UNIT III

Internet/Intranet Security Issues and Solutions: The need for Computer Security – Specific Intruder Approaches – Security strategies – Security tools – Encryption – Enterprise Networking and Access to the Internet – Antivirus programs – Security Teams.

2 MARKS

1. What is meant by File transfer?

- Using FTP and HTTP, users can request and send a variety of bulk data including databases, files in all formats, documents, software, images and voice.
- While useful and convenient, file transfer can be insecure both in terms of confidentiality and virus threats.

2. Define IP Spooling(Apr 2014)

- IP spooling is a technique that can lead to root access on a system.
- It is the tool that intruders often use to take over open terminal and login connections after they get root access.
- Because of IP spooling, no address-based authentication is possible.

3. Define Password guessing:

- Most host administrators have improved their password controls, but group accounts still abound, and password-dictionary and password-cracking programs can easily crack at least 10 percent of the passwords users choose.
- The deterrent is enforcement of good passwords

4. Describe about Password sniffing:

- CERT estimates that, in 1994, thousands of systems were the victims of password sniffers.
- On LANs, any internal machine on the network can see the traffic for every machine on that network.
- Sniffer programs exploit this characteristic, monitoring all IP traffic and capturing the first 128 bytes or so of every encrypted FTP or Telnet session.
- The deterrent is to utilize programs that provide on-time passwords.

5. What is meant by Telnet: (Apr 2014)

- Telnet enables users to log on to remote computers.
- Telnet does little to detect and protect against unauthorized access.

- Telnet is generally supported either by using an application gateway or by configuring a router to permit outgoing connection using something such as the established screening rules.

6. Discuss about Viruses: (Nov 2012)

- Viruses do not necessarily give intruders access to a computer system, but may be a way to copy and forward information or otherwise create denial-of-service problems
- A virus is a program that can infect other programs by modifying them to include a copy of itself.

7. Lists of various computer virus infractions:

- Alter data in files.
- Change disk assignments.
- Create bad sectors.
- Decrease free space on disk.
- Destroy FAT (FILE Allocation Table).
- Erase specific programs.
- Format specific programs
- Hang the system.
- Overwrite disk directory.
- Suppress execution of RAM resident programs.
- Write a volume label on the disk.

8. Define SATAN:

- SATAN (Security Administrator Tool for Analyzing Networks) is a vulnerability detection application designed to hack into Internet-connected hosts.
- It is a UNIX program that checks both local and remote hosts for vulnerabilities.
- SATAN is a program freely available via the Internet.

9. List out the various Components of SATAN:

- HTTP server that acts as dedicated SATAN Web server.
- Magic cookie generator that generates a unique 32-bit magic cookie that includes a session key.
- Policy engine that defines which hosts are allowed to be probed and to what degree.
- Target acquisition that decides exactly which probes to run on various hosts when performing data acquisition.
- Data acquisition to gather security-related facts about the targeted hosts.
- Inference engine that is driven by a set of rule bases and input from data acquisition.

- Report and analysis, based on its findings.

10. What is meant by Encrypted data:

- Encrypted data is binary data, which cannot be sent by standard electronic mail.
- The ASCII Armor encoding actually uses four ASCII characters to represent three binary characters.

11. Discuss about Standard file extensions

- .txt- is attached to files created by a text editor or word processor before the file is encrypted.
- .pgp- is attached to an encrypted binary file. It is also used for key rings.
- .asc- is attached to an ASCII-armored encrypted file.
- .bin-is created when you use PGP's key-generate option.

12. Define Anti-virus software: (Nov 2014)

It consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).

13. What is meant by Encryption:

- Encryption is used to protect the message from the eyes of others.
- Cryptographically secure ciphers are designed to make any practical attempt of breaking infeasible.
- Symmetric-key ciphers are suitable for bulk encryption using shared keys, and public-key encryption using digital certificates can provide a practical solution for the problem of securely communicating when no key is shared in advance.

14. Define Firewalls:

Firewalls are systems that help protect computers and computer networks from attack and subsequent intrusion by restricting the network traffic that can pass through them, based on a set of system administrator-defined rules.

15. Define Honey pots:

Honey pots are computers that are either intentionally or unintentionally left vulnerable to attack by crackers. They can be used to catch crackers or fix vulnerabilities.

16. What is meant by Intrusion-detection systems: (Apr 2013)

Intrusion-detection systems can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.

17. Define Pinging

The ping application can be used by potential crackers to find if an IP address is reachable. If a cracker finds a computer, they can try a port scan to detect and attack services on that computer.

18. Discuss about Social engineering

Social engineering awareness keeps employees aware of the dangers of social engineering and/or having a policy in place to prevent social engineering can reduce successful breaches of the network and servers.

19. Define S-HTTP

- S-HTTP is an extension of HTTP that provides a variety of security enhancements for the web.
- S-HTTP provides independently application security services for transaction confidentiality, authenticity/ integrity, and non-reputability of origin.

20. Define Secure Socket Layer (SSL)

- It is a transport layer security technique that can be applied to HTTP as well as to other TCP/IP-based protocols.
- The SSL protocol is designed to provide privacy between two communicating applications.

21. Define Electronic data interchange (EDI)

- EDI is defined as the inter-organization exchange of documents in standardized electronic form directly between computer applications.
- The ability to transmit EDI over the Internet has the potential to improve the penetration rate of this technology.

22. Define CERT

- Computer Emergency Response Team is a name given to expert groups that handle computer security incidents.
- The purpose of CERT-In is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country.

23. Define FIRST

- Forum of Incident Response and Security Teams (FIRST) is a collection of organizations modeled on the computer emergency response team idea.
- It is a voluntary umbrella organization that mainly offers help to systems administrators who find their systems under attack from intruders.

24. What are the two types of Anonymous remailers? (Nov 2012)

Anonymous remailers are of two types

1. Remailers that mask the sender's return address
2. Remailers that provide anonymity for both the sender and destination addresses.
   - **Privacy Enhanced Mail**
   - **Pretty Good Privacy**
   - **Multipurpose Mail Extension**

25. Define Network Security? (Apr 2012)

Network Security can be defined as the protection of network-connected resources against unauthorized disclosure, modification, utilization, restriction, incapacitation, or destruction. Hundreds of thousands of system are now connected to the internet. There is no accurate way of measuring the threat that may be launched by an inimical agent.

25. What are called as passive threats? (Apr 2012)

Passive threats involve monitoring the transmission data of an organization. The goal of the attacker is to obtain information that is being transmitted. In general, this is not the easiest task to undertake.

Two types,

- Release of message
- Traffic analysis

26. Difference between visa card and master card.(Nov 2014)

Visa's two levels. Visa offers two levels of benefits: base level and Visa Signature. Most of the company's base-level cards come with auto rental collision damage coverage, extended purchases warranties, unauthorized purchase coverage, emergency assistance and urgent card replacement.

MasterCard's three tiers. MasterCard offers three tiers of benefits: base, World and World Elite.MasterCard offers one notable service that Visa does not: price protection. If you buy an item with a MasterCard and the price is reduced within 60 days, MasterCard will cover the difference, though there are exclusions.

27. Define key and list out the keys.(Apr 2015)

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. Without a key, the algorithm would produce no useful result. In encryption, a key specifies the particular transformation of plaintext

into ciphertext, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

28. What is the use of anti virus software? (Apr 2015)

Antivirus (or anti-virus) software is used to safeguard a computer from malware, including viruses, computer worms, and Trojan horses. Antivirus software may also remove or prevent spyware and adware, along with other forms of malicious programs.

11 MARKS

1. **Explain in detail about internet /intranet security issues and solutions (or) Explain need for computer security (Nov 2014)(Apr 2015)**

NEED FOR COMPUTER SECURITY:

- A debate has taken place over the past decade whether security should be the burden of the host or of the network. To say that security is the responsibility of the internet is surely wrong. Both hosts and networks must be secure; the responsibility is at least equally shared, if not more slanted toward the hosts. Some believe that, pragmatically, given how information is actually hacked today, the major burden lies with the end system.
- Security addressed here relates to three general areas:
    1. Secure file/information transfers, including secure transactions.
    2. Security of information as stored on internet-connected hosts.
    3. Secure enterprise networks, when used to support web commerce.

❖ Implementing security involves assessing the possible threats to one's network, servers, and information. Security in an internet environment is important because information has significant value: information can be bought and sold directly or can be used to create new products and services that yield high profits. Security on the internet is challenging, prima, facie, because security involves understanding when and how participating users, computers, services, a and networks can trust one another, as well as understanding the technical details of network hardware and protocols.

REASONS FOR INFORMATION SECURITY:

❖ The requirements of information security in an organization have undergone two major changes in the last several decades.

❖ Computer and network security can be defined as the protection of network-connected resources against unauthorized disclosure, modification, utilization, restriction, incapacitation, or destruction. Hundreds of thousands of system are now connected to the internet. There is no accurate way of measuring the threat that may be launched by an inimical agent. However, as a gauge, internet security systems (ISS) made the following list from actual recent computer security breaches and news releases:

- The FBI estimated that American companies lose $ 7.5 billion annually to electronic attacks.
- There were over a half-million attacks against government computer just in 1995.
- It has been reported that the department of defense has found 88 percent of its computers are penetrable. In 96 percent of the cases where hackers got in, their intrusions went undetected.
- In recent year(1993), the Computer Emergency Response Team(CERT) found a 73 percent increase in security breaks.
- Russian computer hackers successfully breached a large number of Citicorpcoprorate accounts, stealing $400,000 and illegally transferring an additional $11.6 million (wall street journal, august 21, 1995).
- In April of 1995, SATAN was freely distributed on the internet.
- "The security of information systems and networks is the major security challenge of this decade and possible the next century", says scot charnel, chief, computer crimes unit, u.s.
- Nearly half of the respondents lost valuable information in the last two years;
- At least 20 respondents lost information worth more than $1 million.

PROTECTING RESOURCES:

- The term computer and network security refers in a broad sense to confidence that information and services available on a network cannot be accessed by unauthorized users. Security implies safety, including assurance of data integrity, freedom from unauthorized access, freedom from snooping or wiretapping, and
- Freedom from disruption of service, of course, just as no physical property is absolutely secure against crime, no host is absolutely secure.
- Data integrity is crucial, so is data availability. Because information can in prevent unauthorized read/write/delete. That is, network security must include a guarantee of privacy.

TYPES OF RISKS:

- The internet increases, the risk of security violations increases with it. Computer and security have evolved with computer technology, but the issues remain similar.
  - In the 1960s, computer security was not a significant issue. Dumb terminals attached to mainframe computers in effect fostered data security.
  - The 1970s saw the emergence of the ARPAnet, the internet of the academic world that interconnected several different defense contractors, defense agencies, and universities.
  - In the 1980s, enter the age of PCs, distributed networks and viruses, Researches stated that to show interest in confidentiality, integrity and availability of data.
  - With extensive use of the internet, today's enterprise networks and web servers are open to attack.

SECURITY THREATS:

- Some of the threats that simulated the upsurge of interest in security include the following
  - Organized and internal attempts to obtain economic or market information from completive organizations in the private sector.
  - Organized and intentional attempts to obtain economic information from government agencies.
  - Inadvertent acquisition of economic or market information
  - Inadvertent acquisition of information about individuals
  - International fraud through illegal access to computer respositories including acquisition of funding data, economic data, law enforcement data, and data about individuals.
  - Government intrusions on the rights of individuals
  - Invasion of individuals rights by the intelligence community.

PASSIVE THREATS:

- Passive threats involve monitoring the transmission data of an organization. The goal of the attacker is to obtain information that is being transmitted. In general, this is not the easiest task to undertake.

Two types,

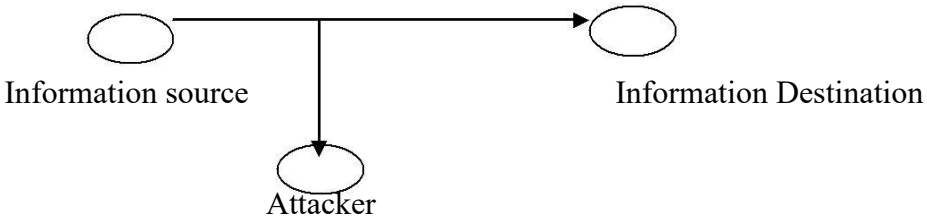
- Release of message
- Traffic analysis

Release of message:

❖ Is clearly a concern. A telephone conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information.

Traffic Analysis:

❖ Is more subtle and often is more applicable to military situations.

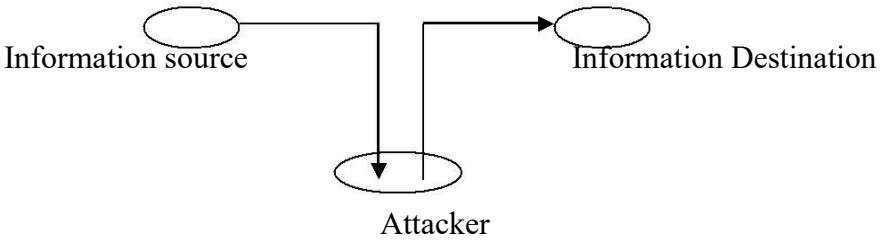


PASSIVE THREAT.

Active threats:

The second major category of threats is active threats . These involve some modification of the data stream to the creation of a false stream. One can clarify these into three categories:

- Message-stream
- Modification
- Denial of message service and masquerade



ACTIVE THREAT

❖ **Message –stream modification means** that some portion of a legitimate message is altered or that messages are delayed, replayed, or reordered to produce an unauthorized effect.

❖ **Denial of service prevents or inhibits** the normal use or management of communication facilities.

❖ **Masquerade** takes place when an attacker pretends to be someone else. A masquerade attack usually includes one of the other two forms of active attack.

2. Explain In Detail About Specific Intruder Approaches.

❖ The intruder approaches covers more detail in the following.

- Bulletin boards
- Electronic mail
- File transfer

- Ip spoofing
- Password guessing
- Password sniffing
- Telnet
- Viruses and SATAN

Bulletin boards:

❖ These internet services provide a clearinghouse for information and correspondence about a large variety of subjects. Many commercial organizations, especially technology houses, use them to provide customer service. Bulletin boards have been notorious hangouts for hackers and other antisocial types. A lot of pirated and virus-laden software appears on bulletin boards.

Electronic mail:

❖ This store-and-forward mail service allows users to communicate throughout the network, requiring only a target address and a point of access currently, e-mail is one of the most commonly used services and is all some organization use. E-mail poses fewer security problems than other forms of internet communication but is subject to interception(at he communication or gateway level), if it is unencrypted. However, an organization should be careful about what it sends and accepts. For example , unsolicited , executable code sent via e-mail could be a virus . (viruses remain generally harmless in message form until and useless executed)

File transfer:

❖ Using FTP and HTTP, users can request and send (download and upload) a variety of bulk data including databases, files in all formants, documents, software, images, and voices. While useful and convenient, file transfer can be insecure both in terms of confidentiality and threats. The network administrator must control how outsiders gain access to internal files and protect the files from misuse or unauthorized use. Normally, this requires a dedicated and isolated server(e.g. a bastion).

IP spoofing:

❖ IP spoofing is a technique that can lead to root access on a system. It is the tool that includes often use to take over open terminal and login connections after they get root access. Intruders create packets with spoofed or impersonated source IP addresses. Other types of ip attacks include user-in-the middle attacks and source-routing attacks.

Password guessing:

❖ Most host administrators have improved their password controls, but group accounts still abound, and password-dictionary and password-cracking programs can easily crack at least 10 percent of the passwords users choose. The deterrent is enforcement of good passwords.

Password sniffing:

❖ CERT estimates that, in 1994, thousands of systems were the victims of password sniffers. On LANs, any internal machine on the network can see the traffic for every machine on that network. Sniffer programs exploit this characteristic, monitoring all IP traffic and capturing the first 128 bytes or so of every encrypted FTP or telnet session. The deterrent is to utilize programs that provide on-time passwords.

Telnet:

❖ Telnet enables users to log on to remote computers. Telnet does little to detect and protect against unauthorized access. Fortunately, telnet is generally supported either by using an application gateway or by configuring a router to permit outgoing connection using something such as the established screening rules.

Viruses:

Viruses do not necessarily give intruders access to a computer system, but may be away to copy and forward information or otherwise create denial-of-service problems. A virus is a program that can infect other programs by modifying them to include a copy of it. It is possible infected with the virus. Virus attack humans, computer viruses can grow, replicated, travel, adapt and learn, attack and defend, camouflage them, and consume recourses. The following lists various computer virus infractions.

- Alter data in files
- Change disk assignments
- Create bad sectors
- Decrease free space on disk
- Destroy FAT(file allocation table)
- Erase specific programs
- Format specific tracks or entire disk
- Hang the system
- Overwrite disk directory
- Suppress execution of RAM resident programs
- Write a volume label on the disk

SATAN:

- In 1995, Dan Farmer, a software programmer for silicon graphics released a program named SATAN (security administrator tool for analyzing networks). The designer unleashed SATAN as a warning to companies and administrators that can thoroughly scan systems and entire networks of system for a number of common critical security holes. SATAN can be used by administrators to check their own networks; unfortunately, it is also used by hackers trying to break into a host. SATAN is a program freely available via the internet. its primary components include,
  - HTTP server that acts as the dedicate SATAN web server.
  - Magic cookie generator that generates a unique 32-bit magic cookie that include a session key.
  - Policy engine that decides exactly which probes to run on various hosts when performing data acquisition.
  - Target acquisition that decides exactly which probes to run on various hosts when performing data acquisition.
  - Data acquisition to gather security-related facts about the targeted hosts.
  - Inference engine that is driven by a set of rules bases and input from data acquisition.
  - Report and analysis , based on its findings.
  - More general information about SATAN and obtaining SATAN is available for anonymous FTP at fttp://ftp.win.tue.nl/pub/security/and ftp://mcs.anl.gov/pub/security/. It should be noted that security-auditing tools are now becoming available to analyze patterns of analyze patterns of attack. These are called network sniffers.

3. Explain in detail about security strategies.

- There are basic security strategies that can be utilized to combat the threats discussed so far: access control, integrity, confidentiality, and authentication.

a. Policy issues
b. Mechanisms for internet security.

POLICY ISSUES:

- Although the need for a policy is obvious, many organization attempt to make their network secure without first defining what security means. Before an organization can enforce security, the organization must access risks and develop an unambiguous policy regarding information access and protection.
- The policy needs to specify which parties are granted access to each element of the information to others, and a statement of how the organization will react to violations. The policy should also address details such as information entrusted to the organization by

clients in the normal course of conducting business and information that can be deduced about clients from their orders for goods and services.

- Establishing an information policy and educating employees is critical because humans are usually the most susceptible point in any security scheme. A worker who is careless or unaware of an elaborate mechanisms that may be in place.

- After an information policy has been established, achieving the desired level of security Can be daunting because doing so means enforcing the policy throughout the organization. Difficulties arise when dealing with external organization, when polices may conflict. For example, consider organizations A, B and C. Suppose the policy at A allow information to be exported to B, not to C. If the policy at B permits export to c, information can flow from A to C thought B. More importantly, although the end effect might compromise security, no employee at any organization would violate the organization's policy.

POLICY GUIDELINES:

- When a system administrator sets security policies, he or she is developing a plan for how to deal with computer security. One way to approach this task is to do the following.
  - Look at what it is you are trying to protect
  - Look at what you need to protect these data/resources from
  - Determines how likely the threats are
  - Implement measures which will protect your assets in a cost-effective manner.
  - Review the process continuously and improve processes when a weakness is found.

- There are a number of issues that need to be addressed when developing a security Policy, some of these issues are as follows:
  - **Who is allowed to use the resources?** The policy should explicitly state and Explain who should have access to what parts of the system, and who is authorized to use which resources.
  - **What is the proper use of the resources?** One needs to establish guidelines for the acceptable use of the resources. Those guidelines could be different if there is more Than one category of users.
  - **Who is authorized to grant access and approve usage?** The policy should clearly state who is authorized to use the resources furthermore, it must state what type Of access those users are permitted to give. A system administrator, who has no control Over who is granted access to his/her system, has no control over that system.
  - **What are user's rights and responsibilities?** The policy should incorporate a Statement on the user's rights and responsibilities concerning the use of the organization's computer systems and services. It must state what type of access those users are responsible for understanding and respecting the security rules of the system they are using.

What should be covered in the policy? The following is a list of topics that should Be covered in this area of the policy:

- What guidelines you have regarding resource use
- What might constitute abuse
- Whether users are permitted to share accounts or let others use their accounts.
- How users should keep their password secret.
- How often users should change their passwords and any password restrictions of requirements
- Restrictions on disclosure of information that may be proprietary
- Statement on electronic mail privacy
- Policy on electronic communications, mail forging, and so on
- The organization's policy concerning controversial mail or postings to mailing lists or discussion groups.

INADEQUATE MANAGEMENT:

❖ Related to the topic of policy is the topic of rational resource management. Solid Procedures and good management of computer systems as related to software are Critically important.

Installing untested software or incorporating unproved hardware has the potential to debilitate your business. Application and software changes open up the possible for bugs to be exploited to an attacker's advantage.

MECHANISM FOR INTERNET SECURIY (4.Explain in detail about Mechanisms for internet security)

❖ Mechanisms that help make internet based communication secure can be divided into three broad categories.

- Set focuses on the problems of authorization, authentication and integrity
- Set focuses on the problem of privacy
- Set focuses on the problem of availability by controlling access.

AUTHENTICATION AND INTEGRITY MECHANISMS.

❖ Authentication mechanisms address the problem of identification of individuals and entities requesting service or access. Many servers, for example, are configured to reject a request unless the request originates from an authorized client. When a client makes contact, the server must verify that the client is authorized to undertake the specific task before granting service.

There are three categories of authentication

- User-to-host: a host identifies a user before providing services
- Host-to-host: hosts validate the identity of other hosts

- User-to-user: users validate that data is being transmitted by the true sender and not an impostor posing as the sender.

❖ In **user-to-host** authentication, a host identifies users in order to provide services for which users are authorized and to deny those services for which they are not authorized. These services may include interactive login sessions, access to a network file system, or access to particular devices. There are a variety of implemented user-to-host authentication techniques. The most popular method, although not all the strongest, is based o password.(for example account name)

The following list provide some corrective suggestions,

Password don'ts

- Do not use a portion or variation of your account name or another account name.
- Do not use a portion or variation of your real name, office or home address, or phone number.
- Do not use words or variation of words found in any dictionary, especially /usr/dict words.
- Do not use pairing of short words founds in any dictionary (such as dogcat).
- Do not use dictionary words or names spelled backward (such as leinad).
- Do not use syllables or words from a foreign language.
- Do not use repeated character strings (such as AAAABBBB or CCAATT).
- Do not use passwords containing o0nly number digits (such as 123456).

Password dos:

- Run a password generator to generate one-time-only passwords. This ensures the passwords are constantly changing and are less likely to be guessed.
- Engage password aging by requiring users to reset passwords on a regular basis, such as once a week or once a month.
- Run a password guesser to test security of your own system password. This is a good way of determining weak passwords that may allow an intruder to enter.
- Prevent unsecured password at least seven characters long, if possible.

❖ **Host-to –host** authentication is concerned with the verification of the identify of computer systems. This method is employed by hosts on the internet.

❖ **User-to-User:** Authentication establishes proof of one user's identify to another user. This can be employed as a form of digital signature with electronic mail.

PRIVACY CONTROL

❖ Confidentiality is the assurance of privacy, often achieved on the internet through the use of encryption as previously discussed in the context of the integrity. An e-mail message that is sent via the internet can be compared to a postcard sent via the U.S.mail. Confidentially can

be achieved much like data integrity with the usage of encryption. This includes digital encryption, public keys, and ciphers.

ACCESS CONTROL

- Access control relates to who or what may have access to a certain service or system. Access control, essentially, is a form of authorization. A user's or service's privilege and rights dictate what services what services or objects (file and file systems, etc) may be accessed.

USER-ORIENTED ACCESS CONTROL

- An example of user access control on a time-sharing system is the user logon, which requires both a user identifier (ID) and a password.
- User access control can be either centralized or decentralized. In a centralized approach, the network provides a logon service, determining who can use the network and to who the user can connect, Decentralized user access control treats the network as a transparent communications link, and the usual logon procedure is carried out by the destination host.

DATA-ORIENTED ACCESS CONTROL

- The database management system, however, much control access to specific records or even portions of records. For example, anyone in administration may be able to obtain a list of company personnel, but only selected individuals may be access to salary information.
- The network considerations for data-oriented access control parallel those for user-oriented access control. If only certain users are permitted to access certain items of data, encryption may be required to protect those items during transmission to authorized users.
- Typically data access control is decentralized, that is it is controlled by host-based management systems. If a network database server exists on a network, data access control becomes a network functions.

5. Explain in detail about Security Tools(Apr 2014)

- Secure Transport Stacks
- Kerberos
- Secure Transactions over the Internet
- UNIX Security
- Password Security Systems
- Electronic Mail
- Server Security
- Trusting Binaries

Secure Transport Stacks

❖ The Internet uses the TCP/IP protocol as the primary network protocol.

- Each IP packet contains the data that is to be sent to destination. The IP packets consist of a 32-bit source and destination address optional bit flags, a header checksum, and data itself. There is no guarantee at the network layer that the IP Protocol data units will be

received and even they are received ,the data may not be received in a particular order in which they are sent from the source system.

- TCP provides retransmission of lost or corrupted protocols data units.

The acknowledgement number is the sequence number of the last packet transmitted.

❖ There are various network protocol encryption schemes that offer secure information being transmitted. Two most prominent Secure Transmission protocol for web communication are,

- **Secure Sockets Layer**
- **Secure-HTTP**

❖ **SECURE SOCKETS LAYER**

- This Secure Socket Layer was advanced by Netscape Communications Corporation.
- It is used to encrypt communication within higher-level protocols, such as HTTP, NNTP and FTP.

❖ The SSL Capable to Perform

- Server Authentication (verifying the server to the client)
- Data Encryption
- Client Authentication (verifying the client to the server).

❖ SSL employs RSA Cryptographic techniques to implement data encryption.

- RSA uses variable – length public key Cryptographic algorithm which uses mathematical formula to encrypt the data.
- The larger the key, the harder it is to decrypt.

Secure-HTTP

- S-HTTP is an encryption algorithm advanced by commerce net.
- S-HTTP is a higher-level protocol that currently only works with the HTTP protocol.

KERBEROS

❖ Kerberos uses a trusted third-party authentication scheme, in which users and hosts rely on the third-party to bear the burden of trust- both the hosts and the users trust the third party and not each other. The model postulates that the third party (also called the key distribution center, KDC) verifies the identity of users and hosts, based on a shared cryptographic key.

- This key enables the third-party to decrypt an encrypted password and thus prove the identity of a user or host without revealing its password.
- Some of the design principles of Kerberos are as follows:
  - Both one-way and two-way authentications are supported.
  - Authentication should be achieved without transmitting unencrypted passwords (clear text) over a network.
  - No unencrypted passwords should be stored in the KDC(trusted host)
  - Clear text passwords entered by client users should be retained in memory for the shortest time possible, and then destroyed.
  - Authentication compromises that might occur should be limited to the length of the user's current login session.
  - Each authentication should have a finite lifetime, lasting about as long as atypical login session. During this lifetime, the authentication may be reused as often a s needed
  - Network authentication should be nearly unnoticed by users: the only time users should be aware that authentication is occurring is when entering a password at the time of login.
  - Minimal effort should be required to modify existing applications that formerly used other, less-secure authentication schemes.
- The following is a brief example of the Kerberos protocol as it applies to a user accessing a network service in a client\sever environment.
- A user wishes to use a certain network services. The client sends two items to the server: a session key and a service ticket. The ticket contains four things:

  1. The name of the user it was issued to,
  2. The address of the workstation that the person was using when he or she acquired the ticket
  3. A session key, and
  4. An expiration date in the form of a lifespan and a timestamp
- All this information has been encrypted in the network service's password.

  - User sends [session key | ticket]
  - The network service decrypts the ticket with the session key so the ticket resembles this: { session key : username: address: service name: lifespan: timestamp}
  - Authenticator{Username: address}is encrypted with session key

KERBEROS AUTHENTICATION PROCESS

- Client sends a request to the authentication server requesting credentials for a giver server. Authentication server responds with these credentials, encrypted in the client's key. The credentials consist of the following.

    1. A ticket for the server
    2. A temporary encryption key (often called a session key)

- The Kerberos system relies on the premise of mutual authentication via an encrypted to. It is not, however, without its limitations. Among them are the following.

    - Vulnerability of passwords and encryption keys when presented to or maintained by the workstation
    - The need for synchronized clocks
    - No support for authenticated messages to multiple recipients
    - Weak assurances against repudiation

Secure Transactions over the Internet

- Secure transaction mechanisms for transaction processing across the internet. Business customers digitally sign encrypted credit card information; merchants then pass this information to the banks. The banks then decrypt and process information. An authorization is then returned to the merchant.

- As an alternative to the use of credit cards over the Internet is the use of e-cash. E-cash allows users to transfer electronic money over the Internet for the purchase of goods and services with relative ease.

- Digit cash is a system that provides the service of electronic cash to the Internet community; the computer system which stores the digital cash is protected by a series of passwords, access restrictions, and encryption.

UNIX SECURITY

- UNIX provides various built-in security features, such as user passwords, file access, directory access, file encryption, and security on password files.
- A UNIX system can be used for web support or more generally for FTP or related support.
- Password security on UNIX systems provides eight-character passwords for users.
- Passwords are not displayed on the screen when they are typed in, to prevent anyone else from reading them. User passwords are generally encrypted using DES algorithm.
- Once a password has been encrypted, it cannot be decrypted back to its text format; this helps to prevent hackers from reading the password file and stealing passwords.
- Users have the responsibility for the maintenance of their passwords

PASSWORD SECURITY SYSTEMS

❖ Passwords are the most widely-used security measures in existence today. Login attempts should be limited to three or less tries. Password security is only as good as the password itself.

❖ Attackers today have sophisticated password breaking tolls, which will keep trying different combinations of numbers and characters until the password has been breached.

- **One-time passwords**
- **Smart Cards**

One-time passwords

❖ There are several ways to implement one-time passwords:

One of the most common involves the use of an internal clock, a secret key and a handheld display. The current time and the secret key are processed thought some function and are displayed on the screen. The displayed value will change about once per minute, so that the value will not be repeated. The host processor proceeds to validate the user by matching the user's output to the hosts calculated output

Smart Cards

❖ A smart card is a portable device that contains some non-volatile memory and a microprocessor. This card contains some kind of an encrypted key that is compared to a secret key contained on the user's processor. Some smart cards allow users to enter a personal identification number (PIN) code.

ELECTRONIC MAIL

❖ Electronic mail or E-mail is one of the most widely used forms of communication over the Internet today. The simple Mail Transfer Protocol (SMPT) provides inter-machines e-mail transfer services.

❖ Anonymous retailers provide a service that forwards a user's mail message onto The destination address but without disclosing the return address of the sender. This protects the sender of a message from intruders learning the sender's e-mail address.

Anonymous remailers are of two types

1. Remailers that mask the sender's return address
2. Remailers that provide anonymity for both the sender and destination addresses.
   - **Privacy Enhanced Mail**
   - **Pretty Good Privacy**
   - **Multipurpose Mail Extension**

Privacy Enhanced Mail

❖ PEM describes formats and techniques for encryption and authenticating message senders. PEM allows users to send e-mail and have automatically encrypted.PEM supports confidentiality, originator authentication, message integrity, and no repudiation of origin

There are three types of PEM message

- MIC(Message Integrity Code)-CLEAR, message integrity checked in clear text has a digital signature affixed to its unencrypted content
- MIC-ONLY. Message integrity checked is encoded to protect the message's content.
- ENCRYPTED messages are also integrity checked and contain cipher text.

Pretty Good Privacy

PGP utilize the

- International Data Encryption Algorithm (IDEA)
- RSA
- MD5 algorithm to provide message encryption .

- PGP incorporates features such as digital signature and allow user to choose the size of the encryption key
- PGP also provides compression of data prior to applying the encryption algorithm

Multipurpose Internet Mail Extension

❖ MIME is a standard that defines the format of textual messages exchanged on the internet.

Its purpose is to standardize the format of message bodies in the way that enables them to carry many types of recognizable non-ASCII data.

❖ MIME-encoded message are tagged with content types

SERVER SECURITY

❖ Many of the web browsers allow user to save the html source code used to create the web pages that are viewed.

❖ The source code, once save on a user's pc is capable of recreating html formatted text. the source code contains all the designation and file name of the respective graphic video , programs and hyperlinks that would be executed clicking on the web page item.

❖ There is a security risk if a hacker were to save the web page source code and access the associated file and also they can modify or they can perform any destructive action.

❖ To overcome this, a Netscape corporation provides a web servers encrypt the communication links between pc and the server by using RSA public key cryptographic technology which is transparent to the user.

Some of the security techniques used by the commerce server include

- Data Encryption over the Communication Link.
- Server Authentication
- Message Authentication – which verify the message received are in the fact the messages that were sent.

TRUSTING BINARIES

- Security does not end with the various firewall and browser security products available. These products may not take into account the issue of trusting executables. Effective security, especially if the Internet is to become the "marketplace of the future", must be end to end. This means that not only must the protocol layer be secure to communication over an insecure network, but the binaries at both ends must be secure as well.

- Based on a security Web page, "Basic Flaws in Internet Security and Commerce," the Web page authors attempted various IP spoofing attacks to prove that security could be compromised. The results of their testing showed that they could spoof NFS (Network File System) to patch binaries on the fly, as long as they were on some subnet between the client running NFS and the NFS server itself. Being able to patch binaries, they were able to patch the Netscape executable so that it used a fixed key that was only known to the authors.

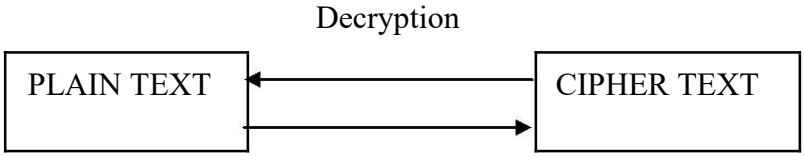
6. Explain in detail about Encryption(Apr 2014)

- Most effective way of securing the contents of electronic data i use of encryption.

- Encryption involves the scrambling of data by use of a mathematical algorithm. The term cryptography mean secret. In the simple words, cryptography is the science of disguising message so only the writer and the intended receivers are able to read them.

- Caesar was one of the first to use cryptography because of his distrust in his messengers; he used the shift-by-three method each letter of the alphabet replaced by the third letter ahead of it, for example the word “GOOD” when encrypted would become “JRRG”.

  Today's encryption is much more sophisticated.



Encryption Process

- Encryption methodologies are being used by many financial, communications, software, and credit card companies to secure the integrity of incoming and outgoing messages as well as to authenticate that messages received are actually from the persons who sent.

- Encryption is a process where the cryptographer puts an input plaintext into a codified algorithm and a key to get an output cipher text.

- Decryption on the other hand, is the reversing of encryption with the cipher text as the input and the plaintext as the output.

- The function involves both an algorithm and a key, because it would be difficult and time-consuming to keep coming up with new effective algorithms every time one wants to send a secure message.

- In most cases, the algorithm is known to all parties, since the algorithm - is useless without the key.

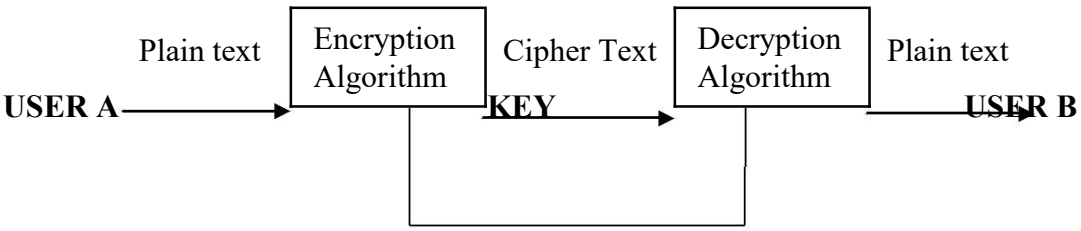
- The ease of figuring out the key depends on its length. The shorter, in number of bits, the key is easier it is to figure out. Therefore, cryptographic algorithms should have variable-length keys.
- The key is short, say 4 bits, the scheme would not be secure, for it would be easy to try all possible keys to find the corresponding plaintext.
- If the length of the block is too long, it would be inconvenient and complex. Usually the practical length is 64 bits because it is not too easy or too hard to manipulate.
- The following lists the highlights of encryption.
- Encryption is a process that conceals meaning by changing messages into unintelligible messages.

Uses a code or a cipher.

- Code system uses a predefined table or dictionary to substitute a in word or phrase for each message or part of a message.
- Cipher uses a computable algorithm that translates any stream of message bits into an unintelligible cryptogram.
- There are three kinds of cryptographic functions:
- **Hash functions (involve the use of no keys).** .
- **Secret-key functions (involves the use of one key).**
- **Public-key functions (involves the use of two keys).**

Conventional Encryption

- The encryption process consists of an algorithm and a key. The key is a relatively short bit string that controls the algorithm. The algorithm produces output depending on the key used: changing the key radically changes the output of the algorithm.
- After the cipher text is produced, it is transmitted. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.



Conventional Encryption

- It's also known as conventional cryptography or symmetric cryptography. Involves the use of a single key.

❖ Given a message (plaintext) and the key; encryption produces unintelligible data (ciphertext), which is about the same length as the plaintext.

- If two parties agree on a shared key, then by using secret -key cryptography they can send messages to one another on a medium that can be tapped, without worrying about eavesdroppers.
- Also used for securely storing data on insecure media: you can encrypt data using your own secret key and store it anywhere you want, since nobody knows the key.

❖ Decryption, which is the reverse process, uses the same key as encryption.

❖ The security of conventional encryption depends on several factors.

❖ The encryption algorithm must be powerful enough so that it is impractical to decrypt a message on the basis of the ciphertext alone. Beyond that, the security of conventional encryption depends on the secrecy of the key, not the secrecy of the algorithm.

❖ With the use of conventional encryption, the principal security problem is maintaining the secrecy of the key.

❖ Authentication is another benefit of secret-key cryptography. The term strong authentication means that someone can prove knowledge of a secret without revealing it. Strong authentication is possible utilizing cryptography. It is useful when two computers are attempting to communicate over an insecure network.

❖ For secret-key cryptography is integrity checking. A secret-key scheme can be used to generate a fixed-length cryptographic checksum associated with a message.

❖ A traditional checksum protects against accidental corruption of a message. The sum is sent along with the message. The receiver checks the sum. If the sum does not match the sum sent, the message is rejected. To provide protection against malicious changes to a message, a secret checksum algorithm is required, such that an attacker not knowing the algorithm cannot compute the right checksum for the message to be accepted as authentic.

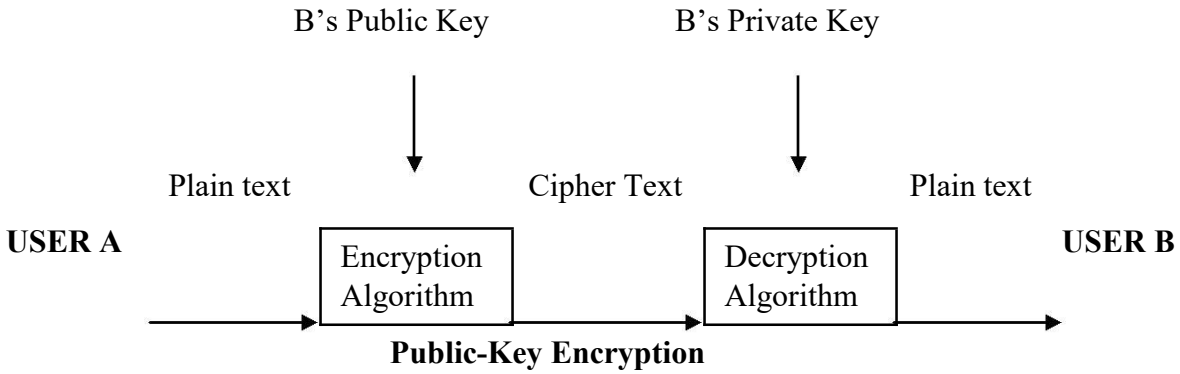
Public-Key Encryption

❖ One of the major difficulties with conventional encryption schemes is the need to distribute the keys in a secure manner.

❖ Public-key encryption, first proposed in 1976, does not require key distribution.

❖ For conventional encryption schemes, the keys used for encryption and decryption are the same. But it is possible to develop an algorithm that uses one key for encryption and a companion but different key for decryption.

❖ Furthermore, it is possible to develop an algorithm such that knowledge of the encryption algorithm plus the encryption key is not sufficient to determine the decryption key.



Public-Key Encryption

Thus the following technique will work.

- Each end system in a network (say Emil and Gabrielle) generates a pair of keys to be used for the encryption and decryption messages that it will receive.
- 2 Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.

  If Emil wants to send a message to Gabrielle, he encrypts it using Gabrielle's public key.

  When Gabrielle receives the message, she decrypts it using Gabrielle's private key. No other recipient can decrypt the message because only Gabrielle knows Gabrielle's private-key.

Public-key encryption solves the distribution problem because there are no keys to distribute. All participants have access to public keys, and private keys are generated locally by each participant

Public-key cryptography is sometimes also referred to as asymmetric cryptography. Using public-key technology, one can generate a digital signature on a message, called message integrity code or message authentication code.

A digital signature is a number associated with a message, like a checksum. However, unlike a checksum, which can be generated by anybody, a digital signature can only be generated by someone knowing the private key.

A public key differs from a secret key because verification of a MIC requires knowledge of the same secret as was used to create it.

Application of encryption:

The strength of cryptographic system rest with the key distribution technique, term that refers to the mean of delivering a key to two parties that want to exchange data without allowing other to see key. Key distribution can be achieved in number of ways.

Two keys are identified.

Session key: When two end system want to communicate, they establish a logical connection for the duration of that logical connection, all user data in encrypted with a one time session key.

Permanent Key: A permanent key is used between entities to distribute session key.

The configuration consist of following elements:

Access control center: The access control center determines which system can communicate with each other.

Key distribution center: The network interface unit performs end to end encryption and obtain session key on behalf of its host terminal.

Breaking an encryption scheme:

There are 2 basic attacks.

1. Ciphertext only, known plain text

2. Ciphertext only, chosen plain text

Known plain text is an attack using old pairs of to decipher new ciphertext messages.

Chosen plaintext attack, hackers choose any plaintext they want and have the system give them corresponding encrypted version.

Data Encryption Standard(DES):

DES has also been the subject of much controversy as to how secure it is. The main concern is in the length of the key, which some observe consider too short.

Commercial Communication security endorsement program:

The replacement is family of algorithm developed under NSA commercial COMSEC(Commercial Security Endorsement Program(CCEP). CCEP is a joint NSA and industry effort to produce a new generation of encryption devices that are more secure than DES algorithm.

Government Security Levels:

The features and capabilities of a secure operating system require significant amount of processing power and disk space.In low end servers one may find that enabiling the security features seriously affects the number of users a server can support.

The Clipper Chip:

The Clipper chip uses key escrow which is type of private key encryption that allows user for two parties to hold the secret key. the encryption algorithm is based on NSA's Skipjack algorithm.

Commercial outlook encryption:

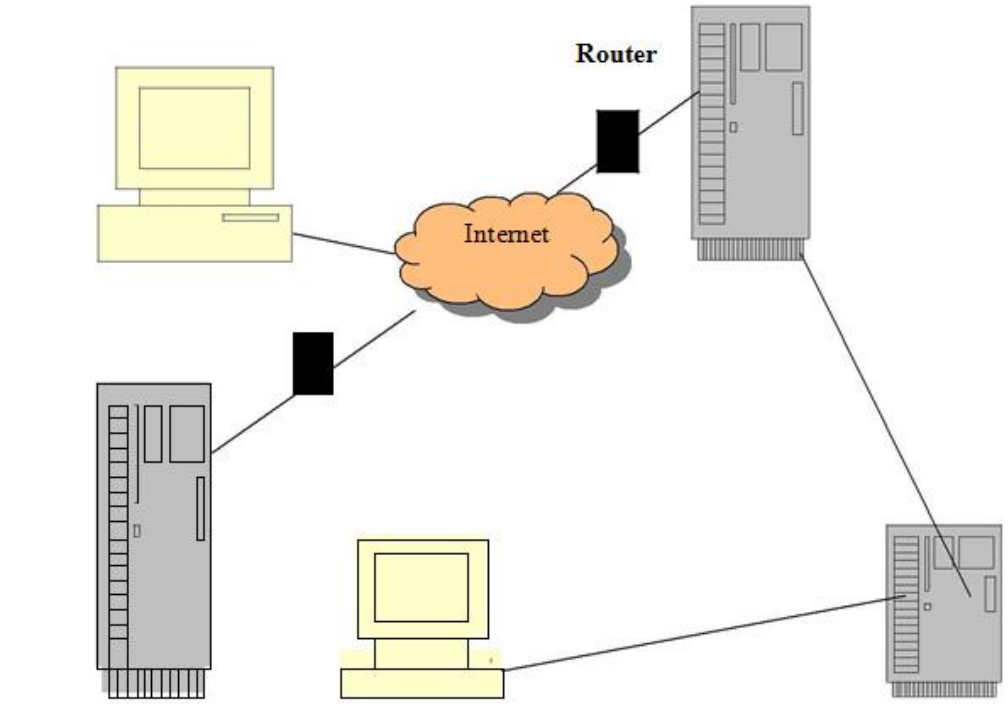
Security experts recommend layering security because no single layer of encryption is sufficient

7. Explain In Detail About Enterprise Networking And Access.

Many companies, including electronic merchants, have their employees working off of LAN-based PCs and servers. Generally, LANs am interconnected with other LANs within a company over a local or wide area network (WAN) internetworking infrastructure. With the Internet increasingly becoming a useful corporate tool (e.g., World Wide Web, e-mail, etc.), company

users are requesting access to the Internet. In addition, companies may have exposed sites to draw surfers and customers. All of this opens the enterprise-based hosts up to the outside world

Access to the Internet is accomplished in a number of ways. Access can be attained through company's LAN-resident Internet gateway by using modem



Example of VPN

- When the system is connected to the internet there may be a lot of insecurity for the data to handle that we may use firewall.

- Firewalls that control Internet access handle the problem of screening a particular network or an organization from unwanted communication. Such mechanisms can help prevent outsiders from obtaining information, changing information, or disrupting communication organization's enterprise network.

Approaches for Enterprise-Level Security

- A firewall is a security device that allows limited access out of a one's network from the Internet. So, a firewall is a piece of hardware is connected to a network to protect it from agents reaching re: on the network via public open networks .In effect, permits approved traffic in and out of one's local site. This type security measure allows an administrator to select applicable service

- Firewalls operate at the application layer of the protocol stack .They can also operate at the network and transport layers; in this case, they examine the IP and TCP headers of incoming and outgoing packets and reject and pass packets based on the programmed packet filter rules Security concerns go beyond the headquarters location. If a company has a corporate-wide backbone that connects corporate sites in several cities or countries, the network manager at a given site may choose to connect the site to a local ISP The organization must form a security perimeter by installing a firewall at each external connection. It needs an Internet firewall at the access (boundary) point of the network to be protected.

❖ Firewall are classified into three main categories

- Packet filter
- Application –level Gateway
- Proxy server

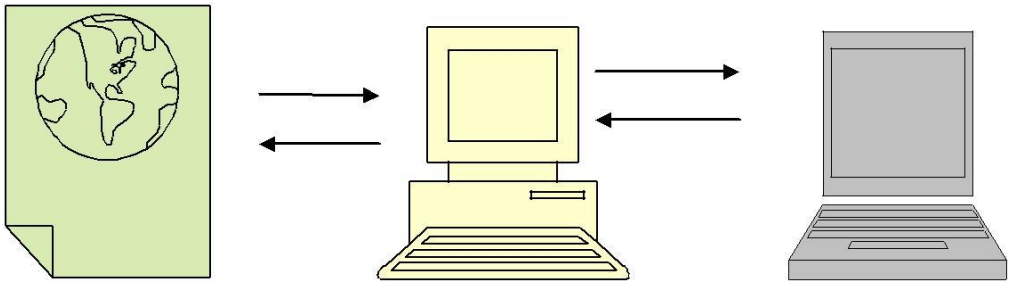
PACKET FILTER

❖ Packet filtering at the network layer can be use first defense.

❖ Filtering can occur on incoming packets, outgoing packets, or both. Limitations may exist on one's router as to where one can apply a filter. Filtering of incoming packets may protect the router from becoming compromised by an attacker.

❖ Firewalls are generally a good way of protecting an organization against attacks through the Internet.

❖ Some security issues may come in the form address spoofing. IP address spoofing is defined as sending pa from an outside host that allege to be sent from an internal Attacks using IP address spoofing are difficult to detect unless logging is performed and activities are correlated against legitimate. Hence, though filtering helps in the fight against security threats does not by itself prevent attacks from address spoofing. A threat could still be realized by an attacker portraying a trusted host that may be on an internal network.



The Global Internet The Fire wall The corporate Network

Use of Firewall

APPLICATION –LEVEL GATEWAY

An application-level gateway provides mechanism for filtering traffic for various applications. The administrator defines and implements code specific to applications or service. Services or users that can compromise the network security then be restricted . To counter some weaknesses associated with filtering routers, firewalls utilize software applications to forward filter connections for services such as Telnet, FTP, and HTTP

❖ A key distinction between a packet-filtering router application-level gateway is the ability to filter and log at the application level rather than just the IP level.

❖ In this way, administrators do not have to worry about security holes in foreign hosts which may only invoke simple measures. Another advantage to an application -level gatewa3 they

control all traffic going in and out of the network and allow logging. Utilizing a gateway provides a central point for monitor logging activity, which means administrators have the ability to all data being passed through the gateway, which could be used to look for suspected illegal activity."

- Application gateways have a number of advantages over filtering routers, including logging, hiding of internal host names and IP addresses, robust authentication, and simpler filtering rules. FTP gateway might be configurable to permit incoming FTP outgoing FTP, a particularly useful combination in main secure firewall.

PROXY SERVER

- A proxy server terminates a user's connection and sets up a new connection to the ultimate destination on behalf of the user, proxying for the user. A user connects with a port on the proxy; the connection is routed through the gateway to a destination port, which is routed to the destination address. Logging can be set up to track such transmission information as number of bytes sent, inbound IP address, and the outbound destination IP address. Usually, if a proxy is used, the proxy server provides most of the Internet connectivity. An example of a proxy is a Web services proxy server (HTTP).

- As for the disadvantages, most proxy servers require two steps to connect inbound or outbound traffic and may require modified clients to work correctly.

Variation and combinations:

a. **Dual homed host:** In TCP/IP networks, the term multihomed host describes a host that ha multiple network interface connections.
b. **Dual homed gateways:** The dual homed gateway is an alternative to packet filtering routers. It consist of an application gateway with two network interfaces and with the host's forwarding capability disabled.
c. **Screened host firewall:** The screened host firewall is more flexible than the dual homed gateway; however the flexibility is achieved with the some cost to security.
d. **Screened Subnet Firewall:** It is a variation of dual homed gateway and screened host firewall. It can be used to locate each component of the firewall on separate system, thereby achieving greater throughput and flexibility, although cost to simplicity.
e. **Bastion host:** It is any host subject to criterical security requirement. Because of this, the bastion host must be well fortified. This means that the bastion host is closely monitored by network administrators.

Design Consideration:

a. Deployment approach
b. The consequences of restricted access for clients
c. Bastion deployment approach
d. Monitoring and logging

8. Explain In Detail About Antivirus Programs.

Viruses and Worms

- A new thread has arisen in the past few years to cause concern among data processing and data communications manger – the virus and its relative worms
- These entities range from harmless to the destructive.
- A virus is a program that can affect other programs by modifying them; the modified program includes a copy of the virus program, which can then go on to infect other programs.

❖ A worm is a program that makes use of networking software to replicate itself and move from system to system. The worm performs some activity on each system it gains access to, such as consuming processor resources or depositing viruses.

Nature of Viruses

❖ A computer virus carries in its instructional code the capability for making copies of itself.

❖ Lodged in a host computer, the typical virus takes temporary control of computer disk operating system. Then, whenever a computer comes in contact with an uninfected piece of software, a fresh copy of the virus passes into a new program. Thus the infection can be spread through one computer to another computer.

❖ A virus can do anything that other program do; the only difference is that it attaches itself to another program and executes secretly every time the host program run. If after a virus program is executed it can perform any function, such as erasing files and programs.

How the infected program might works

- Find the first program instruction
- Replace it with a jump to the memory location following the last instruction in the program
- Insert a copy of the virus code at that location
- Have the virus stimulate instruction replaced by the jump
- Jump back to the second instructions of the host program
- Finish executing the host program

❖ Every time the host program is run the virus would infect another program and then execute the host program.

Countering the Threat of Viruses

❖ The best solution for the threat of viruses is prevention; do not allow a virus to get into the system

❖ The next approach is to do following steps

- **Detection:** After infection has occurred, determine that it has occurred and locate the virus.
- **Purging:** Remove the virus from all infected systems so that the disease cannot spread further.
- **Recovery:** Recover any lost data or program.

There is no universal remedy for protecting the system from the viruses even many number of program are provided for protection.

9.Explain the Security Teams. (Nov 2012)
SECURITY TEAMS

- The issues of network and internet security have become increasingly more important as more business and people go on-line.
- Teams of people have been formed to assist in solving hackers attacks and to disseminate information on security attacks and how to prevent them.
- Two such teams are

  - **Computer Emergency Response Team(CERT)**
  - **Forum of Incident Response and security Teams(FIRST)**

Computer Emergency Response Team (CERT)

- Computer Emergency Response Team (CERT) exists as a point of contact for suspected security problem related to the internet.
- CERT can help determine the scope of the threat and recommend an appropriate response.
- A World Wide Web page supplied by the software Engineering Institute post CERT advisories.

Forum of Incident Response and security Teams (FIRST)

- Security threats are a problem that affects computer and networks around the world.
- FIRST is made up of a variety of computer emergency response teams including teams from the government, business and academic sectors.
- FIRST plans to cultivate cooperation and coordination between teams in an attempt to decrease reaction time to security incidents and promote information sharing among team members.

FIRST is made up of following teams

- AUSCERT
- CERT Coordination center
- DFN-CERT
- CERT-NL
- CIAC
- NASIRC
- NAVCIRT
- PCERT
- SUNSeT
- SWITCH-CERT
- ANS
- VA

PONDICHERRY UNIVERSITY

2 MARKS

1. Name any three intrusion detection approaches. **(Apr 2013) (Ref.Qn.No.16)**
2. State the need for security features in e- commerce. **(Apr 2013)**
3. What are the two types of Anonymous remailers? **(Nov 2012)(Ref.Qn.No.24)**
4. What is a virus? **(Nov 2012) (Ref.Qn.No.6)**
5. Define: Network security. **(Apr 2012)(Ref.Qn.No.25)**
6. What are called as passive threats? **(Apr 2012)(Ref.Qn.No.26)**
7. Write a note on IP Spoofing**?(Apr 2014)(Ref.Qn.No.2)**
8. What is meant by Telnet**(Apr 2014)(Ref.Qn.No.5)**
9. List out some antivirus software.**(Nov 2014)(Ref.Qn.No.12)**
10. Difference between visa card and master card.**(Nov 2014)(Ref.Qn.No.26)**
11. Define key and list out the keys.**(Apr 2015)(Ref.Qn.No.27)**
12. What is the use of antivirus software?**(Apr 2015)(Ref.Qn.No.28)**

11 MARKS

1. Discuss the need and concept of antivirus software in detail. **(Apr 2013)(Ref.Qn.No.8)**
2. Explain about security tools for e-commerce. **(Apr 2013) (Apr 2012)(Apr 2014) (Ref.Qn.No.5)**
3. Explain the Specific Intruder approaches. **(Nov 2012) (Apr 2012) (Ref.Qn.No.2)**
4. a. Discuss the various security Teams. **(Nov 2012) (Ref.Qn.No.8)**
5. b. Explain the three main categories of firewalls. **(Ref.Qn.No.7)**
6. Discuss about Encryption?(**Apr 2014) (Ref.Qn.No.6)**
7. Describe the different security issue. (**Nov 2014) (Ref.Qn.No.1)**
8. Discuss about the security protection and recovery. (**Nov 2014)**(**Apr 2015) (Ref.Qn.No.1)**
9. Describe the antivirus program.(**Apr 2015) (Ref.Qn.No.8)**