Abstract

In this paper, we focus on the usability challenges presented by personal firewalls. Nowadays, the focus of IT security is changing from patching system to securing remote access, so many personal computer owners install a personal firewall to increase the security of end nodes on a network by monitoring both incoming and outgoing traffic [2]. But there are tons of personal firewalls to choose from, each with their features and complexity. The warnings or questions asked by prompts for these firewalls are often cryptic; many of their rules are not needed, or are too flexible, and are always enabled, making the network nodes vulnerable to a variety of attacks.

KEYWORDS: Firewall, usability, network security.

1 Introduction

Currently, more and more people connect their PC to the Internet. For instance, Home broadband adoption in the US grew by 40 percent from March 2005 to March 2006, twice the growth rate of the year before [4, 8]. The security of the PC is key to safe and trusted usage of the Internet. To provide this security, firewalls have a major role acting as a safety guard for PCs against various network attacks, also protecting the Internet from malicious users [5]. But the warnings given and the rules asked by these firewalls can often be cryptic. So it really confuses the users and makes the users have no way to know what applications are running on their PC. How many files are created by the applications that we know? Does it modify my registry, modify the variables of system, and modify files of my OS? Does it read data from the network transmission? Does it read data from my keyboard when I typing my password? Does it steal my account or even credit card number?

However, in order to solve this problem, a survey of a broad range of personal firewall users—from tech students to the elderly will be conducted. This experiment involves collecting different security prompts from different personal firewalls, then asking the user to respond to these prompts.

2 Background

In order to fully understand this survey, it is important to first know some definition about personal firewalls.

2.1 What a personal firewall is, and why we need one

For the same reason we lock doors, firewalls are used to control access to a set of valuable resources. With the help of a firewall, the resources in your own computer or in your local area network (LAN) are protected from other networks. The main concept is controlling access - a firewall is not a silver bullet which guarantees immunity from all kinds of evil, it is just a simple way of regulating access to our computers.

2.2 How does firewall work

The work method of a firewall is just examining all of the network traffic which passed through it, allowing the traffic which adheres to our security rules to pass and denying otherwise.

3 Related research

3.1 Whether users want application monitoring

With the help of a study which address application surveillance [2] by Almut Herzog and Hahid Shahmehri, we find that although people would not actively search for applications used for monitoring, they are still interested in that behavior.

3.2 Is the firewall is widely used by home computer user?

According to Munro and Jay’s survey [6], although firewalls are keystone in communication security, they are still used less frequently than antivirus. More than 90% of PC Magazine readers run antivirus software, but far fewer have firewalls.

3.3 Suggestions from HCISec

From the rules HCISec(Human Computer Interaction and Security) [3], we can find that:

1. You can know what users want by their actions. If a user doubleclicks a mp3 file, he wants to listen it. If a user run a bittorrent client, he wants to download or upload something, and doesn’t want to be bothered by a firewall. If a firewall did that, users will close a firewall or uninstall it.
2. Security details and decisions should be hidden from users as much as possible. We use a SSH client as a normal remote login shells to connect with servers.

3. User should be taught by security software, in order to avoid making serious mistakes.

4. Some security issues which happened frequently should be made invisible to users. A user will be botherd the needs to allow permissions to the application each time he executes it.

4 Research methodology

I have performed this survey in the following method. In this study, I selected 18 users and divided them into two groups: technical users and non-technical users. In the technical group, 8 responders were from Communication Corporation, university whose major is technical programs and all of them have experience with using personal firewalls. In the non-technical group, 10 responders were from Business Corporation, university whose major is not technical and also some housewives and retirees who use their computer just as a media player.

For both of the groups, different security prompts from different personal firewall were collected. I sent them a screen-print of security prompts given by a personal firewall installed on my computer. Then they should answer some question about that warning given by firewall:

For both two groups:
- Do you know what happened to your computer?
- What information can you get from this security prompt?
- Do you think this warning information is understandable?

For technical users, there are some additional questions:
- Does this warning mean a network attack on your computer?
- Is there something wrong with your computer that lets it be attacked by other computers, and what should you do?

In this survey, I choose these personal firewalls which are widely used in the world and in my home country China. Here is a list of them:

1. ZoneAlarm Pro
2. Outpost Firewall Pro
3. Kaspersky Anti-Virus
4. Tiny Firewall
5. Norton Personal Firewall
6. Rising Firewall

5 Feedback and result

Firewalls used for this study were installed on a personal computer with Intel Core 2 Duo E6600 CPU and 2048MB memory. The operation system of the computer is Microsoft Windows XP Professional - Service Pack 2, and its version is 5.1.2600. The default OS language is Chinese, but all the firewalls were English version. There also are some daily used applications which installed in the computer, such as firefox, emule, IM softwares (MSN and QQ [1]), BT client and Microssoft Office.

5.1 For process control

I did the following steps before I got the print screen of process control.

1. Restart the computer, and run the setup program of Outpost Firewall Pro.
2. Restart the computer again, after the firewall was completely installed.
3. After the OS was completely loaded, I opened the interface of firewall and wanted to get a glance to it. Because the interface was in English, so I run the xdict.exe which is a translation application of Chinese-English to help me. When the file "xdict.exe" was executed, a security prompt is presented on the screen.

(In this part, I was focus on the process control of personal firewall. So I ignored those security prompts which weren’t related to process control.)

In the technical group, all of the respondents knew what this prompt(Fig. 1) means. It means the application "XDICT.exe" wants to modify another application’s memory, they should set permissions for this application to "allow" or "block". 6 respondents were familiar with this application, so they knew it should be allowed to execute, and it is not harmful to the computer. The other two
<table>
<thead>
<tr>
<th>Understood</th>
<th>Technical</th>
<th>Non-technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Deny</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Not Understood</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 1: Respondents result of process control. Understood: The respondents who knew what the prompt means. Not Understood: The respondents who didn’t know what the prompt means.

respondents don’t know which application is, so they have no idea about this, both of them want me to provide more information about this security prompt. But finally one of them chose “block once” to find out what would happen if it was blocked. And the other one chose “allow once” to trust this application this time.

In the non-technical group, there are 7 users know that why this prompt is presented. The other 3 users were totally confused by this warning. They don’t know the concept of modifying memory; they have no idea if this process is harmful to the computer. But when all of the respondents were asked to choose one option, 8 users chose to allow this application to modify the others’ memory. 7 user chose the option “allow”(6 users knew what this prompt means and 1 user who didn’t), because they have used this application frequently, so they trust it. The remaining one user allows this application just because she chose the default option and clicked “OK” button. When I asked why she did that, she told me that she just wanted this prompt disappear as soon as possible, and the “ok” button did that.

You can find the result of what the respondents choice in Table. 1.

5.2 For access control

I did the following steps before I got the print screen of access control.

1. Restart the computer, and run the setup program of Rising Personal Firewall.
2. Restart the computer again, after the firewall was completely installed.
3. After the OS was completely loaded, I opened the interface of firewall and wanted to get a glance to it. Because the interface was in English, so I run the xdict.exe which is a translation application of Chinese-English to help me. When I was typing Chinese characters into the translation application, a security prompt is presented on the screen.

(In this part, I was focus on the access control of personal firewalls. So I ignored those security prompts which weren’t related to network access.)

In the technical group, all of the respondents know there is an application named "PinyinUp.exe" that wants to connect to the network with local port 4899 to port 80 of the destination address 61.135.132.20 from this prompt(Fig. 2). But only 5 respondents chose to allow for this application, 2 respondents want to get more information by clicking "view module list" and "view file" before they make choice, and 1 respondent chose the deny option. The respondents who understand what this prompt means but didn’t choose the allow option gave me the reason that they found a key word “Trojan” in this security prompt, so all of them thought this application must be related to a Trojan. Of course, nobody wants to allow a Trojan to access internet from their own computer.

In the non-technical group, all the users knew what this prompt means too. And 8 of them chose “allow” option, cause they knew this application is just an input program which were used daily. The other 2 respondents denied the application to access network. One was confused by the word “Trojan” mentioned above, the other one was scared by the red text. When I asked the users who allowed this application to connect to the Internet that “why such an input program wants an Internet connection?” Only 5 people gave the right answer - it needs to connect to its server for updating. The other 3 user made their explanation like this: “it is just an input program, if it wants that, let it does that. It’s not a big deal.”

The result of what the respondents choice is in Table. 2.
## 5.3 For attack warning

I did the following steps before I got the print screen of attack warning.

1. Restart the computer, and run the setup program of Kaspersky Anti-Virus Personal.

2. Restart the computer again, after the program was completely installed.

3. I left home for my dinner before the OS was completely loaded, then when I back home, I found there was a security prompt which was presented on the screen.

(In this part, I was focus on the attack warning of network. So I ignored those security prompts which weren’t related to attack warning.)

In the technical group, from this warning (Fig. 3), all the users knew that the computer was attacked from address 61.138.108.154, and the attack has been successfully repelled. 6 respondents thought that it is just an attack which usually happens, don’t need worry about that. Just click the OK button, and continue your work, it is not a big deal. The other 2 users felt nervous when they saw this warning, and one of them used Google to search this attack which described in this prompt, in order to find out what happened to the computer. The other one wants to run anti-virus software to scan computer to check whether this is something wrong with this computer.

In the non-technical group, all respondents knew that this computer was attacked. But only 5 users knew that this attack is not harmful to their computers, because it usually happens and was successfully repelled. 3 respondents were worried whether this attack has done something to the computer, and want to use anti-virus software to check that. 2 respondents didn’t care about this; they just click the OK or press Spacebar to ignore this warning.

The result of what the respondents choice is in Table. 3.

<table>
<thead>
<tr>
<th></th>
<th>Technical</th>
<th>Non-technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>More info</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Deny</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 2: Respondents result of access control

<table>
<thead>
<tr>
<th></th>
<th>Technical</th>
<th>Non-technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t worry</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>Feel nervous</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Don’t care</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Respondents result of attack warning

### 5.4 Overall

#### 5.4.1 The problem of usability of personal firewalls

- From the result above, we can find that most technical users can get useful information from security prompts. But not all of them could understand what the prompt given by the firewall means. For instance, in attack warning, the security prompt just tells you that an attack was repelled successfully, but some users were scared when they saw this warning. Sometimes the firewall told too much to the users, which users can not totally understand. For example, in process control, the prompt shows that the program "xdict.exe" wants to modify some other applications memory. So this warning information confused some users who didn’t know that’s the way the program works. There are also firewalls that give some cryptic warning, just like the screenshot in access control. The prompt just means that this application is using the local port 4899 which is often used by some Trojan software, you need to consider that whether this application is Trojan software or not. But it is really easy to make users believe that the application running on this port is a malicious application.

- For the non-technical users, only some of them know what the warning means. But most of then choose the option just dependent on whether they are familiar with the application or not. They don’t really care about the information given by these security prompts. Some users were sensitive to the color of the warning, they thought that the warning message given using red means forbidden, maybe orange or yellow means probable or possible, green means acceptable.

#### 5.4.2 Some suggestions for the problem

For the reasons mentioned above, some feedback was given by some warm-hearted respondents. I want to suggest improvements to the personal firewall usability with the following approach.

- For expert users:
1. Give them security prompts as often as possible, so they can find whether there are some potential risks of their computers.

2. Give them an option "always", so they can avoid to be disturbed frequently by the security prompts of firewalls. Once the expert was sure about this program is safety, the warning will not be presented anymore.

For normal users:

1. Give them appropriate security prompts but with more detailed information. For instance, when an application wants to modify another application’s memory. The warning should tell the user what kind of application is trying to modify an other’s memory and what kind of process has changed when you execute it. Therefore the users could choose the correct option when they find some application they aren’t familiar with.

2. Remember to teach users how to change their options, when they set some process to permanently allow or block, because sometimes after users clicks the button "always block", their program can’t access internet anymore.

For the beginning users:

1. Hide the security prompts which aren’t given by high risk processes[2]. To achieve this function, we can make a trust-list(Fig. 5) given by firewalls automatically. Some widely used applications such as MSN, firefox, emule and bittorrent client should be added to this list.

2. If a network attack was repelled successfully, it should not be presented, just log them into log files (Fig. 4). when users want to check their network security, they will find them in log files.

5.4.3 How to achieve these functions

How can we distinguish users that install a firewall belonging to a group? I think we can let users choose the group when they are installing their firewall. The setup program should have one page to let users choose their group. If they want more security prompts, choose the expert group; if they want to get more information about their network security, but worried about incorrect responses when the prompt present, choose the normal user group; if they just want to install a firewall to secure their computer, and don’t want be disturbed by it, choose the beginning group. If they want to change their group, they can find it in the options of the firewall.

5.4.4 Be security or usability?

Of course, what I suggested is not a security approach to solve the usability of personal firewall, because the usability and security are often two opposite directions in computer systems [7]. But anyway, once the users think the firewall disturbs them too frequently, they will uninstall the firewall to avoid be disturbed.

6 Conclusion

We have described a survey of three different categories of the usability of personal firewalls, and got many different responses from different respondents with different backgrounds. Just as some similar surveys, the results show that some security prompts given by some type of personal firewalls are not helpful to unskilled users. As a whole, users with a technical background can understand those prompts easier than non-technical users. But anyway, personal firewalls are for every computer end-user. So it should be designed for users with any skill level. Making the warning messages clearer and more detailed for experts, hiding some cryptic information of security prompts for beginning user may be a good approach to achieve usability for everyone.
References


