International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-03, June 2018

Relationship between Vulnerability and Security: A Design Stage

Dr. Brijesh Kumar Bhardwaj, Assistant Professor, Department of MCA,
Dr. R. M. L. Avadh University, Faizabad, India.

Abstract - Several attention have provided by experts for software security at designs level such as vulnerability. However, vulnerability which measure the security attribute have received more attention. In this work, we focus on the design of an object-oriented application and define the complete description of vulnerability respect to security. These studies consent to software designers to discover and fix security vulnerabilities at an early stage, and help compare the potential security of various alternative designs. In particular, we present security concept based on object-oriented property.

Keywords —Security issues, Software quality, vulnerabilities, security

I. INTRODUCTION

Present time, software systems are playing essential and multifaceted parts in our everyday life. The software segments are the heart and noticeable constituent of the all present day and complex systems. Hence, associated what's more, arranged software systems are generally utilized by a few associations for their business choices. These software systems are utilized to oversee and control the business activities and execution [6, 7]. All businesses have extended their business skylines, enhanced the business execution and earned gigantic benefit through the use of the software systems yet at the same time a few associations have additionally brought about gigantic misfortune regarding cash and notorieties because of security breaks, low security standard, violation of security, security dangers and assaults, and prompted software vulnerabilities in heritage and present day systems. Krsul understands that decreasing vulnerabilities ahead of schedule in the development life cycle can diminish extensive exertion for later stages [2]. Suggested changes and alterations at configuration stage may effortlessly be adjusted. Additionally, vulnerabilities presented in the stage show themselves with the progressing improvement life cycle [11]. Yet, nonattendance of any productive instrument or system to deal with the vulnerabilities at this stage [10] has influenced the procedure to time and re-source devouring, and also mistake inclined [8]. Most staggeringly, relatively insignificant work has been done to address security issues at this period of question arranged software [9].

II. SECURITY AND VULNERABILITY

If you are using In this situation, it is important to gauge the software vulnerabilities at configuration stage. In any case, lamentably, both subjective and quantitative procedures to evaluate vulnerabilities at beginning time of software advancement life cycle are as yet missing [5]. Scientists and specialists are over and over upholding for the likelihood of inte-grinding weakness appraisal amid the plan [3, 12]. The reality roused the develop to build up an effective measure for question in order to plan weakness. Vulnerabilities are fault in a system which can be exploited at any point of time and lead to undesired consequences. Unfortunately, the models, metrics and tools available can only be used at later stage of software development life cycle, sometimes after deployment [4]. Threat vulnerability and fault have produced the security risk.

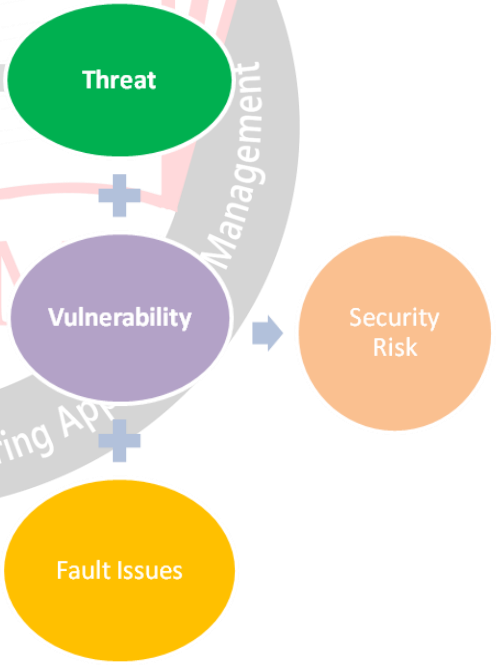

Fig 1 Security Impacts

III. VULNERABILITY ANALYSIS

The study of the vulnerability analysis is similar to the study of the fault issues and their mitigation. Vulnerability is an accidental condition that causes a functional unit to fail to perform its required function. Minimization vulnerability is secure to configuration of software such that its execution can violate security policy [1].

 DOI : 10.18231/2454-9150.2018.0322

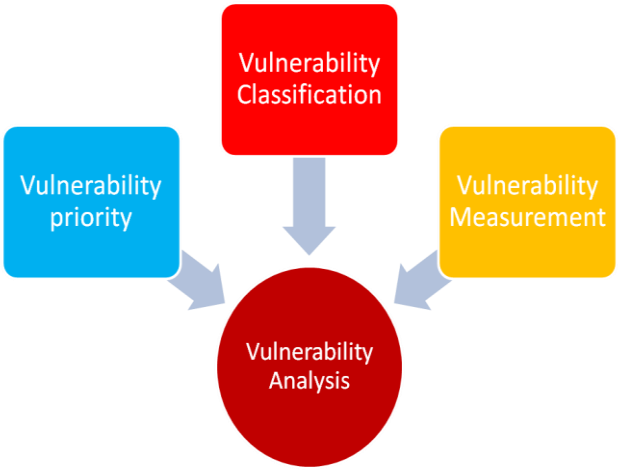

Fig 2 View of Vulnerability analysis

IV. PREMISES

Submission In this paper, Vulnerability is used to improve the software security and security to meet the acceptance criteria of a system. In design stage, the designers assesses and reports on overall design practices and security. The designers can trace vulnerabilities as shown in Figure 2 based on analysis view. The many steps are involved in the vulnerability tracking process are: i) Designers design complete system. ii) Designers generate the fault at minimal certainty. iii) Designers submit vulnerabilities into vulnerability tracking system, entering vulnerabilities description.

V. SUGGESTION

The contents of after successful completion of the systematic study and observation some important critical observation is as follows.

1. If we minimize vulnerability initial phase of software development process may greatly supports to software system.
2. A factors affecting to vulnerability must be identified and then the set of factors relevant at the software development phase should be finalized.
3. Further, the no of affecting factors must be selected in software system then matching with the responsibility of designers.

VI. CONCLUSION

Security at design stage will definitely reduce the cost and effort of software development process. The intent of this paper is to improve highly secured product using a vulnerability minimizing and vulnerability removing approach. In Last, paper concludes that vulnerability is an important category to generate fault issues in software at design level. So designer has taken to a negative impact for vulnerability.

REFERENCES

[1] M. Young, Chu C William, I U Chih-wet, Yuehmin Huang, Boowen Xu. Software Security Improvement: Integrated standard and Models. Proc. Of 28th Annual Intl. Computer Science and Application Conf. (COMPSAC02). 2002.

[2] Krsul, I. V., Software Vulnerability Analysis, PhD Thesis, West Lafayette, Purdue University, 1998.

[3] Alhazmi O H, Woo S W and Malaiya Y K 2006 Security vulnerability categories in major software systems. In: Proceedings of Communication, Network, and Information Security 2006, 138–143

[4] Bishop M and Bailey D 1996 A critical analysis of vulnerability taxonomies. Technical Report, CSE-96-11, Department of Computer Science at the University of California at Davis, September.

[5] Chen Y, Boehm B and Sheppard L 2007 Value driven security threat modeling based on attack path analysis. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 3–6 January, IEEE Press, Big Island, Hawaii, p. 280

[6] Anshul Mishra, D. Agarwal and M. H. Khan, "Integrity Estimation Model: Fault Perspective", International Journal on Recent and Innovation Trends in Computing and Communication, Vol 5, Issue 5, pp 1246-1249, May 2017.

[7] B. Madan, and K. S. Trivedi, "Modeling and Quantification of Security Attributes of Software Systems", Proceedings of the International Conference on Dependable Systems and Networks (DSN'02), IEEE, 2002.

[8] Dai H, Murphy C and Kaiser G 2010 Configuration fuzzing for software vulnerability detection. In: Proceedings of the International Conference on Availability, Reliability and Security, pp. 525–530.

[9]] J. Viega and G. McGraw, Building Secure Software: How to Avoid Security Problems the Right Way, Boston: Addison-Wesley, 2002.

[10] J. H. Saltzer and M. D. Schroeder, "The protection of information in operating systems," in Proc. the IEEE, vol. 63, 1975, pp. 1278–1308.

[11] M. Dowd, J. McDonald, and J. Schuh, The Art of Software Security Assessment Identifying and Preventing Software Vulnerabilities, Addison Wesley Professional, 2006.

[12] Anshul Mishra, Devendra Agarwal and M. H. Khan, "Availability Estimation Model: Fault Perspective", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 6, June 2017.

 DOI : 10.18231/2454-9150.2018.0322