Chapter 3

APPLICATION SECURITY

INSIDE THIS CHAPTER

- Database Security
- E-mail Security
- Internet Security
- Backups
- Archival Storage of Data
- Disposal of Data
- Firewall
- Virtual Private Networks (VPNs)
- Intrusion Detection System
- Access Control
- Layered Approach to Security

3.1. DATABASE SECURITY

A database are individual records or groups of records to satisfy various criteria. Databases support the operations and management functions of an enterprise. Data warehouses contain the archival data, collected over time to develop and market new products or serve the existing customers better.

A database stores in a meaningful way that enables multiple users and applications to access, view, and modify data as needed. A software used referred to as a database management system (DBMS) and is usually controlled by a database administrator. Databases not only store data, but may also process data and represent it in a more usable and logical form. DBMSs interface with programs, users, and data within the database.

A database provides structure for the data collected. A database should have the following characteristics:

(a) It centralized by not having data held on several different servers.

(b) Easier backup procedures.

(c) Transaction persistence.

(d) Consistency since all the data are held and maintained in one central location.

(e) Recovery and fault tolerance.

(f) Sharing of data with multiple users.

(g) Security controls that implement integrity checking, access control, and the necessary level of confidentiality.

It is essential to first implement security within the organization, to make sure the right people have access to the right data. Without these security measures in place, you someone must destroy the valuable data, or selling the company's secrets to the competitors, or someone invading the privacy of others. Authentication is to verify a username and a password, a smart card, retina scan, fingerprints and voice recognition. Authorization is the mechanism to determine the what level of access a particular authenticated user should have.

3.1.1. Authentication

After a specified login name and password, SQL Server performs the authentication itself by checking to see if a SQL Server login account has been set up and if the specified password matches the one previously recorded. If SQL Server does not have a login account set, authentication fails and the user receives an error message. Windows authentication secure, therefore, it secure is the recommended security mode, as it is more.

3.1.2. Authorization

Role-based security is a form of user-level security where a server doesn't focus on the individual user's identity but rather on a logical role he is in. A role is nothing but a group to which individual logins and users can be added, so that the permissions can be applied to a group, instead of applying the permissions to all the individual logins and users.

There are three types of roles in SQL Server namely Fixed server roles, Fixed database roles and Application roles .

(a) **Fixed Server Roles:** Logins can be added to these roles to gain the associated administrative permissions of the role. Fixed server roles cannot be altered and new server roles cannot be created.

(b) **Fixed Database Roles:** The fixed database roles are unique within the database. While the permissions of fixed database roles cannot be altered, new database roles can be created.

(c) **Securable:** Securable are objects to which access can be controlled. These are the resources to which the DBMS authorization system regulates access.

These are individual rights, permissions namely granted or denied to a head, to access a securable object. The following T-SQL commands are used to manage permissions at the user and role level. It Grants the specific

permission to the specified user. Removes a previously granted or denied permission from a user. Denies a specific permission to the specified user.

SQL injection is a technique whereby an intruder enters data that causes the application to execute SQL statements not intended to be exectured. SQL injection is possible as soon there is dynamic SQL which is handled carelessly, be that SQL statements sent from the client or dynamic SQL generated in T-SQL stored procedures. SQL injection may be possible if input is not filtered for escape characters and is then passed into a SQL statement.

3.2. E-MAIL SECURITY

Email security is a collective measure used to secure the access and content of an email account or service. It helps to protect the overall access to one or more email addresses/accounts. An email service provider implements email security to secure subscriber email accounts and data from hackers.

Email security encompasses multiple techniques used to secure an email service. From an individual/end user standpoint, proactive email security measures include, Strong passwords, password rotations, spam filters, desktop-based anti-virus/anti-spam applications.

A service provider also ensures email security by using strong password and access control mechanisms on an email server; encrypting and digitally signing email messages when in the inbox or in transit to or from a subscriber email address. It also implements firewall and software-based spam filtering applications to restrict unsolicited, untrustworthy and malicious email messages from delivery to a user's inbox.

It is very easy to spoof e-mail messages, and alter the name in the From field. All an attacker requires to modify information within the Preferences section of his mail client and restart the application. This is the act of sending spoofed messages that pretend to originate from a source the user trusts and has a business relation with, such as a bank.

A user has an e-mail client that is used to create, modify, address, send, receive, and forward messages. This e-mail client may provide other functionality, such as a personal address book and the ability to add attachments, set flags, recall messages, and store messages within different folders.

There are security implications associated with the management of email storage, policy enforcement, auditing, archieving and data recovery. Managing large, active stores of information takes time and effort in order to avoid failures. Email management can be broken drawn into a number of components on mail flow, storage and user access for both at the sewer

and use level. These must be viewed as part of a total security agenda. The security of mail flow is focused around the auditing and emailing of mails into and out of the organisation. Content monitoring and ensuring that any email that has been sent and received complies with business policy is fundamental.

There are a variety of methods including hardware and software protection systems such as spam filters and virus scanners as the gateway into the mail system. Actual email data storage includes physical storage, logical storage, archiving system as well as backup and recovery solutions. The threat is most likely to come from lost or stolen hardware, such as laptops containing offline email files. In order to reduce the risk, users should be frequently educated about email retention policies and an archiving solution should enable administrators to remove items from users mail boxes based on administrator. There must be a plan from the inevitable request to retouch data from backups and archives.

3.3. INTERNET SECURITY

The Internet is a network of networks, connecting billions of computers located on every continent. Networking helps users to gain away to information resources, such as large databases, and to other individuals.

Internet security encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol. A network security system in shown in figure 3.1. Trusted network is created by ensuring any outside network data is filtered before reaching the trusted network. Figure 3.2 illustrates another network security system. The untrusted network data is passed through external router, firewall, and internal router. The network security perimeter is composed of outher security perimeter and internal security perimeter network. Internet security relies on specific resources and standards for protecting data that gets sent through the Internet. This includes various kinds of encryption such as Pretty Good Privacy (PGP). Other aspects of a secure Web setup includes firewalls, which block unwanted traffic, and anti-malware, anti-spyware and anti-virus programs that work from specific networks.

Telecommunications connect and transmit information. Connections are done by using wired or wireless media. Wired technologies includes coaxial cable and fibre optics. Wireless technologies, based on the transmission of microwaves and radiowaves may support mobile computing. Sensors such as radio frequency identification devices (RFIDs) can be attached to products moving through the supply chain to enable the tracking of their location and the monitoring of their condition. Wireless sensor

networks that are integrated into the internet can be used for monitoring the environment and higher productivity. Various computer network configurations are possible depending on the needs of an organization. Local area networks (LAN) join computers at a particular site, such as office building see figure 3.4. Metropolitan Area Network (MANs), cover a limited densely populated area. Wide Area Networks (WANs) connect widely distributed data centres.

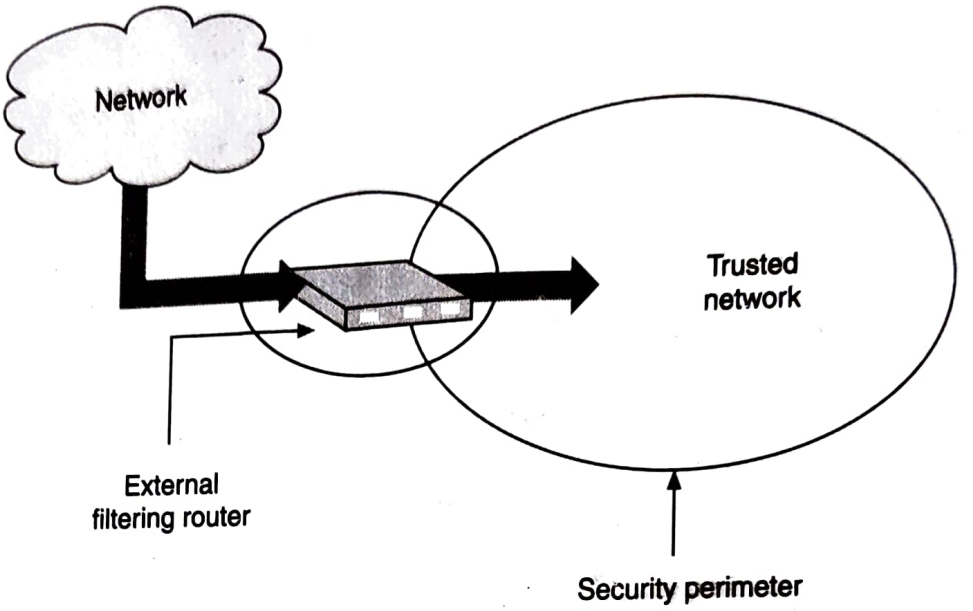

Fig. 3.1. Network Security

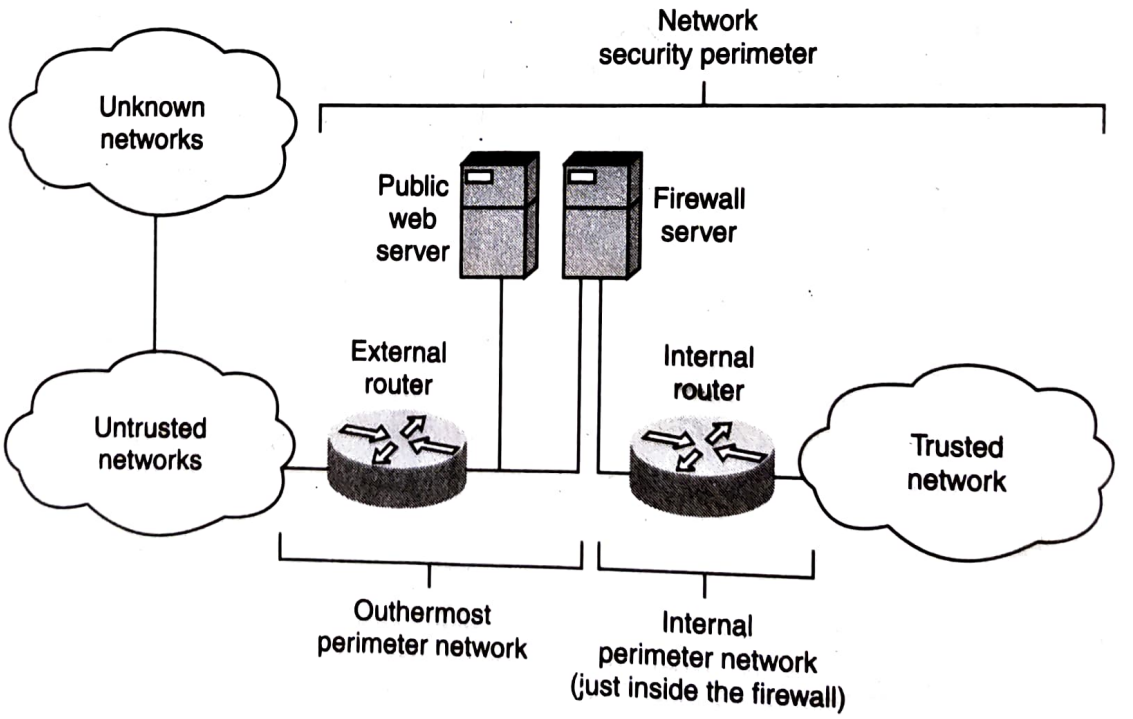

Fig. 3.2. Network security system

The Internet Protocol Security (IPSec) protocol suite provides a techniques of setting up a secure channel for protected data exchange

between two devices such as two servers, two routers, a workstation and a server, or two gateways between different networks. IPSec uses strong encryption and authentication methods, and although it can be used to enable tunneled communication between two computers, it is usually employed to establish virtual private networks (VPNs) among networks across the Internet.

IPSec can work in one of two modes namely and tunnel made. In transport mode, the payload of the message is protected, and tunnel mode, the payload and the routing and header information are protected. ESP in transport mode encrypts the actual message information so it cannot be sniffed and uncovered by an unauthorized entity. Tunnel mode provides a higher level of protection by also protecting the header and trailer data an attacker may find useful.

IPSec can authenticate the sending devices of the packet by using MAC (covered in the earlier section, "The One-Way Hash"). The ESP protocol can provide authentication, integrity, and confidentiality if the devices are configured for this type of functionality. IPSec is very complex with all of its components and possible configurations.

3.4. BACKUPS

Backing up software and having backup hardware devices are two large parts of network availability. The more frequent the backups, the more resources will be dedicated to it, so there needs to be a balance between backup costs and the actual risk of potentially losing data. The integrity of these backups needs to be checked to ensure they are happening as expected.

HSM (Hierarchical Storage Management) provides continuous online backup functionality. The HSM system dynamically manages the storage and recovery of files, which are copied to storage media devices that vary in speed and cost include optical disks, magnetic disks, and tapes. HSM is based on the trade-off between the cost of storage and the availability of information, by migrating the actual content of less used files to lower-speed and lower-cost storage.

3.5. ARCHIVAL STORAGE OF DATA

This identifies the different steps involved in the data curation process, from data creation and retention for reuse or archiving. The decision to retain data include:

(*a*) "compliance to minimum retention periods;

(*b*) "effective use of storage resources for data which has long-term value;

Data archiving is process of moving data that is no longer actively used to a separate storage device for long term retention.

(c) "reduced volume of data making it easier to manage and maintain descriptive metadata records;

(d) "reduced storage costs; and

(e) "efficient and effective file organisation for quick reuse.

The data must be retained in order to satisfy:

(a) "needs in the present day

(b) "future needs; and

(c) "compliance with policies.

The appropriate data preservation format should be selected for each dataset. Digitisation of print data may also need to be considered for long term preservation purposes. Longer minimum retention periods may be necessary for certain types of data, for example:

(a) "data which has long-term impacts on the particular field.

(b) "data which has high common interest; and

(c) "data which is instrumental in the establishment of intellectual property rights such as patents, trademarks or copyright.

3.6. DISPOSAL OF DATA

Secure destruction of research data involves using irreversible methods to ensure that the data is no longer usable. It is particularly critical that confidential or sensitive data remains unreadable. Files deleted from a computer c: drive are often placed in a "recycle bin", and some e-mail programs store deleted items in a "deleted items" folder.

However, this sort of deletion does not eradicate the data. If a file or e-mail is deleted, it remains on the disk in a hidden form, and, for information held on servers or shared drives, will be kept on a back up tape for a specified period. Likewise, reformatting a disk may leave hidden data on the disk. It is possible to retrieve information deleted in this way. When dealing with sensitive information, further measures are necessary to erase the data fully.

If the saved information on a PC or floppy disk, CD or other storage medium, measures are needed to ensure that the information is fully deleted before disposing of the item. For portable media such as a disk or CD, the best way of destroying the information they contain is to destroy the items concerned. Floppy disks should be bent out of shape, broken, or cut into pieces. CDs should be broken, or you should score lines over them.

To "destroy" information held on a hard drive, everything needs to be destroyed that is on the drive, including software. For this reason, it is advisable to carry out this sort of destruction only when the computer is to

be disposed of. If the computer has been used to process highly sensitive information, one may also need to use the decommissioning tool before passing on the computer.

Audio and video tapes should be recorded over with silence, unless highly sensitive, in which case they should be physically destroyed.

Failure to comply with the Freedom of Information (Scotland) Act and the Data Protection Act can have serious consequences. A university in England disposed of a computer that had been used to store research data about paedophiles and their victims. A subsequent owner retrieved the data from the computer. As a result of this, the victims of the crimes and their families suffered significant distress, the university received substantial adverse publicity, the university was sued for a substantial sum, and there was a risk that researchers' access to sensitive material would be curtailed in future. .

Although this is an extreme case, it demonstrates the need to exercise extreme care in the destruction of highly sensitive material. Table given below is an example of template for recording disposal of records. A strategy for reliably erasing data files is an essenatil part of managing data securely and is relevant at various stages in the data cycle.

Disposal activities depending on the sensitivity level of the data held on a system. It depends on the data and the company's policy about destroying sensitive information. The software is integrated into every part of the company's processing in structure, properly extracting it without affecting productivity and security is very important.

Data files which are not to be preserved need to be disposed of securely. However, deleting files or reformatting a hard drive will not prevent the possible recovery of data from the drive.

(a) Erasing Hard Drives

Hard drives are magnetic storage devices, therefore, just deleting does not erase a file. Instead it, removes a reference to the file. Files need to be overwritten to ensure they are effectively scrambled and remain inaccessible. Special software is needed for the secure erasing of files from hard discs.

(b) Erasing Memory Disks

Flash-based solid state discs, such as memory sticks, are constructed differently to hard drives and the techniques for securely erasing files mentioned above cannot be relied upon. Physical destruction is advised as the only certain way to erase files.

(c) Secure Disposal

The most reliable way to dispose of data is physical destruction. Shredders certified to an appropriate security level should be used for destroying paper and CD/DVD discs. Computer or external hard drives can be removed from their casings and disposed of securely through physical destruction.

3.7. FIREWALL

Management must decide which data is valuable and needs to be protected, who is responsible for protecting the data, to what extent employees may access and use the data. Good security is planned, designed, implemented, and maintained, and is capable of evolving. Security must be in line with the company's business goals and objectives Security must be understood, supported, and funded from the top down. Management does not need to know the security mechanisms used. Through hacking thousands of customers' credit cards are stolen, confidential information is leaked, or the organization's reputation is damaged, therefore, the management is accountable.

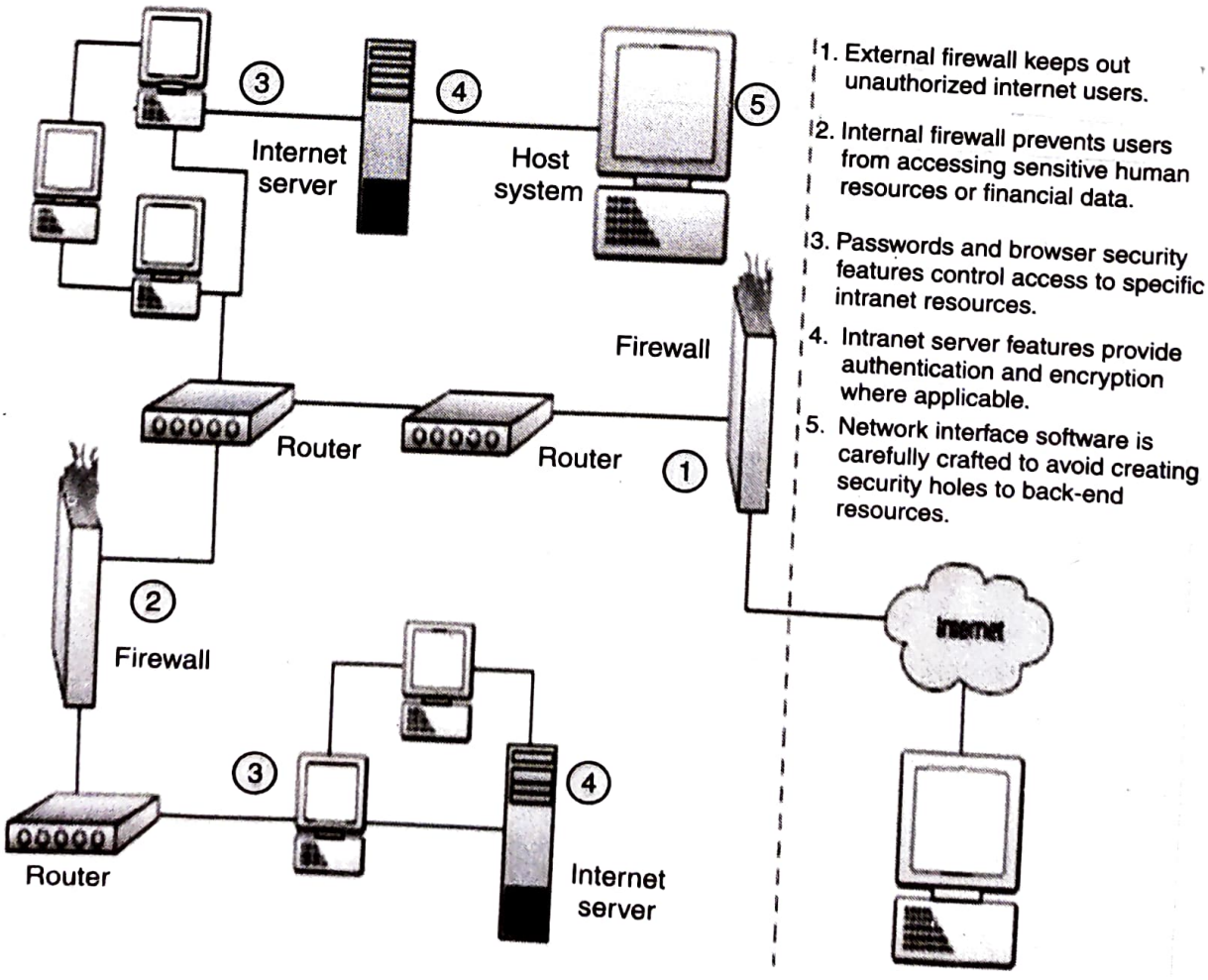

Fig. 3.3. Firewall Security

A firewall serves as a gatekeeper system that protects a company's intranets and other computer networks from intrusion by providing a filter and safe transfer point for access to and from the Internet and other networks, see figure 3.3. Firewall can be a communications processor, a router, or a dedicated server, along with firewall software. It screens all network traffic for proper passwords or other security codes and only allows authorized transmissions in and out of the network. Firewall software has also become an essential computer system component for individuals connecting to the Internet with DSL or cable modems because of their vulnerable, "always-on" connection status. Figure 3.4 illustrates an Internet/intranet firewall system for a company. In some cases, a firewall may allow access only from trusted locations on the Internet to particular computers inside the firewall, or it may allow only "safe" information to pass.

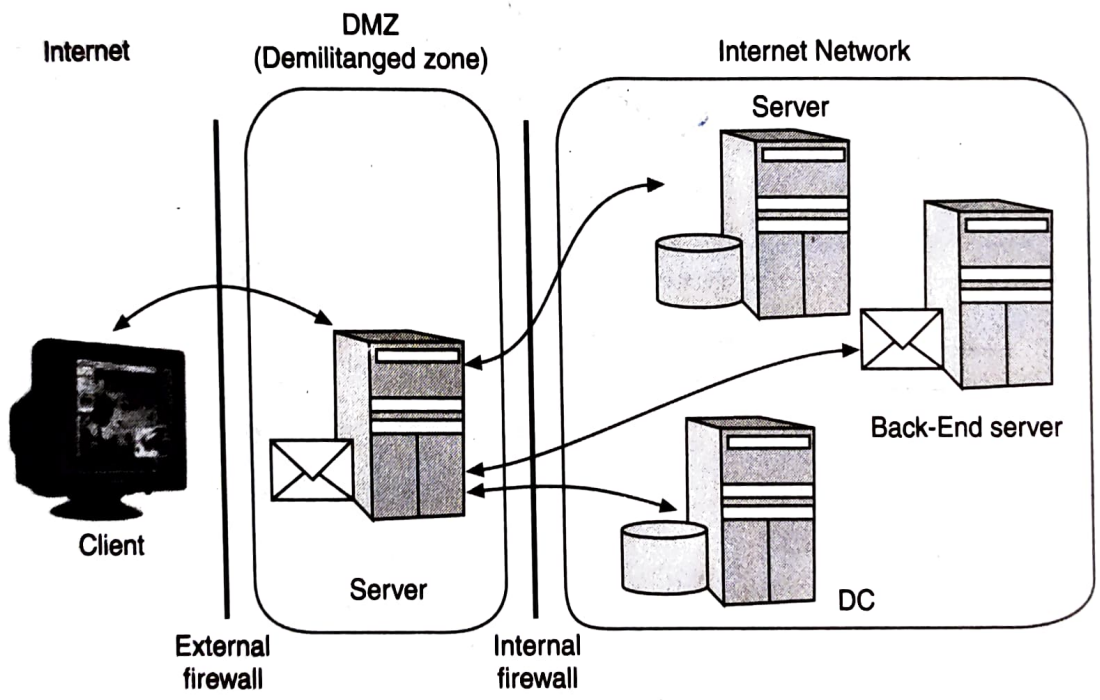

Fig. 3.4. Internet to internet network protection

3.8. VIRTUAL PRIVATE NETWORKS (VPNs)

VPN is a set of sites that communicate over the open interent, but with the security and management capabilities of dedicated circuit. It has low overhead and good communications performance. The basic functions of VPN are authentication, authorization, and establishment of secure tunnel in network.

VPN tunnel encapsulates data of one protocol inside the data field of another protocol. VPN encrypts corporate data inside IP packet data field which is managed by TCP, which is called by ATTP. The corporate data is encripted via the VPN's security protocol. VPNs operate over Ethernet,

IP, LANs, WANs DSL, cable, etc. Figurte 3.5. illustrates that internet carries packet between routers R_1 and R_2. Packet is encripted, and intruder only sees R_1 and R_2 IP address. Actual IP addresses can not be seen or nor the packet contents.

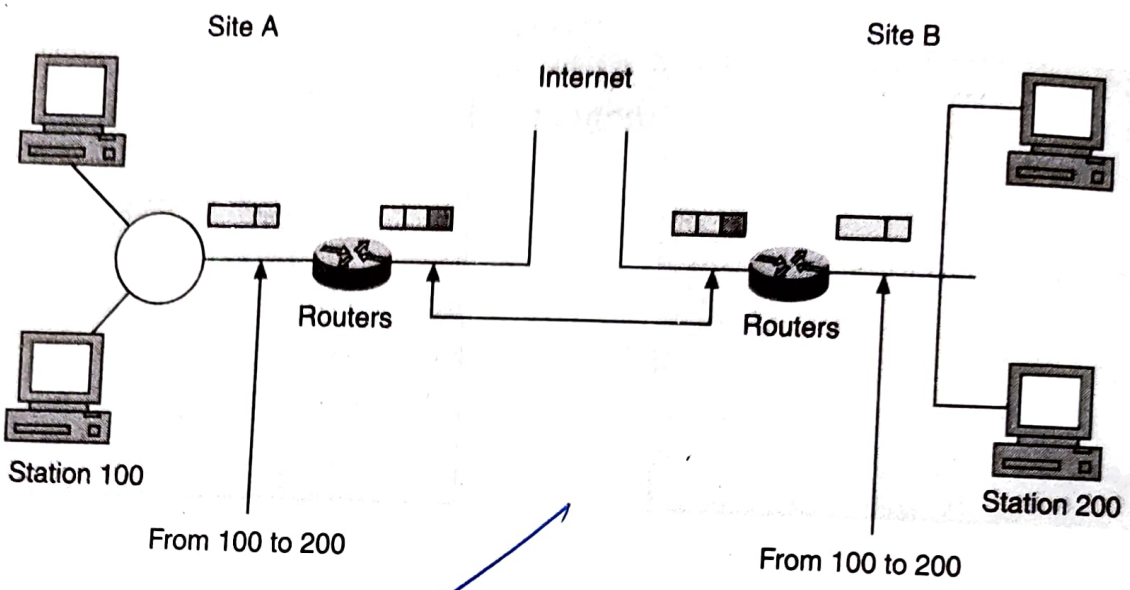

Fig. 3.5. VPN tunnel

Figure 3.6. shows a data VPN which illustrates connections through internet among head offic, branch offic and an user through VPN access devices. Application of router and firewall is also shown in this figure.

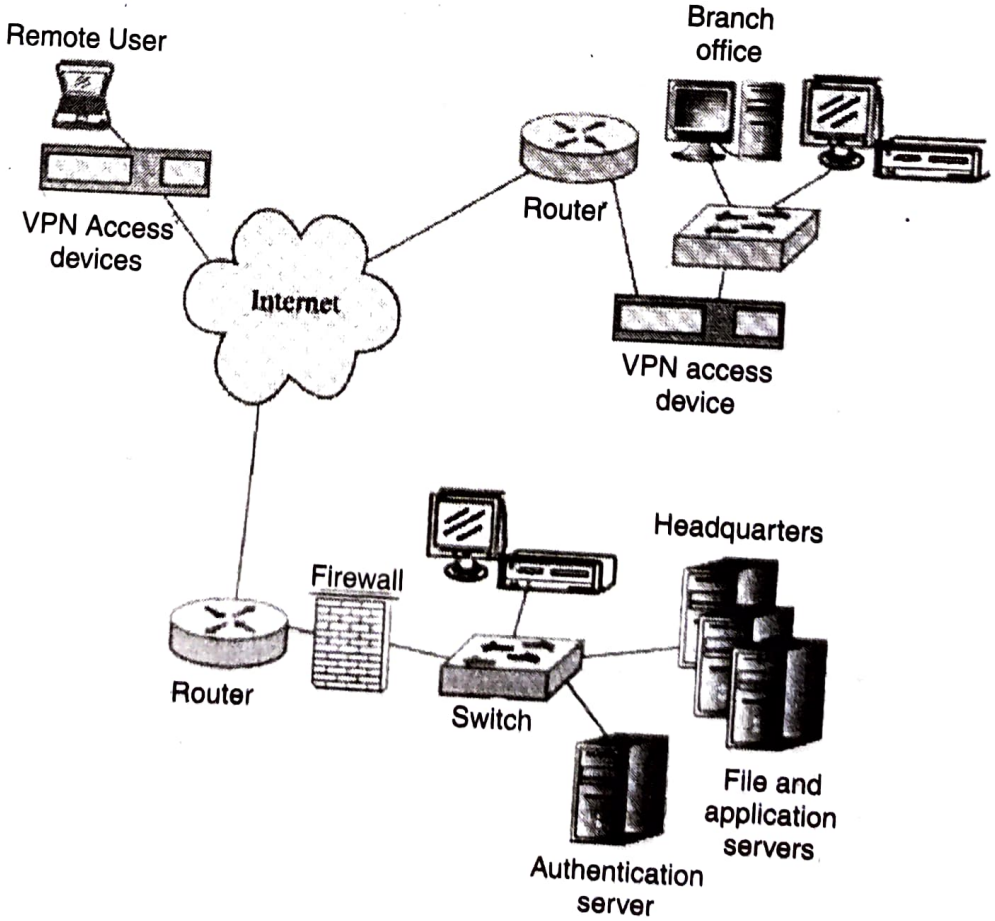

Fig. 3.6. Data virtual private network

3.9. INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) is a device or software which monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network, see figure 3.7.

IDS also monitors system activities for malicious activities or policy violations and produces reports to a management station. IDS are available based on various techniques and approach depending on the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding.

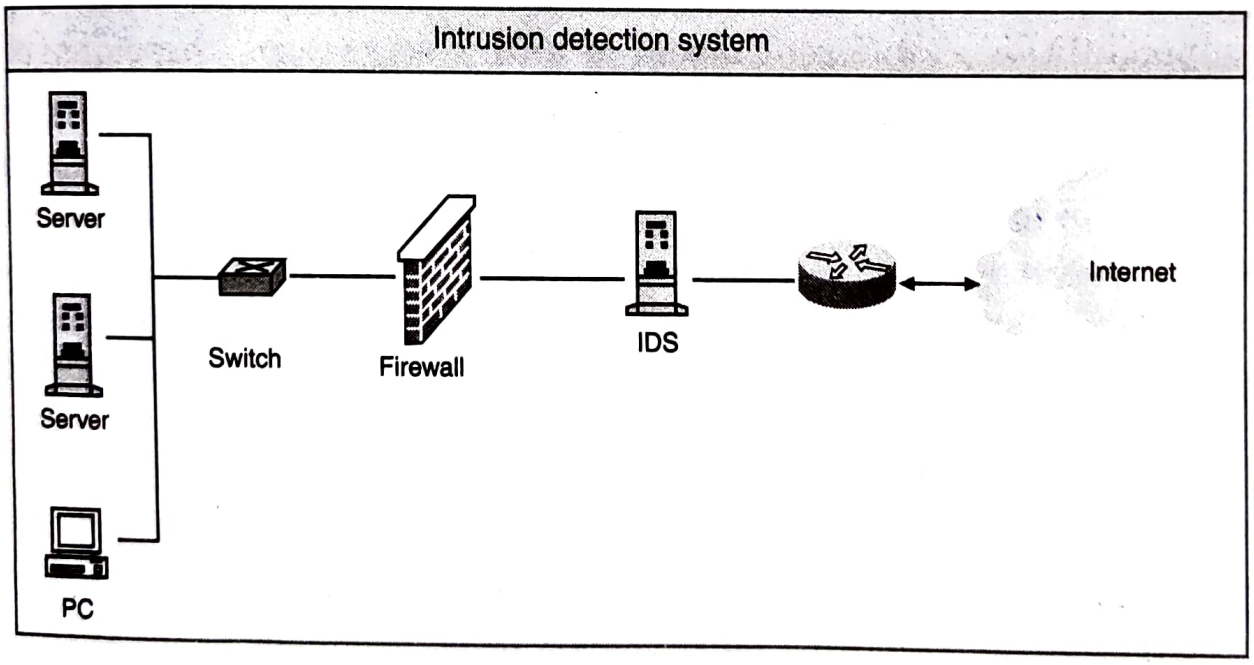

Fig. 3.7. Intrusion detection system

3.10. ACCESS CONTROL

Various types of security threats are: denial of service, unauthorized access, and theft and fraud. Denial of Service (DOS) has two primary types of DOS attacks namely. Spamming and viruses. Spamming is sending unsolicited commercial emails to individuals. E-mail bombing one computer or network, by sending thousands of email messages to it.

Hackers place software agents onto athird-party system to send requests to an intended target. DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target.

Access Control specially addresses admission of a user into a trusted area of the Organization such as Computer rooms, Power Rooms; Combination of policies , Programs, and Technologies. Types of Access controls are Mandatory Access Controls (MACs) which gives users and data owners limited control over access to information resources.

There are Non discretionary Controls which are managed by a central authority in the organization; can be based on individual's role or a specified set of assigned tasks. Discretionary Access Controls (DAC) are implemented at discretion or option of the data user Lattice-based Access Control is variation of MAC. Users are assigned matrix of authorizations for particular areas of access.

SECURITY THREATS

4

INSIDE THIS CHAPTER

- Introduction
- Hacking and Attacking
- Denial-of-Service (DOS) Attack
- E-Commerce Security
- Threats to Electronic Payment Transactions
- E-cash/Digital Cash
- Credit & Debit Cards/ATM
- Cryptography Definitions and Concepts
- Password Management
- Signature/Biometrics/Smart Card

4.1. INTRODUCTION

There are security threats from Virus, Worms, Trojan horses, Logic bombs, Backdoor, etc. Organizations must implement controls to limit damage.They must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans, to limit losses in the face of these threats.

Viruses and Worms actually evolve, changing their size, and appearance to elude detection by antivirus software programs. Trojans are Data Sending Trojans, Proxy Trojans, Security Software Disabler Torjans, and Denial of Service Attack Trojans. Blended threats combine the characteristics of virus, worm, Trojan horses and malicious code with server and Internet Vulnerabilities.

Power irregularities create problems due to fluctuations, due to power excesses. power shortages and power losses This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment. When voltage levels spike or surge the extra voltage can severely damage or destroy equipment. The more expensive uninterruptible power supply (UPS) can protect against spikes and surges.

Technical hardware failures or errors may unreliable service or lack of availability. Some errors are as that they result in unrecoverable loss of equipment. Some errors are intermittent, as they resulting in faults that are not easily repeated. Technical software failures or errors involves threats that come from purchasing software with unknown, hidden faults. Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved. These failures range from bugs to untested failure conditions.

Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks, Therefore, technological obsolescence can lead to unreliable and untrustworthy systems.

(a) Viruses

Virus are segments of code that performs malicious actions. Virus transmission is at the pening of Email attachment files. A computer virus is a self-replicating computer program written to alter the way a computer operates, without the permission or knowledge of the user. Viruses can be intentionally destructive-destroying data.

There can be Macro virus, embedded in automatically executing macro code common in word processors, spreadsheets and database applications. There is also a Boot Virus which infects the key operating files located in the computer's boot sector.

Anti-virus software alone can't protect from all threats of viruses, on the computer. New viruses and worms are released all the time and anti-virus companies have to quickly write new code to stop these new threats, but can only do so when they have been notified of the new threat. System may have already received the virus, or not updated the anti-virus software in time, thereby causing havoc to your computer.

(b) Worms

A worm is a malicious program that replicates constantly, without requiring another program to provide a safe environment for replication. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth. Once the worm has infected a computer , it can redistribute itself to all e-mail addresses found on the infected system. Furthermore, a worm can deposit copies of itself onto all Web servers that the infected systems can reach, so that users who subsequently visit those sites become infected.

(c) Trojan Horses

Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage. There are software programs that hide their true nature and reveal their designed behaviour only when activated. A Trojan horse may be widely redistributed as part of a computer virus.

Trojans are installed or executed by a user to be effective. Often, these are disguised as helpful or entertaining programs which can include operating system patches, or games. Once executed, may start Trojans opening certain ports for later intruder access, replacing certain files with other malicious files.

Trojan is a destructive program that masquerade on beginning application, unlike. Virus or Worm has a payload that installs a backdoor or trapdoor component in a system, which allows the attacker to access the system at will with special privileges.

(d) Bombs

Bombs or Logic bombs are small programs or sections of a program triggered by some event such as a certain date or time, a certain percentage of disk space filled, the removal of a file, and so on. A programmer could establish a logic bomb to delete critical sections of code deliberately. Logic bombs are most commonly installed by insiders with access to the system.

(e) Trap Doors

Trapdoors, also known as backdoors are bits of code embedded in programs by the programmer to quickly gain access at a later time, often during the testing or debugging phase. If an unscrupulous programmer purposely leaves this code in or simply forgets to remove it, a potential security hole is introduced. Hackers often plant a backdoor on previously compromised systems to gain later access. Trap doors can be almost impossible to remove in a reliable manner. Often, reformatting the system is the only way.

(f) Spoofs

Spoofing is a technique used to gain unauthorized access to computers, where in the intruder sends messages to a computer that has an IP address that indicates that the messages are coming from a trusted host. Routers use the "destination IP" address in order to forward messages through the Internet, but ignore the "source IP" address. That address is only used by the destination machine when it responds back to the source.

A common misconception is that "IP spoofing" can be used to hide the IP address while surfing the Internet, chatting on-line, sending e-mail, and so forth. This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning one cannot create a normal network connection. However, IP spoofing is an integral part of many network attacks that do not need to see responses.

(g) E-mail Viruses

An e-mail virus is computer code sent as an e-mail note attachment which, if activated, will cause some unexpected and usually harmful effect, such as destroying certain files on the hard disk and causing the attachment to be remailed to everyone in the address book, e-mail viruses are the best known and undoubtedly cause the greatest loss of time and money overall. The best two defenses against e-mail viruses for the individual user are a policy of never opening an e-mail attachment unless sender is known and what the attachment contains, and installing and using anti-virus software to scan any attachment before opening it.

(h) Macro Virus

A type of malicious code that attaches itself to documents and uses the macro programming capabilities of the document's application to execute, replicate, and spread or propagate itself.

(i) Malicious Software

Code written to perform activities that circumvent the security policy of a system. Examples are viruses, malicious applets, Trojan horses, logical bombs, and worms. Software that compromises the operation of a system by performing an unauthorized function or process.

(j) Spam

Spam is unsolicited commercial E-mail. It has been used to make malicious code attacks more effective. Spam is considered as a trivial nuisance rather than an attack. It is the waste of both computer and human resources it causes by the flow of unwanted E-mail.

Another form of E-mail attack is a mail bomb. Attacker routes large quantities of e-mail to the target. The target of the attack receives unmanageably large volumes of unsolicited e-mail. By sending large e-mails, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.

(*k*) Sniffer

A sniffer is a program or device that can monitor data travelling over a network. Unauthorized sniffers can be extremely dangerous to a network's security,because they are virtually impossible to detect and can be inserted almost anywhere. It is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker. An attacker gets more information by calling others in the company and asserting the authority.

A network sniffer is a tool that monitors traffic as it traverses a network. Administrators and network engineers often use sniffers to diagnose network problems. Sniffers are also referred to as network analyzers or protocol analyzers. When used as a diagnostic tool, a sniffer enables the administrator to see what type of traffic is being generated, in the hope of getting closer to the root of the network problem. When a sniffer is used as a tool by an attacker, the sniffer can capture user names, passwords, and confidential information as they travel over the network.

The sniffer tool is usually a piece of software that runs a computer has been compromised by an attacker, the attacker will often install a sniffer on that system to look for interesting traffic. Some sniffers only look for passwords that are being transmitted and ignore the rest. Sniffers have been very successful because a majority of LANs use Ethernet, which is a broadcast technology.

To combat sniffers within an environment, secure versions of services and protocols should be used whenever possible. Most protocols are vulnerable because they do not require strong authentication, if it is required at all.

4.3. DENIAL-OF-SERVICE (DOS) ATTACK

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Illegitimate use of resources may also result in denial of service.

Denial-of-service attacks can essentially disable the computer or the network. Depending on the nature of your enterprise, this can effectively disable your organization.

Some denial-of-service attacks can be executed with limited resources against a large, sophisticated site. Denial-of-service attacks come in a variety of forms and aim at a variety of services:

(*a*) Consumption of scarce, limited, or non-renewable resources. Can be in the form of Network Connectivity, Using Own Resources Again, Bandwidth Consumption, Consumption of Other Resources.

(*b*) Destruction or Alteration of Configuration Information.

(*c*) Physical Destruction or Alteration of Network Components.