Computer

Technology, Computer

Computer security arouses the ethics and risk analysis, and is concerned with topics such as computer crime, the prevention, detection, remediation of attacks, identity and anonymity in cyberspace. In this paper, I want discuss the main problems of computer security and its serious threats. Computer security, also known as cyber security or IT security, is information security as applied to computing devices such as computers and smartness, as well as computer networks such as private and public networks, including the Internet.

Computer security, which is the composition of hardware, software network system and the safety of delivering information through network, has been an essential issue. Computer security has not only technical problems but also management problems, and at the same time, both of them affect each other. The major technical areas of computer security are usually represented by the initials CIA: confidentiality, integrity, and authentication or availability. Confidentiality means information cannot be access by some parties unauthorized.

It is a kind of secrecy or privacy, which reaches of confidentiality range from the embarrassing to the disastrous. Integrity means that information is protected in order to against unauthorized changes that are not detectable to authorized users. Authentication means that users are who they claim to be. Availability means that resources are accessible by authorized parties. The major management area of computer security is that the defects and deficiencies in the operation and management system restricts the computer security.

The information security policies, programs and management tools, are all effect the operation and management system. The threats that computer security faced are multifaceted, including both threats from human error and malicious attacks artificially. It is a very serious problem that many incidents of hacking compromise the databases and other resources on some important system such as bank and government on purpose. Just like Leon Penetrate said, the USA should consider any crippling attack on the Internet as a declaration of war on it. In fact, it has been a common question to the whole international community.

Over the past ears, there is a kind of computer virus Stunned that wiped out nearly 60 percent of Iran's computer network. It illustrates that nation-states are easy to be effected by crippling cyber actions from other nation-states or individuals. And even the international community can not find the exact source and purpose of the virus, but clearly, because of this attack, they has realized their big vulnerability. First of all, in order to reduce the risk of attack from a similar virus, the policy makers must recognize that current security measures and systems are not powerful enough to reverent the attack with this type.

In addition, people should attempt to discern the source of a cyber attack from different ways. Even though it may not be efficient enough to prevent Stunned right now, they also can build a well-architecture and self-reinforcing manner to greatly improve an organization's ability to prevent, detect, and respond to these types of cyber incidents. For example, government can encourage experimentation with promising technologies

and practices. Why are almost all the systems in service today extremely vulnerable to attack?

The main reason is that security is expensive to set up and a nuisance to run, so people Judge from experience how little of it they can get away with. It seems fair to say that in an absolute sense, the security of the hundreds of millions of deployed computer systems is terrible. Moreover, computer security is not Just about computer systems. It is only the weakest link, and the links include the people and the physical security of the system. For computer security, we should not reliance on prevention rather than detection and punishment.