Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 7, July 2017, pg.138 – 146

Review: Network Security Mechanisms and Cryptography

Mohammad Tanveer Khan

Assistant Professor Computer Applications, ICSC, University of Kashmir, Srinagar, India

Jimmy_comp@yahoo.com

Abstract- As Information Technology becomes ever more prevalent in nearly every aspect of our lives especially with the emergence of ecommerce applications and social networks, the amount of data generated and stored continues to grow at an astounding rate which necessitates the improved data security mechanisms in ensuring the safe transmission of data across the networks. Security is a field of significance that consists of the provisions made in underlying computer network infrastructure, mechanisms and policies adopted to protect the network and the network-accessible resources from unauthorized access and the effectiveness of these measures combined together. Network security refers to all the features, characteristics, measures, operational procedures, protocols and administrative and management policies and practices required to monitor an unauthorized access and to provide an acceptable level of protection for data transmission across the network and at the same time preserve the integrity, availability and confidentiality of information. With the advent of the digital information age and advancements in communications and eavesdropping technologies, cyber crimes have increased proportionally and thus there is an overwhelming need to protect the information in computer systems and networks using cryptographic techniques. Network security covers the use of cryptographic algorithms in network protocols and network applications.

This paper concentrates on reviewing the various network security and cryptographic concepts and discusses the range of cryptographic algorithms and other security mechanisms that are adopted to prevent any attempt to destroy, expose, alter, steal information or gain unauthorized access to a system in a network.

Keywords- Network security, cybercrimes, cryptography, cryptanalysis, firewalls.

1. Introduction

Network Security & Cryptography is a concept to protect data transmission across the network. A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware components. All these components work together to increase the overall security of the computer network. The study of security in computer networks is rapidly growing area of interest [1, 2].

Network security [5] consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

Cryptography is the science of converting plain text into secret code. More generally, it is about constructing and analyzing protocols that block adversaries [3]. Various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation [4] are central to modern cryptography. Modern cryptography is the combination of the disciplines of mathematics, and computer science. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Techniques used for decrypting a message without any knowledge of the encryption details fall into the area of cryptanalysis. the art or process of deciphering coded messages without knowing the key. The areas of cryptography and cryptanalysis together are called cryptology. Encryption is the process of converting ordinary information (called plaintext) into unintelligible text (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. Cryptosystem is the ordered list of elements of finite possible plaintexts, finite possible cipher texts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. This paper reviews various network security services and cryptographic approaches that are currently being used across the networks. In this paper sections are organized as follows:

Section 2 gives the idea about types of security attacks. Section 3 deals with security services. Section 4 describes the various cryptography mechanisms. Section 5 shows network and internet related security approach. Intrusion Detection Systems are discussed in section 6. Firewalls technique is provide in section 7. Section 8 concludes the paper.

2. Types of Security Attacks

Network security attacks can be classified into two types :

2.1. Passive Attacks

This type of attacks includes observation or monitoring of communication. A passive attack attempts to learn or make use of information from the system but does not affect system resources. The goal of the opponent is to obtain information that is being transmitted. Types of passive attacks:

a) *Traffic Analysis*: The message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.

b*) Release of Message Contents*: Read contents of message from sender to receiver.

2.2. Active Attacks

An active attack attempts to alter system resources or affect their operation. It involves some modification of the data stream or the creation of a false stream. Types of active attacks:

a) *Modification of Messages:* some portion of a legitimate message is altered, or that messages are delayed or reordered.

b) *Denial of Service*: An entity may suppress all messages directed to a particular destination.

c) *Replay*: It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

d) *Masquerade:* It takes place when one entity pretends to be a different entity.

3. Network Security Services

It is a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. It enhances the security of data processing and transferring.

3.1. Data Integrity

It can apply to a stream of messages, a single message, or selected fields within a message. A loss of integrity is the unauthorized modification or destruction of information.

3.2. Data Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

3.3. Authenticity

Provide authentication to all the node and base station for utilizing the available limited resources. It also ensures that only the authorized node can participant for the communication.

3.4. Non-repudiation

Non-repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

3.5. Access Control

Access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

4. Cryptography Mechanisms

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling plaintext message (ordinary text, sometimes referred to as plaintext) into ciphertext (a process called encryption), then back again (known as decryption). There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below.

4.1. Symmetric cryptosystems:

In symmetric cryptosystems (also called conventional, secret-key or one-key cryptosystems), the enciphering and deciphering keys are either identical or simply related, i.e one of them can be easily derived from the other. Both keys must be kept secret, and if either is compromised further secure communication is impossible. Keys need to be exchanged between users, often over a slow secure channel, for example a private courier, and the number of keys can be very large, if every pair of users requires a different key, even for a moderate number of users, i.e. n(n — l)/2 for n users. This creates a key-distribution problem which is partially solved in the asymmetric systems. Examples of symmetric systems are the data encryption standard (DES) [8] and rotor ciphers.

4.2 Asymmetric cryptosystems:

There are practical problems associated with the generation, distribution and protection of a large number of keys. A solution to this key-distribution problem was suggested by Diffie and Hellman in 1976 [6]. A type of cipher was proposed which uses two different keys: one key used for enciphering can be made public, while the other, used for deciphering, is kept secret. The two keys are generated such that it is computationally infeasible to find the secret key from the public key. If user A wants to communicate with user B, A can use B's public key (from a public directory) to encipher the data. Only B can decipher the ciphertext since he alone possesses the secret deciphering key. The scheme described above is called a public-key cryptosystem or an asymmetric cryptosystem [7]. If asymmetric algorithms satisfy certain restrictions, they can also be used for generating so-called digital signatures [9]. Examples of Asymmetric systems are ElGamal, Diffie–Hellman key exchange, RSA etc.

4.3. Hash Functions:

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. A hash function H accepts a variable-length block of data M as input and produces a fixed-size hash value h = H(M) as shown in Figure 6. In general terms, the principal object of a hash function is data integrity. A change to any bit or bits in results, with high probability, in a change to the hash code. Virtually all cryptographic hash functions involve the iterative use of a compression function. The compression function used in secure hash algorithms falls into one of two categories: a function specifically designed for the hash function or an algorithm based on a symmetric block cipher. SHA and Whirlpool [10] are examples of these two approaches, respectively.

The hash algorithm involves repeated use of a compression function, f, that takes two inputs (an -bit input from the previous step, called the chaining variable, and a -bit block) and produces an -bit output. At the start of hashing, the chaining variable has an initial value that is specified as part of the algorithm. The final value of the chaining variable is the hash value. It is seen that b > n. A cryptographic hash function can be used to construct a pseudorandom function (PRF) or a pseudorandom number generator (PRNG). Secure Hash Algorithm (SHA) is a family of cryptographic hash functions.

5. Network and Internet Security

Internet security is a tree branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules, design policies and measures to use against attacks over the Internet. External attackers gain access to network resources mostly through the internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as malware, trojans, and phishing. Different methods have been used to protect the transfer of data across the network, including data encryption. Network security involves the authorization of access to data in a network, maintaining the integrity as well as protecting and overseeing operations being done using both hardware and software technologies. Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls.

Types of Network Security:

5.1. Wireless Network Security:

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WAP security is primarily provided by the Wireless Transport Layer Security (WTLS), which provides security services between the mobile device (client) and the WAP gateway to the Internet. There are several approaches to WAP end-to-end security. One notable approach assumes that the mobile device implements TLS over TCP/IP and the wireless network supports transfer of IP packets. Two important WTLS concepts are the secure session and the secure connection, which are defined in the specification as:

a) *Secure connection*: A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session. Between any pair of parties (applications such as HTTP on client and server), there may be multiple secure connections. In theory, there may also be multiple simultaneous sessions between parties, but this feature is not used in practice.

b) *Secure session*: An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection. There are a number of states associated with each session. Once a session is established, there is a current operating state for both read and write (i.e., receive and send). In addition, during the Handshake Protocol, pending read and write states are created. Upon successful conclusion of the Handshake Protocol, the pending states become the current states.

5.2 IP Security:

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec is said to be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol. IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. IPsec protects any application traffic over an IP network. Applications can be automatically secured by IPsec at the IP layer.

5.3 Transport-Level Security:

Transport-Level Security (TLS) is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL. Secure Socket Layer (SSL) provides security services between TCP and applications that use TCP. The Internet standard version is called Transport Layer Service (TLS). The TLS Record Format is the same as that of the SSL Record Format. SSL/TLS provides confidentiality using symmetric encryption and message integrity using a message authentication code. SSL/TLS includes protocol mechanisms to enable two TCP users to determine the security mechanisms and services they will use. HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server. Secure Shell (SSH) provides secure remote logon and other secure client/server facilities. The SSH Connection Protocol runs on top of the SSH Transport Layer Protocol and assumes that a secure authentication connection is in use. All types of communication using SSH, such as a terminal session, are supported using separate channels.

6. Intrusion-Detection systems

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

There are basically two types of intrusion-detection systems (IDS):

a) Host-based IDS
b) Network-based IDS

- *Host-based IDS:* These systems are installed on a particular important machine (usually a server or some important target) and are tasked with making sure that the system state matches a particular set baseline. For example, the popular file-integrity checker Tripwire is run on the target machine just after it has been installed. It creates a database of file signatures for the system and regularly checks the current system files against their known safe signatures. If a file has been changed, the administrator is alerted. This works very well because most attackers will replace a common system file with a trojaned version to give them backdoor access.
- *Network-based IDS:* These systems are more popular and quite easy to install. Basically, they consist of a normal network sniffer running in promiscuous mode. (In this mode, the network card

picks up all traffic even if it is not meant for it.) The sniffer is attached to a database of known attack signatures, and the IDS analyzes each packet that it picks up to check for known attacks. For example, a common Web attack might contain the string /system32/cmd.exe? in the URL. The IDS will have a match for this in the database and will alert the administrator.

Newer versions of IDS support active prevention of attacks. Instead of just alerting an administrator, the IDS can dynamically update the firewall rules to disallow traffic from the attacking IP address for some amount of time. Or the IDS can use "session sniping" to fool both sides of the connection into closing down so that the attack cannot be completed.

Unfortunately, IDS systems generate a lot of false positives. A false positive is basically a false alarm, where the IDS sees legitimate traffic and for some reason matches it against an attack pattern. This tempts a lot of administrators into turning them off or even worse -- not bothering to read the logs. This may result in an actual attack being missed.

This might be totally missed by the IDS. Furthermore, an attacker could split the attack into many packets by fragmenting the packets. This means that each packet would only contain a small part of the attack, and the signature would not match. Even if the IDS is able to reassemble fragmented packets, this creates a time overhead and since the IDS has to run at near real-time status, they tend to drop packets while they are processing. IDS evasion is a topic for a paper on its own.

The advantage of network-based IDS is that it is very difficult for an attacker to detect. The IDS itself does not need to generate any traffic, and, in fact, many of them have a broken TCP/IP stack so that they don't have an IP address. Thus the attacker does not know whether the network segment is being monitored or not.

7. Firewalls

In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted. Firewalls impose restrictions on incoming and outgoing Network packets to and from private networks. Network firewalls filter traffic between two or more networks; they are either software appliances running on general purpose hardware, or hardware-based appliances. They can also serve as the platform for IPsec. Using tunnel mode capability, firewall can be used to implement VPNs. Firewalls can also limit network exposure by hiding the internal network system and information from the public Internet. A firewall may be designed to operate as a filter at the level of IP packets, or may operate at a higher protocol layer. Firewalls can be categorized into following types:

- *Packet-filtering firewalls* or Network layer (Layer 3) firewalls make decisions based on the source and destination addresses and ports in IP packets. This basic form of firewall protection is really no more than a simple sorting algorithm. Generally they enable you to have some control through the use of access lists. Packet filtering can also often be performed by other network devices such as routers and is generally what you get when you download free firewall software. This type of firewall has little or no logging capability, making it difficult to determine if it’s been attacked.

- *Circuit-level gateways* monitor the TCP handshaking going on between the local and remote hosts to determine whether the session being initiated is legitimate -- whether the remote system is considered "trusted." They don't inspect the packets themselves, however.

- *Stateful inspection firewalls* on the other hand, these firewalls not only examine each packet, but also keep track of whether or not that packet is part of an established TCP session. This offers more security than either packet filtering or circuit monitoring alone, but exacts a greater toll on network performance.

- *Application-level gateways (proxies)* combine some of the attributes of packet-filtering firewalls with those of circuit-level gateways. They filter packets not only according to the service for which they are intended (as specified by the destination port), but also by certain other characteristics such as HTTP request string. A system establishes a connection to the proxy, which serves as an intermediary, and initiates a new network connection on behalf of the request. This prevents direct connections between systems on either side of the firewall and makes it harder for an attacker to discover where the network is, because they don't receive packets created directly by their target system. While application-level gateways provide considerable data security, they can dramatically impact network performance.

- *Multilayer inspection firewalls* combine packet filtering with circuit monitoring, while still enabling direct connections between the local and remote hosts, which are transparent to the network. They accomplish this by relying on algorithms to recognize which service is being requested, rather than by simply providing a proxy for each protected service. Multilayer firewalls work by retaining the status (state) assigned to a packet by each firewall component through which it passes on the way up the protocol stack. This gives the user maximum control over which packets are allowed to reach their final destination, but again affects network performance, although generally not so dramatically as proxies do. While inspection firewalls are the most secure, they are also rather complex and the most likely to be misconfigured.

8. Conclusion

With the rapid growth in the Internet, network data security has become an inexorable concern for any individual or organization whose internal private network is connected to the Internet. The security for the data has become highly important and the user’s data privacy across the network is a central question. Use of cryptographic techniques to secure data across networks is gaining more importance and with more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. Cryptography, along with suitable communication protocols, can provide a high degree of protection in digital communications against intruder attacks as far as the communication between two different computers is concerned. In an increasingly sophisticated threat environment, organizations need to ramp up their network security beyond existing security mechanisms. The paper presented various schemes which are used for the purpose of network security. In current scenario there are number of ways, which guarantee for the safety and security of the network but it cannot be said that they will be everlasting. Network security is a continuous process and demands regular network analysis, testing and maintenance. Furthermore there is a prominent need for continuously upgrading the security protocols, policies, mechanisms and their dynamic adaptation to cope with the evolving security threats.

References

[1] IEEE Journal on Selected Areas in communications, Special issue on Secure Communications, vol. SAC-7,May 1989.

[2] IEEE Network Magazine, Special issue on Network Security, vol. 1, April 1987.

[3] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography. p. 10.

[4] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. “A. Handbook of Applied Cryptography”. ISBN 0-8493-8523-7.

[5] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317-323.

[6] Diffie, W., and Hellman, M.: 'New directions in cryptography', IEEE Trans., 1976, IT-22, pp. 644-654.

[7] Simmons, G.J.: 'Symmetric and asymmetric encryption', ACM Comput. Surveys, 1979, 11, pp. 305-330.

[8] Data encyption standard, FIPS PUB 46, National Bureau of Standards,Washington, DC Jan. 1977.

[9] Rivest, R.L., Shamir, A., and Adleman, L: 'A method for obtaining digital signatures and public-key cryptosystems', Communication of the ACM, 1978, 21, pp. 120-126.

[10] M. Lamberger, F. Mendel, C. Rechberger, V. Rijmen, M. Schlaer, \Rebound distinguishers: results on the full Whirlpool compression function," Advances in Cryptology, Proceedings Asiacrypt'09, LNCS 5912, M. Matsui, Ed., Springer, Heidelberg, 2009, pp. 126-143.

Mohammad Tanveer Khan is currently working as assistant professor in computer Applications at ICSC, University of Kashmir, India. He received Master’s degree in computer science from Technology, New Delhi India. (NIELIT) in 2005 and is currently pursuing Ph.D. in computer science from NOIDA International university, India. His major research interest is in programming, computer networking and security.