Computer Security

Today, computer security is a very wide problem in the computer world. And I would like to consider this theme now.

In general a computer attack is any attempt to perform some illegal actions with information. Usually professionals distinguish three aspects that need protection. It is privacy, integrity and accessibility of information resources.

Creating a secure system is a very hard and expensive task, and to achieve it developers should follow special rules. Creating a secure system is also a very specific problem, in comparison with others tasks that are solved in real life, because to solve this problem a developer must understand how the criminals attack modern systems.

That is why considering computer security definitely requires discussion not only computer security approaches, but at first we must consider themes like computer attacks by itself, vulnerabilities and malware.

There are a lot of classifications of computer attacks. An attack can be active or passive depending on influence upon the system, outside or inside depending on its source. The attack can also be classified by vulnerabilities used in it. A typical approach in producing an attack consists of three steps: firstly, we should discover information about the target, secondly we should find out its vulnerabilities, and finally, we should perform the attack.

Know I would like to enumerate some examples of computer attacks. First is vulnerability scanner, it searches the internet IP addresses and computer ports to find out non-blocked systems of applications. Second is password cracking, this attack tries to guess password for different systems. The next is packet sniffer, which is used to capture packets in the internet and search them for passwords. Another attack is called fishing, it is based on different tricks, and as the result user gives his password voluntarily. Next we come to well known viruses, worms, and Trojans. Finally exists very specific attack called key logger. It is used to record different user actions.

All attacks use some vulnerabilities in systems. A vulnerability is a weakness which allows an attacker to reduce a system's information assurance. The main causes of vulnerabilities are complexity, familiarity, connectivity, password management flaw, internet website browsing, software bugs, unchecked user input and of course not learning from past mistakes.

After vulnerability was found out, somebody must make a disclosure. Full disclosure is done when all the details of vulnerability is publicized. Disclosure per se is not a very fast process, because information must be freely available to the public and been proved by trusted source. Unfortunately another problem appears. After a disclosure made it will take some time before developers will close it.

Let’s move on now to malware. Malware is a harmful software, that can combine different attacks, and use different vulnerabilities. Malware became so widespread, that modern world started to create special software against it.

Now, when we have got acquainted with threats, we may look up different computer security approaches.

First security approach is security by design. If you want to create protected system, you must interpret the security as one of the main feature. To correspond to this approach the developers must create system relying on special rules. These rules are the principle of least privilege, automated theorem proving, code reviews and unit testing, defense in depth, safety engineering and full disclosure.

Another approach is called security architecture. Its main idea lies in looking at the system architecture, and position security defense in correct places.

Next we come to very effective approach called secure operating system. It is based on a special microprocessor hardware and special operating system kernel.

The next approach is secure coding. Many programming languages provide flexibility, but not all features in these languages are secure. Programmer must carefully choose which language capabilities he may use. Unfortunately, there is no theoretical model of secure coding practices.

One more very useful approach is capabilities and access control list. This list describes subjects, objects and actions that one can permit under another.

Finally, exists hardware mechanisms that can perform some physical actions in case of attack, but they are not used extensively.

Computer security has special segment of industry called network security. Network security requires different efforts to protect computer systems. These efforts require special software, for example anti-viruses or internet security firewalls. Another problem is that users are now more involved in process of providing security.

Like computer security, network security has some approaches too. Firstly, you must authenticate at least only with password, but the more authentication factors you use the better. Secondly, use firewall. Thirdly, enable the encryption. And finally, you can create honeypots. Honeypot is a special computer system designed to draw out hackers attention and immediately inform in case of attack.

The network security must be different depending on what system you are going to protect. Examples of systems, that can be protected are homes, small, medium and large businesses, school, large government. Every system requires different security measures.

At the end, I would like to enumerate basic types of hackers. White hats are hackers, who break security of systems not for malicious reasons. Black hats is a typical hackers. Elite hackers is the most skilled representatives. Blue hat is someone outside computer security consulting other companies. Also exist other types of hackers, but they are usually not very skilled, and do not represent any serious danger.

In conclusion, I would like to point out that computer security has different approaches, but every approach demand from developer or even user, very good knowledge about computer attacks. Because computer security is a defensive technique.

Thank you for your attention.