SECURITY METRICS FOR ENTERPRISE INFORMATION SYSTEMS

Victor-Valeriu PATRICIU
PhD, University Professor
Department of Computer Engineering
Military Technical Academy, Bucharest, Romania

E-mail: vip@mta.ro

Iustin PRIESCU
PhD
Department of Computer Engineering
Military Technical Academy, Bucharest, Romania

E-mail: iustin999@gmail.com

Sebastian NICOLAESCU
PhD Candidate - Military Technical Academy, Bucharest, Romania
Verizon Business, New York, USA

E-mail: sebastian.nicolaescu@gmail.com

Abstract: *Managing the security of enterprise information systems has become a critical issue in the era of Internet economy. As any other process, security can not be managed, if it can not be measured. The need for metrics is important for assessing the current security status, to develop operational best practices and also for guiding future security research. The topic is important at a time when companies are coming under increasing compliance pressures that require them to demonstrate due diligence when protecting their data assets. Metrics give companies a way to prioritize threats and vulnerabilities and the risks they pose to enterprise information assets based on a quantitative or qualitative measure. This paper presents a framework for ranking vulnerabilities in a consistent fashion, and some operational metrics used by large enterprises in managing their information systems security process.*

Key words: *system security, security metrics, vulnerabilities, security management*

1 Introduction

The current strategies for evaluating or validating IT systems and network security are focused on examining the results of *security assessments* (including red-teaming exercises, penetration testing, vulnerability scanning, and other means of probing defences for weaknesses in security), and on examining the *building blocks, processes,* and *controls* (for example: auditing business processes and procedures for security policy compliance,

assessing the quality of security in infrastructure components, and reviewing system development and administration processes for security best practices).

These measurement strategies are not good enough considering higher frequency the new vulnerabilities are identified, and the shorter interval the exploit becomes available to the attackers after the vulnerability is publicly announced. As practice showed that any prevention mechanism may fail, a real-time security monitoring strategy and a set of good metrics would help both to determine the status of IT security performance, and to enhance it by minimizing the windows of exposure to the new vulnerabilities.

Metrics—measurable standards—monitor the effectiveness of goals and objectives established for IT security. They measure the implementation of security policy, the results of security services and the impact of security events on an enterprise's mission.

IT security metrics can be obtained at different levels within an organization. Detailed metrics, collected at the system and network level, can be aggregated and rolled up to progressively higher levels, depending on the size and complexity of an organization. If measurements are instantaneous snapshots of a particular measurable parameters, then metrics are more complete pictures, typically comprised of several measurements, baselines, and other supporting information that provide context for interpreting the measurements.

Good metrics are *goal-oriented* and should have the following features: *specific, measurable, comparable, attainable, repeatable,* and *time dependent*.

2. Standardization - Drivers and Results

Security performance measurement by using standardized metrics gained increasingly interest during the last years with the help of guidelines, code of practices and standards accepted widely over the world, and with the efforts of international organizations and companies. Code of practices like BS7799, ISO17799, NIST SP800-33 are useful as a starting point for security measures in organizations. They focus mainly on providing sets of controls, but the measurement of the quality and applicability of these controls is not handled in detail.

In 2004, Security Metrics (SECMET) Consortium was founded to define standardized quantitative security risk metrics for industry, corporate and vendor adoption by top corporate security officers of the sector.

Another standardization effort is led by the Metrics Work Group of International Systems Security Engineering Association (ISSEA). This group is tasked to develop metrics for Systems Security Engineering - Capability Maturity Model (SSE-CMM). SSECMM has adopted the NIST 800-55 methodology of developing security and process metrics. The work group has proposed 22 Process Areas (PA) for metrics development grouped in two sections: security base practices and project and organizational base practices.

Meanwhile, governments around the world already released laws and regulations driving and facilitating IT security measurements. Some example of laws and government regulations are: Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act of 2002 (FISMA) – for the US, and The Data Protection Directive 95/46/EC of the European Parliament – for the EU.

The most important methods used to develop security metrics are: the IT performance assessment methodology, the stakeholder-based model and the capability-based model.

Capability-based model is a product of SSE-CMM international metric project. It addresses the functional capabilities: protect, detect, and respond. SSE-CMM defines required performance of the best practices to generate specific results. *IT performance assessment methodology* (coordinated by US Department of Defence) has three components namely: capabilities, attribute level, and specific metrics. The attribute level addresses the requirement that support that mission and the specific metrics component addresses specific measurable activities that support those mission requirements. The *stakeholder-based model* views metrics from an organizational role perspective: stockholders, stockholders responsibility, stockholders interest and actions.

The challenge of defining security metrics lies on the problem that metrics must be quantifiable information (like percentage, average or absolute numbers) for comparison, applying formulas for analysis and tracking the changes. The result from the manual collection or automated resources should be meaningful performance data and must be based on IT security performance goals of the organization. Metrics should also be easily obtainable and feasible to measure. But research methodology plays an important role here, not to have biased data as a result; and to cover all dimensions of IT security from organizational (people), technical and operational points of view.

3. Metrics to Evaluate the Security Vulnerabilities

CERT reported in 2005 a number of 5,990 vulnerabilities, which represents an increase with 58% from 2004. To determine the urgency and priority of response to vulnerabilities, organizations need models that would convey vulnerability severity.

One such model is the Common Vulnerability Scoring System (CVSS) which was designed to provide the end user with an overall composite score representing the severity and risk of a vulnerability. The 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 which represent the most fundamental features of vulnerability:

- *Access vector* (AV) measures whether the vulnerability is exploitable locally or remotely.
- *Access complexity* (AC) measures the complexity of attack required to exploit the vulnerability once an attacker has access to the target system (high or low).
- *Authentication* (A) measures whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability. (required or not required)

- *Confidentiality impact* (CI) measures the impact on confidentiality of a successful exploit of the vulnerability on the target system. (none, partial or complete)
- *Integrity impact* (II) measures the impact on integrity of a successful exploit of the vulnerability on the target system. (none, partial or complete)
- *Availability impact* (AI) measures the impact on availability of a successful exploit of the vulnerability on the target system. (none, partial or complete)
- *Impact bias* (IB) allows a score to convey greater weighting to one of three impact metrics over the other two. The value can be *normal* (CI, II and AI are all assigned the same weight), confidentiality (CI is assigned greater weight than II or AI), integrity (II is assigned greater weight than CI or AI), or availability (AI is assigned greater weight than CI or II)

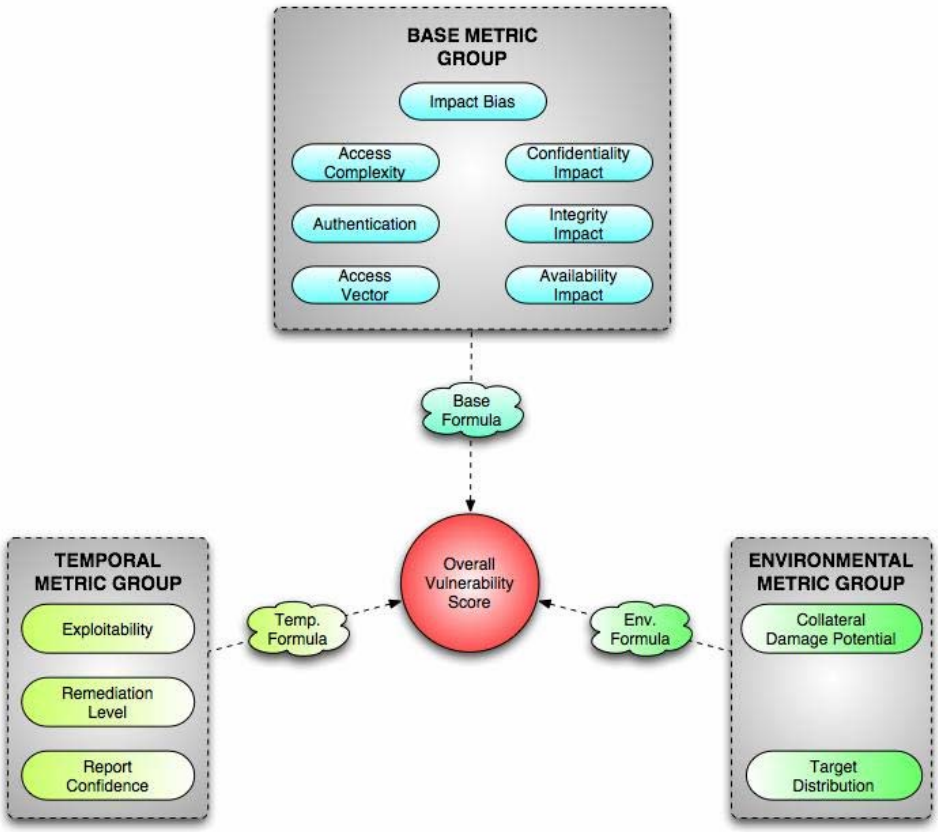

Figure 1. Common Vulnerability Scoring System Framework

The temporal metrics which represent the time dependent features of the vulnerability are:

- *Exploitability* (E) measures how complex the process is to exploit the vulnerability in the target system. The possible values are: unproven, proof of concept, functional, or high.
- *Remediation level* (RL) measures the level of an available solution. (official fix, temporary fix, workaround, or unavailable)

- *Report confidence* (RC) measures the degree of confidence in the existence of the vulnerability and the credibility of its report. (unconfirmed, uncorroborated, or confirmed)

The environmental metrics represent the implementation and environment specific features of the vulnerability.

- *Collateral damage potential* (CDP) measures the potential for a loss of physical equipment, property damage or loss of life or limb. (none, low, medium, or high)
- *Target distribution* (TD) measures the relative size of the field of target systems susceptible to the vulnerability. (none, low, medium, or high)

Scoring is the process of combining all the metric values according to specific formulas. *Base Score* is computed by the vendor or originator using the following formula:

BS= round (10 * AV * AC * A *((CI*CIB) + (II*IIB) + (AI*AIB)),

Once is set and published, the BS score is not expected to change.

It is computed from "the big three" confidentiality, integrity and availability. This is the "foundation" which is modified by the Temporal and Environmental metrics. The base score has the largest bearing on the final score and represents vulnerability severity.

Temporal score is also computed by vendors and coordinators for publication based on the following formula:

TS= round (BS * E * RL * RC),

It allows for the introduction of mitigating factors to reduce the score of the vulnerability and is designed to be re-evaluated at specific intervals as a vulnerability ages. The temporal score represents vulnerability urgency at specific points in time.

Environmental score is optionally computed by end-user organizations and adjusts combined base-temporal score based on the following formula:

ES= round ((TS + ((10 – TS)* CDP))* TD),

This should be considered the final score and represents a snapshot in time, tailored to a specific environment. User organizations should use this 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.

4. Metrics to Evaluate the Information Systems Security Controls

In most large organizations, measurements of information 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.

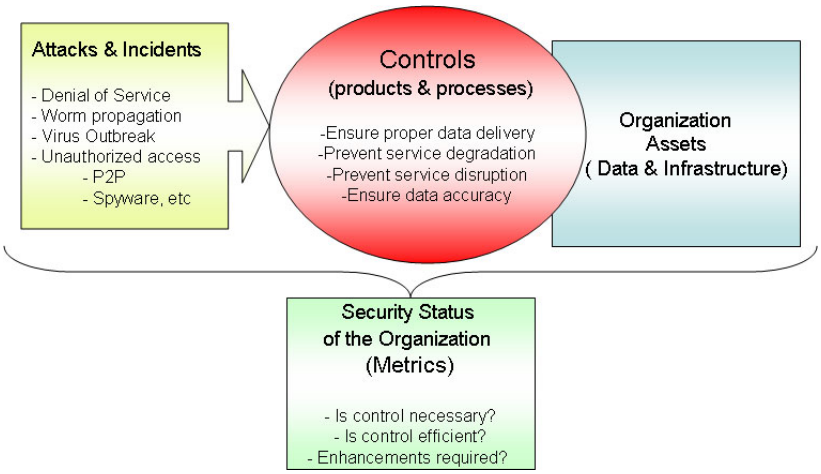

Figure 2. Network and systems security based upon metrics

Depending upon their role in interacting with the information system (stakeholder-based model), various users are concerned about different aspects of information systems security.

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?

An example of the information systems security metrics used at the management level is:

- *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.
- *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.
- *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 taken to improve information systems security.
- *Peer performances* – Service level benchmarks from similar enterprises.

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?
- 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:

- *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.

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).

5. Conclusions

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.

In the last section we covered the metrics for network security from the perspective of stakeholder based model, and presented the major technical-operational metrics used by 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 (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. Nicolăescu, **Security Monitoring - An Advanced Tactic for Network Security Management,** Communications 2006 Conference, Bucharest, Romania, 2006
8. VV Patriciu, I. Priescu, S. Nicolăescu, **Operational Security Metrics for Large Networks,** International Conference on Computers, Communications & Control (ICCC 2006) - Oradea, Romania, 2006
9. ISO/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/)
13. US President's Information Technology Advisory Committee – **"Cyber Security: A Crisis of Prioritization", Report to the President,** National Coordination Office for Information Technology Research and Development, 2005