Computer insecurity

Many current computer systems have a very poor level of computer security. This computer insecurity article describes the current battlefield of computer security exploits and defenses. Please see the computer security article for an alternative approach, based on security engineering principles.

Contents

1 Security and systems design
   1.1 Financial cost
   1.2 Reasons
2 Vulnerabilities
   2.1 Exploits
   2.2 Eavesdropping
   2.3 Social engineering and human error
   2.4 Denial of service attacks
   2.5 Indirect attacks
   2.6 Backdoors
   2.7 Direct access attacks
   2.8 Reducing vulnerabilities
3 Security measures
   3.1 Difficulty with response
   3.2 Further reading
4 See also
5 References
6 External links

Security and systems design

Most current real-world computer security efforts focus on external threats, and generally treat the computer system itself as a trusted system. Some knowledgeable observers consider this to be a disastrous mistake, and point out that this distinction is the cause of much of the insecurity of current computer systems - once an attacker has subverted one part of a system without fine-grained security, he or she usually has access to most or all of the features of that system. Because computer systems are very complex, and cannot be guaranteed to be free of defects, this security stance tends to produce insecure systems.

The 'trusted systems' approach has been predominant in the design of many Microsoft software products, due to the long-standing Microsoft policy of emphasizing functionality and 'ease of use' over security. Microsoft claims that this is the result of consumer choice. Since Microsoft products currently dominate the desktop and home computing markets, this has led to unfortunate effects. However, the problems described here derive from the security stance taken by software and hardware vendors generally, rather than the failing of a single vendor. Microsoft is not out of line in this respect, just far more prominent with respect to its consumer marketshare and its mistakes are more pervasive.

It should be noted that the Windows NT line of operating systems from Microsoft contained mechanisms to limit this, such as services ran under dedicated user accounts, and Role-Based Access Control (RBAC) with user/group rights, but the Windows 95 line of products lacked most of these functions. Before the release of Windows 2003 Microsoft has changed their official stance, taking a more locked down approach. On
1/15/2002, Bill Gates sent out a memo on Trustworthy Computing, marking the official change in company stance.

Financial cost

Severe financial damage has been caused by computer security breaches, but estimating reliable costs is quite difficult. Figures in the billions of dollars have been quoted in relation to the damage caused by malware such as computer worms like the Code Red worm, but such estimates may be exaggerated. However, other losses, such as those caused by the compromise of credit card information, can be more easily determined, and they have been substantial, as measured by millions of individual victims of identity theft each year in each of several nations, and the severe hardship imposed on each victim, that can wipe out all of their finances, prevent them from getting a job, plus be treated as if they were the criminal. Volumes of victims of phishing and other scams may not be known.

On a personal level, people who have been infected with spyware or other types of malware have to go through a stressful and time-consuming process of cleaning their systems. If they decide that they must re-install an operating system, and they did not keep registration or product keys for proprietary software on their system, they sometimes have to pay for software that they already bought. The cost can therefore be days of time, and hundreds or even thousands of dollars.

Reasons

There are many similarities (yet many fundamental differences) between computer and physical security. Just like real-world security, the motivations for breaches of computer security vary between attackers, sometimes called hackers or crackers. Some are teenage thrill-seekers or vandals (the kind often responsible for defacing web sites); similarly, some web site defacements are done to make political statements. However, some attackers are highly skilled and motivated with the goal of compromising computers for financial gain or espionage. An example of the latter is Markus Hess who spied for the KGB and was ultimately caught because of the efforts of Clifford Stoll, who wrote an amusing and accurate book, The Cuckoo's Egg about his experiences. For those seeking to prevent security breaches, the first step is usually to attempt to identify what might motivate an attack on the system, how much the continued operation and information security of the system are worth, and who might be motivated to breach it. The precautions required for a home PC are very different for those of banks' Internet banking system, and different again for a classified military network. Other computer security writers suggest that, since an attacker using a network need know nothing about you or what you have on your computer, attacker motivation is inherently impossible to determine beyond guessing. If true, blocking all possible attacks is the only plausible action to take.

Vulnerabilities

To understand something about techniques for securing a computer system, it is important to first understand the various types of "attacks" that can be made against it. These threats can typically be classified into a number of categories:

Exploits

Software flaws, especially buffer overflows, are often exploited to gain control of a computer, or to cause it to operate in an unexpected manner. Many development methodologies rely on testing to ensure the quality of any code released; this process often fails to discover extremely unusual potential exploits. The code exploits often come in the form of Trojan horses, for example non-executable media files which are disguised to function in the application.
Computer insecurity - Wikipedia, the free encyclopedia

Eavesdropping

Any data that is transmitted over a network is at some risk of being eavesdropped, or even modified by a malicious person. Even machines that operate as a closed system (ie, with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware, such as TEMPEST. The FBI's proposed Carnivore program was intended to act as a system of eavesdropping protocols built into the systems of internet service providers.

Social engineering and human error

A computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them, for example sending messages that they are the system administrator and asking for passwords. This deception is known as Social engineering.

Denial of service attacks

Denial of service attacks differ slightly from those listed above, in that they are not primarily a means to gain unauthorized access or control of a system. They are instead designed to overload the capabilities of a machine or network, and thereby render it unusable. This type of attack is, in practice, very hard to prevent, because the behavior of whole networks needs to be analyzed, not only of small pieces of code.

Indirect attacks

Attacks in which one or more of the attack types above are launched from a third party computer which has been taken over remotely. The term usually used is "zombie computer". By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker.

Backdoors

Methods of bypassing normal authentication or giving remote access to a computer to somebody who knows about the backdoor, while intended to remain hidden to casual inspection. The backdoor may take the form of an installed program (e.g., Back Orifice) or could be in the form of an existing "legitimate" program, or executable file.

Direct access attacks

Someone gaining physical access to a computer can install all manner of devices to compromise security, including operating system modifications, software worms, keyboard loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup devices, e.g CD-ROM or DVD-ROM, or onto portable media such as keydrives, digital cameras or digital audio players.

See also: Category:Cryptographic attacks

Reducing vulnerabilities

Computer code is regarded by some as just a form of mathematics. It is theoretically possible to prove the correctness of computer programs (within very limited circumstances) though the likelihood of actually achieving this in large-scale practical systems is regarded as unlikely in the extreme by most with practical experience in the industry -- see Bruce
It's also possible to protect messages in transit (i.e., communications) by means of cryptography. One method of encryption — the one-time pad — has been proven to be unbreakable when correctly used. This method was used by the Soviet Union during the Cold War, though flaws in their implementation allowed some cryptanalysis (See Venona Project). The method uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message. For transmitted computer encryption this method is difficult to use properly (securely), and highly inconvenient as well. Other methods of encryption, while breakable in theory, are often virtually impossible to directly break by any means publicly known today. Breaking them requires some non-cryptographic input, such as a stolen key, stolen plaintext (at either end of the transmission), or some other extra cryptanalytic information.

Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Even in a highly disciplined environment, such as in military organizations, social engineering attacks can still be difficult to foresee and prevent.

In practice, only a small fraction of computer program code is mathematically proven, or even goes through comprehensive information technology audits or inexpensive but extremely valuable computer security audits, so it's usually possible for a determined cracker to read, copy, alter or destroy data in well secured computers. You can reduce a cracker's chances by keeping your systems up to date, using a security scanner or/and hiring competent people responsible for security. The effects of data loss/damage can be reduced by careful backing up and insurance.

**Security measures**

A state of computer "security" is the conceptual ideal, attained by the use of the three processes:

1. Prevention,
2. Detection, and
3. Response.

- User account access controls and cryptography can protect systems files and data, respectively.
- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) block the normal packet types, preventing some kinds of attacks.
- Intrusion Detection Systems (IDS's) are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.
- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored.

Today, computer security comprises mainly "preventive" measures, like firewalls or an Exit Procedure. We could liken a firewall to the building of a good fence around your warehouse. Firewalls are common amongst machines that are permanently connected to the Internet (though not universal, as demonstrated by the large numbers of machines "cracked" by worms like the Code Red worm which would have been protected by a properly-configured firewall). However, relatively few organisations maintain computer systems with effective detection systems, and fewer still have organised response mechanisms in place.

**Difficulty with response**

Responding forcefully to attempted security breaches (in the manner that one would for attempted physical security breaches) is often very difficult for a variety of reasons:

- Identifying attackers is difficult, as they are often in a different jurisdiction to the systems they attempt
to breach, and operate through proxies, temporary anonymous dial-up accounts, and other anonymising procedures which make backtracing difficult and are often located in yet another jurisdiction. If they successfully breach security, they are often able to delete logs to cover their tracks.

- The sheer number of attempted attacks is so large that organisations cannot spend time pursuing each attacker (a typical home user with a permanent (eg, cable modem) connection will be attacked at least several times per day, so more attractive targets could be presumed to see many more).

- Law enforcement officers are often unfamiliar with information technology, and so lack the skills and interest in pursuing attackers. There are also budgetary constraints. It has been argued that the high cost of technology, such as DNA testing, and improved forensics mean less money for other kinds of law enforcement, so the overall rate of criminals not getting dealt with goes up as the cost of the technology increases.

Further reading

Computer security is a highly complex field, and is relatively immature, except in the area of designing computers that are secure. Because such computer systems are significantly more expensive than those with little or no security, the market place has driven several such secure systems out of the PC business, IBM for example. The ever-greater amounts of money dependent on electronic information make protecting it a growing industry and an active research topic.

There is an extensive culture associated with electronic security; see electronic underground community.

See also

- Computer forensics
- Computing
- Cryptography (aka cryptology)
- Data remanence
- Defensive programming
- Full disclosure
- Hacking
- Physical security
- RISKs Digest
- Security engineering
- Recovery
- Microreboot
- Restartability
- Crash-only software

References

- Clifford Stoll: The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, an informal -- and easily approachable by the non-specialist -- account of a real incident (and pattern) of computer insecurity, ISBN 0-7434-1146-3

External links

- Participating With Safety (http://secdocs.net/manual/lp/sec/) , a guide to electronic security threats from the viewpoint of civil liberties organisations. Licensed under the GFDL.