Unit 1: Cyber Security Essentials

1

Unit Structure

1.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Define cyber security concepts
- Basic cryptography and its working
- Symmetric and asymmetric encryption
- Hash function and digital certificate
- Concept of public key

1.2WHAT IS CYBER SECURITY?

Cyber Security is a very complex term which passes through multi-dimensional request and response. In the current age, it is a challenging task for a small enterprise to big enterprise to secure themselves from external and internal cyber-attacks.

Cyber Security is a subset of information security which deals with securing the information, data and from both internal and external cyber threats. It is a proactive practice to safeguard the confidential information of the organization from unauthorized access by enforcing the layered security policies and protocol.

The task is more complex due to the variety of nature of cyber-attacks and the inability of quality response in the absence of adequate security measures.

The word 'Cyber' is not singular, it has its many forms to understand the concept using different terminologies such as:

- Cyber Space: It’s a virtual world of the digital data formed by bits.
- Cyber Economy: Complex structure of interconnected networked systems and its environment.

Cyber Space is a manmade ecosystem. It comprises of all interconnected networks, database, a source of information.

Cyber Space is not only including the software, hardware, data and information system, but the people surrounding it and social interaction within this network and infrastructure.

According to NIST (National Institute of Standards and Technology), Cyber Security is "The ability to protect or defend the use of cyberspace from cyber attacks."

1.3 INDIAN CYBERSPACE

The National Informatics Centre (NIC) was set up as early as 1975 with the goal of providing IT solutions to the government. Between 1986 and 1988, three Networks were set up: INDONET, connecting the IBM mainframe installations that made up India’s computer infrastructure; NICNET (the NIC Network), is a nationwide very small aperture terminal (VSAT) NW for public sector organizations as well as to connect the central government with the state governments and district administrations; and the Education and Research Network (ERNET), to serve the academic and research communities.

India is an emerging country with a large scale change in digitization and scaling in all directions in every business sector. So at a national level, it is important to have the cybersecurity policy for the smooth functioning of its critical infrastructure such as Power Grids, Water Distribution, Rail Transportation, Metro Networks, Aviation Networks, Telecommunication Systems, Financial Sector, Public and Private Organizations, Healthcare and Education Sector.

Today’s Cyber Space majority users are the citizens of the country using the interconnected networks of devices which is increasing every day. It is difficult to draw the boundary in the cyberspace among the different groups of people and data accessed by them.

So Indian Government has taken many initiatives in sectoral reforms and national level programs to create a safe cyber ecosystem which enables a user in access digital data and creates adequate trust and confidence in using them effectively and securely. Which includes Awareness programs, strengthen monitoring policy, Research, and Development in Cyber Security, Creating Open Standards, Strengthen Regulatory Framework, Protection of Critical Infrastructure.

There are various ongoing activities and programs of Government to address the current cybersecurity challenges and creating safe cyberspace and cyber economy in the country. Below are some of the key initiatives launched by **GOI (Government of India)** such as:

NATIONAL CYBER SECURITY POLICY: This is created with an objective to build secure and resilient cyberspace for the citizens, businesses, and Government. It was released in 2013.

NATIONAL CYBER SECURITY COORDINATION CENTER(NCCC): The NCCC help to perform the real-time threat assessment and create early warning signs of potential cyber threats to the country.

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTER: This was created under section 70A of the Information Technology(IT) Act. It is established as a nodal agency in respect of the critical information infrastructure protection. Its aim is to protect the critical information infrastructure against the external and internal cyber threats along with the other threats.

CYBER SWACHHTA KENDRA: It was launched in 2017 to provide a platform for users to analyze and clean their systems from Viruses, Bots, Malware, Trojans, etc. It can be accessed using the following URL: *https://www.cyberswachhtakendra.gov.in*

INDIAN COMPUTER EMERGENCY RESPONSE TEAM(CERT-IN): It is National Incident Response Centre, operated under Department of Electronics and Information technology, Ministry of Communication and Information Technology, Government of India. Its primary role is to raise the security awareness among the citizens of Indian and provide the 24 x 7 technical assistance to the different organization in handling the critical security incidents.

NATIONAL TECHNICAL RESEARCH ORGANIZATION(NTRO): NTRO has the responsibility to look after the nations critical infrastructure security such as power grids, nuclear installation security, air traffic and control, monitoring satellite communications, UAV surveillance, Oil and Gas facilities.

It has three different wings. Information domination group looks after hacking and cyber applications. Net Security Team looks after emerging cyber-attacks and its analysis and mitigations. Research Group is looking towards the monitoring and surveillance of the internet.

NATIONAL INTELLIGENCE GRID (NATGRID): It is an integrated grid of connecting different state-run databases between intelligence agencies and organization providing information to enhance India's counter-terrorism measures. NATGRID would collect and collate information from different databases such as tax and bank account details, credit card information, visa and immigration records, itineraries of rail and air travel.

Combined data will be made available to 11 central agencies which are Research and Analysis Wing, Intelligence Beauro, Central Bureau of Investigation, Financial Intelligence Unit, Central Board of Direct Taxes, Directorate of Revenue Intelligence, Enforcement Directorate, Narcotics Control Board, Central Board of Excise and Customs and Directorate General of Excise and Customs.

Now below we will look at some fundamental concepts of principles of cybersecurity. Essentially in the following chapters, we will also learn more in detail regarding the Cyber Attacks, Vulnerability and Threats.

1.4SECURITY CONCEPTS

Information content & information determinacy determine the type of software applications. Content refers to input & output data, determinacy refers to the predictability of order & timing of information

There are three different tools which are useful for system designers to make a robust and secure product i.e. Confidentiality, Integrity, and Availability.

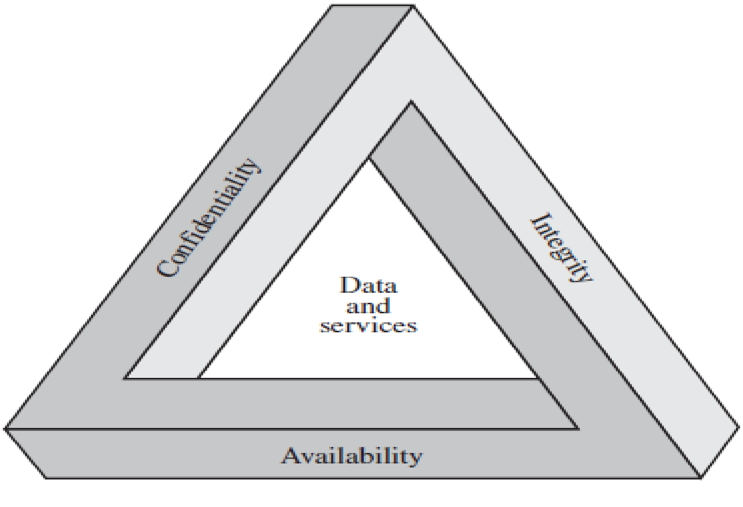

Figure 1 CIA Triad

In the above image, there are three key concepts shown and all three are related to each other, which is known as the CIA triad, it is considered to be the main pillars of the security, which anyone who protects an information system must understand: Confidentiality, Integrity, and Availability. Each component is critical to overall security, with the failure of any one component resulting in potential system compromise.

Confidentiality: It means to protect personal privacy information from unauthorized access to devices, processes or individuals. If we understand it in the parts, it can be described as Information must have protection enable from the different types of users to access it. There must be a limitation to access the information, who are authorized can only access the information. And last the authentication system which authenticates the user before accessing information.

Integrity: It normally refers to the data integrity, or to make ensure that data stored is accurate and no unauthorized modifications are done. The loss of integrity is considered as the unauthorized modification or destruction of the information. Disrupting a message in transit can have serious consequences.

For E.g.: if it is possible to modify the fund transfer message during online banking, an attacker can take this advantage to fulfill his or her benefit by stealing the credentials. So to ensure the integrity of this type of message is important for any security systems.

Availability: Ensuring the timely and reliable access of information to the authorized users for the systems to provide a value. The loss of the availability of the information is the loss or disruption of access to the information.

Although the use of CIA TRIAD to define security objective is well established, there are additional concepts which are important to learn and understand which makes the complete picture, they are Authentication, Authorization, and Nonrepudiation. Understanding each of the six concepts will help to implement robust security mechanisms.

Authentication: The primary goal is to focus the information on being genuine and source of the message for any security systems. This means that users are who they say and every piece of information came from the trusted source.

Nowadays we have seen Authentication system requires more than one factor of authentication, it is called Multifactor Authentication.

Such as password required combining with Fingerprint or retina scan or voice verification and PIN (Personal Identification Number), as it is useful in validating the user (owner of the fingerprint) and PIN number (something that user knows).

Authorization: It focuses on whether the user is verifiably granted permission to do so. When the system authenticates the user it also verifies and checks access privileges granted to the user. Which in simple terms means what a user can or cannot do while using the system.

Nonrepudiation: It is assuring that the sender of the data is provided with the proof of delivery and recipient is provided with the sender’s identity, so neither can deny in later part of having processed the data. In the normal physical world, it can be understood as the notary done on the stamp paper for any kind of deals. Where neither of the parties can deny the deal in the later stages.

To meet such requirements, systems have to normally rely on the asymmetric cryptography or public key cryptography. While symmetric key systems use a single key to encrypt and decrypt the data. Asymmetric cryptography uses one key(private) for signing the data and another key(public) for verifying the data.

Check Your Progress 1

1. List all components of CIA TRIAD

   ____

2. What do we call if we combine Retina Scan with PIN

   ____

3. Which property ensures user is able to access data anywhere and anytime____________

1.5BASIC CRYPTOGRAPHY

This section will provide the information on basic cryptography to explain basics of ciphers and cryptanalysis. Our objective is to discuss the basic operation on symmetric and asymmetric encryption algorithms. Also we will discuss the concept of the digital signatures.

The word cryptography is derived from the Greek and its literal translation is “hidden writing”. In the old times, it mostly used to send the secret messages in a way that the intended recipient can only be able to read.

Cryptography is a very critical and important part of the security applications, products, and applications in terms of using different cryptographic algorithms. Understanding how cryptography works it is important to understand to make sure that the data which is transferred between sender and receiver is safe. In early around 1900 bc Egyptians began to use pictographic to convey the secret message. This was known to be as ciphers.

Cryptography can be strong or weak. Its strength is measured in time and resources it would require to recover the plaintext.

1.5.1 HOW DOES CRYPTOGRAPHY WORK?

A cryptographic algorithm is a mathematical function which is used in encryption and decryption process. While cryptography is a science of securing data, cryptanalysis is the science of analyzing and breaking secure communication without knowledge of the key.

Combining both *Cryptography* + *Cryptanalysis* = *Cryptology*

The most common to known is the classical cipher is the substitution cipher which works by substituting each letter in the alphabet with one another when writing the secret message. The key here is the number of characters which is used for substitution. Below is one such example:

abcdefghijklmnopqrstuvwxyz

nopqrstuvwxyzabcdefghijklm

where a=n, b=o, c=p, d=q and so on

Using this cipher, the message, “hello world” would be written as “uryybjbeyq”. It is a simple substitution cipher known as Caeser Cipher.

1.5.2 SYMMETRIC ENCRYPTION

Symmetric Encryption is also known as conventional encryption which has been introduced in the late 1970s. This technique is used to provide confidentiality for the data transmission or to store data using the symmetric encryption method. There are two well-known symmetric encryption algorithms used they are: Data Encryption Standard(DES) and Advanced Encryption Standard (AES), both algorithms are block cipher encryption algorithms.

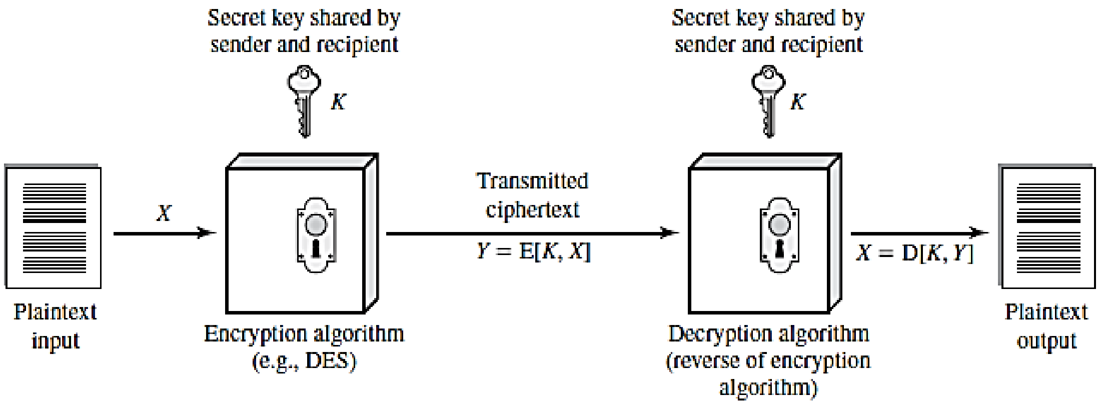
Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E[K, X]
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2 Symmetric Encryption Model

Let us understand each component which is shown in the above symmetric encryption model.

Plaintext: Original message or data provided as input into the algorithm.

Encryption Algorithm: Encryption algorithm used which performs operations on the plaintext.

Secret Key: Secret Key is also an input provided to the encryption algorithm. The exact number of substitution or transformations performed by an algorithm depending on the key.

Ciphertext: Encrypted message which is produced as output which depends on the plaintext and key used. For the same message, if there are different keys used, ciphertext will be different for both keys used.

Decryption Algorithm: It is the same encryption algorithm which runs in the reverse manner which takes the ciphertext and secret key as the input and generates the original plaintext.

There are two requirements for the symmetric encryption algorithms to work, the first one is strong encryption algorithms know to both the party sender and receiver and the second one is the secret key should be known only to sender and receiver only.

Ceaser cipher is a very form of symmetric key encryption. Symmetric cryptography doesn't address the following issue: Attacker can eavesdrop the shared key between sender and receiver and can steal the key and decrypt the data. This is where the concept of the Public Key Encryption OR Asymmetric key cryptography comes in picture.

1.5.3 ASYMMETRIC ENCRYPTION

Aasymmetric encryption is also known as Public Key key cryptography. It uses two mathematically related but unique keys: a public key and a private key. Each key has its own unique function. The public key is used to encrypt the data and the private key is used to decrypt the data. It is computationally infeasible to obtain the private key from the public key. Its primarily used for the authentication, non-repudiation and key exchange.

Anyone with the public key can encrypt the data but cannot decrypt the same. Only the appropriate receiver with the private key can decrypt the data. Even if the attacker knows that the sender is transmitting data to the receiver, also data passes through multiple channels, there is nothing he or she can do. As the data can only be decrypted by the private key.

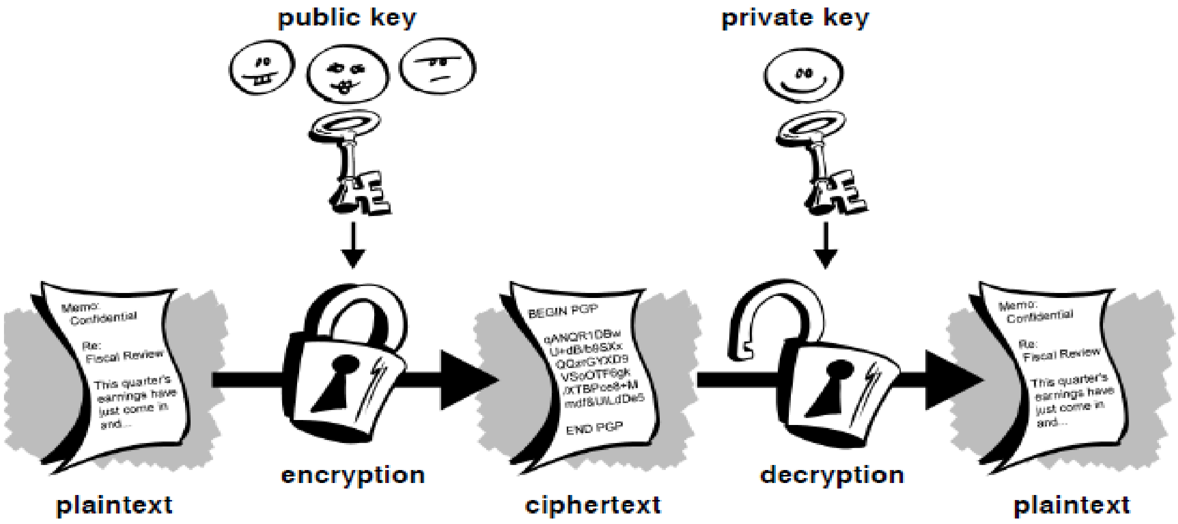
public key
private key
Memo: Confidential
Re: Fiscal Review
This quarter's earnings have just come in and...
BEGIN PGP
qANQR1DBw U+dB/b9SXx QQzrGYXD9 VSoOTF6gk /XTBPce8+M mdf8UILdDe5
END PGP
Memo: Confidential
Re: Fiscal Review
This quarter's earnings have just come in and...
encryption
decryption
plaintext
ciphertext
plaintext

Figure 3 Asymmetric Encryption Model Source: PGP Corporation, Introduction to Cryptography

All communication which takes part between sender and receiver includes the public key. The private key is never shared, they are simply stored on the software or on the machine used. Some of the examples of the public key cryptosystem are Elgamal(named after its inventor Taher Elgamal), RSA (Ron Rivest, Adi Shamir, Leonard Adleman) which is most widely used even in current times. Diffie-Hellman.

1.5.4 HASH FUNCTIONS

Cryptographic Hash Functions are a mathematical algorithm that take the input of the arbitrary size of data and generates the fixed length hash value or message digest or simply digest and they are also designed to be the one-way functions. This means they are not reversible in nature.

There are few properties of the HASH Function which are mentioned below due to which they are still widely used in a different information security application.

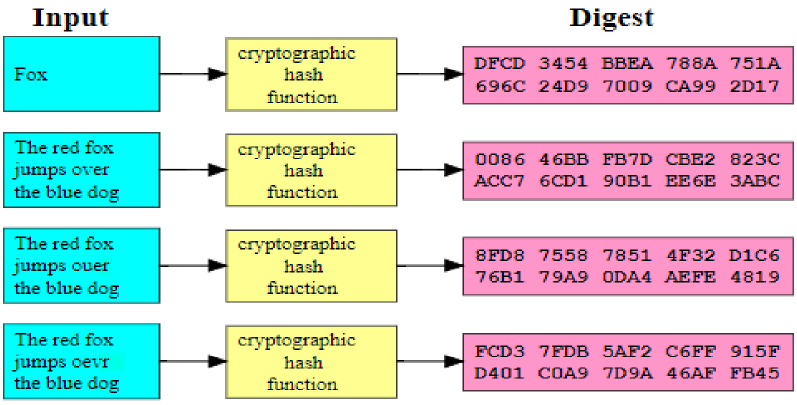
Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A
696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C
ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6
76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45

Figure 3 Hash Function Source: Wikipedia

- It is deterministic which means it will always give the same hash value for the same input message.
- Computing hash value of the message is faster.
- It is infeasible to generate the same message from the hash value.
- Even a very small change in the message will change the hash value completely.
- It is infeasible to find two different messages with the same hash value.

Due to such properties they are widely used for digital signatures, Message Authentication Code, Indexing data in the hash table, fingerprinting, finding duplicate data, Checksums to identify any modification in data.

Hash Algorithms which are commonly used today:

- **Message Digest(MD) Algorithm:** A byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message. There are various versions of these algorithms present such as MD2(RFC 1319), MD4(RFC 1320), MD5(RFC 1321).

  MD5 is the third message digest algorithm after MD3 and MD4, which process data in 512-bit blocks which is broke down into 16 words composed of 32 bit each. The output from MD5 is 128-bit message digest value.

- **Secure Hash Algorithm:** It is a cryptographic hash function published by the National Institute of Standards and Technology(NIST) as a U.S. Federal Information Processing Standard which takes an input and produces a 160-bit hash value known as a message digest – typically rendered as a hexadecimal number which is 40 digits long. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. There are a series of algorithms exist such as SHA-1, SHA-2, SHA-3.

Apart from this, there areotherwell-known HASH Functions exist which are used such as RIPEMD, WhirlPool.

Check Your Progress 2

---

1. List out atleast 3 differnet HASH Algorithms

   ____

2. What do call the output generated for the HASH algorithms

   ____

3. Describe atleast two uses of the HASH Algorithms

   ____

1.5.5 DIGITAL CERTIFICATE

There are several issues which exist with the public key cryptosystems; one of them is the man-in-the-middle attack in which is one of the potential threat. In this attack someone tries to fake the key with user ID and name, and tried to pretend the same person, which is not and resulting in this, the data is encrypted with the attackers key.

It is vital to know that the public key to which you are encrypting the data is the actual key of the intended recipient and not a forged one.

To overcome this, Digital Certificates has been introduced, which will ensure that whether a public key truly belongs to the actual owner or not. It acts much like a physical certificate.

Digital certificates consist of three things:

- A Publick Key.
- Certificate Information(Identity information about the user).
- One or more digital signature.

1.5.6PUBLIC KEY INFRASTRUCTURE

A Public Key Infrastructure(PKI) is a combination of policies, role, and procedures, which are needed to create, manage, distribute, use, store, and revoke digital certificates and manage, public-key encryption. It includes components such as Certificate Authority(CA) and the Registration Authority(RA).

Certificate Authority creates a certificate and digitally signs them using its own private key. As it is the central component of the PKI system. Using the public key of the CA one can verify the authenticity of the digital certificate and can check the integrity of the content of the certificate.

Registration Authority refers to the people which can include group, company, process, and tools which will help users to enroll them with the PKI system. It also checks the public key belongs to its owner or not. On the other hand, CA is the software which issues the actual certificates.

1.7LET US SUM UP

This chapter has provided details regarding basic cybersecurity details and current cybersecurity posture of the Nation. Moving forward we have also seen the basic security fundamentals and building blocks of the cybersecurity which are confidentiality, integrity, and availability and why are they important. Also how that can be achieved using the different encryption models and its understanding using pictorial representation.

1.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check your progress 1

1. Components of CIA TRIAD Confidentiality, Integrity and Availability
2. Two Factor Authentication
3. Availability

Check your progress 2

1. HASH Algorithmsare MD5, SHA-1, RIPEMD
2. Message Digest OR Hash Value
3. Uses of the HASH Algorithms Data Integrity, Indexing Data in Hash Table