Defense-in-Depth: An Introduction
Brian Nelson
June 30, 2001

Introduction

In today's fast-paced world, computers and networking are at the top of society's priorities and concerns. Networked computers affect and play an important role in business, education, government, medicine, and recreation among many other things. Everyday, large corporations, medical institutions, government agencies, and universities, and so on trust and utilize these computers for data manipulation and storage, communication, and operation, as well as a host of other useful tasks. All of these tasks assist in making the computers function more quickly and efficiently. Computers have become the basis of everyday life.

On these computers, corporations, institutions, agencies, etc. have trusted their most valuable information: information critical to business development and growth, information containing people's credit card numbers, status, and identity, even top-secret information concerning the defense and well being of our countries. Yet, computer security (integrity, confidentiality, and availability) is hardly implemented and occasionally it is even overlooked.

This information and data must be well protected in order for our society to thrive and successfully advance in a positive direction. Therefore, we must implement the principle of Defense in Depth to our networked (or standalone) computer systems. Computer-Network-Security.com defines defense in depth as the security approach whereby each system on the network is secured to the greatest possible degree.

Many strategies exist to secure computer systems. However, no single method is sufficient to repel all forms of attacks. In fact, even with every strategy implemented, there will still be imperfections and deficiencies in every secure network. However, the goal of defense in depth is to decrease the chance of an attacker breaking into a system by increasing the layers of security and defense.

This paper will briefly cover security policy, employee training, firewalls, passwords, cryptography, anti-virus software, and physical security. A particular strategy of defense will be named, followed by a description of that strategy, noting its strengths, then noting its weaknesses, and finally, relating it to defense in depth.

Security Policy

A well-written, thorough security policy should always be the first layer of defense in computer security. How can one build an intricate model car without precise instructions? Similarly, how can one effectively build a secure network without a complete and well-defined security policy? A security policy must state its purpose, identify its scope, define terms, declare the rights of users, delegate responsibility and action, reference related documents, and must always change to meet nearly all criteria. It must be easily understandable, well structured, and recognized as an authoritative document (usually accomplished through acknowledgment by upper management).

A well-written, complete security policy is the foundation to building a secure computing environment. It is the definitive guide on how to protect an institution's information. A good security policy will not only protect computers, but it will do the same for system administrators and users. Without a security policy, many situations and aspects would be overlooked and discounted.

Though a security policy should always be the first line of defense, it cannot be the only line of defense. A security policy that is not implemented, or incorrectly implemented, offers no help with confidentiality, integrity, and availability. A policy that is not implemented is just a piece of paper. Furthermore, it is impossible for a security policy to address every situation.

A security policy will always be the first step in implementing information protection. It is the first layer in the concept of defense in depth.

Employee Awareness

Employee awareness is often the most overlooked layer of defense in computer security. Although most employees have a basic understanding of computers and the terms associated with them, they still lack the essential knowledge related to computer security, security policy, viruses, Trojan horses, worms, and other related issues. Actually employees cause more than half of all inflicted damage to computer networks. Some of this damage is unintentional; however, disgruntled employees can certainly impose a significant amount of damage as well. Required training for every employee is crucial in order to successfully gain complete employee awareness. It will educate those who fall short of proper computer security education and will warn those who are tempted to tamper or harm computers and networks. The training should provide each employee with a copy of the security policy and should emphasize each person's rights and responsibilities.

Employee awareness will help reduce damage caused by employees by educating those that lack computer security knowledge. It can also reduce destruction caused by unhappy employees by warning them of the consequences. This will give more time for system administrators and security officials to concentrate on preventing outside hackers and malicious people from breaking into or tampering with company computers and networks.

Employee awareness may help to reduce damage incurred by employees, but it will not prevent all damage. Mistakes are always prone to occur in a fast-paced computing environment, and there will always be employees that do not consider the consequences before intentionally causing damage to computers, networks, and so on.

Employee awareness should always be included as a layer in the implementation of defense in depth. Effective implementation of employee awareness will allow more time to be spent on other security related issues.

Firewalls

Firewalls are some of the most common means of protection between the Internet and an institution's LAN(s). A firewall is a system or group of systems that enforces an access control policy between two networks. It can either choose what traffic to permit, or it can choose what traffic to prohibit. Depending on the amount of security required, firewalls can allow a host of protocols through (such as http, ftp, telnet) or it can just permit e-mail through. Loosely speaking, there are two types of firewalls: Filtering Firewalls and Proxy Servers. Filtering Firewalls examine packets as they arrive (sometimes even at the router) and allow the packets to travel based on the firewall's rules. Proxy servers (both application and SOCKS) monitor outbound traffic. A user "logs" into the outside world via the proxy server. Because of this, records and logs can be kept (through cached data) of all traffic in and outbound.

Firewalls work very efficiently as perimeter defenses. They unquestionably define what traffic is permitted. They can log information such as files that are transferred (through ftp), every URL that is visited (for http), and each server that it logs into (for telnet). Some firewalls even have some anti-virus software built-in to reject known viruses. Firewalls are great for blocking much of the evil that the Internet offers.

Firewalls, however, cannot be one's only line of defense. Though firewalls can block certain traffic that passes in and out of the network, it cannot prevent an employee from creating a dial-up connection to the Internet from their modem. Moreover, firewalls cannot prevent an employee from taking out or bringing in data on portable media. It only offers a kind of gateway between an institution's LAN and the outside traffic/networks.

Firewalls can be a very important and powerful part of strong computer security. But, all too often, many companies rely on firewalls for complete protection. A firewall is just as powerful as a good security policy and strong employee training.

Passwords

Passwords are another great means of preventing outside or unauthorized users from gaining access to information on a computer or on a network. When implemented correctly, password authentication can be very difficult and almost impossible to attain. An institute must simply require that a user choose a password (preferably with symbols and non-dictionary words) to use with his or her user name.

Password utilization is a very standard practice at most institutions. It is easy to implement, and it can discourage unauthorized users from trying to log onto a system or network. Password logging is also a great means of monitoring failed (or successful) logging attempts. When implemented with simple programs, it can notify security officials of possible break-in attempts or unauthorized logging.

Although password authentication is a strong means of defense, it has some serious shortcomings. Users tend to choose passwords that are easy to guess or easy to crack with free password cracking software. Even strong passwords that don't use dictionary words and contain symbols can be cracked when using a brute force password attack.

Password usage is yet another strong layer of defense in depth. Hard-to-guess passwords will help to protect systems and networks. Even brute force attacks can take weeks to crack a password. Strongly implemented passwords help turn away hackers and crackers, thus adding more defenses to systems.

Cryptography

Cryptography is the art or science of keeping messages secret. Encryption is the act of encoding the contents of the message in such a way that hides its contents from outsiders. Encryption is used with computers to ensure that a message sent over networks (and especially over the Internet), cannot be read easily by on-lookers. The sender begins by encrypting a message with his or her own private encryption key. The message (now called ciphertext) is then sent to the recipient, who decrypts the ciphertext with the public key that corresponds to the sender's private key. The message is then readable, and hopefully is only read by the recipient. Also related to encryption is Public Key Infrastructure (PKI), a tool for securing net-based communications and transactions. With PKI, one can generate a private key and publish his or her public key on one of many servers that others can access.

Cryptography is a very useful science that allows for confidentiality and integrity. One can send a message, append a signature, and send it to another. If the message is intercepted and tampered with, the recipient will recognize that signatures do not match. This can allow the message to be checked for authenticity. Cryptography also makes it very difficult for on-lookers to decrypt messages.

Encrypted messages, however, are still vulnerable to cracking. Though, with development of the new encryption standard (128 bit encryption), this is still very difficult. Encryption also delays communication slightly.

Cryptography is a very nice addition to the implementation of defense in depth. It is yet another shield that will keep away or discourage malicious people.

Anti-Virus Software

Anti-Virus software scans a system or systems for known viruses. Anti-Virus software can be updated manually or automatically in order to remain up-to-date with viruses that are out in the wild or in the zoo. After detection, anti-virus software will free the system of that virus and, in some cases, fix any problems the virus created. It can be customized to be completely automated and user friendly. There are many vendors that sell very powerful anti-virus software; there are many freely distributed anti-virus tools as well.

Anti-viral tools provide a means of protection against known viruses. They are very useful to have in order to protect innocent, naïve, or susceptible users from dangerous viruses. The simplicity of these software packages makes anti-virus software appropriate and extremely useful for computer security.

Anti-viral tools, however, cannot catch all viruses, Trojan horses, worms, etc. If one slips past the software, it can cause irreparable damage to a computer or even an entire network. Anti-virus tools can also be very expensive for a site license.

Anti-virus software is yet another necessity for strong computer security. It will prevent many incidents from occurring. When implemented with other security measures, it promises a secure computing environment.

Physical Security

So much time and effort is spent securing networks and computers on the "working" level that physical security is often unnoticed or ignored. Computers and networks are just as susceptible to natural disasters, theft, and destruction as any other item. Servers (web, file, e-mail, and such) should be locked in a well-ventilated, air-conditioned room where access is very limited. Computers containing top-secret, high priority, or classified information should be located in an area that is monitored and access is logged. Food, drinks, and other related things should be kept away from computers. Computers, network cables, and the like should not be accessible to outsiders.

Physical security is as important as any other aspect of computer security. Damaged or stolen (from physical theft) information is just as bad as viruses, hackers, and crackers. Computers that are protected according to the information that is enclosed are an essential part of defense in depth.

Physical security can never be perfected. Accidents are prone to occur and systems, as with any other valuable object, are vulnerable to theft.

As mentioned, physical security is as important as any other computer security aspect. The physical computer and network connections must be as secured as the data contained therein.

Conclusion

To conclude, excellent computer security is achieved by implementing the concept of defense in depth. No computer or network can ever be completely secured; a secure computing environment will make the effort of hacking and cracking outweigh the any possible benefits. The examples given here are just a few of many essential computer security applications. Other computer security applications include virtual private networks, PGP, intrusion detection systems, and a host of other things. Defense in depth is the only way to assure good computer security, data safekeeping, and integrity, availability, and confidentiality.

References:

"Computers in Society."
URL: http://cgms.dade.k12.fl.us/cgms/127/Workbook/comps in socty/compsSociety.html (1 July 2001).

"Glossary." Computer Network Security.
URL: http://www.computer-network-security.com/glossary.html (29 June 2001).

McMillan, Rob. "Site Security Policy Development."
URL: http://security.tsu.ru/info/policy/AusCERT.html (1 July 2001).

Roback, Ed. "Computer and Information Security Policy." July 2000.
URL: http://secinf.net/info/policy/hk_polic.html (1 July 2001).

Curtin, Matt and Ranum, Marcus J. "Internet Firewalls: Frequently Asked Questions." December 2000.
URL: http://www.interhack.net/pubs/fwfaq/ (23 June 2001).

Grennan, Mark. "Understanding Firewalls: Firewall and Proxy Server HOWTO. v0.80. February 2000.
URL: http://www.linuxdoc.org/HOWTO/Firewall-HOWTO-2.html (20 June 2001).

"Introduction to Cryptography."
URL: http://www.ssh.fi/tech/crypto/intro.html   (1 July 2001).