Network Security And Cryptography-A Study

Juveria, Tanvir A. Abbasi
Assistant Professor[1], Professor[2]
COMM-IT Career Academy
Affiliated to GGSIP University, New Delhi, India

Abstract - Internet is very useful for everyone because it is the superhighway of information. The cost of Internet has been reduced over-time and the cost of the computer system, modem and other associated hardware is also reduced. In case computer is not available, one can browse internet over the smart phones. All major smart-phones support browsing functionality. In recent era, social networking has become a foremost activity in the Internet today, attracting hundreds of millions of users, spending billions of minutes on such services. Protecting the data in internet is a crucial activity where computing is ubiquitous and information systems are interconnected globally. Network security plays an important role in protecting the data from hackers. This paper focuses on various types of network security and cryptographic techniques.

Keywords - Network Security, Cryptography, CIA Triad, DES, AES, RSA, DSS

I. Introduction

Network security is an organization's policy and provisions for ensuring the security of its assets and all network traffic. It includes both software and hardware technologies. Network security is a process of integrating multiple layers of defenses in the network. Various policies are implemented by each network security layer. Access to networks is gained by authorized users, whereas, unauthorized users are blocked from executing threats and exploits. Enforcement concerns analyzing all network traffic flows and should aim to preserve the confidentiality, integrity, and availability of all systems and networks. These three principles compose the CIA triad:

Confidentiality: When we talk about confidentiality of information, we are talking about not to allow the information to be used by unauthorized persons. Confidentiality is basically the protection of information from unauthorized access. Confidentially is actually an important component of privacy that is implemented to protect sensitive data from unauthorized access.

In today's world information has values, especially, information of bank accounts, personal information, credit card details, other important secrets, and official documents. Mostly officials have information which they want to keep a secret. Information security is basically a very important part of protecting the information from unauthorized access.

By using encryption techniques information can be protected from unauthorized access. With the encryption techniques one can ensures that only the right people will be able to read the information. However there are other ways also to protect the confidential information from unauthorized access.

Integrity: Sometimes an unauthorized person can change or modify the secret information. Integrity refers to the same. Integrity is maintaining and assuring the accuracy and completeness of sensitive information. Integrity of information is ensuring that information is protected from modification by unauthorized users. This ensures that the data cannot be modified or altered in any unauthorized manner. Unauthorized access to modify the information should be avoided. The information is useful if it has correct values. If somebody by any means modifies the information than it may be of no use. Hence it is very important to protect the information from modification or alteration by unauthorized users. Tempering of information can be avoided for this, cryptographic techniques may be used.

Availability: Availability refers to ensure timely and consistent access to, and use of information by authorized user whenever is required. For any information system to serve its purpose, its very important that the information must be available when it is required. This means that the data is stored in computing systems properly and process the information, the security controls used to protect it, and the communication channels used to access it are functioning properly.

The parties for whom the information is sent be able to access the information when needed. This phenomenon is referred to as availability of information. Availability of information ensures that authorized parties are able to access the information when they are in need of the same and the information is available for them for use by them when they require.

It is very important that the information is available to the authorized person for use when they are in need of the same. It has value when the information is available for the right time to the right person. If it is not available to the right person when required than the information has no meaning.

II. Types of Network Security

1. **Access control:** Access control is a security technique that regulates who can view or use resources in systems or networks. Access control systems perform identification, authentication and authorization of users by evaluating required login credentials such as passwords, personal identification numbers (PINs), biometric scans, security tokens etc.

2. **Antivirus and Antimalware Software:** Antivirus software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and systems. Antivirus software was designed to detect and remove viruses from computers, can also protect against a wide variety of threats. Antimalware is a type of software program designed to prevent, detect and remove malicious software on systems, as well as individual computing devices.
3. **Application Security:** Application security is a practice of adding features or functionality to software to prevent different types of threats. These include denial of service attacks and other types of attacks. Application security is one of several levels of security that is used to protect IT systems.
4. **Behavioral Analytics:** Behavioral analytics is an area of business analytics which focus on finding out how and why people behave the way they do when using ecommerce platforms, social media sites, online games and other applications to identify opportunities to optimize in order to realize specific business outcomes.
5. **Data Loss Prevention (DLP):** Data loss prevention is a set of tools that are used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. Data loss prevention is a strategy for making sure that users do not send sensitive information outside the corporate network. The term is also used to describe software products that help a network administrator to control what data end users can transfer outside the network.
6. **Email Security:** Email security is a method of keeping sensitive information in email communication and accounts secure against unauthorized access. Email is a popular medium for the spread of malware, spam, phishing attacks etc.
7. **Firewalls:** A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on pre-planned security rules. A firewall typically establishes a barrier between an authorized internal network and unauthorized external network.
8. **Intrusion Prevention Systems:** An Intrusion Prevention System (IPS) is a network security prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. An intrusion prevention system is typically located between a company's firewall and the rest of its network and may have the ability to stop any malicious traffic from getting to the rest of the network.
9. **Network Segmentation:** Network segmentation involves partitioning a network into smaller networks. The aim of network segmentation is to restrict the level of access to sensitive information, hosts and services. To be effective, network segmentation must be carefully planned, robustly enforced, closely monitored and be unable to be bypassed.
10. **Security Information and Event Management (SIEM):** SIEM is a combination of SIM (Security Information Management) and SEM (Security Event Management) functions into one security management system. The underlying principle of every SIEM system is to collect relevant data from multiple sources, identify deviations and take appropriate action.
11. **VPN (Virtual Private Network):** A virtual private network is a technology that creates an encrypted connection over a less secure network, such as the internet. VPN technology is a technique which was developed to allow remote users to securely access corporate applications and other resources.
12. **Web Security:** Web security is the process of securing confidential data from unauthorized access. Security threats can compromise the data stored by an organization with malicious intentions try to gain access to sensitive information. Web Security is a branch of information security that deals with security of websites, web applications and web services.
13. **Wireless Security:** Wireless security primarily protects a wireless network from unauthorized access. Wireless security is delivered through wireless devices such as a wireless router/switch etc. that encrypts and secures all wireless communication. Wireless intrusion detection and prevention system has a provision that enable protection of a wireless network by alerting the wireless network administrator in case of a security breach.

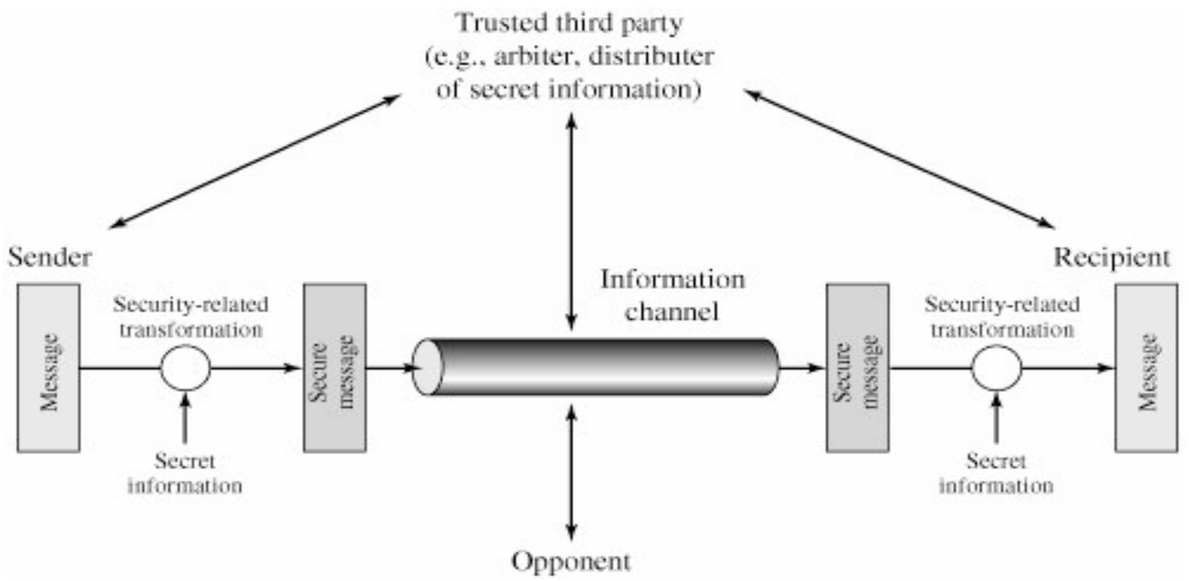
III. A Model for Network Security

A message is to be transferred from one party to other party through internet. The two parties, who are the principals, must cooperate for the exchange to take place. A channel is established by defining a route from source to destination and by the cooperative use of communication protocols by the two principals.

Techniques for providing security:

• A security-related transformation on the message to be sent. Message should be encrypted by key so that it is indecipherable by the opponent.

• An encryption key used in combination with the transformation to encrypt the message before transmission and decrypt it on reception.



Model for Network Security

Four basic tasks in designing a security service:

1. First of all, design an algorithm for performing the security-related transformation.
2. Generate the secret information.
3. Develop methods for the distribution of the secret information.
4. A protocol to be used by the two principals that makes use of the security algorithm and the secret information.

Cryptography

Cryptography is a technique for encoding message in an encoded form so that only intended receiver can read and process it.

Objectives of Cryptography:

1. **Confidentiality**: Confidentiality is used to make sure that the message can be understood for whom it was intended. The system is designed in such a way that the sensitive information is protected from reaching the wrong people.
2. **Integrity:** It means maintaining the consistency of data accuracy, of data over its entire life cycle. The message cannot be altered in transmission between sender and intended receiver without the alteration being detected.
3. **Non-repudiation**: The sender of the message cannot deny his or her intention in the transmission of the message.
4. **Authentication**: The sender and intended receiver can confirm each other's identity and the origin of the message.

IV. TYPES OF CRYPTOGRAPHIC ALGORITHMS

Most commonly used algorithms for cryptography are Secret Key Cryptography and Public Key Cryptography.

Secret Key Cryptography (SKC): Uses a single key for encryption as well as for decryption; normally used for privacy and confidentiality sometimes it is also known as symmetric encryption. The most popular symmetric key algorithms are Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

A symmetric encryption has five components:

- **Plaintext:** Plaintext is the original message that is fed into the algorithm as input.
- **Encryption Algorithm:** The encryption algorithm performs several substitutions and transformations on the plaintext.
- **Secret key:** A secret key is input to the algorithm. It is used for encryption and decryption.
- **Ciphertext**: Ciphertext is an encrypted message produced as output. Ciphertext depends on the plaintext and the secret key. For a message, two distinct keys will produce two different ciphertexts.
- **Decryption Algorithm:** Decryption algorithm accepts the ciphertext and the same secret key and produces the plaintext.

Data Encryption Standard (DES): The most widely used encryption scheme is Data Encryption Standard. This algorithm is also referred as Data Encryption Algorithm. In this algorithm, the plaintext is 64 bits in length and the key is 56 bits in length .From the original 56- bit key, 16 subkeys are generated, one of which is used for each round. The process of decryption in DES is same as the encryption process. The rule is: Use the ciphertext as input to the DES algorithm, but use the subkeys in reverse order.

Triple DES (3DES): The **Triple** Data Encryption Standard (3DES) is a symmetric-key block cipher, which applies the **DES** cipher algorithm three times to each data block. It is also known as **Triple** Data Encryption Algorithm (TDEA or **Triple**DEA). The triple DES uses three keys and three executions of the DES algorithm.

The function for encryption is:

$C=E\ (K_3, D\ (K_2, E\ (K_1, P)))$

The decryption is same as encryption with the keys reversed. The decryption function is:

$P=D\ (K_1, E\ (K_2, D\ (K_3, C)))$

C=ciphertext

P=plaintext
E[K,X]=encryption of X using key K
D[K,Y]=decryption of Y using key K

Advanced Encryption Standard (AES): In Advanced Encryption Standard (AES), a symmetric block cipher with a block length of 128 bits and support for key lengths of 128,192 and 256 bits. We assume a key length of 128 bits, which is likely to be one of the most commonly implemented. The input to the encryption algorithm is a single 128-bit block and the input to decryption algorithm is also a single 128-bit block. This block represents as a square matrix of bytes. This block is copied into a state array, which is modified at each stage of encryption or decryption. After the final stage, this state is copied to an output matrix. Likewise, the 128-bit key is depicted as a square matrix of bytes. This key is expanded into an array of key schedule words: each word is four bytes and the total key schedule is 44 words for the 128-bit key.

Public Key Cryptography (PKC): In Public Key Cryptography**,** one key is used for encryption while another key for decryption; it is also called asymmetric encryption. This type of system is normally used for authentication, non-repudiation, and key exchange. PKC is also known as public key encryption, asymmetric encryption, asymmetric cryptography, asymmetric cipher and asymmetric key encryption.
A public key cryptography has six components:

- **Plaintext:** Plaintext is the readable message that is fed into the algorithm as input.
- **Encryption Algorithm:** The encryption algorithm performs several transformations on the plaintext.
- **Public key and Private key:** A pair of keys that have been selected so that if one is used for encryption and the other is used for decryption.
- **Ciphertext**: Ciphertext is an encrypted message produced as output. It depends on the plaintext and the key. For a message, two distinct keys will produce two different ciphertexts.
- **Decryption Algorithm:** Decryption algorithm accepts the ciphertext and the matching key and produces the plaintext.

RSA Algorithm: RSA (Rivest–Shamir–Adleman) is a public key encryption algorithm. RSA is an algorithm to encrypt and decrypt messages. RSA involves public key and private key. RSA is block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.
$C=M^e \bmod n$
$M=C^d \bmod n$
Sender and receiver must know the values of n and e and the receiver knows the value of d. RSA algorithm is a public key encryption algorithm with a public key of KU={e,n} and a private key of KR={d,n}.
Digital Signature Standard (DSS): Digital Signature Standard (DSS) is the digital signature algorithm (DSA) to generate a digital signature for the authentication of electronic documents. Digital signatures are generated through Digital Signature Standard. Signatures are generated in conjunction with the use of a private key and the verification takes place in reference to a corresponding public key. Each signatory has their own paired public and private keys. A signature can only be generated by an authorized person using their private key and the public key can be used by anyone to verify the signature.

V. Conclusion

The dependence on the network is increasing day by day. The E-market and other such type of business organizations are totally dependent upon the internet. Hence IT industries require smooth communication and reliable outputs on the internet. Because of increased use of internet the information technology industry must become more concerned about the possible security threats which can disturb the security that may damage or destroy the costly information. Hence some sort of network security must be used to maintain certain level of security of network. Network Security is an essential component in information security because it is responsible for securing and authorizing all information passed through networked computers. Cryptographic techniques are used to secure information from unauthorized uses.

VI. References

[1] Network Security Essentials Applications and Standards, Fourth Edition, William Stallings, Pearson
[2] https://en.wikipedia.org/wiki/Network_security
[3] "**A Brief Survey of Importance of Information Security**" published in IJEDR (International Journal of Engineering Development and Research) Volume 6 Issue 3 September 2018.
[4] "**An Overview of Intrusion Detection and Prevention System**" published in JETIR (International Journal of Emerging technologies and Innovative Research), Volume 5 Issue 10 October 2018.
[5] https://www.techopedia.com
[6] Cryptography and Network Security, Principles and Practices(4th Edition), William Stallings