

Cyber Security Essentials Chapter 1 Dr. Sarah Mohamed 1.1. Biometrics can be human characteristics, for instance, fingerprint, face recognition, iris recognition, retina and palm print as shown in the following figure: Figure 1: Biometric authentication methods

1.3.2 Encryption It is a technique to convert the data in unreadable form before transmitting it over the internet. There are many applications of steganography, which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft, digital watermarks for IPR issues, etc. Biometric based Authentication: Biometric based authentication is a security process that relies on the unique biological characteristics of an individual to identify the user's identity; biometric authentication is used to manage access to physical and digital resources such as buildings, rooms and computing devices. Authorization is the process of verifying what you have access to. There are three main types of authentication mechanisms, password entry, and smartcard and biometric. Software Firewalls: These firewalls are installed on the server and client machines and it acts as a gateway to the organization's network. Unknown: Those who have not presented authenticated credentials. Every individual who initially approaches an access control system is unknown until he or she attempts to authenticate. Password Based Authentication: The server maintains a list of names and passwords, if a particular name is on the list, and if the user types the correct password, the server grants access. Only the person who have the access to the key, convert it in the readable form, and read it. Formally, encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. 1.3.4 Firewall It is a hardware/software, which acts as a shield between an organization's network and the internet and protects it from the threats like virus, malware, hackers, etc. The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc. Identity management Identity management is the process of creating, maintaining, and removing user accounts and providing the mechanisms used to authenticate

users and providing the mechanisms used to authenticate users. Cyber security refers to the protection of computer devices, systems, networks and programs from cyberattacks. Attackers use new methods, which are powered by social engineering, artificial intelligence and machine learning, to bypass security checks. Token based Authentication: Token based authentication is a security technique that authenticates the user who attempt to login to a server, a network, or some other that authenticates the user who attempt to login to a server, a network, or some other secure system, using a security token provided by the secure system, using a security token provided by the server.

Figure 2: Encryption

1.3.3 Antivirus There are varieties of malicious programs like virus, worms, Trojan horse, etc. Using firewall, it is possible to configure and monitor the traffic of the ports (A port is a virtual point where network connections start and end. Technical methods, such as file system access controls and network firewalls, used to enforce policies. They utilize the network by collecting, processing, storing, and sharing vast amounts of digital information. As more digital information is gathered and shared, the protection of this information is becoming even more vital to our national security and economic stability.

1.3 Cyber security techniques There are many cyber security techniques to combat the cyber security attacks. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.)) Examples: Access control deals with subjects, objects and access rights as shown on the following figure: Organizations rely upon access controls to grant and restrict user access to information, systems, and other resources. Access control systems, when properly designed; implement business rules and often—direct implementations of policy in such a manner that individuals have access to the information and resources needed to perform their responsibilities but no more. Theoretically, identity management allows you to confirm that a person is who they claim to be (authentication), and access control allows you to restrict his or her activities to authorized actions (authorization). Objects—The resource to which the subject desires access (e.g., files, databases, subject desires access (e.g., files,

databases, printers, and physical facilities) printers, and physical facilities) Any time you have to decide whether to allow or deny access by a subject to a resource, Any time you have to decide whether to allow or deny access by a subject to a resource, you have entered the access control problem domain. you have entered the access control problem domain. Procedures: Nontechnical methods, such as business processes and background checks, used to enforce policies. Nontechnical methods, such as business processes and background checks, used to enforce policies ? On the other hand, if the user's password is correct, the system now knows with certainty who the user is and must check to see if the user is authorized to access the requested resource. Cyber security is protecting yourself from someone stealing your digital information/personal data or from pretending to act as you online. pretending to act as you online.

1.3.1 Authentication

1.3.1 Authentication It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. Authentication is a process of granting a user access to an information system. It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is already installed into the system. Only the packets from trusted source address can enter the organization's network and the sources, which are blacklisted and unauthorized address, are denied access to the network. Access controls define the allowable interactions between subjects and objects. Preventing legal users from accessing resources in an unauthorized manner ? Authorized: Those who have presented authenticated credentials and have been approved for access to the resource ? Unauthorized: Those who have presented authenticated credentials but are not approved for access to the resource ?

Introduction to cyber security

The connected electronic information network has become an integral part of our daily lives. Cyberattacks are a globally increasing and evolving threat to sensitive data. The next section discusses some of the popular techniques to counter the cyberattacks. Users are identified using different authentication mechanisms. In a security system, the authentication process checks the information provided by the user with the database that are spread over internet to compromise the security of a computer either to destroy data stored spread over internet to compromise

the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc. It is important to have firewalls to prevent the network from unauthorized access, but it is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly. A firewall can be implemented using hardware as well as software or the combination of both. hardware as well as software or the combination of both. Figure 4: Firewall Hardware Firewalls Hardware Firewalls: example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet. Access control implements a security policy that specifies who or what (e.g. process may have access to each specific system resource and the type of access that is permitted in each instance. Preventing unauthorized users from gaining access to resources (deals more with authentication) ? Subjects—The user, network, process, or application requesting access to a resource ? They utilize the network by collecting, processing, this network to operate effectively. As more digital information is storing, and sharing vast amounts of digital information. Cyber security is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm. At the company level, it is everyone's responsibility to protect the organization's reputation, data, and customers. Attackers use new methods, which are powered by social engineering, to sensitive data. Governmental and industry information systems from theft and damage attempted by criminals. The next There are many cyber security techniques to combat the cyber security attacks. Authentication is a process of validating the user's identity. Biometrics are a strong authentication method based on certain human characteristics. The human characteristics are distinct to each individual. To prevent these into the computer or gain financial benefits by sniffing passwords etc. It can be used to internet and protects it from the threats like virus, malware, hackers, etc. 1.3.5 Steganography It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. Access can be defined in terms of social rules, physical barriers, or can be defined in terms of social rules, physical barriers, or informational restrictions. The purpose of access control is to provide quick, convenient access control for authorized persons, while at the same time, restricting access for unauthorized people. Enabling legal users to access resources in an authorized

manner. users to access resources in an authorized manner. Access Control Systems Access Control Systems A well A well--defined access control system consists of three elements: ined access control system consists of three elements: ? Access Control Subjects Access Control Subjects The subject in an access The subject in an access--control scenario is a person or another application requesting control scenario is a person or another application requesting access to a resource such as the network, a file system, or a printer. Someone allowed to access the resource moves to the the resource moves to the ""authorizedauthorized"" state. Otherwise, the user is still known, but now state. Otherwise, the user is still known, but now moves to the moves to the ""unauthorizedunauthorized"" state.state.PPrivate ??????????????..?????????????????????..(informationrivate information ?(authorization