The Journal of Systems and Software xxx (2009) xxx–xxx

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

Quantifying security risk level from CVSS estimates of frequency and impact

Siv Hilde Houmb [a,*], Virginia N.L. Franqueira [b], Erlend A. Engum [c]

[a] Connected Objects Laboratory, Service Platforms Group, Tele nor R&I, Otto Nielsens vei 12, 7004 Trondheim, Norway
[b] Information Systems Group, CTIT, University of Twente, Drienerlolaan 5, 7522 NB Enschede, The Netherlands
[c] National Oilwell Varco, Lagerveien 8, 4069 Stavanger, Norway

ARTICLE INFO

Article history:
Received 15 January 2009
Received in revised form 22 July 2009
Accepted 19 August 2009
Available online xxxx

Keywords:
Quantitative risk analysis
Security risks
Risk estimation
Common Vulnerability Scoring System (CVSS)
Dependable systems
Remote operation

ABSTRACT

Modern society relies on and profits from well-balanced computerized systems. Each of these systems has a core mission such as the correct and safe operation of safety critical systems or innovative and effective operation of e-commerce systems. It might be said that the success of these systems depends on their mission. Although the concept of "well-balanced" has a slightly different meaning for each of these two categories of systems, both have to meet customer needs, deliver capabilities and functions according to expectations and generate revenue to sustain today's highly competitive market. Tighter financial constraints are forcing safety critical systems away from dedicated and expensive communication regimes, such as the ownership and operation of dedicated communication links, towards reliance on third parties and standardized means of communication. As a consequence, knowledge about their internal structures and operations is more widely and publicly available and this can make them more prone to security attacks. These systems are, therefore, moving towards a remotely exploitable environment and the risks associated with this must be controlled.

Risk management is a good tool for controlling risk but it has the inherent challenge of quantitatively estimating frequency and impact in an accurate and trustworthy way. Quantifying the frequency and impact of potential security threats requires experience-based data which is limited and rarely reusable because it involves company confidential data. Therefore, there is a need for publicly available data sources that can be used in risk estimation. This paper presents a risk estimation model that makes use of one such data source, the Common Vulnerability Scoring System (CVSS). The CVSS Risk Level Estimation Model estimates a security risk level from vulnerability information as a combination of frequency and impact estimates derived from the CVSS. It is implemented as a Bayesian Belief Network (BBN) topology, which allows not only the use of CVSS-based estimates but also the combination of disparate information sources and, thus, provides the ability to use whatever risk information that is available. The model is demonstrated using a safety- and mission-critical system for drilling operational support, the Measurement and Logging While Drilling (M/LWD) system.

1. Introduction

Making informed and justifiable trade-offs between cost, safety, security and mission is essential for controlling risks to safety- and mission-critical systems. This is of particular importance during the planning and development of such systems as early decisions can reduce development cost and ease the risk control. Controlling risk is non-trivial and involves a number of trade-offs: both safety and security must be balanced with mission and security, safety and mission must be balanced with costs, time-to-market and other business constraints.

In general, a trade-off involves an analysis where the risks of one solution and those of alternative solutions are evaluated against each other. Such an analysis is best made based on quantitative data, provided that the data has clear semantics. Although quantitative data is more precise than qualitative data, the latter is often more descriptive but harder to compare as both the syntax and the semantics might be unclear. Thus, a Risk Level Estimation Model that produces quantitative risk estimates is preferable. One such model is the CVSS Risk Level Estimation Model presented in this paper. This model supports trade-off analysis of any type of system but, in this paper, it is applied to the control of risks in a Measurement and Logging While Drilling (M/LWD) system on oil and gas drilling installations (Haines et al., 2006). Such systems are becoming more dependent on data transfer over infrastructure that is remotely accessible and, therefore, prone to inherent accidental and intentional faults from known vulnerabilities[1] (passive)

* Corresponding author. Tel.: +47 913 07 714; fax: +47 73 54 37 00.
E-mail addresses: siv-hilde.houmb@telenor.com (S.H. Houmb), franqueirav@ewi.utwente.nl (V.N.L. Franqueira), Erlend.Engum@nov.com (E.A. Engum).

[1] Know vulnerabilities refer to vulnerabilities made known to the public by publishing on the Internet, in bulletin boards or similar.

0164-1212/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2009.08.023

sources such as software, operating system or hardware; and (ii) environmental (active) sources such as malicious software (e.g. worms and Trojans) and malicious users (e.g. attackers). In addition, there are accidental faults that may arise from a design flaw or as a result of usability issues (system misbehaviour caused by unintentional actions performed by authorized users). Nevertheless, a safety- and mission-critical system such as the M/LWD system should deliver services as a result of authorized requests and deny the execution of unauthorized requests. This means that such a system needs the ability to maintain the system integrity, also referred to as the attack resistance of the system, regardless of the source or type of faults it may be exposed to.

Gaining knowledge of the risks involved, including the security risks, is essential for ensuring sustainable profit. This is because budget might be restricted and both risk and cost should be within acceptable limits. Considering our example system, dedicated communication links are both costly and resource demanding but the risks involved are more controllable. Thus, the following trade-off question is relevant for the M/LWD system, "*Can security risks be kept under control if a less expensive communication infrastructure is implemented between the drilling rig and the support centres?*" As this decision depends on the costs associated with each alternative (i.e., a dedicated or an open communication infrastructure) as well as the risks related to safety, security and mission, controlling risk and considering potential trade-offs, thus, become essential.

The first steps towards controlling risks to the M/LWD system are to define the system boundaries and the system environment and to ensure a good and common understanding of both, but particularly the system environment. By setting the system boundary on the communication end-points it becomes necessary to gather information about: (i) vulnerabilities on the communication link itself and on its end-points; (ii) the potential ways to exploit these vulnerabilities; and (iii) the consequences of their successful exploitation. As we are talking about future events, little experience-based data is available and this makes information gathering rather challenging. However, vulnerability information sources do exist that, even though do not provide information collected from similar systems in the context of the safety domain, can be used to aid risk level estimation. The Risk Level Estimation Model described in this paper makes use of experience data from one such vulnerability source, namely the Common Vulnerability Scoring System (CVSS) (CVSS calculator, 2007; Mell et al., 2007).

The CVSS provides a universal and vender-independent score of known vulnerabilities. Several large hardware and software development organizations have already adopted CVSS as a reporting metric in vulnerability bulletins, as well as scanning tool vendors such as Nessus and Qualys and the NIST (National Institute of Standards and Vulnerabilities). NIST (2009) maintains the National Vulnerability Database (NVD, 2009), which is a large worldwide database of known vulnerabilities. The CVSS score is composed of three metric groups (base, temporal and environmental). Each provides equations and input arrays that together create one CVSS score for a particular vulnerability. The CVSS Risk Level Estimation Model presented in this paper uses neither the CVSS equations nor the final CVSS scores directly but, rather, restructures the attributes of the three metric groups to estimate the frequency of potential fault introduction and the magnitude of the impact that these may cause. These two estimates are combined into a risk level estimate. The model is implemented as a Bayesian Belief Network (BBN) (Jensen, 1996; Pourret et al., 2008) as this allows for multiple frequency and impact estimation sources and for combining CVSS information with expert opinions supporting disparate information sources. BBN also allows the input of information on multiple abstraction layers by means of forward and backward calculation to derive the frequency, impact and risk level estimates. Thus, if a certain risk level is imposed, it is possible to use the BBN model to derive the frequency and impact estimates needed to meet this demand and, from that, better select effective security measures.

The contribution of this paper is three-fold:

1. It presents a model for the quantitative estimation of the security risk level of a system or particular parts of a system. Although the model in this paper is considered only for a safety- and mission-critical system, it can be applied to any kind of computerized system where security is a critical factor.
2. The model takes advantage of publicly available data from the CVSS. The CVSS performs two roles in the risk model: (i) it is used to construct the model, determining the structure of the BBN; and (ii) it is used as input information when running the model, e.g. by providing rating values as conditional probability functions used in the calculation of the risk level; and
3. The implementation of the model as a BBN topology provides flexibility. It allows estimates from the CVSS to be combined with information from other sources (e.g. data derived from risk management best practices) and to input information at various levels of abstraction.

These are the main advantages of the CVSS Risk Level Estimation Model and represent the novelty of our model in relation to alternative models.

The paper is organised as follows: Section 2 details the problem context within which the model is applied in this paper, i.e., the M/LWD system. Section 3 introduces the CVSS and the three metric groups of CVSS. Section 4 presents the CVSS Risk Level Estimation Model, where: Section 4.1 describes the computational steps involved in deriving security risk level; Section 4.2 discusses how CVSS has been reorganized in the model for frequency and impact estimation; Sections 4.3 and 4.4 introduce the concept of BBN, present the BBN implementation of the model and discuss how CVSS were used to determine the structure of the BBN. Section 5 gives an example of using the CVSS Risk Level Estimation Model implemented as a BBN to derive frequency and impact estimates and, from these, the security risk level in the context of the M/LWD system. This section also discusses how to use CVSS as an information source to the frequency and impact estimation variables in the BBN. Section 6 puts the Risk Level Estimation Model into the context of related work and discusses its strengths and weaknesses and Section 7 summarises the main contributions of the paper and outlines some of the plans for future work.

2. Problem context

In a modern offshore drilling environment the M/LWD system is an integral and important part of maintaining business continuity and safety. The system is integrated with collar-mounted tools (i.e., sensors) placed physically close to the drill bit. These are responsible for performing a wide variety of measurements which are then sent to the surface using, most commonly, pressure pulses in the drilling mud (Gardner and Merchant, 1996). Data collected by the MWD subsystem include the direction and inclination of the well, drilling and mechanical information and pressure indicators. Data logged by the LWD subsystem relates to the formation evaluation (FE) data such as natural gamma radiation, formation porosity, density and formation resistivity (Clark et al., 1996; Wright, 1991; Minette, 1995) used by geologists to optimise the placement of the well in real-time. The safety of personnel on a drilling installation is always the first priority. The M/LWD system provides a set of safety-critical data that is constantly monitored by engineers situated both onshore and offshore. One example of such data is the pressure readings from the surface and downhole that are used to

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023

identify kicks, blowouts, stuck pipe situations, lost circulation and higher-than-certified pressure on the standpipe.

The mission of most oil and gas wells is to penetrate a formation containing hydrocarbons and thus the drilling operation is mission and safety critical. Well drilling is associated with high costs with average rig rates in the range of USD 30,000 per day (for a Drill Barge drilling at up to 150ft water depth) to over USD 380,000 per day (for a Semisubmersible offering in excess of 4000ft water depth) (Rigzone.com, 2009). Additional costs come from services, logistics and administration. Consequently the oil companies and oilfield service providers find it important to maintain continuous and effective operations. In response to this demand, several onshore drilling operational support centres have been established to support multiple offshore installations simultaneously (Schlumberger Remote Operations Management, 2009). These centres host the most experienced experts who are best suited to support the offshore staff with valuable advice. As the focus on safety, effectiveness and cost optimisation increases it becomes an attractive option to reduce the field staff and run as much as possible of the operations remotely from the support centres. A history of technological advances in drilling and a case study of remote operations can be found in Aldred et al. (2005). This is particularly interesting for the M/LWD system because it enables it to be operated directly by remote access to the offshore computers. Having fewer people offshore is safer as personnel are less likely to hurt themselves in an office as can be seen from the UK Health and Safety Executive statistics which lists various onshore injury rates (Health and Safety Executive, 2009a) and offshore injury rates (Health and Safety Executive, 2009b). It is also significantly less expensive and logistically easier to work from an onshore office.

One of the drawbacks of running the M/LDW system remotely is the need for a communication link. To gain remote access to the computers offshore and to receive all the important data, communication must remain uninterrupted at all times. Without the correct interpretation of the downhole data the operations on the rig may have to stop at short notice. Thus, the use of these onshore operational centres adds to the demands for the reliability, availability, confidentiality and integrity of the communication links and the data communicated between the offshore and onshore sites. Traditionally, all communication is over dedicated, company owned or trusted third party leased communication links. Due to cost constraints this situation is changing and remotely accessible communication means have been introduced. This exposes data to vulnerabilities in the communication channel itself and on the communication end-points. Fig. 1 illustrates the transition from traditional thinking to the new situation where a shared satellite link hosts the communication from the rig to the experts onshore. As we can see in the figure, in the new situations experts are also allowed to access rig information from additional locations such as from their home computer or small, personal handheld devices. In this paper, we show how the CVSS Risk Estimation Model, described in Section 4, can be used to derive the risk level of the new communication paradigm by estimating the frequency and impact of vulnerabilities inherent in the M/LWD system communication. This risk estimate can be used to help decision makers to plan future investment, to determine the level at which a particular solution is safe and financial sustainable and, from that, to ensure safety and mission continuity.

3. Common Vulnerability Scoring System (CVSS)

The following paragraphs describe those parts of the CVSS relevant to building and using the CVSS Risk Level Estimation Model.

The CVSS, maintained by FIRST (Forum of Incident Response and Security Teams) (www.first.org), was launched in 2004 and is currently on its second version. It is a system that provides one score, the so-called CVSS score, for each known vulnerability reported in vulnerability databases such as the NVD (National Vulnerability Database, 2009). It calculates this score using attributes grouped into three metric groups: base, temporal and environmental. A CVSS score is a decimal number in the range [0.0, 10.0], where the value 0.0 is no rating (vulnerability close to not possible to exploit) and the value 10.0 is full score (vulnerability easy to exploit).

The base metric group quantifies the intrinsic characteristics of a vulnerability in terms of two sub-scores: (i) *exploitability_subscore*; composed of *access vector* (*B_AV*), *access complexity* (*B_AC*) and *authentication instances* (*B_Au*), and (ii) *impact_subscore* to confidentiality (*B_C*), integrity (*B_I*) and availability (*B_A*). The access vector is evaluated in terms of *local*, *adjacent network* or *network*; access complexity in terms of *high*, *medium* or *low*; authentication instances in terms of *multiple*, *one* or *none*; and the base impact attributes are all rated in terms of *none*, *partial* or *complete*. Experts (from NIST) analyse the vulnerabilities reported in the NVD and assign one of the above-mentioned qualitative values to each base attribute for all vulnerabilities. Experts can only use the pre-defined qualitative values when evaluating vulnerabilities as the main intention of CVSS is to produce comparable vulnerability ratings. The base metric attributes are often provided by the vendor of the product in which the vulnerability has been discovered or by a third party. Furthermore, the characteristics of the base metric attributes are such that they are testable and hence can be validated. As an example, it is possible to prove or demonstrate the

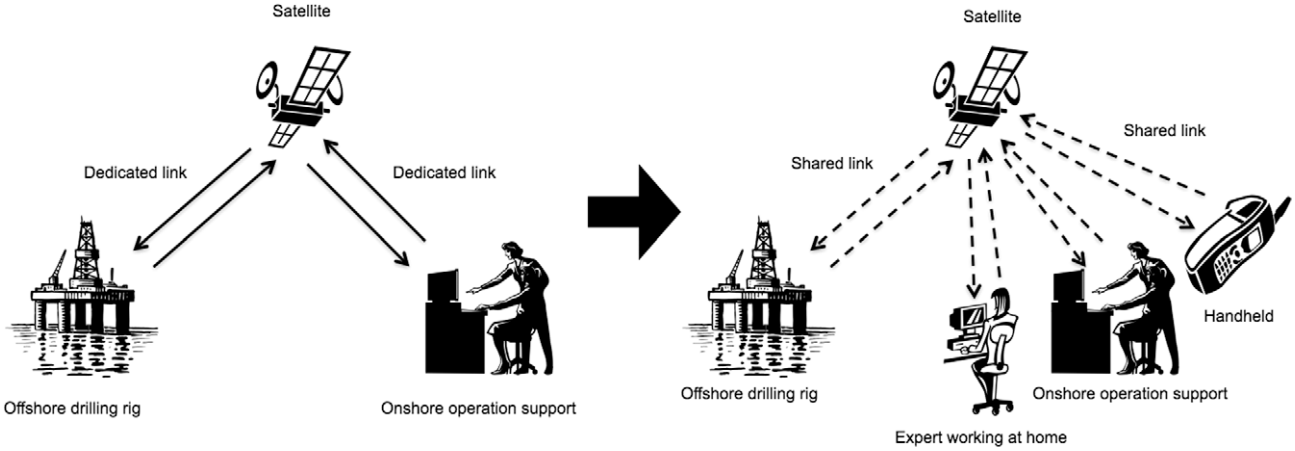

Fig. 1. Transition from controlled communication (left-hand side) to open communication (right-hand side) between drilling rig and onshore experts.

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023

ability to exploit a particular vulnerability from a network-type location such as the Internet, as either the exploit is already documented (an attack exploiting the vulnerability from a network-type location is already known) or it can be simulated.

The NVD reports the following information relevant to the base metric attributes: (i) the base score; (ii) the exploitability and impact sub-scores; and (iii) the base vector from which the base score has been derived. This makes it possible to perform an additional evaluation, if necessary, as all relevant information is made known to the public. For example, the vulnerability CVE-1999-0196 (National Vulnerability Database, 2009) has a base vector (AV:N/AC:L/AU:N/C:P/I:N/A:N) which is interpreted as follows:

AV:N – the access vector is "network" (i.e., the vulnerability can be exploited remotely);
AC:L – the complexity involved in exploiting the vulnerability is "low";
AU:N – authentication required for the exploitation of the vulnerability is "none";
C:P – the impact on confidentiality of a successful exploitation of the vulnerability is "partial"; and
I:N/A:N – the impact on both integrity and availability of a successful exploitation of the vulnerability is "none".

The temporal metric 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 (*T_E*) refers to the availability of code or techniques for automatically or manually exploiting a vulnerability and is evaluated in terms of: *unproved, proof-of-concept, functional* or *high*. The remediation level attribute (*T_RL*) refers to the type of remediation available for the vulnerability in terms of: *official fix, temporary fix, workaround* or *unavailable*. The report confidence attribute (*T_RC*) refers to the status of the information about the existence of the vulnerability (whether it is confirmed by trustable sources or not). 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 metric group quantifies three relevant aspects of a vulnerability that all depend on the system environment and the stakeholders' values: (i) *collateral damage potential* (*E_CDP*), (ii) *target distribution* (*E_TD*) and (iii) *security requirements*. The collateral damage potential attribute (*E_CDP*) measures the potential damage to life and the loss of value for physical assets, revenue and productivity in terms of the qualitative scale: *none*, *low*, *low-medium*, *medium-high* or *high*. The security requirements attributes identify to the desired levels of security within a system in terms of: *confidentiality* (*E_CR*), *integrity* (*E_IR*) and *availability* (*E_AR*). Each is measured as: *low*, *medium* or *high*.

Target distribution is not used explicitly in the CVSS Risk Level Estimation Model but, rather, is included as part of the CDP attribute. This attribute is intended to estimate the percentage of systems that could, potentially, be affected by a particular vulnerability and, as it is still difficult to estimate how much the impact is increased if several instances of a vulnerability are present in a system, it is assumed that this can be considered implicitly as part of the collateral damage potential, if available. Also, for safety- and mission-critical systems such as the M/LWD system, best practice is to design for robustness, e.g. use different operating systems and software from several vendors to avoid situations where the same vulnerability may be present simultaneously in several components of a system. Nevertheless, the model could be extended with target distribution should a need arise to distinguish between the distribution of a vulnerability within a system and the ability of this vulnerability to harm the system.

There is a set of equations and vector specifications in the CVSS that are used together to produce the CVSS score. Specifically, the CVSS score is determined by first calculating the base score from the base metric group using a base score equation and then updating it by examining the temporal metric group with its associated equation set. If such is done, the CVSS base score is given as input to the temporal metric group equations in addition to the temporal attributes prescribed by the CVSS and, from these, the base score is updated with a factor produced from the temporal metric. Finally, the equation set of the environmental metric group is used initially to derive the environmental update score and then to update the score derived from the base and temporal metric group equations. The final score, i.e., the CVSS score, is an expression of the severity level of a vulnerability. A low CVSS score means low severity, while a high score means high severity. No details on the three equation sets used by CVSS are given in this paper as they are not used directly in the CVSS Risk Level Estimation Model. The CVSS metric attributes are restructured within the model in order to estimate both the frequency and impact associated with vulnerabilities. The risk level is then derived from these two estimates. However, the model maintains the rating schema from CVSS, as discussed in the following section. More information on CVSS in general and the CVSS equation sets in particular can be found in the CVSS guide and online calculator (Mell et al., 2007; CVSS calculator, 2007).

4. CVSS Risk Level Estimation Model

As mentioned in the introduction, there are two main categories of fault introduction sources in safety- and mission-critical

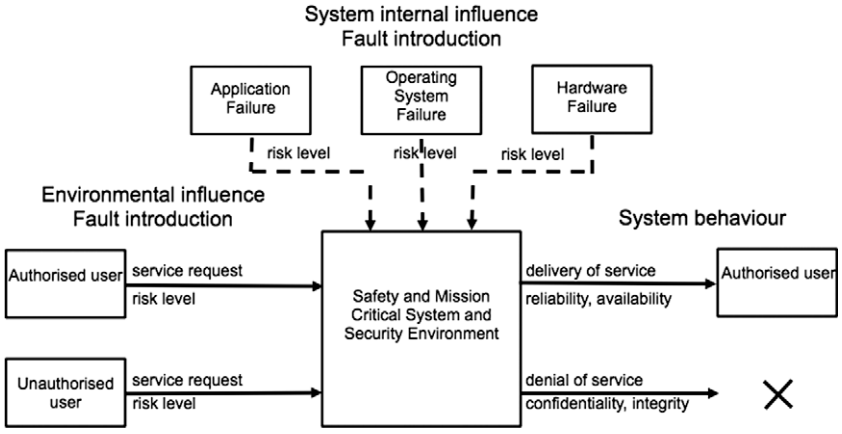

Fig. 2. System internal and environmental fault introduction as risk level influence sources and how they may affect the system behaviour.

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023

systems: internal fault introduction (e.g. software, operating system or hardware), and environmental fault introduction, (e.g. attackers, viruses, Trojans or other types of malware). Fig. 2 illustrates the two categories of fault introduction sources, how these two categories influence the risk level of a system and how this may affect the behaviour of a system. In general, the risk level of a system is the aggregate of the faults introduced to the system and the desired system behaviour is to deliver services according to authorized requests and to deny execution of unauthorized requests. If a system is able to do both, it has high attack resistance capabilities. Furthermore, the ability of a system to resist security attacks depends on both the vulnerabilities present in the system and the effectiveness of the security measures already employed in the system. These aspects are all taken into consideration when deriving the risk level in the CVSS Risk Level Estimation Model.

Fig. 2 extends the fault introduction model from Jonsson (2006) which includes the conceptual definition of dependability, its attributes and how it relates to security, as also discussed in Laprie (1992) and Avizienis et al. (2004). It is sufficient here to provide only the main definitions and a short description of how security relates to dependability. Please consult Jonsson (2006) and Avizienis et al. (2004) for details. Note that the definitions below are tailored to safety- and mission-critical systems as well as being made explicit for the CVSS Risk Level Estimation Model. Also note that "mission" in this context is considered to be the core business purpose of a system; i.e., for our example we consider that the mission of the M/LWD system is: "to drill wells profitably with no harm to people or the environment and to optimise the extraction of hydrocarbons to its maximum level".

Definition. *A fault* occurs when an authorized user, an unauthorized user (e.g. an attacker) or a system internal input causes an error in the system.

Definition. *A failure* is an undesirable system state caused by one or more faults. A failure may lead to the degradation of safety and/or mission level and affects the ability of a system to deliver services to authorized users and to deny services to unauthorized users.

Definition. *Risk level* is the combination of the frequency and impact of a fault on the safety and/or mission of a dependable system. The risk level of a system is influenced by fault introduction (as shown in Fig. 2).

4.1. Computational procedure for deriving risk level

The CVSS Risk Level Estimation Model is supported by a three step computational procedure:

Step 1: Identify vulnerabilities and potential fault introduction sources.
Step 2: Estimate frequency and impact of vulnerabilities using CVSS.
Step 3: Derive risk level from frequency and impact estimates.

Step 1 involves the identification of both the vulnerabilities and the potential fault introduction sources that are capable of exploiting the vulnerabilities. To achieve this, the following two activities should be undertaken: (i) passive vulnerability exploration and (ii) active vulnerability assessment.

During passive vulnerability exploration vulnerability databases are examined manually to check for recently reported problems and to evaluate their relevance for the system in question. Note that the temporal and environmental metric attributes are provided by domain and security experts and that experts tend to disagree (Cooke, 1991; Cooke and Goossens, 2000). Hence, it is not sufficient to consult only one source. At least two, and preferable more sources, should be consulted for the purpose of cross-checking vulnerability information. In cases where the protocols or applications used are proprietary, implying that there is very limited relevant vulnerability information available, it is necessary to carry out a manual system-specific vulnerability exploration. There are several ways to do this. One approach is to perform model-based security analysis such as that described in (Jürjens, 2005) using simulation or test-beds. Another approach is to use existing security standards, which is the approach taken in the CORAS framework (CORAS Project, 2003). For example, the CORAS framework includes vulnerability exploration questionnaires based on the guidelines in the security standard ISO/IEC27001:2005 (ISO/IEC27001, 2005).

An easily available and regularly updated source of vulnerability data is the NVD which provides the CVSS base vector directly. However, even in cases where CVSS information is not provided directly, vulnerability information in the NVD can still be used as input to the risk estimation model by interpreting the information according to the CVSS metric groups, i.e., make the vulnerability information explicit.

Active vulnerability assessment involves, for example, running a vulnerability scanner (Nessus, 2008) on the system or parts of the system and "tiger-team" hacking. For the "tiger-team" activity to be efficient in the use of time and resources it is important to follow a structured procedure. Please consult Laakso et al. (1999) for details. Active assessment can also be performed in real-time using, for example, Honeypots or Honeynets (Spitzner, 2003) or similar real-time simulations of the system.

The result of Step 1 is a list of vulnerabilities and threat scenarios, i.e., a description of how vulnerabilities can be exploited. Note that active vulnerability assessment is not always a practical option. Reasons for this might be that the necessary ports to run a vulnerability scanner are not enabled due to a lack of access to test installations of the system or due to demands on continuous normal operation (no ability to take the system offline to run a vulnerability scanner safely).

The frequency and impact of the vulnerabilities identified in Step 1 are estimated in Step 2 using the available CVSS information, i.e., the vector from which the base score has been derived. The CVSS metric groups have been reorganized in the CVSS Risk Level Estimation Model in order to derive frequency and impact estimates directly, rather than a severity score. Both the frequency and the impact values are quantitative and in the range [0.0, 1.0], where the value 0.0 means that the vulnerability will never be exploited or that the exploitability of the vulnerability will result in no impact and the value 1.0 means that the vulnerability is certain to be exploited or that its exploitation will certainly lead to the worst-case impact. Values in the range $\langle 0.0, 0.5\rangle$ imply a low possibility of the vulnerability being exploited or causing a severe impact; values in the range $\langle 0.5, 1.0\rangle$ imply a high possibility of the vulnerability being exploited or causing a severe impact. The value 0.5 should be interpreted as an equal likelihood of the vulnerability being exploited or not being exploited or that there is a 50% chance of a severe impact.

The frequency and impact estimates derived in Step 2 are combined into a risk level estimate in Step 3. The risk level of a particular vulnerability defines its severity and is the result of combining the frequency and impact along the fault introduction paths. This means that the estimated frequency refers not to the possibility of the vulnerability being present in the system but, rather, to the frequency of the vulnerability being exploited by one or more fault introduction sources, as illustrated in Fig. 2. However, even if two vulnerabilities have the same risk level, this does not necessarily mean that they pose the same threat in terms of a reduction in the service level (safety and mission level) of a system. That is to say that there is no simple relationship between risk level and system service level which is influenced by

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023

other factors as well. Also, risk is often perceived differently by different stakeholders and only has meaning within a particular context.

4.2. Re-organising CVSS for Frequency and Impact Estimation

Each of the three CVSS metric groups comprises a set of attributes and it is these attributes that are re-organised to estimate the frequency and impact of vulnerabilities in Step 2 of the computational procedure (see previous section). The rationale behind the rearrangement is that a highly exploitable vulnerability is more likely to be misused by attackers and, consequently, should have a higher frequency. By considering the intrinsic exploitability factors of the vulnerability itself (i.e., the base metric attributes relevant to exploitability) and the temporal factors, it is possible to calculate the exploitability frequency of each vulnerability present in a system. The same rationale applies to impact. The potential impact of a vulnerability depends not only on the impact intrinsically caused by the vulnerability (i.e., the base metric attributes relevant to impact) but also on the security requirements of the system and the distribution and collateral damage potential associated with a vulnerability (i.e., the environmental metric attributes relevant to impact).

CVSS also provides some descriptions of the dependencies between the attributes that are relevant to frequency and impact estimation. These are used in the CVSS Risk Level Estimation Model to specify the variable structure and their internal probabilistic dependencies. Fig. 3 shows the attributes of the three CVSS metric groups and highlights which attributes are used for frequency and impact estimation, respectively. The attributes used to calculate frequency are emphasised in the figure with short dotted lines and the attributes used to calculate impact are emphasised with long dotted lines.

4.3. Estimating frequency from base and temporal attributes

As shown in Fig. 3, we use three attributes from the base metric group and three attributes from the temporal metric group to estimate the frequency of vulnerability exploitations. The attributes from the base metric group are: access vector (*B_AV*), access complexity (*B_AC*) and authentication instances (*B_Au*) and from the temporal metric group: exploitability tools & techniques (*T_E*),

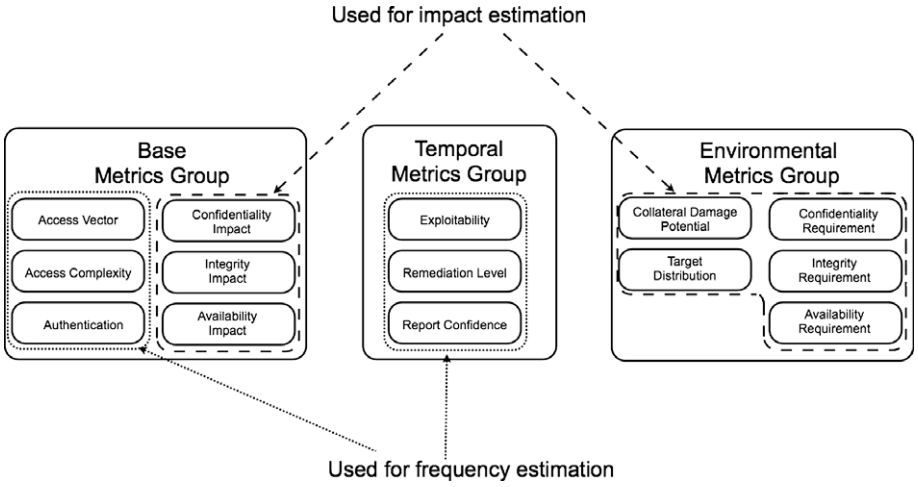

Fig. 3. Emphasised subset of attributes from the CVSS (Mell et al., 2007) used in our model.

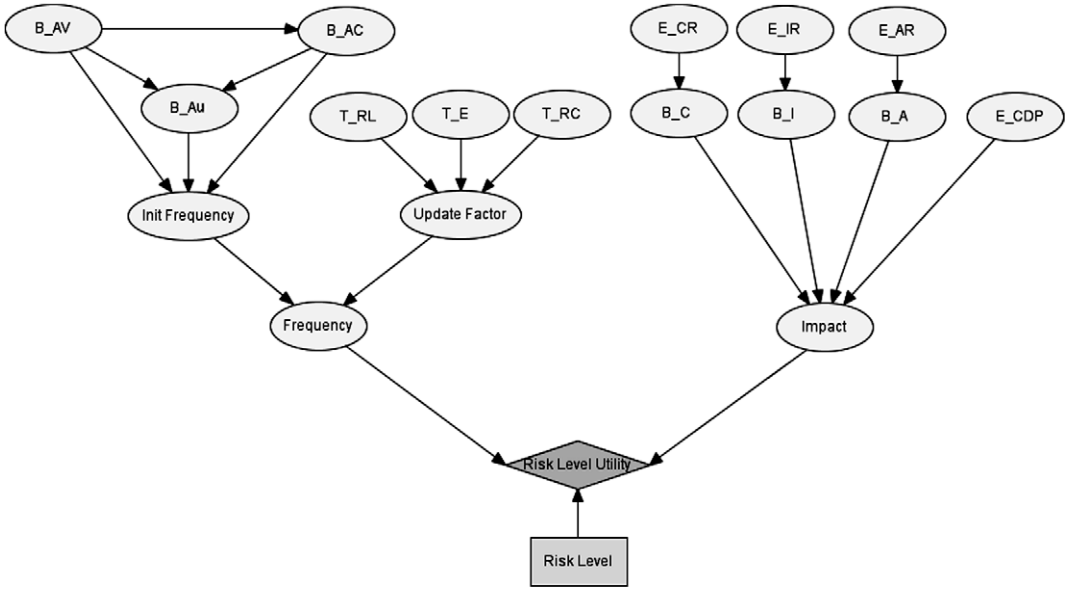

Fig. 4. BBN topology of the CVSS Risk Level Estimation Model.

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023

remediation level (*T_RL*) and report confidence (*T_RC*). The base metric attributes are intrinsic to a vulnerability in that they refer directly to it, while the temporal metric attributes describe seasonal factors related to a vulnerability. For this reason the base metric group attributes are used to establish an initial frequency value that is later updated using the temporal metric group attributes. Each attribute used in frequency estimation is input as a variable to the Bayesian Belief Networks (BBN) implementation of the CVSS Risk Level Estimation Model shown in Fig. 4, and discussed in the following. This is done by using the internal attribute ratings (column entitled *rating* in Table 1) and the rating values (column entitled *rating value* in Table 1), as given in the CVSS.

The left-hand side of Fig. 4 represents the frequency part of the model where attributes from the basic metric group are used as variables to derive the initial frequency estimate and the attributes from the temporal metric group are used to update this initial frequency estimate. Furthermore, the attribute ratings are modelled as states of each variable and the rating values are input as the prior probability distributions for each variable. Fig. 4 also illustrates the dependency between the access complexity attribute, *B_AC*, and the required access vector, *B_AV*. This dependency is mentioned indirectly in the CVSS and made explicit in the CVSS Risk Level Estimation Model. The underlying reasoning is that it is easier to exploit a known vulnerability if only network access is required. If local access is required, it becomes substantially more difficult both to launch and to carry out an attack (note that local access does not refer to local physical access but, rather, local logical access). Authentication instances is dependent on both the attack complexity and the access vector (*B_Au|(B_AV,B_AC)*) as it is likely that it requires several authentication instances if the exploit is complex and if it requires local access. It is also possible that attack complexity may, conversely, be dependent on authentication instances but this is not taken into account in the model. Please see Houmb and Franqueira (2009) for details on the internal dependencies between the variables which are defined in terms of equation sets specifying the conditional probability relations between the variables.

Using BBN, with its computational capabilities, as the implementation language makes it possible to take advantage of risk information on various abstraction levels, work with incomplete information and to use the model as a decision support engine. BBN is a directed acyclic graph (DAG) together with an associated set of probability tables. A DAG consists of nodes representing variables 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. The state of each node is expressed as a probability density function (pdf) which expresses the confidence in the various outcomes of the set of variables connected to a node and which depends on the status of the parent nodes of incoming edges. There are three types of nodes in a DAG: (i) target nodes, (ii) intermediate nodes and (iii) observable nodes. Target nodes are those about which the objective of the network is to make an assessment (the question that needs an answer or the decision that needs to be taken). The directed arcs between the nodes denote the causal relationship between the underlying variables. Evidence or information is entered at any node in the network and propagated forward or backward in the network using the causal relationships and an evidence propagation algorithm based on the underlying computational model of BBN (Pourret et al., 2008). The CVSS Risk Level Estimation Model is implemented using the BBN tool HUGIN™ (Hugin, 2007a, b). This introduces the following additional semantics: 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.

A BBN differs from a decision network in that information can be inserted into any suitable node regardless of its level in the network. This means that information or observations are not merely inserted into the leaf (observable) nodes and propagated forward along the edges of the network. For example, empirical data on the frequency, if available, can be inserted directly into the intermediate node 'Frequency' in Fig. 4. The information is then propagated backward to the observable nodes and forward to the target node. This is one of the strengths of BBN and is, along with its ability to reason under uncertainty (Gran, 2002), the main reason why BBN was chosen as the implementation language for the model. Another reason is that it enables decision reasoning. For example, if there is a specific demand on the risk level but only limited information available at the observable nodes, the backward propagation of BBN can be used to reason how this risk level can be achieved (how much the frequency and/or impact must be changed to meet the required risk level). Furthermore, the CVSS attribute ratings and rating values (see Table 1) are used to instantiate the model, i.e., to establish the prior probability distributions. This means that the model is easy to use as no additional initialisation is needed (the model is pre-initialised according to the domain knowledge in the CVSS). That is to say that there is no need for a user of the model to specify probability matrices for the nodes. Whenever using the model the user simply inputs the available information into the relevant nodes (depending on the abstraction level of the available information) and observes the output. However, the pre-initialisation which was part of the implementation was not trivial and needs to be updated whenever new relevant attributes are included in the CVSS and in cases of change in the attribute internal rating values.

Table 1
CVSS attributes relevant for the calculation of frequency estimate.

CVSS metric group	CVSS attribute	Rating	Rating value
Base metric	Access vector (B_AV)	Local (L) adjacent	0.395
		Network (A)	0.646
		Network (N)	1.0
	Access complexity (B_AC)	High (H)	0.35
		Medium (M)	0.61
		Low (L)	0.71
	Authentication instances (B_Au)	Multiple (M)	0.45
		Single (S)	0.56
		None (N)	0.704
Temporal metric	Exploitability tools & techniques (T_E)	Unproved (U)	0.85
		Proof-of-concept (POC)	0.9
		Functional (F)	0.95
		High (H)	1.0
	Remediation level (T_RL)	Official fix (OF)	0.87
		Temporary fix (TF)	0.90
		Workaround (W)	0.95
		Unavailable (U)	1.0
	Report confidence (T_RC)	Unconfirmed (UC)	0.90
		Uncorroborative (UR)	0.95
		confirmed (C)	1.0

4.4. Estimating impact from base and environmental data

The impact part of the CVSS Risk Level Estimation Model is shown on the left-hand side of Fig. 4. As can be seen, three attributes from the base metric group and four attributes from the environment metric group are used to derive the impact estimate. Those from the base metric group are: confidentiality impact (*B_C*), integrity impact (*B_I*) and availability impact (*B_A*). Those from the environmental metric group are: confidentiality requirement (*E_CR*), integrity requirement (*E_IR*), availability requirement

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023

Table 2
CVSS attributes relevant for the calculation of impact estimate.

CVSS metric group	CVSS attribute	Rating	Rating value
Base metric	Confidentiality impact (*B_C*)	None (N)	0.0
		Partial (P)	0.275
		Complete (C)	0.660
	Integrity impact (*B_I*)	None (N)	0.0
		Partial (P)	0.275
		Complete (C)	0.660
	Availability impact (*B_A*)	None (N)	0.0
		Partial (P)	0.275
		Complete (C)	0.660
Environmental metric	Confidentiality requirement (*E_CR*)	Low (L)	0.5
		Medium (M)	1.0
		High (H)	1.51
	Integrity requirement (*E_IR*)	Low (L)	0.5
		Medium (M)	1.0
		High (H)	1.51
	Availability requirement (*E_AR*)	Low (L)	0.5
		Medium (M)	1.0
		High (H)	1.51
	Collateral damage potential (*E_CDP*)	None (N)	0.0
		Low (L)	0.1
		Low medium (LM)	0.3
		Medium high (MH)	0.4
		High (H)	0.5

(*E_AR*) and collateral damage potential (*E_CDP*). Note that the environmental metric group attribute 'Target Distribution' is not included as a separate variable but integrated into the 'E_CDP' variable. This is because within the problem context for which the model was initially developed (see Section 2), it is highly unlikely that the same vulnerability would be distributed across several system components as this violates the principles of robust design. However, if this principle is violated, there might be a vulnerability distribution issue but it was decided to handle this as part of functional design testing. Furthermore, it is the way in which vulnerabilities, whether single or multiple, affect the service level of the system which is of interest for safety- and mission-critical systems in general and the problem context discussed in this paper in particular. Therefore, target distribution is interpreted in the perspective of the damage potential associated with a particular vulnerability.

The ratings and rating values for all attributes from the CVSS are summarised in Table 2 for the purpose of estimating impact. Impact estimation uses a different updating schema to that used for estimating frequency. Firstly, the environmental metric attributes, which are context specific, are evaluated. Here, context specific refers to the security requirements of and the potential for damage to a particular system. This is independent of the vulnerabilities and is evaluated separately. It is also the reason why the impact of a specific vulnerability varies from system to system. Secondly, the impact information intrinsic to a vulnerability is evaluated. This information is given by means of base metric attributes and is linked to the vulnerability rather than to the system. To derive the impact on a particular system, the general vulnerability information provided by the base metric information must be interpreted in the context of the environment in which the system operates. Furthermore, the impact update schema used in the model is based on the assumption that there is only an impact if there is a relevant requirement (such as an asset with a value that will be affected). This is represented by a dependency between the impact variables (*B_C*, *B_I*, *B_A*) and the requirement variables (*E_CR*, *E_IR*, *E_AR*) in the impact part of the BBN (Fig. 4), i.e., impact depends on the security requirements of a specific system.

5. Example of use of the CVSS Risk Level Estimation Model

Referring to the communication trade-off decision described in Section 2, the L/MWD system produces, holds and transfers safety- and mission-critical data from the drilling rigs to support centres. When looking at the risks present in the system, there are several perspectives and several sources of fault introduction to consider (see Fig. 2). However, this example only looks at the trade-off between staying with dedicated and expensive communication links and opting for shared and, therefore, less expensive communication links (both alternatives are shown in Fig. 1). This trade-off does not consider the possible introduction of internal system faults as the sources of these are, in principle, the same in both cases. Hence, the analysis can be limited to the communication link and end-points. Furthermore, it is only the safety- and mission-critical data being transferred between the drilling rig and the support centres which is of concern.

As described in Section 4.1, Step 1 of the computational procedure of the CVSS Risk Level Estimation Model focuses on identifying potential vulnerabilities by means of passive and active vulnerability assessment. During the passive vulnerability assessment of the M/LWD system we examined vulnerability databases to check for recently reported problems relevant to the communication media category (in general, all layers in the communication protocol stack should be analysed but most communication-related vulnerabilities are on the link, network and transport layers). In parallel with this activity, we examined vulnerability databases to identify problems relevant to the communication end-points (both sender and receiver sides), and to the application and protocols used for the data transfer. We did not perform any active vulnerability assessment as no representative simulation environment could be established. As stated previously, parts of the assessment are for potential future communication solution, so no real-time scanning could be performed.

The Step 1 activities resulted in more than 20 potential vulnerabilities distributed over the communication link and the sending and receiving end-points. The receiving end-point is a central firewall in the DMZ of the support centre network which is a critical component in the communication scenario.

Step 2 of the computational procedure concerns estimating the frequency and impact of the vulnerabilities identified in Step 1 according to the CVSS metric attributes. In the following, we focus on the firewall mentioned above and examine one of the vulnerabilities that this firewall may exhibit and that significantly affect the overall risk level of the M/LWD data exchange. The CVSS information available in the NVD for this vulnerability is as follows: *B_AV = 'network'*, *B_AC = 'low'* and *B_AU = 'none'*. These are the base metric attribute variables that we use to derive the initial frequency estimate in the CVSS Risk Level Estimation Model (using the frequency part of the BBN in Fig. 4). Expert evaluation of this vulnerability reveals the following associated temporal metric attribute values: *T_E = 'functional'*, *T_RL = 'workaround'* and *T_RC = 'confirmed'*. These are the variables used to derive the frequency estimate update factor and that later are used to derive the resulting frequency estimate by combining these with the initial frequency estimate, as shown in Fig. 5.

Fig. 5 shows the initial frequency estimate, the update factor and the resulting frequency estimate all as probability distributions. The resulting frequency estimate is: *low* = 0.0, *medium* = 0.25 and *high* = 0.75 (see left side of the figure), which means that it is *three times more likely that the frequency is high than medium* (it is never low). This resulting frequency, always in the range [0.0, 1.0], means that there is a high chance (75%) that the vulnerability will be exploited. Also shown in Fig. 5 is that the ratings mentioned above are fed into the network as confirmed

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023

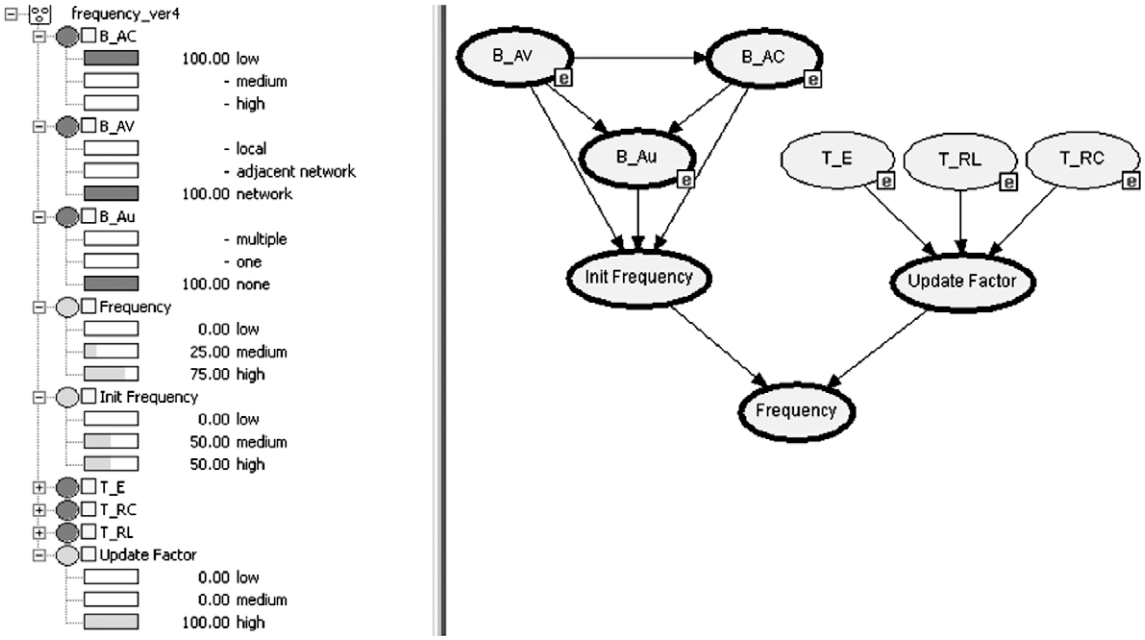

Fig. 5. Resulting frequency estimate after information has been inserted.

information or hard evidence. BBN, and hence the implementation of the CVSS Risk Level Estimation Model, deals with two types of information or evidence: (i) hard evidence (marked with a solid bar on the left-hand side of Fig. 5 and an 'e' attached to the relevant node on the right-hand side of Fig. 5) and (ii) soft evidence (marked with an 'f'). The difference between these two evidence or information types is that hard evidence represents an instantiation of a specific value for a particular node and this should be interpreted as being known or having been observed that the state of the node has this value. Soft evidence for a node represents any information collected that enables us to update the prior probability values for the states of the node. This information can be based on expert opinion, domain knowledge, experience and recommendations that an expert has acquired from standards or from a domain experts group. In any of these cases, the evidence (information) is propagated through the network by updating the prior probability distributions with the inserted information using a propagation (updating) algorithm. Details of evidence types and propagation algorithms can be found in Jensen (1996), Pourret et al. (2008) or the HUGIN™ user guide (Hugin, 2007a, b). Descriptions of how to evaluate knowledge, experience and recommendations of information sources such as experts, can be found in Ray and Chakraborty (2005) and Houmb (2007).

Note that the CVSS rating values given in Table 1 are used as the prior probability distributions, as described in Section 4.3. This is the main advantage of using the CVSS as the basis for the Risk Level Estimation Model and means that the multi-dimensional node probability matrices are pre-initialised using information provided by the CVSS. Hence, the use of the CVSS Risk Level Estimation Model is, in practice, reduced to the gathering and insertion of the available information, whether complete or not. Thus, the implementation of the model has two main advantages: (i) BBN as the implementation language allows for reasoning with incomplete information and for supporting security risk and cost trade-offs; and (ii) CVSS reduces the complexity of using the BBN model by providing details on the probabilistic relationships between the involved variables.

In order to calculate the impact we consider that the vulnerability has the following impact-related base metric attributes from CVSS: *B_C = 'complete'*, *B_I = 'none'* and *B_A = 'none'*, as shown at the upper left-hand side of Fig. 6. We then consider the relevant security requirements for the support centre firewall. These are: *E_CR = 'high'*, *E_IR = 'medium'* and *E_AR = 'medium'* and the collateral damage potential is: *E_CDP = 'low'*. Note that the CDP variable includes the target distribution information from the CVSS as discussed in Sections 3 and 4.4. Deriving the impact distribution according to the impact part of the CVSS Risk Level Estimation Model results in the impact estimate distribution: *low* = 0.4, *medium* = 0.3 and *high* = 0.3, also shown in Fig. 6. This resulting impact, always in the range [0.0, 1.0], means that the impact information is inconclusive as it is almost *as likely that the impact will be low as it is that it will be medium or high*. The reason for this is that, in addition to the collateral damage potential being low, there are no integrity and availability requirements for the integrity and availability impacts to affect. As stated in Section 4.4, there are several rules (reflecting assumptions made) employed when deriving the impact estimate using the model. In this example we have used the rule that there is no impact if there is no relevant requirement.

We have now derived both the frequency and impact estimate distributions. In Step 3 these two estimate distributions are combined into a risk level distribution, expressing the risk level that an exploitation of this particular vulnerability poses to the communication. In the example, the resulting frequency distribution is: [*low* = 0.0, *medium* = 0.25, *high* = 0.75], and the resulting impact distribution is: [*low* = 0.4, *medium* = 0.3, *high* = 0.3]. These distributions are not insightful for making decisions, such as whether it is better to stay with the dedicated communication link or to go for the other more open communication solution. Therefore, a higher-level distribution, i.e., at the level of the risk, is required. Of course, there are many other aspects involved when making such a decision as well as more vulnerabilities to consider. This example simply serves the purpose of demonstrating how to get an overview of the level of risk that the existence of a particular vulnerability may pose to a system. To get a system-wide overview, all vulnerabilities identified on all parts of the system (communication link and its sending and receiving end-points in this example) must be aggregated into a system-wide risk level distribution. This is done by first performing Steps 1 and 2 for all vulnerabilities separately and then by aggregating the resulting frequency and

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023

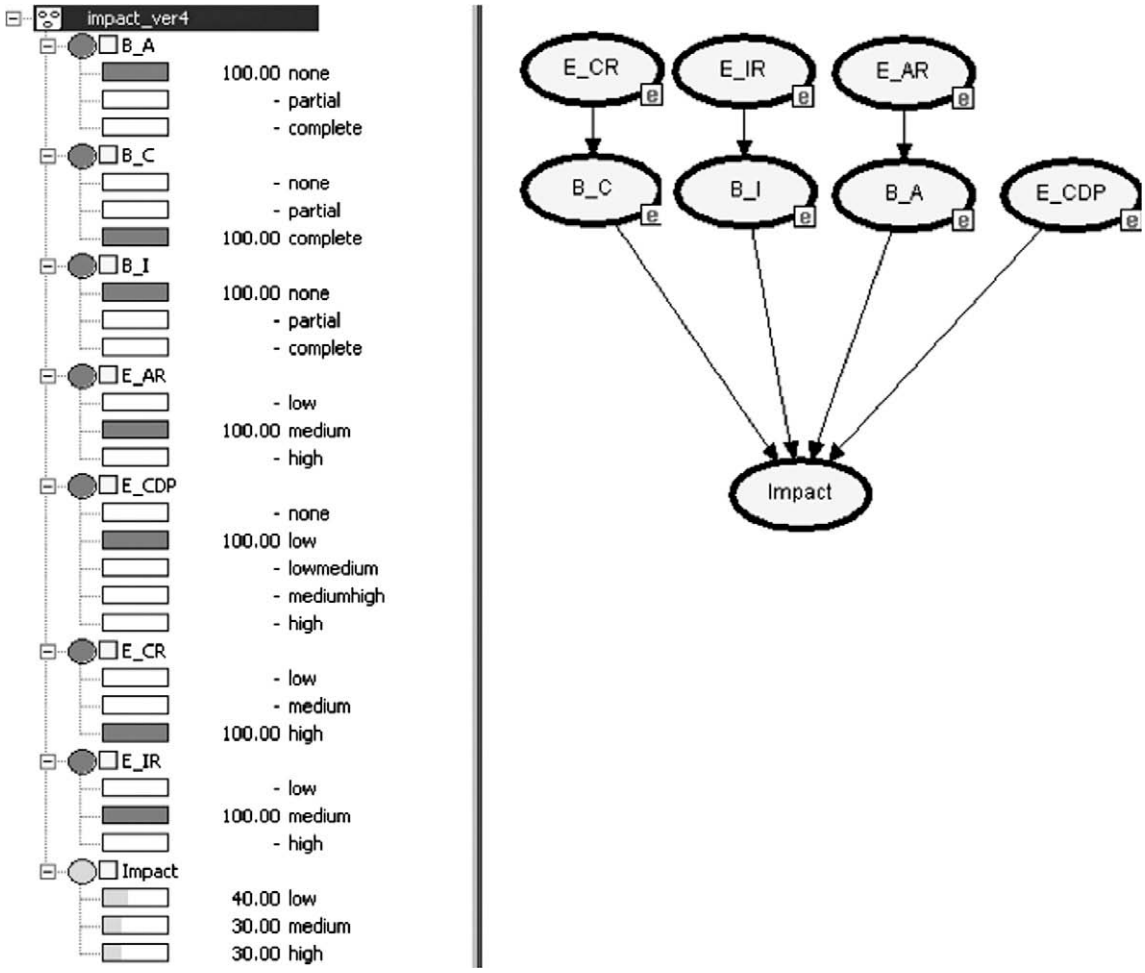

Fig. 6. Resulting impact estimate after information has been inserted.

impact estimate distributions into an overall risk level expression in Step 3. Alternatively, one can take the average of all frequency and impact estimates (note that important details may be overlooked when working with average values) or use a performance-based weighting aggregation as described in (Cooke and Goossens, 2000; Goossens et al., 2000). Currently, in the CVSS Risk Level Estimation Model we use the HUGIN^{TM} update algorithm when aggregating estimates from several vulnerabilities. This means that the frequency and impact estimates of a particular vulnerability become the prior distribution for the following vulnerability and so forth. We do not discuss this aspect further in this paper and refer the reader to Jensen (1996) and Pourret et al. (2008) for details on BBN evidence aggregation and propagation.

The resulting risk level estimate distribution for the vulnerability that we are considering is: *low* = 0.05, *medium* = 0.57 and *high* = 0.38. Note that as for frequency and impact, the risk level is always a value in the range [0.0, 1.0]. Interpreting this result identifies that the level of risk posed to the communication by the vulnerability is most likely to be *medium* (57% *chance*). It is also possible that the risk level will be *high* (38% *chance*). This risk level distribution is derived by means of frequency and impact information propagation to the target node, 'Risk Level', using the utility function specified in the 'Risk Level Utility'. This utility function specifies the rules determining the affect that various frequency and impact distributions have on the resulting risk level distribution. It can easily be updated as new knowledge or experience is gained. Currently, the utility function specifies that for the resulting risk level to be skewed towards the value 'high', both frequency and impact estimate distributions must be heavily skewed towards the value 'high'. The same applies to the risk value 'low', where both estimate distributions most be skewed towards the value 'low'. Note that the prior probability distribution for risk level is skewed towards the value 'medium'. To summarise for the example: the frequency estimate value is 'medium' with probability 0.25 and the impact estimate value is 'medium' with probability 0.3 and combining these two values using the prior probability distribution for risk level which is skewed towards the value 'medium', results in a risk level value of 'medium' with probability of 0.57. This result is reached even though frequency is in the value 'high' with a probability of 0.75 as the resulting impact estimate distribution is inconclusive (it could equally be any of the three values).

Looking at this vulnerability in isolation indicates that there is a need to secure at least the receiving end-point (the support centre firewall) if the more open communication model (right-hand side, Fig. 1) is to be used. However, this one vulnerability is not necessarily representative of the overall risk level. However, it does pinpoint the important aspect of examining and securing all parts of the communication and not merely the communication link itself using, for example, encryption.

At the end of the analysis, the trade-off involved is the willingness to: (i) assume a medium-to-high security risk and save on cost (the open communication option); (ii) not assume the security risk but maintain high communication cost (the dedication communication option); or (iii) take measures to reduce the risk to an acceptable level (e.g. by patching the vulnerability) while saving

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023

on the cost of communication (open communication option with additional security measures).

6. Related work

The Risk Level Estimation Model discussed in this paper concerns itself with controlling security risks. In particular, the model focuses on producing meaningful risk exposure expressions that a decision maker can use to make more informed trade-off decisions. The current strategies for controlling security risks are: (i) "penetration and patch", (ii) standards, (iii) security risk management/assessment and (iv) "wait and see". The latter is similar to the first and differs only in the fact that penetration and patch includes authorized activities such as tiger-team activity. "Wait and see" is a passive security strategy where problems are fixed if budget allows and only after the fact. This strategy is not suitable for safety- and mission-critical systems such as the M/LWD system discussed in this paper where the consequences may be catastrophic and non-repairable after the fact. Controlling risk is about gaining knowledge about the potential security problems and, whenever necessary and financial possible, taking the necessary preventive actions.

Standards provide domain knowledge for evaluating both the security and safety controls of systems. Examples of standards are: (i) ISO 15408:2007 Common Criteria for Information Technology Security Evaluation (ISO 14508, 2007) which includes a schema for certification of IT Products, in addition to security best practises and (ii) the ISO/IEC 27000 series which includes ISO/IEC27002, 2005 Information technology – Security techniques – Code of Practice for Information Security Management (ISO/IEC27002, 2005) for security, and (iii) IEC 61508, 1998 Functional safety of electrical/electronic/programmable electronic safety-related systems (IEC 61508, 1998) for safety. However, most evaluations are of a qualitative and subjective nature, heavily biased by the evaluator. Also, the underlying reasoning is often not made public, only the result of the evaluation. Hence, these evaluations rely heavily on the expertise and experience of the particular evaluator. These standards also only provide general advice and have a slow evolution process. The model discussed in this paper is not aimed at improving or setting best practices and does not require an evaluation or certification schema. The model emphasises the use of multiple experts and other information sources for estimating the variables involved and, from these, deriving risk level estimates. The model is based on an open best practice, the CVSS, which is regularly updated and which reveals the details behind the scores provided such as ratings and ratings values.

Risk assessment was initially developed within the safety domain but has since been adapted to security critical systems as security risk assessment. The three most relevant approaches are the OCTAVE framework (Alberts et al., 1999), CCTA Risk Analysis and Management Methodology (CRAMM) (Barber and Davey, 1992) and the CORAS framework (Stølen et al., 2002; CORAS Project, 2003). The OCTAVE framework was developed by the NSS Program at SEI and provides guidelines that enable organisations to develop appropriate protection strategies based on risks to critical information assets. CRAMM is an asset-driven strategy tailored to health-care information systems. The CORAS framework is based on the Australian/New Zealand Standard for Risk Management AN/NZS4360:2004 (AN/NZS4360, 2004), and is inspired by the asset-driven strategy of CRAMM. In addition, CORAS provides a security risk assessment documentation framework and specifies how to use models to assist in risk assessments. The main deficiency of these and other security risk assessment approaches is that the focus is not on trade-offs and calculated risks meaning that there has been no prior activity on determining what are acceptable risks based on budget, time and resource constraints. The CVSS Risk Estimation Model is built as a security trade-off decision-support engine that can be used, for example, to support a decision maker in balancing security with cost.

Security trade-off analysis, as discussed in (Houmb et al., 2005a, 2006), looks at security from a cost-benefit perspective considering both financial and project factors such as budget and time-to-market. However, the challenge is still to measure the risk level accurately. An example of such for the security attribute availability is provided in (Houmb et al., 2005b) where an availability estimation model based on system service levels is outlined. However, this model relies on experts to define the service levels, modelled as a state model, and to estimate the state transition rates. Furthermore, no method for aggregating several information sources, for estimating transition rates for example, is provided. The CVSS Risk Level Estimation Model can be used in the context of the service level concept from (Houmb et al., 2005a) as described in (Houmb and Franqueira, 2009) but is not restricted to it. Houmb and Franqueira (2009) describe the underlying equation sets used to estimate risk level in the CVSS Risk Level Estimation Model. These are derived from the CVSS and represent an interpretation of the CVSS equation sets in the context of frequency and impact estimation as described in Section 4 in this paper. The implementation of the model as a BBN topology was first described in Houmb et al. (2008). The reason for using BBN as the implementation language is that it allows for multiple information sources, enables the use of risk information on multiple abstraction levels and allows for a more seamless aggregation of vulnerabilities as the vulnerability information can be inserted directly into the BBN topology without the prior establishment of a service level model.

There are few relevant works regarding the CVSS and its use. Chen et al. (2007) and Chen (2007) discuss an approach for measuring security investment benefits for Commercial-Off-The-Shelf (COTS) software systems using CVSS. The argument made by the authors is that the CVSS may be misleading as it does not take the context of the values into account. Rather than using the environmental metric group attributes of CVSS to give context to the values, the authors propose an Analytic Hierarchy Process (AHP) that focuses on stakeholders-values such as the productivity, reputation and privacy of systems. However, both productivity and reputation are of a subjective nature and equally hard to estimate as the environmental metric group attributes as different stakeholders may have different perceptions on the extent that a particular vulnerability might affect, for example, productivity. Our opinion is that it is better to use the environmental metric attributes from the CVSS as stakeholders often find it just as easy to evaluate confidentiality, integrity and availability as productivity, reputation and privacy and as it is valuable in itself if a standard set of environmental attributes can be widely adopted.

An approach to vulnerability prioritisation using fuzzy risk analysis is presented in Dondo (2008) where the asset value (AV) is used to derive the risk level or risks to a system and is assumed given. The approach derives risk level from the CVSS base metric attributes, a measure of time from when the vulnerability was reported and an assessment of the safeguards already in the system. The author applies fuzzy rules to compute impact (I) and likelihood (L) and, from these, derive risk level as: $AV \times I \times L$. This approach is similar to that of the Risk Level Estimation Model described in this paper but differs in that it uses asset value and safeguards to estimate the risk level rather than the temporal and environmental metric group attributes specified by the CVSS. Asset value is not necessarily easy to evaluate and is context- and stakeholder-specific. The CVSS Risk Level Estimation model uses the CVSS temporal and environmental information which is easily accessible and publicly-available context information that is regularly updated, has a stable data model and is used by many commercial parties. Also,

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023

the underlying equations within the CVSS (that is, how the CVSS scores or values are computed) are well known.

Sawilla and Ou (2008) use two attributes from the CVSS to prioritise vulnerabilities under the perspective of attackers. These are: access complexity (*B_AC*) and exploitability tools and techniques (*T_E*). However, instead of using the rating values directly from the CVSS as we do in the CVSS Risk Estimation Model, they use their own values. For example, they use the following probabilities that an attacker will successfully exploit a vulnerability for the attribute, *T_E*: Unproven (0.01), Proof-of-concept (0.40), Functional (0.80) and High (0.99). We believe that keeping CVSS ratings and rating values offers a clear advantage as it maintains compliance with the CVSS and, hence, can easily adopt any updates and extensions to the CVSS.

7. Conclusion

Controlling security risks is important for safety- and mission-critical systems as security attacks might lead to serious and even non-repairable safety and core mission consequences. This paper presents the CVSS Risk Level Estimation Model which addresses parts of the challenge of controlling security risks. The model computes the overall risk level of a system based on frequency and impact estimates derived from a re-arranged version of the CVSS attributes over all vulnerabilities present, or potentially present, in a system. The CVSS consists of three metric groups: base, temporal and environmental. The model uses attributes from the base and temporal metric groups to estimate frequency and attributes from the base and environmental metric groups to estimate impact. The model is implemented as a BBN topology and, in this paper, is applied to the M/LWD system for drilling rigs as an example of its use.

The CVSS provides rating values in all attribute categories for each given attribute in all three metric groups. The CVSS Risk Level Estimation Model uses these rating values as prior probability distributions in its BBN implementation. This means that the values specify the conditional probabilities to be used when propagating frequency and impact variable information and from these derive the risk level in the BBN topology. When new and relevant information is available regarding the relations or dependencies between the variables involved, such as changes in temporal attribute ratings, these can be inserted into the appropriate part of the BBN topology to update the prior probability distributions by means of propagation along the edges of the network to all connected nodes. This is how the prior probability distributions of the model, which defines the probabilistic (quantitative) relationships between the variables, are updated. The structure of the BBN topology (i.e., that there is a relationship between two variables) is expressed in the graphical representation of the model. Both aspects are included in the actual implementation of the model and, together, make it easy to evolve the model. When using the model for risk level estimations, information and observations are inserted into the relevant nodes as evidence. Note that information may be inserted into any level in the topology and that the model allows for both soft and hard evidence, meaning that all types of observation and belief (expressed as single values for observations and as probability distributions for beliefs) are valid input information.

It is important to note, however, that the outcome of a BBN computation is very sensitive to the configuration of the BBN topology with its subnets and associated probability distribution functions. Hence, the topology should be constructed carefully to ensure representative results. Also, different BBN topologies might interpret the same observations similarly or differently depending on which nodes in the network are sensitive, i.e., which nodes are given high priority by the computation engine. These are called neighbouring networks. The reason for the latter is that the HUGIN™ evidence propagation algorithm first reduces the topology according to a set of rules and then transfers the BBN topology into a set of trees that are computed separately. Therefore, understanding how the evidence propagation works is crucial in constructing a representative BBN topology. In practice, sensitivity analysis is performed to assist the construction process by validating that nodes identified as being of high importance are, in fact, that important. Note that only the principles of this information propagation have been explained in this paper. The reader should consult Jensen (1996) and Pourret et al. (2008) for the theoretical background and Houmb (2007) for a more extensive example.

Future work will involve amending the BBN-based CVSS Risk Level Estimation Model with concrete guidelines on effective and accurate ways of aggregating alternative information sources of frequency and impact estimation such as vendor-specific vulnerability bulletin lists, attack reports (security bulletin lists, news groups, etc.) and expert opinion. Currently, all types of information are given equal importance. This will require information aggregation across sources for which we have developed a trust-based information aggregation schema, that handle several information source categories and that derive a trustworthiness weighting for each information source. This weighting measures the relative importance of one information source in respect to other information sources. Future work will also include a series of practical field studies using the model at our industrial partners. Besides this, we also plan to merge the CVSS Risk Level Estimation Model into a security solution trade-off analysis (Houmb, 2007) as part of a larger security budgeting support tool that we are building. An attempt to do this is currently in progress as part of a field study.

References

Alberts, C., Behrens, S., Pethia, R., Wilson, W., 1999. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0, Technical Report, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

Aldred, W., Belaskie, J., Isangulov, R., Crockett, B., Edmontson, B., Florence, F., Srinivasan, S., 2005. Changing the way we drill. Schlumberger Oilfield Review 17 (1), 42–49.

Australian/New Zealand Standards, 2004. AS/NZS 4360:2004 Risk Management.

Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, G., 2004. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing 1 (1), 11–33.

Barber, B., Davey, J., 1992. The use of the CCTA risk analysis and management methodology CRAMM in health information systems. In: Lun, K.C., Degoulet, P., Piemme, T.E., Rienhoff, O. (Eds.), Proceedings of MEDINFO'92. North Holland Publishing Co., Amsterdam, pp. 1589–1593.

Chen, Y., Boehm, B., Sheppard, L., 2007. Measuring security investment benefit for off the shelf software systems – a stakeholder value driven approach. In: Online Proceedings of Sixth Workshop on the Economics of Information Security (WEIS 2007), June 25–27, New Hampshire, USA, 18 p. <http://weis07.infosecon.net/papers/46.pdf> (last visited September 2008).

Chen, Y., 2007. Stakeholder value driven threat modeling for off the shelf based systems. In: Proceedings of the 29th International Conference on Software Engineering (ICSE 2007), Washington, DC, USA, IEEE Computer Society, pp. 91–92.

Clark, B., Bonner, S.D., Jundt, J., Luling, M., 1996. Logging while drilling apparatus with blade mounted electrode for determining resistivity of surrounding formation. United States Patent 5339036, August 1996.

Cooke, R., 1991. Experts in Uncertainty: Opinion and Subjective Probability in Science. Oxford University Press.

Cooke, R., Goossens, L., 2000. Procedures guide for structured expert judgment in accident consequence modelling. Radiation Protection and Dosimetry 90 (3), 303–311.

CORAS Project, 2003. CORAS Project Web Site. <http://coras.sourceforge.net/> (last visited December 2008).

CVSS calculator, 2007. <http://nvd.nist.gov/cvss.cfm> (last visited October 2008).

Dondo, M., 2008. A vulnerability prioritization system using a fuzzy risk analysis approach. In: Proceedings of the IFIP TC 11 23rd International Information Security Conference, vol. 278, IFIP International Federation for Information Processing, Springer, November 4–6, pp. 525–539.

Gardner, W.R., Merchant, G.A., 1996. Nonlinear equalizer for measurement while drilling telemetry system. United States Patent 5490121, February 1996.

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023

Goossens, L., Harper, F., Kraan, B., Meacutetivier, H., 2000. Expert judgement for a probabilistic accident consequence uncertainty analysis. Radiation Protection and Dosimetry 90 (3), 295–303.

Gran, B.A., 2002. The use of Bayesian Belief Networks for combining disparate sources of information in the safety assessment of software based systems. Doctoral of Engineering Thesis 2002:35, Department of Mathematical Science, Norwegian University of Science and Technology.

Haines, L., Darbonne, N., Ghiselin, D., Schempf, J.F., 2006. Service and Supply, An Investor Primer Supplement to Oil and Gas Investor. Hart Energy Publishing LP, Houston, Texas, USA. pp. 12-19.

Health and Safety Executive, 2009a. <http://www.hse.gov.uk/statistics/tables/occ1.htm> (last visited April 2009a).

Health and Safety Executive, 2009b. <http://www.hse.gov.uk/offshore/statistics/hsr0708.pdf> (last visited April 2009b).

Houmb, S.H., 2007. Decision Support for Choice of Security Solution: The Aspect-Oriented Risk Driven Development (AORDD) Framework. Ph.D. Dissertation, Norwegian University of Science and Technology (NTNU), November 2007.

Houmb, S.H., Franqueira, V.N.L., 2009. Estimating ToE risk level using CVSS, In: Proceeding of the Forth International Conference on Availability, Reliability and Security (ARES 2009), IEEE Computer Society, Fukuoka, Japan, March 16–19, pp. 718–725.

Houmb, S.H., Georg, G., France, R., Bieman, J., Jürjens, J., 2005a. Cost-benefit trade-off analysis using bbn for aspect-oriented risk-driven development. In: Proceedings of the 10th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 2005), Shanghai, China, pp. 195–204.

Houmb, S.H., Georg, G., France, R., Reddy, R., Bieman, J., 2005b. 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, vol. X: 2nd Symposium on Risk Management and Cyber-Informatics (RMCI'05), International Institute of Informatics and Systemics, Orlando, Florida, USA, pp. 396–403.

Houmb, S.H., Georg, G., Jürjens, J., France, R., 2006. An integrated security verification and security solution design trade-off analysis. Integrating Security and Software Engineering: Advances and Future Visions, 190–219 (Chapter 9).

Houmb, S.H., Franqueira, V.N.L., Engum, E.A., 2008. Estimating impact and frequency of risks to safety and mission critical systems using CVSS. In: ISSRE 2008 Supplemental Proceedings: 1st Workshop on Dependable Software Engineering, 11 November 2008, Seattle, US, IEEE CS Conference Proceedings, IEEE Computer Society Press, ISBN 978-1-4244-3417-6, 6 p.

Hugin Expert A/S, Hugin User Guide, Part of HUGIN Version 6.8, 2007a. <http://www.hugin.com> (downloaded June 2007).

Hugin Expert A/S, HUGIN Version 6.8, 2007b. <http://www.hugin.com> (downloaded June 2007).

IEC 61508:1998. Functional safety of electrical/electronic/programmable electronic safety-related systems.

ISO/IEC 27001:2005. Information technology – security techniques – information security management systems – requirements.

ISO/IEC 27002:2005. Information technology – security techniques – code of practice for information security management.

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.

Jensen, F., 1996. An Introduction to Bayesian Network. UCL Press, University College London.

Jonsson, E., 2006. Towards an integrated conceptual model of security and dependability. In: Proceedings of the First IEEE International Conference on Availability, Reliability and Security (ARES 2006), pp. 646–653. ISBN:0-7659-2567-9.

Jürjens, J., 2005. Secure Systems Development with UML. Springer-Verlag, Berlin Heidelberg, New York.

Laakso, M., Takanen, A., Røning, J., 1999. The vulnerability process: a tiger team approach to resolving vulnerability cases. In: Proceedings of the 11th FIRST Conference on Computer Security Incident Handling and Response, pp. 13–18.

Laprie, J.C., 1992. Dependability: Basic Concepts and Terminology. Springer-Verlag.

Mell, P., Scarfone, K., Romanosky, S., 2007. 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> (last visited December 2008).

Minette, D.C., 1995. Method for analysing formation data from a formation evaluation measurement-while-drilling logging tool. United States Patent 5397893, March 1995.

National Vulnerability Database (NVD) Version 2, 2009. <http://nvd.nist.gov/> (last visited January 2009).

Nessus, 2008. Tenable network security: the Nessus security scanner. <http://www.nessus.org> (last visited December 2008).

National Institute of Standards and Technology (NIST), 2009. <http://www.nist.gov/> (last visited January 2009).

Pourret, O., Na, P., Marcot, B., 2008. Bayesian Networks: A Practical Guide to Applications (Statistics in Practice). John Wiley & Sons Ltd.. ISBN:978-0-470-06030-8.

Ray I., Chakraborty, S., 2005. A vector model of trust for developing trustworthy systems, In: Samarati, P., Ryan, P., Gollmann, D., Molva, R. (Eds.), Proceedings of the 9th European Symposium on Research in Computer Security (ESORICS 2005), pp. 260–275.

Rigzone.com, Offshore Rig Day Rates, 2009. <http://www.rigzone.com/data/dayrates/> (last visited January 2009).

Sawilla, R.E., Ou, X., 2008. Identifying critical attack assets in dependency attack graphs. In: ESORICS '08: Proceedings of the 13th European Symposium on Research in Computer Security, Malaga, Spain, Springer-Verlag, pp. 18–34. ISBN:978-3-540-88312-8.

Schlumberger Remote Operations Management, 2009. <http://www.slb.com/content/services/drilling/rtd/rom.asp> (last visited January 2009).

Spitzner, L., 2003. Honeypot – Tracking Hackers. Addison-Wesley.

Stølen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B., Houmb, S.H., Stamatiou, Y., Aagedal, J.Ø., 2002. Model-based risk assessment in a component-based software engineering process: the CORAS approach to identify security risks. In: Business Component-Based Software Engineering. Kluwer, pp. 189–207.

Wright, P.D., 1991. Methods and apparatus for evaluating formation characteristics while drilling a borehole through earth formations. United States Patent 5017778, May 1991.

Siv Hilde Houmb works as a researcher focusing on security issues in the Service Platform group at Telenor R&I, Norway. She received her Ph.D. in 2007 from the University of Science and Technology (NTNU), Trondheim, Norway. Her research interests are in risk estimation, security evaluation and certification, security standards and security decision support methodologies and techniques for choosing between sets of security solutions for critical information systems. Chosen solutions must be able to balance contracted security levels, available resources and end-user expectations while still fulfilling financial, project and development constraints.

Virginia N.L. Franqueira is currently a Ph.D. candidate at the University of Twente, The Netherlands. Her main research interests are network security, attack graphs, and quantification of risk derived from vulnerabilities present in networks. She received her M.Sc. in Computer Science from the Federal University of Espirito Santo, Brazil, with a thesis in the field of Combinatorial Optimisation applied to a routing problem and gained industrial experience working at a Xerox Software Development Centre in Vitoria, Brazil, in the areas of System Test and Business Proposals.

Erlend A. Engum holds a masters degree in computer science from the Norwegian University of Science and Technology (NTNU), Norway. Since graduating he has worked for Schlumberger Drilling and Measurements as a field engineer providing Measurement and Logging While Drilling services to clients around the world. He has worked both on offshore rigs and in operation support centres. His research interests are in how to use information systems to transfer knowledge effectively, development of safe and dependable systems and software development process improvements.

Please cite this article in press as: Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software (2009), doi:10.1016/j.jss.2009.08.023