Recording end-users security events: A step towards increasing usability

D.Chatziapostolou and S.M.Furnell

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

Abstract

End-user security is nowadays an integral part of our everyday life since modern computer applications frequently dedicate parts of their functionalities to security. As a consequence computer end-users potentially come across with security related events, which may be either system- or user-initiated. However, computer security is often viewed as a difficult and complicated task, which eventually prevents end-users from achieving the protection that they desire and anticipate. This paper presents the results of an initial study from 26 participants, the purpose of which was to investigate the usability of security events that were encountered over a two week period. The results reveal difficulties in dealing with the security events, with more intense problems encountered when end-users attempt to make use of security intentionally.

Keywords

Security, Usability, Security event, End-users

1. Introduction

Nowadays, it is a common observation that end-users are much closer to security than in the past. With the increasing volume of IT threats, end-users more often come into contact with security-related events. Indeed, security functionality is now frequently integrated within software such as operating systems, and tools and applications. For instance, in Windows XP, the integration of security has significantly improved since the introduction of Service Pack 2 in 2004 (Microsoft Corporation, 2006b). However, as a consequence, end-users potentially come across security terminologies such as pop-up blockers, software update messages, and security alerting messages for possibly unsafe attachments. Additionally, use of security-oriented software, such as firewalls, antivirus and antispyware products has significantly increased as the associated threats become more widespread and recognised. Moreover, general applications now often incorporate security functionalities. For example, applications within the Microsoft Office suite employ encryption functionality in order to protect misuse of data (Microsoft Corporation, 2006a).

Unfortunately, the reality of this situation is serious. Users can be deterred if they are not able to understand the security presented to them. In fact, this is often the case as security is frequently not optimally designed for end-users. Software designers often give less attention to usability when designing security within products. Usability of security applications has critical importance because an unusable product might

prevent end-users from enabling security features in their systems. This means that end-users, either at work or home, might left unprotected. Therefore, usability considerations include ensuring that end-users are able to find the security available for them and determine the protection they require at any time.

This paper presents an investigation into the usability of security and the challenges that end-users face in using the related software features. The first part of the investigation examines prior works on usability and security, with references and examples. The rest of the paper presents the results from a related study, the aim of which was to examine end-users' understanding of security events encountered while making ordinary use their computers.

2. Examples of unusable security

Examples of security usability problems have been witnessed numerous times by security researchers. In the area of security-oriented tools, a prominent example is Whitten and Tygar's (1999) evaluation the usability of PGP version 5.0. Their work is one of the first standard examinations of usability of security applications. Specifically, they had carried out a cognitive walk-through analysis along a heuristic evaluation, which completed with a user testing. Their findings showed that PGP 5.0 user interface had severe problems which made public key cryptography a difficult task for an average user to accomplish.

Unfortunately, this is not the end of the list. General applications are also found to lack usable security. Internet Explorer (IE), the standard Web browser of Microsoft Windows, has been used to illustrate improper implementation of usability and security. Furnell (2005) indicated that "Users may struggle to make appropriate use of IE's security features". Although IE is a general application rather than a security-specific tool, it includes security functionalities within the options. According to Furnell, the related security options of IE violate key principles of Human Computer Interaction (HCI). These key principles apply for friendly visual state and informative feedback to the end-users. In reality IE seems to have been designed with security features to be primarily meaningful for advanced users, who have prior security knowledge. This lack of usability could possibly reduce end-users protection rather than encourage its use.

3. The study

With the above points in mind, a study has been conducted in order to investigate end-users' encounters with actual security events. The aim was to record the participants' experiences over a two week period. A recording sheet was created and distributed to participants for use during this time. In addition to one-off collection of background details about the participants, the sheets sought to record two specific categories of ongoing information, relating to system- and user-initiated events. These two broad categories encompass the types of security event that end-users might experience, as described in the sections that follow.

3.1 System-initiated events

These types of events occur with intention to inform the end-user about security. Thus, that type of events initiates from the computer system and targets the end-user. This could be done in different ways, such as security messages and warning screens, pop ups etc. depending on the computer system, operating system, and the applications installed. We define system-initiated events as: *'Events initiated by a computer system with the intention to advise and inform end-users' operations'*.

For example, many users may be familiar with seeing pop-up dialogs in their web browser asking them whether or not they wish to allow an event, such as that in Figure 1. In such cases the participants make an entry on the recording sheet providing details of the application that initiated the security event. Additionally there is a series of key questions which contribute the investigation of usability. In brief, the included questions concerned whether participants understood the event, if they had to take a decision, if there was a help feature and whether it was used, and if that event prevented participants from completing the task they were trying to perform. From the participants' comments the usability level of an application could be assessed.

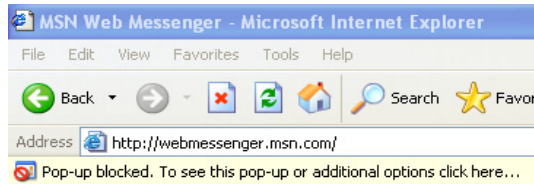

Figure 1: A system-initiated event in the form of pop up message

3.2 User-initiated events

User-initiated events differ from system-initiated events as at this time an end-user initiates an event with intention to deal with security. Specifically, this applies when end-user intends to take control of a computer system by configuring security-related features within applications and tools. We define user-initiated events as: *'Events initiated by an end-user of a computer system who intentionally wishes to utilize security toward distinct goals'*.

As the definition states, these types of events are requests from an end-user who has settled a goal relating to security and wants to accomplish it. An example of a user-initiated event is shown in Figure 2. In this example the application used is Internet Explorer (IE), in which security functions are available under the options tab. As Figure 2 shows, an end-user might intentionally attempt to configure security options, such as whether ActiveX controls, plug-ins, scripts and other security-related operations should be enabled or not. Imagining this was a real case, a participant experiencing this user-initiated event could make an entry in the recording sheet providing information of the application used, the actual intention and whether or not they were able to accomplish the task.

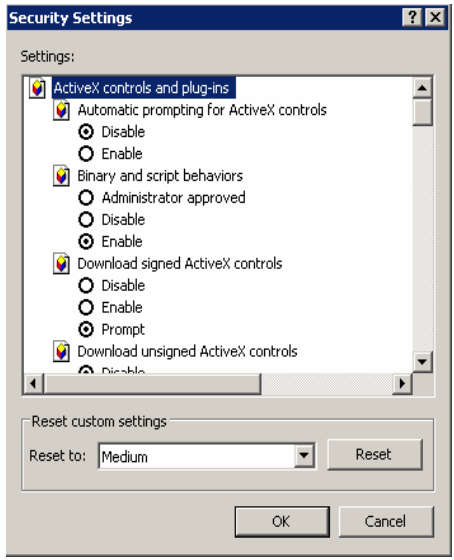

Figure 2: A user-initiated event in Internet Explorer

4. Study results

The total number of participants was 26 people with an equal split between genders. Most of the participants (68%) were in 21-29 group of age, with the rest evenly split between participants under 20, and those aged 30-39 and 40-49. The focus in the age category of 21-29 expected the participants to have a good appreciation in information technology as part of their everyday lives. This is confirmed as 92% of the participants used a computer on a daily basis and 88% rated themselves as 'intermediate' or 'advanced' users. Moreover, the participants' level of education is considered high, as 88% claimed to hold a university level qualification.

The results showed a total of 87 recorded system-initiated events. The majority of them were recorded from security-specific applications, which translate to 76% from the total system-initiated events. A tabulation of the applications and tools that initiated the events can be seen in Table 1.

The type of system-initiated events experienced by the participants were primarily in the form of 'warning messages' (41%), followed by 'security alerts' (38%), 'update messages' (15%) and less commonly 'password requests' (6%). From the total of 87 events, 82% were fully understandable by the participants, while in the remaining 18% of cases respondents claimed that they were not able to fully understand. This translates to 16 system-initiated events out of 87 that were not fully understood by the participants.

The results also revealed that 66% of the system-initiated events required the participants to take a decision. The participants were asked to specify whether they were clear on what to do as a result, and the replies were as shown in Table 2. The

majority were clearly comfortable, but this still left more than a third of cases in which participants claimed to be confused.

Application / Tool	No. of recorded events	Amount in %
Windows Security Centre	25	30%
Zone Alarm	15	17%
McAfee	14	16%
Norton	11	13%
Internet Explorer	9	10%
Firefox	7	8%
MSN Messenger	2	2%
Safari	2	2%
Word	1	1%
Outlook	1	1%
Total	**87**	**100%**

Table 1: Ranked listing of the system-initiated events recorded during the study

Was it clear what to do next?	No. of Times	Amount in %
Totally clear	25	29%
Mostly clear	28	32%
Mostly unclear	20	23%
Not at all clear	14	16%
Total	**87**	**100%**

Table 2: Participants' understanding of what to do next at the occurrence of system-initiated events

The results relating to the help and assistance that participants used in the incidents of system-initiated events show that only 11% of the recorded events involved use of a 'help' feature, as shown in Table 3. Meanwhile, in 48% of the total system-initiated events a 'help' feature was not used, whereas in the remaining 41% the participants recorded that there was no help available. In terms of other guidance, the answer was 'no' in 92% of cases, while in 6% participants refereed to the Internet, and to other people for the remaining 2%.

In response to the final question, participants were asked if the system-initiated event prevented them from completing a task they were trying to perform at the time. Again, while the majority (78%) were not prevented, it is notable that in 22% of cases the user was effectively defeated.

Did you use a help feature?	No. of Times	Amount in %
Yes	10	11%
No	41	48%
N/A	36	41%
Total	**87**	**100%**

Table 3: Usage of a 'help' feature from the total system-initiated events

The results concerning the user-initiated events recorded a total of 29 events, which is a significant drop when compared with the system-initiated category. As with the system-initiated events, the applications and tools that were primarily recorded were

security-oriented, accounting for 66% of the total user-initiated events. Table 4 represents in detail the applications/tools and their related occurrence in user-initiated events.

Application / Tool	No. of recorded events	Amount in %
McAfee	7	25%
Norton	5	17%
Zone Alarm	4	14%
Windows Security Centre	3	10%
Router security configuration	3	10%
Back up	2	7%
Firefox	2	7%
MS Word	2	7%
Internet Explorer	1	3%
Total	**29**	**100%**

Table 4: Ranked listing of the user-initiated events recorded during the study

In most of the cases (59%) the participants were asked to take a decision at the time they initiated an event. This situation demands good understanding of the event by the participant in order to correctly take decisions. In fact the study results revealed that in more than half (15) of the total recorded user-initiated events the participants did not have a clear view when asked what to do next in the event as shown in Table 5.

At this point, considering the fact that more than the half of the user-initiated events claimed 'not clear of what to do next', the presence of a 'help' feature is considered imperative. In reality the study results revealed that for 58% of the user-initiated events recorded by the participants that there was no help available, as shown in Table 6.

How clear was it to do what you had to do?	No. of Times	Amount in %
Totally clear	10	34%
Mostly clear	4	14%
Mostly unclear	6	21%
Not clear at all	9	31%
Total	**29**	**100%**

Table 5: Participants' understanding of how to perform user-initiated events

Did you use any help feature?	No. of Times	Amount in %
Yes	**4**	**14%**
No	**8**	**28%**
N/A	**17**	**58%**
Total	**29**	**100%**

Table 6: Usage of a 'help' feature from the total user-initiated events

The absence of a help feature reduces the usability which is one of the main considerations in HCI. In the remaining 14% of user-initiated events (i.e. four instances) the participants actually made use of an available 'help' feature. This result indicated that end-users did not often use a 'help' feature, considering that the

option was present twelve times, and eight times the participants did not use it. Additionally, in the majority of the cases (23 times) no other guidance was drawn upon. Only six times did the participants look after for some additional help, with four cases on the Internet, and in two cases they turned to other people.

The last question asked if participants were able to complete their intended action. Even though in the majority of the cases (66%) they managed to accomplish their tasks, there were ten user-initiated events (34% of the total cases), in which participants did not manage to complete their task. This certainly suggests problems in terms of the clarity and usability of the provided security, and represents an area for further attention.

5. Discussion

The participants' feedback was analysed in order to investigate the usability of security in applications that end-users normally use. The main objective was to indicate if they are capable to deal with them. The study results relating to the system-initiated show that 18% of the total events were not fully understandable. This is much more intense when considering the user-initiated events, since the survey results revealed that ten out of the 29 events were not able to be completed. If these findings are representative of wider user experiences, then they certainly highlight a significant problem. Moreover the infrequency of user-initiated events in the study suggests that many end-users do not actually use security intentionally, and instead rely upon the default features of their applications. Furthermore, some recorded incidents indicated that when participants attempted to accomplish an advanced task, such as setting firewall rules, they failed and ended up frustrated. Some participants underlined the fact that there was no appropriate help, which made their tasks even more difficult. Additionally, plenty of times there was no help available, which made participants simply give up. Participants eventually spend time and effort without any outcome. This has as a consequence that end-users probably avoid security related tasks in the future.

6. Conclusion

This paper highlighted some real incidents that end-users are facing when they come across security events. The results from the survey indicate the importance of the situation. End-users barely make intentional use of security. This abstention has as a consequence that end users are not able to have full usage of the available security. Ideally, they should derive confidence to use security by having complete control over security events in order to fulfil their tasks. Security functionality within applications has been seen to demand experience and knowledge from end-users. This leads to an immediate discrimination between users: on one side some users are able to protect themselves, whereas on the other side are users that simply cannot do so. It is very difficult for an end-user with limited computer literacy and experience to be able to use the available security features.

In terms of future research, it is recognised that the user population involved in this initial study was relatively small. As such, it would be desirable to undertake a

wider exercise involving more participants, with a wider range of backgrounds. In addition, it would be beneficial for such a future study to further simplify the task of recording events, so as to prevent participants from neglecting to do so.

7. References

Furnell, S. M. (2005), 'Computers and Security: Why Users Cannot Use Security', *Computers and Security* 24(4), 275–279

Microsoft Corporation Web Site (2006a), "*Security*", Available at: http://office.microsoft.com/en-us/assistance/ha011403111033.aspx, (Accessed on 20 August 2006)

Microsoft Corporation Web Site (2006b), "*Windows XP Service Pack 2 Overview White Paper*", Available at: http://msdn.microsoft.com/security/productinfo/xpsp2/default.aspx, (Accessed on 21 August 2006)

Whitten, A. and Tygar, J. D. (1999), 'Why Johnny Can not Encrypt: A Usability Evaluation of PGP 5.0.', *in Proceedings of the 8th USENIX Security Symposium* pp. 23–26. 56