© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 01 | January - March 2016

ENHANCED SECURITY OF NETWORK SYSTEM USING IP FILTER & CRYPTOGRAPHY

[1]Reena Kumari, [2]Ms. Shilpa Nagpal, Deptt. Of CSE

Abstract: *This research is concerned with Network Security. Major issue in network systems is that re is lot of threat to Client & server from external attacks. Many Security have been developed to enhance security but they have some limitation. Objective of our research is to make network system more secure by merging IP filters & Cryptography Techniques.*

Keywords: Firewall, Hacker, Cryptanalyst, IP Filters, TCP, IP, Cryptography

[I] INTRODUCTION

Network security consists of policies adopted to prevent & monitor unauthorized access, misuse, modification, denial of a computer network & network-accessible resources. Network security consists of authorization of access to data in a network that is controlled by network administrator. Users are assigned an ID & password or other authenticating information that allows access to information & programs within authority. Network security covers a variety of computer networks, both public & private, that are used in everyday jobs; conducting transactions & communications among businesses, government agencies & individuals. Networks can be private/within a company, & others which might be open to public access. Network security is involved in organizations, enterprises, & other types of institutions.

[2] THREATS TO NETWORK SECURITY

Types of attack

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, & attacks through service provider. Information systems & networks offer attractive targets & should be resistant to attack from full range of threat agents, from hackers to nation-states. A system must be able to limit damage & recover rapidly when attacks occur.

Five types of attack are as follow

Passive Attack

A **passive attack** monitors unencrypted traffic & looks for clear-text passwords & sensitive information that can be used in other types of attacks. **Passive attacks** consists of traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, & capturing authentication information such as passwords. Passive interception of network operations allows adversaries to see upcoming actions. Passive attacks result in disclosure of data files to an attacker without knowledge of user.

Active Attack

In an **active attack,** attacker breaks into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, & to steal or modify information. Attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in disclosure or dissemination of data files, DoS, or modification of data.

Distributed Attack

A **distributed attack** requires that adversary introduce code, such as a Trojan horse or back-door program, to a "trusted" component or software that will later be distributed to many other companies &

users Distribution attacks focus on malicious modification of hardware or software at factory or during distribution. Attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

Insider Attack

An **insider attack** involves someone from inside, such as a disgruntled employee, attacking network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.

Close-in Attack

A **close-in attack** involves someone attempting to get physically close to network components, data, & systems in order to learn more about a network Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into network, open access, or both.

One popular form of close in attack is **social engineering** in a social engineering attack, attacker compromises network or system through social interaction with a person, through an e-mail message or phone. Various tricks can be used by individual to revealing information about security of company.

Phishing Attack

In phishing attack hacker creates a fake web site that looks exactly like a popular site such as SBI bank or paypal. Phishing part of attack is that hacker n sends an e-mail message trying to trick user into clicking a link that leads to fake site. When user attempts to log on with account information, hacker records username & password & n tries that information on real site.

Hijack attack

In a hijack attack, a hacker takes over a session between you & another individual & disconnects other individual from communication. You still believe that you are talking to original party & may send private information to hacker by accident.

Spoof attack

Spoof attack In a spoof attack, hacker modifies source address of packets he or she is sending so that y appear to be coming from someone else. This may be an attempt to bypass your firewall rules.

Buffer overflow

A buffer overflow attack is when attacker sends more data to an application than is expected. A buffer overflow attack usually results in attacker gaining administrative access to system in command prompt or shell.

Exploit attack

In this type of attack, attacker knows of a security problem within an operating system or a piece of software & leverages that knowledge by exploiting vulnerability.

Password attack

An attacker tries to crack passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, & a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. A brute-force attack is when attacker tries every possible combination of characters.

[III] CRYPTOGRAPHY

In cryptography, **encryption** is process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies message content to interceptor. In an encryption scheme, intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt message without possessing key, but, for a well-designed encryption scheme, large computational resources & skill are required. An authorized recipient can easily decrypt message with key provided by originator to recipients, but not to unauthorized interceptors.

Types of encryption

Symmetric key encryption

In symmetric-key schemes, encryption & decryption keys are same. Communicating parties must have same key before they can achieve secure communication.

Public key encryption

In public-key encryption schemes, encryption key is published for anyone to use & encrypt messages. However, only receiving party has access to decryption key that enables messages to be read. Public-key encryption was first described in a secret document in 1973;[5] before then all encryption schemes were symmetric-key (also called private-key).A publicly available public key encryption application called Pretty Good Privacy (PGP) was written in 1991 by Phil Zimmermann, & distributed free of charge with source code; it was purchased by Symantec in 2010 & is regularly updated.

USES OF ENCRYPTION

Encryption has long been used by military & governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, & 53% utilized encryption for some of their data in storage. Encryption can be used to protect data "at rest", such as information stored on computers & storage devices. In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them should physical security measures fail. Digital rights management systems, which prevent unauthorized use or reproduction of copyrighted material & protect software against reverse engineering, is another somewhat different example of using encryption on data at rest.

Encryption is also used to protect data in transit, for example data being transferred via networks, mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices & bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. Data should also be encrypted when transmitted across networks in order to protect against eavesdropping of network traffic by unauthorized users.

[IV] SOCKET PROGRAMMING IN JAVA

The term *network programming* refers to writing programs that execute across multiple devices (computers), in which devices are all connected to each other using a network.

The java.net package of J2SE APIs contains a collection of classes & interfaces that provide low-level communication details, allowing you to write programs that focus on solving problem at hand.

The java.net package provides support for two common network protocols:

- **TCP:** TCP stands for Transmission Control Protocol, which allows for reliable communication between two applications. TCP is typically used over Internet Protocol, which is referred to as TCP/IP.
- **UDP:** UDP stands for User Datagram Protocol, a connection-less protocol that

allows for packets of data to be transmitted between applications.

Sockets provide communication mechanism between two computers using TCP. A client program creates a socket on its end of communication & attempts to connect that socket to a server.

When connection is made, server creates a socket object on its end of communication. client & server can now communicate by writing to & reading from socket.

The java.net.Socket class represents a socket, & java.net.ServerSocket class provides a mechanism for server program to listen for clients & establish connections with them.

The following steps occur when establishing a TCP connection between two computers using sockets:

- The server instantiates a ServerSocket object, denoting which port number communication is to occur on.
- The server invokes accept() method of ServerSocket class. This method waits until a client connects to server on given port.
- After server is waiting, a client instantiates a Socket object, specifying server name & port number to connect to.
- The constructor of Socket class attempts to connect client to specified server & port number. If communication is established, client now has a Socket object capable of communicating with server.
- On server side, accept() method returns a reference to a new socket on server that is connected to client's socket.

After connections are established, communication can occur using I/O streams. Each socket has both an OutputStream & an InputStream. client's OutputStream is connected to server's InputStream, & client's InputStream is connected to server's OutputStream.

TCP is a twoway communication protocol, so data can be sent across both streams at same time. There are following usefull classes providing complete set of methods to implement sockets.

[V]OBJECTIVE OF RESEARCH

1. Analyzing threats to Network Security.
2. Study of existing security mechanisms.
3. Study of loop hole of existing Security Mechanisms.
4. To enhance network security by merging IP Filter with cryptography.
5. Study of socket programming mechanism to write secure protocol using cryptography API & IP Detection mechanisms.
6. To develop socked based network client & server module to simulate research.

[VI] SCOPE OF RESEARCH

Such system would be more secure & would help in reducing loop hole of existing security mechanisms. Unauthentic person would be unable to decrypt data as IP Address of person would be confirmed before decryption. Server & client both sides would be programmed using socket programming. So due to presence of our own secure protocol cryptanalyst would be unable to decrypt data even if he has stolen Decryption Key.

REFERENCE

[1] David Pointcheval, Olivier Blazy, *New Smooth Projective Hash Functions & One-Round Authenticated Key Exchange*(18_22 august 2013, Santa Barbara, California, USA), Springer-Verlag, LNCS 8042, pages 449_475.

[2] David Pointcheval, Olivier Blazy, *Effcient UC-Secure Authenticated Key-Exchange for Algebraic Languages*(26 February - 1 March 2013, Nara, Japan)), 16th International Conference on Practice & Theory in Public-Key Cryptography (PKC '13)Springer-Verlag, Kaoru Kurosawa Ed., Springer-Verlag, 2013.

[3] David Pointcheval, *Password-based Authenticated Key Exchange.* (21-23 may 2012, Darmstadt, Germany)Springer-Verlag, LNCS 7293, pages 390-397.

[4] David Pointcheval, Michel Abdalla, *Contributory Password-Authenticated Group Key Exchange with Join Capability*, (February 14-18, 2011, San Francisco, CA, USA), A. Kiayias Ed. Springer-Verlag, LNCS 6558, pages 142-160.

[5] David Pointcheval, Xavier Boyen, *Strong Cryptography from Weak Secrets*, (3 – 6 may 2010, Stellenbosch, South Africa), D. Bernstein & T. Lange Eds., Springer-Verlag, LNCS 6055, pages 297–315.

[6] David Pointcheval, Michel Abdalla, *Flexible Group Key Exchange with On-Demand Computation of Subgroup Keys*, (3-6 May 2010, Stellenbosch, South Africa)), D. Bernstein & T. Lange Eds., Springer-Verlag, LNCS 6055, pages 351-368.

[7] David Pointcheval, Michel Abdalla, *Distributed Public-Key Cryptography from Weak Secrets*, (18_20 march 2009, Irvine, CA, USA), S. Jarecki & G. Tsudik Eds. Springer-Verlag, LNCS 5443, pages 139_159.

[8] David Pointcheval, Michel Abdalla, *Password-Authenticated Group Key Agreement with Adaptive Security & Contributiveness*, (21 – 25 june 2009, Gammarth, Tunisia) B. Preneel Ed., Springer-Verlag, LNCS 5580, pages 254–271.

[9] Rafael Álvarez, Leandro Tortosa, *Analysis & design of a secure key exchange scheme*, Information Sciences 179 (2009) , Elsevier

[10] David Pointcheval, Michel Abdalla, *Anonymous & Transparent Gateway-based Password-Authenticated Key Exchange* , December 2–4, 2008, Hong-Kong, China – M. Franklin, L. Hui & D. Wong Eds. Springer-Verlag, LNCS 5339, pages 133–148.

[11] Emmanuel Bresson, Olivier Chevassut, & David Pointcheval, *Provably-Secure Authenticated Group Diffie-Hellman Key Exchange*, ACM Transactions on Information & System Security, Vol. 10, No. 3. August 2007.