Security Technologies: Why are they not used correctly?

M.Al-Tawqi and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

It is a fact that security technologies suffer usability difficulties, with prior studies revealing that end-users are not able to correctly use security technologies as a result of difficulties arising from complexity of design and mis-presentation of security features. In this aspect, this research presents the findings of an interview study conducted amongst over 75 end-users to explore the reasons behind such behavior, where known applications (Windows XP, Word, Internet Explore and e-mails & passwords) were used as examples. The findings revealed that participants were keen to show their wide awareness of security usefulness, with 87% of them using antivirus software, but with only 34% updating them either daily or weekly. It was also revealed that more than 57% of the participants disagreed that it is very easy to use software security features, while more than 60% disagreed that understanding the security features in software is easy. The roots of the problem were attributed to the complexity and unfriendly nature of the software, which require urgent moves from designers to simplify their security products.

Keywords

Security, Usability, Human computer Interaction, Windows XP, Word, Internet Explorer

1. Introduction

Information Security experts are now aware that in many cases breaches occur as a result of software not being used appropriately. Although suitable technology solutions are available to prevent computer users from such incidents, end-users are frequently unable to use them in the correct manner. This can take the form of end-user not knowing that those features exist, not caring enough to install them, or even willingly neglecting security, as in the case when people traded their passwords for candy bars (Saita, 2004). The other reason for such problems is related to the complexity of the software provided, which often scares away end-users instead of encouraging them to use such technologies.

2. Factors and contributors to the usability issue

One of the most common problems encountered within software security features is that it is *difficult to find and utilize security options,* as most of the times they are hidden instead of being placed in the forefront of the user interface. As a result, a user would only be able to access security features through routes such as the Tools – Option menu; which in many cases does not happen because of lack of knowledge that they exist (Furnell, 2005). Unfortunately, even when features are located, another immediate problem may be *the ability to understand and use the features.*

Indeed, the understandability problem was recognized and hence considered by the CRA (2003) as one of the four grand challenges in Information Security. The reason behind this can be attributed to either the lack of awareness amongst end-users, or the difficulty in finding meaning in the provided interface. The latter again relates to the unfriendly nature and complexity of the software itself, often as a result of designers and developers being more concerned with the software itself rather than taking the needs of regular end-users in consideration. The two problems were then extended by Furnell et al. (2006) to cover many other problems, as listed below:

- *Forcing Uninformed Decisions.* Difficulties in using security features can encourage poor security decisions (Zurko, 2005). The other problem faced by end-users is the detection of intrusion attempts accurately, whether before hands or afterwards (McHugh, 2001).
- *Lack of Integration.* If different elements of security do not work together, users might end-up getting a deceived message asking them to do something or install a software such as an anti-virus protection one when the user has already installed one. Good et al. (2005) agreed that this problem is in fact is doing more harm than helping at all.
- *Lack of Visible Status and Informative Feedback.* In addition to having difficulties finding the security options, users will also not have feedback from the system to inform them about the new state of security configurations.

Others have found that aspects of the Human Computer Interaction (HCI) were ignored by developers of security related products, who then tried to prove that use of security technologies can be improved if HCI techniques are employed. In this regard, Zurko and Simon (1996) came with solutions to help in providing user-centered security; these are:

- Applying HCI design and testing techniques to secure systems.
- Providing security mechanisms and models for human collaboration software.
- Designing security features directly desired by users for their immediate and obvious assurances (for example, signatures).

3. Investigative methodology

Much previous research has been conducted in a survey manner, where there was no interaction between participants and the questionnaire initiator; and with all of the factors mentioned above in mind, the investigation for this study was conducted in a form of a structured interview during the period 10th June- 15th July 2006. This method was considered to provide the benefits of having a questionnaire and a face-to-face interview at the same time, so that accurate observations are easily obtained and recorded from the mouth of the interviewees. The questionnaire was titled *Software Security Usability Survey*, while 71 participants' replies out of 76 replies were taken in consideration as there was evidence that the remaining 5 replies were either answered randomly or returned uncompleted. The questions of the research touched on the following areas: background, awareness, utilization and importance of certain security features, E-mails and their passwords, use of Windows XP and some of its applications. The analysis and interpretation of the questionnaire has been guided (in most cases) by Nielsen's usability heuristics to check on the usability of the operating system and applications discussed (Nielsen, 1994). In addition, previous studies of the same subject were used as means of guidance in terms of comparisons of findings.

3.1 Participants demographics and background

Two thirds of the participants were male, and the majority (64%) was between 18-34 years of age, which suggests that most were computer users from a generation who have grown up with such technology. Findings also indicated that majority of participants were degree holders (79%), with most of them holding a Bachelor degree as a minimum. Although 56% of participants viewed themselves as being intermediate users, it turned up not to be quite right after having heard their answers to some of simple questions during the interview. Those participants can be excused as they have no other choice but to select that option since they neither consider themselves as novice users nor advanced. It is worth noticing that such result is applicable to many other studies in regard to assessing computing experience. On the other hand, computers usage appeared to be widely spreading, with 80% using it continuously at work and home for various reasons. It is also worth mentioning that among those who use computers at work only, are IT-related employees who try to escape the work environment by trying to live a computer life free when they are at home.

3.2 Security Features Awareness, Utilization and Importance

When participants were asked about the knowledge of security features within MS Windows and some of its applications, as well as the use of antivirus software for their home computers, they were keen to show that they have a wide awareness of those features. It was noted that 87% used antivirus software, which is a promising result in a way. Although Word, Outlook Express and Internet Explorer have received the least percentage of awareness, this was justified since these results were utilized from the number of participants who only said they used them, which meant that more than 80% of those who claimed to be using the 3 applications were aware of there features. When compared to findings from other research, these results show an improvement in awareness amongst participants; with previous research having reported percentages of 68% for Internet Explorer, 56% for Word, and 32% only for Outlook Express (Furnell et al. 2005).

The results were less promising when participants were asked whether features shown in Figure 1 were actually utilized, as they revealed that majority have either never used the feature or used it seldom, even though they were concerned about security breaches. Reasons stated by participants for not using the security features have agreed to a great extent with some of other researchers findings, such as: *visibility*, *unfriendliness, difficulty* and *performance penalty* (Nielsen, 1994; Johnston et al. 2003). Participants also listed other barriers such as: their feeling that whatever type of protection implemented is *breakable any way; time consuming* to set up to desired functions; *insufficient knowledge & information;* and *carelessness &*

laziness. All of these factors make it difficult to convince end-users to take the initiative to secure their systems to the required level.

Participants' answers were in line with the findings of security feature awareness and utilization sections, which proved that participants have the sense for importance of security and that they are aware about the obstacles preventing them from fully utilizing security technologies. This shows that although people are aware of the implications of security breaches, they do not do much to prevent them from occurring, either because they do not bother, think that the problem will solve itself, or it will not occur to them for them being 'ordinary' users with 'ordinary' data. This was not necessarily correct when findings were compared to those of the IT-related employee findings, who proved to be better in applying necessary measures to protect their systems.

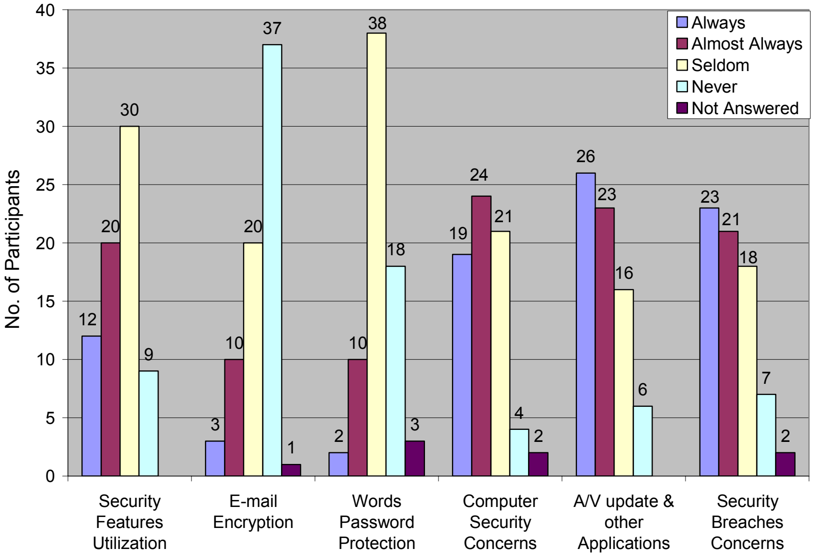


Figure 1: Utilisation of security

3.3 Windows XP, Anti-virus & Firewall

Despite the publicity of the inclusion of security features when Windows XP Service Pack 2 (SP2) was introduced, findings revealed that only 58% of participants heard of it, with less than 41% of total participants being able to list some (not all) of the features. This is another indication that end-users are not benefiting from an available facility that is been well advertised. Again, reasons can be attributed to carelessness and laziness from those who knew about it, or to the lack of knowledge for those who did not know about its existence.

When considering the aspects of protection that the Windows Security Center can control, the findings revealed that the majority of participants installed antivirus software, and were able to explain its role correctly (68%). However, this was not true for firewalls, as 59% of them did not know how firewalls are set to protect computers, while 63% did not know how exceptions are selected for allowing some programs not to be blocked by firewalls. Lack of knowledge about firewalls was further confirmed, as 58% did not know about the difference between an antivirus and a firewall. These findings confirm earlier research, which found that almost 45% of participants did not know about the difference between anti-virus and firewall protection (AOL & NCSA 2005). However, when such answers were compared to those of the IT-related employees, it revealed that the second group is well-informed and more educated about such differences, with more than 76% being able to give the right answer.

3.4 MS Word

This section checked on the knowledge of protection for Word files, and on the knowledge of what Macros are. Results revealed that majority of participants are aware that password protection for Word exists (85%), with 67% utilizing it while 83% gave the correct answer for the difference between modify and read only files (this case was true for IT-related employees participants, with 95%, 76% and 86% results respectively). This overwhelming knowledge and utilization of such facilities is understood and expected for Word being popular with almost every single user of computers. As for the knowledge of Macros, results revealed that 62% of participants are aware that such facility exists, with 85% of these aware participants utilizing it, while only 48% saying that they know how to set security level for Macros. This case was almost true for IT-related employees, with 71%, 83% and 67% (slight difference) results respectively, which can be related to the familiarity of Word with most computer users.

3.5 E-mail

Answers of participants revealed that only 39% knew about SSL certificates, with only 64% of these participants knowing about the way of obtaining them. This demonstrates that if a feature's existence is not known, then there is no way it will be widely recognized and hence used. Findings also revealed that: 82% did not agree that *internet email is very secure* with more than 80% agreeing that *sent e-mails can be read, intercepted or modified by others* which indicated that participants are aware that they might be spied upon by others, as there is no security once they are online, and that (unless specifically protected) every single message sent by them can be intercepted by others. However, findings revealed that this knowledge of such problem did not prevent them from being victims of message interception, as 87% admitted that they have no means of knowing if messages received or sent by them were modified. Unfortunately, this is not the only area where end-users become victims to security breaches, but in fact it is them who make it easier for others to hack on them as a result of their reactions to security matters, when findings indicated that 67% of them will open an e-mail from a stranger with 57% saying that they will even open attachments before saving them first.

3.6 Passwords and other authentication methods

Participants were asked about their awareness of password, token, and biometric methods. The first significant finding was that the majority (69%) did not know about all three categories; which explains why only 25% have considered using the other 2 methods instead of using a password only. Thus, it is understood why most end-users (85%) use passwords the most. However, although password authentication was still preferred over other methods, the percentage here was less than the current level of usage, with a noticeable portion of participants claiming that they would prefer other methods (61% *passwords*, 24% *combination* and 5% for *biometrics* and *tokens*). The preference to use passwords is understood, when it is known that most users have not encountered the other two methods, which means that they are forced to choose passwords as the only method they are familiar with. On the other hand, biometric authentication was preferred because fingerprints – for example - are unique and therefore cannot be imitated. However, this same justification was the reason why others refrained from preferring such method (as they would rather have their token or password stolen than their thumb), while others felt it would not be cost effective. Figure 2 gives a clear explanation of participants' awareness of password importance, where variation in wrong doing revealed the following:

- *Participants are having difficulties keeping up with more than one password*, which makes it difficult for them to remember them all or come up with new ones, and hence being forced to either use a changed password more than once or/and use it for more than one system.
- *Participants are less willing to share passwords with friends or write them down,* though they sometimes do that but to a lower extent. This highlights that participants are aware of risks of losing passwords, but they will only compromise when there is no other way of getting around it.

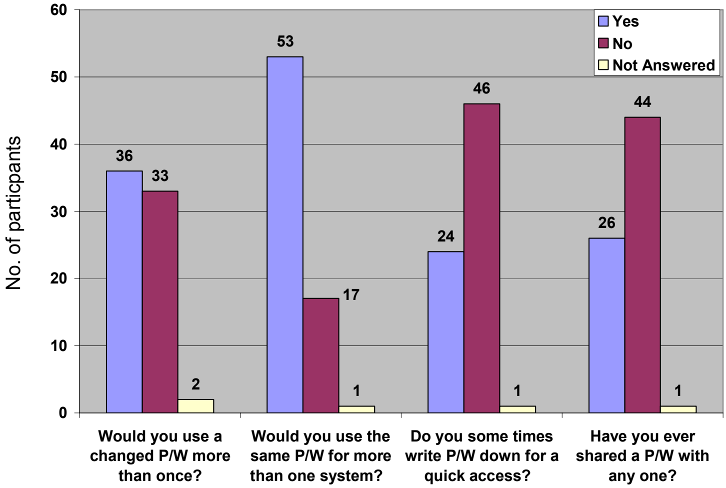


Figure 2: Participants' responses about awareness of password importance

Opinions provided by participants for guidelines or steps that should be taken or imposed for better selection of passwords were as follows:

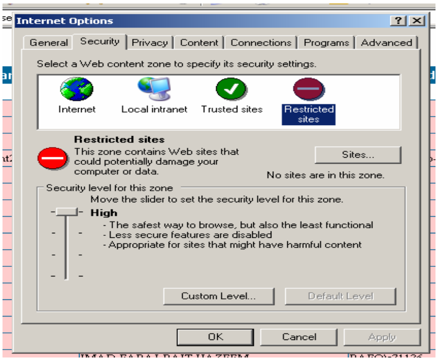
- *Never use personal data.*
- *Use different combinations of characters, numbers and symbols.*

- *Change passwords every 45 days and never use old passwords again.*
- *Promote better security awareness and education.*

3.7 Internet Explorer

Users were asked about their knowledge of using trusted and restricted sites, and restriction of cookies. The results revealed that 61%, 62% and 55% of participants are aware of the their existence (81%, 81% and 76% of IT-related employees). However, this variation in percentages of the two compared groups did not prove that the second group is fully utilizing such available facilities, as results revealed that it barely reached 29% for the first group and 38% for the second group as the highest result reached for the utilization of any single feature.

Participants were also asked to consider the manner in which security features are presented and explained. When they were asked about Figures 3 and 4, their most common comments were that: *there should be an explanation of the actions taken with examples, description is a bit vague and may scare novice users away*, *such screens should be automatic, there should be better explanation for beginners*, and *the figure should properly explain the feature, not the words.*



Select a Web content zone to specify its security settings.

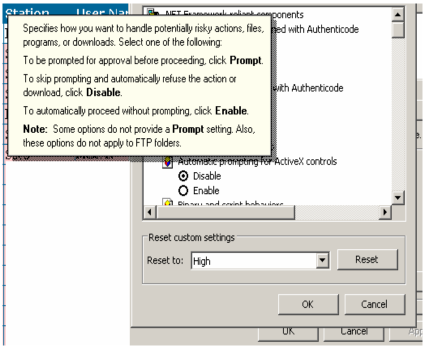
Restricted sites
This zone contains Web sites that could potentially damage your computer or data.

No sites are in this zone.

Security level for this zone
Move the slider to set the security level for this zone.

High
- The safest way to browse, but also the least functional
- Less secure features are disabled
- Appropriate for sites that might have harmful content

Figure 3: Explanation of what restricted sites are



Specifies how you want to handle potentially risky actions, files, programs, or downloads. Select one of the following:

To be prompted for approval before proceeding, click **Prompt**.

To skip prompting and automatically refuse the action or download, click **Disable**.

To automatically proceed without prompting, click **Enable**.

Note: Some options do not provide a **Prompt** setting. Also, these options do not apply to FTP folders.

Figure 4: Explanation provided when clicking to enquire about settings

3.6 General

Evidence showed that end-users believe that security issues should be the concern of all of those dealing with or effected by them, as more than two thirds (68%) of participants said that security issues should be handled by both end-users and designers.

Other relevant findings were that:

- 80% agreed that security alerts provide a good indication of current status;
- 73% asked for a centralized security option for all MS-related software;
- 82% agreed to introducing different warning levels for moving from one site to another;

- 86% agreed that security tips and hints should be provided at the start of sessions.

Findings have also agreed and confirmed to those established by previous studies on the same field for e-mails being the main cause for infections with 64%, where other studies have revealed higher percentage (80%) for e-mails being the main source of virus infection, (Panda Software, 2006).

4 Conclusion

Unfortunately, some end-users do not take the initiative of updating themselves in regard to information security issues; mistakenly assuming that it is solely the duty of their organization to take care of training and educating them on how to fight security threats. In fact, it is end-users' responsibility to make sure that they keep up with the pace of information security development, as it is them who will eventually be directly effected by any breaches. On the other hand, designers must understand that they are developing such software so that they are useable, and that not every user has their level of knowledge, which means that they have to picture regular end-users and put themselves in their shoes so they can come up with tools that are widely accepted by majority of computer users. Therefore, the research highlights the need for action by designers and employers in order to assist end-users, where employers must foster knowledge and understanding of security features to their employees in order for those features to be appropriately utilized. On the other hand, designers must provide features which are visible and friendly with very clear explanation.

5 References

AOL and NCSA, 2005. *AOL/NCSA Online Safety Study*, http://www.staysafeonline.info/pdf/safety_study_v04.pdf#search=%22AOL%2FNCSA%20Online%20Safety%20Study%20%22 (06 August 2006)

CRA Web Site, 2005. Challenges in Information Security & Assurance, http://www.cra.org/Activities/grand.challenges/security/home.html (17 August 2006)

Furnell, S.M. 2005. "Why users cannot use security", *Computer & Security*, vol.24, pp274-279.

Furnell, S.M., Jusoh, A. and Katsabas, D. 2005. "The challenges of understanding and using security: A survey of end-users", *Computers & Security*, vol. 25, no.1. pp27-35.

Furnell, S.M., Jusoh, A., Katsabas, D. and.Dowland, P.S. 2006. "Considering the Usability of End-User Security Software", *Proceedings of 21st IFIP International Information Security Conference (IFIP SEC 2006)*, Karlstad, Sweden, 22-24 May 2006, pp307-316.

Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D. and Konstan, J. 2005. "Stopping Spyware at the Gate: a User Study of Privacy, Notice and Spyware", *Proceedings of the 2005 Symposium On Usable Privacy and Security*, Pittsburgh, Pennsylvania, pp 43 – 52.

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

McHugh, J. 2001. "*Intrusion and Intrusion Detection*", Integrated Justice Information Sharing IJIS, 2001, vol.. 1, pp 14 – 35.

Nielsen, J. 1994. "Ten Usability Heuristics", http://www.useit.com/papers/ heuristic/heuristic_list.html. (25 January 2006)

Panda Software, 2006, Virus Entry Points, http://www.pandasoftware.com/virus_info/about_virus/information1.htm (18 September 2006)

Saita, A. 2004. "Password protection no match for Easter egg lovers", http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci960468,00.html (17 August 2006)

Zurko, M. E. 2005. "*User-Centered Security: Stepping Up to the Grand Challenge*", 21st Annual Computer Security Applications Conference (ACSAC'05) pp. 187-202

Zurko, M.E and Simon, R.T. 1996. "User-Centered Security", *Proceedings of the 1996 Workshop on New Security Paradigms,* Lake Arrowhead, California, United States, pp. 27 – 33.