IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⵘ Impact Factor 7.105 ⵘ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9741

Study of Cryptography Encryption for Network Security

Mariyam E. Maniyar

Assistant Professor, MCA Department, K. K. Wagh Institute of Engineering Education & Research, Nashik, India

Abstract: In order to provide security for network and data transmission for wireless network, cryptography and network encryption techniques are being used. One of the key aspects of wireless network data transmission is to provide data protection and security. In the wireless networks sensors are linked to the base station. The need for protecting wireless network sensor is very critical and hence encryption and network security are essential. Network security comprises security for the entire network system. Network security is important because it protects valuable data, which, when possessed by the wrong person, could end up causing a wide spectrum of problems, from inconveniences to catastrophes. An organization without adequate network security cannot function. Secure communication can be achieved through various encryption techniques viz. cryptography, digital signatures, steganography, digital watermarking etc. Cryptography is a technique of encryption used to secure information and protect the network, as various networks are related and admire attacks and intrusions. In this paper we discuss the cryptography with its aims, forms and algorithms.

Keywords: Cryptography, Network Security, Wireless Network, Encryption.

I. INTRODUCTION

Cryptography and Data encryption is a common and effective security method, a sound choice for protecting an organization’s information. In a world where cybercrimes are on the rise, it’s comforting to know that there are as many methods available to protect network security as there are ways of trying to penetrate it. The real challenge is deciding which techniques an internet security expert should employ that best suits their organization’s specific situation.
Computer data moves from one node to another node. When the data is transmitted outside the network, intruders or attackers can alter or forge the original data. Data encryption and cryptography can in turn secure the original data. The technology is built on secret codes, which are enhanced by modern mathematics that powerfully protect our data.

- Computer Security: Computer security is the protection that is set up for computer systems and keeps critical information from unauthorized access, theft, or misuse. There are various practices in place that are widely in use, mainly for the protection of computer systems and networks and preventing potential malicious activities.
- Internet Security: Internet security is a term that describes security for activities and transactions made over the internet. It is a component of the larger ideas of cybersecurity and computer security, involving browser security, online behaviour and network security.
- Information Security: Information security ensures good data management. It involves the use of technologies, protocols, systems and administrative measures to protect the confidentiality, integrity and availability of information.
- Security attack: In computer networks and systems, security attacks are generally classified into two groups, namely active attacks and passive attacks. Passive attacks are used to obtain information from targeted computer networks and systems without affecting the systems.
- Security mechanisms: Security mechanisms are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service. Examples of common security mechanisms are as follows: Cryptography. Message digests and digital signatures.
- Security service: Network Security Services (NSS) is a collection of cryptographic computer libraries designed to support cross-platform development of security-enabled client and server applications with optional support for hardware TLS/SSL acceleration on the server side and hardware smart cards on the client side.

Basic Terminology

Cryptography: Today, cryptography is used to protect digital data. It is a division of computer science that focuses on transforming data into formats that cannot be recognized by unauthorized users. An example of basic cryptography is an encrypted message in which letters are replaced with other characters.

Plain Text: An original / intelligible message or data
Cipher text: coded message
Enciphering/Encryption: process of converting plain text to cipher text
Deciphering/ Decryption: restoring the plain text from the ciphertext
Key: the secret material used for performing encryption

II. CRYPTOGRAPHIC ATTACKS

Cryptography involves hiding the information to be transmitted so that only the receiver is able to view it. This is done by encoding the information to be sent at the sender's end and decoding the information on the receiver's end. A cryptographic attack is a method for circumventing the security of a cryptographic system by finding a weakness in a code, cipher, cryptographic protocol or key management scheme. Attacks are typically categorized based on the action performed by the attacker. An attack, thus, can be passive or active

[1]. Passive Attacks

The main goal of a passive attack is to obtain unauthorized access to the information. For example, actions such as intercepting and eavesdropping on the communication channel can be regarded as passive attack.These actions are passive in nature, as they neither affect information nor disrupt the communication channel. A passive attack is often seen as stealing information.

[2]. Active Attacks:

An active attack involves changing the information in some way by conducting some process on the information.

For example, Modifying the information in an unauthorized manner. Initiating unintended or unauthorized transmission of information. Alteration of authentication data such as originator name or timestamp associated with information unauthorized deletion of data.

Other types of attacks

[3]. Dictionary Attack

This attack has many variants, all of which involve compiling a 'dictionary'. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.

[4]. Brute Force Attack (BFA)

In this method, the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible keys is 28 = 256. The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long.

[5]. Birthday Attack

This attack is a variant of brute-force technique. It is used against the cryptographic hash function. When students in a class are asked about their birthdays, the answer is one of the possible 365 dates. Let us assume the first student's birthdate is 3rd Aug. Then to find the next student whose birthdate is 3rd Aug, we need to enquire 1.25*□√365 ≈ 25 students. Similarly, if the hash function produces 64 bit hash values, the possible hash values are 1.8×1019. By repeatedly evaluating the function for different inputs, the same output is expected to be obtained after about 5.1x109random inputs. If the attacker is able to find two different inputs that give the same hash value, it is a collision and that hash function is said to be broken.

[6]. Man in Middle Attack (MIM)

The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place. Host A wants to communicate to host B, hence requests public key of B. An attacker intercepts this request and sends his public key instead. Thus, whatever host A sends to host B, the attacker is able to read. In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to B. The attacker sends his public key as A's public key so that B takes it as if it is taking it from A.

[7]. Buffer flow attack

A buffer is a temporary space for data storage. Buffer overflow occurs if the data is stored by a program or process in a buffer is greater than the maximum capacity of the buffer. The extra data can overflow into adjacent buffer corrupting or overwriting the valid data held in them.

[8]. Ping of death attack

Ping of death attack takes advantage of a weakness in TCP-IP protocol. The weakness is that many computer system cannot handle an IP packet larger than the maximum IP packet size of 65535 bytes. Buffer overflow is occure in ping of death attack. The ping of death sends ping packet larger than 65535 bytes to the victim by fragmenting the packets, then a receiving computer reassemble the packet a buffer overflow occur which aften cause computer to crash.

[9]. DoS Attack (Denial of Service Attack)

A Denial-of-Service attack or DoS is an attack targeting the availability of web applications. Unlike other kinds of attacks, DoS attacks' primary goal is not to steal information but to slow or take down a web site. The attackers' motivations are diverse, ranging from simple fun, to financial gain and ideology (hacktivism). A denial of service attack generates high or slow rate attack traffic exhausting computing resources of a target, therefore preventing legitimate users from accessing the website.

[10]. Teardrop attack:

A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device.

III. Network Security

Network security is any activity designed to protect the usability and integrity of your network and data.

- It includes both hardware and software technologies
- It targets a variety of threats
- It stops them from entering or spreading on your network
- Effective network security manages access to the network

Network security combines multiple layers of defences at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors is blocked from carrying out exploits and threats.

Types of network security

- Firewalls: Firewalls put up a barrier between your trusted internal network and untrusted outside networks, such as the Internet. They use a set of defined rules to allow or block traffic. A firewall can be hardware, software, or both. Cisco offers unified threat management (UTM) devices and threat-focused next-generation firewalls.
- Email security: Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.
- Anti-virus and anti-malware software: "Malware," short for "malicious software," includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.
- Network segmentation: Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.
- Access control: Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).
- Application security: Any software you use to run your business needs to be protected, whether your IT staffs builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, those attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.
- Behavioural analytics: To detect abnormal network behaviour, you must know what normal behavior looks like. Behavioural analytics tools automatically discern activities that deviate from the norm. Your security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.
- Data loss prevention: Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.
- Intrusion prevention systems: An intrusion prevention system (IPS) scans network traffic to actively block attacks. Cisco Next-Generation IPS (NGIPS) appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.
- Mobile device security: Cybercriminals are increasingly targeting mobile devices and apps. Within the next 3 years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, you need

DOI: 10.17148/IARJSET.2022.9741

to control which devices can access your network. You will also need to configure their connections to keep network traffic private.

- Security information and event management: SIEM products pull together the information that your security staff needs to identify and respond to threats. These products come in various forms, including physical and virtual appliances and server software.
- VPN: A virtual private network encrypts the connection from an endpoint to a network, often over the Internet. Typically, a remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between device and network.
- Web security: A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.
- Wireless security: Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network.

IV. NETWORK SECURITY

Unauthorized access to all types of data is an ever-present risk in today's cyber world. Financial and payment system data are the most vulnerable data, which may reveal consumers' and clients' personal identifying information (PII) or payment card records. Encryption is critical for securing personally identifiable information and mitigating the threats for companies that perform payment transactions every minute of the day. This makes cryptography crucial. There are mainly two types of cryptography: symmetric and asymmetric cryptography.

Symmetric Key Cryptography: Symmetric Key Cryptography, or Symmetric Encryption, uses a secret key for both encryption and decryption. Data is translated to a format that cannot be interpreted or inspected by someone who does not have the secret key used to encrypt it during this phase.

The strength of the random number generator used to generate the secret key determines the effectiveness of this method. Symmetric Key Cryptography, commonly used on the Internet today, comprises two kinds of algorithms: Block and Stream. The Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) are two common encryption algorithms. This type of encryption is typically much faster than Asymmetric Encryption, but it allows the secret key to be held by both the sender and the data receiver.

Symmetric cryptography is based on a single shared key that all parties are aware of and can use to encrypt and decrypt data.

Symmetric key encryption employs one of the following encryption techniques:

- Stream ciphers: Encrypt a message's digits or letters one at a time.
- Block ciphers**:** Encrypt a group of bits as a single entity, inserting the plaintext to make it a block size multiple. 64-bit blocks are widely used. The NIST-approved Advanced Encryption Standard (AES) algorithm and the GCM block cipher mode of operation all use 128-bit blocks.

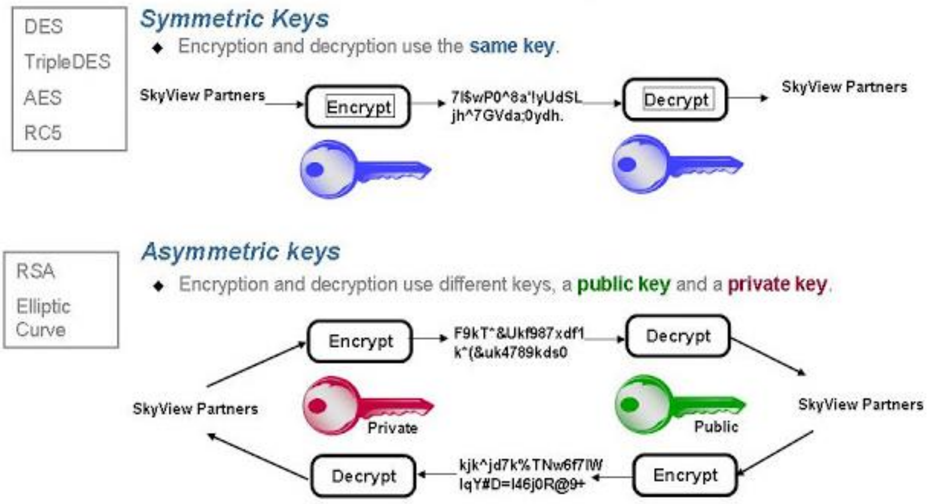

Fig 1: Symmetric Key and Asymmetric Key Encryption

DOI: 10.17148/IARJSET.2022.9741

Asymmetric Key Cryptography : Asymmetric cryptography, better known as public-key cryptography, encrypts and decrypts a message using a pair of similar keys. In asymmetric key cryptography, the private key is kept by one public key and one private key — to prevent unauthorized entry or usage. Anybody can use a public key to encrypt a document so that only the expected receiver can decrypt it with their private key. A private key or secret key is only known to the key's generator.

When anyone tries to submit an encrypted message, they will use a shared directory to retrieve the recipient's public key and use it to encrypt the message until submitting it. The message will then be decrypted by the receiver using their associated private key.

However, when the sender encrypts the message using their private key, the message may only be decrypted using the sender's public key, thus authenticating the sender. These encryption and decryption procedures are automatic; users don't need to lock and unlock the message manually.

Numerous protocols, including the transport layer security (TLS) and safe sockets layer (SSL) protocols that allow HTTPS, depend on asymmetric cryptography. Encryption is often used in browsers that need to create a stable link over an unstable network, such as the Internet, or to verify a digital signature.

The key advantage of asymmetric cryptography is increased data security. Since users are never expected to disclose or exchange their private keys, the risks of cyber activity on a user's private key during transmission are reduced.

V. Conclusion

Cryptography is a vital component for providing protection for data communication over different network. Network security is used against unauthorised users to protect data. The key can be shared more securely between sender and receiver. Data security can be preserved by using techniques like cryptography, watermarking, digital signatures, firewalls etc. The importance of secure communication has led to cryptographic systems becoming popular so that we can assume that cryptography has proven to be a key to protect our confidential information.

References

[1] Preneel, B. (2010, September). Cryptography for network security: failures, successes and challenges. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (pp. 36-54). Springer, Berlin, Heidelberg.

[2] Kumari, S. (2017). A research Paper on Cryptography Encryption and Compression Techniques. International Journal Of Engineering And Computer Science, 6(4).

[3] Bhatia, P., & Sumbaly, R. (2014). Framework for wireless network security using quantum cryptography. arXiv preprint arXiv:1412.2495.

[4] Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology, 10(5), 763- 770.

[5] Panda, M. (2014). Security in wireless sensor networks using cryptographic techniques. American Journal of Engineering Research (AJER), 3(01), 50-56.

[6] Dhamdhere Shubhangi, T., & Gumaste, S. V. Security in Wireless Sensor Network Using Cryptographic Techniques.

[7] Kumar, S. N. (2015). Review on network security and cryptography. International Transaction of Electrical and Computer Engineers System, 3(1), 1-11.

[8] Kaur, S., Kaur, R., & Raina, C. K. (2017). Review on Network Security and Cryptography.

[9] Duong, T., & Rizzo, J. (2011, May). Cryptography in the web: The case of cryptographic design flaws in asp. net. In Security and Privacy (SP), 2011 IEEE Symposium on (pp. 481- 489). IEEE.

[10] Stallings, W. (2006). Cryptography and Network Security, 4/E. Pearson Education India

[11]Analysis of Cryptography Encryption for Network Security, V. Esther Jyothi[1], Dr. BDCN Prasad[2] and Dr Ramesh Kumar Mojjada[3] , Published under licence by IOP Publishing Ltd

BIOGRAPHY

Prof. Mariyam Maniyar, Assistant Professor, Department of MCA, K. K. Wagh Institute of Engineering Education and Research, Nashik. Completed Master of Computer Application from Savitribai Phule Pune University.