MOVING TOWARD NETWORK SECURITY AND FIREWALLS FOR PROTECTING AND PRESERVING PRIVATE RESOURCES ON THE INTERNET

Dr.S.S.Riaz Ahamed.
Director, Dept of Computer Applications, Mohamed Sathak Engg College ,Kilakarai & Principal, Sathak Institute of Technology, Ramanathapuram,TamilNadu, India-623501.
Email : ssriaz@yahoo.com

ABSTRACT

Computer and network security are challenging topics among executives and managers of computer corporations. Internet security is the practice of protecting and preserving private resources and information on the Internet. Even discussing security policies may seem to create a potential liability. As a result, enterprise management teams are often not aware of the many advances and innovations in Internet and intranet security technology. Without this knowledge, corporations are not able to take full advantage of the benefits and capabilities of the network.

Key words: *Operating System Security (OSS), File Transfer Protocol (FTP), Virtual Private Network (VPN), Digital Encryption Standard (DES), Pretty Good Privacy (PGP), Privacy Enhanced Mail (PEM).*

1. ELEMENTS OF NETWORKING SECURITY

1.1 Orange Book Security Levels and Firewalls

There are many strong tools available for securing a computer network. By themselves, the software applications and hardware products that secure a business’ computer network do not comprise a security policy, yet they are essential elements in the creation of site security. While these technologies are not the focus of this paper, a basic understanding of them will facilitate the creation of a site security policy[2].

Tools to protect your enterprise network have been evolving for the last two decades, roughly the same amount of time that people have been trying to break into computer networks. These tools can protect a computer network at many levels, and a well-guarded enterprise deploys many different types of security technologies. The most obvious element of security is often times the most easily overlooked: physical security—namely, controlling access to the most sensitive components in your computer network, such as a network administration station or the server room. No amount of planning or expensive equipment will keep your network secure if unauthorized personnel can have access to central administration consoles. Even if a user does not have evil intent, an untrained user may unknowingly provide unauthorized outside access or override certain protective configurations[1][5].

The next level of computer security is operating system security (OSS). The U. S. Department of Defense (DOD) established general guidelines for operating system security, and other countries around the world (as well as other federal organizations) have set their standards as well. In the past few years, certified (tested and approved) secure OSS has been introduced in commercial operating systems like UNIX® and Microsoft Windows NT. These are at the C2 level, which provides discretionary access control-file, directory read and write permission, and auditing and authentication controls[1]-[5].

1.2 Orange Book Security Levels

The DOD has defined seven levels of computer OSS in the Trusted Computer Standards Evaluation Criteria, otherwise known as the Orange Book. The levels are used to evaluate protection for hardware, software, and stored information. The system is additive—higher ratings include the functionality of the levels below. The definition centers around access control, authentication, auditing, and levels of trust. D1 is the lowest form of security available and states that the system is insecure. A D1 rating is never awarded because this is essentially no security at all. C1 is the lowest level of security. The system has file and directory read and write controls and authentication through user login. However, root is considered an insecure function and auditing (system logging) is not available. C2 features an auditing function to record all security-related events and provides stronger protection on key system files, such as the password file[2][8][10].

A B-rated system supports multilevel security, such as secret, top secret, and mandatory access control, which states that a user cannot change permissions on files or directories. B2 requires that every object and file be labeled according to its security level and that these labels change dynamically depending on what is being used. B3 extends security levels down into the system hardware; for example, terminals can only connect through trusted cable paths and specialized system hardware to ensure that there is no unauthorized access. A1 is the highest level of security validated through the Orange Book. The design must be mathematically verified; all hardware and software must have been protected during shipment to prevent tampering. A word of caution on secure operating systems must be mentioned: the features and capabilities require significant amounts of central processing unit (CPU) processing power and disk space. In low-end servers, enabling the security features may seriously affect the number of users a server can support[8][9].

1.3 Firewalls

While in theory firewalls allow only authorized communications between the internal and external networks, new ways are always being developed to compromise these systems. However, properly implemented, they are very effective at keeping out unauthorized users and stopping unwanted activities on an internal network. Firewall systems protect and facilitate your network at a number of levels. They allow e-mail and other applications, such as file transfer protocol (FTP) and remote login as desired, to take place while otherwise limiting access to the internal network. Firewall systems provide an authorization mechanism that assures that only specified users or applications can gain access through the firewall. They typically provide a logging and alerting feature, which tracks designated usage and signals at specified events. These systems offer address translation, which masks the actual name and address of any machine communicating through the firewall. For example, all messages for anyone in the technical support department would have his/her address translated to techsupp@company.com, effectively hiding the name of an actual user and network address. Firewall system providers are adding new functionality, such as encryption and virtual private network (VPN) capabilities.

Firewall systems can also be deployed within an enterprise network to compartmentalize different servers and networks, in effect controlling access within the network. For example, an enterprise may want to separate the accounting and payroll server from the rest of the network and only allow certain individuals to access the information. Unfortunately, all firewall systems have some performance degradation. As a system is busy checking or rerouting data communications packets, they do not flow through the system as efficiently as they would if the firewall system were not in place[1]-[13].

2. PASSWORD MECHANISMS

Passwords are a way to identify and authenticate users as they access the computer system. Unfortunately, there are a number of ways in which a password can be compromised. For Example, someone wanting to gain access can listen for a username password as an authorized user gains access over a public network. In addition, a potential intruder can mount an attack on the access gateway, entering an entire dictionary of words (or license plates or any other list) against a password field. Users may loan their password to a co-worker or inadvertently leave out a list of system passwords. Fortunately, there are password technologies and tools to help make your network more secure. Useful in ad hoc remote access situations, one-time password generation assumes that a password will be compromised. Before leaving the internal network, a list of passwords that will work only one time against a given username is generated. When logging into the system remotely, a password is used once and then will no longer be valid.

2.1 Password Aging and Policy Enforcement

Password aging is a feature that requires users to create new passwords every so often. Good password policy dictates that passwords must be a minimum number of characters and a mix of letters and numbers. Smart cards provide extremely secure password protection. Unique passwords, based on a challenge-response scheme, are created on a small credit-card device. The password is then entered as part of the log-on process and validated against a password server, which logs all access to the system. As might be expected, these systems can be expensive to implement.

Single sign-on overcomes what can only be the ultimate irony in system security: as a user gains more passwords, these passwords become less secure, not more, and the system opens itself up for unauthorized access. Many enterprise computer networks are designed to require users to have different passwords to access different parts of the system. As users acquire more passwords—some people have more than 50—they cannot help but write them down or create easy-to-remember passwords. A single sign-on system is essentially a centralized access control list which determines who is authorized to access different areas of the computer network and a mechanism for providing the expected password. A user need only remember a single password to sign onto the system.

Good password procedures include the following:

- Do use a password with mixed-case alphabetics.
- Do use a password with non-alphabetic characters (digits or punctuation).
- Do use a password that is easy to remember, so you don’t have to write it down
- Do not use your login name in any form (as is, reversed, capitalized, doubled, etc.).
- Do not use your first, middle, or last name in any form or use your spouse’s or children’s names.
- Do not use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the make of your automobile, the name of the street you live on, etc.
- Do not use a password of all digits or all the same letter.
- Do not use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words.
- Do not use a password shorter than six characters.

2.2 Encryption, Authentication, and Integrity

A firewall system is a hardware/software configuration that sits at perimeter between a company's network and the Internet, controlling access into and out of the network. Encryption can be understood as follows:

- the coding of data through an algorithm or transform table into apparently unintelligible garbage
- used on both data stored on a server or as data is communicated through a network
- a method of ensuring privacy of data and that only intended users may view the information

There are many forms of encryption, but only the most popular forms will be discussed in this tutorial. The digital encryption standard (DES) has been endorsed by the National Institute of Standards and Technology (NIST) since 1975 and is the most readily available encryption standard. One major drawback with DES is that it is subject to U. S. export control; programs that deploy DES technology are generally not available for export from the United States. Rivest, Shamir, and Adleman (RSA) encryption is a public-key encryption system, is patented technology in the United States, and thus is not available without a license. However, the fundamental DES algorithm was published before the patent filing, and RSA encryption may be used in Europe and Asia without a royalty. RSA encryption is growing in popularity and is considered quite secure from brute force attacks. An emerging encryption mechanism is pretty good privacy (PGP), which allows users to encrypt information stored on their system as well as to send and receive encrypted e-mail. PGP also provides tools and utilities for creating, certifying, and managing keys. PGP should not be confused with privacy enhanced mail (PEM), a protocol standard.

Encryption mechanisms rely on keys or passwords. The longer the password, the more difficult the encryption is to break. DES relies on a 56-bit key length, and some mechanisms have keys that are hundreds of bits long. There are two kinds of encryption mechanisms used—private key and public key. Private-key encryption uses the same key to encode and decode the data. Public-key encryption uses one key to encode the data and another to decode the data. The name public key comes from a unique property of this type of encryption mechanism—namely, one of the keys can be public without compromising the privacy of the message or the other key. In fact, usually a trusted recipient, perhaps a remote office network gateway, keeps a private key to decode data as it comes from the main office. VPNs employ encryption to provide secure transmissions over public networks such as the Internet[7]-[18].

2.3 Authentication and Integrity

Authentication is simply making sure users are who they say they are. When using resources or sending messages in a large private network, not to mention the Internet, authentication is of the utmost importance. Integrity is knowing that the data sent has not been altered along the way. Of course, a message modified in any way would be highly suspect and should be completely discounted. Message integrity is maintained with digital signatures. A digital signature is a block of data at the end of a message that attests to the authenticity of the file. If any change is made to the file, the signature will not verify. Digital signatures perform both an authentication and message integrity function. Digital signature functionality is available in PGP and when using RSA encryption. Kerberos is an add-on system that can be used with any existing network. Kerberos validates a user through its authentication system and uses DES when communicating sensitive information—such as passwords—in an open network. In addition, Kerberos sessions have a limited lifespan, requiring users to login after a predetermined length of time and disallowing would-be intruders to replay a captured session and thus gain unauthorized entry[3][5].

3. CONCLUSION

Every business has a different threshold of well-being, different assets, a different culture, and a different technology infrastructure. Every business has different requirements for storing, sending, and communicating information in electronic form. Just as a business evolves in changing market conditions, a site security policy must adapt to meet changing technology conditions.

REFERENCES

[1] S. Allman, "Encryption and Security: the Advanced Encryption Standard," *EDN*, 31 October 2002, pp. 62-97.

[2] N. Borisov et al., "Intercepting Mobile Communications: The Insecurity of 802.11," Proc. Mobicom 2003.

[3] B. Cromwell, "Securing Unlicensed WLAN Data Communications," RF Design Magazine, February 2003, pp. 50-59.

[4] Garfinkel and Spafford. Practical UNIX Security. O'Reilly & Associates.

[5] Quarterman, J. and Carl-Mitchell, S. The Internet Connection, Reading, Massachusetts: Addison-Wesley Publishing Company; 1994.

[6] Ranum, M. J. Thinking about Firewalls, Trusted Information Systems, Inc. Stoll, C. The Cuckoo's Egg. Doubleday.

[7] Treese, G. W. and Wolman, A. X through the Firewall and Other Application Relays.

[8] I. Akyildiz, et al., "AdaptNet: An Adaptive Protocol Suite for the Next-Generation Wireless Internet," IEEE Communications Magazine, March 2004, pp. 128-139.

[9] H. Balakrishnan et al., "A comparison of mechanisms for improving TCP performance over wireless links," IEEE/ACM Trans. on Networking, Vol. 5, pp. 756-776 (December 1999).

[10] M. Chiani, E. Milani, and R. Verdone, "A Semi-Analytical Approach for Performance Evaluation of TCP-IP Based Mobile Radio Links," Proc. GlobeCom 2000.

[11] Hiroshi Yoshimura et al, "Future Photonic Transport Networks Based on WDM Technologies", Vol 37, No 2, pp 74-81, February 1999.

[12] E. Lowe, "Current European WDM Deployment Trends", IEEE Communications Magazine, Feburary 1998, pp. 46-50.

[13] J. P. Ryan, R. H. Kent, "WDM: North American Deployment Trends", IEEE

Communications Magazine, Feburary 1998, pp. 40-44.

[14] J. R. Kiniry, "Wavelength Division Multiplexing: Ulta High Speed Fiber Optics", IEEE Internet Computing, March-April 1998, http://computer.org/internet/

[15] P. R. Trischitta and William C. Marra "Applying WDM Technology to Undersea Cable Networks", IEEE Communications Magazine, Feburary 1998, pp. 62-66.

[16] Cheswick, B. and Bellovin, S. Firewalls and Internet Security. Addison-Wesley,Pp 87-154.

[17] Comer, D.E and Stevens, D.L., Internetworking with TCP/IP. Volumes I-III. Englewood Cliffs, New Jersey: Prentice Hall; 1991-1993,Pp 56-110.

[18] Curry, D. UNIX System Security—A Guide for Users and System Administrators,Pp 77-112.