University of Technology
الجامعة التكنولوجية

Computer Science Department
قسم علوم الحاسوب

Cybersecurity

الامن السيبراني

Assistant Prof Dr. Ayad Hazim
ا.م.د اياد حازم

cs.uotechnology.edu.iq

Introduction to Cyber Security

Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats: - Cyber Warfare-Cyber Crime-Cyber Terrorism-Cyber Espionage, Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.

Cyber Security Vulnerabilities and Cyber Security Safeguards

Cyber Security Vulnerabilities-Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness. Cyber Security Safeguards-Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, social engineering, Firewalls, Response, Scanning, Security policy, Threat Management.

Cyber security architecture and operations:

physical and process controls that can be implemented across an organisation to reduce information and systems risk, identify and mitigate vulnerability, and ensure organisational compliance. Service continuity and reliability, Security architecture, Process and Technology Control, Defence in depth, Operational fundamentals of technical controls

Testing and monitoring, Usability, awareness and behaviour

Cybersecurity management:

Understanding the personal, organisational and legal/regulator y context in which information systems could be used, the risks of such use and the constraints (such as time, finance and people) that may affect how cybersecurity is implemented.

Secure systems and products

Introduction, Basic security for HTTP Applications and Services, Basic Security for SOAP Services, Identity Management and Web Services, Authorization Patterns, Security Considerations, Challenges.

intrusion Detection systems

- Intrusion detection system types

Network intrusion detection system

Network node intrusion detection system

Host intrusion detection system

Protocol based intrusion detection system

- Methods of intrusion detection system

Cyberspace and the Law:

Cyber Security Regulations, Roles of International Law, the state and Private Sector in Cyberspace, Cyber Security Standards

References:
Cyber-security-essentials, James graham, Ryan Olson, Richard Howard, 2010

Chapter One
Introduction to Cyber Security

1. 1. Overview of Cyber Security

The internet has made the world smaller in many ways but it has also opened us up to influences that have never before been so varied and so challenging. As fast as security grew, the hacking world grew faster.

Cyber Security is a set of processes, technologies, and methods to protect servers, computers, networks, electronic systems, data, and mobile devices from unauthorized access through malicious attacks, thus it is focused on the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.

Common **cybersecurity categories** include

- **Application Security**: Compromised applications can facilitate unauthorized access to data. Application security protects devices, applications, and software from cyber-attacks.
- **Operational Security:** From access permissions to decisions and processes that determine where and how data will be shared or stored, fall under operational security. It places a great emphasis on securing data assets.
- **Information Security**: All about protecting the privacy and integrity of data in transit and storage.
- **Network Security**: The process of ensuring security to computer networks from opportunistic الانتهازيه malware or targeted attackers.
- **End-user Education**: This cybersecurity category covers an extremely unpredictable factor—**humans**. End-user education aims to teach users about cybersecurity threats and the best security practices to avoid them

Cybersecurity solutions protect against three types of cyber threats, which are

- **Cyber Attack**: Unauthorized information gathering, often involves politically motivated information gathering. Cyber-attacks can be classified in a number of ways. For example, cyber-attacks are classified according to their goal or the goal of their implementation, and also can be classified according to the technology or gaps on which they depend, and they can be classified according to their effects.
- **Cyber Crime**: Groups or single actors targeting systems, networks, or servers for monetary benefit or for causing disruption.
- **Cyber Terrorism**: Undermines electronic system to cause fear or panic

1. 2. Cybersecurity objectives

The objective of Cybersecurity is to protect information from being stolen, compromised, or attacked. Securing the **availability, confidentiality, and integrity** of an organization’s digital assets and software against internal or external threats is the

primary objective of cybersecurity. Thus Cybersecurity can be measured by at least one of three goals-

1. Protect the **confidentiality** of data, where the protection of information from any unauthorized disclosure.
2. Preserve the **integrity** of data, the accuracy, and completeness of the information
3. Promote the **availability** of data for authorized users. The ability to access information and resources required by the business process.

These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs. The CIA triad is a security model that is designed to guide policies for information security within the premises of an organization or company. This model is also referred to as the **AIC (Availability, Integrity, and Confidentiality)** triad to avoid confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.

Figure (1.1) : AIC or CIA Model

1. 3. Cyber Security and Network Security

Network Security: Network Security is the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data has a degree of solutions against many cyber threats.

Cyber Security: Cyber Security is the measure to protect our system from cyber-attacks and malicious attacks. It is basically to advance our security of the system so that we can prevent unauthorized access to our system from an attacker. It protects cyberspace from attacks and damages. Cyberspace can be hampered by inherent vulnerabilities that cannot be removed sometimes.

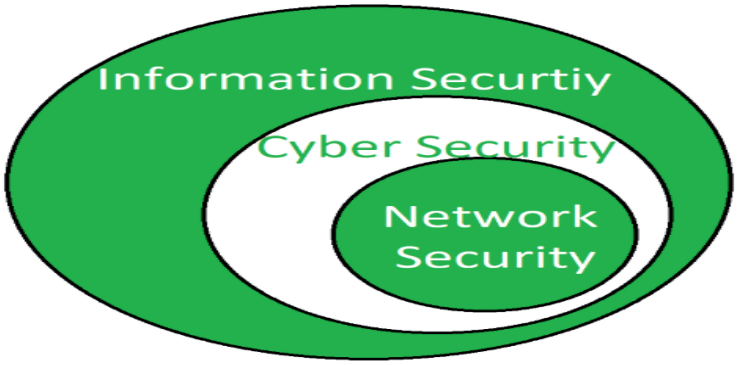


Figure (1.2): Shows relation between Information, Cyber, and Network Security.

Table (1.1): Difference between Network Security and Cyber Security

Network Security	Cyber Security
It protects the data flowing over the netwo secures the data traveling across the netwo terminals. Network security ensures to pro the transit data only.	It protects the data residing in the devices servers. Cybersecurity ensures to protect e digital data.
It is a subset of cybersecurity.	It is a subset of information security.
It protects anything in the network realm	It protects anything in the cyber realm.
It deals with the protection from DoS atta	It deals with the protection from cyber-att
Network Security strikes against Trojans, and worms.	Cyber Security strikes against cyber-crim cyber frauds الاحتيال , phishing and pre-tex

1. 4. Cyber Security and Information Security

The terms Cybersecurity and Information Security are often used interchangeably. As they both are responsible for the security and protecting the computer system from threats and information breaches and often Cybersecurity and information security are so closely linked that they may seem synonymous and unfortunately, they are used synonymously. Information security can be simply defined as "a set of strategies for managing the processes, tools, and policies necessary to prevent, detect, document and counter threats to digital and non-digital information." Any point of data storage and transfer is considered to be an "information system," meaning this practice can apply to a wide variety of environments, including that outside cyberspace.

Data security is all about securing data. Now another question that arises here is the difference between data and information? Not every piece of data can be information. Data can be called information when it is interpreted in a context and given meaning. For example, "14041989″ is data. And if we know that this is the date of birth of a person, then it is information. So, Information means data that has some meaning. Information security is all about protecting the information, which generally focuses on the confidentiality, integrity, availability (CIA) of the information.

While cybersecurity is about securing things that are vulnerable الضعيفه, it also considers that where data is stored and technologies used to secure the data. Part of cybersecurity

about the protection hardware and software, is known as information and communications technologies (ICT).
The following Venn diagram can be helpful to understand the differences.

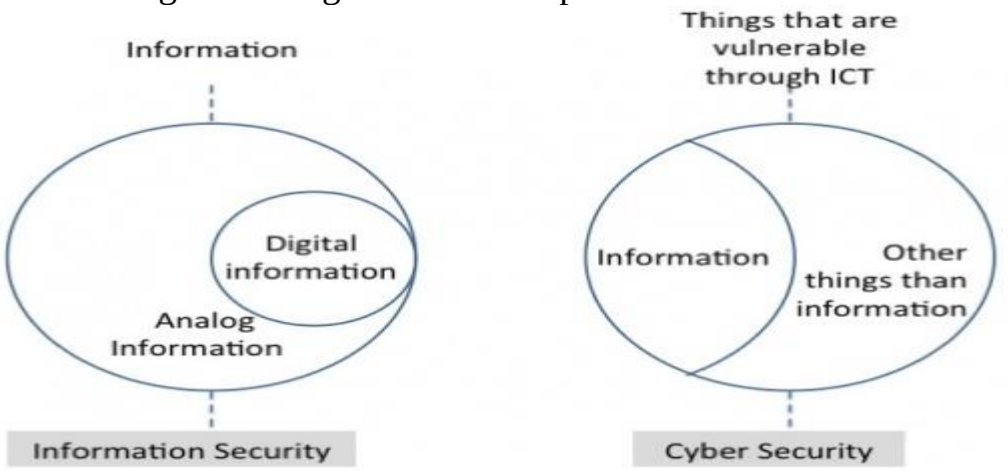


Figure (1.2): Venn diagram shows the differences between CIA and ICT

Table (1.2): Difference between Cybersecurity and Network Security .

Cybersecurity	Information Security
It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal to provide confidentiality, integrity, and availability.
It is about the ability to protect the use of cyberspace from cyber-attacks. Cybersecurity to protect anything in the cyber realm. Thus, it deals with danger against cyberspace.	Information security is for information irrespective of the realm. Thus , Its deals with the protection of data from any form of threat .
Cybersecurity strikes against Cybercrimes, cyber frauds , and law enforcement.	Information security strives against unauthorized access, disclosure modification, and disruption
On the other hand cybersecurity professionals deal with the advanced persistent threat.	Information security professionals are the foundation of data security and security professionals associated with it prioritize resources first dealing with threats.

1. 5. Computer and Internet Safety

For Computer and Internet Safety it's better to understand security threats associated with the use of computers and the internet, and by understanding how these threats are exploited, we can better protect our congregation, our congregation's information, computers, and computer files.
The following tips are considered the most common tips needed for Computer and Internet Safety:-

1) Run antivirus software and keep all computer software patched
2) Use a unique, strong password to access resources and every site/service you use, opt-in for multifactor authentication
3) Learn to identify phishing emails and social engineering and use email securely
4) Work as a non-administrator on your computer
5) Use secure Wi-Fi and practice network security.
6) Back up important information
7) Secure your mobile device
8) Limit social network information
9) Download files legally

1. 6. Internet Governance – Challenges and Constraints

To understand Internet governance challenges, it is important to have a clear idea of the main technical principles.
" The Internet is a communication network made up of millions of networks, owned and operated by various stakeholders. It connects these networks to each other and facilitates the overall exchange of information. Hundreds of stakeholders have been involved in the design and regulation of the Internet, including governments, international organizations, companies, and technical committees among many others".
"Internet governance is the development and application by Governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet".
The following are the most Internet Governance Challenges and Constraints:

- Many issues, many institutions
- Rapid technological progress
- Rapid societal impact
- Need structure, abstraction, models, and taxonomies .Major structural features of the governance problem in cybersecurity and internet governance are analogous. The joint production of internet services and cybersecurity makes them heavily interdependent. This means that cybersecurity governance and internet governance models need to be compatible, and the approach we take to one will influence how we approach the other.

1. 7. Cybersecurity Challenges

All stakeholders agree on the importance of cybersecurity. As it known, **only secure and reliable cyberspace can generate and preserve trust in the Internet**. With the development of the Internet and new technologies, the cybersecurity question has

become more complex, translating into a wide range of angles and issues and engaging a multiplicity of players.

The following issues some **of the main challenges of cybersecurity:**

1- **Privacy:** Cybersecurity and privacy are often intertwined and interdependent. They impact the trust in the digital space and may limit its potential for growth and prosperity. Cooperation based on mutual recognition and successful models of engagement between governments, the private sector, technical community and the civil society, can address privacy and cybersecurity concerns without undermining the open, free and secure nature of the Internet

2- **The Internet architecture**: The very nature of its organization affects the security of the Internet. Most past developments in Internet standards have been aimed at improving performance or introducing new applications; security was not a priority. The Internet Engineering Task Force develops and promotes Internet standards, in particular, the standards that make up the Internet protocol suite.

3- **Electronic commerce**: Another issue discussed is the relationship between security and electronic commerce. Cybersecurity is often mentioned as one of the prerequisites for the rapid growth of e-commerce. Without a secure Internet, customers will be reluctant to provide confidential information online, such as credit card numbers.

4- **Internet of Things**: The Internet of Things is the key driver of the digital revolution and creates new opportunities for our society, such as new products and services, but also creates vulnerabilities. Cybersecurity is a basic requirement for trust in the Internet of Things, as vulnerabilities could undermine the trust of individual users, and the society as a whole. A joint global or regional approach is also needed, as the Internet of Things is a cross-border phenomenon.

5- **Legal & Regulatory issues**: Cybersecurity norms could be viewed as an important mechanism for State and non-State actors to agree on a responsible way to behave in cyberspace, given that the speed of legislation often falls behind the pace of changes in the sphere of cybersecurity.

6- **Cybersecurity Best Practices:** The successful implementation of a collaborative model for cybersecurity strategy development and implementation resides in agile adaptability, transparency, and trusted information sharing among and between all participants. Participation should extend not only to public and private sector entities who tend to own and control critical information infrastructure but also to stakeholders from other sectors (e.g., the banking and finance sectors, business process outsourcing (BPO),

health, tourism, and energy sectors) and non-profit stakeholder groups (e.g., the technical community, academia, and civil society).

1. 8. Cyber Threats

A cyber-attack is best understood not as an end in itself, but as a means to a wide variety of other ends, some of which have tangible political, military, criminal, and social consequences. A cyber-attack is not a strategy, but a tactic that may be employed as one of many other, cyber and non-cyber tactics toward the attainment of a broader strategy. A cyber attacker's ultimate goal could be anything personal amusement, intellectual property theft, political revolution, terrorism, or even international war.
In this section, five types of cyber espionage, crime, activism, terrorism, and war are explored.

1. **Cyber Espionage**: In this type, a hacker does not do anything to data, except take it and read it. However, the amount of data that hackers can steal has already made this generation the Golden Era of Espionage. And as more and more of our lives are played out online, and as once-isolated computers are connected to the Internet, the level of sensitivity of the stolen data continues to rise.
2. **Cyber Crime Criminals:** those criminals are no strangers to technology. Counterfeiting. Today, counterfeiters likely have it much easier, as both money and intellectual property exist in electronic bits that can be transmitted around the world at light speed.
3. **Cyber Activism**: is the process of using Internet-based socializing and communication techniques to create, operate and manage activism of any type. It allows any individual or organization to utilize social networks and other online technologies to reach and gather followers, broadcast messages and progress a cause or movement.
4. **Cyber Terrorism**: Cyber-terrorism involves the use of computers and/or related technology to cause harm or damage, to coerce a civilian population, and influence the policy of the target government or otherwise affect its conduct. Furthermore, cyber-terrorism which should be differentiated from hacktivism and cyber-warfare implies targeting Critical Infrastructures. There are linkages as well as discrepancies between cyber-terrorism and terrorism broadly speaking, which unavoidably affect the counterterrorism response in either case.
5. **Cyber Warfare**: involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

1. 9. Need for a Comprehensive Cyber Security Policy

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information. It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when they will occur. A security policy is also

considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes. The following issues describe the requirement of Security policies:-

1) **It increases efficiency**.

The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources. The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

2) **It upholds discipline and accountability**

When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law. The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.

3) It can break a business deal

It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information. It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.

4) It helps to educate employees on security literacy

A well-written security policy can also be seen as an educational document which informs the readers about their importance of responsibility in protecting the organization sensitive data. It involves on choosing the right passwords, to providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened.

We use security policies to manage network security. Most types of security policies are automatically created during the installation.

The following are a description of some important cybersecurity policies recommendations:-

1. Virus and Spyware Protection policy

This policy provides the following protection:

- It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
- It helps to detect the threats in the files which the users try to download by using reputation data from Download Insight.
- It helps to detect the applications that exhibit suspicious behavior.

2. Firewall Policy

This policy provides the following protection:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals.
- It removes the unwanted sources of network traffic.

3. Application and Device Control

This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system. The device control policy applies to both Windows and Mac computers.

6. Exceptions policy

This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.

7. Host Integrity policy

This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure.

Chapter Two
CybersSecurity Vulnerabilities and Cyber Security Safeguards

2.1 Cyber Security Vulnerabilities

Vulnerability is, in broad terms, a weak spot in your defense. The term cybersecurity vulnerability refers to any kind of exploitable weak spot that threatens the cybersecurity of an organization.

The following subjects are effecte on vulnerabilities of Cybersecurity

1) **Vulnerabilities in Software**
2) **System administration**
3) **Complex Network Architectures**
4) **Unprotected Broadband Communications**
5) **Por Cyber Security Awareness**

1) **Vulnerabilities in Software**

Software vulnerability can be seen as a flaw, weakness, or even an error in the system that can be exploited by an attacker to alter the normal behavior of the system. Because the number of software systems increases every day also the number of vulnerabilities is increased. Usually, the goal of an attacker is to gain some privileges in the system to take control of it or to obtain valuable information for its benefit. The following some Software vulnerability instances :

- **XSS or cross-site scripting: usually associated with web applications, consists of the injection of code in the pages accessed by other users. If exploited, an attacker can bypass access controls, perform phishing, identity theft, or expose connections.**

If exploited, an attacker can bypass access controls in XSS then attacker

- **perform phishing, identity theft, or expose connections.**

- **SQL injection: it consists of the injection of code to exploit the content of a database. Usually happens because the inputs are not handled correctly, the attacker can get sensitive information from the database.**

How and why SQL injection happen

2) **System administration**

A security systems administrator **is someone who gives expert advice to companies regarding their internal security procedures and can also help to detect any weaknesses in a company's computer network that may make them vulnerable to cyber-attacks.**

Who is give expert advice to companies regarding their internal security procedures and can also help to detect any weaknesses in a company's computer network that may make them vulnerable to cyber-attacks? A security systems administrator

Security systems administrators are a company's first step in monitoring suspicious activity either within the local network or from outside internet traffic.

How is done the first step in monitoring suspicious activity either within the local network or from outside internet traffic.? Security systems administrators

What the chargement of Security systems administrators?

Security systems administrators are in charge of the daily operation of security systems, and can handle things like systems monitoring and running regular backups; setting up, deleting, and maintaining individual user accounts; and developing organizational security procedures.

A security systems administrator responsible of of Security systems administrators ? yes

A security systems administrator's responsibilities :

1. **Defending systems against unauthorized access**
2. **Performing vulnerability and penetration tests and Identifying threats and working on steps to defend against them**
3. **Monitoring traffic for suspicious activity**
4. **Configuring and supporting security tools (firewalls, antivirus, and IDS/IPS software)**
5. **Implementing network security policies, and providing technical security advice**
6. **Analyzing and establishing security requirements**
7. **Identifying threats and working on steps to defend against them**
8. **Consulting with staff, managers, and** executives **on be+st security practices**
9. **Developing and updating disaster recovery protocols**
10. **Conducting security audits**

3) Complex Network Architectures

Complex networks have more entryways and points of interaction than ever for cybercriminals to target, making it more likely they will be able to find a vulnerability to exploit, that inconsistent security measures can slip, and that threats can spread rapidly once the perimeter has been compromised.

Improving Complex Network Security

Network security refers to any activities designed to protect the confidentiality, integrity, and availability of the network, as well as the information assets that rely upon it.

What are the network security fundamental objectives?

- **To protect the network itself;**
- **To reduce the vulnerability of computer systems and applications to threats originating from the network; and,**
- **To protect data during transmission across the network.**

Cybercriminals are continuously searching for weaknesses in an organization's Internet-facing network protection devices give example ?
(e.g. firewalls). These devices protect an organization from threats that emanate from the Interne.

4) Unprotected Broadband Communications

Broadband communications are usually considered to be any technology with transmission rates above the fastest speed available over a telephone line.
Broadband transmission systems typically provide channels for data transmissions in different directions and by many different users.
For example, the coaxial CATV system is a broadband system that delivers multiple television channels over the same cable. In addition, it can handle data transmissions (primarily Internet access for home users) in an entirely different frequency spectrum.

Typical broadband communication systems include the following:
ISDN (Integrated Services Digital Network) ,
ATM (Asynchronous Transfer Mode) ,
DSL (Digital Subscriber Line) and
Cable (CATV) Data Networks

.

5) Poor Cyber Security Awareness.

Cyber security awareness is the combination of both knowing and doing something to protect a business's information assets. When an enterprise's employees are cyber security aware,

it means they understand what cyber threats are, the potential impact a cyber-attack will have on their business and the steps required to reduce risk and prevent cyber-crime infiltrating their online workspace.

2.2 Cyber Security Safeguards

Cybersecurity safeguards protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system.

Safeguards may include :

- **security features,**
- **management constraints,**
- **personnel security, and security of physical structures, areas, and devices**

, thus Cybersecurity safeguards are considered all kind of control measures that support the fulfillment of requirements or the achievement of objectives related to cybersecurity

Authentication, Access control, and Audit together provide the foundation for information and system security. Authentication, Access control, and auditing are the three basic types of security controls to ensure information confidentiality, integrity, and availability.

- **Authentication establishes the identity of one party to another. Most commonly authentication establishes the identity of a user to some part of the system, typically using a password. More generally, authentication can be computer-to-computer or process-to-process and mutual in both directions.**
- **Access control: Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources.**
- **Through authentication and authorization, access control policies make sure that users have appropriate access to company data.**

- **Access control usually requires authentication as a prerequisite.**

Some examples of virtual and physical access control systems include:

- **Login credentials (such as usernames and passwords).**
- **PINs and One-Time Passwords (OTPs).**
- **Virtual Private Network (VPN) access to internal networks.**
- **Physical access cards, FOBs, tokens, locks, and keys.**

- **The Audit process gathers data about activity in the system and analyzes it to discover security violations or diagnose their cause.**
- **Analysis can occur offline after the fact or online in real-time.**
- **In the latter case, the process is usually called intrusion detection.**
-

2.3 Biometrics

Biometric is a methodological study of measuring and analyzing biological data for

- **authentication or identification**
- **encryption**
- **physical acess**
- **broad cast**

. Biometric technology is ancient Egyptian times technology. The word " biometric" is originated from the Greek words 'bios' (life) and 'metric 'or 'metrikos' (measure), which directly translates into "life measurement".

- **Physical characteristics : include Face , Fingerprint, DNA, Ear, Iris, Retina, and Hand geometry, they are associated with the shape or measurements of the human body.**
- **Behavioral characteristics: include Signature, Voice, and Gait and they are associated with the behavior or dynamic measurements of an individual. Each biometric trait has its own merits and demerits. Depend on the application requirement, an appropriate biometric trait should be used for a given authentication application. The figure below shows the categories of biometrics.**

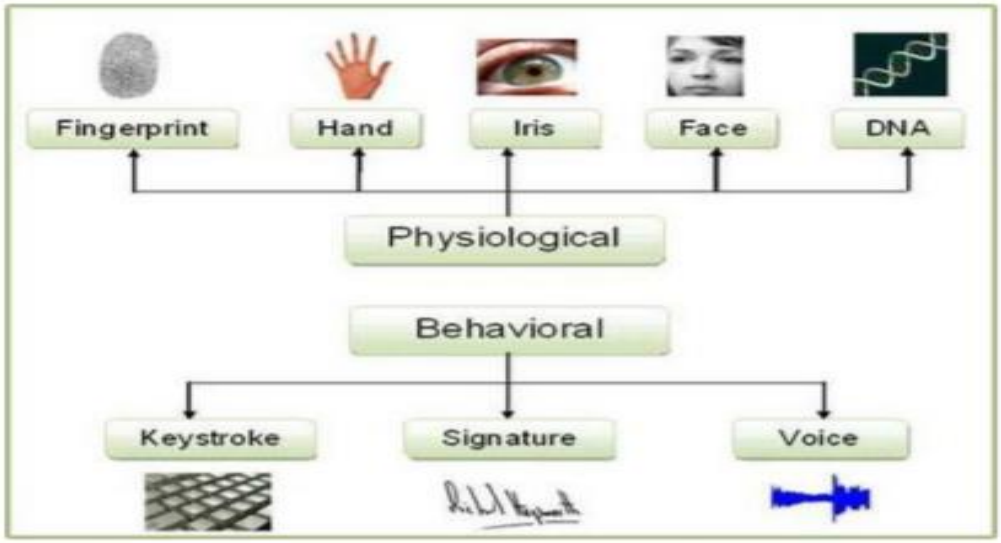


Figure 2.1: Categories of Biometrics

Two general uses of biometrics are identification and verification which both require the existence of reference data that the person's measured traits will be compared with reference templates or raw data.

During these processes, a biometric data sample is compared against the respective biometric data of every person enrolled in the database or against a single reference template of a particular enrolled individual to confirm the identity of that person respectively.

When a biometric system correctly identifies a person, then the result of the identification process is a true positive,
whereas if the system correctly rejects a person as not matching the respective enrolled template, the result is a true negative.
Similarly, when the system incorrectly identifies or rejects a person then we speak about a false positive or a false negative, the security aspects of which will be discussed in a subsequent section.

Examples of Popular Biometric Security

- Facial Recognition
- Iris Scanning
- Retinal Scan
- Fingerprinting
- Voice Recognition
- Vein Recognition
- Hand Geometry

The following are some application of Biometric Security Systems

- Banking
- Business Security
- Self Check-In
- Device Security
- Money Security
- Home Security

2.4 Cryptography and Network Security

Cybersecurity experts use cryptography to design algorithms, ciphers, and other security measures that codify and protect company and customer data. Thus cryptography is essential to many models of cybersecurity. Cryptography applies algorithms to shuffle the bits that represent data in such a way that only authorized users can unshuffle them to obtain the original data. Encryption is needed for the following reasons:

1. **Confidentiality (secrecy)**
2. **Integrity (anti-tampering)**
3. **Authentication**
4. **Nonrepudiation**
5. **Access Control**
6. **Availability**

1. **Cryptography**

The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography, thus Encryption is the process of encoding a message so that its meaning is not obvious. A message is plaintext (sometimes called clear text). The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is cipher text. The process of turning cipher text back into plaintext is decryption.

2. **Encryption and Decryption**

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system. The various components of a basic cryptosystem are as follows:

- **Plain text**
- **Encryption Algorithm**
- **Cipher text**
- **Decryption Algorithm**
- **Encryption Key**
- **Decryption Key**

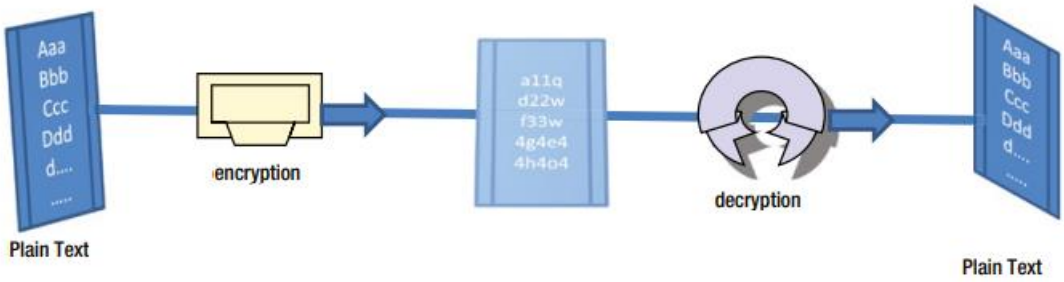


Figure (1): The components of a basic cryptosystem

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces يشمل both cryptography and cryptanalysis

- **Types of Cryptography**

A. Symmetric Key Cryptography
B. Asymmetric Key Cryptography
C. Hash Functions

A. Symmetric Key Cryptography

Also known as Secret Key Cryptography or Conventional Cryptography, Symmetric Key Cryptography is an encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. The Algorithm use is also known as a secret key algorithm or sometimes called a symmetric algorithm. A key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. The key for encrypting and decrypting the file had to be known to all the recipients. Else, the message could not be decrypted by conventional means.

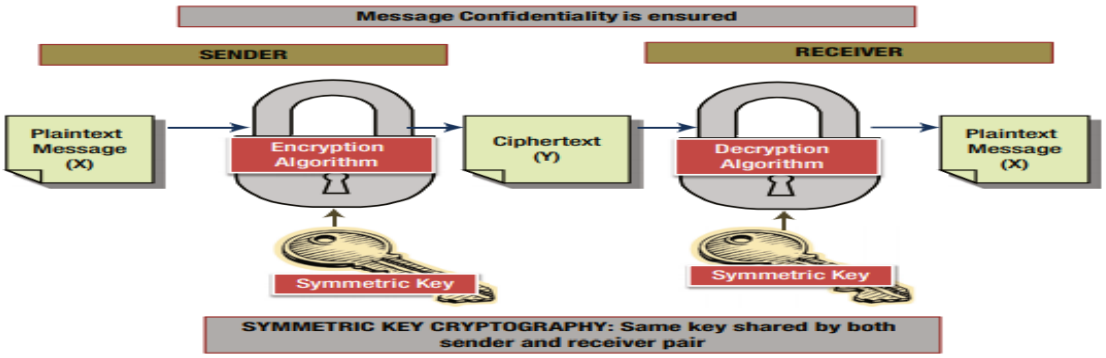


Figure (2) : Symmetric Key Cryptography

Symmetric Key Cryptography - Examples

- **Data Encryption Standard (DES): The Data Encryption Standard was published in 1977 by the US National Bureau of Standards. DES uses a 56 bit key and maps a 64 bit input block of plaintext onto a 64 bit output block of cipher text. 56 bits is a rather small key for today's computing power.**
- **Triple DES Triple: DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES.**
- **Advanced Encryption Standard (AES): Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES)**

- **Problems with Conventional Cryptography**

Key Management Symmetric-key systems are simpler and faster; their main drawback is that the two parties must somehow exchange the key in a secure way and keep it secure after that. Key Management caused nightmare for the parties using the symmetric key cryptography. They were worried about how to get the keys safely and securely across to all users so that the decryption of the message would be possible. This gave the chance for third parties to intercept the keys in transit to decode the top-secret messages. Thus, if the key was compromised, the entire coding system was compromised and a "Secret" would no longer remain a "Secret". This is why the "Public Key Cryptography" came into existence.

B. Asymmetric Key Cryptography

Asymmetric cryptography, also known as Public-key cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is private

and one of which is public. The public key is used to encrypt the message and the private one is used to decrypt the message.

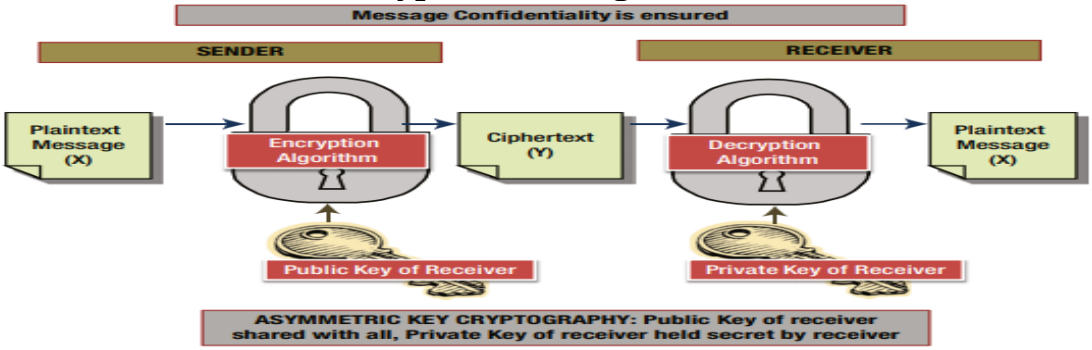


Figure (3) : Public Key Cryptography – How Confidentiality is ensured

The Public Key Cryptography (PKC) concept was invented by Whitefield Diffie and Martin Hellman in 1976 paper. The primary benefit of the PKC is that only the public key is shared, the need to share private key via some secure channel is eliminated, and private keys are not transmitted or shared. A public key system is constructed using a mathematically infeasible solution where one key cannot be generated using the other key and both the keys are required for a secured communication. There are many algorithms based on PKC, but the most popular ones are:

- **Diffie Hellman**
- **RSA (Rivest, Shamir, Adleman)**
- **Digital Signature Algorithm**
- **Elliptical Curve Cryptography (ECC)**

- **Asymmetric Key Cryptography - Examples**

Algorithm - RSA

RSA (Rivest, Shamir and Adleman who first publicly described it in 1977) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations; the following figure illustrates the RSA algorithm

- **Key Generation**

  Select two large primes p and q, such that $p \neq q$.
  $n = p * q$.
  $\varphi(n) = (p-1)*(q-1)$, where φ is Euler's totient function.
  Select an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n))=1$ (coprime).
  $d = e^{-1} \bmod \varphi(n)$
  Public key $\leftarrow (e,n)$
  Private key $\leftarrow d$

- **Encryption**

  $c = m^e \bmod n$

- **Decryption**

  $m = c^d \bmod n$

Example of RSA Algorithm

- **Choose p = 3 and q = 11**
- **Compute n = p * q = 3 * 11 = 33**
- **Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20**
- **Choose e such that 1 < e < φ(n) and e and φ (n) are coprime. Let e = 7**
- **Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]**
- **Public key is (e, n) => (7, 33)**
- **Private key is (d, n) => (3, 33)**
- **The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$**
- **The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$**

Heart of cryptographic network communication is the public key Infrastructure (PKI), which is used to encrypt the TCP/IP communication between two network end points.
Public Key Infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.
The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method, and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.
PKI uses various encryption algorithms to ensure data security.
The whole idea behind encryption is to make it so difficult that it becomes a time consuming task to try out all the possible keys. For example, if a message is encrypted using an 8bit key, it means that 256 different combinations of the key need to be tried, to decrypt the data. Any computer can perform this task in less than a second. However if the key length is extended to 32, it would need 65536 combinations to be tried, needing few seconds. Extending this trick further, a 256 bit key would result into a large number of combinations, thus needing literally many years even for a powerful computer to crack it.

C. Hash Functions

A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string; a hash function usually means a function that a compress, and the output is shorter than the input. Often, such a function takes an input of arbitrary or almost arbitrary length to one whose length is a fixed number, like 160 bits. Hash functions are used in many parts of cryptography, and there are many different types of hash functions, with differing security properties. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digests.

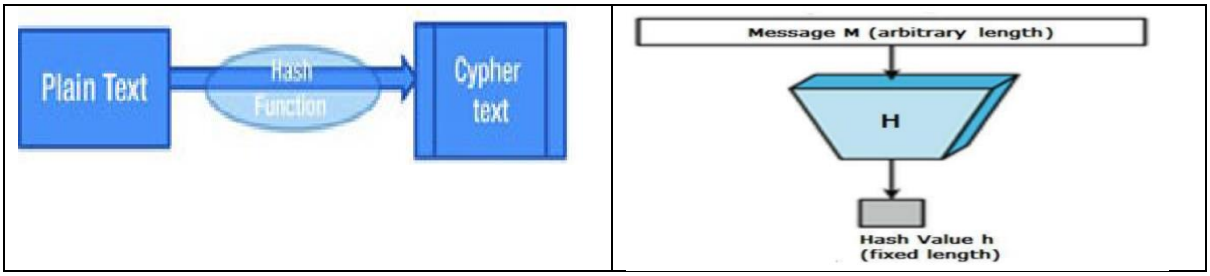


Figure (4) : A cryptographic hash function

Fundamentally, Hashing is defined by two distinct characteristics – irreversibility and uniqueness. Irreversibility points to the fact that once you hash something, there is no way back. Unlike Encryption and Encoding, you can't easily de-hash a message/data. Unique, because no two hash values are ever the same for two different pieces of data. If two hashes are found to be the same for two different pieces of data, it's called a 'hash collision' and that algorithm becomes useless.

Examples of Hash Function

SHA1 , SHA2, Message Digest MD2 , MD4, MD5 and MD6

2.5 Deception Technology

The aim of deception technology is to prevent a cybercriminal that has managed to infiltrate a network from doing any significant damage. **The technology works by generating traps or deception decoys that mimic legitimate technology assets throughout the infrastructure**. These decoys can run in a virtual or real operating system environment and are designed to trick the cybercriminal into thinking they have discovered a way to escalate privileges and steal credentials. Once a trap is triggered, notifications are broadcast to a centralized deception server that records the affected decoy and the attack vectors that were used by the cybercriminal.

Honeypots were the first form of **deception** technology. IT security researchers started using them in the 1990s, with the intent to **deceive** malicious actors who had made it onto the network into interacting with a false system. In this way, **honeypots** could gather and assess the behavior of the malicious actors

This however means that a honeypot can be anything - a program sitting on a computer logging all the users who log into the system and by means they log into, just a dummy account on the system which when logged into generates an alarm, and to some very extent it could even not be a computer system but just a mouse trap inside the computer cabinet which when touched traps a intruder's hands. In this broad sense any resource can be a honeypot, which unravels its existence just by unauthorized penetration or access to that resource.

This next generation of deception technology is smarter, too. **Automation and machine learning** support rapid deployment and touch-free refreshes to maintain deception authenticity. Intelligent deception systems can recommend and craft customized network, system, application, server and data deceptions that appear native to the environment.

2.6 Denial of Service(DoS)

A denial-of-service (DoS) attack is a type of cyber-attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by **overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users**. A DoS attack is characterized by using a single computer to launch the attack.

DoS attacks typically fall in 2 categories:

1. **Buffer overflow :** An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of-service.

- **Flood attack by** saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service.
- **Example :** Amazon Web Services, 2020
- **Denial of Service Filters,: it** Identifies sources as authenticated users, or by IP address or session ID. The DoS Filter keeps track of the number of requests from a

source per second. The **filter** gives first priority to authenticated users, then to connections identified by IP addresses

2.7 Ethical Hacking القرصنة الأخلاقي

Ethical Hacking is an authorized practice of bypassing system **security** to identify potential data breaches and threats in a **network**. The company that owns the system or **network** allows **Cyber Security** engineers to perform such activities in order to test the system's defenses

Ethical Hacking is a part of **Cyber Security**. **Cyber Security** isn't one set thing, it's a rainbow of skillsets, tools, and passions – often combined, to make the most effective **secure** environment.

An ethical hacker, also referred to as a white hat hacker, is an information security (InfoSec) expert who penetrates a computer system, network, application or other computing resource on behalf of its owners -- and with their authorization. Organizations call on ethical hackers to uncover potential security vulnerabilities that malicious hackers could exploit.

Benefits of Ethical Hacking

1. Weak points of a system can be easily found and resolved by performing penetration testing.
2. Implement solutions for vulnerabilities to prevent security breaches.
3. Ethical Hacking protects data from being stolen by 'black-hat hackers.', "**Black Hat hackers** are criminals who break into computer networks with malicious intent. They may also release malware that destroys files, holds computers hostage, or steals passwords, credit card numbers, and other personal information"
4. It helps protect networks with continuous assessments.
5. Customers and investors will trust company if the security of the data and the system is well maintained.

Now, it might be thinking that Ethical Hacking and Cyber Security are the same as their purpose of protecting the system from malicious attacks is similar. However, there is indeed a difference between Ethical Hacking and Cyber Security.

Table (2.1) Difference between Ethical Hacking and Cyber Security

Cyber Security	Ethical Hacking
It deals with protecting data and the syste malicious activities by recognizing and re all security issues	The purpose of Ethical Hacking is to find vulnerabilities in the system and report it to owner
The focus is on how to protect the system	The focus is on how to attack the system
Cyber Security is a broad term that includ various security techniques	Ethical Hacking is part of Cyber Security
It offers professions like Security Analyst Engineer, etc.	Penetration Tester and Security Manager are major Ethical Hacking roles
Cyber Security is on the defensive side	Ethical Hacking is on the offensive كرهside

It is responsible for developing access pri for a system	It is responsible for making reports on 'how hack was performed'
It identifies issues and protects the system security violations	It exploits the weaknesses or performs penet testing to identify weaknesses
Regular maintenance is done in Cyber Se ensure that the security system is updated	Regular testing on the system is done to disc flaws present in it and to resolve those issue

2.8 Social Engineering

Social engineering as one of the simplest methods to gather information about a target through the process of exploiting human weakness that is inherits to every organization. In a cybersecurity context, it is primarily used to induce victims towards disclosing confidential data, or to perform actions that breach security protocols, unknowingly infecting systems or releasing classified information.

The most dangerous element of social engineering is that it deals with human vulnerabilities rather than system failure or network vulnerabilities

Social engineering attacks: is a psychological **attack** against a company or an organization that **aims** to exploit people's natural tendency to trust others

A social engineering attack can be classified by one of two possible categories:

1. **Hunting**: This approach seeks to execute the social engineering attack through minimal interaction with the target. Once the specified objective is achieved and the security breach is established, communication is likely to be terminated. This is the most frequently used methodology to support cyberattacks .
2. **Farming:** Social engineering farming is not often practiced; nevertheless this technique may be used for situational purposes. The attacker aims to establish a relationship with the victim in order to extract information for a longer period of time. Throughout the process, the interaction can change, the target may learn the truth and the social engineer may attempt to bribe or blackmail the target, thus resorting to traditional criminal behavior.

Some of most common examples of social engineering attacks are: Phishing ,Spear Phishing , Baiting, Malware, Quid Pro Quo, Tailgating , Vishing.

2.9 Firewalls

The most common first line of defense in a network connected to the Internet is a *firewall.* These devices usually consist of some combination of hardware and software used to protect a private network from unauthorized access by way of the Internet. This is accomplished by limiting security exposures, enforcing the organization's security policy, and sometimes logging or monitoring Internet activity.

Firewalls can be implemented in various ways in different network arrangements. A firewall might be a mission-specific hardware device, or it may be a function that is built into a router or switch, or it may be implemented in a computer that has multiple Ethernet interfaces. It can even be a pure software firewall installed on a host computer like any other application. Many network appliances are available that offer firewall and security capabilities along with other network features.

In a corporate or industrial network environment, the administrator controls firewall installations and configurations. The advantage of the network firewall is that it enables

the administrator to control the flow of information to all the devices attached to their network, but its *disadvantage* is that firewalls cannot prevent internal threats, virus attacks and authentic mechanisms used by hackers (like username password). Network firewall illustrated in following figure :

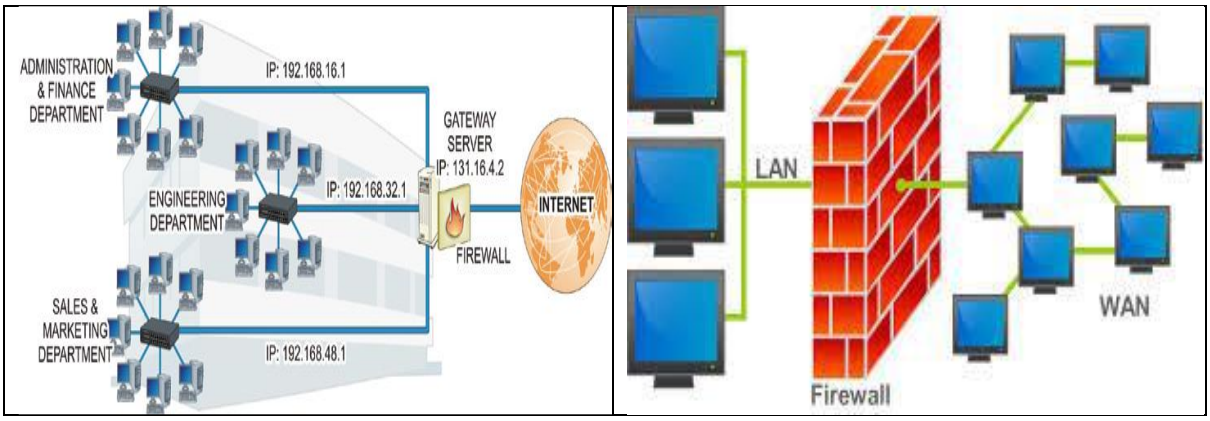


Figure (1) : Network Firewall

Firewalls must act as gateway devices, authorizing and granting access to both network applications and protocols. They might also act as proxy servers, provide Network Address Translation, and act as DHCP servers. Firewalls typically also filter both incoming and outgoing traffic.
A good firewall will provide packet filtering using defined rules to reject or accept both incoming and outgoing packets. This can be more challenging to configure, but effective firewall rules are really critical to security.
A packet-filtering firewall can be established through routers by configuring them with packet-filtering rules to allow or deny client access based on factors such as their source address, destination address, or port number. There are generally two types of packet-filtering firewalls to consider: static packet filtering and stateful packet filtering.

- **Packet-filtering firewalls** are considered not to be very secure. This is because they will forward any traffic that is flowing on an approved port. So there could be malicious traffic being sent, but as long as it's on an acceptable port, it will not be blocked.

- **Stateful inspection firewalls** are considered more secure than packet filtering firewalls. Stateful inspection firewalls process application layer data. Therefore, they are able to take a deeper look into the transaction to understand what is going on.

2.9Intrusion Detection Systems

Every day, new vulnerabilities and malicious code threaten systems on networks. The constant update of threats requires strenuous patching schedules and antivirus updates. Patching and antivirus updates in an enterprise environment take time, which prolongs the period in which devices are vulnerable. In the event that no patch exists for a given vulnerability (such a case is known as a zero-day vulnerability), devices are vulnerable

for an even longer period while the vendor develops a patch. There is a need for systems to detect vulnerabilities and malicious code activity during these vulnerable periods. **Intrusion Detection System** (IDS) can satisfy this need very quickly, as these devices can receive one update and detect malicious activity across an entire network of computers.

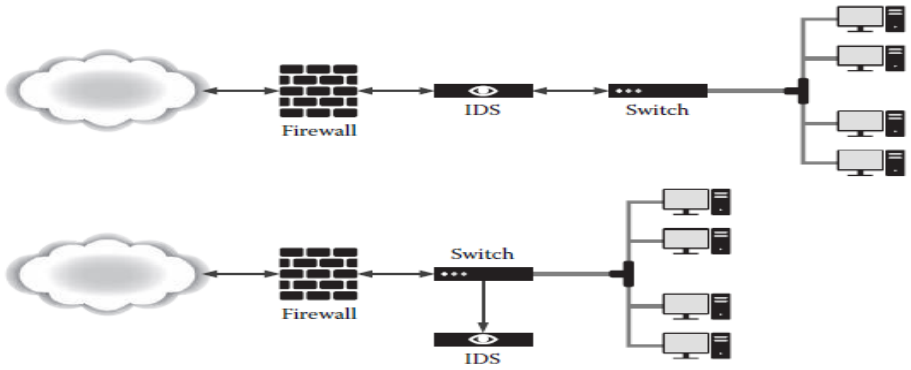


Figure (2) : IDS

An IDS is a device that monitors network traffic for malicious activity. IDS devices, referred to as sensors, detect malicious activity by searching through traffic that traverses a network. The IDS sensor requires access to network packets, which is possible through two different implementations called **out of line** and **inline.**

2.10 Incident Response

Incident response (IR) is a structured methodology for handling security incidents, breaches, and cyber threats. A well-defined incident response plan (IRP) allows you to effectively identify, minimize the damage, and reduce the cost of a cyber-attack, while finding and fixing the cause to prevent future attacks. Example : Incident Response Plan created by NIST

NIST INCIDENT RESPONSE PROCESS
1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity

2.11 Scanning

Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the **network**. **Network scanning** is used to create a profile of the target organization

Scanning has three types:

- Port scanning - used to list open ports and services.

- Network scanning - used to list IP addresses.
- Vulnerability scanning - used to discover the presence of known vulnerabilities

2.12 Security policy

Cybersecurity policy sets the standards of behavior for activities such as the encryption of email attachments and restrictions on the use of social media.

Improved **cybersecurity policies** can help employees and consultants better understand how to maintain the **security**

Three main types of policies exist:

- Organizational (or Master) **Policy**.
- System-specific **Policy**.
- Issue-specific **Policy**

2.13 Threat Management.

Threat management is a process used by **cybersecurity** professionals to prevent **cyber**-attacks, detect **cyber threats** and respond to **security** incidents

Threat management is an exercise of using a combination of the detection system, like intrusion detection system (IDS), event management (SIEM)
and security information system, etc.

A threat management platform, a system designed to enable a security team to address potential cyber threats against the entire enterprise from a single location, is an essential component of an organization's network security strategy. By unifying threat management across the entire organization, it enables cybersecurity analysts to more quickly and effectively respond to potential cyberattacks and other incidents.

Effectively managing cyber threats requires more than identifying and responding to ongoing attacks against the organization. Minimizing the potential damage and cost associated with these attacks requires proactive security policies and tools capable of identifying and blocking these attacks.

Chapter Three
Cybersecurity Architecture and Operations

3. 1 Cybersecurity Architecture

Cybersecurity architecture combines security software and appliance solutions, providing the infrastructure for protecting an organization from cyber-attacks and ensures that all components of its IT infrastructure are protected.

The Cybersecurity architecture should be able to adapt to the evolving cyber threat landscape as organizations engage in digital transformation initiatives and expand IT services beyond the traditional perimeter. With cyber threats existing inside and outside the security perimeter, it has become essential for security architecture to be based on a Zero Trust framework.

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data

When cyber-security architecture adheres to all seven principles of the Zero Trust security model (devices, people, data, networks, workload, automation & orchestration, visibility & analytics) an enterprise can secure data and IT resources wherever they reside.

The primary goals of **effective cybersecurity architecture** are:

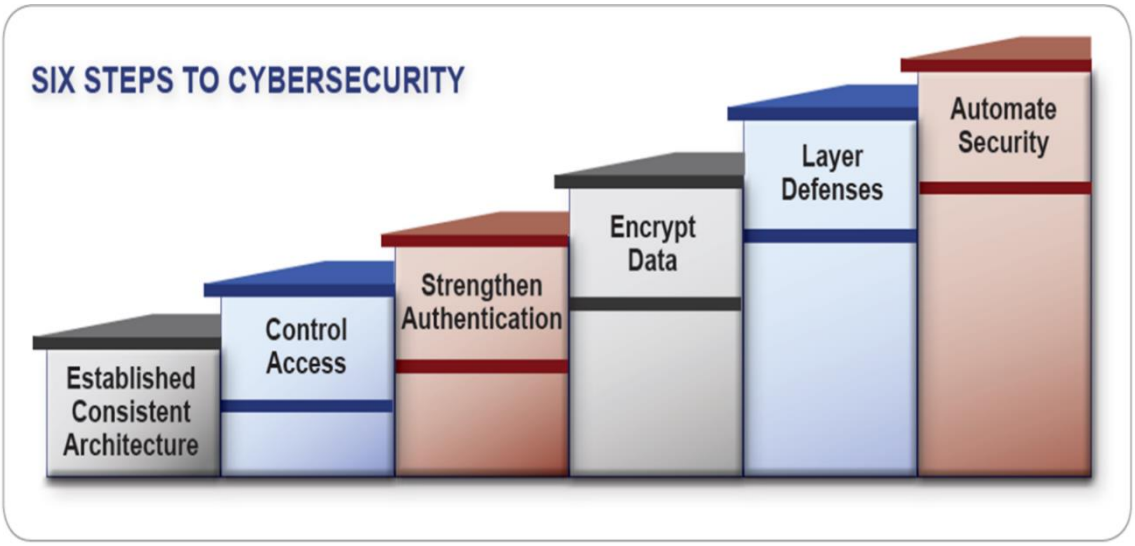
1. To ensure that all cyber-attacks are minimized, mitigated against, hidden or dynamic.
2. To ensure that cyber-attack surfaces should be relatively small in size, covertly stored, so that they are stealth in moving towards threat targets and difficult for cyber threats to detect and penetrate.
3. To make sure all confidential and sensitive data is strongly encrypted, and be subject to end-to-end encryption techniques during transfer.
4. All cyber-attacks are aggressively detected, mitigated, and countered using countermeasures like Moving-Target Defenses (MTD).

Environments that are secured by cybersecurity architecture include:

- Networks
- Cloud
- IoT
- Endpoints
- Mobile

Trusted Computing Group (TCG's) cybersecurity standards, addressed six steps to Cybersecurity for maximum effectiveness, cybersecurity programs should take the following six steps:

- **Establish consistent architecture.** Use consistent security architecture across all devices and networks. This enables security policies to be written once.
- **Control access.** Know who and what's on your network, check the health of the devices on your network, and then use access controls to ensure that only authorized personnel with secure devices are granted access to sensitive data.
- **Strengthen authentication.** Require strong user and machine authentication for any accesses to most valuable assets .
- **Encrypt data.** Encrypt all sensitive data in transit and at rest.
- **Layer defences.** Layer security defences, not only to repel attacks but to better contain intrusions.
- **Automate security.** Automate security controls to provide rapid attack detection and response. Automation frees scarce information security resources from dealing with spam, malware, and other nuisances, allowing them to focus on more high-value security activities, such as refining policies and remediating attacks.



Figure(1): six steps should take for maximum effectiveness, cybersecurity programs

3.2 Features of Cybersecurity Architecture

The following are **some of the features** of cybersecurity architecture:

- **Network Elements:**
  - Network nodes like computers, NICs, repeaters, hubs, bridges, switches, routers, modems, gateways.
  - Network communication protocols (TCP/IP, DHCP, DNS, FTP, HTTP, HTTPS, IMAP)
  - Network connections between nodes using specific protocols
  - Network topologies among nodes such as point-to-point, circular, chain, and hybrid
- Security Elements
  - Cybersecurity devices like firewalls, Intrusion Detection/Protection Systems [IDS/IPS], encryption/decryption devices.
  - Cybersecurity software (anti-virus software, spyware software, anti-malware software)
  - Secure network communication protocols (TCP/IP, DHCP, DNS, FTP, HTTP, HTTPS, IMAP).
  - Strong encryption techniques like end-to-end encryption, zero-knowledge privacy, blockchain.
- **Security Frameworks & Standards**
  - Cybersecurity framework architecture standards like NIST Risk Management Framework (RMF) SP 800-37 and ISO IEC 27000-Series.
  - Technology standards for cybersecurity software choices.
- **Security Procedures & Policies**
  - These are security procedures and policies directed towards your organization and enforced. According to Cybersecurity Forum, cybersecurity architecture should ideally be definable and simulatable using an industry-standard architecture modeling language (e.g., SysML, UML2).

3. 3 Cybersecurity Architect

The purpose of cybersecurity architecture is simply to ensure that the main network architecture of the company including: sensitive data and critical applications are fully protected against any present or future threats and breaches. Thus it's important to understand the various weak points in the system in order to effectively and quickly proffer a solution. The best way to identify system's weak point is to employ the services of a cybersecurity architect

Cybersecurity architect: is a senior-level position responsible for planning, designing, testing, implementing and maintaining an organization's computer and network security infrastructure. The role requires thorough knowledge of the employer's business and a comprehensive understanding of the technology it uses to conduct operations.
Several key attributes of an effective cybersecurity architect include:

1. The ability to think like a malicious hacker to anticipate and defend one's organization against information security risks
2. The ability to think like a business executive, manage security team members and communicate effectively with key stakeholders
3. The experience and technical expertise to build security infrastructure from scratch or update existing systems in response to ongoing changes in the security landscape, including new risks and adherence to applicable regulations

.

- TCG , Trusted Platform Module (TPM) was conceived by a computer industry consortium called Trusted Computing Group (TCG), and was standardized by International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) in 2009 as ISO/IEC 11889

Intrusion Detection system

What is intrusion detection

Process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusion.

Types of Intrusion Detection Systems

Information Sources: the different sources of event information used to determine whether an intrusion has taken place.

Network-based IDS

Host-based IDS

Application-Based IDS

Analysis: the most common analysis approaches are

Misuse Detection

Anomaly Detection

Response: the set of actions that the system takes once it detects intrusions.

Passive measure: reporting IDS findings to humans, who are then expected to take action based on those reports.

Active measure: involving some automated intervention on the part of the system.

Misuse Detection (signature-based ID)

Looking for events or sets of events that match a predefined pattern of events that describe a known attack. The patterns are called signatures.

Rule-based systems: encoding intrusion scenarios as a set of rules.

State-based intrusion scenario representations.

Advantages:

Very effective at detecting attacks without generating an overwhelming number of false alarms.

Disadvantages

Can only detect those attacks they know about—therefore they must be constanly updated with signatures of new attacks.

Many misuse detectors are designed to use tighly defined signatures that prevent them

from detecting variants of common attacks.

Anomaly Detection

Identify abnormal unusual behavior (anomalies) on a host or network. They function on the assumption that attacks are different from “normal” (legitimate) activity and can therefore be detected by systems that identify these differences.

Static and dynamic:

Static: Static means a portion of the system remain constant, e.g. data integrity, tripwire, virus checkers.

Dynamic: profile. A profile consists of a set of observed measures of behavior for each

of a set of dimensions. Frequently used dimensions include:

- Preferred choices, e.g., log-in time, log-in location, and favorite editor.
- Resources consumed cumulatively or per unit time

- Representative sequences of actions.
- Program profiles: system call sequence.

Methods

Threshold detection: certain attributes of user and system behavior are expressed in terms of counts, with some level established as permissible. Such behavior attributes
can include the number of files accessed by a user in a given period of time, the number of failed attempts to login to the system, the amount of CPU utilized by a process, etc.

Statistical measures

- Parametric: The distribution of the profiled attributes is assumed to fit a particular pattern
- Non-parametric: The distribution of the profiled attributes is "learned' from a set of historical values, observed over time.

Rule-based measures: similar to non-parametric statistical measures in that ooberved data defines acceptable usage patterns, but differs in that those patterns are specified as rules, not numeric quantities.

Other methods:

- Machine learning
- Data mining
- Neural networks, genetic algorithms, etc.

Advantages

Can detect unusual behavior and thus have the ability to detect symptoms of attacks without specific knowledge of details.
Can produce information that can in turn be used to define signatures for misuse detectors.

Disadvantages

Usually produce a large number of false alarms due to the unpredictable behaviors of users and networks.
Often require extensive "training sets" of system event records in order to characterize normal behavior patterns.

Host-based IDS

Using OS auditing mechanisms: e.g. BSM in Solaris logs all direct and indirect events generated by a user; `strace` monitors system calls made by a program.
Monitoring user activities: analyzing shell commands.
Monitoring executions of system programs, e.g. `sendmail`'s system calls.

Advantages

Can detect attacks that cannot be seen by NIDS
Can operate in an environment in which network traffic is encrypted
Unaffected by switched networks
Can help detect Trojan horse or other attacks that involve software integrity breaches

Disadvantages

Since at least the information sources reside on the host targeted by attacks, the IDS may be attacked and disabled as port of the attack
Are not well suited by detecting network scans or other such surveillance that targets an entire network

Since they use the computing resources of the hosts they are monitoring inflicting a performance cost on the monitored systems.

Chapter Four

Cybersecurity management

4. 1 Cybersecurity Management

Cybersecurity management is an organization's strategic-level capability to protect information resources and competitive advantage in a complex and evolving threat landscape.

Today's highly dynamic and fast-paced business environment shapes the way in which enterprises use their assets such as digital processes, information and IT systems to gain a competitive advantage. These assets are increasingly exposed to security threats, both external and internal, such as theft, fraud, sabotage, embezzlement, and industrial espionage. Cybersecurity management mitigates the risk exposure of organizations using a range of managerial, legal, technological, process and social controls.

Management should instruct the executive in charge of implementing cybersecurity measures (CISO etc.) on the following ten important directions.

Direction 1 : Recognize cybersecurity risk and develop a company-wide policy

Recognize cybersecurity risk as one important element among a variety of management risks and develop a company-wide policy (security policy)

Direction 2 : Build a management system for cybersecurity risk

Establish a structure for cybersecurity risk management (including defining the responsibility of each relevant person) in order to implement cybersecurity measures. In doing so, make sure that such structure is consistent with other risk management structures within the organization

Direction 3 : Secure resources (budget, workforce etc.) for cybersecurity measures

Secure the budget to implement measures for cybersecurity risks and provide training for cybersecurity personnel.

Direction 4 : Identify cybersecurity risks and develop plans to address them

Identify information that should be protected from the perspective of corporate strategy, identify cybersecurity risks from the threat of cyber-attacks and level of its impact, and develop a plan for such risks. In that process, consider measures of risk transfer (cyber insurance, outsourcing etc.) and finally identify residual risks

Direction 5 : Establish systems to effectively address cybersecurity risks

Establish a system to implement protection measures (measures for protection, detection and analysis) in order to address cybersecurity risks.

Direction 6 : Implement a PDCA cycle for cybersecurity measures

Implement cybersecurity measures as a PDCA cycle in order to execute and improve plans. As part of the PDCA cycle, regularly report the status of measures to management and make improvements if a problem occurs. Disclose the status of measures to enhance the trust of stakeholders

Direction 7 : Develop a cybersecurity incident response team and relevant procedures

Establish a response structure within the organization (CSIRT, etc.) to identify the scope of impact and damage, take initial action in order to prevent further damage, and implement measures to prevent similar incidents from happening. Decide what information should be reported to whom in case of emergency, and support management to report that information to internal and external stakeholders appropriately.

Direction 8 : Develop a recovery team and relevant procedures in preparation for damage due to cyber incidents

if business operations are suspended due to an incident, set recovery goal (by when operations should recover), taking into consideration the impact on corporate management, make a recovery procedure manual and develop a structure for recovery. The recovery goal and plan should be consistent with organization-wide plans such as BCP. Additionally, execute practical drills to prepare for recovery from the suspension of operations

Direction 9 : Understand cybersecurity status and measures in the entire supply chain including business partners and outsourcing companies

A PDCA cycle of cybersecurity measures including auditing etc. should cover group companies, business partners and outsourcing companies in the company's supply chain. When considering outsourcing operations such as systems management, the boundary between insourcing and outsourcing should be set appropriately.

Direction 10 : Gather, utilize, and provide cyber-threat information through information sharing activities

In order for the whole society to have capability against latest cyber-attacks, participate in information sharing activities on cyber-attacks. Additionally, develop environments to effectively utilize the information obtained

4.2 Risk management

Management security controls, in conjunction with technical and operational controls, are implemented to manage and reduce the **risk** of loss and to protect an organization's mission.

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions.

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment.

- Risk Assessment:
  - Identify and describe each organizational system
  - Assess threats, vulnerabilities, likelihood of adverse actions, and potential consequences
  - Quantify the level(s) of risk based on the assessment
  - Develop a set of security controls based on the level(s) of risk

- Document decisions made during the assessment.
- Risk Mitigation
- Evaluate security controls and select those that provide the greatest level of risk reduction at the lowest cost
- Identify appropriate security controls and assign responsibility to those individuals who will implement and maintain those controls
- o Implement security controls and document the implementation to provide input to the configuration baseline.
- Evaluation and Assessment
- The first two activities (risk assessment and risk mitigation) are properly
- documented and reflected in the system baseline
- Security controls are implemented

The Plan-do-check-act **cycle** as shown in Figure 4.1 consists of four-step model for carrying out change. Just as a circle has no end, the **PDCA cycle** should be repeated again and again for continuous improvement. The **PDCA cycle** is considered a project planning tool

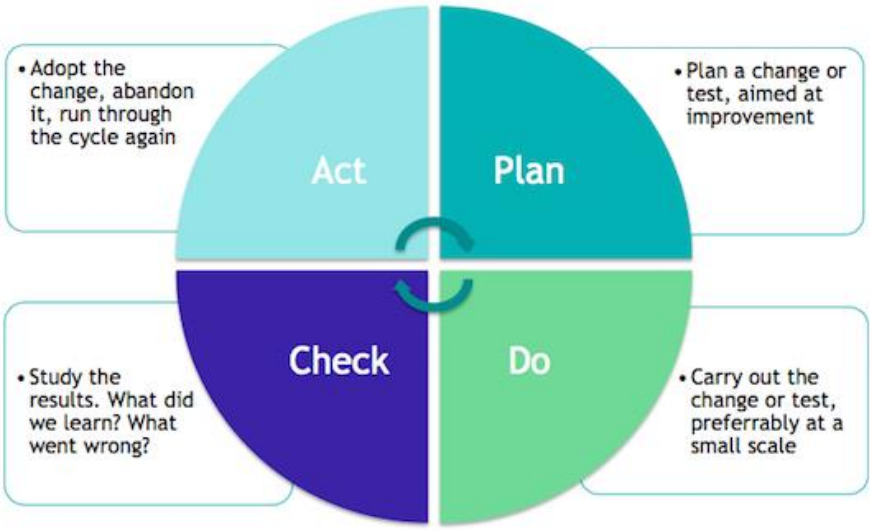


Figure 4.1: Plan-do-check-act **cycle**