International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Enterprise Software Management Systems by Using Security Metrics

Bhanudas S. Panchabhai[1], A. N. Patil[2]

[1]Department of Computer Science, R. C. Patel Arts, Commerce and Science College, Shirpur, Maharashtra, India
[2]Vasantrao Naik Arts and Science College, Shahada, Maharashtra, India

Abstract: ***Metrics are quantifiable measurement. Security metrics are quantitative indicators for the security attributes of an information system or technology. Metrics helps us to understand quality and consistency. Metrics provides a universal way to exchange ideas, to measure the product or service quality, and to improve a process. We cannot improve security if we cannot measure it. This applies to security as well. Security metrics are assuming tremendous importance as they are dynamic for measuring the current security status, to develop operational best practices and for managing future security research. This topic is very applicable at a time when organizations are coming under increasing pressure requiring them to demonstrate due persistence when protecting the data assets of themselves and their users. In these situations metrics (CVSS) can give the organizations a way to prioritize vulnerabilities and the risks they pose to enterprise information assets. This paper presents a framework for ranking vulnerabilities in a consistent fashion, and some operational metrics used by large enterprises in managing their software systems security process and to cover all dimensions of IT security from organizational (people), technical and operational points of view.***

Keywords: Common Vulnerability Scoring System, Vulnerabilities, Security Metrics, System Security, Security Management

1. Overview

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 situation 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 window of exposure to the new vulnerabilities. Metrics display the effectiveness of goals and objectives established for IT security. They can measure the implementation of a security policy, the results 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 and measurements – 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 understanding the quantities.

2. Present Methodologies

Security measurement using metrics has involved great interest in recent years with the help of guidelines, practices and standards accepted worldwide and with the efforts of International Organizations. Code of practices like S7799, ISO17799, and 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 Association) has lead another standardization effort in this area. This group develops metrics for SSE-CMM (System Security Engineering – Capability Maturity Model).One model used widely for conveying the vulnerability severity is the CVSS (Common Vulnerability Scoring System).

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of three groups: Base, Temporal and Environmental. Each group produces a numeric score ranging from 0.0 to 10.0, and a vector, a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of vulnerability. The Temporal group reflects the characteristics of vulnerability that change over time. The Environmental group represents the characteristics of vulnerability that are unique to any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities. The metrics are organized into three groups: base, temporal, and environmental metrics.

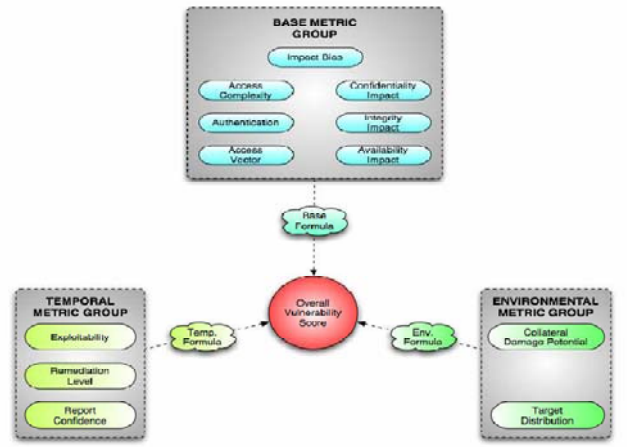

Figure 1: Common Vulnerability Scoring System Framework

2.1 Base Metrics

There are seven base metrics which represent the most fundamental features of vulnerability: The base metric group captures the characteristics of vulnerability that are constant with time and across user environments. The Access Vector, Access Complexity, and Authentication metrics capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it. The three impact metrics measure how vulnerability, if exploited, will directly affect an IT asset, where the impacts are independently defined as the degree of loss of confidentiality, integrity, and availability.

Table 1

Base Metric	*Measures*	*Values*
Access Vector AV	Whether the vulnerability is exploitable locally or remotely	Local, Adjacent Network, Network
Access Complexity AC	The complexity of attack required to exploit the vulnerability once an attacker has access to the target system	High, Medium, Low
Authentication A	Whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability	Single, Multiple, None
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	

2.2 Temporal Metrics

The threat posed by vulnerability may change over time.

Table2

Temporal Metrics	*Measures*	*Values*
Exploitability (E)	This metric measures the current state of exploit techniques or code availability	Unproven (U), Proof-of-Concept (POC), Functional (F), High (H), Not Defined (ND)
. Remediation Level (RL)	The remediation level of vulnerability is an important factor for prioritization. The typical vulnerability is unpatched when initially published. Workarounds or hot fixes may offer interim remediation until an official patch or upgrade is issued.	Official Fix (OF), Temporary Fix (TF), Workaround (W), Unavailable (U), Not Defined (ND)
Report Confidence(RC)	This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details. Sometimes, only the existence of vulnerabilities are publicized, but without specific details.	Unconfirmed (UC), Uncorroborated (UR), Confirmed (C)

2.3 Environmental Metrics

Different environments can have an immense bearing on the risk that vulnerability poses to an organization and its stakeholders.

Table 3

Environmental Metrics	*Measures*	*Values*
Collateral Damage Potential (CDP)	This metric measures the potential for loss of life or physical assets through damage or theft of property or equipment.	None(N), Low(L), Low-Medium (LM), Medium-High (MH), High (H), Not Defined (ND)
Target Distribution (TD)	This metric measures the proportion of vulnerable systems	AS Above
Security Requirements (CR, IR, AR)	These metrics enable the analyst to customize the CVSS score.	AS Above

The base equation is the foundation of CVSS scoring. The base equation is: Base Score = round_to_1_decimal (((0.6*Impact) + (0.4*Exploitability)–1.5)*f (Impact)) **Temporal Score** = round_to_1_decimal (Base Score*Exploitability*Remediation Level*Report Confidence) **Environmental Score** = round_to_1_decimal ((Adjusted Temporal+ (10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)

An Environmental score should be considered as the final score and used by organizations to prioritize response within their own environments. CVSS differs from other scoring systems (e.g. Microsoft Threat Scoring System, Symantec Threat Scoring System, CERT/CC 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.

Metrics should also be easily obtainable and feasible to measure. But research methodology plays an important role here, not to have partial data as a result; and to cover all dimensions of IT security from organizational (people), technical and operational points of view.

3. Security for Enterprise Software Systems

In most large organizations, measurements of software systems security are often conducted by separate teams that independently define, collect, and analyze technical metrics. These metrics include the numbers of vulnerabilities found in network scans, known incidents reported, estimated losses from security events, security bug discovery rate in a new software application, intrusion detection system alerts, number of virus infected e-mails intercepted, and others. The security metrics described in this section focus on network and systems integrity and reliability. The other aspects like information asset value, loss, and opportunity cost are not subject of this presentation. Depending upon their role in interacting with the software system various users are concerned about different aspects of information systems security.

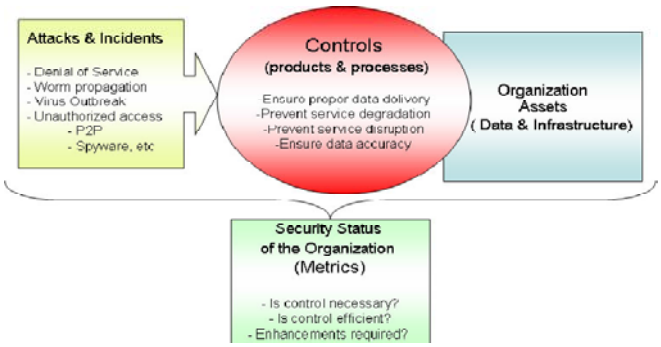

Figure 2: Network and systems security based upon metrics

3.1 Managerial 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:

Table 4

Sr. No.	*Questions*
1.	How does enterprise software systems security this year compare to last year?
2.	How does the enterprise software systems security compare to that of similar enterprises?
3.	What are the costs and consequences of not acting to improve information systems security?
4.	Do the security costs generate the expected return?

An example of the Enterprise Software systems security metrics used at the management level

Table 5

Example	*Description*
1.Systems Service Level	Percentage of time that information systems services are available for a given period of time as well as part of a time series to give historical context.
2.Network Service Level	Percentage of time that network services are available for a given period of time as well as part of a time series to give historical context.
3.Corporate Requirements Met	Percentage of business needs supported by the infrastructure and which are being met.

3.2 IT Systems Operations Groups

It is responsible for infrastructures, 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 is compromising enterprise's security?
- Where are they?
- 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 machines?

An example of the security metrics used by network and IT operation groups is:

Table 6

Example	*Description*
1.Compliant Devices	Percentage of network devices that are security policy compliant
2.Managed Devices	Counts of systems and devices under active management
3.Total Devices and Users	Total numbers of devices and users on the network
4.Network Latency	Mean time for packet delivery in the network.
5.Packet loss	Percentage of packet losses
6.Network Utilization	Bandwidth utilization at key gateways in the network.
7.Network throughput	Transfer rate for defined end-to-end network services, such as FTP, POP3, HTTP, etc.
8.Viruses detected in e-mail messages	Percentage of emails infected by viruses

3.3 An IT 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.

Table7

Sr. No.	*Questions*
1.	Where the computers responsible for compromising the network policy compliant?
2.	What changes should be made to security policies and procedures?
3.	What behavior changes should policy modifications be aiming to achieve?
4.	What technologies could help prevent future compromises?
5.	What was the impact of the compromise?

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

Table 8

Example	*Description*
1.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.
2.Intrusion attempts	Number of true/false positive/negative intrusions attempts
3.Unauthorized accesses attempts	Percentage of unauthorized access for various network services (VPN, HTTP, SSH, etc.) and networked systems
4.Detailed Compliance Reports	Numbers of users and devices compliant with each element of the security policy.
5.Incident Forensics	The numbers of incidents attributable to policy failures vs. policy compliance failures.
6.Impact of Compromise	Users affected (service degraded, disrupted, or otherwise compromised); data lost, modified, or destroyed;

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

3.4 Other metrics: Other several metrics that are as: We use following metrics for software project management of enterprise systems. The following figure shows the security metrics program for software project management.

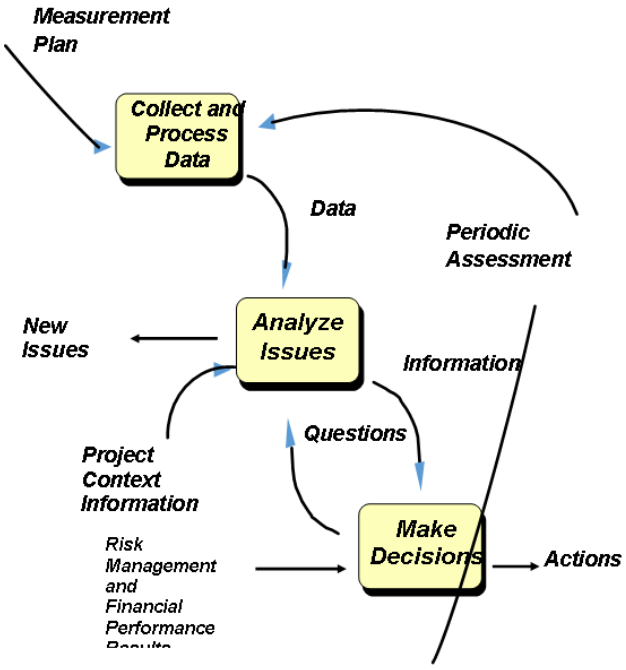

Figure 3: Security Metrics Program

3.5 Collect Metrics data mainly from

- Project Manager
- Development Team
- Testing Team
- Quality Team
- Help Desk

Table 9

Sr. No.	*Name of the Metrics*
1.	Schedule performance (milestones, variances)
2.	Cost performance (actual vs. planned; variances)
3.	Effort performance (actual vs. planned; allocations)
4.	Requirements management (total, growth, traceability)
5.	Program size (page counts - planned vs. actual)
6.	Test performance (requirements tested, passed test)
7.	Quality - Defect data status (problems open, closed, density, origin, etc.)
8.	Process performance (tasks completed, action items)
9.	Computer resource utilization (memory loading, CPU loading)
10.	Management planning performance (estimates vs. actual, re-planning etc.)

4. Conclusion

- The Metrics are central for measuring the cost and effectiveness of complex security controls.
- 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).
- In 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.
- To achieve accurate measurements of productivity and quality requires automated metrics collection and analysis.
- In order to characterize, evaluate, predict and improve the process and product a metric baseline is essential.
- Nowadays enterprise software systems use the major technical-operational metrics for large enterprises.

References

[1] Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainty, 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)
[4] Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison Wesley, 2006
[5] Mike Schiff man, Cisco CIAG, A Complete Guide to the Common Vulnerability Scoring System (CVSS), Forum Incident Response and Security Teams (http://www.first.org/)

Author Profile

Bhanudas Suresh Panchabhai is presently working as Assistant Professor, Department of Computer Science, R. C. Patel ACS College, Shirpur, Dhule, Maharashtra, India. His research area include CVSS(Common Vulnerability Scoring System) as a Security Metrics for IT System.

Dr. A. N. Patil is presently working as Principal, Vasantrao Naik College, Shahada, Nan durbar, and Maharashtra, India