Cyber Security Essentials Chapter_1 Dr. Sarah Mohamed 1 1..Biometrics can be human characteristics, for instance, fingerprint, face recognition, Biometrics can be human characteristics, for instance, fingerprint, face recognition, iris recognition, retina and palm printiris recognition, retina and palm print as shown in the following figure: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 areThere are many applications of many applications of steganography, whichsteganography, which includes sending secret messages includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access without ringing the alarms, preventing secret files from unauthorized and accidental access and and theft,theft, digital watermarks for IPR issues, etc.digital watermarks for IPR issues, etc.Biometric based AuthenticationBiometric based Authentication:: Biometric based authentication is a security Biometric based authentication is a security process that relies on the unique biological characteristics of an individual to process that relies on the unique biological characteristics of an individual to identify the useridentify the user"ss identity;identity; biometric authentication is used to manage access to biometric authentication is used to manage access to physical and digital resources such as buildings, rooms and computing devices.physical and digital resources such as buildings, rooms and computing devices.Authorization is the process of verifying what you have access to. verifying what you have access to. TThere are three main types of authentication here are three main types of authentication mechanisms, password entry, mechanisms, password entry, and smartcardand smartcard and biometricand biometric:: ?Software Firewalls: Software Firewalls: These firThese firewewalls are installed andalls are installed and on the server and client machines on the server and client machines and it acts as a gaand it acts as a gateway to the organizationsteway to the organizations network.UnknownUnknown: Those who have not prese: Those who have not presented authenticated credentialsnted authenticated credentials Every individual who initially approaches an access control system is unknown until he or Every individual who initially approaches an access control system is unknown until he or she attempts to authenticate.Password Based AuthenticationPassword Based Authentication:: The server maintains a list of names and The server maintains a list of names and passwords, if a particular name is on the list, and if the user types the correct passwords, if a particular name is on the list, and if the user types the correct ppassword, the server grants access.assword, 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 1.3.4 FirewallFirewall It is a hardware/ It is a hardware/software, whichsoftware, which acts as a shield between an organizationacts as a shield between an organization"s network and the 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 program regularly updates its database and provides immunity to the system against these new viruses, worms, etc.new viruses, worms, etc.Identity management Identity management is the process of creating, maintaining, and is the process of creating, maintaining, and removingremoving user accounts user accounts and providing the mechanisms used to authenticate

usersand providing the mechanisms used to authenticate users.Cyber Cyber security refers to the protection osecurity refers to the protection of computer devices, systems, networks and f computer devices, systems, networks and programs from programs from cybercyber−−attacksattacks.Attackers use new methods, which are powered by social engineering, artificial intelligence and machine leartificial intelligence and machine learning, to bypass security checks.arning, to bypass security checks.Token based Authentication:Token based Authentication: Token based authentication is a security technique 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 1.3.3 AntivirusAntivirus There are There are varieties varieties of malicious programs like virus, worms, of malicious programs like virus, worms, TrojanTrojan horse, etc.Figure 3: Different antivirus available on the market Using firewall, it is possible to configure and mo Using firewall, it is possible to configure and monitor the traffic of the ports (nitor the traffic of the ports (A port is a A port is a virtual point where network connections start and end.ToolsTools:: Technical methods, such as file system access controls and network firewalls, Technical methods, such as file system access controls and network firewalls, used to enforce policiesused 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 informgathered and shared, the protection of this information is becoming even more vital to our ation is becoming even more vital to our national security and economic stability.national security and economic stability.1.3 1.3 CCyber security yber security techniquestechniques 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 bemails go to a different port than webpages, for instance, even though both reach a oth reach a computer over the same Internet connection.computer over the same Internet connection.)) Examples: Examples: ?Access control deals with Access control deals with subjects, objects and access rights as shown on the following subjects, objects and access rights as shown on the following figure:figure: Organizations rely upon access controls to grant and restrict user access to information, Organizations rely upon access controls to grant and restrict user access to information, systems, and other resources.Access control systems, when properly designed;designed; implement implement business rules and business rules and oftenoften−−directdirect implementations of policy in such a manner thaimplementations of policy in such a manner that individuals t individuals have access to the information and resources needed to perform their responsibilities but have access to the information and resources needed to perform their responsibilities but no more.no more.Theoretically, identity management allows you to confirm that a person is who they claim to be (authentication), 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 and access control allows you to restrict his or her activities to authorized actions (authorization).ObjectsObjects−−−−The resource to which the 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.ProceduresProcedures: Nontechnical methods, such as business processes and background : Nontechnical methods, such as business processes and background checks, used to enforce policieschecks, used to enforce policies ?On the other hand, if the user"s s password is correct, the system now knows with certainty who the user is and must check password is correct, the system now knows with certainty who the user is and must check to see if the user is authorizeto see if the user is authorized to access the requested resource.CyberCyber securitysecurity is protecting is protecting yourself yourself fromfrom someone stealing your digitalsomeone stealing your digital information/personal data or from 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 It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be.he/she claims to be. Authentication is a process of granting a user access to Authentication is a process of granting a user access to an information an information system.system.It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is alcode to enter the system but also detects and destroys the malicious code that is already ready installed into the system.Only the packets from trusted Only the packets from trusted ssource address can enter the organizationource address can enter the organization"s network and the s network and the sources, which are blacklisted and sources, which are blacklisted and unauthorized address,unauthorized address, are denied access to the network.Access controls define the allowable interactions between subjects and objects.Itcontrols define the allowable interactions between subjects and objects.Preventing legalPreventing legal users from accessing resources in an unauthorized mannerusers from accessing resources in an unauthorized manner ?AuthoAuthorizedrized: Those who have presented authenticated credentials and have been : Those who have presented authenticated credentials and have been approved for access to the resource approved for access to the resource ?UnauthorizedUnauthorized: Those who have presented authenticated credentials but are not : Those who have presented authenticated credentials but are not approved for access to the resource approved for access to the resource ?IntroductionIntroduction to cyberto cyber security security The connected electronic information network has become an integral part of our daily The connected electronic information network has become an integral part of our daily lives.CyberCyber--attacksattacks are a globally increasing and evolving threat are a globally increasing and evolving threat to sensitive data.The next section discusses section discusses some of the popular techniques to counter the cybersome of the popular techniques to counter the cyber--attacks.attacks.Users are identified using different authentication mechanismusing different authentication mechanismss.In a security system,system, the authentication process the authentication process checks the information provided by the user with the datachecks the information provided by the user with the database.base.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 usingbe 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 : example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. network is connected to the network outside the organization i.e. InternetInternet.Access control implements a security policy that specifies who or what (e.g. process may 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 ishave access to each specific system resource and the type of access that is permitted in each permitted in each instance.instance.Preventing Preventing unauthorized users from gaining access to resources (deals more with unauthorized users from gaining access to resources (deals more with authentication)authentication) ?SubjectsSubjects−−−−The user, network, process, or application requesting access to a resourceThe 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 Cyber security is the ongoing effort to protect these networked systems and all of the data security is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm.At the companycompany level, it is everyonelevel, it is everyone"s s resresponsibility to protect the organizationponsibility to protect the organization"s reputation, data, and customers.Attackers use new methods, which are powered by social engineering, to sensitive data.GGovernmental and industry information systems fromovernmental and industry information systems from theft and damage attemptheft and damage attempted ted by by criminals.criminals.The next There are many cyber security techniques to combat the cyber security attacks.Authentication is a process of validating the userAuthentication is a process of validating the user"s identity.Biometrics are a strong authentication method based on certain human Biometrics are a strong authentication method based on certain human characteristics.The human characteristics are distinct to each individualre 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 1.3.5 SteganographySteganography It is a technique of hiding secret messages in a document file, image file, and program or 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.informational restrictions.The purpose of access control is to provide quick, convenient access control for 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.authorized persons, while at the same time, restricting access for unauthorized people.Enabling Enabling legallegal 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--defdefined 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)..??????????????..????????????