Firewalls Usability: An Experiment Investigating the Usability of Personal Firewalls

Bander AlFayyadh
Queensland University of Technology, Australia
Email: b.alfayyadh@student.qut.edu.au

Mohammed AlZomai
K.F. Security College, KSA
Email: zomaim@kfsc.edu.sa

Audun Jøsang
University of Oslo, Norway
Email: josang@mn.uio.no

***Abstract*—Poor usability of IT security systems and applications represents a serious security vulnerability, which can be exploited to compromise systems that otherwise could be considered technically secure. This problem is of particular concern with the huge number of users regularly connecting to the Internet but who know very little about the principles of IT security. Personal firewalls are important security mechanisms for protecting users against Internet security threats. However, the knowledge and skills required to effectively operate some aspects of a personal firewall may surpass the capability of the average user. In previous work, we conducted a usability evaluation of personal firewall by cognitive walkthrough against a set of security usability principles. We concluded that there are many usability issues of personal firewalls that can cause security vulnerabilities. In this paper, we report the results of a practical usability experiment with participants using commercial firewalls in a controlled environment. The experiment setup is described and participants' feedback and behaviour are analysed to evaluate the impact of usability of a modern firewall on the overall security of personal workstations.**

Keywords–Usability; Security; Firewalls.

I. INTRODUCTION

The number of computer and Internet users is huge and still growing worldwide, with client terminals roaming between wireless and wired networks that potentially enable access from the Internet to processes or to private data on the client terminal. Protecting private data in this environment is becoming more and more important. As computer users face threats and attacks they look for tools to protect their data. According to the Computer Crime and Security Survey [7], one of the most popular tools used for this purpose is a personal firewall. A firewall is defined on an abstract level as "an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system" [2]. More specifically, a firewall is a checkpoint that controls and filters traffic between two separate networks or network segments, according to specific rules based on content or network parameters. Threats are prevented by denying access to or from specific hosts or processes when it is in conflict with the firewall rules. Generally, if used correctly a personal firewall should provide reasonably good security against network threats. The crucial point of operating a firewall is to specify the appropriate network filtering rules. Personal firewalls have become an essential part of online security. But as with many other security tools, a sound security system could be compromised by users' ignorance or carelessness about firewall operation [8], [9].

Inappropriate operation of security tools can in general be the result of human apathy towards security policies, but in many cases it may very well be due to the poor usability of the security tool or system itself. Usability of personal firewalls is especially important and critical. The target market for personal firewalls is typically the normal Internet user with little or no knowledge about IT security, so given the inherent sophisticated nature of personal firewall configurations, it is easy to understand why usability is a concern.

Poor usability of a security system can lead to serious consequences as pointed out by several authors. Whitten and Tygar's study [11], [10] on the usability of PGP showed that the security vulnerabilities were a direct result of usability problems. The same could be said about personal firewalls; personal firewalls usually run in the background and alert the user if needed, the alert can be as clear as a pop-up window or as subtle as a color change of a small icon in the system tray. The user typically reads for example the content of the pop-up window. Based on his/her understanding of the message from the firewall the user must make a security decision and potentially take some action that will affect the security of the system.

A novice computer user may not have the required level of knowledge to manage a firewall properly. They may not understand the terminology used by the firewall or the consequences of some of the decisions he/she is required to make. Users may often click away just to continue on with their computer related task, thus exposing themselves to possible threats that the firewall could have prevented. This behavior can be attributed to poor usability or users' apathy or maybe both. We aim to test the usability of firewalls by observing users' interaction with firewalls, specifically, what decision/action they make during that interaction and why they make it.

To conduct usability evaluation, we designed an experiment in a controlled lab environment. We configured several machines with selected firewalls and observed participants while interacting with the firewalls. We tried to make the experiment as realistic as possible by creating a familiar scenario that resemble normal computer usage for the participants. The scenario was not directly aimed at performing security tasks since security normally is not the primary goal of users when accessing the Internet. We asked participants to perform a simple task such as playing a game, during which several events (e.g., a pop-up message) caused by the firewall would occur, and that requires their attention. The participants were observed during the events, and based on the information provided by the firewall we examined whether they understood or did not understand the events.

 ISBN: 978-1-61208-298-1

In a previous work, we evaluated the usability of personal firewalls by cognitive walkthrough against a set of eight usability principles proposed by Jøsang *et al.* [5] which in turn were inspired by security principles suggested by the Belgian cryptographer Auguste Kerckhoffs [3], [6]. Jøsang *et al.*'s security usability principles are divided into principles for security action and security conclusion described as follows:

- A *security action* is when users are required to produce information and security tokens, or to trigger some security relevant mechanism. For example, typing and submitting a password is a security action.
- A *security conclusion* is when users observe and assess some security relevant evidence in order to derive the security state of systems.

The eight security usability principles are:

1) Security Action Usability Principles
   a) The users must understand which security actions are required of them.
   b) The users must have sufficient knowledge and the practical ability to make the correct security action.
   c) The mental and physical load of a security action must be tolerable.
   d) The mental and physical load of making repeated security actions for any practical number of transactions must be tolerable.
2) Security Conclusion Usability Principles
   a) The user must understand the security conclusion that is required for making an informed decision. This means that users must understand what is required of them to support a secure transaction.
   b) The system must provide the user with sufficient information for deriving the security conclusion. This means that it must be logically possible to derive the security conclusion from the information provided.
   c) The mental load of deriving the security conclusion must be tolerable.
   d) The mental load of deriving security conclusions for any practical number of service access instances must be tolerable.

Whenever one or more of these principles is violated during user interaction with the firewall we considered that to be a usability problem. Violating these principles will not necessarily indicate a security risk when using non-security software (e.g., a word processor) but it may cause security vulnerability when using security software (e.g., anti-virus filter or a firewall). The difference between normal usability and security usability has been pointed out in the literature [11]. Personal firewalls normally have decent usability from a traditional CHI point of view. However, when tested against these security usability principles, specific usability problems were detected.

The rest of the paper is organized as follows: Sec. II gives a brief description of firewalls interface. Sec. III describes the study design and experiment procedure. Sec. IV presents the experiment results; the results are analyzed in sec. V and discussed in sec. VI. The paper is concluded in sec. VII.

II. Personal Firewalls Interface

In this section we provide a brief description of general firewall interface and the way a user can interact with it. Personal firewalls are transparent and usually work in the background. When they need to communicate with the user they do it through a pop-up window or an alert message. When they communicate with the user it is either to alert for a possible threat or to ask them to make a decision regarding the function of the firewall.

Users can interact with firewalls through the following interface channels:

A. Main Menu

The main way to control and configure the firewall is through its main menu. The user can check here the status of the firewall, security status of the system, recent events, logs and other information.

B. Pop-Up Notifications

Pop-up notifications are commonly used by the firewall to inform a user of a current event which requires the user's attention. The pop-ups occur when the firewall requires the user to make a decision, or needs to inform the user of a decision or an event.

C. System Tray Notifications

It is common for firewalls to display a small icon on the bottom right of the screen in what is known in Windows as "System tray". The purpose of this icon is to provide quick access to the firewall menu; it also serves as warning mechanism or status alert through a change of color. Usually, it is green for "System Safe" status and red otherwise.

We suspect that the subtle change in color could go on unnoticed by users. We addressed that issue in our experiment.

III. Study Design

In this section, we will describe our study in detail. The goal of the study is to investigate whether users with little knowledge about IT security would be able to understand the information provided by a firewall when they are asked to make a decision.

We conducted a firewall usability experiment where we had participants operating computers in a lab environment while we observed how they dealt with firewall alerts and messages. In addition, the participants were asked to answer several questions before, during and after the experiment. A description of the questions is in section III-B. The result is shown in section IV.

 ISBN: 978-1-61208-298-1

A. Participants

The experiment target were computer users who were not skilled in IT security. For our selection process, we asked for participants who are not studying IT or working in the IT field. Most of our participants were from disciplines such as Law or Business. Another screening excluded some participants that had high IT skills gained from personal experience.

The participants age, sex and ethnicity varied. We did not record any personal details except their discipline/profession. However, the participants signed a consent form which contains their name, these forms are kept separate from the questionnaire forms.

There was no risk to participants other than those inherent to using a computer for about an hour. After the experiment, the participants were briefed about their performance and whatever questions they had were answered.

B. Questions

The questionnaire was divided into three groups of questions denoted A,B and C.

- **Question Group A.** These questions were given before the experiment, with the goal of determining the background knowledge each participant has or thinks that he/she has about firewalls. The questions are:
  Q1) Do you know what a firewall is?
  Q2) Do you know the purpose of a firewall?
  Q3) Do you know how to operate a firewall?

- **Question Group B.** These questions were given during the experiment, and were repeated for every event during the experiment. From the beginning of the event (e.g., A Pop-Up would appear) until the end of the event (When the user makes a decision and takes action). The goal was to determine how much the participant understood from the information contained in the alert, if the participant did not understand, then how would that affect his/her decision.
  These events are:
  1) Warning message alerting the user that a web browser is trying to access the interenet.
  2) Warning message alerting the user that an application from another machine is trying to access local files using a File Transfer Prorocol (FTP) client.
  3) Warning message alerting the user that a game he is playing is trying to send some information to an outside server.
  4) Change in color in the system tray icon of the firewall indicating a change in the system security status.

- **Question Group C.** These questions were given after the experiment. The participants answered several questions that should reflect their evaluation of the usability of personal firewalls during the experiment. The questions are listed below.
  While doing the experiment:
  Q1) Was it easy to make the decisions when prompted by the firewall?
  Q2) Did you make a decision that you thought might have been wrong but did it anyway in order to get on with your task?

C. Experiment Procedure

We prepared the experiment in a computer laboratory at QUT (Queensland University of Technology). The PCs were identical and all participants were familiar with the Windows operating system on the machines.

We had 30 participants for our experiment. Participants would come in and we would ask them to use the computer for a while until they are comfortable with the environment. Afterwards, we would explain to them the nature of the experiment and ask them to answer questions from group A of the questionnaire. We instructed the participants to behave as they normally do when using their own computers.

The participants were asked to perform simple tasks such as browsing the internet or playing a game. While they are doing that, an event caused by the firewall would occur. The event could be as direct as a firewall pop-up message that prompt for a decision or a subtle change of color in the firewall system tray icon. During each event the participants' behavior was observed and we would ask them several questions regarding each event. The questions would be about things such as their understanding of the event, why it occurred and what decision they made.

After several events, we conclude the experiment by asking participants to answer the last part of the questionnaire. Every participant did the exact experiment and dealt with the same events as every other participant. The duration of the experiment had an average of 40 minutes.

IV. Results

The study consisted of three stages. In the first stage the participant were asked to answer group A questions, their answers can be seen in Table I and Fig. 1.

TABLE I - Stage 1 results

Question no.	Yes	Somewhat	No	Total
Q1	14	9	7	30
Q2	10	11	9	30
Q3	6	10	14	30

Stage two represents the interactive part of the study. Participants had to deal with four firewall generated events while using a computer. Three of theses events were represented by firewall pop-ups or warning message that required the participant to make a decision and take action. In each of these three events, the participant must either allow the event or block it. The participant also may chose to close the warning window without taking an action.

The purpose of these three events is to evaluate the participant's ability to understand events created by the firewall and

 ISBN: 978-1-61208-298-1

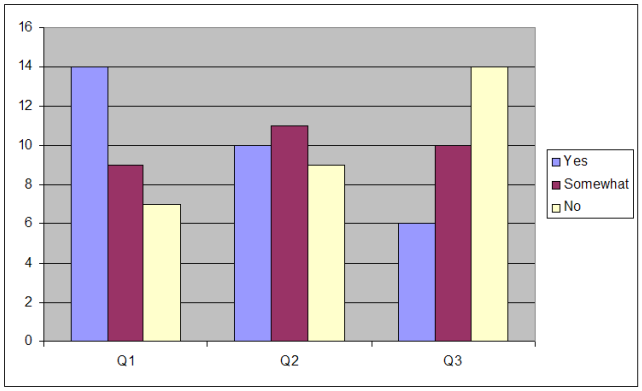

Fig. 1. Stage 1 results

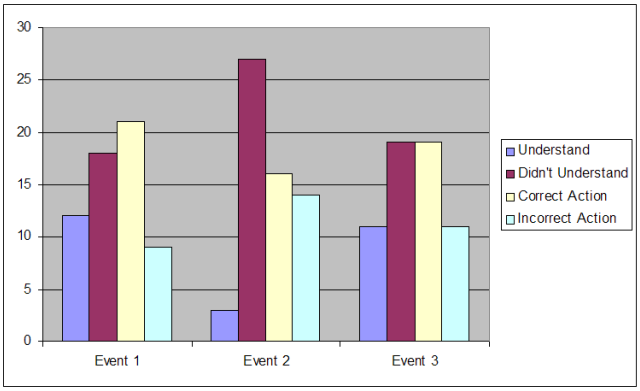

Fig. 2. Stage 2 results

hence make correct decisions. Accordingly, we interpret our data in terms of how many participants understood the event and how many took the correct decision.

We classify the data from the participant's interaction with these three events into the following four categories:

- **Category 1 (Understand)** Number of participants who understood the event: This occurs when a participant states that he/she understood the event's warning message, explains it correctly and makes the correct decision.
- **Category 2 (Didn't Understand)** Number of participants who didn't understand the event: This occurs when a participant states that he/she didn't understand the event's warning message or fails to explain it correctly.
- **Category 3 (Correct Action)** Number of participants who made the correct decision.
- **Category 4 (Incorrect Action)** Number of participants who made incorrect decision: This occurs when a participant made an incorrect decision or closed the event's warning message without making a decision.

Tables II, III and Fig. 2 show the data collected from observing participants interaction with the firewall and their answers to group B questions during their interaction.

TABLE II - STAGE 2 RESULTS (A)

Event No.	Understand	Didn't Understand	Total
Event 1	12	18	30
Event 2	3	27	30
Event 3	11	19	30
Total	**26**	**64**	**90**

TABLE III - STAGE 2 RESULTS (B)

Event No.	Correct Action	Incorrect Action	Total
Event 1	21	9	30
Event 2	16	14	30
Event 3	19	11	30
Total	**56**	**34**	**90**

In category 2 (participants who didn't understand the event's warning messages), when we asked why they didn't understand the event's warning message, the participants gave one of two reasons: The first was that the message language was unclear (e.g., too technical) and the second was insufficient information provided in the message contents. Table IV and Fig. 3 show the breakdown of the participants answers.

TABLE IV - REASONS FOR NOT UNDERSTANDING THE EVENT WARNING MESSAGE

Event No.	Unclear Language	Insufficient Information	Total
Event 1	12	6	18
Event 2	20	7	27
Event 3	13	6	19
Total	**45**	**19**	**64**

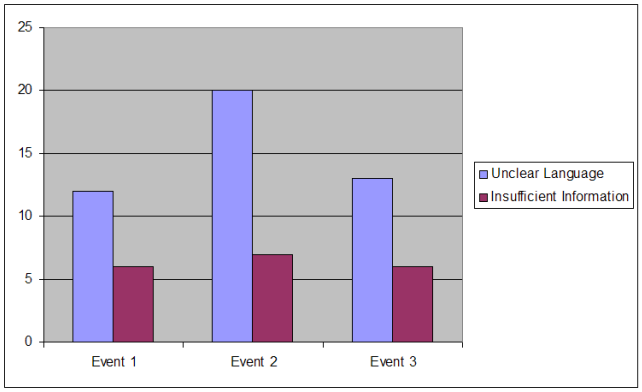

Fig. 3. Reasons for not understanding the event warning message

The last part of stage two was to examine if the participants would notice and respond to the fourth event (color change in the firewall icon in the system tray). While the participant is performing a computer task, we initiated some traffic that made the firewall change it's system tray icon from green to red, which may indicate a risk. Then we asked the participants if they noticed the event. For those who noticed the subtle color change we asked them if they understood the meaning

 ISBN: 978-1-61208-298-1

behind it. Accordingly, we classified the participants into three categories:

- Participants who didn't notice the event (23 out of 30).
- Participants who noticed and understood the event (6 out of 30).
- Participants who noticed the event but didn't understand what was the meaning of the icon alert (1 out of 30).

After stage two, participants were asked to answer questions from group C. The answers to these questions can be Yes, No or Somewhat. Their answers are shown in Table V and Fig. 4.

TABLE V - STAGE 3 RESULTS

Question no.	Yes	Somewhat	No	Total
Q1	7	4	19	30
Q2	16	5	9	30

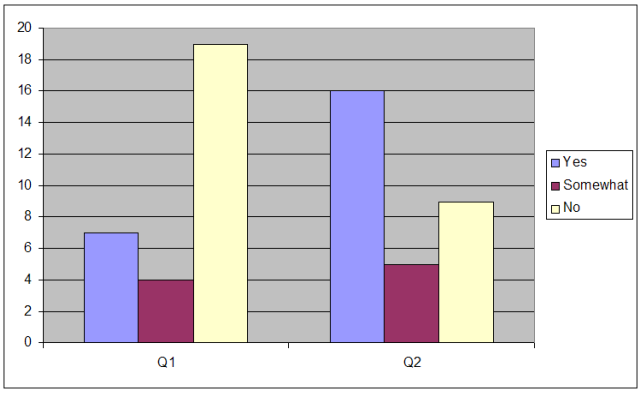

Fig. 4. Stage 3 results

V. ANALYSIS

A common behavior that we noticed is that at the beginning of the experiment participants would carefully examine each event, taking time to read messages in detail. But as the experiment progressed they tend to be quicker and dismissive. We interpreted this as the participant is "getting into" their assigned tasks. The tasks were chosen to be entertaining to create an atmosphere where the participant would be eager to continue on with the task, which is the case when he/she is working on their own computer.

From Table I, it is clear that the participants were not experienced in dealing with firewalls, almost 25% declared that they don't know what a firewall is exactly, and 30% stated that they don't know what a firewall is used for. Also, from their answers to the first group of questions, about 50% said they do not know how to operate a firewall and this was confirmed from our observation as well. We put their general skill level from low to moderate.

Stage two of the study in which participants interact with the firewall is the significant part of the study, we observed how the level of usability of the firewall affected the participants decision making when faced with security concerns. Tables II, III and IV represent the result of this stage.

Table II shows that less than a third of the warning messages (26 out of 90) that occured during the experiment were understood by participants, which means that more than two thirds of the firewall warning alerts were not understood by the participants. This is an alarming indication of serious usability weakness in the way firewalls give feedback to users.

Table IV shows the reason why those warning messages were not understood. When asked, 70% of the participants said the warning messages contained "Unclear Language" while 30% said it was due to "Insufficient Information" in the content of the warning message provided by the firewall.

Even though only 29% of the warning messages were understood by participants, it was interesting to see that 62% (56 out of 90) of the actions taken by participants were correct decisions (see Table III). This means even though some participants did not understand the message, they still made correct action.

In the fourth event of stage 2, only 23% of the participants noticed the change of color from green to red in the firewall system tray icon while 77% did not.

Table V shows that 63% of the study participants do not consider making decisions when prompted by the firewall an easy task. Also, more than 50% of the participants said that the firewall was an obstacle to them while working and that they made decisions that might have been wrong in order to get on with their task.

It was interesting to see how users' behavior changes when we set the firewall to the maximum security settings. This caused the firewall to produce more alerts than usual, resulting in users becoming frustrated after few alerts and getting to the point were they started closing the alert windows without reading them.

Fig. 5. Firewall alert when trying to open a web browser

VI. DISCUSSION

Previous studies have reported usability issues in personal firewalls [4], [1]. Our study provides more detailed insight into the usability problems of personal firewalls. In particular we found that many users can be considered totally ignorant about firewalls, and the question is whether this group of people get any benefit from personal firewalls at all.

An interesting behavior is that in some cases, a participants would think that he/she understands the message content provided by the firewall in a warning and therefore he/she is sure they are making the secure decision. However, when asked to explain the message, it was clear they understood it completely or partially wrong. When we explained it to them, we asked them if this would change their future behavior dealing with this type of warnings many said that it wouldn't. Their reasoning was that they always behave like that and nothing bad happens.

To evaluate the usability of firewalls in our study, we will examine the participants behavior against the security usability principles described in section I.

One of the messages that appeared while participants were working on their tasks is a warning that an application from another machine is trying to access local files using an FTP client, 90% of the participants did not understand the meaning of that message or why it appeared. They described the content of the message to be difficult for them to understand since they didn't have any knowledge or enough knowledge of what an FTP client is. Clearly, this is a violation to principle 2.a. described in section I.

When a participant tries to open a web browser (e.g., Firefox) he would create an event, in this case a pop-up warning (see Fig. 5) that Firefox is trying to access the internet. Although this action was initiated by the participant, 60% of them said they don't understand this message even though the browser name was mentioned in the pop-up. Again, this violates principle 2.a.

Two reasons were given by the participants for not understanding the firewall warning messages, the first was due to unclear language in the message, which represents a violation to principle 1.a, the second reason was that the message does not provide sufficient information, this is clearly violates principle 1.b. The color change in the firewall system tray icon from green to red was not noticed by 77% of participants, this violates principal 2.a.

About 63% of the study participants stated that it was difficult for them to make a decision when prompted by the firewall and more than 50% considered the firewall to be an obstacle while working on the experiment. This represents an obvious violation of principles 1.d and 2.d.

As the complexity of firewalls warning messages increases, the participants make hasty or random decision in order to get their work done. In general, frustrated users usually ignore or bypass sound security measures when faced with tedious and sophisticated security tasks, which in turn make these measures, and the tools that provides them -such as firewalls- ineffective.

Finally, our study gives a strong indication that firewalls suffer from a serious security usability problem which make them insecure. Therefore, it is necessary to improve the usability of firewall to make them a more secure tool.

VII. CONCLUSION

In this paper, we presented a study on the usability of personal firewall by conducting an experiment that investigated whether users understand the information provided in warning alerts/messages from the firewall and how they would make security decision based on these alerts/messages. This study has shown that feedback to users from the firewall is mostly not understood. In case the general meaning of the messages are understood the users do not see the possible consequences this could have on the security of their system.

Firewalls act as a protective barrier between users (usually not very skilled in IT) and skilled attackers. This reality makes the job of the firewall interface hard when trying to maintain a certain level of simplification without losing technical details while giving feedback to users. In conclusion, personal firewalls typically fail to provide an adequate user interface to users. This seems to be a relatively hard problem to solve, because it would need to include an element of security learning, as well as an improved interface design.

As a final remark it can be noted that the term "firewall" itself might be part of the problem, because it gives wrong mental associations. The term "firewall" indicates that it is impenetrable and can stop all malicious traffic, which is inaccurate. A more accurate term would, e.g., be "Check Point" because it clearly indicates the aspect of checking the traffic. People would also more easily understand the the check point needs specific instructions about what should be allowed to pass and what should be stopped.

REFERENCES

[1] B. Alfayyadh, J. Ponting, M. AlZomai, and A. Jøsang. Vulnerabilities in Personal Firewalls Caused by Poor Security Usability. In *Proceedings of IEEE International Conference on Information Theory and Information Security.*, 2010.

[2] Online Dictionary. http://www.dictionary.com. Retrieved: June-2013.

[3] P. Gutmann and I. Grigg. Security Usability. *IEEE Security and Privacy*, 3(4):56–58, 2005.

[4] A. Herzog and N. Shahmehri. Usability and Security of Personal Firewalls. In *New Approaches for Security, Privacy and Trust in Complex Environments*. 2007.

[5] A. Jøsang, B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara. Security Usability Principles for Vulnerability Analysis and Risk Assessment. In *proceedings of ACSAC 2007 - Annual Computer Security Applications Conference*, Dec 2007.

[6] A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, Vol. IX(38):5–38 (January) and 161–191 (February), 1883. Translation available at F. Petitcola's Website: http://www.cl.cam.ac.uk/∼fapp2/kerckhoffs/.

[7] R. Richardson. CSI/FBI Computer Crime and Security Survey. Technical report, Computer Security Institute, San Francisco, USA, San Francisco, USA, 2003.

[8] M. A. Sasse. Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI2003), (Workshop on Human-Computer Interaction and Security Systems)*, 2003.

 ISBN: 978-1-61208-298-1

[9] M. A. Sasse and I. Flechais. Usable security: What is it? How do we get it? In L.F. Cranor and S. Garfinkel, editors, *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly, Sebastapol, CA, USA, 2005.

[10] A. Whitten and J.D. Tygar. Usability of Security: A Case Study. Computer Science Technical Report CMU-CS-98-155, Carnegie Mellon University, 1998.

[11] A. Whitten and J.D. Tygar. Why johnny can't encrypt: a usability evaluation of pgp 5.0. In *Proceedings of the 8th USENIX Security Symposium (Security'99)*, 1999.

 ISBN: 978-1-61208-298-1