International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

DEVELOPING SECURITY METRICS FOR INFORMATION SECURITY MEASUREMENT SYSTEM

Ms. Deepti Juneja Ms. Kavita Arora Ms. Sonia Duggal

Asst. Prof., Faculty of Business and Computer applications

Manav Rachna International University, Faridabad.

Abstract

This paper covers the basic aspects of security metrics. It provides a definition of security metrics explains their value, discusses various aspects or issues in developing the security metrics and design considerations for information security measurement systems. More than 100 years ago, Lord Kelvin insightfully observed that measurement is vital to deep knowledge and understanding in physical science. During the last few decades, researchers have made various attempts to develop measures and systems of measurement for computer security with varying degrees of success. This paper provides an overview of the security metrics area and looks at possible avenues of measuring the security metrics.

Keywords: Design considerations, Measurement, Metrics management, Security metrics

1. Introduction

A metric implies a system of measurement that is based on quantifiable measures. Good metrics are those that are SMART, i.e. specific, measurable, achievable, repeatable, and timedependent. Useful metrics indicate the degree to which security goals, such as data confidentiality, are being met, and they drive actions taken to improve an organization's overall security program.

Measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time. Measurements are generated by counting; metrics are generated from analysis.

In other words, measurements are objective raw data and metrics are either objective or subjective human interpretations of those data. The method of measurement that is employed should be reproducible, and should achieve the same result when performed independently by different competent evaluators. Also, the result should be repeatable, so that a second assessment by the original team of evaluators produces the same result. A method of measurement used to determine the unit of a quantity could be a measuring instrument, a reference material, or a measuring system. The measurement of an information system for security involves the application of a method of measurement to one or more parts of the system that have an assessable security property in order to obtain a measured value of measurements should be timely and relevant to the organization.

2. Background

The term "security metrics" is used often today, but with a range of meanings and interpretations.

> "Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. The purpose of measuring performance is to monitor the status of measured

> activities and facilitate improvement in those activities by applying corrective actions, based on observed measurements. … While a case can be made for using different terms for more detailed and aggregated items, such as 'metrics' and 'measures,' this document uses these terms interchangeably." [Swa03]
>
> "Measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time. Measurements are generated by counting; metrics are generated from analysis. In other words, measurements are objective raw data and metrics are either objective or subjective human interpretations of those data." [Pay06]

For information system security, the measures are concerned with aspects of the system that contribute to its security. That is, security metrics involve the application of a method of measurement to one or more entities of a system that possess an assessable security property to obtain a measured value.

3. Metric lifecycle

The business logic associated with a metric follows a simple processing pattern:

- Create: Obtain primary input data from one or more authoritative providers, including commercial products or homegrown customer applications.

- Calculate: Apply a series of analytic operations (called actions) on the primary data to derive a result and store the result in the metric results database in the form of one or more rows in a table.

- Communicate: Communicate the metric results in any of the following formats: default visualization, email notification, email alert based upon detection of some policy violation.

4. Security Metrics Management: More than measurement

A metric produces results that are stored in a specified metric database which is accessible via standard SQL and JDBC interfaces to support the following functions.

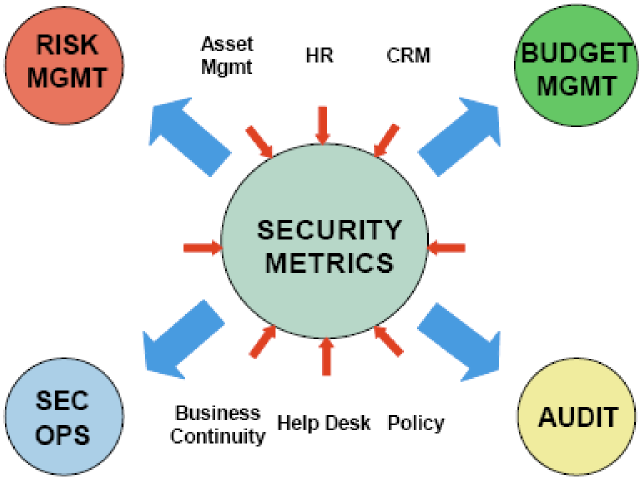

Figure 1: Security Metrics Management: More than Measurement

:

- Risk Management: Metrics that compute threat probability, vulnerability, Counter measure coverage and asset value yield results that can be used to model risk.

- Budget Management: Metrics that measure level of effort, impact, and available can be transformed into dollar values for the purpose of establishing budgets as well as computing return on investment.

- Audit & Compliance Assessment (Internal or External): Metrics that measure policy compliance for individual as well as groups of definitions yield results that can enhance reports generated by compliance tools.

- Security Operations: Metrics that accumulate data over time can be used to identify trends that suggest specific actions to be taken by data center operations staff.

5. Some pragmatic design considerations for information security measurement systems

1. *Which* things are we going to measure?

This is clearly an important issue but in practice identifying the right metrics is really tricky. We can achieve a lot without expensive solutions or elaborate processes. The true measure of availability, for instance, is the amount of time that an IT service is fully available to the business, expressed as a proportion of the time the business needs that service.

2. *How* will we measure things?

This raises some supplemental questions: where will the data come from and where will they be stored? If the source information is not already captured and available to you, you will need to put in place the processes to gather it. The KISS (Keep It Simple Stupid) principle is helpful: start by making use of readily available information and extend the data collection later if you need to.

3. How will we report?

What do senior management actually want? Managers are likely to feel more comfortable with conventional management reports, so look at a range of sample reports to pick out the style cues.

4. How should we *implement* our reporting system?

It is always worth soliciting feedback from the intended audiences about whether the metrics are both comprehendible and useful. Changes in both the organization and the information security risks it faces mean that some metrics are likely to become outdated over time. Expect management to challenge the source, capture, analysis and presentation of the data, especially if they are under pressure to comply with information security pressures.

6. **Issues/Aspects of Security Measurement**

Insights into some critical aspects of security measurement are discussed below. The purpose is not to give a list of common pitfalls rather the objective is to highlight those factors that are believed to be pertinent to a research effort in security metrics.

1. Correctness and Effectiveness

Correctness denotes assurance that the security-enforcing mechanisms have been rightly implemented (i.e., they do exactly what they are intended to do, such as performing some calculation).

Effectiveness denotes assurance that the security-enforcing mechanisms of the system meet the stated security objectives (i.e., they do not do anything other than what is intended for them to do, while satisfying expectations for resiliency).

2. Leading versus Lagging Indicators

Leading and lagging indicators reflect security conditions that exist respectively before or after a shift in security. A lagging security metric with a short latency period or lag time is preferred over one with a long latency period. Many security metrics can be viewed as lagging indicators

3. Organizational Security Objectives

Organizations exist for different purposes, hold different assets, have different exposure to the public, face different threats, and have different tolerances to risk. Because of these and other differences, their security objectives can vary significantly. Security metrics are generally used to determine how well an organization is meeting its security objectives.

4. Qualitative and Quantitative Properties

Qualitative assignments can be used to represent quantitative measures of security properties (e.g., low means no vulnerabilities found; medium, between one and five found; and high, more than five found).

Quantitative valuations of several security properties may also be weighted and combined to derive a composite value.

5. Measurements of the Large Versus the Small

Security measurements have proven to be much more successful when the target of assessment is small and simple rather than large and complex. As the number of components in a system increases, the number of possible interactions increases with the square of the number of components. Greater complexity and functionality typically relate inversely to security and require more scrutiny to evaluate.

7. The Value of Security Metrics

Metrics can be an effective tool for security managers to discern the effectiveness of various components of their security programs, the security of a specific system, product or process, and the ability of staff or departments within an organization to address security issues for which they are responsible. Metrics can also help identify the level of risk in not taking a given action, and in that way provide guidance in prioritizing corrective actions. Additionally, they may be used to raise the level of security awareness within the organization. Finally, with knowledge gained through metrics, security managers can better answer hard questions from their executives and others, such as:

- Are we more secure today than we were before?
- How do we compare to others in this regard?
- Are we secured enough?

8. Conclusion

Information security is a complex area which makes it difficult but not impossible to identify useful metrics. We have described the factors that should be taken into account and suggested a pragmatic approach to the design and implementation of a system of measuring, reporting and improving information security.

The security metrics area poses hard and multi-faceted problems for researchers. Quick resolution is not expected and the likelihood is that not all aspects of the problem are resolvable.

Several factors impede progress in security metrics:

- . The lack of good estimators of system security.
- . The entrenched reliance on subjective, human, qualitative input.
- . The protracted and delusive means commonly used to obtain measurements.
- . The dearth of understanding and insight into the composition of security mechanisms.

References:

[1] http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55.

[2] 2. Burris, Peter, and Chris King. "A Few Good Security Metrics." METAGroup, Inc. audio, 11 Oct. 2000. URL: http://www.metagroup.com/metaview/mv0314/mv0314.html (10 July 2001).

[3] Nielsen, Fran. "Approaches To Security Metrics." NIST and CSSPAB Workshop, Washington, D.C., 13-14 June 2000: 7. URL: http://csrc.nist.gov/csspab/june13-15/metrics_report.pdf.

[4] Craft, James P. “Metrics and the USAID Model Information Systems Security Program.”

[5] NIST and CSSPAB Workshop, Washington, D.C., 14 June 2000. URL:

[6] http://csrc.nist.gov/csspab/june13-15/Craft.pdf (10 July 2001)

[7] http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=9140&copyownerid=8844