IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011
ISSN (Online): 1694-0814
www.IJCSI.org

A Stake Holder Based Model for Software Security Metrics

Sree Ram Kumar T[1], Alagarsamy K[2]

[1] Research Scholar, Madurai Kamaraj University
Madurai, India

[2] Associate Professor, Madurai Kamaraj University
Madurai, India

Abstract

It is common wisdom that any process that cannot be measured cannot be managed. This applies to security as well. Security metrics are assuming tremendous importance as they are vital for assessing the current security status, to develop operational best practices and for guiding future security research. This topic is very relevant at a time when organizations are coming under increasing pressure requiring them to demonstrate due assiduousness when protecting the data assets of themselves and their customers. In these circumstances metrics can give the organizations a way to prioritize threats and vulnerabilities and the risks they pose to enterprise information assets. This paper propounds a stakeholder based model of security metrics.

Keywords: *Common Vulnerability Scoring System, Security Metrics, Stake holder*

1. Introduction

Red teaming exercises, penetration testing, vulnerability scoring, and means of probing defenses for weaknesses in security are some of the methods currently being used for evaluating IT systems and network security. These strategies are not adequate in the present scenario considering higher frequency of new vulnerabilities discovered. Practice has shown that a set of good metrics would help both to determine the status of IT security performance and to enhance it by minimizing the windowa of exposure to the new vulnerabilities.

Metrics monitor the effectiveness of goals and objectives established for IT security. They can measure the implementation of a security policy, the resuls of security services and the impact of security events on an enterprise's mission.

IT security metrics can be collected at various levels and detailed metrics can be aggregated and rolled up to progressively higher levels depending on the size and complexity of the organization. It is essential here to highlight the important difference between metrics amd neasurments – while measurements are instantaneous snap shots of particular measurable parameters, metrics are more complete pictures, and typically comprised of several measurements, baselines and other supporting information that provide the context for interpreting the measurements.

2. Existing Methodologies

Security measurement using metrics has attracted great interest in recent years with the help of guidelines, practices and standards accepted world wide and with the efforts of international organizations. Code of practices like BS7799, ISO17799, NIST SP800-33 provide a good starting point for organizations in this context. In 2004, SECMET (Security Metrics Consortium) was founded to define quantitative security risk metrics for industry, corporate and vendor adoption by top corporate security officers of the sector. The Metrics work group of ISSEA(International Systems Security Engineering Asociation) has lead another standardization effort in this area. This group develops metrics for SSE-CMM(System Seciurity Engineering – Capability Maturity Model).

One model used widely for conveying the vulnerability severity is the CVSS (Common Vulnerability Scoring System). Tjis provides the end user with an overall composite score representing the severity and risk of a vulnerability. score is derived from metrics and formulas. The metrics are in three distinct categories that can be quantitatively or

qualitatively measured. Base metrics contain qualities that are intrinsic to any given vulnerability that do not change over time or in different environments. Temporal metrics contain vulnerability characteristics which evolve over the lifetime of vulnerability. Environmental metrics contain those vulnerability characteristics which are tied to an implementation in a specific user's environment. The particular constituent metrics used in CVSS were identified as the best compromise between completeness, ease-of-use and accuracy. They represent the cumulative experience of the model's authors as well as extensive testing of real-world vulnerabilities in end-user environments.

There are seven base metrics that represent the most fundamental features of vulnerability.

Base Metric	Measures
Access Vector AV	Whether the vulnerability is exploitable locally or remotely
Access Complexity AC	The complexity of attack required to exploit the vulnerability once an attacker has access to the target system (high or low)
Authentication A	Whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability (required or not required)
Confidential Impact CI	The impact on confidentiality of a successful exploit of the vulnerability (none, partial, complete)
Integrity Impact II	The impact on integrity of a successful exploit of the vulnerability (none, partial, complete)
Availability Impact AI	The impact on availability of a successful exploit of the vulnerability (none, partial, complete)
Impact Bias IB	Allows to convey a greater weighting to one of three impact metrics over other two

Temporal Metrics

Temporal Metric	Measures	Possible Values
Exploitability E	How complex the process is to exploit the vulnerability in the target system	Unproven, proof of concept, functional, high
Remediation Level RL	The level of an available solution	Official fix, temporary fix, workaround, unavailable
Report Confidence RC	The degree of confidence in the existence of the vulnerability and the credibility of its report	Unconfirmed, Uncorroborated, Confirmed

Environmental Metrics

Environmental Metric	Measures	Possible Values
Collateral Damage Potential (CDP)	Potential for a loss of physical equipment, property damage or loss of life or limb	None, low, medium, high
Target Distribution TD	Relative size of the field of target systems susceptible to vulnerability	None, low, medium, high

Base Score BS is computed as
BS=round (10 * AV * AC * A * ((CI * CIB) + (II * IIB) + (AI * AIB))
Temporal Score TS is computed as
TS=round (BS * E * RL * RC)
Environmental Score ES is computed as
ES=round ((TS + ((10 – TS) * CDP) * TD)

The ES should be considered as the final score and used by organizations to prioritize responses within their own environments.
CVSS differs from other scoring systems (e.g. Microsoft Threat Scoring System, Symantec Threat Scoring System, CERT Vulnerability Scoring or SANS Critical Vulnerability Analysis Scale Ratings) by offering an open framework that can be used to rank vulnerabilities in a consistent fashion while at the same time allowing for personalization within each user environment. As CVSS matures, these metrics may expand or adjust making it even more accurate, flexible and representative of modern vulnerabilities and their risks.

3. A Stakeholder Based Model Of Security Metrics

The security metrics discussed below focus only on network and systems integrity and reliability. The other aspects like information asset value, loss, and opportunity cost have not been considered here.
Depending upon their role in interacting with the information system (stakeholder based model), various users are concerned about different aspects of information systems security.

3.1 Executive Officers

Executive officers, being responsible for the overall performance of the enterprise, are concerned with the ability of the information systems to support operations. Because they have the authority to allocate resources, both personnel and financial, to deal with problems of information systems security, they would be interested in answers to the following questions:
How does the enterprise's information systems security compare to that of similar enterprises?
How does information systems security this year compare to last year?
Does the security spending generate the expected return?
What are the costs and consequences of not acting to improve information systems security?
Example metrics used at the management level include:

- Systems Service Level – Percentage of time that information system services are available for a given period of time
- Network Service Level – Percentage of tome that network services are available for a given period of time
- Business Requirements Met – Percentage of business needs supported by the infrastructure and which are being met
- Number of Compromises – Number of incidents during a given period in which network or systems security was compromised
- Organizational Impact of Compromises – For each incident, the number of hours, time of day, and people affected by the degradation or disruption of network, systems or application services
- Costs and benefits of improvements – The direct and indirect costs and benefits of steps that can be traken to impreove information systems security
- Peer Performances – Service level benchmarks from similar enterprises

3.2 Network and IT Systems Operations Groups

Network and IT systems operations groups, responsible for infrastructure, and systems production support, are generally interested in a more granular view of the network and systems security. Whereas executives look for support for resource allocation decisions, network and IT operations people seek help to prevent, detect, and respond to network and systems security intrusions. Thus, questions of concern include:
. What computers, applications, or services are compromising enterprise's security?
. How is the compromise taking place? Is it getting worse? How and where?
. How serious is the impact of the compromise?
. What technical measure can be taken to isolate and remediate the problem
An example of the security metrics used by network and IT operation groups is:

- Compliant Devices – Percentage of network devices that are security policy compliant.
- Managed Devices – Counts of systems and devices under active management
- Total Devices and Users – Total numbers of devices and users on the network.
- Network Latency – Mean time for packet delivery in the network.
- Packet loss – percentage of packet losses

- Network Utilization – Bandwidth utilization at key gateways in the network.
- Network throughput – transfer rate for defined end-to-end network services, such as FTP, POP3, HTTP etc.
- Viruses detected in e-mail messages – percentage of emails infected by viruses
- Unauthorized accesses attempts– percentage of unauthorized access for various network services (VPN, HTTP, SSH etc.)
- Impact of Compromise – Users affected (service degraded, disrupted, or otherwise compromised), number of devices participating in compromise, decrease in network performance, increase in network utilization, and increases in wait times during a network compromise

3.3 The network and systems security team

The network and systems security team is typically responsible for the organization's security policies and programs. Although they may not have direct operational responsibility, they are interested in how security policies, procedures, and programs are ensuring or failing to ensure network and systems security.

. Were the computers responsible for compromising the network policy compliant?

. What changes should be made to security policies and procedures?

. If policies are not working, what behaviour changes should policy modifications be aiming to achieve

. What technologies could help prevent future compromises?

. What was the impact of the compromise?

A sample of the security metrics used by security operation team is available below:

- Vulnerability Counts – Numbers of vulnerabilities found on the network, broken out by those on policy-compliant devices vs. those found on devices that are not.
- Intrusion attempts – Number of true/false positive/negative intrusions attempts
- Unauthorized accesses attempts– percentage of unauthorized access for various network services (VPN, HTTP, SSH, etc) and networked systems
- Detailed Compliance Reports – Numbers of users and devices compliant with each element of the security policy.
- Incident Forensics – The numbers of incidents attributable to policy failures vs. policy compliance failures
- Impact of Compromise – Users affected (service degraded, disrupted, or otherwise compromised); data lost, modified, or destroyed; number of devices participating in compromise; decrease in network or systems performance; increase in network utilization; and increases in wait times during a network or systems compromise.
- Suspect Port Scans – number of suspect scans on organization's network (e.g. requests sent on port 80 to routers are suspect)
- Remediation Time – Time between compromise discovery and completion of system remediation

The measurement process can be automated by implementing the network and systems security monitoring solutions. In this way, measurement errors and the subjective interpretations are eliminated, making possible for credible measurement comparisons across either time (time-series) or organizations (benchmarks).

4. Conclusions And Future Work

Metrics are central for measuring the cost and effectiveness of complex security controls. Security metrics, at least such metrics trying to define a measure for the security of an entire organization, are a quite new area of research. Without widely accepted security metrics, separating promising developments from dead-end approaches would be very difficult.

Security improvement begins by identifying metrics that quantify various aspects of security for the enterprise. Given the increased number of vulnerabilities the enterprises have to handle, we presented an open source framework (CVSS) that can be used to rank vulnerabilities in a consistent fashion while at the same time allowing for personalization within each user environment.

The paper presented a stakeholder-based model of security metrics. In the future, we propose to

establish the validity of these metrics by validating them against real set of data collected from software projects. We also propose to prove that these metrics are sound, objective and evident of the security in the software.

5. References

[1] Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainity, and Doubt, Addison Wesley, 2006

[2] Gerald L. Kovacich, Edward Halibozek, Security Metrics Management: How to Measure the Costs and Benefits of Security, Butterworth-Heinemann, 2005

[3] Marianne Swanson P & others, Security Metrics Guide for Information Technology Systems, NIST Special Publication 800-55, 2003 (http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf)

[4] Ron Ross, & others, Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53, 2005 (http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf)

[5] Systems Security Engineering-Capability Maturity Model Group, SSE-CMM – Model Description Document version 3.0, International Systems Security Engineering Association, 2003 (http://www.sse-cmm.org/docs/ssecmmv3final.pdf).

[6] Mike Schiffman, Cisco CIAG, *A* Complete Guide to the Common Vulnerability Scoring System (CVSS), Forum Incident Response and Security Teams (http://www.first.org/)

[7] VV Patriciu, I. Priescu, S. Nicolãescu, Security Monitoring - An Advanced Tactic for Network Security Management, Communications 2006 Conference, Bucharest, Romania, 2006

[8] VV Patriciu, I. Priescu, S. Nicolãescu, Operational Security Metrics for Large Networks, International Conference on Computers, Communications & Control (ICCC 2006) - Oradea, Romania, 2006

[9] SO/IEC. Information Technology – Security Techniques, Code of practice for information security management (final draft), ISO, 2005.

[10] British Standard Institute, Information Security Management. Code of Practice for Information Security Management (BS 7799-1), British Standard Institute, 1999.

[11] Basel Committee on Banking Supervision, Working Paper on the Regulatory Treatment of Operational Risk Bank for International Settlements, Basel Committee, 2001 (http://www.bis.org/publ/bcbs_wp8.pdf).

[12] CERT, CERT/CC Statistics 1988-2005, CERT, 2005 (http://www.cert.org/stats/)