Assessing the usability of system-initiated and user-initiated security events

D. Chatziapostolou[1], S.M.Furnell[1,2]

[1] Network Research Group, School of Computing, Communications & Electronics, University of Plymouth, Plymouth, United Kingdom
[2] School of Computer and Information Science, Edith Cowan University, Perth, Australia

Abstract

The increasing deployment of security-oriented software, as well as the inclusion of related functionality within general tools and applications, means that end-users are increasingly likely to encounter security-related events. However, the way in which security is conveyed can often serve to complicate matters, which may ultimately prevent users from using security as they desire or expect. This paper presents the results from an initial study involving 26 end-users in order to assess the extent to which system- and user-initiated security events occur during their day-to-day use of their system, and the extent to which these events are understood. The results expose issues of difficulties on the security events, with more intense when actually end users make use of security intentionally.

Keywords: *Security, Usability, System Events, User Events, Barriers*.

Introduction

It is now common for end-users to find themselves more frequently exposed to security functionality than they were in the past. With the increasing volume of threats in IT world, users will encounter security during many forms of system usage and interaction. A significant factor here has been the integration of security features into software such as operating systems (OS) and general applications. For instance, in Windows XP, the integration of security has significantly improved since the introduction of Service Pack 2 in 2004 (Microsoft, 2004). As a consequence, end-users of the OS potentially come across with security terminologies such as pop-up blockers, software update messages and alerting messages for possibly unsafe attachments. Additionally, the usage of software dedicated to security, such as firewalls, antivirus and antispyware, has significantly increased as the associated threats become more widespread and recognised. Additionally, many general applications can incorporate security functionalities. For example, several applications within the Microsoft Office suite provide password and encryption functionality in order to protect against misuse of data.

Although the increased deployment of security is encouraging, the full reality of this situation is less positive. Even though functionality is provided, users can be deterred if they are not able to understand the security presented to them - which is often the case because security is not optimally designed for the end-user audience, and problems arise at the level of interaction between end users and the IT systems. The clarity and usability of security functionality is of critical importance, because an unusable product might prevent end-users (in both workplace and domestic contexts) actually benefiting from the protection provided.

Therefore, end users must be able to find the security available to them, and determine how to use it.

This paper presents details of an initial investigation of usability challenges that end-users may face in commonly used software. After a brief acknowledgement of prior works on usability and security, the paper proceeds to present the results from a study conducted to examine end-user understanding of security events occurring during routine daily use of PC systems. The findings reveal that users can face significant challenges in dealing with both the events that they initiate, and those that the system presents to them.

Examples of security usability problems

Examples of security being difficult to understand and use have been witnessed numerous times by security researchers. In the area of security-oriented tools, a prominent example is Whitten and Tygar's evaluation the usability of PGP 5.0 (Whitten and Tygar, 1999). Their work is one of the first standard examinations of usability of security applications, and their findings showed that the PGP 5.0 user interface had severe problems which made public key cryptography a difficult task for an average computer user. A later study by Johnston et al. (2003) focused upon the Internet Connection Firewall (as it was then named) in Windows XP. The work identified a number of deficiencies against proposed HCI criteria, and then presented a redesigned version of the firewall interface, that was more compatible with these recommendations. Another study involving redesign to improve usability was conducted by Belfanz et al. (2004) and focused upon a Public Key Infrastructure (PKI) system. Testing with 200 participants revealed that while the old PKI took an average of 140 minutes and 38 steps for users to deploy, the redesigned version took just 1 minute and 39 seconds, and could be performed in only four steps. The important lesson that learned from this study is that security and usability have to be considered together, and it evidences the differences that can result when this is not the case.

Unfortunately, the problem of usability can extend beyond dedicated security tools, and can also be observed within applications that support security functionality. For example, a study from Furnell et al. (2006) revealed that users frequently had problems understanding the presentation of security functionality in a number of standard tools and applications (including web browsing, word processing and email software).

Given the potential for users to face challenges from several directions, it is considered relevant to examine the extent to which this occurs in practice, and the nature of the security-related encounters that they are likely to experience. This forms the basis for the current investigation, and can also be partially related to work from de Paula et al. (2005), who identify that problems often occur as a result of the way security manifests itself during users' interaction with systems.

Security events facing end-users

Broadly speaking, end-users are likely to face two categories of security event during their use of a system – those that they initiate for themselves, and those initiated by the system.

- **System-initiated events:** These types of events occur with intention to inform the end-user about security issues and/or require related decisions. Thus, this type of event is initiated by the system and targets the end user. For example, many users will 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 depicted in the Figure 1.

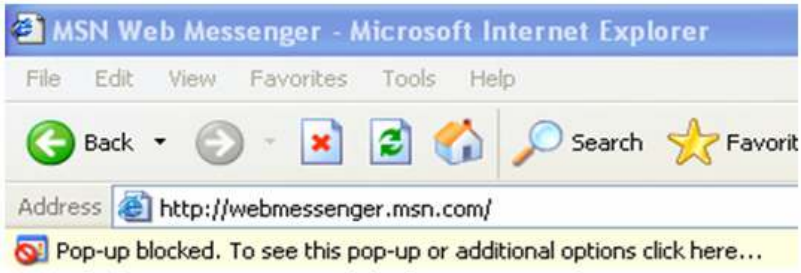

Figure 1 : A system-initiated event in the form of pop up message

- **User-initiated events:** These types of events differ from the system-initiated events because this time the user intends to deal with security. More specifically, this applies when an end-user actively seeks to invoke an element of security (e.g. encrypting a message) or perform a security-related task (e.g. controlling or configuring security-related features within applications and tools). An example of a user-initiated event is shown in Figure 2 – in this case the decision to adjust the security settings in a web browser.

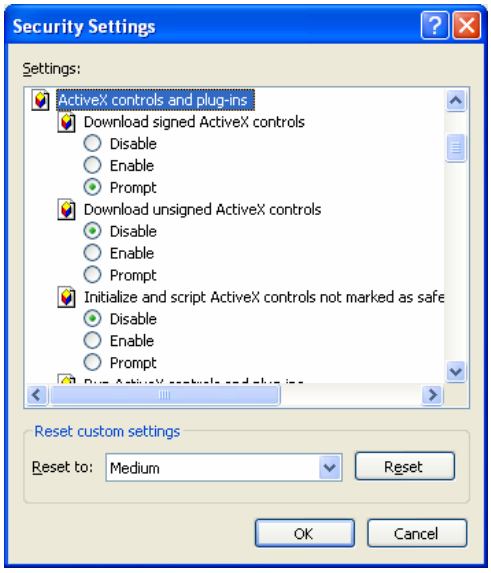

Figure 2: A user-initiated event in Internet Explorer

Experimental methodology

The study aimed to assess the degree to which end-users find themselves encountering security in day-to-day use of their own system, and the extent to which any associated events were understood when they occurred. In order to enable a reasonable assessment, participants were asked to voluntarily record details of all security-related events that they encountered

over a period of two weeks. They were asked to make a distinction between system- and user-initiated events, and were provided with separate recording sheets for each category. The aspects that users were asked to record in relation to each type of event are listed in Table 1. The aspects to be recorded were somewhat different according to whether they related to system- or user-initiated events, recognising that in the former case the user was being confronted with security (potentially unexpectedly), whereas in the latter case they presumably had a security objective in mind that they were wishing to accomplish. The recording exercise sought to determine how users dealt with each scenario, and the extent to which they understood what was required of them. Although each category appears to entail a significant number of questions, the majority were designed to require brief (often yes/no) responses, and the explanation/comments aspects were optional.

System-initiated events	User-initiated events
▪ Date and time of event ▪ Application in use ▪ Type of event ▪ Did you fully understand this event? ▪ Was it clear what to do next? ▪ Did you use a 'help' feature? ▪ Did you use any other guidance? ▪ Did the event prevent you from completing the task you were trying to perform? ▪ Brief explanation of the event and any comments?	▪ Date and time of event ▪ Application in use ▪ What did you intend to do? ▪ Were you asked to take a decision? ▪ How clear was it to do what you had to do? ▪ Did you use a 'help' feature? ▪ Did you use any other guidance? ▪ How much time did you spend in total? ▪ Were you ultimately able to complete the intended action? ▪ Brief explanation of the event and any comments?

Table 1 : Details recorded for system- and user-initiated events

Field	Response
Application	Firefox
Type of event	Warning
Did you fully understand this event?	No
Were you asked to take a decision?	Yes
Was it clear what to do? (3=totally clear; 2=mostly clear; 1=mostly unclear; 0=not at all clear)	0
Did you use a help feature?	NA
Did you use any other guidance?	No
Did the event prevent you from completing the task you were trying to perform?	No
Brief explanation of the event and any comments?	I was trying to open a website but it turned out that the site's certificate having a problem. Not sure what will happen to my computer if I opened it (decided to open).

Table 2 : Typical response recorded for a system-initiated event

After a brief trial of the recording sheets, they were distributed to an end-user population, with accompanying guidance notes and the request that they be used to record details of all events occurring that were perceived to be security-related. Table 2 depicts an example of an actual entry made by a participant (in this case relating to a system-initiated event), which is typical of the type of feedback received.

Findings and analysis

A total of 26 participants were recruited for the study, with an equal split between genders. The majority (68%) were in their twenties, with the remainder fairly evenly split between participants under 20, and those aged 30-39 and 40-49. The concentration in the 20-29 category was because a large proportion of the participants were drawn from the student community. Although this was consequently not a balanced sample in terms of background, it did serve to ensure a good level of exposure to information technology, with 92% using a computer on a daily basis, and 88% rating themselves as 'intermediate' or 'advanced' users. The participants' level of education was also high, with 88% claiming to hold a university level qualification. A final demographic of note is that the majority of responses were based upon the participants' use of Windows-based systems.

The sub-sections that follow consider the findings in relation to the system- and user-initiated events that were recorded. In both cases, the investigators had no means of gauging how accurate or comprehensive the participants had been in recording the events that they encountered. It is expected that some participants will have been more dedicated than others in their use of the recording sheets, with some regarding the expectation to record their encounters as burdensome during periods of other significant activity. Nonetheless, all of the participants provided some level of input, enabling some insights into both types of event under analysis. However, due to the fact that the sample sizes were still relatively small, the results are presented as averages across the full set of responses rather than attempting to identify patterns within subsets.

System-initiated events

A total of 87 system-initiated events were recorded, with all participants reporting at least one event. The vast majority of events (76%) were found to originate from security-specific software. The full breakdown of the specific software and applications that initiated the events can be seen in Table 3.

In terms of the actual event types involved, the most common response was categorised as 'warning messages', which contributed to 41% overall. This was followed by 'security alerts' (38%), 'update messages' (15%) and finally 'password requests' (6%). Encouragingly, in the majority of cases (82%) the participants reported that they had understood the event that they encountered. However, this still left almost a fifth of cases in which users were not clear about what was going on – thus potentially putting them at risk of making a mistake. This finding is even more significant when it is realised that 66% of events required participants to make a decision in terms of how to proceed. When asked to indicate whether they were clear on what to do as a result, the responses were as shown in Figure 2. While the majority were clearly comfortable, this still left more than a third of instances in which participants were confused. Prior work from DeWitt and Kuljis (2005) has observed that, when faced with a

requirement to make security-related decisions, users will often take whatever path seems quickest in order to get their work done – even if this means compromising their security. As such, encountering events that are unclear in the first place will add further incentive for security to be sidelined.

Application / Tool	No. of recorded events	Amount in %
Windows Security Center	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 3 : Ranked listing of the system-initiated events recorded during the study

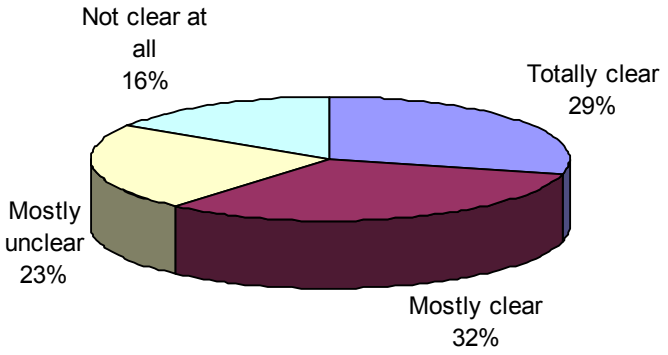

Figure 2 : Participants' understanding of how to respond to decisions required by system-initiated events

In terms of help and assistance, participants only made use of a 'help' feature in 11% of the recorded events. In 48% of cases help was not used, while 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 referred to the Internet and to other people in the remaining 2%.

In response to the final question, participants were asked if the system-initiated event prevented them from completing whatever 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.

User-initiated events

The study period saw a significantly lower number of user-initiated events, with only 29 being recorded during the two week period. Indeed, it is notable that, whereas all users had recorded system-initiated events, only 46% reported that they had initiated one. The largest incidence was again associated with security-oriented applications, with a total of 9 applications being represented in total (see Table 4). The lesser number of events reflects the fact that, in many applications, users do not have to routinely involve themselves with initiating security events once the application has been installed and configured. For example, in many cases, users are happy to accept default settings, and some of the most common security tasks (e.g. virus scanning) can rely upon automated, scheduled tasks rather than requiring a manual intervention from the user each time they need to be used. However, there are still some decisions that security-conscious users might be expected to make on a case-by-case basis, such as password-protecting their documents, or encrypting email messages, but the results observed here tend to suggest that these were not frequent requirements amongst the participant group.

Application / Tool	Number of recorded events	Amount in %
McAfee	7	25%
Norton	5	17%
Zone Alarm	4	14%
Windows Security Center	3	10%
Router security configuration	3	10%
Backup	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

The majority of events (59%) again required participants to make some decision, and again the extent to which they felt able to do so was variable (see Figure 3). Although a greater proportion felt 'totally clear' in this context (possibly reflecting the fact that the users themselves were in control of the situation when initiating events), there was also a far greater proportion that were not clear at all.

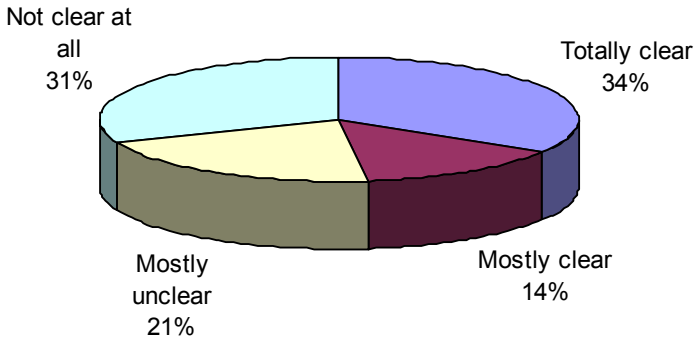

Figure 3 : Participants' understanding of how to perform user-initiated events

In the 14% of cases (4 actual instances), participants made use of 'help' facilities, but it was notable that in 58% of cases they reported that none was available. As with the system-initiated events, in the majority of cases (80%) no other guidance was drawn upon. On 6 occasions (13%) participants sought some additional help on the Internet, and in two instances they turned to other people.

The participants' responses suggested that tasks took an average of almost 6.5 minutes to accomplish. However, the investigators suspect that this value was somewhat skewed by some users recording the entire duration of tasks such as back-ups, rather than the time it took to initiate them.

The final question for each event again asked whether participants were able to complete the intended action. Although this was positive in 62% of cases, there were 10 user-initiated events 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.

Conclusions

This paper has highlighted the real challenges that end-users can face when they encounter security-related events. Both sets of event samples recorded during the study period included significant proportions in which users were unclear on what they had to do and/or were prevented from completing the task that they were attempting to undertake. Even from the relatively small sample involved, it is clear that the security features within applications can demand knowledge that end-users do not possess. This leads to an unfortunate separation between users, and whereas one side are capable of protecting themselves the other side simply cannot. In addition, it is worth remembering that the results were obtained from a group that largely classed themselves as 'intermediate' or 'advanced' users, which certainly does not bode well for the likely experience of novices.

The lower volume of user-initiated events suggests that end-users rarely make intentional use of security functions within applications and tools. The likely truth is that users often rely on default security settings of security applications. However, such settings should not be taken

for granted to be appropriate for all users. With this in mind, the problems encountered with the user-initiated events are of particular concern, because it suggests that even when users were aware enough to recognise that they had a security requirement, the system often prevented them from carrying it through. As an example, there were some incidents in which participants attempted to set firewall rules for their computers. However, many found themselves without any appropriate help which made their task difficult and left them frustrated. Moreover, the fact that they lost time and effort without any useful outcome could possibly lead them to avoid security-related tasks in the future.

Given that the findings were collected over a two-week period, it can be concluded that on average users appear to face relatively few security-related demands during typical day-to-day use. However, it is recognised that some participants were more diligent than others in terms of their voluntary recording of events, and (especially from the authors' own experience of encountering system-initiated security events) it is suspected that there were more instances that could have been recorded. As such, a clear area for improvement in a future study would be to further simplify the recording task, so as to prevent participants from neglecting to do so.

Another limitation in the initial study was the relatively small user population. As such, it would be desirable to undertake a wider exercise involving more participants, with a wider range of backgrounds. With sufficient participants, it would also be interesting to conduct a comparison between the different user groups (e.g. novices versus advanced users), as it would instinctively be expected that those with less technical ability would face more difficulty with system-initiated events, as well as potentially encountering fewer scenarios in which they wished to initiate security for themselves.

Further opportunities for a future study would include more specific analysis of the contexts in which users were recording their events. For example, the initial study made no attempt to determine aspects such as the regular daily activities of the participants, or the range of applications installed and used, or the prior settings of the system. It is clear that all of these could influence the nature of security-related events that users might wish to initiate for themselves, as well as the types of system-initiated event that they may be exposed to. For example, even if participants were using the same application, the configuration settings could affect their experience of security within it (e.g. if the system had been previously been instructed to suppress certain types of warning).

References

Balfanz, D., Durfee, G., Smetters, D. K. and Grinter, R. E., (2004), In Search of Usable Security: Five Lessons from the Field, IEEE Security & Privacy Journal, vol. 2, no. 5, 19-24.

de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D., Ren, J., Rode, J. and Silva Filho, R., (2005), Two Experiences Designing for Effective Security, Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS '05), Pittsburgh, Pennsylvania, USA, July 6- 8, 25-34.

DeWitt, A. J. and Kuljis, J., (2006), Aligning usability and security: a usability study of Polaris, Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS '06), Pittsburgh, Pennsylvania, USA, July 12-14, 1-7.

Furnell S. M., Jusoh, A. and Katsabas, D., (2006), The challenges of understanding and using security: A survey of end-users, Computers & Security, vol. 25, no.1, 27-35.

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

Microsoft, (2004), Windows XP Service Pack 2 Overview, White Paper, Microsoft Security Developer Center, February 2004. http://msdn.microsoft.com/security/productinfo/xpsp2/default.aspx.

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, 169-184.