Volume 7, Issue 4, April 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Usability of the Secured System - An Overview

Shubhangi T Raut*
Research Scholar, R. T. M Nagpur University,
Nagpur, Maharashtra, India

Dr. Abha S. Khandelwal
Head, Dept. Of Computer Science, Hislop College,
R. T. M Nagpur University, Nagpur, Maharashtra, India

Abstract— The concept of Human computer interaction has been accepted as a very promising and challenging area for research in today's world. HCI has grown rapidly and steadily, attracting professionals from many other disciplines. With a growing recognition for the need to design systems that are both secure and usable, HCI Security is increasingly becoming active. The relationship between a human and computer involves many factors. Various human factors play an important role while dealing with HCI or we can say that HCI's roots are present in human factors. A fundamental rule of designing security mechanisms is that, as the mechanisms grow more complex, they become harder to configure, to manage, to maintain, and indeed even to implement correctly. Many people believe there is an inherent tradeoff between computer security and usability. For ex. a computer without passwords is usable, but not secure. The lack of consideration of the exact Human Factors is the main issues in security and usability. The aim of this paper is to provide a overview of secure and usable systems, and how designers can ensure that security mechanisms are usable and effective in practice.

Keywords— HCI, Input, Output, Security, Usability, User

I. INTRODUCTION

During the 1980s, using computers required knowledge and experience. Nowadays, the interaction has been simplified drastically and no specialized knowledge or experience needed to run simple and everyday tasks. People have the ability to manage their personal lives, their jobs, their health, their education and entertainment through computing devices due to the fact that the devices and software have more user-friendly interfaces. With the development of the Web, the significance of proper interaction becomes even more important which otherwise result in security incidents and breaches. The most commonly accepted definition of HCI is "Human-computer interaction is a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them."

The main objective of HCI is to produce usable and safe system. In order to produce a system with good usability, designer must attempt to:

- Realize the factors that determines how people use technology
- Develop tools and technique to enable building suitable system
- Achieve efficient, effective and safe interaction
- keep user at first

Human computer interaction is made up of three components:

- Human – The people who interact with the system. This may include groups of people or specific individuals.
- Computer – The computer or hardware device that is being interacted with which includes devices beyond the standard desktop computer. For example: PDA, cell phone, car, door lock and ATM.
- Interaction – The sharing of data between the computer and the human.

In human-computer interaction (HCI) knowledge of the capabilities and limitations of the human operator is used for the design of systems, software, tasks, tools, environments, and organizations. The purpose is generally to improve productivity while providing a safe, comfortable and satisfying experience for user.

It is commonly said that the security must be designed into a system and not added as an afterthought, however in practice, most systems have security added on, which can result in security that is ill-suited, expensive to maintain and inefficient. The reasons why some systems continue to be designed without security can fall into three categories:

1. Security is deliberately sacrificed in the design. For example because of time and cost concerns.
2. Security is not viewed as important.
3. Security is desired, but the wrong decisions are made during design and implementation.

II. INTERACTION MODEL

With the rapid development and deployment of Information Systems, Information and Communication Technology, and related services the security has become critical. Security deals with the various factors like deterrence,

avoidance, prevention, detection and reaction to events in a system which is unwanted to the owner of that system. This definition of security is useful and in that it distinguishes between following:

1. How security works – deterrence, avoidance, prevention, detection and reaction.
2. What security applies to – undesirable events in a system.
3. Who requires security – the owner of the system.

Formal methods are used extensively in many fields of computer security. They are rarely used in HCI- even for security critical systems .The main reason is that HCI does not deal with the interaction of two machines but with the interaction of a machine and a human. As the behavior of a machine can be described precisely with formal methods, but human behavior is more difficult to describe in a precise way. Security and usability are both essential for the effective use of system. The goal of HCI is to produce usable and safe system, as well as functional systems. In order to produce computer system with good usability, developer must attempt to: Understand the factors that determine how people use technology, in general the system.

The communication between the user and the system has four parts:

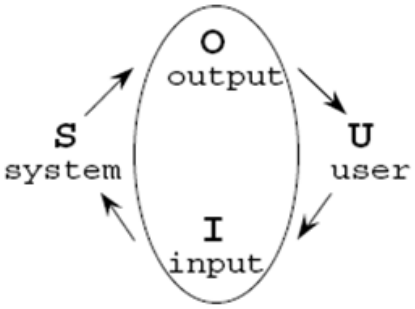

Fig. 1 Interaction model

- ***User***
- ***Input***
- ***System***
- ***Output***

Interaction models help us to understand what is going on in the interaction between user and system. They address the translations between what the user wants and what the system does. The interaction takes place within a social and organizational context that affects both user and system. The user acquires a central role and the design and development of any technological product is made according to their needs and specifications. As many problem solving solutions involve removing the factor that is causing the problem. In our case, that would require "user less," computer systems. However, preventing users from interacting with systems also prevents work from getting done. Since users cannot be prevented from interacting with the system, what can be done?

III. SECURITY AND USABILITY

Usability is defined as "the ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component." Usability and security are attributes that are odd to each other, because security is aimed at making undesirable actions more difficult while usability aims at making desirable ones easier for the user. Security mechanisms are only effective when used correctly. For example, whenever users change their passwords periodically may improve security but increase burden on users. This can arise the possibility of forgot passwords, as it is very difficult to remember passwords to their workstations. A problem that typically comes with the used of standard passwords is the user themselves. Or, a user can avoid password and may be replaced passwords by hardware token; this relieves the user of having to remember a password but again keep a new burden on the user to carry the token wherever that access is required. A usable system will minimize unintentional errors, while a secure system will aim at ensuring that undesirable actions in a system are prevented. Usability necessarily has different meanings in different contexts. For some, efficiency may be a priority, for some, learnability, for others, flexibility. But in a security context, it is like whatever needed in order for the security to be used effectively. Past researches [1] has claimed that configuration errors are the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical. As one solution, we might attempt to educate the user for the use of computer security. This is a worthy goal, but how is it to be accomplished? We can try to minimize the need for security management by users, automating security mechanisms as much as possible, and invoking legal penalties for the trespassing that does occur. Again, these are worthwhile strategies, but insufficient as a solution. Automating the encryption of a communication can sometimes work well, since in the case of encryption it may be clear what the security mechanism is meant to accomplish. As for the legal penalties, how is the user to know when someone has trespassed, so that he or she can take legal action? The theft of private data does not necessarily leave any evidence behind. Even when there is evidence, a lawsuit is far more realistic as a course of action for a corporation than for an individual home computer user.

Finally, we can work on improving user interfaces for computer security, in the hope that we can find ways to make security sufficiently clear and intuitive that most people can use it effectively. It is tempting to think that this is a task that can be given to user interface designers after the security mechanisms have already been developed, but we believe that will not lead to effective security, for the following reasons:

- Design techniques that create good user interfaces for other types of software are ill-fitted to creating user interfaces that enable effective security.
- There is as yet no body of security-specific user interface design techniques. There are no recognized examples of good user interface design for security, and human-computer interaction (HCI) research to date has not focused much on security applications.
- The development of security-specific user interface design techniques requires expertise in security as well as in HCI. Because security concepts are often subtle to understand, and because they must be used perfectly, an HCI expert who is unskilled in security is likely to produce a system where the security mechanisms are not used in exactly the correct fashion. Moreover, good security software should teach a user about underlying security concepts – which certainly requires that its designer have a fundamental understanding of those concepts.

It is likely that many security mechanisms have been developed which simply cannot be made usable for the general population, as they are too complicated or too arcane. No user interface can make these complex mechanisms accessible. To avoid this, HCI considerations need to be addressed early in the process of designing the security mechanisms, not left until the finished design is handed off to a user interface team.

IV. CONCLUSIONS

Usability concept has been under focus over the years and has evolved with different definitions by researchers. Different attributes have been built for a clear view of usability and its aspects. The usability has been decomposed into several sub attributes which are hypothetical constructs to define the success of a system. User involvement plays key role in determining the software usability after it has been developed. Currently the only effective means of ensuring that a secure system is usable is to periodically conduct evaluations and test user responses. But the additional problem is that designing, conducting and interpreting an evaluation currently requires specialist knowledge. Whilst in the field of HCI this is common practice, this knowledge is not widespread in the security community and this poses an additional difficulty.

REFERENCES

[1] Foundations and Trends in Human–Computer Interaction Vol. 1 No. (2007) 1–137_c 2007 G. Iachello and J. Hong

[2] N. S. Good and A. Krekelberg, "Usability and privacy: A study of KaZaAP2P file-sharing," in Proceedings of CHI 2003, pp. 137–144, ACM Press.

[3] B. Brunk, Understanding the Privacy Space. http://www.firstmonday.org/issues/issue7 10/brunk/, 2002.

[4] E. Ball, D. W. Chadwick, and D. Mundy, "Patient privacy in electronic prescription transfer," IEEE Security and Privacy, vol. 1, no. 2, 2003.

[5] M. S. Ackerman and S. D. Mainwaring, "Privacy issues and humancomputer interaction," in Security and Usability: Designing Secure Systems that People Can Use, (S. Garfinkel and L. Cranor, eds.), pp. 381–400, Sebastopol, CA, USA: O'Reilly, 2005.

[6] U. Jendricke and D. Gerd tom Markotten, "Usability meets security: The identity-manager as your personal security assistant for the internet," in 16th Annual Computer Security Applications Conference (ACSAC 00), New Orleans, LA, USA, 2000.

[7] C. Jensen, C. Potts, and C. Jensen, "Privacy practices of Internet users: Selfreports versus observed behavior," International Journal of Human-Computer Studies, vol. 63, 2005

[8] Sutcliffe, "On the effectuve use and reuse of HCI knowledge," in Human-Computer Interaction in the New Millennium, (J. M. Carroll, ed.), ACM Press, 2000.

[9] D. Povey, "Optimistic security: A new access control paradigm," in Proceedingsof 1999 New Security Paradigms Workshop, pp. 40–45, ACM Press.

[10] Hewett, Baecker, Card, Carey, Gasen, Mantei, Perlman,Strong and Verplank (1996) ACM SIGCHI Curricula for Human-Computer Interaction. Last updated 2004-06-03. http://sigchi.org/cdg/index.html.

[11] Nielsen, J. Usability Engineering. Morgan Kaufmann.(1993)..

[12] Barton, B.F. & Barton, M. S. (1984) "User-friendly password methods for computer-mediated information systems. Computers and Security, 3, 186 - 195.

[13] Alan Dix and Colin Runciman. Abstract models of interactive systems. In P. Johnson and S. Cook, editors, HCI'85: People and Computers I: Designing the Interface, pages 13{22. Cambridge: Cambridge University Press, 1985.

