Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

Metrics for Information Security - A literature review

Raj Sharman
State University of New York

Raghav Rao
State University of New York, Buffalo

Shambhu Upadhyaya
State University of New York

Metrics for Information Security – A literature review

Raj Sharman
School of Management,
Department of Management Science and Systems,
State University of New York, Buffalo,
New York 14260, USA
rsharman@buffalo.edu

Raghav H. Rao
School of Management,
Department of Management Science and Systems,
State University of New York, Buffalo,
New York 14260, USA
mgmtrao@buffalo.edu

Shambhu Upadhyaya
Dept. of Computer Science & Engineering,
State University of New York, Buffalo,
New York 14260, USA
shambhu@cse.buffalo.edu

ABSTRACT

It is important to know how vulnerable systems are for a wide variety of reasons. Information Systems managers have the duty to advise senior management of the level of risks faced by the information systems. Therefore an assessment of the level of risk is necessary. Research work in this area is in its infancy. Further, the efforts are varied and deal with different aspects of the issue. There is no coherent approach. This paper provides a review of the literature and will be presenting a framework for analysis and development of metrics for security at the conference.

.

Keywords

Security Metrics, reliability, Vulnerability Analysis, Security Policy

INTRODUCTION

We are increasingly becoming a connected world. Our judgment as a people is increasingly leading us to conclude that to be electronically connected is better than to be isolated. Business-to-Business and Business-to-Consumer transactions have increased better than Moore's law expectations. We have let the public roads come to the doorstep of our systems (personal and corporate). This has placed our systems at risk. They are more vulnerable now. We have moved past wondering if our systems have become more vulnerable. The more relevant question to ask is how vulnerable is our data, the processes and the system. What is the risk? To answer these questions we need to have a yardstick by which we can measure. This yardstick is what we call metrics for measuring security. The presumptive understanding is that "if something can't be measured, it can't be managed" (Craft, 2000).

According to a recent survey conducted by Berinato and Cosgrove (2003) for CIO Magazine and PriceWaterhouseCooper, although seven out of ten survey respondents used intrusion detection systems, eight of ten used firewalls, and nine of ten used antivirus software, only 50% of adverse events were detected through those technologies or through security service providers managing those technologies for a company. The other half were detected the hard way—by customers, colleagues or news outlets alerting the company of a breach; or worse yet, by the damages the event caused. The question of how to measure the vulnerability of our information system remains dominant. A metric is necessary so that information security could include a risk management philosophy.

According to NIST Report sp800-55, security metrics measure the accomplishment of performance goals and objectives by quantifying the level of implementation of the security controls and the effectiveness and efficiency of the controls, analyzing the adequacy of security policies, processes and products and identifying possible corrective actions and/or improvements. The NIST Report sp800-55 provides further elaboration that a good set of metrics must yield quantifiable information (percentages, averages, and numbers), the data supporting the metrics needs to be unambiguous, easy to obtain and interpret and only repeatable processes should be considered for measurement. Metrics must be useful for tracking performance and directing resources. The goals and objectives of a company must be clearly identified and prioritized to ensure that the measurable aspects of security performance correspond to the operational priorities of the organization.

Requirements for securing and evaluating IT systems are included in a number of laws, including the Clinger-Cohen Act, the Government Performance and Results Act, the Government Paperwork Elimination Act and the Federal Information Security Management Act. These laws do not specify how the evaluation is to be done, and the NIST document provides guidance on developing and using metrics to do this job according to William Jackson (2003). However, the actual metrics and metrics development at a detail level is not provided.

Research in this area is in its infancy. The discipline is largely too young and unscientific. The unanswered questions relate to deciding what and how to measure? What is the quantification? This paper is devoted to providing a survey of the literature in the area of metrics for security. Metrics can be viewed from different perspectives. For example, Bartlett (2000) views security metrics as consisting of three categories: people, operations & training, equipment & infrastructure. However, in OUR approach we categorize the research literature as being either dealing with behavioral policy compliance issues or with technical issues. This categorization can also be viewed as goal based and process based. Section-II is devoted to metrics that that deal with policy compliance issues, while Section-III is devoted to papers that focus on technical metrics based on empirical or analytical methods. Section-IV provides a conclusion.

METRICS BASED ON POLICY COMPLIANCE

The papers in this area deal with metrics that tend to parameterize the percentage of security policies in place that are complied with. Much of the audit based metrics do not specify what needs to be measured; the guidance is more in the form of policy statements. Suggested metrics include industry standard specifications of security policy such as the RAND report and other standards published by federal & private agencies and standard-setting bodies such as NIST. The policy based metric usually covers the entire information systems and not part of the system. In this aspect, these are much more comprehensive than most of the metrics currently proposed using empirical or analytical methods. Policy and qualitative assessments also include gap analysis, where the risks are assessed. Policy based metrics include percentage compliance with security policies, authentication, policies, percentage of operational and business units within an organization have done a risk assessment and gap analysis, etc.

According to Dunbar (2000), some examples are metrics such as: 95% of your Information Assets have Information Owners identified; 83% of your Information Assets have been classified; 74% of your desktop computers have been identified as high risk; 90% of your business units have completed an Information Security Gap Analysis this quarter, etc. An example of this is the Information Security Evaluation Model (ISEM) Model.

In short, the percentage of compliance to security and audit polices is used as a yardstick to get a handle on a systems' vulnerability. According to Jennifer Bayuk (2000) of Bear Stearns, System audit is the process of verifying that management has achieved a designated set of industry standard control objectives. Audit steps specify the actions that an auditor will take to independently gather evidence of activity established by management that contributes to control objectives. Multiple audit steps are usually required to cover a given control objective completely. Audit based approaches usually deal with strategy, policy, awareness, implementation, monitoring and compliance with regards to Identification, Authentication and Access, Security of Online Access to Data, User Account Management, Management Review of User Accounts, User Control of User Accounts, Security Surveillance, Data Classification, Central Identification & Access Rights Management, Violation & Security Activity Reports, Incident Handling, Firewall Architectures, Connections with Public Networks, etc.

The limitations of such measures are that the actual measure of the risk is unknown. There is great reliance on the efficacy of policies that are at best good practices. Good practices reduce risks against known dangers. However, there is no measure of how these policies help deter intrusion, and therefore compliance may not be a good measure of vulnerability. Non-compliance implies greater risk and in that there is merit to such measures. Coming up with good guidelines for every aspect of the system that provides a measure of reliability is a problem. The details of what software protection scheme or program to use is not spelled out in such measures. Dr. Stuart Katzke (2000) proposed a model showing the relationship of objects (being measured (e.g., product, system, security program effectiveness, personal and organizational professional competence)), security objectives (the object is being measured against (i.e., attempting to meet)), and the processes to measure them.

Heim (2000) describes the audit based metric called FISCAM (Federal Information System Controls Audit Manual) which covers six control areas: security program planning / management, access control, application software, development & change control software and practices, system software, segregation of duties, service continuity. This model is comprehensive but there is no measure on how a practice is. Even Best Practices may be suspect in a discipline that is in its infancy.

TECHNICAL METRICS

Technical metrics are created using both empirical and analytical methods.

According to Brocklehurst et al. (1994), ideally, a measure of the security of a system should capture quantitatively the intuitive notion of 'the ability of the system to resist attack'. That is, it should be operational, reflecting the degree to which the system can be expected to remain free of security breaches under particular conditions of operation (including attack). Instead, current security levels at best merely reflect the extensiveness of safeguards introduced during the design and development of a system. While we might expect a system developed to a higher level than another to exhibit 'more secure behavior' in operation, this cannot be guaranteed; more particularly, we cannot infer what the actual security behavior will be from knowledge of such level. In Brocklehurst et al. (1994), the authors discuss similarities between reliability and security with the intention of working towards measures of 'operational security' similar to those that we have for reliability of systems. Very informally, these measures could involve expressions such as the rate of occurrence of security breaches (cf. rate of occurrence of failures in reliability), or the probability that a specified 'mission' can be accomplished without a security breach (cf. reliability function).

According to Olovsson et al (1993) it is in most contexts not feasible to guarantee that a system is 100% secure. Measures and predictions of operational security of computer systems are therefore obviously of interest to any owner of a system which is a candidate for potential intrusion. Such measures would allow assessment of current and future expected loss to the system owner due to security breaches in a given attacking environment and at a given level of protection. Littlewood et al. (1991) suggest a probabilistic approach to modeling operational security, analogous to that used in reliability. It is clear that empirical data would be useful in deriving a plausible probabilistic approach to security modeling. Such data can be acquired experimentally, by allowing a group of selected people to perform security attacks on a given computer system in a controlled way. The attack process can then be monitored and relevant data recorded.

Empirical efforts are limited by the knowledge of the people who participate in exploiting the weakness of the system. Further, it is difficult for a controlled group to behave as hackers, intruders, etc. who have malicious intent. So the metrics developed on the basis of such empirical evidence is limited in its ability to capture the vulnerability of the system.

As computer systems become more complex and more widely distributed, it is becoming increasingly difficult to remove all the vulnerabilities that can potentially be exploited by intruders (Singh et al., 2002). Before intrusion tolerance is accepted as an approach to security, there must be quantitative techniques to measure its efficacy. However, there have been very few attempts at quantitative validation of intrusion-tolerant systems or, for that matter, of security in general. Singh et al (2002) demonstrate an approach to compute an intrusion metric by using stochastic activity networks to quantitatively validate an

intrusion-tolerant replication management system. They characterize the intrusion tolerance provided by the system through several measures defined on the model, and study variations in these measures in response to changes in system parameters to evaluate the relative merits of various design choices.

Evans (2001) has used the classical Kolmogorov complexity measure in his development of a security metric and has modified it to the security context. The problem of Information Assurance is approached from the point of view of Kolmogorov Complexity and Minimum Message Length criteria to detect abnormal system behavior. Data and process vulnerabilities are put forward as two different dimensions of vulnerability that can be discussed in terms of Kolmogorov Complexity.

Tanna et al. (2004), in another study, develop a security metric for assessing the vulnerability of electronic bill presentation and payment systems (EBPPS). They take a workflow approach to analyzing business processes. They consider the system architecture needed for the EBPP systems. At each node point, they analyze the vulnerability for each type of threat. An overall metric is computed by aggregation on the vulnerabilities at each node. The probability of a compromise for each type of threat is determined by seeking expert opinion. The cost value of failure is also taken into account. The data is obtained by eliciting information from experts.

CONCLUSION

This paper is part of an ongoing broad effort to develop a comprehensive metric for workflow systems. Due to restrictions on word count other material that readers may have found interesting as well was not included. A framework is being completed and this will be presented along with a more detailed analysis of the state of the art at the conference.

REFERENCES

1. Bayuk, J. (2002), Information Security Metrics - An Audit-Based Approach, *Computer System Security and Privacy Advisory Board (CSSPAB) workshop on security metrics*, June 13-15.
2. Brocklehurst, S., Olovsson, T., Littlewood, B., Jonsson E. (1994), "On Measurement of Operational Security", *Compas '94, proc. Ninth ann. IEEE Conf. computer Assurance, Gaithersburg, ISBN 0-7803-1855-2, IEEE Conf. Computer Society,* pp.257-266.
3. Dacier, M., Deswarte, Y., Kaniche, M. (1994) *"Quantitative Assessment of Operational Security: Models and Tools",* Technical Report 96493, LAAS, 1994.
4. Evans, S., Bush, S., Hershey, J. (2001), "Information assurance through Kolmogorov complexity," in *DARPA Information Survivability Conference and Exposition II (DISCEX-II)*
5. Heim, D. (2000), "Overview of FISCAM", *Computer System Security and Privacy Advisory Board (CSSPAB) workshop on security metrics*, June 13-15.
6. Katzke, S. (2000), "Security Metrics - What Are They?", *Computer System Security and Privacy Advisory Board (CSSPAB) workshop on security metrics*, National Security Agency, June 13-15, 2000.
7. Moore, A., Ellison R., Linger, R. (2001), "Attack Modeling for Information Security and Survivability", *Carnegie Mellon Technical Note CMU/SEI-2001-TN-001.*
8. Olovsson, T., Jonsson, E., Brocklehurst, S., Littlewood, B. (1993), "Data Collection for Security Fault Forecasting: Pilot Experiment" , *Technical Report no. 167, Dept. of Computer Eng., Chalmers Univ. of Technology, and ESPRIT/BRA* Project no. 6362 (PDCS2) First Year Report, Toulouse, pp. 515-540
9. Singh, S., Cukier, M., Sanders, W.H. (2003), "Probabilistic Validation of an Intrusion-Tolerant Replication System", *Master's thesis, University of Illinois at Urbana-Champaign*
10. Smith, L. (2002), "Cryptographic Algorithm Metrics", *Computer System Security and Privacy Advisory Board (CSSPAB) workshop on security metrics,* Institute for Defense Analysis June 13-15 2000.
11. Tanna, G., Gupta, M., Rao, H.R., Upadhyaya, S. (2004), "Information Assurance Metric Development Framework for Electronic Bill Presentation and Payment Systems using Transaction and Workflow Analysis", *under review, DSS,* 2004.