# RESEARCH PAPER ON FIREWALLS SYSTEM

Mohit Rathi, Manish Lohia

***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.**

## I. ELEMENTS OF NETWORKING SECURITY

### *A. 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. 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. system security (OSS).

### *B. 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. 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.

### *C. 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. 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.

## II. 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.

*A. 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.

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.

*B. 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 email.

*C. 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.

## 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 of802.11," 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