of the associated requirements and the collateral damage potential relevant for a particular system. Hence, the base metrics describe the magnitude of the effect on each security property, which is later made system specific by applying the environmental metrics to the base metrics. The impact part of the risk level estimation model BBN is shown on the right side of Figure 2.

6. Example

In the modern offshore drilling environment the Logging and Measurement While Drilling (LWD and MWD) subsystems are integral parts of maintaining business continuity and safety. LWD data is formation evaluation (FE) data used by geologists to optimise the placement of the well in real-time. MWD data includes the direction and inclination of the well, drilling and tool mechanical information and pressure indicators. For the drilling operation, the FE data together with tool and drilling mechanical data are mission critical. The safety critical data are the pressure readings from surface and down hole, which are used for identification of kicks, blow-outs and stuck-pipe situations, and directional data relevant for collision prevention.

Over the last half-decade several on-shore drilling operational support centres have been established. These centres simultaneously support multiple offshore installations with field, directional drilling, safety, etc. experts that monitors the drilling operations in real-time. By doing so, the experts are physically co-located and can assist each other in real-time. This is particularly important during failure situations.

The use of these on-shore operational centres adds demands on the reliability, availability, confidentiality and integrity of the communication link and communicated data between the offshore and on-shore sites. Earlier all communication was over shield, company owned or trusted third party leased communication links. Due to cost constraints the situation is changing and remotely accessible communication means have been introduced. This exposes data to remotely accessible vulnerabilities in the communication mean or the communication end-points. In the following we discuss how to use the CVSS to estimate the risk level of safety and mission critical data in the context of drilling support operational centres.

Lets say that we identify a vulnerability with the following base attributes: *B_AR=network*, *B_AC=low* and *B_AU=none*. These are the base metric sub variables used to derive the initial frequency (see Figure 2). Expert evaluation of the vulnerability reveal the following associated temporal metric sub variable values: *T_E=functional*, *T_RL=workaround* and *T_RC=con-firmed*. Combining these two sets of information gives the frequency estimate: *low=0.0*, *medium=0.25* and *high=0.75*, which means that there is *three times more likely that the frequency is high than medium* (it is never low). Note that the prior probability distributions for the sub variables are provided by the CVSS.

The impact information available (in the CVSS) for the vulnerability is the following: *B_CI=complete*, *B_I=none* and *B_A=none*. The relevant security requirements are: *E_CR=high*, *E_IR=medium*, *E_AR=medium* and the collateral damage potential is: *E_CDP=low*. Deriving the impact distribution according to the impact part of Figure 2 results in: *low=0.4*, *medium=0.3* and *high=0.3*.

The frequency and impact distributions are then used to derive the risk level estimation distribution (see Figure 2). The resulting risk level estimate distribution is: *low=0.05*, *medium=0.57* and *high=0.38*, which means that the risk level most likely is *medium* (57% chance). It is also relatively likely that the risk level is high (38% chance).

7. Conclusion

This paper has shown how to use the CVSS to estimate frequency and impact of remotely reachable vulnerabilities for safety and mission critical systems. The CVSS consists of the three metrics groups: base, temporal and environmental. We use the base and temporal metrics to estimate frequency and the base and environmental to estimate impact. Frequency and impact estimates are then combined to a risk level estimate using a risk level estimation model BBN.

Future work involves extending the estimation model BBN to support alternative frequency and impact estimation information sources, such as vendor specific vulnerability bulletin lists, attack reports (NIST, security bulletin lists, news groups, etc.) and subjective expert judgments. We have developed a trust-based information aggregation schema that will be used to aggregate these disparate sources of information.

8. References

[1] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing", *IEEE Transactions on Dependable and Secure Computing*, January 2004, 1(1):11–33.

[2] B. Barber and J. Davey, "The Use of the CCTA Risk Analysis and Management Methodology CRAMM in Health Information Systems" In *K.C. Lun, P. Degoulet, T.E. Piemme, and O. Rienhoff (editors): Proceedings of MEDINFO'92*, North Holland Publishing Co, Amsterdam, 1992, pp. 1589–1593.

[3] Common vulnerability scoring system v2 calculator, http://nvd.nist.gov/cvss.cfm. Accessed 13 October 2008.

[4] S.H. Houmb, G.Georg, R.France, J. Bieman, and J. Jürjens. "Cost-Benefit Trade-Off Analysis using BBN for Aspect-Oriented Risk-Driven Development", In *Proceedings of Tenth IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 2005),* Shanghai, China, June 2005, pp. 195–204.

[5] S. Houmb, G. Georg, R. France, R. Reddy, and J. Bieman, "Predicting Availability of Systems using BBN in Aspect-Oriented Risk-Driven Development (AORDD)", In *Proceedings of the 9th World Multi-Conference on Systemics, Cybernetics and Informatics, Volume X: 2nd Symposium on Risk Management and Cyber-Informatics (RMCI'05)*, International Institute of Informatics and Systemics, Orlando, Florida, USA, July 2005, pp. 396–403.

[6] Hugin Expert A/S, HUGIN Version 6.8, 19 April 2007. http://www.hugin.dk..

[7] IEC 61508:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems, 1998.

[8] ISO 15408:2007 Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, CCMB-2007-09-001, CCMB-2007-09-002 and CCMB-2007-09-003, September 2007.

[9] Jensen, F, *An introduction to Bayesian Network*. UCL Press, University College London, 1996.

[10] E. Jonsson. "On the integration of security and dependability in computer systems". In *IASTED International Conference on Reliability, Quality Control and Risk Assessment*, Washington, November 1992, pp. 93–97.

[11] Laprie, J.C., *Dependability: Basic Concepts and Terminology*, Springer, 1992.

[12] B. Littlewood, S. Brocklehurst, N. Fenton, P. Mellor, S. Page, D. Wright, J. Dobson, J. McDermid, and D. Gollmann, "Towards Operational Measures of Computer Security", *Journal of Computer Security*, 1993, (2):211–229.

[13] B.B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, and K.S. Trivedi. "Modeling and Quantification of Security Attributes of Software Systems". In *Proceedings of the International Conference on DependableSystems and Networks (DSN'02)*, volume 2, IEEE Computer Society, 2002, pp. 505–514.

[14] Mell, P, Scarfone, K, and Romanosky, S., *A complete guide to the common vulnerability scoring system*, version 2.0. Published by FIRST - Forum of Incident Response and Security Teams, June 2007. http://www.first.org/cvss/cvss-guide.pdf.

[15] K. Stølen, F. den Braber, T. Dimitrakos, R. Fredriksen, B. Gran, S. Houmb, Y. Stamatiou, and J. Aagedal, "Model-based Risk Assessment in a Component-Based Software Engineering Process: The CORAS Approach to Identify Security Risks", Chapter in *Business Component-Based Software Engineering*, Kluwer, 2002, pp. 189-207.

[16] D. Wang, B.B. Madan, and K.S. Trivedi, "Security Analysis of SITAR Intrusion Tolerance System", In Proceedings of the 2003 ACM workshop on Survivable and self-regenerative systems: in association with 10th ACM Conference on Computer and Communications Security, ACM Press, 2003, pp. 23–32.