Improving the Usability of Security Features – a Survey of End Users

M.O.Adjei and S.M.Furnell

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

Abstract

Computer users today face a myriad of threats most of which are as a result of the Internet. The numbers of applications available to help combat these threats also exist in an equal measure. This means that end users are likely to encounter security events on a daily basis. This reiterates the need for usable and effective security applications to counter these threats. This paper presents the results from a survey conducted to sample the views and record the experiences of 46 end users over a 21 day period. Security related events were categorised into user initiated and system initiated events. Under these two categories, a total of 294 events were recorded. It was also found that out of the total of all user initiated events, 27% of them were not fully understood by the participants with 16% of the events were unable to be completed meaning that this number although willing to set protection on their systems, were unable to do so. Indeed this shows a serious problem in usability and has the possibility of presenting vulnerable systems that can be easily compromised.

Keywords

Usability, Security, User-Initiated Events, System Initiated Events

1 Introduction

Since the ability to greatly reduce the size of computers while still maximising its power and storage, end user computing has seen a corresponding increase throughout this time. The Internet has become an important part of end user computing with most users having one form of computer identity or the other from e-mail accounts, social websites and online shopping accounts. This has also resulted in new and sophisticated approaches to Internet crime commonly referred to as cyber crime. Users face such threats as identity theft, deliberate service disruption and electronic theft of valuable information. Undoubtedly, both corporate and end user systems are being used to hold more sensitive and valuable information now than ever before partly because these systems now have the ability to do so. The theft and subsequent profits at stake for this information has also become very high. There is therefore the need for these systems that hold and transport the information to be adequately secured. (Polstra III, 2004).

2 Usability

The interaction of end users with security is an important aspect of Human Computer Interaction (HCI) with what is now known as Human Computer Interaction-Security, (Johnston et al, 2003) indicating that security should inevitably lead to trust of the system by the user. Indeed it can also be argued that users need to see security working but also more importantly need to understand what it is the security is actually doing in order to establish that required level of trust for the system (Furnell et al, 2006). Although a previous study has infamously acclaimed end users as the weakest link in security (Gross and Rosson, 2007), another on the contrary showed that some end users do indeed differentiate between security and general issues concerning their systems (Gross and Rosson, 2007). It is important to note that some users may be genuinely concerned about security but may be constrained by usability challenges. The problem of security should therefore not be blamed on end users alone. The tools and applications for the protection of their systems needs to also be put under equal scrutiny. They must be usable to ensure effective protection overall.

2.1 Usability and Security

System threats have evolved considerably and today's varied malware run silently but deep in the background. They steal information or use such compromised systems as a storage or in other cases as transit for the stolen information. These malicious codes in most cases operate without affecting the resource use of the compromised systems or disrupting their normal workings in a noticeable way. As (Thompson, 2005) put it, "*Theft through spyware could be the most important and least understood espionage tactic in use today."* This is can in fact be confirmed by the sheer number of security tools and applications available to combat current threats. For instance (Kaspersky Labs, 2008) indicate that their antivirus databases currently contain over 724,538 records with around 3,500 new records are added weekly. The threats themselves have also evolved in much the same way in terms of technology as is used to try to fight them. Since malware are in fact just computer programs, most are analysed by reverse engineering the original software code, analysing the behaviour then writing counter-code to annul its destructive effects. To effectively conceal their true behaviour from de-compilation and reverse engineering, some malware code now employ obfuscation by specifically using transform algorithms to alter code into a meaning in the programming language used which will be much harder to comprehend if actually de-compiled, and thereby making it extremely difficult to neutralise (Anckaert et al, 2007). This shows that even the efforts to curb end user threats do not come at a light expense. Among other things various encryption algorithms that activate at each infection (Zhang et al, 2007) used by other malware developers making the behaviour analysis even more difficult. All this shows the gravity of threats that computer users are faced with today. However the average end user cannot be expected to be on top of the finer details of these threats as described, but there is the need for them to at least be made aware of their existence and more importantly be presented with usable security to offer adequate protection for their systems and information contained therein.

3 Research Methodology

The research was primarily aimed at trying to establish how to improve the usability of the security features that are contained in end user applications. Similar work had been done prior to this research by other authors, some employing end user population survey using paper and online questionnaires and others reviewing the usability of specific applications (Chatziapostolou and Furnell, 2007; Gross and Rosson, 2007). For this research it was considered to gather information on end user experiences with security related events as much as possible when the events are actually occur. The target platform was to be Microsoft Windows primarily because it has the widest distribution. This it was believed would give an insight into how in reality end users deal with these events. To effectively accomplish this, it meant that the questionnaire that was to be used had to be available to collect and store user responses whenever an event of relevance occurred irrespective of the system's network status.

3.1 The Electronic Questionnaire (e-Quest)

Given the current work done and the fore going, it was decided that a custom computerised self-administered questionnaire (CSAQ) would be the best option. This approach would ensure the availability of the questionnaire on-demand and to store responses locally even with the absence of a network connection. A custom utility called, *e-Quest* was therefore developed for the purpose using Visual C# 2005.

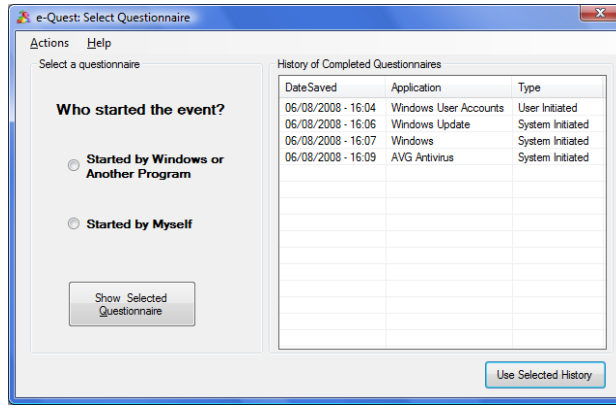

Figure 1: e-Quest Questionnaire Selection Window

The utility was distributed participants who took part in the survey which was for a period of 21 days. The respondent selection criteria were mainly on their ability to make regular use of a system that has at least an Internet connection to send questionnaire data. Participants were duly briefed prior to the survey and it was ensured that they fully understood the whole process. *e-Quest* also contained the relevant help files and examples for any further help should the participants need them. Responses were saved locally in the working folder of e-*Quest* in open Extensible Mark-up Language (XML) format to ensure storage compatibility which were later compressed into a single file to be attached and sent via email.

4 Survey Results

The CSAQ approach and *e-Quest* utility presented a useful tool in sampling the experiences of the 46 participants who took part in the survey for the 21 day period As will be delved into in a little more detail in the discussion section of this paper, some participants recorded very interesting encounters with security with some resulting in unsatisfactory consequences. Out of the total number of participants, 67% were male and 13% female. 76% were between the ages of 18-30 years with only 2% being over 50. All the participants made regular use of their computer systems with 89% using them every day and 87% having been using a computer for 5years or more. The remainder used their systems at least 2-3 days in the week and having also been using their system for 3-4 years respectively. Half of the participants considered their computer literacy to be of intermediate level with 48% considering themselves as advanced users.

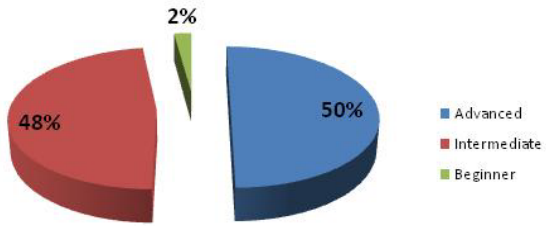

Figure 2: Computer Literacy Distribution of Respondents

For the Respondent-Event distribution, a total of 294 security related events were recorded. In all 57 different applications were recorded by the participants as in the events encountered. The highest number of events recorded by one participant throughout the whole survey was 34 events. Two participants recorded 1 event each being the lowest events recorded. Figure 3 shows the distribution of the number of participants versus the events that were recorded.

With respect to the activities that participants used their systems for, 80% had social networking accounts while 70% shopped online. More than half of the 46 participants representing 63% used online banking services as well and in terms of the most threat prone activities, half of the participants use peer to peer file sharing software. All the earlier mentioned activities require end users to have some security knowledge information as authentication and verification procedures and 39% of the participants stated that they in fact do store some if not all this information on their systems as well. These results clearly show the areas of high risk in end user computing and the more important need for the security to meet up to the challenge not only in performance but also in the ability to effectively use the power these tools and applications are said to provide. Table 3 below shows the list of activities and the corresponding user population that uses them as recorded by the participants during the survey.

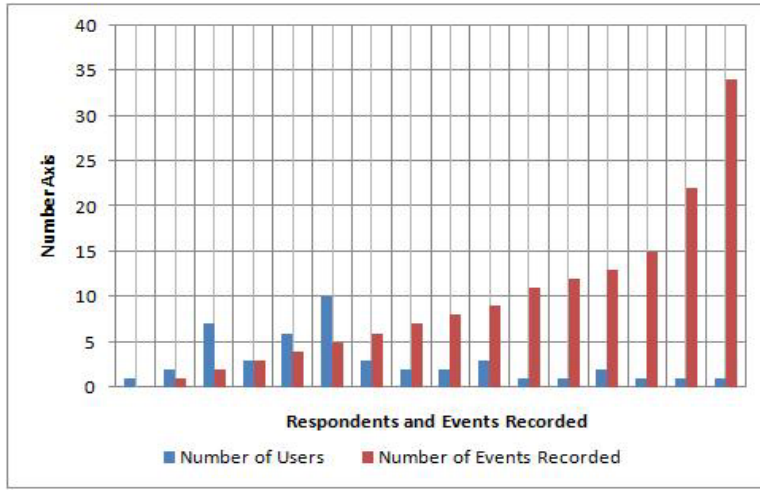

Figure 3: Number of Users versus Events Recorded

Do you use your computer for any of the following?		
Computer Activity	**Number of Participants**	**Percentage(%)**
Online Gaming	4	***9***
Peer – to – Peer file sharing	23	***50***
Internet Banking	29	***63***
Online Shopping	32	***70***
Storing of personal information	18	***39***
Social Networking	37	***80***

Table 1: List of computer activity versus participant numbers distribution

In terms of the security available on their systems, all the participants had some antivirus protection with 89% indicating they had a firewall installed. 58% of the participants also had some Internet solution application. However, only 48% of all participants had ever changed the settings of these applications from the default.

4.1 User-Initiated Events

A total of 70 events from 26 different applications were initiated by respondents in an attempt to deal with security. For these, 63 had respondents satisfactorily complete the user-initiated events questionnaire. Norton Internet Security was found attributed the most number of events initiated by a subset of 3 respondents. The research results showed that for the total number of events that users started themselves, 27% were not fully understood. Table 2 shows the number of events and the degree to which they were understood as presented on the user-initiated events questionnaire. Another 16% events prevented users from completing events that they initiated.

To what extent did you understand this whole event?	Total Number of Events	Percentage (%)
Fully	46	**73**
Partially	15	**24**
Not at all	2	**3**

Table 2: Participants understanding of user-initiated events

4.2 System-Initiated Events

A total of 222 system-initiated events from 31 named applications were recorded. Similar to the user-initiated events, Norton Internet Security recorded the highest number of events totalling thirty seven, 37 from 13 respondents. Respondents completed the system-initiated event questionnaire 217 times with 5 activations of the questionnaire for which it was not completed. From the respondent's understanding of events, similar to the user-initiated events responses, 26% of events were not satisfactorily clear to participants out of which 10% prevent them from completing activities they were performing or about to perform prior to the occurrence of the event. Table 3 below displays these results in detail.

Were you clear on what was going to happen next with this event?	Total Number of Events	Percentage (%)
Very Clear	100	**46**
Quite Clear	60	**28**
Clear	28	**13**
Not Quite Clear	23	**10**
Not Clear	6	**3**

Table 3: Participants understanding of system-initiated events

5 Discussion

A lack of understanding of security technologies may lead to inadequate protection from the threats that exist, (Furnell, 2005) and this was evident in this research. If users are not very sure of what to do or what will happen next with a security related occurrence but are placed in a position, as in most cases where they need to respond, they might make a wrong decision. In a situation where this user's system is among others in a closed network scenario, such as exists in company local area networks, this can lead to a serious breach affecting part or the whole firm (Gross and Rosson, 2007). Figure 4 below shows part on one user's response to an event during a browsing session where a modal pop-up dialog requested them to install a free security application, *Antivirus 2009* to help protect their system.

Figure 4: System-Initiated Prompt To Install Antivirus 2009

From this user's response, they did not understand why the event occurred yet and the event stopped them from performing whatever that they were doing before its occurrence. The XML tags *<Understand>* and *<StopFromPg>* indicate this respectively. XML as stated in the methodology was the storage format for user responses.

A background check on the said security tool revealed that it was in fact rogue spyware product and a variant of earlier versions *Antivirus 2008*, *Antivirus 2008 XP and Antivirus2009*. This confirms the earlier analysis in this paper of the sophistication and repackaging of variants of malicious code to evade detection (Anckaert et al, 2007; Zhang et al). Figure 5 below shows a security assessment of the spyware by Computer Associates website.

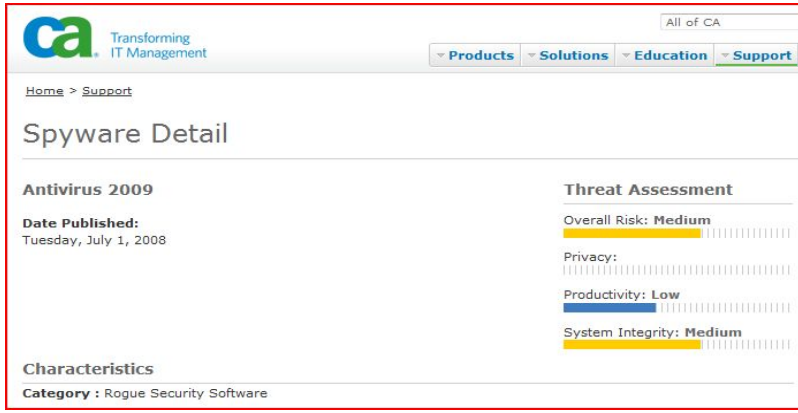

Figure 5: Threat Assessment of Antivirus 2009 - CA Website (2008)

The particular user did in fact go ahead to install the tool in the utmost sincerity of adding to their security protection. Another problem is that although the user did not understand the particular event, they did not seek any help or guidance for it. It proves right the claim that most users do not like to read instructions unless it actually pertains to something they already want to do (Furnell, 2005). This scenario clearly shows that even though majority of events were in reality understood by users, the relative few which were not can still pose a major security risk. The user's

systems and those of others might be put in danger of compromise with neither of them realising the full consequences.

6 Conclusion

As presented in this paper, the need for usable security cannot be treated lightly as the consequences may be too high. The use of the CSAQ enabled this research to realise firsthand how such scenarios in effect can occur. With all the advancement in usability study, there are still current problems facing end users. While conceding that the ideal of every user being protected to the required level may not be a realistic enough premise for evaluating usable security, the contrary cannot also be accepted either. Even the least percentage of users who might not use properly, use at all or understand security, the overhead cost can still be very high as shown in the results.

This research was limited to the Windows platform. Future work may be useful to combine multiple survey methods on various platforms. A survey of a larger user population over a longer period of time may also be desirable. These will be useful to unearth whether or not usable security is in effect getting better and any new challenges that users may face.

7 References

Anckaert, B., Matias Madou, B., DS., De Bus., B., De Bosschere, K. and Preneel, B., (2007), Program obfuscation: a quantitative approach, *QoP '07: Proceedings of the 2007 ACM workshop on Quality of protection*, ACM (Online Resource)

Antivirus Database Updates (2008). Kaspersky Labs http://www.kaspersky.com/ avupdates, [Date Accessed 23RD April,2008]

Chatziapostolou, D. and Furnell, S., M., (2007). Assessing the usability of system-initiated and user-initiated security events, *Proceedings of ISOneWorld 2007, Las Vegas*,

Computer Associates (2008) Antivirus 2009 Threat Assessment http://ca.com/ securityadvisor/pest/pest.aspx?id=453137270 [Date Accessed, 28TH August, 2008]

Furnell, S., (2005) Why users cannot use security. Computers & Security, 24, 274e279, Elsevier Ltd. (Online Resource)

Furnell, S. M., Jusoh, A. and Katsabas, D.,(2006) The challenges of understanding and using security: A survey of end-users. *Science Direct, Computers & Security, vol. 25, no.1, pp27-35*

Gross, J., B. and Rosson, M., B., (2007) End User Concern about Security and Privacy Threats.

SOUPS '07: *Proceedings of the 3rd symposium on Usable privacy and security*, ACM (Online Resource)

Gross, J., B. and Rosson, M., B., (2007) Looking for Trouble: Understanding End-User Security Management CHIMIT '07: Proceedings of the 2007 symposium on Computer human interaction for the management of information technology, ACM (Online Resource)

Johnston, J., Eloff, J. H. P. and Labuschagne, L. (2003) Security and human computer interfaces, *Science Direct, Computer and Security*, *Volume 22, No.8*

Polstra III and Robert M., (2005), A case study on how to manage the theft of information, *InfoSecCD '05: Proceedings of the 2nd annual conference on Information security curriculum development*, ACM (Online Resource)

Thompson, R., (2005), Why spyware poses multiple threats to security, *Communications of the ACM, Volume 48 Issue 8*, ACM (Online Resource)

Zhang, Q., Reeves, S.R., Ning, P.S. and Iyer, S.P., (2007). Analyzing Network Traffic To Detect Self-Decrypting Exploit Code, *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security,* ACM (Online Resource)