Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Metrics: Expectations & the Reality

Deepak Gupta
M.Tech Student, FMIT, Jamia Hamdard
New Delhi, India

Ehtiram Raza Khan
Asst. Professor, FMIT, Jamia Hamdard
New Delhi, India

Abstract--The most amazing thing about security is - we know we are secure but we don't know how much and also we are never sure if we are really secured from all the potential threats. We can justify the security implemented only by the levels of security implemented but again we fail while defining it in terms of some numbers as we do to physical things. Security metrics are one solution to this. Security metrics extend the definition of security quantitatively, providing best possible way of understanding and assessing the performance index of any security mechanics implemented. In this paper, we have tried to understand and analyze the trends, as seen, in past for quantizing the security and describe the expectations from the realization of the security and the harsh reality faced in developing the security metrics.

Keywords: Security, Security metrics, Quantification, Security frameworks, Security realization

I. INTRODUCTION

Now-a-days by mere implementing proper antivirus and firewalls one can make a system very secure .A new security policy is formulated with the advent of a new threat in the market. It has become a very common scenario to talk about the security measures and their effectiveness in the IT world but if we are to discuss about the exactness of any of the implemented security, then everything hangs between nine and eleven. Nobody takes hid of "how much" while implementing security which is when he really should know the figure of the effectiveness of the security he has gained. The reality is we are more concerned in increasing the levels of security than really having it. For an individual, security can be defined as the mechanism of prevention from any virus, worm etc. and protecting the data from any unauthorized access and alterations. But it really matters when the entire perspective changes to an organization. Organizational IT resource safety and security need far more policies and security measures than that is required by an individual. So, to measure the effectiveness and the completeness of any security implemented in an organization, it needs to be evaluated timely and compared with the security standards and the security implemented in other organizations as well. For this reason only, security needs to be quantized, though it has always been viewed as an abstract entity. Security quantification is the basic aspect of any security metrics, thus helping an organization evaluate its security effectiveness and reform its security policies and measures.

So, security metrics bring forth a methodology of quantifying the security implemented in any of the forms viz. layers, levels, policies and or standards and in any scenario-individual or organizational. The effectiveness of the security policies and layers is compared to a standard and then a security metric is formulated. But it is a difficult task to numerate the security.

The paper is designed as follows: Section II deals with the latest literature reviews and related work; Section III presents the expectations of an organization and security experts from the security metrics; Section IV discusses reality of security metrics; Section V ends up with the conclusion and future work.

II. RELATED WORK

Security metrics are the tools that help in understanding and assessing the performance of the implemented security mechanics, coverage and /or the extent of security provided, and decision making of various security processes, mechanisms and procedures. Security metrics are used in the testing of web based applications etc. [1]. Metrics act as a base for project planning and also play a vital role in organizing, controlling and improving the software development activities [2].

To exfoliate the layers of security metrics real one needs to discuss about the recent advancement and necessity of the security metrics as the parameters for security realization and assessment.

Vaarandi et al described an open source log management technology based production framework for metrics collection and reporting in their paper [3] which was an elaborative discussion with an emphasis on the use of security metrics. In a report [4] CIS, Center for Internet Security have devised standard metrics and data definitions to be adopted by organizations for analyzing the security processes so that it will be easy for the organizations to reevaluate their security infrastructures.

Going a bit far the Council on Cyber Security [5] proposed 15+ critical controls as a measure of cyber defense considering the security logs and network monitoring using the similar concept of logs evaluation by Vaaarandi et al[3]. Jouini et al, in their publication[6] discussed the use of the MFC model based on some practical application, that

enables cloud service providers and cloud subscribers to quantify the risks taken with the security of their assets and to make security related decisions on the basis of quantitative analysis.

In the ISO/IEC 27004:2009 standards [9], the measurement and management of security metrics have been discussed thereby elaborating the methodology for improving the effectiveness of Information Security Management System as already defined in ISO/IEC 27001.Martinelli et al, in [10] proposed an elaborative specification model for security analysis implementing the security metrics formally. Hatonen et al. [12], provided an overview of management of security in complex systems like cloud computing, focusing on the technical aspects of security in the distributed architecture by comparing the various taxonomies of security metrics.

Bistarelli et al [16] presented a methodological review in their paper describing the policy based security metrics through quality of protection tools for information flow in the multilevel security in computer networks emphasizing on the use and effectiveness of security metrics. R.Savola [17], [18] discussed various taxonomies for the security metrics for the information systems and in [19] the taxonomy of security metrics for software intensive systems have been proposed.

TABLE 1 shows the clear view of the effectiveness of security measures as computed by CSO magazine in 2005. [20]

Table 1 Effectiveness of Security Management Practices [20]

How effective are your organization's security measurement practices?	
Effective	38.5 %
Neither effective nor ineffective	23.1 %
Very effective	23.1 %
Don't know	7.7 %
Ineffective	7.7 %

From the above discussion, it can be concluded that there has been significantly a lot of research on the security metrics, but as the prevailing conditions alter so does the system, and hence the metrics also need to be changed. They cannot be same for all-one that may satisfy the need of the small system may not be appropriate for larger ones. So there are a lot of expectations from the security metrics and its advancement. As being in the very beginning stage, there are a lot of expectations in the advancement of the security infrastructures and metrics which we have discussed in the next section.

III. WHAT DO WE EXPECT FROM SECURITY METRICS?

Measurement is very important for understanding and evaluating the performance and comparison. While we work on security issues, the same is expected. We wish to measure the security both qualitatively and quantitatively so that we can judge whether we have been completely successful in achieving immunity or not from the desired threats. For that purpose, security metrics help us in evaluating the system on the basis of processes, policies and procedures. The use of security metrics advocates transparency, decision making, predictability and proactive planning [7]. Metric is a measurement standard, defining both what is being measured (the attribute) and how it is measured (the unit of measure) [8].

What a security analyst expects from the metric matters a lot as it will be the base, he will be having, in the proposal of developing a secure environment for an organization. The security metrics will help him analyze his security implementations by reviewing it in accordance to the compliance reports provided and the standards and also in the computation of some significant numbers to justify his achievements. The score he will get will verify the shortcomings and the level maintained in the security implementation in the company.

An organization will learn its state of protection from the vulnerabilities by comparing its security policies and processes with the standard policies and procedures as described in the security metrics. The metrics used in the organization can be subjective / quality oriented or abstract /quantifying.

The goals of security metrics can be summarized as below:

1. *Evaluation of System Performance and defining it judiciously.*
2. *Contributions in the improvement of the existing security implementations.*
3. *Optimization of the security controls implemented in the organization.*
4. *Monitoring the existing security levels and hence improving them to a certain level.*
5. *Advocating the justified use of the budget in security.*
6. *Collaborating the managerial departments with the technical departments as both needs to go through security metrics port folio of the organization for the proper functioning of the organization.*
7. *Work as indicator of how well the security services are present in the system.*

Therefore what is expected from security metric has an unpredictable answer varying from organization to organization and person to person.

In the next section we will be discussing about the reality we face when we enter the security metric domain. Our expectations are realized or not, this is discussed in the coming section.

IV. SECURITY METRICS:THE REALITY

Security measurement, quantification of security, security metrics etc. are different terms used for the mathematical formulations presented in measuring the security in numbers. Specifically many get confused in measurement and metrics. The reality is these are competently different terms- Measurements can be defined as the single-point-in-time views of specific, discrete factors, while metrics are derived by the sequential comparison of a predetermined baseline with two or more measurements taken over time [11]. Measurements are generated by counting; metrics are generated from analysis [12] [14].

The reality of security metric formulation is that –many have proposed the relevant security metrics according to the time and situation but none of them fit to the entire scenario if Information Technology is concerned. There are many factors that prevent security metrics development: viz. *1.Scope of the metric 2.Quantification of security controls 3.A standard framework for all 4.Degree of understanding the security issues etc. [6] [12]* So when we say security metric, we are still in the infant stage of generating a standardized metric framework or platform that could cater all the basic needs of a quality security measurement remaining unspecific to any domain.

1. Difficult To Define The Scope Of The Metric

The threats to security can come from anywhere –human, software, hardware, nature etc. So the threats can be classified as technical (hardware/software) and non-technical (human beings, natural calamities etc).So it is beyond the scope of any one security metric to cover all. Apart from this, the technical threats can be further subdivided into application level, network level, etc which again make it difficult to define the scope of the security metrics.

2. Quantification Of Security Controls

Depending upon the nature and type of the security controls, it is impossible to match each implemented security control with a metric. As the behavior of the same control may be different in different environments, it is unlikely to use the same metric for all security control implementations.

3. Lack Of A Standard Framework

Due to layers and different levels in information system, security control mechanisms and the threats, a single metric cannot be efficient in describing the effectiveness of security mechanism. There will be a need of different security metrics for different scenarios; hence a standard framework could not be created. This is a very big obstacle in the generation and implementation of security metrics.

A metric used for a small simple system can never be used for the large systems as the number of processes to be evaluated increases multi fold and also the security policies for a standalone system will always vary with that of the complex and distributed systems(cloud).

4. Minimal Degree Of Understanding Of The Security Issues

Tackling with the security means properly understanding and prioritizing the concerned issues which act as the vulnerabilities effectively, which is not an easy task. And creating the metrics becomes a nightmare if all the issues are not properly dealt with. Hence, lack of proper knowledge and technical expertise in understanding the key security holes has also created a big hurdle in proper security metric formulation. Now, when everything is moving to clouds-distributed-ness and sharing, the objective of having an efficient mechanism to evaluate the security has become an inevitable need for the cyber security experts.

5. Difficult In Representation Of Metrics

The most difficult task in security metric is the representation of the attributes like complexity, usability and scalability, etc. No standard unit has been proposed. Either the metrics are denoted as ”Low”, ”Medium” or “High” or just as the levels or degrees or percentile.

If two systems with different configurations are selected for security testing, then what will be the exact answers to the following questions?

1. *How to Compare the Security Mechanics of the Two Systems?*
2. *Which Is Most Secure and By How Much?*
3. *Which System Will You Like To Use For Yourself? And Why?*

Here comes the existence and role of the security metrics, but the present definition and the scope of security metrics too will not help in giving the exact answers.

For the answering the first question, the two systems need to be tested for the same security concerns, and threats, keeping the similar relative factors, but will we able to trust the mathematics if both score the same, will be a matter of curiosity than a fact.

Now, for answering the second question (seems so simple), we need a base given by the answer of the first question, but if both score the same, which system is to be called best and which is to be called the worst. Again, we are in the dilemma .So let's suppose first system scored/secured low value in terms of metrics only because it does not favor some special security aspects but worked well and scored high if they were not present . Now, which is to be stated as the most secure is a dubious point to consider.

If one cannot answer the second question properly, then he will surely hang between nine and eleven to make a choice out of the two, and hence the third question will never have a significant answer. It will depend merely on the choice, environment factors.

So, even if we try to devise metrics for measuring security, it will change according to time, situations, attributes and the conditions of the implementations.

The Bitter truth that we learnt from the discussion is that, whatever compliances and procedures we follow to maintain the security, there will always be a flaw, a flaw that cannot be corrected- economically or technically. The only thing that we can do is monitoring and prevention. Though security metrics are of great help but we cannot discard their shortcomings as well.

V. CONCLUSION

From the above discussion, it is sure that to have one metric to be used for all scenarios is a questionable matter. Also, working with several metrics at a time to cover all the security measures, compliance issues, factors etc is another hard thing to achieve but yes, not an impossible task. There will certainly be a possible solution for this - may be implementation of maturity models etc which can be one. Requirement and automated security metric generation is the current information technological necessity, which needs to be extracted out and developed soon to keep pace with the technology growing like anything and essentially.

Our future perspective would be to get involved in developing security metrics and look into embedding of security metrics in the cloud computing security domain with a feel to analyze the security concerns therein. "It would be an interesting matter of interest to bring into the top that has been hidden underneath the realms of security".

REFERENCE

[1] Software test metrics (QConTrain,Consult,Improve), www.qcon.in/simple%20metrics.ppt.

[2] Software metrics guide, http://sunset.usc.edu/classes/cs577b_2001/metricsguide/metrics.html#p1.

[3] Risto Vaarandi and Mauno Pihelgas "Using security logs for collecting and reporting Technicl Security metrics," in the preceedings of 2014 IEEE Military Communications Conference

[4] "The CIS Security Metrics,"The Center for Internet Security, Technical Report, ver1.1.0, November 1 2010

[5] "The Critical Controls for Effective Cyber Defense,"Council on CyberSecurity, Technical Report, ver5.0, 2014.

[6] Mouna Jouini, Anis Ben Aissa, Latifa Ben Arfa Rabai, Ali Mili ," Towards quantitative measures of Information Security: A Cloud Computing case study" in International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 248-262 ;The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2305-0012)

[7] H. L., IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill Osborne, 2010.

[8] D. S. Herrmann, Complete guide to security and privacy metrics. Auerbach Publications, 2007, ISBN: 0-8493-5402-1.

[9] ISO/IEC 27004:2009 standard "Information technology – Security techniques -- Information security management -- Measurement", 2009

[10] L. Krautsevich, F. Martinelli, and A. Yautsiukhin, "Formal approach to security metrics.: what does "more secure" mean for you?" Proceedings of the Fourth European Conference on Software Architecture – ECSA '10, vol. Companion Volume, pp. 162–169, 2010.

[11] Jelen, George. "SSE-CMM Security Metrics." NIST and CSSPAB Workshop, Washington, D.C., 13-14 June 2000. URL: http://csrc.nist.gov/csspab/june13-15/jelen.pdf (10 July 2001).

[12] Alger, John I., "On Assurance, Measures, and Metrics: Definitions and Approaches," Applied Computer Security Associates Workshop on Information-Security-System Rating and Ranking, Williamsburg, Virginia, 21-23 May 2001: 1-2. URL:http://www.acsac.org/measurement (16 June, 2006)

[13] P. Halonen and K. Hatonen, "Towards holistic security management through coherent measuring," 2010, pp. 155–161.

[14] Raddack,Sherley ," Security metrics: measurements to support the continued development of information security technology" for NIST.

[15] Igli TASHI, Solange GHERNAOUTI-HÉLIE ," Security metrics to improve information security system" in Proceedings of the 6th Annual Security Conference, April 11-12, 2007, Las Vegas, NV www.security-conference.org

[16] S. N. Foley, S. Bistarelli, B. O'Sullivan, J. Herbert, and G. Swart, "Multilevel security and quality of protection," in QUALITY OF PROTECTION - Security Measurements and Metrics, ser. Part 3, vol. 23. Springer US, 2006, pp. 93–105.

[17] R. M. Savola, "Towards a security metrics taxonomy for the information and communication technology industry," International Conference on Software Engineering Advances (ICSEA) - IEEE, p. 60, 2007.

[18] R. M. Savola, "Towards a taxonomy for information security metrics," Proceeding QoP '07 Proceedings of the 2007 ACM workshop on Quality of protection - ACM, pp. 28–30, 2007.

[19] R. M. Savola, "A security metrics taxonomization model for software-intensive systems," Journal of Information Processing Systems, vol. 5, p. 197,2009.

[20] Dr. Anton Chuvakin, Chief Security Strategist," Metrics: Optimising Security Operations Performance" November 2005.

