Quest Journals
Journal of Software Engineering and Simulation
Volume 2 ~ Issue 1 (2014) pp: 01-03
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Securo-Phobia: A New Challenge to Usage of Security Technologies

A. Agrawal[1], R. A. Khan[2]

Received 21 December, 2013; **A**ccepted 06 January, 2014 © The author(s) 2013. **P**ublished with open access at **www.questjournals.org**

ABSTRACT:- *The main objective of the security is to provide restricted access to the security intensive information whereas the objective of usability is to provide easy access of the secured application and this is the point where conflict begins. An effort has been made to enlighten a great barrier to the usage of security technologies and is termed as secure-phobia. This is going to be one of the most challenging for the security providers, and must be addressed for optimal usage of the security technologies.*

Keywords: - *Software security, software usability, security technology, software quality, human psychology.*

I. INTRODUCTION

Software security is concerned with maintaining confidentiality, integrity and availability of data managed by the software[1]. Often security issues are overlooked by software developers during software development or taken into consideration very late in the software development process that to of using some traditional mechanism including penetration testing, add-on security software and penetrate-and-patch[2]. It is believed that security must be addressed well in advance right from designing phase of software development life cycle. Incorporating security in early stage reduces the developmental budget and effort[2-3]. Therefore, it has become an established fact that effort needs to be made in bringing security mechanisms in design phase in order to properly address security issues while developing secure software. Researcher has made an effort in this direction on evolving a mechanism to enhance security of software under development by ensuring security of object oriented design.

Usability of software is defined as the capability of the software system to be understood, learned and used by user[4]. Similar to security, usability features can also not be sprayed into the software after its development; rather these must be incorporated during the design phase of software development life cycle[5]. Though, security and usability both are the attributes of quality, a trade off exits between both of them. Researcher has made a critical review of the literatures and established that security and usability are reciprocal to each other in context. Undoubtedly, process of improving security makes usage restricted. On the other hand, usability, by nature, will always try to facilitate the end users by providing maximum facility for optimal utilization without any restriction. When both, security and usability, are taken into account, the development process of secure software becomes more challenging. Therefore, researcher has taken the opportunity to reveal the basic reason of their conflicting nature. The researcher tried to pinpoint the reasons so that both can be taken in a balanced way to achieve a neutral point in order to guarantee for the development of secure software application with optimal utilization. Researcher, as a result, found during the literature survey that the following pertinent issues form the strong basis for their conflicting nature:

- Security is a technical issue whereas usability is purely psychological[6].
- Security focuses on the people who want to abuse the software whereas usability focuses on the people who want to use the software[7].
- Security believes that vulnerabilities in the software attract attackers whereas usability vulnerability proves to be the weakest link in the security chain of the software[8].

*Corresponding Author: A. Agrawal
Department of Computer Science, Khwaja Moinuddin Chishti
Urdu, Arabi-Farsi University, Lucknow, India

These issues prove that security and usability have always been two opposite school of thoughts. There is a common belief that if anything is kept under different locks, automatically the ease of accessing the same will be difficult, which as a result will reduce its usage. To make it more usable, it must be easily available as human psychologies always avoid stress.

Rest of the paper is organized as: section 2 discusses how security mechanisms develop security phobia in human mind. Section 3 presents major findings of the study and finally paper is concluded in section 4.

II. SECURITY MECHANISMS AND SECURITY PHOBIA

Security mechanisms are designed and implemented to increase user confidence in the software but actually it is not happening. Users are overwhelmed with the increased burden of the security technology. This is the reason users have developed Security Phobia (Securo-Phobia). The main reason behind security phobia is the ignorance of human psychology during design and implementation of security mechanisms[5]. Available literature about information security is flooded with strict security mechanisms and approaches. Industry and researchers both are claiming that their approaches are securing the information in a better way. Unfortunately, these approaches are not easily adaptable by a common user and thus are failed to be acceptable. Whether these approaches belong to network security or software security, one thing is common in all of these, which is noting but the ignorance of the fact that these are meant for the human and these must be easily understandable and usable by the human.

The flip side of the problem is that now a day’s almost everything is automated. There is almost no choice but to use the computers and its software whether it is fund transfer or booking a ticket for flight. This is a very tough situation when one is neither able to adapt nor escape. Few of many usability reasons are worth to discuss. Just after entering into system, end user falls into pool of security related overwhelming experiences: what to respond on technical security warnings, how to deal with user interfaces, and above all, a tough authentication process. Various mechanisms available for authentication process including passwords, biometrics etc. again imposes mental pressure to the user.

When the user does not know what to respond on security warning, the user would choose the alternative with which he could continue with his work or when he is not able to remember the long passwords, he would write them. As a result, the user becomes the most vulnerable link of the security chain and contributes to enlarge the attack surface of a system. Unfortunately, all the research which claims to address technical vulnerabilities present in different databases including NVD, OSVDB etc fails to address this critical security usability vulnerability[9].

Most surprisingly, it is not getting the level of attention it must attain from the industry and academia. The available literature which claims to address usability issue while working on security just talk either about friendly user interfaces or at the max they advocate security education of human. They are of course right at their part but what about the problem like tedious authentication process where people are suggested to change long passwords frequently. Suppose if a person have ten accounts having two dimensional authentication process then what mental stress he will have to face while remembering the passwords. The problem would be worsening when he would have to change the password according to security reasons.

Of course, there are other authentication process but they have their own drawbacks which again contribute to increasing mental pressure on the user. They have fear about stealing of their passwords if he writes them on paper (psychological pressure) and if he does not write then he has fear of forgetting the passwords (mental pressure). He has fear of disclosing his important information while he responds to the technical security warning whose interpretation is beyond the understanding of a common user (restricting of usage). This is one of the problem, a common user is facing. Similar kind of problems is increasing security fear inside human being and they are developing a kind of securo-phobia.

III. MAJOR FINDINGS

It has been reported that even the best security mechanisms are exploited by exploiting human psychology. While addressing the fact, objectives of security and usability should be taken into consideration. The main objective of the security is to provide restricted access to the security intensive information whereas the objective of usability is to provide easy access of the secured application and this is the point where conflict begins. A security technology should not be successfully implemented until it is accepted by the human for whom it is developed. One once it is accepted by the actual users, the fear of operating the same will be reduced, and usability of the application will be increased without compromising security.

To deal with the security intensive information, strict security mechanisms are in demand. Because of the enhanced security; its breach has become very difficult. But, there is a great chance of exploiting the end users psychology by means of retrieving the vulnerable information in different ways. Security technologies may be breached even in presence of excellent security mechanism by the following ways:

- By way of restricting the usage/ reducing usability.
- By way of creating psychological pressure.
- By way of increasing mental stress.

IV. CONCLUSION

The research problem under reference aimed to address the burning issue for the design of object oriented software. The idea is to address security and usability issues together right from the very beginning of the development of object oriented software with the help of object oriented design constructs including coupling, cohesion, inheritance and encapsulation. A metric based approach is to be developed. The approach will state objectively the effect on usability on addressing security of an object oriented software design at the design phase itself. The problem could not be addressed completely because of the suspension of the project in mid. But, the problem which has never been taken into consideration has been defended properly by the researchers. In addition to this, a strong idea has been generated and validated to achieve a common neutral point of both security and usability. This will form a basis for other researchers and practitioners to take the challenge to achieve the target point in order to deliver secure software with optimal usability of software application. This will help in reducing the end users securo-phobia.

REFERENCES

[1]. B. D. R. Marino. and H. M. Haddad, “Security Vulnerabilities and Mitigation Strategies for Application Development,” Proc. IEEE Conf. on Information Technology: New Generations (ITNG’09), IEEE, 2009, pp. 235-240.

[2]. D. Byers and N. Shahmehri, “Design of a Process for Software Security”, Second International conference on Availability, Reliability and Security (ARES’07), IEEE, 2007, pp. 301-309.

[3]. J.Viega & G. McGraw, “Building Secure Software” Addison Wesley, 2005.

[4]. L. Aversano, T. Bodhuin, G. Canfora and M. Tortorella, “A Framework For Measuring Business Processes Based on GQM”, Proc. 37th Hawaii International Conference on System sciences, IEEE, 2004, pp. 1-10.

[5]. K.-P.Yee, “Aligning Security and Usability”, IEEE Security & Privacy, IEEE ,Sep-Oct 2004, pp. 48-55.

[6]. R. Anderson and T. Moore, “Information Security: Where Computer Science, Economics and Psychology Meet ”, Philosophical Transactions of the Royal Society, vol. 367, no. 1898,2009, pp. 2717-2727.

[7]. I. Flechais, C. Mascolo and M. A. Sasse, “Integrating Security and Usability into the Requirement and Design Process”, International Journal of Electronic Security and Digital Forensics, vol. 1, no. 1, 2007, pp. 12-26.

[8]. A. Josang, B. AlFayyadh, T. Grandison, M. AlZomai and J. McNamara, “Security Usability Principles for Vulnerability Analysis and Risk Management”, Computer Security Application Conference, 2007, pp. 269-278.

[9]. A. Josang, B. AlFayyadh, T. Grandison, M. AlZomai and J. McNamara, “Security Usability Principles for Vulnerability Analysis and Risk Management”, Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual, pp. 269-278.