Cyber Security

(Prof. Ashok K. Bhateja, IIT Delhi)

1. Introduction

With the advancement of digital technology new technologies like cyber physical systems and Internet of Things (IoT) have emerged. These models are based on system and devices which connect the physical and digital worlds and provide opportunities to enhance productivity and improved decision-making capabilities. Generally, software in these systems are not designed with adequate amount of security and therefore, the hackers succeed in stealing the important and valuable information/data of the organization. These weaknesses in the system which can be exploited are called cyber vulnerabilities. Cyber security deals with the principles and practices to protect computer systems, networks, software, electronic devices and data from unauthorized users. Cyber security helps to protect the data from the attackers by ensuring confidentiality, integrity, and availability of the data.

Modern industries and research organizations are heavily dependent on the computers that store and transmit sensitive information like intellectual property, financial data, personal information, etc. whose exposure may have negative consequences. Attackers attempt to access these sensitive informations with the aim to disable, disrupt, destroy or steal the data. Cyber security is a necessity to govern the conduct and manners of interacting with any of the computer system having suspicious behavior.

2. Elements of Cyber security

In order to protect the information at system connected through internet, it is essential for an organization to consider the following key elements of cyber security.

2.1 Network security

It is process/activity to protect the computer networks from intruders, may be targeted attackers or opportunistic malware. Network security combines the defenses of the network layers by implementing security policies and controls so that only authorized user may get access to the network.

2.1.1 Types of Network Security

- **Firewalls**: Firewall monitors and filters the incoming and outgoing traffic based on the policies set by the organization. It is essentially a barrier between the internal network and internet which can quickly detect and react to malicious traffic from the external worlds. Firewall may be a hardware or software or both. Router is an example of hardware firewall. Huawei Firewall and CrowdSec are examples of software firewalls.
- **Anti-malware software**: Malwares, in the form of viruses, worms, trojans, spyware, etc. are used to spread and infect the system. Anti-malware program detects and if required, delete the malware on the system before it can penetrate and harm the software/data. Anti-malware software, namely quick heal, Kaspersky, Microsoft Defender mainly use signature and heuristics to identify the malware.

- **Email security**: The aim of email security is to protect email accounts, contents, loss, compromise from any unauthorized access. Special precautions are required to protect sensitive information from attackers.
- **Network Segmentation**: To improve the performance and security, network is divided into multiple segments. It helps to avoid potential threats outside the network to access the sensitive data of the organization. Organizations can also define some more boundaries within the network to have better security.
- **Data Loss Prevention**: Organizations can implement techniques to make sure that sensitive data should not be sent outside in an unsafe manner.
- **Intrusion Detection and Prevention System**: Intrusion Detection and Prevention System identify any malicious activity and apply proactive security measure to prevent an anticipated attack. McAfee, Trend Micro, Darktrace, Cisco are some of examples of Intrusion Detection and Prevention System. Generally, intrusion detection is done using signature or anomaly-based detection system, intrusion prevention is done by dropping malicious packets, blocking offending IPs and alerting security personnel.

2.2 Application security

Cyber criminals try to find the vulnerability in the application of the organization to steal sensitive data and intellectual property. Application security includes various security features like authentication, encryption, logging and application security testing to reduce the vulnerability. Constant updates and continuous testing of application security ensures applications are secure from attacks.

2.3 Information security

Information is data (or raw data) converted into useful form for human being. It includes records, personal data and intellectual property of an organization. Protecting the information is very important as it is the heart of the organization. Cryptography techniques are used to protect the information from cyber threats and unauthorized access.

2.4 Operational security

Operational security encloses the creation and enforcement of policies, procedures, and guideline documents. It is also known as procedural security or administrative security. Its goal is to protect information and observable actions of an organization's capabilities, limitations, and methods to prevent and control exploitation of sensitive information by any unauthorized entity. Operational security is a five-step iterative process:

Step 1 Identification of critical information: Information about research, intellectual property, financial reports, resources, customer and employees are considered as critical informations. In this step organization can focus on vital information rather than on classified or less sensitive information.

Step 2 Analysis of Threats: In this step, analysis about the adversary’s intelligence collection capabilities, their analysis and use to target the organization, are carried out. This step uses law enforcement, intelligence activities and open source information to detect the adversary and the degree of threat.

Step 3 Analysis of Vulnerabilities: Based on the findings of analysis of threat, what critical informations the adversary can obtain, the vulnerability analysis is carried out to find the range and type of activities that can be collected by the adversary to target the organization.

Step 4 Assessment of Risk associate with each vulnerability: The amount of risk is computed based on assessment of degree of threat, its impact, the type and level of vulnerability. Appropriate counter measures in terms of their cost and effectiveness can be used.

Step 5 Application of Appropriate Countermeasures: In this step of operational security, it is required to decide and apply an appropriate countermeasure to eliminate threats and mitigate risks. It may be upgradation of hardware, modification of security policies and training to employees on security policies.

2.5 Cloud Security

Cloud security consists of technologies, policies, procedures and services to protect sensitive data, applications and infrastructure stored in cloud platforms. The cloud analyses the traffic and controls unauthorized access. The privacy and safety of these systems depends on the security efforts of cloud provider and clients that use the cloud. Major threats to the cloud security are data breaches, data leaks, data loss, insecure Application User Interfaces (APIs), misconfigured cloud storage, account hijacking, service traffic hijacking. The wide range of raw data and processed data in the cloud attracts the hackers to extract the important information. Another threat to cloud security is Distributed denial of service (DDoS) attack. This attack makes the service unavailable by overwhelming it with data from multiple systems so that users cannot access their accounts, like email accounts, bank accounts.

Many of the users also think that the data stored in their own servers is safer where they have better control over the data. But it may not be true, the data stored in the cloud may be safer, because the cloud service provider may have better security measures and their employees may also be security experts.

2.5.1 Some cloud security measures

While the cloud service is exceptionally convenient and economic. It is also considered that providing enough security of the data in cloud is the responsibility of the cloud provider. The security prominently lies with the customer to ensure their data is safe. Here are some security measures to be adopted by the cloud customer

Local Backup: In IT world, information is everything and if the data is lost by any reason, it may lead to very serious consequences. The safety and reliability of data is the responsibility of the organization and its loss is not only financial loss but may also attract legal action. Regular and periodic backup in local storage may be an essential precaution towards cloud security.

Use Encryption: Encryption of the data travelling to and from cloud is an excellent precaution against any kind of threat. Encryption ensures that no one have the access of the private information stored in the cloud. Data used in cloud is of two type: (1) data-in-transit (2) Data-at-rest.

Data is valuable whether it is moving during a communication or sitting on a server or any storage device. While data-in-transit and data-in-rest may have different risk profiles, but

protection is required in both the states. Encryption plays very important role in protecting and securing the data in transit and the data at rest.

For protecting the data in transit, organizations generally encrypt the sensitive data before communicating and use secure connections. Hypertext Transfer Protocol Secure (HTTPS) secure version of HTTP, Secure Sockets Layer (SSL), Transport Layer Security (TLS) a more secure version of SSL, File Transfer Protocol Secure (FTPS), etc. are used to protect the contents of the data while moving.

Data-at-rest is not actively used and moved, so, it is considered as less vulnerable than data-in-transit because of the device security features. Data-in-rest generally have more sensitive or critical data so the attacker may be more interested to attack data-at-rest. Advanced encryption schemes like AES are used to protect the data-at-rest.

2.6 Internet of Things (IoT) security

The IoT is a global network connecting things consisting of objects, digital and mechanical devices like home appliances, living things (plants, animals, and people) by providing unique identifiers through various technologies like Radio Frequency Identification (RFID) and barcodes. RFID is a wireless system to identify an object using radio wave. RFID technology does not require direct line of sight unlike barcode and because of its low cost and low power consumption RFID got a strong support in industries/business. It is possible to quickly scan and identify several items at a time using RFID technology.

RFID comprises of two components: tags and readers. RFID tag also called RFID transponder contains an integrated circuit (IC) which stores unique identification /serial number and some other information related to the object, and an antenna to receive and transmit the signals. The data stored in the tag is rewritable. The reader also called interrogator is a network connected device used to detect RFID tag and collect information stored in the tag by transmitting radio wave signals to the tag and receive the signals from the tag. RFID reader is attached to a computer or Electronic Point of Sale (EPOS) device, where further processing of the information is done.

Security in IoT means securing devices and the networks to which the devices are connected. The rapidly growing dependence on IoT applications and the number of devices that are connected through internet are only growing without keeping their security in mind. Connected devices boost the performance of an organization, but anything connected online may be vulnerable to cyberattacks.

2.6.1 Some IoT security threats

- IoT botnets

  A botnet i.e., bot network is a network of internet connected malware infected devices, hijacked and remotely controlled by attackers. With the continuous increase and wide use of IoT, botnets creation has become prominent.

- DNS threats

  IoT device connections often rely on Domain Name System (DNS) protocol, which maps computer name to IP addresses and vice versa. Man in the middle (MITM) attacks, Caching Problems, DDoS attacks are some of the attacks on DNS.

- IoT ransomware

  Ransomware is a malware attack that blocks the IoT device and ask money for regaining access to its functionality. To overcome these attacks, regular data backups, resetting the device, and installing new patches and updates are done.

- IoT physical security

  Attackers can steal the IoT devices and after opening it, attacker can have access of inner circuit and ports to penetrate the network. Therefore, the organization should only allow authorized persons to have physical access of the devices.

2.7 End-User Education

This is a most unpredictable vulnerability in cyber security system. End user may be employees or customers accessing the organization's data/application. Most of cyber-attacks are because of human errors which is caused due to lack of security policies. So, the organizations/companies should provide training to their employees and the customers about the security policies. The employee should not use any insecure network to protect the integrity of the internet connected system from cyber-attack.

3. Cyber Security Threats

Cyber security threat is a malicious attempt to gain unauthorized access to damage or hack sensitive data, intellectual property, IT assets of an organization/company. With the adaption of new technologies in the areas of artificial intelligence, internet of things, many new threats are emerging. Therefore, for an organization/company it is essential to understand the information security threats that exist, as well as the new and emerging threats which may plague the organization in future.

3.1 Types of Cyber Security Threats

Cyber security threats are continuously emerging, some most damaging threats are given below:

- **Social engineering** is manipulation of human psychology to gain confidential information about a target. Because of human natural inclination to trust, social engineering is easier than to discover ways to hack the information. Therefore, criminals generally use social engineering attacks. Phishing is a type of social engineering attack, in which the attackers send malicious emails that seem to come from trusted entity. On clicking the malicious link received, the malware gets installed or the attacker may get the sensitive information. To prevent these attacks, employees and the customers of the organization should be educated on how to identify these types of attacks and how to keep the system protected from these attacks.
- **Ransomware** is a malicious attack to encrypt files on a device to make them unusable or blocked. The attacker demands monetary ransom for decrypting the files. Cryptolocker, Bad Rabbit, Goldeneye, Zcryptor, LeChiffre are some examples of ransomware. Protection against ransomware attacks are to have watchful eye and the right software.

- **DDoS (Distributed Denial of Service) attack** is an intention to make the services of network unavailable to the intended user. It is also known as distributed network attack. DDoS attack send multiple requests to the target system, such that number of requests is more than the target website's capacity to handle multiple requests and the website should not work correctly. This attack is like an unexpected traffic jam preventing the normal traffic on the highway.
- **Third Party Attack** when organizations buy any software or digital product, they assume that it is secure, but in most of the cases it may not be true. The vulnerabilities down the digital supply chain are not addressed. The weaknesses in the digital supply chain may be exploited by the hackers and hackers may succeed to penetrate the internal networks to steal sensitive informations of the organization. Assessing the vendors for before onboarding, incorporating risk management into the contracts, keeping an inventory of the in-use vendors, continuously monitoring vendors for security risks, cutting ties with bad vendors and following the principle of least privilege are some of measures to prevent the third party attack.
- **Man-in-the-middle (MITM) attack** is a session hijacking with the aim to exploit the real time transfer of information. It occurs when the attacker intercepts the communication going on between two parties. After intercepting the communication, attacker can filter out some sensitive information and return changed or other information and data to the users. Sniffing, packet injection, session hijacking, SSL stripping are some of the techniques used for MITM attack.

  In order to protect the system from man in the middle attacks, the following measures may be used

  - WEP/WAP Encryption on Access Points
  - Router Login Credentials
  - Virtual Private Network (VPN)
  - Hypertext Transfer Protocol Secure (HTTPS)
  - Public Key Pair Based Authentication

- **Structured Query Language (SQL) Injection** allows attacker to insert malicious code into targeted system that uses SQL. When infected, the targeted system releases information which may be modified or deleted by the attacker. Through SQL injection attack the attacker may also get access of the sensitive data such as password, credit card details, etc.

4. Importance of Cryptography in Cyber Security

Cryptography plays very important role to protect enterprise information and communication from cyber threats by using mathematical encryption functions. These cryptographic techniques allow only the authorized sender and recipient to see the content of a message. Cyber security is a remedy to mitigate cybercrimes. If an organization deploy cryptography as one of the means of cyber security, the system will be better secured.

Cryptography helps to achieve the goals of cyber security by ensuring Confidentiality, Integrity and Availability, also called CIA triad. Algorithm for encrypting and decrypting data is also called cipher.

Confidentiality

Confidentiality ensure that no one can read the message except the authorized recipient. The data communicated over the network should not be accessed by any unauthorized entity. To avoid this, encryption schemes like AES (Advanced Encryption Standard) can be used to safeguard the data from attacker. Even if the data gets compromised, the encrypted information is completely useless to the attacker without the proper decryption key.

Integrity

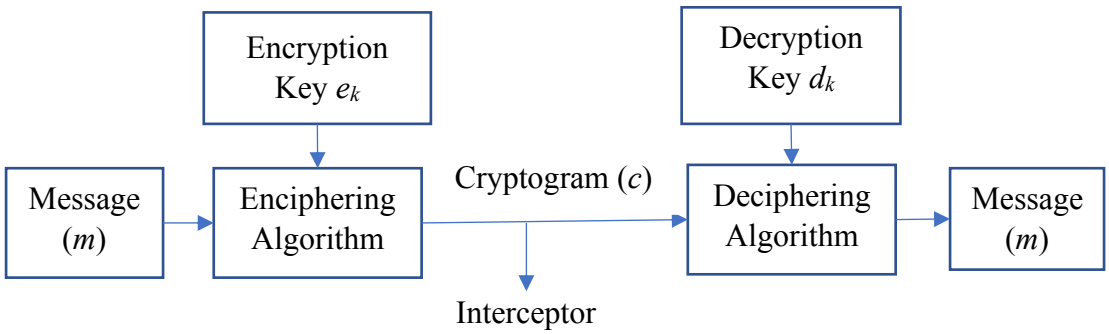
Integrity assures the receiver that the received message has not been changed from the message sent be the sender. To check whether data has been altered in transit, cryptographic hash functions like SHA (Secure Hash Algorithm) and MD5 or MD6 are used.

Availability

It ensures that the system and data are readily available to the authorized users. This requires proper maintenance and regular upgradation of hardware, software, technical infrastructure and systems, holding the information.

4.1 Types of Cryptographic systems

Mathematically cryptosystem is function of input (message) and key. i.e. $c = f(m, k)$.



Cryptosystems is mainly divided into three categories, namely, symmetric key cryptosystems, asymmetric key cryptosystems and hash functions.

4.1.1 Symmetric key cryptosystem

Symmetric key cryptosystem also called secret key cryptosystem is an encryption scheme in which either both the encryption and the decryption keys are same, or it is possible to find the decryption key in polynomial time knowing encryption key. The biggest problem with symmetric key cipher is the distribution of the key (discussed later in asymmetric key cryptosystem).

Symmetric key cryptosystems are divided into two categories: block ciphers and stream ciphers. Block cipher encrypts a fixed size block of bits. To encrypt a given message using a block cipher the given message is divided into fixed size block, which may require some dummy bits for concatenation and encryption is done one block at a time.

Some Block ciphers:

- DES (Data Encryption Standard), block size: 64 bits; key size: 56 bits.
- 3-DES, block size: 64 bits; key size: 128 bits.

- AES (Advanced Data Encryption), a variant of Rijndael, encrypts a block of 128 bits using 128, 198 or 256 bit key.
- IDEA (International Data Encryption Algorithm) block size: 64 bits; key size: 128 bits.
- Blowfish, block size: 64 bits; key size: 32 to 448 bits.

Stream ciphers encrypt bits or bytes or letters of a message one at a time using key stream. Key stream is a random sequence of bits/bytes/letters generated from the key.

Examples of stream cipher:

- One-time pad (OTP) – unconditional secure
- LFSRs (Linear Feedback Shift Register) and NLFSRs (Nonlinear Feedback Shift Register)
- RC4 (Rivest Cipher 4), RC5, RC6 suited for software
- A5/1 is suited to hardware.

4.1.2 Asymmetric key cryptosystem

Asymmetric key cryptosystem or public key cryptosystem is an encryption scheme where the enciphering and deciphering operations, as well as the generation of inverse key, all take polynomial time, but the deduction of deciphering key (private key) from enciphering key (public key) needs exponential time.

Public key cryptosystems were developed to solve the following problems:

- **Key distribution** – problem of key distribution in symmetric key cryptosystems.
- **Digital signatures** - assurance that message has been generated only by sender who own the matching secret private key and no one else.

  Public key cryptosystem requires a one-way function with trapdoor. A function f is called one-way function with trapdoor if for a given x it is easy to compute $f(x)$, but it is computationally hard to find x for a given $f(x)$ without the knowledge of trapdoor.

Examples of Public Key Cryptosystems:

RSA – invented in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman. It is based on the dramatic difference between the ease of multiplying two large numbers and the difficulty of factoring a composite number. The public and the private keys are computed using a pair of large prime numbers. Security of the system lies in the difficulty of the problem of factoring large integers.

ElGamal public-key cryptosystem - The security of this cryptosystem is based on the intractability of the discrete logarithm problem. It encrypts the same plaintext to different cipher text each time it is encrypted. The disadvantage of ElGamal cryptosystem is that the size of ciphertext is twice the size of the plaintext.

Diffie-Hellman Key Exchange – It is secure key exchange protocol developed in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman key exchange protocol is the first practical solution of the problem of key distribution to the users. The protocol allows both the users to generate a common secret key using an insecure medium without any prior secrets. Security of the Diffie-Hellman key exchange protocol is based on the intractability of Discrete Logarithm problem. This key can be used as a key of a symmetric key cryptosystem for encryption of actual communication between the users.

Public key cryptosystems such as RSA, Diffie Hellman have been used as security solutions on the Internet, but they are not practical to implement for IoT devices due to their overheads

in computations, storage and communications of security parameters such as keys. Therefore, there is a need of an efficient public key cryptosystems specially for IoT security. Elliptic curve-based cryptosystems can provide same amount of security (or better) with less computing power. 160-bit ECC key provides the same amount of security as of 1024-bit RSA. The keys required in Elliptic curve cryptography (ECC) are smaller in size and can be generated more efficiently.

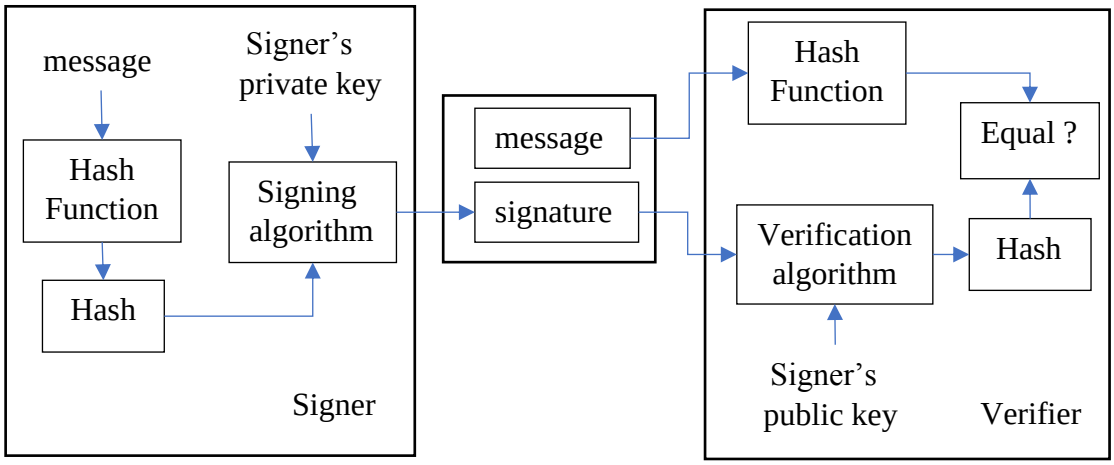
Elliptic curve is a set of points satisfying the plane curve $y^2 = f(x)$, with $f(x)$ a cubic polynomial having non repeated roots. Security of ECC lies on the fact that multiplying a point on the curve by a number produces another point on the curve, but knowing both the original point and the result, it is computationally hard to find the number which was used.

Elliptic-curve Diffie–Hellman (ECDH) is a key exchange protocol used to generate a common key for both the parties. Elliptic curve digital signature algorithm (ECDSA) is used in digital signatures in IoT and in cryptocurrencies like Bitcoin and Ethereum.

4.1.3 Hash Function

It is a mathematical function that converts data of arbitrary length from plaintext to a fixed length hash value. It does not require any key and practically it is impossible to recover the plaintext from the hash value. Example of cryptographic hash functions: Secure Hash Algorithm (SHA-1, SHA-2 and SHA-3), Message Digest Algorithm MD5 & MD6, RACE Integrity Primitives Evaluation Message Digest (RIPEMD), BLAKE2. Hash functions are used in digital signature.

Digital signature, like electronic fingerprint, is a mathematical algorithm used to validate the authenticity and integrity of a message (e.g. email) or document. It also has the property of non-repudiation, which makes it like the signature in the real-world. It uses both hash function and a public key cryptosystem. Digital signature scheme using hash function and public key cryptosystem is shown in the figure below.



For signing hash function with private key of an asymmetric key cryptosystem is used and for verifying hash value with public key of the asymmetric key cryptosystem is used.

Conclusion

In today's high technology environment, organizations are becoming more and more dependence online technology. The threats from hackers are increasing, it is necessary to make information secure as the assets to the organization. This needs for an organization to keep their employees educated with the latest cyber security technologies. The exclusive use of digital technology to store and send sensitive information raised the requirement, of cyber security, a lot for an organization.