Usability of Security Mechanism

J.Ofomata and N.L.Clarke

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

In spite of the available sophisticated security mechanisms to safeguard computer systems and work stations, the rate of computer crime and abuse is still on the increase simply because most computer users find it difficult to effectively implement the available security mechanisms. Consequently, users' inability to secure their system resulted to loss of funds, reputation and other sensitive data. However, this study aims at investigating the problems experienced by end-users which impede their effective implementation of security mechanism, for this purpose, a survey was designed and published online at the CISNR web site for a period of one and half month. The analytical review of the result generated by 231 respondents highlighted many usability weaknesses and based on these identified usability problems, some useful recommendations were suggested to nip these usability problems on board.

Keywords

Security, Usability, Security Mechanisms, Human–computer interaction and Computer interface.

1 Introduction

The purpose of this paper is to draw the attention of the general public on the need to develop usability methods and metrics for information security controls that will tackle usability issues. The need for information security necessitated a revolution in IT security industry that lead to the development of powerful security mechanisms that have the capability of combating various forms of computer crime, most unfortunately, users find it difficult to understand and implement these available security techniques to tackle the problem of attack and other lingering security issues that threatens the confidentiality, availability and integrity of information. Despite the level of publicity and awareness on usability of security mechanisms, the implementation of security applications is still poor, "Generally, security usability is poor" (Microsoft Security Ecology Report, 2008).

Most computer security packages are made up of security features that are presented for computer users to configure and install on their systems for the purpose of safeguarding computer users against intrusion and unauthorised access to their private network or database. Due to the problems posed by unclear functionality of some features in Human Computer Interaction, end-users are often confused at situation where they must take security related decisions.

However, the manner in which security interface features are designed and presented for users' implementation usually play a major role in influencing the users' action either by properly guiding them or complicating the process, such that users cannot actually use the security that they desire. This paper presents the results of a survey of 231 end-users in order to determine their weaknesses in implementing security to safeguard their systems. The study revealed some significant areas of usability difficulty and pointed out the need for a better designed computer interface and more considered approach to present security functionality in order to give computer users a realistic chance of safeguarding their systems.

2 Consequences of poor security implementation

The social and commercial benefits of online activities brought by the advancement of the internet leaves behind some costs associated with them since the internet has proven to have a big influence on criminal activity, as well as legitimate activity. For instance, about 830,000 businesses in the UK suffered an online/computer related security incident in 2007/08, (UK Cybercrime Report, 2008). The study carried out by Symantec indicated that out of 2249 new threats identified during the first 6 months in 2006, 86% were aimed at home users (Symantec, 2006). The personal and confidential nature of the financial data held in E-Banking service therefore inflicts fear into the mind of end-users because of the existing balance between security and usability of security features.

It was estimated that there were about 255,800 cases on online financial fraud in 2007 and with approximately 2.8 billion visitors annually, social networking websites offer a whole new dimension to potential online harassment, (Stefan Fanfinski, 2008). Despite the existence of sophisticated mechanisms like anti-spam software and email filters, the success rate of phishing crimes continues to escalate (Laurie Werner, 2008). A total of 2870 phishing sites were experienced in March 2005, and since then there has been 28% increment of the above figure on the monthly bases, meanwhile as result of phishing and online attack, USA consumers lost an estimated $500 million in 2005. It was also specified that the number of crime-ware-spreading sites infecting PCs with password-stealing codes reached an all time high of 31,173 in December 2008, (APWG, 2008).

3 Security Usability Study

A survey was published online at the CISNR web site of the University of Plymouth between mid July and September 2009 and a total number of 231 participants (126 male and 105 female) responded from over 40 countries across the world. Some of the countries include; Nigeria, USA. UK, Ghana, Germany, Saudi Arabia, Brazil, Pakistan India etc. The major challenge encountered during the course of this research work is problem getting the attention of the respondents who would actively participate in the survey. After the online publication of the survey it was noted that quite few number of respondents were recorded. This triggered the promotion of the survey link to the end-user community via email, telephone call, and postings to Internet forums that is likely to be visited by end-users. The link to the survey was also published on the International Students Advisory Service (ISAS) of the University of Plymouth.

At the surface level the responses overall suggested a high level of general IT experience and usage because above 50% of the respondents see themselves as intermittent users while 20% see themselves as experts. In terms of academic qualification, over 75% indicated to have either a Bachelor or Master's Degree. Almost all age brackets from under 20 and above 60 were represented but 80% of the respondents fall in between the age brackets of 20 and 39. A more in dept investigation into what the respondents claimed to know, proved that they lack most basic IT experience and usage. At the beginning of the security interface configuration section, users were asked if they know how to configure security interfaces, as seen in figure 1, 61% claimed to have a perfect understanding of interface configuration, 23% said they have some ideas while 16% owned up of not having any idea on interface configuration.

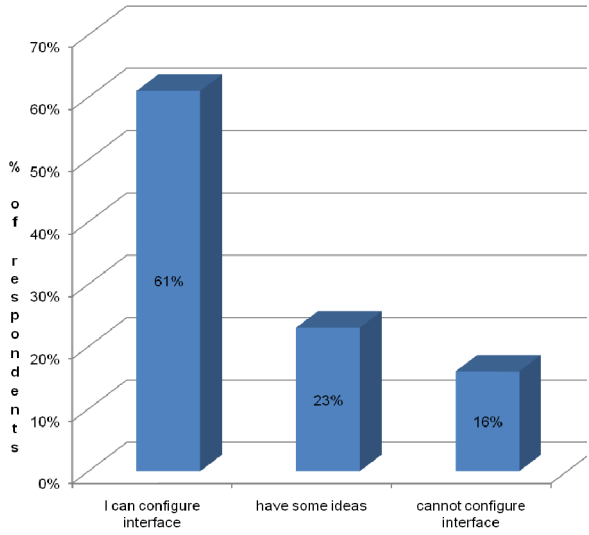

Figure 1: user's ability to configure interfaces

Subsequent test questions presented the images of firewall configuration interfaces to investigate their perception of the features. As seen in the figure 2, 48% of the respondents could not understand most of the features, while 11% did not understand them clearly.

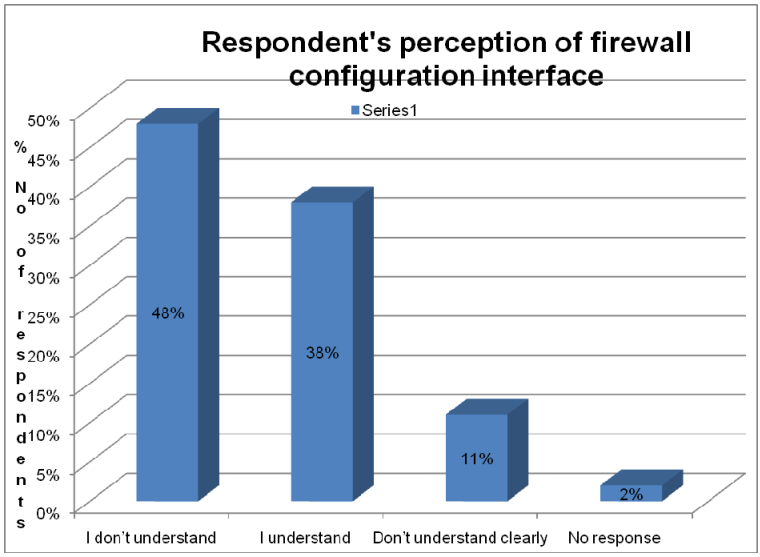

Figure 2: user's perception of interface configuration

However, interfaces are indispensable to human computer interaction because computer users can only be exposed to technology through the user interfaces. The average computer user's perceptions and understanding of certain technology is based on his experience with computer interfaces (Johnston et al., 2003). Therefore if security interface or related features within security software are poorly designed, even the most accomplished users will find it difficult to implement. The interface therefore needs to ensure that the user is guided so as to minimise the potential for the user to be vulnerable to attack. Human Computer Interaction is concerned with how the design of interfaces could be improved to make sure that they are understandable, usable and user friendly

Users were also probed on the frequency with which they update their security mechanisms; it was seen in figure 3 that 27 % carry out update on their security mechanisms at their convenient time, 25% do that on monthly basis while 23% update their mechanisms weekly.

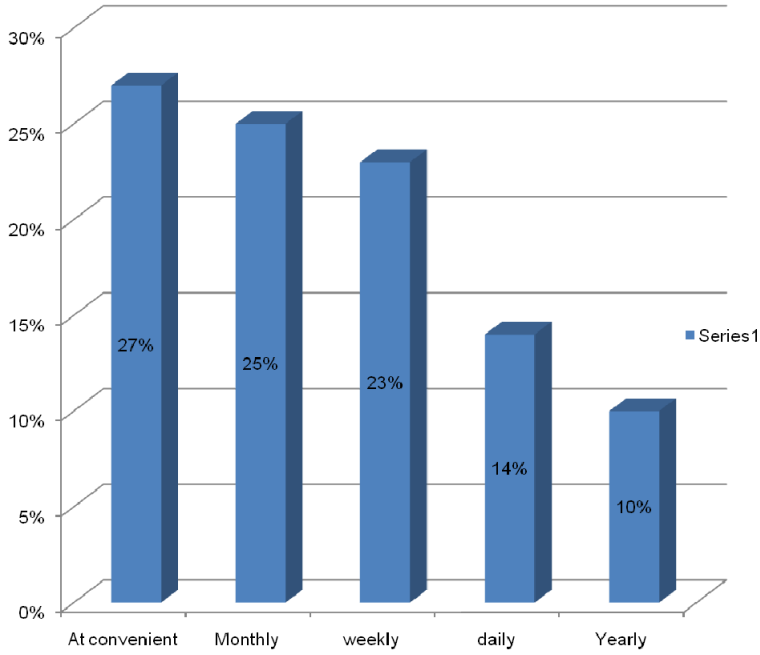

Figure 3: Respondent's frequency of security mechanism update

This really highlighted users' level of usability weakness because security systems need to be updated many times on the daily basis. However, updating security software very frequent will reduce the success rate of a skilled attacker. A skilled attacker has an 80% success rate of doing his exploit if a response is to be carried in 10 hours and 95% success rate if a response is to be issued in 20 hours. Then if an update is done in 30 hours the attacker has 100% of succeeding in his activities but when the response is instant, the attacker is left with almost 0% of succeeding in his malicious exploit (Cohen, 1999). This illustration describes the need for a real-time response and frequent update of security mechanisms in other to minimise the success rate of online attack.

Coming to good selection and usage of password and PIN in authentication processes as shown in figures 4 & 5 , 54% of the respondents use password of 6-8 character length while 18% choose their password to be between 4 and 5 character lengths, also 61% reuse the same password on multiple systems.

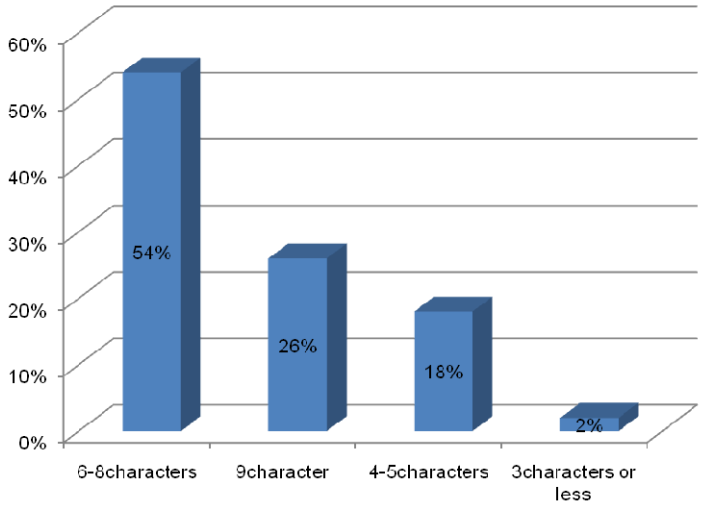

Figure 4: character length of respondents password

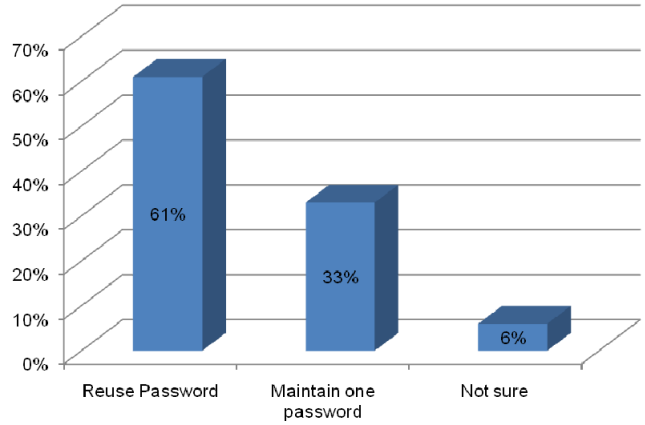

Figure 5: Ability to maintain one passwordon only one authentication process

It was seen from the survey result that end-users share their password with relatives and friends; also the character length of respondent's passwords in most cases are less than 9. However, for the purpose of maintaining good security in authentication processes, Passwords should not be written down let alone sharing with people, they should be strongly selected by ensuring that they are not too short, dictionary words and personal data that is mixed with numbers and special characters. This will foil the password cracker's ability of doing a simple look-up and apply brute-force technique or even apply password cracking tools. The more the password length, the more permutation the attacking tool is forced to try if the attacker must succeed.

Human Computer Interaction as a research discipline is no doubt a well developed area of study with experts who are of the opinion that usability of security mechanism could be significantly enhanced by employing certain interface design criteria in the design of these technologies.

Ben Shneiderman proposed some golden rules for interface design is as follows: the interface must be consistent, enable frequent users to use shortcuts, offer informative feedback, design dialogs to yield closure, offer simple error handling, Permit easy reversal of actions and reduce short term memory load.

However, in spite of the level of usability awareness and volume of academic studies that have been published on the existing relationship between end-users and Human Computer Interaction, user interfaces for security still tend to be clumsy, confusing and non-user friendly.

4 Findings

This study highlighted some of the problems that face end-users while attempting to understand and use related functionality in security software applications. This includes poor perception of security interface features, inability to understand and use security settings and users' lack of awareness of attack method used in social engineering. At the surface level, most respondents actively sort to cover their lack of knowledge, but with in dept exploration of usability issues by some of the designed test questions of the survey, certain usability weaknesses were revealed. Looking at the three major countries that have the highest number respondents, the level of usability and awareness of security were seen to be low in these three major countries, however, respondents from the USA displayed a higher level of usability and security awareness, followed by UK respondents and then Nigeria. On a more general note, the statistics of this result have been correlated with the results of some other related studies that investigated usability problems and there exists some strong similarities among these results. The common characteristic found is that security usability amongst end-users is still poor and as a result, suggestions have been made for security awareness and training sessions to educate computer users on the implementation and usage of specific security interface features. A major problem that hinders users from implementing security is that computer users find it difficult to understand the security features on the interface. The result of this study also pointed out that security interfaces are much relied upon technical terminology which makes interfaces unclear and confusing to users. Interfaces also lack visibility and force uninformed decisions to users, in respect to these, there is need for interface designers to improve on the design of the security interface for the purpose of improving the Human Computer Interaction to ensure effective usability of security mechanisms.

Another usability problem identified by this study is users' improper selection and implementation of password in authentication processes. The obtained result of the survey indicated that passwords are badly selected and implemented. From the result, greater number of the respondents selects their password to be pet names, dictionary words, or even personal data with character length of about 6. It was also seen that end-users share their password with relatives and friends. However, for the purpose of achieving strong security using password, they should be strongly selected by ensuring that they are not too short, dictionary words and personal data, but should be a non-dictionary word that is mixed with numbers and special characters. This will frustrate efforts of the skilled attacker because the more the password length, the more permutation the attacking tool will be forced to try on the password which will

frustrate the attacker's efforts. Also the investigation on users' awareness on phishing techniques illustrates that vast majority of respondents felt that they understood most phishing attack vectors. However, a notable percentage of the participants owed up to have problems in identifying and recognizing phishing sites. This particularly appears very surprising, because phishing threat had been the focus of media attention at the present days due to the escalating level of such attack coupled with the variety of related scams being perpetrated by skilled attackers.

5 Conclusion

This research study explored the existing relationship between computer users and their perception of usability and implementation of software security mechanisms.

The result highlighted some of the problems encounter by computer users while attempting to use security-related functionality within security related software applications.

From the general point of view, this study indicated that large proportion of respondents who claimed to be well knowledgeable regarding the implementation of security could not demonstrate effective security practices. Consequently, user's greater confidence in proper handling and implementation of security systems present a potential risk on its own since it hinders researchers from getting the clear overview of usability difficulties in order to properly device better means of tackling usability problems.

Although majority of the respondents claimed to be experts in the implementation of security systems, the results of this study demonstrated their shallow perception of security usability and lack of awareness of security threats. Considering the question that investigated if users have ever been trained on computer security, it was obvious that quite good numbers of users indicated of never been trained or educated on computer security. However, the major problem that must be addressed is that of awareness and education since users lack deep knowledge regarding their own protection. Also, the use of official and mass media efforts to educate the citizens for awareness creation is seen to be lacking. Consequent upon this, there is a need for more research studies that will look into a more viable model of engagement and awareness promotion amongst the entire populace for an optimised awareness creation on usability of security mechanism.

6 References

Anti-Phishing Working Group, APWG Phishing Archive, http://anti-phishing.org/phishing_archive.htm [Accessed 20 /05/ 09]

Anti-Phishing Working Group, *Phishing Activity Trends Report March 2005*, http://www.antiphishing.org/APWG_Phishing_Activity_Report_March_2005.pdf [Accessed 15 /05/ 09]

AOL/NCSA online safety study America Online and the National Cyber Security Alliance, December 2005.<http://www staysafeonline.info/pdf/safety_study_2005.pdf>;[Accessed 21 /05/ 09]

Audit Commission. 1990. Survey of Computer Fraud & Abuse, Audit Commission Publications, UK. [Accessed 07 /07/ 09]

Audit Commission. ICT fraud and abuse 2004: an update to yourbusiness@risk. Public section update, Audit Commission; June 2005 [Accessed 15 /02/ 09]

Batya Friedman, David Hurley, Daniel Howe, Edward Felten, Helen Nissenbaum, *Users' Conceptions of Web Security: A Comparative Study.* CHI 2002 Extended abstracts of the Conference on Human Factors in Computing Systems, 2002: p. 746-747[Accessed 12 /07/ 09]

Bidgoli, H. (Ed.), 2006. Handbook of Information Security Wiley, Hoboken, NJ. [Accessed 12 /07/ 09]

Bishop M. Psychological acceptability revisited. In: Cranor, Garfinkel, editors. Security and usability O'Reilly; 2005 p. 1–11 [chapter 1] [Accessed 22 /07/ 09]

Cohen F.B (1999) "Simulating Cyber Attacks, Defences, and Consequences", *The Infosec Technical Baseline studies,* http://all.net/journal/ntb/simulate/simulate.html Date accessed(20/7/09).

Eastin M. Diffusion of e-commerce: an analysis of the adoption of four e-commerce activities. Telematics and Informatics 2002; 19(3):251–67. [Accessed 22 /07/ 09]

Fafinski, S. (2008) *UK Cybercrime Report 2008* Available at: http://www.garlik.com/static_pdfs/cybercrime_report_2008.pdf. [Accessed: 6/07/09]

Federal Deposit Insurance Corporation: Division of Supervision and Consumer Protection Technology Supervision Branch: December 14, 2004[Accessed 12 /01/09]

Furnell. S 2007. "Making security usable: Are things improving?" *Computers & Security,* vol. 26, no. 6, pp 434-443. [Accessed 26/01/09]

Furnell, S. and Bolakis, S. 2004. "Helping us to help ourselves: assessing administrators' use of security analysis tools", *Network Security*, February 2004, pp7-12. [Accessed 11 /03/ 09]

Furnell, S, Bryant P and Phippen A. 2007. "Assessing the security perceptions of personal Internet users", *Computers & Security*, vol. 26, no. 5, pp410-417. [Accessed 14/05/09]

Galletta, D. and Lederer, A. (1989). Some Cautions on the Measurement of User Information Satisfaction. *Decision Sciences,* Vol. 20, Issue 3, pp.419-438.

Holzinger, A., 2005 "Usability engineering methods for software developers" *Communications of the ACM* , Vol. 48, Issue 1, pp 71-74

Johnston, J., Eloff, J.H.P. and Labuschagne, L.. 2003. "Security and human computer interfaces", *Computers & Security*, vol. 22, no. 8, pp 675-684. [Accessed 22 /04/ 09]

Lewis, C. and Wharton, C. *Cognitive Walkthroughs Handbook of Human-Computer Interaction, 2nd ed*. M. Helander, Ed. Elsevier, Amsterdam, 1997, 717–732. [Accessed 16/01/09]

National Identity Fraud (2007)" How ID fraud Occurs". [Online] available at: http://www.stop-idfraud.co.uk/How_IDF_Occurs.htm [accessed 16 /02/2009]

Schultz, E.E. et al. (2007) "Research on usability in information security" [Accessed 12 /07/ 09]

Whitten, A. and Tygar, J.D.. 1999. “Why Johnny can’t Encrypt: A usability Evaluation of PGP 5.0”, *Proceedings of the 8th USENIX Security Symposium,* Washington, D.C., USA, August 23–26, pp169-184[Accessed 18 /03/ 09]