International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 4 ǁ 2022 ǁ PP. 11-14

Cryptography and Network Security

Alan John Joseph
PG Department of Computer Applications and AI
Saintgits College Of Applied Science, Pathamuttom, Kottayam

Abhinand K
PG Department of Computer Applications and AI
Saintgits College Of Applied Science, Pathamuttom, Kottayam

Abstract— *As the use of computers and data networks grows, the security of data in the network becomes increasingly important. Because information has almost become one of the most valuable commodities in all aspects of life, mistake tolerance is significantly lower, making it necessary to provide effective network security and data protection. This study examines network security and its many components first, then applying the same notions to the OSI model. The basic concepts of cryptography and its classification, as well as basic nomenclature, are discussed next, followed by some of the most extensively used block cypher algorithms, as well as their working principles and logical algorithms.*

Index Terms *—cryptography, security attacks, security mechanism, security services, block ciphers, permutations ciphers, Feistal Cipher Structure, data encryption standard, substitution and transposition.*

Date of Submission: 06-04-2022 Date of acceptance: 21-04-2022

I. Introduction

Information is a basic building block in an organisation, in the same way as employees, premises and equipment. Information expresses knowledge or message in a concrete form. We can communicate information, we can store it, we can refine it and we can control processes with it - we simply need it for most of what we do. Therefore, information is valuable and needs to be protected based on the needs. Information can be valuable both for organisations and for the individual, sometimes it is even vital. If such information is lost or incorrect, it can have catastrophic consequences. Network security is thus needed to protect the information rather data, during transmission. Security of information have different goals such as confidentiality, integrity and availability. Confidentiality ensures that secret information is protected from unauthorized cover-up. Security controls focused on integrity are designed to prevent data from being changed or corrupted by an unauthorized party. A security service is something that enhances the security of the data processing systems and the information transfers of an organization. They are intended to counter security attacks. In general, they make use of one or more security mechanisms to provide the service or simulate functions normally associated with physical documents. A mechanism that is designed to detect, prevent, or recover from a security attack. No single mechanism that will support all functions required however one particular element underlies many of the security mechanisms in use which is cryptographic techniques. Any action that compromises the security of information owned by an organization is called a security attack. Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems.

II. OSI Security Architecture

The security of an organization is of utmost importance to all who work there. Cyber technology is created on the basis of safety and security. It's difficult to imagine the cyber world without considering security. As a result, security architecture is a critical part of the company. The organization's manager is responsible for all security requirements, which are met through the use of a well-organized OSI Security Architecture. The OSI Security Architecture specifies a well-thought-out standard architecture for computer networking security features. The OSI architecture is widely accepted around the world because it establishes the flow of delivering safety in an organization.
Three pillars of OSI Security Architecture:

A. Security attacks

These are actions that put an organization's safety at risk. They are further classified into 2 sub-categories:

- Passive attacks

Attacks in which a third-party intruder tries to access the message/ content/ data being shared by the sender and receiver by keeping a close watch on the transmission or eave-dropping the transmission is called Passive Attacks.

- Active attacks

Attacks in which neither the sender nor the receiver is aware that their message/data has been modified with by a third-party intruder. The message/data sent does not retain its original format and behaves in an unusual manner. This makes active attacks dangerous since the receivers is unaware that the data/message received is not from the sender because no information about the attack is provided during the communication process.

B. Security services

The OSI architecture categorizes services under five major categories:

- **Authentication** is the most basic service to ensure that desired permission is well verified and safe.
- **Access Control** ensures that only authorized users have access to the available resources.
- **Data Confidentiality** is responsible for ensuring that the data is kept extremely safe from third-party intruders.
- **Data Integrity** ensures that the transmitted information received by the receiver is well- authenticated and there is no tampering with the information received.
- **Non- repudiation** restricts the forwarding of the transmitted message by either of the parties (sender and receiver).

C. Security Mechanism

A security mechanism is a system that is designed to detect any security breach or assault on an organisation. Security Mechanisms are also in charge of ensuring that an attack may be stopped as soon as it is identified.

III. Cryptography

Cryptography is used to protect digital data. It is a division of computer science that focuses on transforming an intelligible message into one that is unintelligible, which cannot be recognized by unauthorized users. Then retransforming that message back to its original form. Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it. The original intelligible message is known as plaintext while the transformed message is called ciphertext. Cipher which is the algorithm used for the conversion, with the key which provides critical information only to the sender and receiver for the same. Enciphering is known as the conversion of plaintext to ciphertext and reverse process is known as deciphering.

Two basic methodologies of classic cryptography include substitution and transposition. Substitution is replacing of say letters, with other letters while transposition is arranging them in a different way. Ciphers can further be either monoalphabetic or polyalphabetic, implying only one substitution/transposition or more than one substitution/transposition respectively. The resultant cipher of many ciphers joined together is called the product cipher.

Cryptography is also divided into two categories: Symmetric cryptography key and Asymmetric key cryptography. Symmetric key cryptography is an encryption system where the sender and receiver of messages. In Asymmetric key cryptography a public key is used for encryption and a private key is used for decryption.

IV. Block Ciphers

Block ciphers best encrypt messages which might be the identical length as their block length, so every block of plaintext with greater or much less blocks wishes to be encrypted separately. Block ciphers system messages in into blocks, every of which is then encrypted or decrypted. It is sort of a substitution on very big characters (64-bits or more) It isn't the same as movement ciphers system messages a chunk or byte at a time while encrypting or decrypting. Majority of the modern-day ciphers are block ciphers

A. Claude Shannon and Substitution-Permutation Ciphers

In 1949, Claude Shannon delivered the concept of substitution permutation (S-P) networks which shape the premise of modern block ciphers. The substitution and permutation are delivered in this type of manner as to offer confusion and diffusion of message Diffusion dissipates the statistical form of plaintext over bulk of cipher text at the same time as confusion makes dating among cipher text and key as complex as possible. These collectively make the unique textual content difficult to understand and for that reason offer computational security.

B. Feistel Cipher Structure

It is primarily based totally on idea of invertible product cipher It first walls the enter block into halves and then:

• process through a couple of rounds which

• carry out a substitution on left facts 1/2 of primarily based totally on spherical feature of proper 1/2 of & sub key

• then have permutation swapping halves

Design Principles:

• block length growing length improves security, however slows cipher

• key length growing length improves security, makes exhaustive key looking harder, however might also additionally sluggish cipher

• wide variety of rounds growing wide variety improves security, however slows cipher

• sub key generation extra complexity could make evaluation harder, however slows cipher

• spherical feature extra complexity could make evaluation harder, however slows cipher.

C. Data Encryption Standard

DES is the most significantly normal and used block code with inside the world. It encrypts sixty-four bit statistics the use of a fifty-six-bit key. The first step is preliminary permutation. It reorders the enter statistics bits through assigning the even bits to left 1/2 of an abnormal bit to proper 1/2 of. It then applies Feistal Cipher on the two 32 bit halves. The ith little bit of left is assigned the (i-1) th little bit of proper. And the ith little bit of proper is the (i1) th little bit of left XORed with the ith little bit of key. Then eight substitution packing containers are used which map the 6 bits to four. The outer bit picks a row and the internal 4 are substituted. This outcome in eight masses of four bits and row choice relying on statistics and key. The keys used with inside the above technique are basically sub keys shaped from the preliminary key. These are shaped through first dividing the important thing into 28 bit halves after which in 16 stages rotate every 1/2 of one by one through one or locations primarily based totally on key rotation schedule. (The decryption entails the reversal of these 16 stages)

DES helps avalanche impact that's an acceptable belonging for encryption keys. An alternate in a single enter or key bit consequences in the alternate of about 1/2 of the output keys which makes it extraordinarily hard to wager keys via way of means of a few techniques. Further, as it's far a fifty-six-bit key there are 2^fifty-six exceptional possible variations which makes brute pressure seek hard. Even if it does succeed, because of preliminary permutation making experience of plaintext could now no longer be obvious. Yet for important programs the key size is taken into consideration small and as a consequence insecure. A variant to the approach is TDES wherein the algorithms is used 3 times, every with an exceptional key. This will increase the protection. Cipher Block chaining is some other approach used. The message is damaged in blocks that are related to every different in the encryption method. It makes use of a preliminary fee to begin the method. This is a superb approach as alternate in a block impacts the relaxation plus protection it multiplied via way of means of the reality that together with key, information of the preliminary fee is important to decrypt. Electronic Code Book makes use of a contrary method wherein every block is encrypted independently. Security is much less and as a consequence it's far used most effective whilst few blocks are to be transmitted.

V. Public Key Cryptography

There are two keys are used for the encryption and decryption of the data or message. One is public and the alternative is non-public. Though both of them are associated with every different mathematically, from general public key the non-public key cannot be derived. Message encrypted through the general public key can best be decrypted through a non-public key. Usually principles of variety concept and comparatively top numbers are used. Eulers Function is used to compute the pretty top numbers lesser than a given variety. Ron Rivet gave a set of rules to compute the keys as herbal numbers. Two top numbers p and q are selected and their product is N. Eulers characteristic say E(N) is then computed. A random integer e is decided on such that gcd of E and e is 1. Then d is calculated as mod(E)/e. Where mod () is the modulus characteristic. The public secret is a characteristic of N and e whilst the non-public of N and d. (Something of the type M^e*mod(N). wherein M is the message data).

Application of Cryptography

➢ Defense service

➢ Secure Data Manipulation

➢ E-Commerce

➢ Business Transactions

- Internet Payment Systems
- Pass Phrasing Secure Internet Comm.
- User Identification Systems
- Access control
- Computational Security
- Secure access to Corp Data
- Data Security

Applications of network security

University academics and corporate staff mostly used computer networks to transmit email and share printers. Security did not receive much attention under these circumstances.

However, millions of ordinary citizens today use the network for:

- Banking
- Shopping
- Filling their tax returns

VI. Conclusions

Network security is essential and you need to provide the same encryption and study different encryption and decryption methods. A variety of algorithms are available for this purpose and should be selected based on factors and parameters such as fault tolerance, data type, amount of data, and other system limitations and requirements. Block ciphers are cheap for computational convenience. There are many different conceptual methods for block ciphers. Each method has its own limitations, so you should choose one if its advantages outweigh the disadvantages. Public-key cryptography has long been popular because it has few of the drawbacks of other methods.

Reference

[1]. “Network security” by Andrew S.Tanenbaum
[2]. “Computer Networks”, by Andrew S.Tanunbaum
[3]. “Cryptography and Network Security” by William Stallings
[4]. “Applied Cryptography” by Bruce Schneier, John Willley and Sons Inc
[5]. Dr. Bill Figg. “Data Networks and Cryptography,”Dakota State University, 2000.
[6]. William Stallings “Cryptography and Internet Security," Upper Saddle River,NJ,Prentice Hall, 1999
[7]. Keith M. Martin, Everyday Cryptography (2017, 2/e; Oxford University Press).
[8]. Dieter Gollmann, *Computer Security*