Setting Up a New Personal Computer

Project ID: 002

Hong Wei honwe861@student.liu.se

Xin Ye xinye971@student.liu.se

Supervisor: Viiveke Fåk

Abstract

This project is for the users from non security field. We interviewed common users from both the IT field and non IT field, suppliers from both the hardware and the software field. With the information we has got from the interviews, we analysis the risks and the threats to the personal computers. On the base of all these work, we provide users with detailed instructions to set up a secure system.

1. Introduction

1.1 The goal of this project

With the personal computer (PC) becomes a common tool like a mobile phone for an average people, the population of personal computer users is also increasing exponentially. According to the updated report from Internet Domain survey (www.nw.com), there are more than 162 million hosts in the DNS, and perhaps as many as 90% of the 162 million nodes connect to Internet are personal computers. PC's wide use also introduces a myriad of security problems, but most of the common PC users have no idea of PC security, their knowledge about PC security is very poor, even those people who work in IT companies always ignore many fatal errors or consciously or unconsciously make some serious mistakes in PC security.

The goal of this project is to provide a kind of guide book for the people who are not from the IT field. With the help of the project provided by our project, people can set up a secure computer which satisfies the security criteria so that they can avoid most of some common problems from security aspect.

1.2 The operation system

This project is for the Microsoft Windows systems. Since the subject is about how to set up a new personal computer. We mainly focus on the Window XP, since it is system the most new PCs will choose.

1.3 The content of this project

1.3.1 Interviews

We have interviewed a large number of people with or without IT background We also interviewed several PC suppliers or software suppliers in security field. From talking with these interviewees, we got much information about how people gain the security knowledge and how much do people know of the security issues as well as their understanding about the responsibility for the information leak cases.

1.3.2 Risk Analysis

The default setting of the Windows XP is far from secure. We will discuss these risks of the system in our daily life.

1.3.3 The threats.

We will discuss the most popular threats nowadays, especially the threats from the net. In the project we will provide some brief introductions of how they work such as Trojan horses or

backdoors.

1.3.4 Set up a secure system

The project will set up the secure system in three aspects:

a) The physical environment and human factor

b) The system backup and recovery

c) The network security.

According to the risks and the threats, the project will provide the users with detailed counter measures.

2. Interviews

2.1 Security Events and Personal Views.

During the summer of 2003, the worm Blaster infected millions of computers in a short time and for a moment all over the world, people helplessly stared at the pop-up window showing the message of RPC error and waited for the system to automatically reboot again and again. During the March of 2004, Mydoom, Netsky and Beagle were spreading throughout the world via the mail attachments, attacking the website of SCO and Microsoft. To people's surprise, the creators of the worms reviled each other in their worm product. Because the source code is published, people are still busy with the variants of these worms now.

From the features of the worms, worms are spread in two ways, the mail attachment and the leaks of the system. Patching the leaks in time still remains as a problem. The crackers download and analyze the patch package. For all the times, they can create worms or crack tools according the corresponding leaks before most of the users have patched their system. As to the purpose, the hackers tend to not only to make great damages for showing off, but to express their own views of some events, such as the worm Mydoom, attacking the SCO website since the creator is a Linux supporter.

However, in the view of a student from security field, most of these security events can be prevented. It is very important to timely patch the leaks and update the security software such as antivirus software. Besides keeping the firewalls on all the time, reconfiguration of some default settings are also necessary, which can protect the system from unknown attacks in advance.

2.2 Interviews.

Before we began to write this report, I interviewed many people, these people are all from different working field. I divided these people into four group according to their experience related to computer security, separately describe their understanding to PC security.

Interviewees from non IT field:

Almost all of interviewees from non IT field response that they have no idea of PC security, they also never care about such issues, perhaps the only knowledge about PC security is how to prevent computer virus, because their PC frequently infect different virus especially when they surf in the Internet. In this group, PCs are mainly used to browse Website, send and receive Email, chat with friends and download music and movies, PC security is not closely related to their

everyday PC using, so security is not a big problem in this group.

Interviewees from IT field.

In this group, I totally interviewed three persons. One is from a telecommunication company. He is mainly responsible for telecomm bill system's developing. The second is from a bank of China, he is mainly responsible for financial data management. The third is from a Telecomm equipment manufactory company, he is the network administrator of his company. The main purpose for them to use PC is for work. From talking their ideas of PC security with them, I find that they all have perfect computer security knowledge and all of their companies have mature computer security policy. In company, they also strictly obey their companies' regulations of computer security. But when I asked them to describe some scenarios of their using PC, many serious problems exposed when they work in their homes. When I pointed out these errors, they quickly realized what a serious mistake they had made, but they all said if I had not mentioned the errors, they would continue ignoring such problems and never thought of this point.

Interviewees from PC hardware suppliers

I interviewed two persons from PC suppliers or vendors. One is a technical engineer; another is a manager of a department. They told me when a customer purchases a PC from their company, they assigns an engineer to install a Windows XP OS with all necessary drivers and an updated anti-virus software. They also configure a secure environment for the customer according to the recommendation of how to set up a secure PC from Microsoft with an user manual , in which it introduces some fundamental knowledge about how to properly use and maintain a PC. When the computer does not work within one year after the user purchased this PC, If the malfunction is caused by hardware which is because of some hard components' poor quality, they will change a new one for free, if it is caused by software, or users incorrectly operations, or virus, they think it is not their responsibility. When I asked them that if a customer leaks the important information of his company when he uses the PC purchased from your company to connect his company's server, or someone steals the sensitive data which is saved in his PC's hard-disk, who should be responsible for this loss? They told me that it is out of their responsibility's scope, if you think it is PC suppliers' responsibility, it will be very absurd.

Interviewees from PC software vendors in security field

People in this group are all from a security company in china, which mainly produces anti-virus software and firewalls. On the forum of customer service, we expressed our intention to purchase security software and asked for some advices with comparison with other security software. We received the reply with highly recommendation for Rising Antivirus 2004 together with his own network firewall. They stated that the most popular threats nowadays are not only the worms but also the Trojan horses, backdoors and spy wares, especially the key loggers, which will steal your passwords and cause the serious information leak. Since some malicious software is open-sourced, it is much easier for people to design private unpublished programs which can avoid the detection of the security software only depending on its virus/Trojan horse definitions.

In general, most of the common PC users are absent of fundamental knowledge and they also do not care much about this issue. Some IT experts have elementary PC security knowledge, but they often ignore some critical errors in PC security or sometime they unintentionally make some fatal mistakes without consciousness. Considering current situation, at the last part of this report, it provides PC configuration guidance for common users to tell them how to set up a secure PC.

3. Risk Analysis

3.1 Assets of a PC include:

Hardware: processors, boards, keyboards, monitors, CD or DVD drives, hard disk, mice, communication controllers and so on. Generally, desktop computer is cheaper than corresponding portable computer, the price of a desktop computer ranges from 800 USD to 2000 USD and a portable computer is about 2000 USD on average. So, if you lose a PC, you will at least lose 2000 USD.

Software: purchased programs, wealthy utility software, operating system, and system software. Some utility and system software are wealthy of several thousands to hundred thousand USD.

Data: the document saved on a PC hard disk. The wealthy of this kind of asset is difficult to estimate, but leaking this sensitive information to some people will cause unexpected loss.

3.2 Vulnerabilities of a PC:

There are many factors which will permit threats happening, for example, put a PC in a room without locking the door or closing the windows, temporally leave your PC without locking the screen, have not a reasonable access control policy in your PC, do not install an updated anti-virus software or firewall for PC and do not securely configure your PC. There are also some factors that will increase the possibility of a threat happening, like living in an area with many people having low characters, PC owners knowing much sensitive information, frequently sending emails containing important information. So, PC owners should consider all different factors and design a reasonable security policy for your PC.

4 Threats

About threats of a PC, we will discuss them from four aspects:

4.1 Threats from PC hardware

The major hardware security problems are about theft and hardware damaging. A desktop PC, especially the portable PC is relatively light, it is easy for a theft to take it away. Some improper operations to PC are the main reasons that cause the computer hardware to be damaged, like spilled of a cup of coffee or tea to the computer, mice have chewed the cable and ash from cigarette smoke has harmed the disk drivers, improperly add or remove some hardware components to or from a PC, put a PC in a very humid, high radiation or full of dust environment.

Static electricity on the components inside the computer is unavoidable, if you put a PC in a room without the static electricity proof facilities, the PC will age fast. Certainly some natural disasters will cause your PC to be totally damaged, like lighting, fire.

4.2 Threats from PC software

About PC threats from PC software, we divide them into two group and separately discuss these threats, one is the threats to operation system and the application software installed on this operating system, another is the threats to sensitive information which is saved on the hard-disk. About the operating system and application software, there are three aspects about security threats, first is misuse of the system software and application software, like operate them without according to the correct operation procedure, delete some parts of software because of carelessness. Second is virus, worms or other malicious code. Once your PC infects some kind of computer virus, some wealthy system software and application software will be damaged. The last

is attacks, if someone penetrates you PC via internet and your computer has not proper access control policy, the attacker will use administrator privilege to delete or modify your system and application software, Or if you temporally leave your PC without locking the PC screen, someone can use this chance to enter your PC and damage your wealthy software. About sensitive information saved in your PC hard disk, security threats can be caused by many factors, like hard disk's damaging, someone access your PC to copy, delete or modify the document without encrypted in the hard-disk, computer virus or malicious code infect your computer and delete or modify the sensitive document in your hard disk. Certainly, it also can be deleted or modifies because of your carelessness.

4.3 Threats from the Internet

The most popular threats nowadays are from the net, such as worms, Trojan horses, backdoors, key loggers, spy or AD wares and etc. Spy wares are used for collecting system information or user's surfing habits without any permission; AD ware is to display some advertisements usually by popping up some windows or extra browser pages.

Among these threats, the most dangerous one is not the worm, most of which only congests the network but the Trojan horses. A Trojan horse can not only monitor other's screen, upload malicious software but also cover the function of key logger, stealing sensitive information such as password, credit card number.

With the development of the personal firewall and antivirus software, the creators of Trojan horses are also searching for the more effective and undetectable way to make their Trojan horses survive. The firewall policy that every program has to ask for the permission before they can connect to the net might not be enough nowadays, because some of Trojan horses only appears as one single DLL (dynamical link library) file and hijacks the permitted process to get onto the net, for example the SvchostDll.dll and the BITs.dll.

There are no universal definitions for the malicious software. Some cover the functions of others, for example the Trojan horse, which usually contains the functions of the backdoor and the key logger. So when we refer to the Trojan horse here, it also includes the backdoors and the key loggers.

4.4 Abuse of a PC

When a user talks about PC security, most important thing he cares about is how to prevent his PC being damaged by others. But here I must point out that to prevent your PC harming others is also important. Abusively using a PC means that someone uses his PC intentionally or unintentionally to do some illegal thing, like using a PC to attack others, accessing to or modifying others' private document without the permission of owners, intercepting others Email, transferring virus or other malicious code to infect people's PC or illegally distribute copyrighted digital document, software, music or movie.

5. Set up a Secure System

In this section, we provide readers with detailed methods to set up a secure system in the following aspects. All the instructions are based on the premise that users know the basic operations of the systems, for example, users know how to use the mouse and the keyboard; users know how to surf on the net, how to copy a file to a specific directory and etc.

We are trying to cover most of the problems users may encounter with their computers.

However, this does not stand for that users must follow all the instructions listed in our project. It is all right that users leave some advanced parts aside if they do not understand, such as the manual setting and the manual checking.

5.1 physical environment and human factor

5.1.1 Physical protections

There are some simple rules user may obey which will prevent common physical damage in advance. The rules seem to be simple but sometimes they are just the very reasons for the system failure.

1) Keep the computer environment clean and dry. It is better to cover the machine box with a cloth cover when the system is off.

2) When drinking in front of the computer, please put the drink as far as possible. Sometimes the drink will be turned over by accident no matter how careful you are and it will probably cause the short circuit of key board.

3) Put the system unit in a steady place. When the hard disk is working, the system unit, which is shaking, causes the bad sectors and the data lost.

5.1.2 Password Management

Some of the information leaks do not result from the system holes or the theft by the malicious software, but the password itself, which means that sometimes the password is not strong enough that it is very easy to be cracked by the brute force or easy to be remembered by someone peeking aside. Using very complicated password is also not a good choice; because it is rather hard for people to remember. However, there are some practical rules which users may follow.

1) Use Relatively Strong Passwords.

A strong password should have no less than 10 characters/digits and is consisted of both the characters and digits. It will be better if you add some other symbols in the password, but it will make the password hard to remember and slow down the input speed. However, this rule is only applied to the important accounts.

It is easy for users to remember the password by using the birthday or the home phone number, but please try not to use your own ones. As the concern of the character part, please try not to use the whole single word which might be guessed out by the hacker dictionary. You may combine two simple words into one word which is easy to remember while will not appear in the word list of the hack dictionary.

2) Classify your passwords

Nowadays, one person has many accounts with all kinds of passwords required. It might cause some security problems if one is using the same password for all his accounts. So the proposal we put forward for the password management is: Classify your passwords.

For the unimportant ones, such as some free online game accounts, you could use some simple passwords such as pure characters or numbers. Sometimes these passwords may need to be shared with others, so they should not have any similarities with the important ones. It is all right to apply the same password to different game accounts for the easy memory.

For your important accounts, such as the mail account which you have to use for your study or

work everyday, you'd better use the strong passwords. Sometimes, you can use the same password for the different mail accounts in the same security level for the easy memory.

Someone may need to backup very personal information or the passwords in a personal network disk or mail box which is unknown to anyone else. Then this password should be ranked as the top class which means that it is not only strong enough but also not to be similar with any other passwords.

Today, many software offer password saving such as browsers and online game clients. As to important accounts, we suggest not saving the password while to some unimportant ones, saving the password is convenient for the daily use. As to the web browser, please see the section 5.3.1.

5.2 The System Backup & Recovery

As we mentioned in the section of the Threats, Windows XP is a milestone of the Windows systems. It is better than any former Windows systems. However, the system still might collapse because of hardware failures or the unknown software bugs. In order to set up a secure system with no data lost, we provide some guidelines as follows.

5.2.1 System Backup

1) Backup the whole partition. After installed the system and all the necessary software, it is a good way to clone the whole active partition. An active partition is the partition where the operation system is installed, which contains two folders of Documents and Settings and WINDDOWS. If there are some serious system errors or the malicious software which you do not know how to do deal with, the easiest way is just to recover the whole partition and everything appears to be as what you have previously installed. Several companies provide the partition clone software, such as Norton Ghost from the Symantec.

2) Backup the registry the registry is the database of all the settings for the Windows and the installed applications. Recovery of the whole active partition will also replace the registry and some software installed in other partitions might not work properly after that. So registry backup is also necessary and it can solve the many problems without the whole partition recovered.

Choose Start > Run> input "regedit" and you will see the registry. Click the "file"-"export", you can back up the registry. It is recommended storing the registry backup file to other partitions. As to the recovery of the registry, just click the "file"-"import" of registry window and then reboot the system.

3) Backup the important data. The window system itself provides the function of the data backup. However, what we care of is where to store the backup files. To some important data, we recommend to backup the data to the disk space out of the system, such as the floppy or the network disk in the case of the hardware failure.

There is lots of system auxiliary software nowadays which provides this function for the registry, the drivers and the important data, such as the Super Rabbit.

5.2.2 System Automatic Recovery

The XP contains the powerful function of partition monitor which can recover the system when serious failure occurs. It is recommended to keep all the partitions' monitor on but as the time goes by, the storage of all the recovery points will consume lots of disk space especially the

active partition. Somehow, the tool provided by the system for deleting the useless recover points does not work in many cases, so we provide the solutions as follows:

1) Reboot the system. (To make sure that there is no error occurred during the last working period.)

2) Choose "My Computer", right click and choose "properties", choose the option of "System Recovery", choose "turn off the system recoveries on all the drivers" and then click "ok". The system will delete all the recover points and release the disk spaces.

3) Turn on the system monitor as the second step.

4) Reboot the system.

5.3 The Network Security

Nowadays most of the threats to the system security are from the net. Here we list out the counter measures to the viruses and invasions. There are some basic rules the users should follow which are required all the time.

1) Install the antivirus software; Update the virus definitions in time; Keep the real time monitor on whenever the system is running.

2) Install a firewall; Update the firewall in time; Set the firewall rules to the highest security level; Keep the firewall on whenever the system has connected to the net.

3) Patch the system holes as soon as possible.

5.3.1 Web Surfing

Since the Internet Explorer is preinstalled with the operation system, IE is the first choice for most of the common user. However the default setting will bring us many security problems.

1) User account and password saving.

IE provides the function to save user's account and the password so that it can automatically fill the password in according to the account. We suggest turning off this function if it is on. In the IE window, you can choose Tools > Internet Options > Content > Auto Complete to turn off the function.

2) The Script, Java Applet and Active X.

These technologies are designed for the web surfing, providing more powerful functions and vivid views of the web browsers. There may contain malicious codes on the web pages. Though most of the antivirus software has a real-time monitor to the web browser, it still can not guarantee for obstructing all the malicious codes.

In the IE window, users can choose Tools > Internet Options > security > Custom Settings to forbid these components. However, some settings will obstruct the page displaying correctly. To some trusted website, it seems a bit meaningless. Besides, users are reluctant to go so deeply to change a setting according to different websites. So what we recommend is to use the web browsers created by the third party based on the core of the IE. It not only guarantees to display web pages correctly, but also more powerful functions. For example, the MyIE2, on the toolbar, user can directly choose what he wants the web browser to load for every tab window, for example, only Java applet is allowed and Java script and Active X are blocked.

3) The IE Recovery

Sometimes the IE setting will be revised maliciously. For example the home page is fixed to

a web site and users can not change it in the Internet Options window. We can recover the registry to fix these problems and also there is lots of free software designed for the IE recovery on the net and even the antivirus software provides the extra tools for it.

5.3.2 Virus Issue

Virus is a computer program that replicates by attaching itself to another object without the owner's permission or conscious. Regardless of the different definitions for the virus and the worms, we regard worms as one part of virus category and we define the worm as "a computer program that replicates independently by sending itself to other system."

Antivirus software is most important countermeasure to the virus. However, the virus definition is always updated after the new virus appears while the detection of the unknown virus still remains as a problem which has not been perfectly solved. So there are some more rules for the virus issue beyond the basic rules.

1) Avoid downloading files from distrusted websites

2) Do not open the mail attachment from the people unknown or from the people you know but with no specific meanings of the mail content which might be created by the worm automatically.

3) Scan the files and attachments which you do not trust while you have to open.

5.3.3 Defend Against the Intrusion

Windows XP provides much more powerful network function than Win98, which brings us much convenience while it also raises the risks because of the system's default settings, for example the IPC (Internet Process Connection).

Using a personal firewall and setting to the highest security level (the basic rule 2) are the best ways to defend against the intrusion, which will hide most of important ports invisible to the scanners. There are many excellent personal firewalls available such as ZoneAlarm, Norton Internet Security and etc. To get more secure features, we also suggest implementing the manual operations as follows.

5.3.3.1 Reconfigure the system

1) Turn off the guest account

As to the personal computer, people will set an administrator account for themselves and left guest account unused. But sometimes, the guest account will be used maliciously by the crackers. So we suggest turning off the guest account if it is no longer in use. The fewer services sometimes stand for the higher security level.

Choose Start > Settings > Control Panel and double click the User Accounts and choose Change an Account > Guest Account > Turn off the guest account

2) Turn off the unneeded services.

Some of the default services will never be used for some users. In order to maintain the minimum number of the ports, we suggest turning off some services.

Choose Start > Setting > Control Panel and double click Manage Tools > Services. You can see all the services listed in the window. You can double click a service to see the property window in which you configure the setting. There are some services listed as follows which users

may turn off.

"Click Board Server" à set to "Manual". This server allows the users to visit your directory from the net.

"Messenger" à set to "Manual". This server will cause serious security problems.

"Network DDE & Network DDE DSDM" à set to "Manual". This service is for the office share.

"Printer Spooler" à set to "Manual" if you do not have a printer.

"Uninterruptible Power Supply" à set to "Manual" if you do not have a UPS.

"Remote Desktop Help Session Manager" à Manual/Disable if you do not need any online help.

"Remote Registry" à set to "Manual"/"Disable" This service allows the people to change the registry remotely.

3) Turn off the net share

The Windows XP provides the function of remote login. However it is mostly used by crackers not the common users. For most of people, they will never use such kind of function. So it is better to turn off the net share.

Choose Start > Run > input "regedit" and then in the registry table, find the branch [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]. Set the "AutoShareWks" to 00000000. This will take effect after the system reboot. You may choose Start > Run > input "cmd" > input "net share" to check the default share.

5.3.3.2 Manual Checking

As we have introduced in the section 2.3, simple program control seems not enough. So we need advanced control function from the firewall, such as the component control of the ZoneAlarm which prevents Trojan horses from using some programs maliciously. However, it still can not guarantee obstructing all the Trojan horses or backdoors from connecting to the net. Thus we sometimes have to manually check for the unknown malicious software.

1) Choose Start > Run > input "cmd" > input "netstat -a" to list out all the opened ports and addresses on both the TCP and UDP protocols. Or you can download the Fport.exe for free and copy it to the path C:\WINDOWS\system32 so that you can use the fport command in the dos shell. This command not only shows the addresses and the ports but also the programs which have created the ports.

2) Choose Start > Run > input "msconfig" and in the startup window, you will see what will run as the system boots up. You can also choose to disable a program in the boot-up list.

3) Check the registry.

Choose Start > Run > input "regedit" to open the registry table. Then find and check the key [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] and [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]. For large part of the Trojan horses, worms or backdoors will add new items to these two branches.

6. Summary & Outlook

What we have to point out is that there is no absolutely secure system in the world. As to the personal computer and the software environment, it is quite certain that not all the discovered

system holes have been published and some malicious codes still can avoid the detection of the security software.

However, what we have listed out in this project should be sufficient for common users. It can be guaranteed that the system will be secure for a long period of time under these instructions.