© 2014 IJIRT | Volume 1 Issue 5 | ISSN : 2349-6002

Security in Computer Network

Varun Saluja, Vanita
Dronacharya College of Engineering

***Abstract*: Network security starts with authenticating, commonly with a username and a password. Covers a variety of computer networks, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, within a company, and others which might be open to public access. It secures the network, protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password consists of the provisions and policies adopted by a network administrator, to prevent and monitor unauthorized access, misuse . Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data travelling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation. Types of attacks include: wiretapping, Port scanner, Idle scan, Denial-of-service attack, Spoofing. This review paper covers a detailed study about computer network security and types of attacks.**

I. INTRODUCTION

With all of the vital personal and business data being shared on computer networks every day, security has become one of the most essential aspects of networking. No one recipe to fully safeguard networks against intruders exists. Network security technology improves and evolves over time as the methods for both attack and defense grow more sophisticated.

Computer Security In the last few decades, the world saw a revolution in information and technology, and the main factor of this revolution was the computer. Computers made life easier for millions of people all over the world, especially in the United States, where the latest innovations in the field of computers take place. Information circulates with extreme speed, and a person with a computer and access to the Internet can follow what is happening on Wall Street, even if he is thousands of miles away from there

Activities designed to protect your network are referred to as network security. If your network security is reliable, it is targeting a wide variety of threats and keeping them from entering your network and spreading.

II. SECURITY MECHANISMS

A security mechanism is a device that is used partially to enforce a security policy. Some mechanisms do this by individually or collectively implementing a security principle. Other mechanisms are implied directly by a security policy. These enforce some component of the policy .The use of personal computers in industry and commerce has expanded dramatically in the last decade. Large gains in employee productivity are possible as a result of this technology. However, ensuring the security of the processes and the privacy of data that these machines access is a very hard problem. Solutions that ensure security by preventing access by legitimate users are inconsistent with the gains in productivity that are possible. The general problem of computer security is being attacked by government and by academic and industrial research with some notable success. The aim of these essays is to review the principles behind these successes, to describe some of the remaining problems and to discuss their application in industry and commerce.

III. LAYERED SECURITY

Network security is often based on the familiar OSI model, which organizes networking into seven layers. When information travels from one network node to another, its control is passed from one layer to the next, starting at Layer 7 at the transmitting node, traveling down to Layer 1, crossing to the next node, and then going from Layer 1 back up to Layer 7 at the receiving node. The OSI Layers are: Layer 1, the Physical Layer: Defines such electrical and mechanical characteristics of networking equipment as voltage levels, signal timing, data rate, maximum transmission length, transmission media, network topology, and physical connectors. Layer 2, the Data Link Layer: Here data packets are encoded and decoded. Layer 3, the Network Layer: Includes switching and routing protocols .Layer 4, the Transport Layer: Provides for the transparent transfer of data between nodes, as well as error recovery and flow control. Layer 5, the Session Layer: Establishes, manages, and terminates connection Layer 6, the Presentation Layer: Formats data to be sent across a network to ensure there are no compatibility problems. Layer 7, the Application Layer: Supports applications and end-user processes .A complete network security plan addresses security at all OSI layers, starting at Layer 1 with securing the hardware and working up through the layers to include password protection, encryption, VPNs, virus scans, and firewalls. A security barrier at each Layer protects against all kinds of attacks and provides complete network security. Layer 1 security can loosely be defined as physical security—keeping persons physically away from the hardware that holds unauthorized data and also protecting that hardware from deliberate or accidental damage .Network security starts from the bottom up at Layer 1. First you must control physical access to a network, then you concern yourself with data security. Expensive and complex software solutions don't do you any good if your network hardware isn't properly secured in the first place. The week after you buy that fancy firewall, your sensitive data could go strolling out the door in someone's pocket.

IV. CRYPTOGRAPHY

The art of protecting information by transforming it (*encrypting* it) into an unreadable format called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called *code breaking*, although modern cryptography techniques are virtually unbreakable.

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is *Pretty Good Privacy* because it's effective and free.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and *public-key* systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

V. PROTECTION AGAINST INTRUDERS (FIREWALLS)

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Hardware and Software Firewalls

Firewalls can be either hardware or software but the ideal firewall configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins.

Hardware firewalls can be purchased as a stand-alone product but are also typically found in broadband routers, and should be considered an important part of your system and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available. Software firewalls are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer.

There are different types of firewalls depending on where the communication is taking place, where the communication is intercepted and the state that is being traced.

Network layer or packet filters

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. The term "packet filter" originated in the context of BSD operating systems.

Network layer firewalls generally fall into two sub-categories, state full and stateless. State full firewalls maintain context about active sessions, and use that "state information" to speed packet processing. Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer, or completion connection). If a packet does not match an existing connection, it will be evaluated according to the rule set for new connections. If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing.

Stateless firewalls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

VI. CONCLUSION

This chapter covers a very large and important area of computer security: networks and distributed applications. As the world becomes more connected by networks, the significance of network security will certainly continue to grow. Security issues for networks are visible and important, but their analysis is similar to the analysis done for other aspects of security. Network assets include the network infrastructure, applications programs and, most importantly, data. Recall that threats are actions or situations that offer potential harm to or loss of confidentiality, integrity, or availability, in the form of interception (eavesdropping or passive wiretapping), modification (active wiretapping, falsification, and compromise of authenticity), and denial of service. In stand-alone computing, most agents have a strong motive for an attack. But in networks we see new threat agents; anyone can be a victim of essentially a random attack. The strongest network controls are solid authentication, access control, and encryption.

KEY CONCERNS: *Encryption authentication key exchange also: increasingly an important area as network connectivity increasesdigital signatures, digital cash, authentication, increasingly important an important social concern*