ELK ASIA PACIFIC JOURNAL OF COMPUTER SCIENCE AND INFORMATION SYSTEMS

ISSN: 2454-3047; ISSN: 2394-0441 (Online) Volume 2 Issue 2 (2016)

ELK
Asia Pacific Journals

www.elkjournals.com

ENHANCING THE EFFECTIVENESS OF MEASURING SOFTWARE SECURITY RE PROCESS

MANISHA TIJARE
CS-IT department, Symbiosis Institute of Technology,
Symbiosis International University- Pune, INDIA
manishat@sitpune.edu.in

ABSTRACT

Security in the software has become a significant concern in society which is dependent on software. Secure software could be achieved by adopting different development methods for securing the software. Main aim of the research is to enhance the effectiveness of measuring software security requirement engineering process. This can be measured by writing the secure code when programming so that it would be easy to safeguard software from exploiting. Further work can be extended as a survey to carry out among users to analyze the effectiveness of measuring the security requirement engineering process in the software.

Keywords: software security, requirement engineering and software security requirement engineering process.

1. Introduction

Security in the software explains that, only authorized users could be able to use and access software in an authorized manner. At the same time, assuring security is complicated since software becomes difficult day by day [1]. Software is continuously found to be attacks of vulnerable and compromises rather than adopting latest security protocols and techniques. Therefore, security is one of the main problems of all common issues in the computer security. Thus, security must be taken into consideration and gauged from early development stage like measurement and measures for secure development of software by Microsoft security lifecycle of development, homeland security department and so on [2]. Measurement in the security identifies weak and strength product's security properties. For this it is required to be determined how, what and when to measure [3]. RE (requirements engineering) is the 1st main stage in the development of software. During such stage, developers and consumers have to follow agreement as to the development of software [4] [5]. RE is about perceiving the goals to be achieved by predicted system in the software. Processes in the requirement include 3 consistent activities or functions such as requirements specification, elicitation and validation [6].

ISSN: 2454-3047; ISSN: 2394-0441 (Online) Volume 2 Issue 2(2016)

Technique of RE for security crucial systems has to fulfil these meta-requirements namely early deployment, incrementality, reasoning about alternatives and high assurance [7]. In the early deployment meta-requirements, criticality of requirements in the security technique has to be applicable as soon as in the process of RE, which is into assertions of declarative as they come from stakeholder's documents and interviews. In the incrementality meta-requirements, techniques have to support the model analysis by building intertwining and permit for reasoning with relative to partial models. In the reasoning about alternatives meta-requirements, technique has to make it probable for representing and assessing alternative options thus, best route to security could be chosen. In the high assurance meta-requirements, technique has to permit for formal analysis where and when required because compelling evidence of assurance in the security could be given [8].

2. Problem Identified

Secure software has become a significant concern with maximizing software integration in different aspects of human society. Software is said to be secure if it does not permit availability, integrity and confidentiality of its service, code or data to be compromised. At the same time, many of today's software are unsecure and involve vulnerabilities in security which could be exploited by human beings with malicious intent that would lead to physical and/or financial harm [9]. Issues in generating secure software are exacerbated because of expansions in the network which would connect the software to internet, extensibility of system to adapt with its circumstances for addressing various client needs and ongoing rise in system inflation and complexity [10][11]. Therefore, this research intends to concentrate on enhancing the effectiveness of measuring software security requirement engineering process.

3. Aim

Aim of the research is to enhance the effectiveness of measuring software security requirement engineering process.

3.1 Research Objectives

Following are the objectives of the study:

i. To explore the significance of software security requirement engineering process.
ii. To measure the effectiveness of software security requirement engineering process.
iii. To enhance the effectiveness of measuring software security requirement engineering process.

4. Literature Review

Mariona et al [12] explored the area of security RE. In this research, security RE is divided into 5 phases which permits for a more detailed probing of support provided by each specific phase at each approach. Proposed frameworks showed different aspects which are significant to secure RE. We could be able to check some RE best practices. It was observed that, this survey unveils some challenges that are present today, safeguarding from characterizing how to maximize support of integration for requirements in the security at later development life cycle stages and identifying if approaches that obtain from prior ones are better instead of those generated particularly for security. It was identified that there are main areas which

ISSN: 2454-3047; ISSN: 2394-0441 (Online) Volume 2 Issue 2(2016)

require enhancement when considering security RE; management and later support from stages.

According to the research by Hadavi et al [13] security requirements are classified as non-functional needs, play a main role in developing secure software process. The solutions explained in this research are 1st steps to integrate security into the process of software development. Every solutions, targets a particular section in the process of security requirements engineering. As illustrated, McDermott and Fox solution is adopted in step of security analysis and UMLsec focuses on policies of access controls and way are modelled in process of developing software. These analyses are needed, at the same time they cover only few work parts which is limited to process of modelling. To build integrated tools for modelling, capturing and analyzing security requirements through standard procedures would be one of the future areas of works.

Islam and Falcarin [14] conducted a research to measure the software security RE. In this research, investigators have a adopted a set of requirements in the security which is obtained from goal of software security and accepted standard ISO/IEC 17799:2005 for security of information as a baseline for developing such metrics in the security. It was clear that there would not be a single security measure as it is concept related to multi-faceted. Goal-question-metrics approach is adopted for a comprehensible and structured derivation of metrics. Further, it permits to obviously relate to defined measures back to real goals in the security. Moreover, this would be well-founded fundamental for the metrics in the security.

Salini and Kanmani [15] conducted a survey to study about the security RE. Some of the organizations would prefer a specific and detailed method in the process of security RE; on the other hand, some other organization would adopt an approach which permits them for selecting methods to include in the prior processes. Moreover, another factor in the process is that extent to which organization or project is mission crucial. Apart from these, it was also stated that most of the organizations are recognizing that requirements in the security has to be addressed early in process of lifecycle.

Mead [16] studied about the approach in the measurement of software security RE, aligning it with SQUARE (Square quality RE) method and adopts both revised and original security approach for SE to examine projects which were developed without and with SQUARE. First and foremost, on the side of requirements, we require to analyze other security RE processes to verify if further considerations have to be incorporated to the driver of security requirements. On the side of measurement, we require to apply revised and original considerations for security driver to projects that were generated with the help of different approaches of security requirements or none at all.

Saranya [17] carried out a survey to examine security measures of software RE. Systematic review on measures of security of software RE summarizes cons and pros of the prior approaches. Moreover, discussions related to present trends in SE defines the demands of privacy and security significance of system. At the same time, it was noticed that parametric evaluation gives overall performance of software RE. For security to be built-in a

ISSN: 2454-3047; ISSN: 2394-0441 (Online) Volume 2 Issue 2(2016)

system of software, a good approach of security RE has to be elected for effective process. This research assists in the selection of proper effective approach. Thus it can be inferred from the survey that for security to be built-in a system of software, a good approach of security RE has to be elected for effective process.

According to the survey by Elahi et al [18] discussed about the common practices of security RE. Findings of the survey, demonstrated that businesses mostly attempt to consider security from early development life cycle stages; at the same time security is left to be constructed into the system at phase of implementation. Practical method of security RE requires giving enough methods and guidelines for professionals of software that are not experts in the security and assists them include available knowledge of security from check lists, standards and web portals into analysis of security requirements activities. Security RE methods are required to give ways for identifying trade-offs in the security and assist decision stakeholders make an informed and explicit judgement. It was noticed that practitioners favour assessment of qualitative risk instead of quantitative approaches and such assists them consider numerous factors when compared with alternative solutions for security design. Thus it can be concluded that methods in the security RE requires to give ways for identifying trade-offs in the security and assist decision stakeholders to make an informed and explicit judgement.

5. Research Design

Purpose of the research is to enhance the effectiveness of measuring the process of software security requirement engineering. Security plays a vital role in the software development. Developers have to adopt some guidelines when developing or coding software. Day to-day life is relied on information technology product. Vulnerability in the software could exploit a human. All applications like desktop applications, mobile applications and more have the possibility to be vulnerable. Moreover, attackers adopt those vulnerabilities in the software and attack the system.

In this research, coding of the software is written in C, it would permit user to run some arbitrary code in the system which cannot run particularly in the normal status. Most of the attacks are stack overflow attacks. In this research, stack overflow attacks are illustrated to demonstrate the vulnerability.

5.1 Limitations of the Research

Following are the limitations of the study:

i. This research is limited to software security requirement engineering process.
ii. Findings of the research exclusively considers about enhancing the effectiveness of measuring software security requirement engineering process.
iii. In this particular research, coding of secure software is implemented in C.

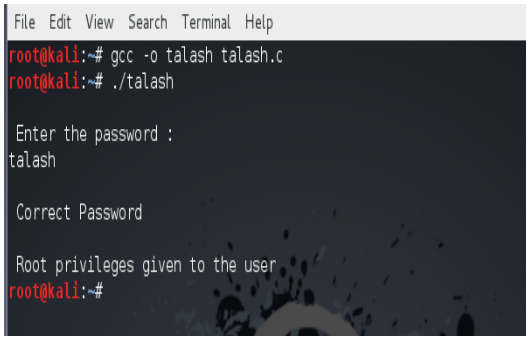
6. Discussion

In this section, stack overflow attacks are illustrated below. This program is a simple program that verifies the password of the user. When user enters right password then, user will be provided all the privileges.

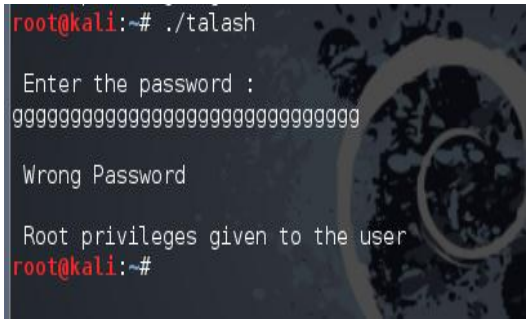
ISSN: 2454-3047; ISSN: 2394-0441 (Online) Volume 2 Issue 2(2016)

```
#include <stdio.h>
#include <string.h>
int main(void)
{
    char buff[15];
    int pass = 0;
    printf("\n Enter your password : \n");
    gets(buff);

    if(strcmp(buff, "talash"))
    {
        printf ("\n no Wrong Password \n");
    }
    else
    {
      printf ("\n yes Correct Password \n");
        pass = 1;
     }

    if(pass)
    {
       printf ("\n Root privilege to the user \n");
    }

    return 0;
}
```

Then the code has to be compiled and executed to check the stack overflow attack.



This screenshot explains about the right password and user privileges. Here, we have taken talash as password to give root privileges to the user. When the user provides correct password that is, talash as an input then the message correct password will be displayed in the screen. Next to that user will be given root privileges.



This screenshot describes about the wrong password and user privileges. When user provides wrong password as an input then the message wrong password will be displayed in the screen. Even though, user has given wrong password, user has given root privileges. Gets () function in the code does not verify the bound in the array. So it simply writes high length string than buffer size. Therefore, over writes in the memory of integer pass.

Therefore, it is significant to write secure code when programming. So that it would be easy to safeguard software from exploiting.

7. Conclusion and Future Work

Security plays a vital role in the software development. Developers have to adopt some guidelines when developing or coding software. Purpose of the research is to enhance the effectiveness of measuring the process of software security requirement engineering. In this particular study, coding of the software is written in C, it would permit user to run some arbitrary code in the system which cannot run particularly in the normal status. Most of the attacks are stack overflow attacks. In

ISSN: 2454-3047; ISSN: 2394-0441 (Online) Volume 2 Issue 2(2016)

this research, stack overflow attacks are illustrated to demonstrate the vulnerability. Therefore, it is significant to write secure code while programming and so that it would be easy to safeguard software from exploiting.

Future work can be extended as a survey to be carried out among users to analyze the effectiveness of measuring the security requirement engineering process in the software. Further strategies will be given to secure software in the process of requirement engineering and will be useful for practitioners and academicians.

References

[1] D. Firesmith. Engineering Security Requirements. Journal of Object Technology, Vol.2, No.1, 53-68, January-February 2003.

[2] R. mead, E. D. Hough and T.R. Stehney, Security Quality Requirements Engineering (SQUARE) Methodology (CMU/SEI-2005-TR-009).

[3] R.Scandariato,B.D. Win, and W.Jossen, Towards a Measuring Framework for Security Properties of Software Framework for Security Properties of Software QoP'06, October 30, 2006.

[4] Olabiyisi S.O., Adetunji A.B, Olusi T.R, "Using Software Requirement Specification as Complexity Metric for Multi-Paradigm Programming Languages", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 3, March 2013.

[5] Balsam A. Mustafa, Hamayoon Ghafory, "Investigating the Inspection Effectiveness of Software Requirements Specification with UML Diagrams: A Concept Paper", Journal of Emerging Trends in Computing and Information Sciences, Vol. 4, No. 11 November 2013.

[6] Kenneth Boness, Anthony Finkelstein, Rachel Harrison, "A method for assessing confidence in requirements analysis", Elsevier Science Direct on Information and Software Technology, May 2011

[7] R. Crook, D. Ince, L. Lin, and B. Nuseibeh. Security Requirements Engineering: When Antirequirements Hit the Fan. In Proc. of RE'02, pages 203–205. IEEE Press, 2002.

[8] C.B. Haley, R. Laney, J.D. Moffett, and B. Nuseibeh, "Security Requirements engineering: A Framework for Representation and Analysis," IEEE Transaction on Software Eng. Vol 34, no. 1, pp. 133-152, Jan/Feb 2008.

[9] M. Bishop, Introduction to Computer Security, Addison Wesley, 2004.

[10] A. Apvrille and M. Pourzandi, "Secure Software Development by Example," IEEE Security and Privacy, IEEE CS Press, 2005, vol. 3, no. 4, pp. 10-17

[11] M.U.A. Khan and M. Zulkernine, "Quantifying Security in Secure Software Development Phases," In Proc. of the 2ndIEEE International Workshop on Secure Software Engineering (IWSSE'08), Turku, Finland, 2008, IEEE CS Press, pp. 955-960, 2008

[12] Mariona et al (2008), Security Requirements Engineering: A Survey, ISR Technical Report.

[13] Hadavi.M.A et al (2008), Security Requirements Engineering; State of the Art and Research Challenges, Proceedings of the International Multi-

ISSN: 2454-3047; ISSN: 2394-0441 (Online) Volume 2 Issue 2(2016)

conference of Engineers and Computer Scientists.

[14] Islam.S and Falcarin.P (2011), Measuring Security Requirements for Software Security, Retrieved on: 22nd July 2015, Retrieved from: http://www.researchgate.net/publication/238594490_Measuring_security_requirements_for_software_security

[15] Salini.P and Kanmani.S (2011), A Survey on Security Requirements Engineering, International Journal of Reviews in Computing, vol 8.

[16] Mead.R (2012), Measuring the software security requirements engineering process, IEEE 36th International Conference on Computer Software and Applications Workshops.

[17] Saranya .R (2014), Survey on Security Measures of Software Requirement Engineering, International Journal of Computer Applications, vol 90-no 17.

[18] Elahi.G et al (n,d), Security Requirements Engineering in the Wild: A Survey of Common Practices, Retrieved on: 22nd July 2015, Retrieved from: http://www.cs.toronto.edu/~gelahi/COMPSAC-SecinWild_11.pdf