The Journal of Systems and Software 83 (2010) 1622–1634

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 23 August 2009

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