Engineering Sciences International Research Journal
ISSN (Print) : 2330 – 4338 ; Volume 1 Issue 1 ǁ February. 2013 ǁ

Usability Evaluation of Human Computer Interaction for Security

Shubhangi T. Raut[1], Abha S. Khandelwal[2]

Abstract: With the development of the personal computer, it was possible for many users to interact with their own personal computer; which was available to only few people in earlier days. Today, the world we live in has become suffused with computer technologies. They have created change and continue to create change. It is not only on our desktops but it is in all aspects of our lives, our communities, and in the wider society of which we are a part. Because of the ease with which information can be accessed, there is continuous increase in the number of security incidents. Such violation of security can have serious consequences like Theft and Fraud, Loss of Confidentiality, Loss of Privacy, Loss of Integrity, Loss of Availability. Many security methods have been developed however; these methods may not accomplish their intended objectives if they are not used properly. This paper provides the overview of usability evaluation of HCI for security.

Keywords*:* Human-Computer Interaction, Privacy, Security, Usability.

1. INTRODUCTION

In the last few decades HCI has grown to be broader, larger and much more diverse than computer science. Human-computer interaction (HCI) is the area of intersection between psychology and the social sciences, on the one hand, and computer science and technology, on the other. With the increasing use of computer systems, Information security is becoming increasingly important and more complex as business is conducted electronically. It is this combination of high usage of computers nowadays and increasing dependence on technology for business that makes the need for computer security more important. In the modern Internet-capable computer environment, it is possible for a large user population to access information at the desktop from sources around the world. Because of the ease with which information can be accessed, there is continuous increase in the number of security incidents and breaches.

Such violation of security can have serious consequences, including theft of confidential documents, unauthorized modification of systems and data, spy on other user sessions, masquerading as another user, misrouting communications, denial of service, and so on. Since average citizens are now increasingly make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical. 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? Many different security control mechanisms have been developed to fill the increasing need for security of computer systems. These mechanisms involve interactions between humans and computer hardware and software, but they were developed with little regard for Usability. So there is a immediate need for research in Human Factors and HCI to focus their efforts on usability issues associated with security- related tasks. The aim of this paper is to overview the various usability evaluation methods of HCI for the security of the system. The research perspective is one of security of HCI system.

2. SECURITY AND USABILITY

Security and Usability are quite opposite terms, because 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 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.

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.

With a growing recognition for the need to design systems that are both secure and usable, HCI Security is increasingly become active. Usability studies have been conducted on authentication systems, email encryption, security tools, and secure device pairing. These studies, however, follow standard HCI methodologies and procedures; methodologies and procedures designed for evaluating the usability of software systems in general, from which recommendations are made to improve ease-of-use.

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.

3. USABILITY EVALUATION

With the rapid growth of networked systems and applications such as ecommerce and internet, the demand for effective computer security is increasing. At the same time, the number of security problems reported over the past couple of years indicates that organizations are more vulnerable than ever. In many of the reported cases, user behavior enabled or responsible for the security breach. Security is aimed at making undesirable actions more difficult while usability aims at making desirable ones easier for the user, it may also be true that improving one also improves the other. A usable system will minimize unintentional errors, while a secure system will aim at ensuring that undesirable actions in a system are prevented or mitigated.

Various security methods have been developed, many of which rely on individuals to implement and use them. However, these methods may not accomplish their expected objectives if they are not used properly. In spite of the influence of usability, a very little research has been conducted on the compromise between usability and the degree of security provided by various security methods. Security Threat is the potency for the occurrence of harmful event like Theft and Fraud, Loss of Confidentiality, Loss of Privacy, Loss of Integrity, Loss of Availability.

Usability evaluation is one of the major cornerstones of user interface design. It helps- “to assess designs and test the systems to ensure that they actually behave as one should expect and meet the requirements of the user”. This is typically done by using an evaluation method to measure or predict how effective, efficient and/or satisfied people would be when using the interface to perform one or more tasks. As commonly practiced, these usability evaluation methods range from laboratory-based user observations, controlled user studies, and/or inspection techniques. This Study figure out the importance of the user interface in making a secure system usable.

Following attributes can be used to evaluate the usability of HCI for the purpose of security,

1. Effectiveness
2. Satisfaction
3. Efficiency
4. Errors
5. Memorability
6. Knowledge/Skill
7. Learnability

4. FUTURE SCOPE

To emphasize the usability of a HCI system through security, we use the simple usage scenarios and some common threat. In this context, usage scenarios as actions that are desirable to users of a secure system and threats as actions that are not desirable and hence the system should not allow them to happen. It is unrealistic to expect to achieve maximum usability and security in all secure systems. In most systems, there will be a trade-off between security and usability. The goal is to minimize as much as possible the possibility of threats and maximize the accessibility of usage scenarios. We used the usage scenarios and threats 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 threats are used to identify areas that may help non-malicious users to break the security of the system. This paper is just an overview of usability of HCI systems through security point of view. With the elaborative study, a much broader approach can be used for evaluating HCI using the additional available information. Future work will be to add detailed metrics that can be used to calculate the chances of users performing threats over a usage scenario. Further the analysis of the activity of malicious users can be done.

5. CONCLUSION

HCI methods and research approaches can make a significant impact in furthering our knowledge about information privacy and personal data protection. formal methods are used extensively in many fields of computer security, they are rarely used in HCI, even for security critical systems. The reason is that HCI does not deal with the interaction of two machines but with the interaction of a machine and a human.

Human–Computer Interaction (HCI) can greatly improve the protection of individual's personal information, because many of the threats and vulnerabilities associated with privacy originate from the interactions between the people using information systems, rather than the actual systems themselves.

6. REFERENCES

[1] D. Te'eni, J. Carey and P. Zhang, Human Computer Interaction: Developing Effective Organizational Information Systems, John Wiley & Sons, Hoboken (2007).

[2] B. Shneiderman and C. Plaisant, Designing the User Interface: Strategies for Effective Human-Computer Interaction (4th edition), Pearson/Addison-Wesley, Boston (2004).

[3] J. Nielsen, Usability Engineering, Morgan Kaufman, San Francisco (1994).

[4] D. Te'eni, "Designs that fit: an overview of fit conceptualization in HCI", in P. Zhang and D. Galletta (eds), Human-Computer Interaction and Management Information Systems: Foundations, M.E. Sharpe, Armonk (2006).

[5] A. Chapanis, Man Machine Engineering, Wadsworth, Belmont (1965).

[6] User Centered Design: New Perspective onHuman-Computer Interaction, Lawrence Erlbaum,Hillsdale (1986).

[7] R.W. Picard, Affective Computing, MIT Press, Cambridge (1997).

[8] J.S. Greenstein, "Pointing devices", in M.G. Helander, T.K. Landauer and P. Prabhu (eds), Handbook of Human-Computer Interaction, Elsevier Science, Amsterdam (1997).

[9] B.A. Myers, "A brief history of human-computer interaction technology", ACM interactions, 5(2), pp 44-54 (1998).

[10] B. Shneiderman, Designing the User Interface: Strategies for Effective Human-Computer Interaction (3rd edition), Addison Wesley Longman, Reading (1998).

[11] L.R. Rabiner, Fundamentals of Speech Recognition, Prentice Hall, Englewood Cliffs (1993).

* * *

[1]Ms. Shubhangi T. Raut Lecturer, Dept. of MCA, RAICIT, WARDHA-442001 shubhangi.raut003@gmail.com
[2]Dr. Abha S.Khandelwal Head, Department of Computer Science, Hislop College,
RTM Nagpur University, Nagpur, Maharashtra, India. abha.ak@gmail.com