Protecting a computer 13718

Technology, Internet

Protecting A Computer

About two hundred years before, the word " computer" started to appear in the dictionary. Some people even didn't know what is a computer. However, most of the people today not just knowing what is a computer, but understand how to use a computer.

Therefore, computer become more and more popular and important to our society. We can use computer everywhere and they are very useful and helpful to our life. The speed and accuracy of computer made people felt confident and reliable. Therefore, many important information or data are saved in the computer. Such as your diary, the financial situation of a oil company or some secret intelligence of the military department. A lot of important information can be found in the memory of computer. So, people may ask a question: Can we make sure that the information in the computer is safe and nobody can steal it

from the memory of the computer?

Physical hazard is one of the causes of destroying the data in the computer.

For example, send a flood of coffee toward a personal computer. The hard disk

of the computer could be endangered by the flood of coffee. Besides, human

caretaker of computer system can cause as much as harm as any physical hazard.

For example, a cashier in a bank can transfer some money from one of his

customer's account to his own account. Nonetheless, the most dangerous thief

are not those who work with computer every day, but youthful amateurs who

experiment at night --- the hackers.

The term " hacker " may have originated at M. I. T. as students' jargon for

classmates who labored nights in the computer lab. In the beginning, hackers are

not so dangerous at all. They just stole computer time from the university.

However, in the early 1980s, hackers became a group of criminals who steal

information from other peoples' computer.

For preventing the hackers and other criminals, people need to set up a good security system to protect the data in the computer. The most important thing is that we cannot allow those hackers and criminals entering our computers. It means that we need to design a lock to lock up all our data or using identification to verify the identity of someone seeking access to our computers.

The most common method to lock up the data is using a password system. Passwords are a multi-user computer system's usual first line of defense against hackers. We can use a combination of alphabetic and number characters to form our own password. The longer the password, the more possibilities a hacker's password-guessing program must work through. However it is difficult to remember a very long passwords. So people will try to write the password down and it may immediately make it a security risk. Furthermore, a high speed password-guessing

program can find out a password easily. Therefore, it is not enough for a computer that just have a password system to protect its data and memory. Besides password system, a computer company may consider about the security of its information centre. In the past, people used locks and keys to limit access to secure areas. However, keys can be stolen or copies easily. Therefore, card-key are designed to prevent the situation above. Three types of card-keys are commonly used by banks, computer centers and government departments. Each of this card-keys can employ an identifying number or password that is encoded in the card itself, and all are produced by techniques beyond the reach of the average computer criminals. One of the three card-key is called watermark magnetic. It was inspired by the watermarks on paper currency. The card's magnetic strip have a 12-digit number code and it cannot be copied. It can store about two thousand bits in the magnetic strip. The other two cards have the

capability of storing thousands of times of data in the magnetic strip. They are

optical memory cards (OMCs) and Smart cards. Both of them are always used in the

security system of computers.

However, it is not enough for just using password system and card-keys to

protect the memory in the computer. A computer system also need to have a

restricting program to verify the identity of the users. Generally, identity can

be established by something a person knows, such as a password or something a

person has, such as a card-key. However, people are often forget their

passwords or lose their keys. A third method must be used. It is using something

a person has --- physical trait of a human being.

We can use a new technology called biometric device to identify the person

who wants to use your computer. Biometric devices are instrument that perform

mathematical analyses of biological characteristics. For example, voices,

fingerprint and geometry of the hand can be used for identification. Nowadays,

many computer centers, bank vaults, military installations and other sensitive

areas have considered to use biometric security system. It is because the rate

of mistaken acceptance of outsiders and the rejection of authorized insiders is

extremely low.

Individuality of vocal signature is one kind of biometric security system.

The main point of this system is voice verification. The voice verifier

described here is a developmental system at American Telephone and Telegraph.

Only one thing that people need to do is repeating a particular phrase several

times. The computer would sample, digitize and store what you said. After that,

it will built up a voice signature and make allowances for an individual's

characteristic variations. The theory of voice verification is very simple. It

is using the characteristics of a voice: its acoustic strength. To isolate personal characteristics within these fluctuations, the computer breaks the sound into its component frequencies and analyzes how they are distributed. If someone wants to steal some information from your computer, the person needs to have a same voice as you and it is impossible.

Besides using voices for identification, we can use fingerprint to verify a person's identity because no two fingerprints are exactly alike. In a fingerprint verification system, the user places one finger on a glass plate; light flashes inside the machine, reflects off the fingerprint and is picked up by an optical scanner. The scanner transmits the information to the computer for analysis. After that, security experts can verify the identity of that person by those information.

Finally, the last biometric security system is the geometry of the hand. In that system, the computer system uses a sophisticated scanning device to record

the measurements of each person's hand. With an overhead light shining down on

the hand, a sensor underneath the plate scans the fingers through the glass slots, recording light intensity from the fingertips to the webbing where the fingers join the palm. After passing the investigation of the computer, people can use the computer or retrieve data from the computer.

Although a lot of security system have invented in our world, they are useless if people always think that stealing information is not a serious crime.

Therefore, people need to pay more attention on computer crime and fight against

those hackers, instead of using a lot of computer security systems to protect the computer.

Why do we need to protect our computers ?

It is a question which people always ask in 18th century. However, every person knows the importance and useful of a computer security system.

In 19th century, computer become more and more important and helpful. You

can input a large amount of information or data in a small memory chip of a personal computer. The hard disk of a computer system is liked a bank. It contained a lot of costly material. Such as your diary, the financial situation of a trading company or some secret military information. Therefore, it just like hire some security guards to protect the bank. A computer security system

can use to prevent the outflow of the information in the national defense industry or the personal diary in your computer.

Nevertheless, there is the price that one might expect to pay for the tool of security: equipment ranging from locks on doors to computerized gate-keepers

that stand watch against hackers, special software that prevents employees to

steal the data from the company's computer. The bill can range from hundreds of

dollars to many millions, depending on the degree of assurance sought.

Although it needs to spend a lot of money to create a computer security system, it worth to make it. It is because the data in a computer can be easily

erased or destroyed by a lot of kind of hazards. For example, a power supply problem or a fire accident can destroy all the data in a computer company. In 1987, a computer centre inside the Pentagon, the US military's sprawling head quarters near Washington, DC., a 300-Watt light bulb once was left burning inside a vault where computer tapes were stored. After a time, the bulb had generated so much heat that the ceiling began to smelt. When the door was opened, air rushing into the room brought the fire to life. Before the flames could be extinguished, they had spread consume three computer systems worth a total of $6. 3 million.

Besides those accidental hazards, human is a great cause of the outflows of data from the computer. There have two kind of people can go in the security system and steal the data from it. One is those trusted employee who is designed to let in the computer system, such as programmers, operators or managers.

Another kind is those youth amateurs who experiment at night ----the hackers.

Let's talk about those trusted workers. They are the groups who can easily become a criminal directly or indirectly. They may steal the information in the system and sell it to someone else for a great profit. In another hand, they may be bribed by someone who want to steal the data. It is because it may cost a criminal far less in time and money to bride a disloyal employee to crack the security system.

Beside those disloyal workers, hacker is also very dangerous. The term " hacker" is originated at M. I. T. as students' jargon for classmates who doing computer lab in the night. In the beginning, hackers are not so dangerous at all.

They just stole some hints for the test in the university. However, in early 1980s, hacker became a group of criminal who steal information from other commercial companies or government departments.

What can we use to protect the computer ?

We have talked about the reasons of the use of computer security system. But

what kind of tools can we use to protect the computer. The most common one is a

password system. Password are a multi-user computer system's which usual used

for the first line of defense against intrusion. A password may be any

combination of alphabetic and numeric characters, to maximum lengths set by the

e particular system. Most system can accommodate passwords up to 40 characters.

However, a long passwords can be easily forget. So, people may write it down and

it immediately make a security risk. Some people may use their first name or a

significant word. With a dictionary of 2000 common names, for instance, a

experienced hacker can crack it within ten minutes.

Besides the password system, card-keys are also commonly used. Each kind of

card-keys can employ an identifying number or password that is encoded in the

card itself, and all are produced by techniques beyond the reach of the average

computer criminal. Three types of card usually used. They are magnetic watermark,

Optical memory card and Smart card.

However, both of the tools can be easily knew or stole by other people.

Password are often forgotten by the users and card-key can be copied or stolen.

Therefore, we need to have a higher level of computer security system. Biometric

device is the one which have a safer protection for the computer. It can reduce

the probability of the mistaken acceptance of outsider to extremely low.

Biometric devices are instrument that perform mathematical analyses of

biological characteristics. However, the time required to pass the system should

not be too long. Also, it should not give inconvenience to the user. For example,

the system require people to remove their shoes and socks for footprint

verification.

Individuality of vocal signature is one kind of biometry security system.

They are still in the experimental stage, reliable computer systems for voice

verification would be useful for both on-site and remote user identification.

The voice verifier described here is invented by the developmental system at

American Telephone and Telegraph. Enrollment would require the user to repeat a

particular phrase several times. The computer would sample, digitize and store

each reading of the phrase and then, from the data, build a voice signature that

would make allowances for an individual's characteristic variations.

Another biometric device is a device which can measuring the act of writing.

The device included a biometric pen and a sensor pad. The pen can converts a

signature into a set of three electrical signals by one pressure sensor and two

acceleration sensors. The pressure sensor can change in the writer's downward

pressure on the pen point. The two acceleration sensor can measure the vertical

and horizontal movement.

The third device which we want to talk about is a device which can scan the

pattern in the eyes. This device is using an infrared beam which can scan the

retina in a circular path. The detector in the eyepiece of the device can

measure the intensity of the light as it is reflected from different points.

Because blood vessels do not absorb and reflect the same quantities of infrared

as the surrounding tissue, the eyepiece sensor records the vessels as an

intricate dark pattern against a lighter background. The device samples light

intensity at 320 points around the path of the scan , producing a digital

profile of the vessel pattern. The enrollment can take as little as 30 seconds

and verification can be even faster. Therefore, user can pass the system quickly

and the system can reject those hackers accurately.

The last device that we want to discuss is a device which can map the intricacies of a fingerprint. In the verification system, the user places one finger on a glass plate; light flashes inside the machine , reflect off the fingerprint and is picked up by an optical scanner. The scanner transmits the information to the computer for analysis.

Although scientist have invented many kind of computer security systems, no combination of technologies promises unbreakable security. Experts in the field agree that someone with sufficient resources can crack almost any computer defense. Therefore, the most important thing is the conduct of the people. If everyone in this world have a good conduct and behavior, there is no need to use any complicated security system to protect the computer.