Model for Usable Security in HCI

Ms. Shubhangi T. Raut[1], Dr. Abha S. Khandelwal[2], Dr. Satish Sharma[3]
[1] Dept of Electronics and Computer Science
[2] Head, Dept. of Computer Science, Hislop College
[3]Head, Department of Electronics and Computer Science
[1, 2, 3] RTM Nagpur University, Nagpur

Abstract- *All users who use computer system demands some form of security. A user is a single entity whosebehavior is uniquely identified within a computer-based system. But as it's a natural fact that human being are never satisfied on a single entity, their expectations are continuously get expanded and human beings are users. While interacting with computer system, user demands not only for security but also for a usable system. Hence for a successful interaction a system should be usable as well as secured. The security usability threat model developed by, Ronald Kainda and Ivan Flechais and A.W. Roscoe in the year 2010 provide a secured usable system but to a certain extent. Hence this paper focuses on the more usability as well as security attributes which increase the level of a usable secured system in Human computer interaction (HCI). This paper examines the current approaches for usability and security of Human Computer Interaction (HCI) and proposes a new model for a usable security of HCI which brings together different factors, criteria and data defined in previous model of usability and security for HCI.*

Keywords- HCI, Security, Usability, Usable system

I. INTRODUCTION

The term usability plays an important role in human life. Human Computer Interaction (HCI) and security has identified the need to improve usability. Security and Usability are quite opposite terms. Security is aimed at making undesirable actions more difficult while usability aims at making desirable ones easier for the user. A usable system will minimize unintentional errors, while a secure system will aim at ensuring that undesirable actions in a system are prevented. Usability evaluations of secure software systems require procedures that deviate from standard HCI techniques. A usability evaluation of secure software should not focus on usability to the exclusion of security: in certain cases it is necessary, for the purposes of security, to include behavior that is complex. Conversely it is possible to weaken the security of a system by simplifying or automating certain elements, which usually improve usability. Usability and security have a closely tied relationship, it is important to consider both factors when evaluating a system.

HCI is about designing computer systems that support people so that they can carry out activities safely. The proposed model for usable security is a conceptual view which lays down the focus areas to demonstrate the usability as well as security of a system. In the field of usability evaluation of HCI through security perspective, issues related to usability and security measurement such as concept related to usable security, characteristics as well as sub-characteristics of usable security there is one point on which researchers generally agree: there is no well-defined model that has been proposed to evaluate and quantify a usable security of HCI system. So considering the issue, this paper developed a proposed model for usable security which analyses different sub-attributes of usability as well as security.

II. BACKGROUND

The central research question in this paper is:

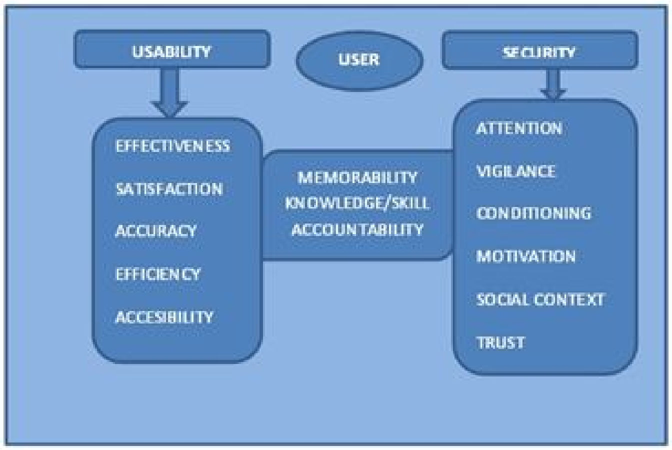
"How is it possible to ensure usability of HCI without compromising security and vice versa?"

Security and usability are both essential in the HCI process. It is broadly held that security and usability are odds to each other in system design but there are several cases in which security and usability can be synergistically improved by reviewing the usable security approach. Multiple offices and banks spend millions of money on secure access devices to maintain security of system, but most of the time they forget the main issue related to the weakest link in the security chain i.e. human beings as "Humans are the weakest link in security chain".In developing the proposed model for usable security, the current HCI Security usability studies are considered and identified the main factors that were the target of measurement for both usability and security

III. PROPOSED MODEL FOR USABLE SECURITY

HCI Security is central to the user. The user needs a system that is both secure and usable. Third party users should not be able to enter in system. Hence a security threat model is required to provide usable security to user. A proposed model is different from a security model. Model is presented in a figure.

Proposed model centers around a user who is not able to break system that means he is an authentic user. The proposed model consists of various factors that needed to investigate during evaluation of usability and security. It identifies factors that are related to either usability or security and also factors that are related to both. Both security and usability factors relate to the authentic user who cannot harm the system. Following are the factors of a proposed model:



Effectiveness: A system is only useful if its users are able to achieve intended goals. Effectiveness is the capability of a software system to carry out the specified task successfully. Effectiveness is measured by whether users are able to complete a particular task or not.

Effectiveness = f (Quantity * Quality)

Task Effectiveness = (Quantity * Quality) % / 100

Satisfaction: Satisfaction provides freedom to user from his discomfort and provide positive attitude towards a computer system. User satisfaction can be assessed through interviews and rating scales.

Accuracy: accuracy is important factor in this model. Basically the accuracy factor was identified in authentication and device pairing studies. Accuracy demands on users are impacted by other demands such as recall of required information, environmental, or personal factors.

Efficiency: Efficiency is described as the number of tasks that a user can perform using software per unit. It could be measured by the task completion rate and task completion time. Efficiency is formulated by calculating the amount of efforts given by user.

Efficiency = Effectiveness / task time

Accessibility: accessibility is a new attribute in this model. Accessibility is defined as, the degree to which software can be used comfortably by a wide variety of people including those who required assistance technologies like voice recognition or screen magnifiers.

Memorability: memorability is an important aspect that does not influence usability of a system but can significantly influence security as well. Various authentication system require user to memories secrets code that they should recall whenever they want to be authenticated by a system.

Knowledge/skill: Various usability definitions often use learnability to refer to how easy it is to learn to use a system. This is based on the assumption that users will learn or actually attempt to learn and understand the system.The above explained factors have a direct effect on the usability of a system. A usability evaluation must determine which factors apply to a specific application and context.

Security Factors:

Attention: this is first attribute of security in proposed model of usable security. . This factor totally depends on user.Users can easily be distracted from their tasks. For Security, tasks must not demand undivided attention from users as this is likely to cause frustrations, and possibly security failures.

Vigilance: In this factor user tend to expect users to be alert and proactive in assessing the security state of a system. For example, experts on web site security indicators did not even look in places where those indicators were, hence falling for simulated phishing attacks which they would have avoided.

Motivation: users have different levels of motivation to perform security tasks in different circumstances. For example, participants in a study indicated that they would prefer typing passkeys longer than 6 digits for financial transactions exceeding a certain monetary value. In this case, participants saw the risk to be more direct to them (losing money) than in a case where risk is perceived to be low or directed at someone else.

Memorability: this is the most important factor for authentication of systems. User often requires to memories secrets that are difficult for someone but they are easy for others to guess. As the number of secrets one has to memories increase, it can become more difficult to recall a particular secret when working with a system asking for one particularly if the system is not used frequently. As a precaution to avoid forgetting and resetting, users write down these secrets. This in itself impacts the security of the system.

Knowledge/skill: users' knowledge or skill level plays a major role in the security of a system. Many users enter sensitive information on vulnerable websites because they do not have the knowledge or skill to differentiate between a secure and an insecure website. Users also share sensitive information unknowingly because they lack knowledge about the operation of systems. An evaluation of a secure system should ask questions such who are the users? What do they know about the system? What should they know?

Social context: humans are social beings. They help each other and share various things. While from our childhood we also have learned that sharing is generally a good thing but it is bad for security. if users share their security secrets. For example, users working on a particular project shared one digital certificate rather than each having their own as intended by system designers.

Conditioning: repetitive security tasks for which users can predict an outcome can become a threat to the security of a system. A common example is popup boxes that ask users whether a particular certificate should be trusted or not.

Trust: trust plays an important role in security of a system. When users shared their passwords for various reasons, they think that they are making their task easy due to their laziness but they didn't get that due to sharing password's, they are increasing the risk in their security chain. This occurs due to trust. As user share their confidential data only to the known people to whom they trust.

IV. CONCLUSION

Secure system has properties that differentiate them from other systems. In This paper we have developed a proposed usable security model and analyses different sub-attributes of usability as well as security. We have proposed an extended model for conducting security-usability analyses. We have used usage scenarios and threat scenarios to understand and identify both system and external elements that are threats to a system's usability, security, or both. Usage scenarios are used to identify areas that may hinder the usability of a system, whereas threat scenarios are used to identify areas that may help non-malicious users to break the security of the system. When a system's threat scenarios are more usable compared to the usage scenarios, users are more likely to perform the former. External factors, too, may cause users to perform actions that they may not normally perform.

This is the initial effort and future work will involve adding detailed metrics that can be used to calculate the possibility of users performing a threat scenario over a usage scenario.

REFERENCES

[1] K.-P. Yee, "Aligning Security and Usability," IEEE Security & Privacy, vol. 2, no. 5, pp. 48–55, 2004.

[2] I. Flechais, "Designing secure and usable system," Ph.D. dissertation, University of London, 2005.

[3] D. Balfanz, G. Durfee, D. Smetters, and R. Grinter, "In search of usable security: five lessons from the field," IEEE Security & Privacy, vol. 2, no. 5, pp. 19–24, 2004.

[4] R. Anderson, "Why cryptosystems fail," CCS '93: Proceed-ings of the 1st ACM conference on Computer and communi-cations security, pp. 215–227, 1993.

[5] A. Whitten and J. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in Proceedings of the 8th USENIX Security Symposium, August 1999, Washington, 1999, pp. 169–183.

[6] A. Adams and M. A. Sasse, "Users are not the enemy," Commun. ACM, vol. 42, no. 12, pp. 40–46, 1999.

[7] A. Brostoff, "Improving password system effectiveness,"

[8] S. L. Garfinkel and R. C. Miller, "Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express," in SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security. New York, NY, USA: ACM, 2005, pp. 13–24.

[9] L. Cranor and S. Garfinkel, Security and Usability. O'Reilly Media, Inc., 2005.

[10] R. Kainda, I. Flechais, and A. Roscoe, "Usability and Security of Out-Of-Band Channels in Secure Device Pairing Proto-cols," in SOUPS '09: Proceedings of the 5th symposium on Usable privacy and security, 2009.

[11] A. Kobsa, R. Sonawalla, G. Tsudik, E. Uzun, and Y. Wang, "Serial Hook-ups: A Comparative Usability Study of Secure Device Pairing Methods," in SOUPS '09: Proceedings of the 5th symposium on Usable privacy and security, 2009.

[12] E. Uzun, K. Karvonen, and N. Asokan, "Usability Analysis of Secure Pairing Methods," in Financial Cryptography and Data Security, 2007, pp. 307–324. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-77366-5 29

[13] A. Whitten, "Making Security Usable," Ph.D. dissertation, Carnegie Mellon University, 2004.

[14] J. Nielsen, Usability Engineering. Boston; London : Aca-demic Press, 1993.