International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 4 –NOVEMBER 2014.

NETWORK SECURITY METRICS IN SOFTWARE DEVELOPMENT

S.V.Achuta Rao[*1] and Dr. Kiran Kumar. Reddi[#2]

[*]*Research Scholar, Computer Science & Technology, Krishna University, Machilipatnam, India*

[#]*Computer Science & Technology, Krishna University, Machilipatnam, India*

[1]sarachyuth@gmail.com

[2]kirankreddi@gmail.com

Abstract— Metrics are the only way you can measure the quality of your network and its security. You need to be able to report this quality to your management and they mainly understand numbers, percentages, graphs and charts.
They need to know the threats to their network and the amount risk in not taking action to correct them. Metrics can help you quantify this information. You need to measure something before you can manage it. Security Metrics are key component of our design and Development Process.

Keywords— Metricst; Network; Quality; Development Process

I. INTRODUCTION

The quality of our nation's economy can be defined in terms of metrics. Metrics is a group of measurements that produce a quantitative picture of something over a period of time. Metrics are specific; measurable; attainable; repeatable and time-dependent [1].

Few Traits of metrics are:

• Understandable – Use the KISS principle, "keep it simple, stupid". If you're the only one to understand the metric then how do you expect your managers to understand the relevance and finance it.

• Field-Tested – Each metric should be confirmed in practice. It may sound like a good metric to take, but, if you can't confirm its usefulness, it's wasted effort.

• Economical –Security logs can be saved as delimited text files and imported into a database for analysis. Security tools should provide metrics as one of their features. Some of them require a separate application to analyze the logs. This should be purchased along with the tool.

• High Leverage – time and money talk best to your manager both in savings and expenditure. The metrics you produce for them should be in this format. Also, metrics should help to pin-point minor changes that provide significant improvements. One way of determining high leverage metrics is to use the Vital Few or 80/20 rule; 80% of improvement comes from eliminating the top 20% of your problems.

Timely what happened last week, last month or last year is good for baselines but not to plug holes in the security system Many metrics can be normalized so that systemic changes are factored out.

II. PREVENT – DETECT - REACT RESTORE METRICS IN PHASES FOR AUDIT & REVIEWS

Security: Different Metrics in various Development Phases In software development metrics, there is no one metric that describes the quality of your network security, no silver bullet. You will need to collect many different metrics and compare them to their respective baseline in order to qualify your security improvements. In the network security cycle of Prevent – Detect – React – Restore, metrics are tracked in the

Prevent and Detect phases. In the React phase, new metrics can be developed to drive improvement to the Prevent – Detect phases[1],[2],[3].

B. Security Metrics for Audits & Reviews

1. Number of Successful Logons – from security audits.

Number of Unsuccessful Logons – from security audits. Number of Virus Infections during a given period Number of incidents reported. Number of security policy violations during a given period. Number of policy exceptions during a given period. Percentage of expired passwords. Number of guessed passwords use a password cracker to test passwords Number of incidents. Cost of monitoring during a given period – use your time tracking system if you have one.

It may make sense to divide your metrics into two major categories:

Process Metrics A metric that represents the maturity of a security process. They are best for reporting to management about the quality of your security and improvements. From the above list, #6 is the only example of a process metric.

Examples of other process metrics include: Percentage of passwords meeting policy Percentage of exposed systems with

IDS Number of firewalls per exposed systems Number of external users.

Security Metrics a metric that indicates the extent a security attribute is present. They are best for reporting the state of security to the members of your organization, the collector metric and process implementers. The rest of the above list is examples of security metrics. You can also include the following: Frequency of audit reviews. Number of compliance with virus updates. Number of virus infected components.

III. OBJECTIVES OF NETWORK SECURITY METRICS

As you design, implement and adjust your metrics program it is important to keep some objectives in mind:

• Collect objective information about the state of the Network's Security. Track your organization's progress toward its improvement goals.

• Assess the impact of process/tool changes.It is easy to loose sight of these objectives and collect data just for the sake of collecting it. Emphasize the business and security results you are trying to achieve. They should be used to drive security improvements and make sure the data you collect get used for constructive purposes[3].

A)Security Policy

A section on Security Metrics must be included in the Security Policy" if you are serious about taking security metrics. The section should include providing for the resources, and training to take the metrics data and define who's responsible/accountable for the metrics program. This is where management agrees to support the metrics program.

B)Document the Network Security ProcessYour network security process must be documented to explain just how your organization provides network security in accordance with the policy. Since the policy now includesproviding for a metrics program, the Network Security Process explains what the metric plan is and how it will be implemented.

C)State the Goals

The goals tell why you are taking the metrics, most important of which is to improve the quality of your security system.

"Reducing the response time for detecting an intrusion, improve the password protection of your accounts, and reduce risks?"

D)Define Metrics Required to Reach Goals

Tells what you're going to measure in order to determine when you've reached a goal. If you want to improve the password protection of your accounts then you need to know what metrics to collect to determine what a "good" password is."How long the password is, is it made up of alphanumeric and how long does it take a password cracker to crack it."

E) Identify Data to Collect

Now that the metrics are defined, they can be expanded into the raw data to collect.

"For passwords, you need to collect for each account name, the number and type of character makeup the password is and measure how long it takes to crack."

F) Define Data Collection Procedures

Tells you how and when you are going to collect the metric, including what tool to use. Also, who is responsible for collecting the data, where it is to be stored and how to verify it. If a tool is used, then you need to include the tool's location, version and setup in the definition. Scripts should be treated the same way.

"On a weekly basis, each network administrator will run LC2 password auditing software on their respective PDCs. They will record the account name, the number and type of characters, and how long it took the tool to crack the each password. This information is to be stored in the Security Metrics.mdb database."

G) Assemble a Metrics Toolset

All tools and scripts should be conveniently stored on the network so that anyone who needs to can access them. Access should be "read only" so they cannot be changed unless specifically authorized. This is especially true of scripts. You might even consider a formal Software Configuration Management system for scripts to track their changes.H) Create a Metrics Database

The database should be easy to use, flexible, interface with or include a graphical reporting routine to enable professional graphs and charts

I) Assemble a Metrics Toolset

All tools and scripts should be conveniently stored on the network so that anyone who needs to can access them. Access should be "read only" so they cannot be changed unless specifically authorized.

J) Create a Metrics Database

The database should be easy to use, flexible, interface with or include a graphical reporting routine to enable professional graphs and charts. It should be capable of storing large amounts a data for historical purposes[2].

IV. LEVELS & STANDARDS OF SYSTEMSECURITY ENGINEERING

In the software development field, one of the most prominent quality programs is the Software Engineering Institute's (SEI)

Compatibility Maturity Model (CMM). The software CMM helps an origination develop cost effective consistent quality software.

SEI has not created a CMM for security, but the International System Security Engineering Association (ISSEA) has created the Systems Security Engineering Compatibility Maturity Model (SSE-CMM). Like the software CMM, the SSE-CMM consists of five levels; each builds upon the previous level until the fifth level is a system that is

continuously improving. Also like the software CMM, metrics plays an important role in measuring the quality of the security procedures and processes. The objective of the SSECMM is to advance security engineering as a defined, mature and measurable discipline. It is important to keep in mind that the SSE-CMM

like the software CMM does not require you to follow a prescribed methodology or process. It does require that you document your processes and that those processes are institutionalized in the organization[4],[5].

A)Level 1"Performed Informally"

Focuses on the security process an organization has in place. That Base Practices are performed.B)Level 2"Planned and Tracked"Focuses on project-level definition, planning and performance.

Metrics are defined, planned and taken to measure performance and establish baselines.

C)Level 3"Well-defined"

Focuses on disciplined tailoring from defined processes at the organizational level. Metrics are expanded to the global enterprise level.

D) Level 4

"Quantitatively Controlled "Focuses on measurements being tied to the business goals of the organization.

E) Level 5 "Continual Improving"

Leverages all the management practice improvements from earlier levels and emphasizes cultural changes that are needed to sustain the improvements. Metrics are used to drive security improvement decisions for the global enterprise.

V. IMPLEMENTATION –LEVEL SECURITY TESTING

Implementation-level security reviews, which are conducted by members of the Development Team in later stages of product development, aim to validate that a software artifact has protection against relevant security threats. Such reviews typically consist of a reevaluation of threats and counter measures identified during security design review, targeted security reviews of security-critical code, selective code reviews to assess code quality from a security perspective, and targeted security testing.

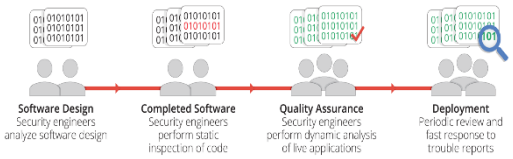

Fig. 1. Systems development Maintain Security Strategy

Automated testing for flaws in certain relevant vulnerability classes. We use both inhouse developed tools and some commercially available tools for this testing. Security testing performed by Software Quality Engineers in the context of the project's overall software quality assessment and testing efforts[3],[4].

VI. CONCLUSION

Metrics need to be a required part of Network Security. All process improvement plans must have feedback loops in order to drive quality as high as it will go. Metrics are the key enabler to improving your network's security. It is the only way you can determine the quality of your security.As it is said, improvising is the mother of invention and since there isn't much written on Network Security Metrics, then you need to draw upon other metric initiatives such as those used by the software development community. Metrics programs are worth the effort and investment

Acknowledgment

Our heartfelt thank to the free on-line dictiory, Americal Software Quality Association, Google White Papers, Wikipedia, Software Security Engineering Team and our supported Principal, Dean and Computer Science Department of Krishna University, Machilipatnam, India of constant guidance to improve standards.

VII. REFERENCES

[1] American Society for Quality and their Bodies of Knowledge for CertifiedQualityEngineer http://www.asq.org/cert/types/cqe/bok.html
[2] Smriti Jain, Maya Ingle, Security Metrics and Software Development Progression, Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 5(Version 7), May 2014, pp.161-167
[3] American Society for Quality, http://www.asq.org/info/
[4] Howe, Denis. (1993-2001), The FreeOnLineDictionary,www.wombat.doc.ic.ac.uk/foldoc/foldoc.cgi
[5] Google's Approach to IT Security,A Google White Paper 2012
[6] SANS Security Essentials. (May 2001). Training, Book; 1-1; page 5-4.
[7] http://www.dictionary.com/cgi-bin/dict.pl?term=security