Active Attacks on Computer Systems

Chris Collins

5th November 2006
It is this paper I outline some of the most frequent attacks used against computer systems. Firstly we introduce the goals of computer security. Then we show how these can be affected by both external and internal threats.

**Goals of Computer Security**

The goals of computer security can be summed up in the words, confidentiality, integrity, availability and authenticity. Confidentiality ensures that only those authorised have access to the data of a computer system. Integrity ensures that a computer system can only be modified by an authorised party. Availability strives to ensure that a computer system is always available to authorised parties in a timely manner. Finally, authenticity requires that a computer system be able to verify the identity of a user.

Attacks on computer systems usually attempt to compromise one or more of these goals. The intention of the attacker may be to steal or intercept data, plant false data or otherwise modify the system, deny access to the system to legitimate users, or grant themselves unauthorised privileges.

Attacks on computer systems can be broken into two groups based on the attacker’s location, external or internal attacks. What is meant by “External Attacker” is a person or entity which is not a legitimate system user. By “Internal Attacker” we mean a legitimate user. We discuss these in the next sections.
External Attacks

There once was a time when computer security meant keeping the computer in a locked room and hiring a guard. As computers became increasingly connected to networks and the Internet, physical security of computers has reduced in importance as attackers no longer require physical access to the computer to compromise security.

External attacks originate from people or processes which are external to the computer system. These are often from computers which share the network of the computer or can otherwise access it via networked connectivity.

Researchers who study these types of attack often use honeynets to analyse what kind of attacks are happening in the wild and how these attacks occur. A honeynet is a network of computers which is set up with the intention of being attacked, and allowing the analysis of that attack.

What researchers (UK Honeynet Project, 2006) have found from this is a rich variety of tools and techniques used by hackers to compromise systems. These generally consist of brute force attacks on passwords to gain access, installation of zombies (or bots) to allow remote control of systems, and an increase in phishing attempts, as well as the usual background noise of automated attacks from viruses and worms.

Viruses & Worms

In recent years computer viruses have become increasingly sophisticated. In earlier years, if a user was unlucky enough to receive a virus infected file, they would have to execute it for the virus to run and perhaps replicate. Recently though, there have been increasing numbers of self-replicating viruses which require no user intervention to spread.
The Nimda virus is a salient example. The CERT Advisory (CERT, 2001) for this virus notes the multiple means of spreading itself which it can use, such as:

- from client to client via email
- from client to client via open networks shares
- from web server to client via browsing of compromised web sites
- from client to web server via active scanning for, and exploitation of various Microsoft IIS 4.0/5.0 directory traversal vulnerabilities
- from client to web server via scanning for the trapdoors left behind by the “Code Red II” and “sadmind/IIS” worms.

Many virus infections are now caused without any user intervention. Once these viruses install themselves, they can do anything on the computer such as open trapdoors, steal information, install zombies, and initiate various attacks on other computers.

Zombies & Bots

Hackers often install hidden software on infected computer systems. This allows them to easier access to the computer if passwords change, but more worryingly it allows them to download, upload or execute any application on the infected computer. Hackers keep score between themselves by quoting the number of “zombies” or “bots” they control, or infected computers they have use of. These computers have been seen to be used to initiate denial of service attacks against websites, or being used as a distributed computer for the purposes of cracking passwords or other encryption schemes.
Active Attacks

This is usually achieved by the installation of IRC (Internet Relay Chat) software. This opens a back door (sometimes called a trapdoor) to the system which the hacker can exploit. Internet Relay Chat is very similar in many ways to Instant Messaging, though the listeners can be software agents. These software agents can then be sent commands via the IRC channel.

Phishing

Phishing is a type of attack that relies on social engineering, usually in order to gain illegitimate access to a person's bank or credit card details. This is often carried out via email, instant message or phone where the attacker misrepresents themselves as a trustworthy person in an effort to gain access to PIN codes, user names or passwords. If these are gained, the attacker will then use them to gain access to the victim's finances.

This is a good example of “spoofing”. Spoofing is the term used to describe how a person or process can misrepresent themselves as a trusted party in order to gain an illegitimate advantage.

Internal Attacks

Internal attacks are perhaps not given the attention they deserve in the media compared with viruses, worms, denial of service attacks etc. Nevertheless this area is often where the most damage can be done by an attacker.

The first (and sometimes only) line of defence to a computer system is the login process. Usually user accounts with passwords are required to access a system, so once these have been compromised, an attacker is often be free to roam any part of the system. “A lot of companies have a hard outer shell, but anybody inside the building gets access to a lot of systems”, says Jason Guy, and IT security consultant with IBM Global Technology (Collins, 2006).
Internal attacks can be either accidental or intentional. Accidental breaches of security are usually caused by a user's misuse of the system. Examples can include users using bad or easily guessable passwords. Users misusing system resources, such as misconfiguration of system software, or deleting important system data. Users can also fall prey to the threat of Trojan horses.

**User Misuse**

In the war against attackers any information you volunteer to the attacker reduces the amount of work they have to do to successfully breach your system. It's surprising then how often users and administrators don't configure their systems for security. An example of this kind of carelessness is not disabling default user names.

For an attacker to log in they need to guess a correct user name and password pair. Take the “Administrator” account on Microsoft Windows or the “root” account on Unix. These are typically attacked because they have the highest privileges on those systems. If systems are configured with these accounts remaining, then an attacker is already half way to compromising the security. All they have to do is break the password.

As mentioned above, passwords are highly important for keeping intruders out, but often through user laziness, bad passwords are chosen. Strong passwords must be long, and contain a mixture of upper and lower case letters, numbers and special characters. The problem with these types of passwords for users is that they are difficult to remember.

Users can compromise security through misuse of the computer system's resources. For example, accidentally (or otherwise) deleting important files, or installing software from non trusted sources. This can lead to Trojan horses being introduced to the computer system.
**Trojan Horses**

A Trojan horse is “a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.” (Webopedia, 2006).

The problem with Trojan horses is that they are run by legitimate system users, and have all the same permissions to other system resources as the legitimate user does. While the user is using the benign part of the software, the malicious part can be doing anything from changing permissions on personal or sensitive files or other system resources, installing trapdoors, zombies or viruses or otherwise misusing the system.

Because Trojan attacks occur inside the security perimeter of the login, and run with the permissions of a legitimate user, they can go unnoticed for long periods. The system security policy, for example, cannot tell if the permissions being changed on a file are for legitimate or illegitimate reasons.

**Conclusion**

Computer security is fundamentally difficult. It depends on the race between software researchers to find and fix software vulnerabilities, before hackers find and exploit them. It involves finding a balance in the trade-off between user convenience and user security. As systems have more security restrictions imposed, they become more secure, but less easy to use. Indeed sometimes security restrictions become an impediment to honest users doing their jobs.

If we are to ever achieve the goal of secure computing, then everybody from user, to administrators to software developers are required to think security in everything they do.
Computer security will be an ongoing war which we may never convincingly win, but we cannot afford to lose.
References


