Security Evaluation

Prince Thomas

University of Stuttgart
Institute of Software Technology (ISTE)
70569 Stuttgart, Germany

Abstract. Software security is an idea implemented to secure software against malicious attack and other hacker risks so that the software continues to function correctly under such potential risks. Security is necessary to provide integrity, authentication and availability. The fast growth rate of software and software products makes the software security aspect even more critical. Most organizations these days want their information system to be managed as safely as possible. Security Evaluation is the basic step in achieving this goal for any organization. Security Evaluation is particularly important because of the rapidly changing environment of the information security system or the operation system.In this survey we are performing a study on Software Security Evaluation techniques. A detailed analysis of Qualitative and Quantitative Security Evaluation approaches is being carried out. The suitability and challenges of different methods of each of this approach is studied. The systems where these techniques are being used are investigated to understand the performance of security evaluation methods. Finally, the paper is concluded with the scope of the different security evaluation approaches for real time systems.

1 Introduction

Software security is the idea of engineering software so that it continues to function correctly under malicious attack [**?**] .The fast-growing software systems and huge amount of data handling makes the software security an important aspect in Modern software development. Software security has to be evaluated to make sure that software is minimally susceptible to threats. Evaluation of software security is so challenging because of the non-predictability of the threats and attacker behaviors.

Introduce the different sections of this paper shortly in one or two sentences.

2 Importance of Security Evaluation

Why do we need Security Evaluation?

3 Software Security Metrics

Metrics is a measurement standard which defines what is to be measured, how to be measured and helps the security practitioners to manage the product efficiently. Security metrics is the powerful tool that helps security practitioners to integrate security features into their system. The security metrics are gaining lot of significance now a days because with the help of the data obtained from them software security decisions can be taken and which in turn helps the software developers to secure their software product.

Security metrics help in decision making regarding security-related attributes of a process, system, or organization. In particular, security metrics can be applied to compare the effectiveness of different security mechanisms, or to indicate the degree to which security requirements of an organization are being met. In addition, they can also be used to systematically improve the security level of a system, or to predict this security level in a future point in time. All the people involved in the software life cycle from developers to users use the security metrics for different use cases. For example Technical Personnels(Developers) use security metrics to decide which configuration change is the most effective to increase network resilience, Management members for financial investment on security and finally end users for the trustworthiness of a software products available in the market.

The desired properties of a good security metric are granularity, availability, cost effectiveness, localization and validation[**?**].

3.1 Importance of Software Security Metrics

Significance of security Metrics

3.2 Classification of Security Metrics

The security metrics can be classified as fig1 [**?**].

1. **Target Type:** Security metrics can be categorized according to the target they evaluate. The most common targets assessed (and respective security metrics) are the following:
   (a) **Process:** Process security metrics quantify the security level of a product by assessing its associated development process.
   (b) **Software:** Software security metrics evaluate software security by assessing source code defects, software (mis)configuration, or other vulnerabilities present in software components.
   (c) **Network:** Network Security Metrics(NSMs) assess the security of entire networks or parts thereof.
   (d) **Organization:** Organization security metrics evaluate the physical and personnel security of an organization.
2. **Objective Type:** Based on its objective type security metric can be classified as:

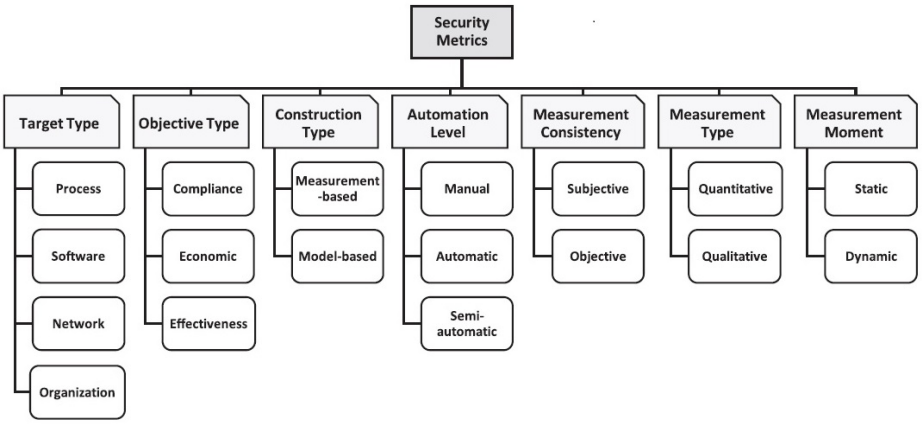

Fig. 1. Classification of Security Metrics

(a) **Compliance:** Compliance security metrics measures how well the security requirements of a target is being met based on the security methods and policies.
(b) **Economic:** Metrics taking into consideration of the financial aspects of security.
(c) **Effectiveness:** It measures how effectively the security measures can perform against security threats or violations.

3. **Construction Type:** Based on the way security metrics is derived, they can be classified as:
   (a) **Measurement-based:** This security metric is used to quantify the security property that is being measured.
   (b) **Model-based:** Here the metrics values are derived from the complex mathematical equations used to define the formal mathematical model of the target. Refer fig2 for a simple representation of a model-based security metric. Examples of models used to evaluate security metrics are attack graphs, Markov models, attack trees, Bayesian networks, etc. In the following sections the detailed evaluation of model-based security metrics is described.

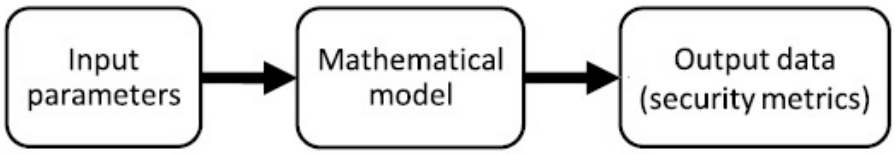

Fig. 2. Evaluation Process of Model-Based Security Metrics

4. **Automation Level:** Based on the level of automation used for the measurements the security metric can be classified as:
   (a) **Manual:** The collection of metrics values are being carried out manually(by humans).
   (b) **Automatic:** Metrics values are being collected with the help of computer system without the intervention of humans.
   (c) **Semi-Automatic:** Measurement is carried out with the help of both humans and computer systems.
5. **Measurement Consistency:** Corresponding to the consistency of the metric values, security metrics can be classified as:
   (a) **Subjective:** Security metric is subjective to the person performing the metric measurement. Different people evaluating the same security property using same method can produce different results.
   (b) **Objective:** Same result is being obtained irrespective of the person performing the evaluation.
6. **Measurement Type:** According to the type of the measurement security metrics can be classified as:
   (a) **Quantitative:** Quantitative security metrics are expressed as percentages or cardinal numbers (i.e., numbers that count something, instead of ordinal numbers, which only denote the position occupied by a given object).
   (b) **Qualitative:** Qualitative security metrics are expressed by labels such as high-medium-low values. Ordinal numbers can also be regarded as qualitative values.
7. **Measurement Moment:** Depending on the instance of time at which the security metrics are applied to assess a given target, they can be classified as either static or dynamic::
   (a) **Static:** Static, or pre-deployment, security metrics are developed to be measured before the assessed target enters operation.
   (b) **Dynamic:** Dynamic, or run-time, security metrics are those developed to be constantly measured, during the operation of the target being evaluated.

Overview of different Security Metrics

Security Metrics for Software Systems[**?**]
"Citation is missing" the paper name: Security Metrics for Software Systems
Phase Wise Review of Software Security Metrics[1]
Survey on Systems Security Metrics[10]

4 Qualitative Software Security Evaluation Methods

Different qualitative evaluation methods will be explained here.
A short introduction about the qualitative approaches.

Different subsections for different methods.
Challenges of Qualitative Security Evaluation.

Qualitative analyzis of software security patterns[2]
Scenario based Security Evaluation[5]
Vulnerability-centric and qualitative risk analysis method[4]
Software System with Vulnerability Life Cycle and User Profiles[?]
"Citation is missing" the paper name: Security Evaluation for Software System with Vulnerability Life Cycle and User Profiles

5 Quantitative Software Security Evaluation Methods

Different quantitative evaluation methods will be explained here.
A short introduction about the quantitative approaches.
Different subsections for different methods.
Challenges of Quantitative Security Evaluation.

Quantifying the security attribute of an intrusion tolerant system[8]
Quantitative Security Evaluation for Software System from Vulnerability Database[6]
Model Based Evaluation, Stochastic approaches[9]
Quantitative evaluation:the vulnerability life cycle; and the attacker behaviour[12]
Machine learning and CVE data base to predict the vulnerabilities in the software[7]

6 Case Study

Different Real time examples where these security evaluation techniques are being used.

[?]
"Citation is missing" the paper name: Attack Modelling and Security Evaluation in SIEM Systems

7 Conclusions

Mention the importance of the security evaluation again and scope of the same in real time scenarios. Future scope of security evaluation methods.

References

[1] R. . A. A. A. Ansar, S A. Khan. A phase wise review of software security metrics. *International Journal of Software Engineering for Smart Device*, 1:25–34, 2017. doi: 10.21742/ijsesd.2017.4.1.03.

[2] A. Alkussayer and W. H. Allen. A scenario-based framework for the security evaluation of software architecture. In *2010 3rd International Conference on Computer Science and Information Technology*, volume 5, pages 687–695, July 2010. doi: 10.1109/ICCSIT.2010.5564015.

[3] Eclipse Foundation. AspectJ – homepage, 2007. URL `http://www.eclipse.org/aspectj/`. Last visited November 14, 2007.

[4] G. Elahi, E. Yu, and N. Zannone. Security risk management by qualitative vulnerability analysis. In *2011 Third International Workshop on Security Measurements and Metrics*, pages 1–10, Sept 2011. doi: 10.1109/Metrisec.2011.12.

[5] S. T. Halkidis, A. Chatzigeorgiou, and G. Stephanides. A qualitative analysis of software security patterns. *Comput. Secur.*, 25(5):379–392, July 2006. ISSN 0167-4048. doi: 10.1016/j.cose.2006.03.002. URL `http://dx.doi.org/10.1016/j.cose.2006.03.002`.

[6] M. T. Hiroyuki Okamura and T. Dohi. Quantitative security evaluation for software system from vulnerability database. *Journal of Software Engineering and Applications*, 06(04):15–23, april 2013. doi: 10.4236/jsea.2013.64A003. URL `http://www.scirp.org/journal/PaperInformation.aspx?PaperID=30073`.

[7] B. Jain, C.-C. Tsai, and D. E. Porter. A clairvoyant approach to evaluating software (in)security. In *Proceedings of the 16th Workshop on Hot Topics in Operating Systems*, HotOS '17, pages 62–68, New York, NY, USA, 2017. ACM. ISBN 978-1-4503-5068-6. doi: 10.1145/3102980.3102991. URL `http://doi.acm.org/10.1145/3102980.3102991`.

[8] B. B. Madan, K. Gogeva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi. Modeling and quantification of security attributes of software systems. In *Proceedings International Conference on Dependable Systems and Networks*, pages 505–514, June 2002. doi: 10.1109/DSN.2002.1028941.

[9] D. M. Nicol, W. H. Sanders, and K. S. Trivedi. Model-based evaluation: from dependability to security. *IEEE Transactions on Dependable and Secure Computing*, 1(1):48–65, Jan 2004. ISSN 1545-5971. doi: 10.1109/TDSC.2004.11.

[10] M. Pendleton, R. Garcia-Lebron, J.-H. Cho, and S. Xu. A survey on systems security metrics. *ACM Comput. Surv.*, 49(4):62:1–62:35, Dec. 2016. ISSN 0360-0300. doi: 10.1145/3005714. URL `http://doi.acm.org/10.1145/3005714`.

[11] M. Shaw. Writing good software engineering research papers: minitutorial. In *Proceedings of the 25th International Conference on Software Engineering (ICSE 2003)*, pages 726–736, Washington, DC, USA, 2003. IEEE Computer Society. ISBN 0-7695-1877-X.

[12] G. Vache. Vulnerability analysis for a quantitative security evaluation. In *2009 3rd International Symposium on Empirical Software Engineering and Measurement*, pages 526–534, Oct 2009. doi: 10.1109/ESEM.2009.5315969.