UNIT 2 INTRANET SECURITY

Structure **Page Nos.**

2.0 INTRODUCTION

Every company starts its operations with a genuine and honest thinking. As time passes, based on the needs of its employees as well as customers, a number of processes evolve automatically, forming the core of its experience and a strong standing for the company.

Through security breaches, companies lose highly valuable information. What is the most valuable thing that any company has with it? Truly, it is the ideology of how to implement its creativity into the market and see that the experience and services reach customers properly so that both the customers as well as the company prosper simultaneously.

Imagine a situation when a company develops a major new product secretly using its Intranet. Hackers break the security and take away all the details or even cause certain damage to the software products. They can even sell the details to the competitors or blackmail the company.

Security has long been seen as a major threatening point in the implementation of the Internet or of Intranet technology in any enterprise. As networks have grown and connected to the Internet, a huge variety of hackers have haunted the professionals responsible for both delivering information within the enterprise and to its partners, and protecting it from unauthorised outsiders.

A good security technology should be powerful enough to support the features that the administrators need, including rules validation to inform the administrator of potential security back doors, automatic incident reporting to inform administrators when a security breach has occurred and secure management of the firewall itself so that the hackers cannot reconfigure the firewall and create security problems.

2.1 OBJECTIVES

Though computerisation helps a lot in proper organisation of experience, it also opens a Pandora’s box simultaneously.

On one side lie the benefits of proper organisation and quick access to the experience and on the other side there are hidden problems of dishonesty, distrust and a number of unforeseen and unwanted conditions.

Security of the contents put on an Intranet could be of great concern since information in this Information Age is as valuable as money. This unit deals with various kinds of threats to an Intranet, and security measures to protect the Intranet from them.

After going through this Unit you will be able to:

- understand the security threats and their solution;
- describe software & hardware solutions to provide security;
- explain different types of Firewalls;
- understand encryption & decryption methods;
- understand different security policies, and
- know the experiences of different experts.

2.2 SECURITY CONCERNS

The history of security concerns is not new. They have been of great worry to man and for many centuries man has been endeavouring to devise new techniques for strong security measures.

Every time technology updates itself, new techniques evolve. At the same time thieves or intruders (in the information technology line, they are called “hackers”) also get equally intelligent since they too must be using increasingly sophisticated tools. Hence, in order to prevent them from intruding, companies which manage Internet and Intranet sites of voluminous information and experience must do proper policing as well, in addition to their day-to-day activities.

Even though the security capabilities of the latest Internet and Intranet technologies have enabled the companies to control the availability of information and its authenticity in a much better manner than ever before, still many things have been left for completion. The increasing sophistication of both server and client software means that extremely strong levels of security have been provided within the system so that authorised users are not required to take complex measures to prevent unauthorised access or hacking.

In order to prevent intruders from entering the house, it is necessary for the house owner to look after the behaviour of internal and external people (who usually deal with the owner directly or indirectly). Similarly to prevent the data from hackers, the Internal or External security concerns, and their possible measures have to be carefully analysed beforehand in order to avert any eventuality.

Persons who can find access to the Intranet can be put into three categories.

1. Those who can enter the site
2. Those who can access the various secured areas
3. Those who can update the site’s contents.

Out of the above three categories, the first two could be considered safe, whereas the users who fall under the third category could cause the company’s professionals to have sleepless nights.

2.3 THREATS

It must be clearly understood that the source of threat and the likely target could be many in number but all of them can be classified as either major or minor threats.

Similarly, they can be organised into two groups viz., internal or external threats. Details of threats have been dealt with in subsequent paragraphs.

2.3.1 Internal Threats

Internal security problems are probably the most common. One never knows what someone is going to do. Even the most loyal employees or workers can change their tune and turn malicious, wreaking havoc on the computing environment.
By thoroughly scrutinising the workers' backgrounds, references, and previous employers carefully, and changing and auditing security methods, especially observation of the work pattern or behaviour of the employees (may be on a day-to-day basis), it would be possible to know about the possibilities of internal threats beforehand. Still further, this information would be useful to track down the line easily when any attack takes place.

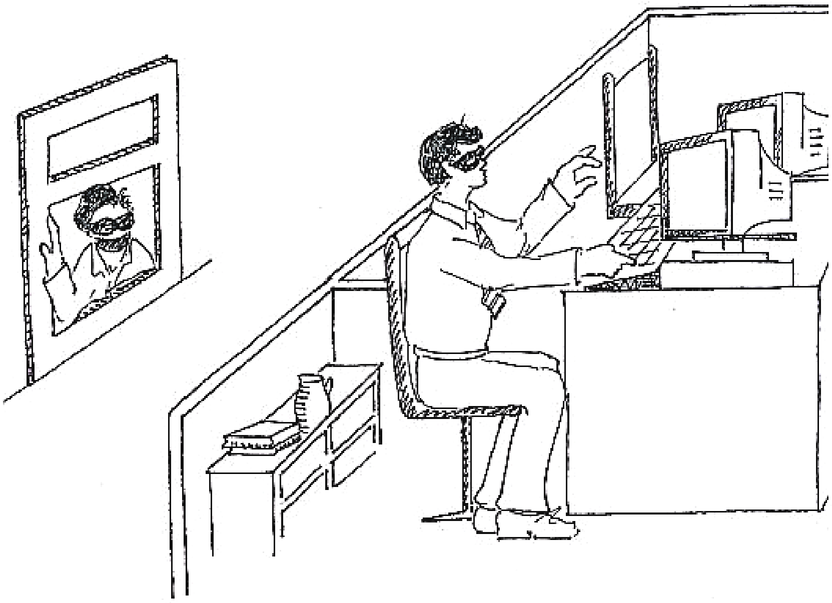


Figure 1: External and Internal threats

2.3.2 External Threats

External security threats are the most problematic ones. Till date the greatest threat was the virus menace. Now, with the sophisticated technology, a number of new threats have developed. It becomes difficult to know when an outsider will attempt to hack the systems or who the intruder may be. There are a number of examples in the past, the recent being hacking of the Indian government's servers by certain terrorists and foreign nationals.

Some people go to great extremes to gain access to the systems and information. If the Intranet is connected with the outside world via the Internet, it will discover a whole new set of potential problems and subject to a number of attacks. Internal & external threats are shown by *Figure1*, where one Internal person in Intranet is trying to break the Internal security and one external person is also trying to enter in the Intranet of the organisation.

Complete and proper security configuration and administration is indeed a complex issue. One should think carefully about the security breaches before connecting to the Internet. One of the simplest and crudest methods could be that too many system administrators connect to the Intranet first assuming that the Internet should be treated as the potentially hostile environment and consider security at a later stage. This method could be highly useful in detecting possible loopholes in the system beforehand.

2.4 SECURITY SOLUTIONS

Though there are a number of security solutions available due to sophistication in technology, there are a number of risks and difficulties attached to them. The attacks could be momentary but the aftermath could be so disgraceful that it may take many months or even years to get back to normal. History has evidence that many such attacks have led to the total shutting down of the company itself.

A matter of prime concern to companies is the overheads in the form of huge investment on extra hardware and software. It is quite possible that while implementing various security measures, the company ends up with investment more than the actual cost of the hardware and software.

Additionally, sufficient training for concerned personnel would also have to be added up to the expenditure statement. Hence, keeping all these issues in view, the company has to plan in such a manner that the investment on providing basic computing infrastructure and on its security are properly balanced.

Security Models

The first and foremost thing one needs to do is to chalk out a security plan and policy based on any security model. The term security policy shall appear a number of times while dealing with different security measures since it forms the foundation for the measures.

It is essential to distinguish between public knowledge information and the more detailed pieces of information relating to specific groups, departments, or projects. Very obviously, there is no need at all to keep documents such as Web site material, press releases, product information, etc. that can be found anywhere is public. They can be found in any newspaper or Website, Care must be concentrated on reviewing and protecting the intellectual property.

A classical case study: (*With due acknowledgements to the security exponent who proposed this theory.*) He has carefully classified the security models by giving striking analogies to the real world in the form of the five generalised examples that happen to everyone during day-to-day activities:

- **The Open House:** In this case, the front door and all the rooms are unlocked. Visitors will be free to move around anywhere from any room to any room. This resembles an unprotected site where users do not require any special authentication to view the information.
- **The Owner:** A case where the front door is locked but all the rooms are unlocked. The owner lives in the house and locks the front door in order to keep the neighbours out but once anyone gets into the house, they will be free to go into all other rooms. This is a useful security model if any company gets a lot of outsiders (i.e., customers, visitors, consultants, etc.) passing through but only want to have its employees access the site.
- **The Garden Party:** An excellent case in which the front door is unlocked but certain rooms inside the house are locked. Anyone may wish to allow people to help themselves to the bar on the front lawn and get into the washrooms but not necessarily into the bedrooms where the owner has kept all of his personal things.
- **The Paying Guest:** This is a more stringent measure than the above in which the front door is locked and certain rooms are locked. The guest has a key to enter the house and is able to get into his room only but the other rooms are off his limits. This model will verify whether or not a user should be allowed to enter the site. Once this user is authenticated, only then may he or she move freely throughout the other rooms as long as s/he has access to them.

- **The Fort:** A locked massive iron gate with barbed wire, front door locked, all rooms also locked, and there is a watchman guarding the house. Simple, unless the users have the proper credentials or certificates or entry passes, they will not be allowed to get in.

Anyone can select any of the above security models or a combination of them. While selecting, it should be borne deep in the mind that every model has its own cost factor and other considerations.

2.4.1 Hardware

The first component in the computer system vulnerable to attacks or threats, and most important to be protected, is the hardware. The following are some of the common threats to the hardware:

- Theft of a computer, printer, or other resources.
- Tampering by a disinterested or frustrated employee who takes every chance to manipulate with control switches, tampering the network or cuts the cable.
- Destruction of resources in a way that can cause terrific problems like fire, flood, or electrical power surges. Since some of them are natural attacks, they may or may not be in the control of the human alone. However, protection should be thought of well in advance.
- Ordinary wear and tear

In order to implement solutions to the above threats, it is advisable that the company should maintain proper password protected hardware. Wherever necessary, it should also consider keeping the other peripherals and networking components out of the reach of common users and employees. Further, the provision of keeping hardware backup (extra computers and servers may be of lesser capacity) as standby. It is likely that the company may find this option costlier but it is strongly recommended to consider this option seriously.

The cabling should be properly laid out in conduits and only a few “trusted” persons should be entrusted the work of overseeing the activities. It is also to be ensured that the passwords, firewalls, etc., are not handled by only one person and also that communication of confidential information such as change of passwords and documents do not fall into the hands of unauthorised persons.

2.4.2 Software

The second component vulnerable to threats to the system is software. Threats to software may include, but are not limited to the following:

- Deletion of a program, either by accident or by malicious intent.
- Theft of a program by the user.
- Corruption of a program, caused either by a hardware failure or by a virus. Usually, it has been observed that more of the attacks are due to virus attacks that cause terrible destruction in a very small time.
- Bugs in the software (intentional or unintentional).
- Virus attack.

Software developers have wide experience of tackling such issues. Students who develop software project spending days and nights struggling with software code to make things happen suddenly find that their files do not open or are missing. Reasons could be many, it could be disk drive media failure, virus attack, unintentional deletion, cross-linking of files, corrupted file allocation table, bad sectors, and many more.

Assume only one attack out of the above list i.e., the virus attack. Though the present anti-virus software solutions can detect and clean as many as 50000 viruses,

it becomes extremely difficult to detect a new virus numbered 50001. The recent happenings of I Love You, Love Bug, Dinner Party with CEO, etc., viruses have virtually spread all over the world not leaving any type of system. As reported at many places, the casualty figure has been extremely high and the organisations could not come to a stable state till date. It would be notable that even for developing an antidote it would take many man-hours of research and testing before the things are set right, and in the meanwhile the virus would have done all the damage it can.

Numerous corporate offices do their day-to-day work on-line. A simple task like sending messages, circulars, interview, meeting, promotions, etc., all are dealt with on the corporate Intranet. The NIC, Indian Oil, Bharat Petroleum, VSNL and many more do work "electronically". Assume that a new virus enters the network passing through the stringent anti-viral tests successfully (and of course, undetected). The story starts then and ends in few more moments.

2.4.3 Information

The third and major component of the system liable to be attacked is the data and data files used by the company. It is the most serious of all the threats. Threats to the hardware and software are considered negligible in comparison with the threats to information since it is this information that acts as the knowledge about the organisation. Hardware can be replaced and software can be reinstalled, but information once lost cannot be got back. Threats to information can include:

- Deletion of a file or files.
- Corruption, caused either by hardware problems or by a bug in the software.
- Theft of company data files.

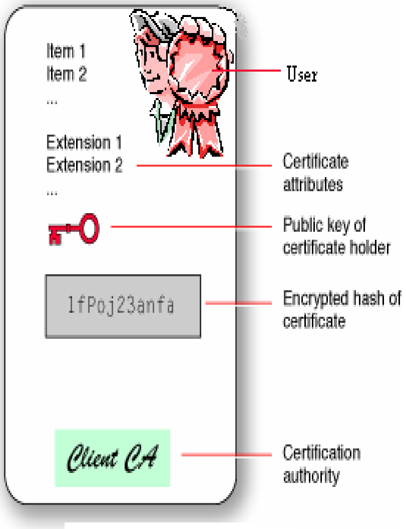
A surge in electrical pulse can cause colossal damage to the data. Dishonesty and distrust as well as frustration have already been discussed in the beginning of this unit, which can be potential threats to the company's information base.

Making and testing backups regularly could be the simplest and easiest of all the security measures. But a new question will immediately arise – "how many backups and where". Clearly, it is possible that the backup could contain a virus or there was a media failure or bad sector. Still a step further, the entire building collapses due to an earthquake or fire. Solutions lie in terms of maintaining a number of backups, some put at a remote server or site (may be a few thousand kilometers away from the location).

Such issues of security threats and management can be found separately as "Disaster Management".

2.4.4 Certification

One solution for the protection of the computing infrastructure is to use digital certificate-based solutions. Users can be given access based on their possession of certificates signed or authorised for access by or on behalf of the server to which they intend to have access. There are a number of certification solutions available in the market today. In India, the Ministry of Communications and Information Technology has set up a whole new organisation to oversee various security related concerns and certification under the title "Controller of Certification Authority."



Digital Certificate

The certificate acts as evidence of the user's digital identity. Certificates can also be combined with other access control mechanisms, such as emails, money transactions, tokens (a form of identification hardware carried by users) or only accepting visitors from certain controlled group or authenticated addresses.

At present, the certification is most easily implemented with a custom solution combined with a server, called the Certification Authority (CA). It is an external or third party service, which can issue and revoke certificates and authenticate any certificates presented in order to gain access.

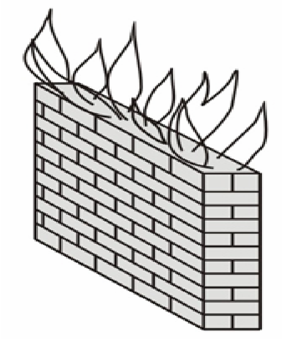
This could be implemented by use of a simple Public Key Infrastructure (PKI), a system that establishes a hierarchy of authority for the issuance and authentication of certificates and users presenting them.

Digital certificates provide excellent means of controlling and monitoring access to the Intranets. The certificate itself acts as a token for access control. The user must present it in order to access the Intranet or Internet site. The certificate could contain a series of digits and alphabets combined together. The best example can be the use of cash card or the prepaid mobile phone card. The customer pays for the required number of hours of mobile phone usage well in advance and scratches the card to obtain the “certificate”. The customer then connects to the Intranet site of the phone company by dialing it and then enters the “secret” code. Upon entering this code, the phone company updates the usage records and permits the customer to use the services for the extended period.

A similar service offered by the popular Internet Service Provider (ISP) of India called the Videsh Sanchar Nigam Limited (VSNL) offers email services for which the customers are handed over a card containing the secret code for the number of hours of usage. Those cards are available at many stores or shops. The customer has to log onto the VSNL server and create a new account with the given code number and thereafter use it as long as it permits. Such services are available for ordinary telephone services as pre-paid facility.

While in many implementations this is done automatically, in many other implementations the certificate is stored on a separate database or token such as a smart card which the user has to present to the local client in order for it to pass it to the server to gain access. Some other implementations use a number of certificates (or multi-level certificates) to ensure proper security measures.

2.4.5 Firewalls



Firewall

For Intranet developers, restricting access of unauthorised users to the Web site has been the greatest challenge. In addition to preventing external users, a watchful eye on the users within the company may also have to be maintained. There are various tools to provide protection against unwanted intruders into the corporate wide networks, but the most popular amidst all security measures is the firewall.

The simplest way to restrict the users to peek inside the internals of the Web site is to use firewalls, where the information cannot be seen or accessed from the Internet at large. Simple firewalls consist of software that prevents access to internal networks from the Internet. While general traffic such as email is allowed into the mail server, programs such as FTP clients, Telnet users or search engine queries cannot access machines beyond the safety premises of the firewall.

Firewalls also offer additional protection to local users who like to browse or surf out from the Intranet to the Internet, by acting as proxy to obtain Web pages so that the name and IP number of machines on the network are not revealed to other Web sites that the users visit. Not revealing the IP address would help prevent hackers from knowing about the details of the structure of the Intranet.

While firewall remains the basic foundation of Internet and Intranet security, for many users getting into the corporate Intranet would require increasing levels of technology. The Intranet technology would need to be expanded beyond those physically present on the same Intranet from time to time.

There are drawbacks to permitting users to access the Intranet as well as not permitting them. A simple consideration such as allowing users to use dial-up access behind the firewall by violating basic security principles could amount to inviting numerous unwanted security concerns; however, restricting them to the same access offered to the rest of the Internet users by denying permissions at the firewall level would deny them valuable and essential services.

In order to implement a successful firewall, the first and foremost activity to be done is that the company's security policy has to be clearly defined.

Though there exist a number of definitions of firewall, in simplest terms it can be defined as "a mechanism used to protect a trusted network from an entrusted network". It can also be defined as "A firewall is a system, or group of systems that enforce an access control policy between two networks, and thus should be viewed as an implementation of policy". From the above two definitions, it can be understood that a firewall is only as good as the security policy it supports.

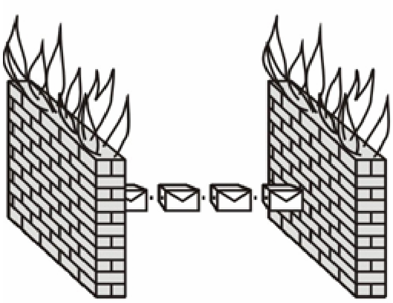
It should be very clear right from the beginning that a firewall is not simply for protecting a corporate network from unauthorised external access via the Internet, but it can also be used internally to prevent unauthorised access to a particular subnet, workgroup or LAN within a corporate network.

It would be highly interesting to note that more than 70 per cent of all security related problems start from within the organisation. Thus, for example, all the branch offices of a big company should have separate servers each protected behind a firewall, while still allowing the users of all branch offices to remain well connected and form an integral part of the global corporate-wide network.

Types of Firewall Architectures

For the sake of simplicity, the firewall technologies have been categorised into three types based on the kind of role they are expected to play. Types of firewalls are:

a) Packet filter firewalls

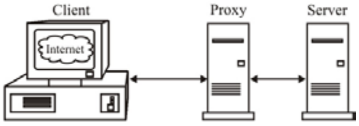


Packet filter firewall

They remain the most common type of firewall in use as of today. They were the earliest firewalls developed and were capable of permitting or denying traffic based on certain simple field-level filters which could determine such things as source or destination packet address, or the protocol being used. The greatest advantage is that they are fast since they have minimum processor overheads, and are transparent as well as inexpensive. On the down side, they are not strong enough at the application level. This is because these firewalls work purely at the level of network layer, making them difficult to configure and manage effectively.

Most of the present day routers include capabilities of such firewalls as a standard feature in their system. This kind of packet filtering can be found in almost every major firewall available today.

b) Proxy servers



Proxy Server

These types of firewalls have been further classified into two types: application level gateways and circuit level gateways.

The application level gateways establish a connection to a remote system on behalf of specific applications. This type of firewall is usually a collection of application proxies, with a one-to-one relationship between the application used and its proxy.

Whereas the circuit level gateways provide the proxy or relay capabilities in a much-generalised form, which is not limited to specific applications. The primary advantage of such firewalls over application level gateways is that they do not require a specific application proxy for each new application that needs to be communicated outside the internal network.

Although in terms of security measure the proxy servers are very secure, they require a lot of programming which can result in a delay in release of new proxies for application level gateways as well as tend to be highly CPU intensive, thereby directly having impact on the overall network performance.

c) Stateful Multi-Layer Inspection (SMLI)

They are considered as the third generation of firewall technology and usually combine the facilities of the above two. They are further classified into two types.

The Stateful multi-layer inspection (SMLI) firewall is similar to application level gateways in the sense that all levels of the OSI model are inspected carefully right from the network wire to the IP application layer.

The SMLI firewalls are different from the conventional "stand in" proxies in a way that the stand-in proxies are used for the applications when communicating to the outside world, thus putting a heavy processing load on the processors. In contrast, the SMLI firewall just examines each packet and compares them against the known states (i.e. bit patterns) to know about the behaviour pattern of the acceptable packets.

The term stateful implies that the firewall is wakeful and is capable of remembering the state of each session of packet exchange across it, allowing it to monitor all the packets for unauthorised access while maintaining high level of security, even with connectionless service protocols such as UDP, SMTP, etc.

A firewall such as the SMLI remains completely transparent to both users and applications. Consequently, SMLI firewall does not put extremely heavy processing overload on the host computer. Since it is rules based, SMLI firewall has the disadvantage that new applications may require new rules to be defined and implemented. However, the efforts are far lower than that involved in writing new proxies altogether, thus allowing SMLI firewall vendors to support a broad range of new Internet applications very quickly (may be as quickly as almost overnight).

2.4.6 Encryption/Decryption methods

One of the best method of ensuring security is to change the form of communication. Let the messages be encoded in such a pattern that it becomes almost impossible to decode for others while the actual user should be able to decode with the use of a simple certificate or key. There are three well known implementations of the encryption/decryption methods:

- Public Key Infrastructure (PKI) solutions
- Web server security through SSL (Secure Socket Layer)
- Virtual Private Networks (VPN).

Even though there are a number of other solutions available, the encryption/ decryption methods have remained most popular and economical in comparison with the other methods. Details about each of the security solution have been discussed in detail in the following paragraphs.

- **Public Key Infrastructure solutions**

The use of public-key based security systems requires great attention and due care in design and management of security features. The security of entire system is dependent on the security of the key since it is the key that will be used for signing certificates of various messages and documents. This is done at the top of the public key infrastructure also commonly called the root. The encryption and decryption is done by specialised hardware.

Usually, all the keys used for accessing the server are held at a secret location in the primary memory of the server. This area or location is highly prone to attacks (for example, in a server core memory dump). It is obvious that a higher degree of protection is required for this target location.

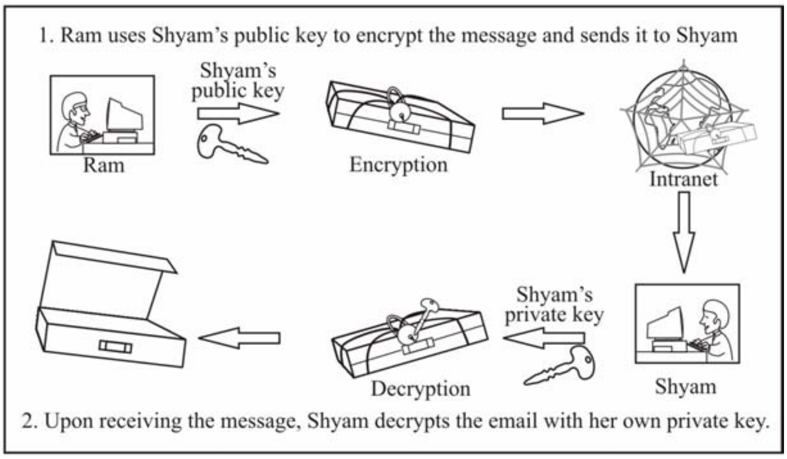

1. Ram uses Shyam's public key to encrypt the message and sends it to Shyam
Shyam's public key
Ram
Encryption
Intranet
Shyam's private key
Shyam
Decryption
2. Upon receiving the message, Shyam decrypts the email with her own private key.

Figure 2: Public Key Encryption/Decryption

We have shown one example of encryption and decryption process in the *Figure 2* where Ram wants to send a confidential message to his friend Shyam. Ram uses Shayam public key to encrypt the confidential message and send it to Shyam. After travelling through Intranet/Internet it reaches to Shayam. After reaching the Ram's message, Shyam decrypts the message with his own private key, and gets the confidential messages.

Specialised hardware such as protected memory or cryptographic memory module for storing and protecting the keys proves to be a good solution. The keys are stored in a highly encrypted format. When loaded for signing, the keys are decrypted using complex encryption/decryption algorithms and loaded into the memory of the secure server, which then performs all the signing operations required on behalf of the server. It should be noted that the keys are never displayed in their unencrypted form to the server or any other user, so even if an intruder manages to access the network, the keys remains safe.

Physical security of the cryptographic modules is also built in order to provide total security of the whole system and protect from unauthorised tampering or any kind of manipulation. The physical security is ensured by use of advanced manufacturing technology wherein strong systems are fabricated to protect the sophisticated security hardware.

Since digital certificates are highly dependent on hardware computations, it is essential that mechanisms are evolved to increase the speed of computing by various means such as parallel processing, provision of additional processors, separate hardware for protection, etc. Assume that a number of users log on to the server, then in such an event it is sure to face a bottleneck at the security gate since it would take considerable time in processing encryption/decryption of the keys or certificates. Now-a-days, in order to reduce this kind of difficulty, a separate server called firewall server is placed in front of the main server. Any one willing to access the main server has to get through this gate.

- **Web server security through SSL (Secure Socket Layer)**

  As it is well known that the Intranets and internet are purely based on use of powerful web servers to deliver information to the users, the username/ password authentication pair has been a highly popular method for preventing access to the web servers. Problem arises with the use of such pairs when these keys are sent in the form of character/text strings, which are prone to be intercepted, read and converted with simple tools.

  A significant enhancement was achieved when communications between the user and the server was sent in encrypted form and later decrypted at the other end. The enhancement went step by step and today it has stood as one of the most secured and popular method of secured communication called the Secure

Sockets Layer (SSL). Today, almost all commercial web sites are using SSL to ensure or guarantee the authenticity of the server and integrity of the data delivered to web site users.

SSL has become fundamental to the spread of Internet community, and commerce and trade over Internet. Over years, the spread of its use for an increasing range of transactions across the Internet has gone manifold.

Finally, it should be noted that by default most SSL implementations on web servers do not support or authenticate the client web browser. Therefore, SSL is at present best suited to the largely anonymous requirements of retailing and definitely requires lot of enhancements to actually pickup worldwide.

- **Virtual Private Networks (VPN)**

  In order to encrypt/decrypt all the communication network traffic that passes through the Internet or Intranet, a VPN uses software or hardware. This kind of implementation is considered the best when limited access to an Intranet is needed, for example, when two branches of the same company want to use the same information, or suppliers and customers trying to hook up their supply chains. Best example is that of Maruti Udyog Limited that uses a similar kind of solution.

  The greatest disadvantage of a VPN implementation is its non-flexibility to accept unknown locations. VPN works extremely well for two fixed known points, but less suitable to the needs of groups of users and the situation even becomes worse if the groups are from unknown locations.

Implementation using the combination of a public key infrastructure, secure web server and virtual private network technologies is considered the most powerful solution for data security. The addition of suitable physical security solutions such as cryptographic keys can further ensure that the security is perfect as well as robust.

2.4.7 Security Policy

In the United States, the government has a separate organisation looking after the security measures and providing guidelines to all departments through the Computer Security Institute (CSI), which works in close association with the Federal Bureau of Investigation (FBI). CSI does not support just the governmental servers but provides every type of guidance to private networks as well. It conducts a number of surveys on many US corporations, government departments, universities, financial institutions, and medical institutions and brings out the importance of forming and implementing a proper security policy.

The scope of security policy depends on aspects such as the size of the Intranet site, type of information hosted on it, and the number of users accessing the site. Each policy is based on a number of parameters like the companies' business rules, objectives, Intranet type, content, and existing security infrastructure. It should be noted that a security policy made for some other Intranet cannot be used for a different intranet by merely changing the name.

Although, an Intranet security policy is a very broad topic and it cannot be covered easily in few pages since it differs from situation to situation, there are some general principles that can be found similar in almost all policies. Some of them are as follows:

- Identification of
  - The content, and needs to be secured
  - User groups or categories
- Procedures
  - Access authorisation procedure
  - Backup procedures
  - Disaster recovery procedures

- Action against misuse
  - Course of action in the event of misuse or attacks
  - Ensuring employees exercise proper etiquette so that they do not misrepresent the company
  - Handling sensitive or secured documents stored on the intranet site
  - Copyright policies for intellectual properties developed by the company.

While every organisation prepares a well documented IT policy, it should also endeavour to prepare an equally comprehensive security policy too.

The security policy should cover aspects such as network service access, physical access, limits of acceptable behaviour, company's procedure for dealing with cases of security violations, responsibility for the maintenance, enforcement of the policy, etc. in addition to those described above.

Security policy for networks and firewalls, has two levels, which directly affect the design, installation and use of a firewall system:

Network Service Access Policy: A high-level, issue-specific policy which defines those services that are allowed or denied from the restricted network. It also contains clear guidelines giving instructions detailing the way in which these services will be used, and the conditions for exceptions to this policy, if any.

Firewall Design Policy: A lower-level policy that describes how the firewall will handle prevention of access and filtering of services as defined in the above network service access policy.

Classification of data is an important requirement of the company's security policy. The company should define various types of information used within the company and the relative value associated with it. The low value information would consist of general product information, specifications, turn over, etc. That may be placed on a web server, whereas high value information would consist of information specific to new product designs, tender quotes, investments, plans and other commercially sensitive information.

An organisation should consider three characteristics concerning the classification of important data:

- **Confidentiality:** Whilst some corporate data is for public consumption, the vast majority of it should remain private.
- **Integrity :** In most cases, corporate data should remain unchanged by third parties, so the system should be capable of ensuring that only authorised personnel can effect changes. Integrity also concerns the subject of non–repudiation–once an order is received, for instance, the customer should not be able to claim later that it did not come from him. Digital signatures allow us to verify the originator, as well as ensuring that data has not been tampered within transit.
- **Availability:** What data needs to be available continually, compared to data which can be "off line" for limited periods.

The security policy must be part of an overall organisational security scheme, which should be abided by everyone in the organisations. For example, even the Chairman of the company tries to turn off virus scanning because he finds it inconvenient to see the emails could be viewed seriously. This kind of policies could stand as acid test of an organisation's commitment to its security policy. In case of emergencies, suspending certain aspects of the security policy, even temporarily can be risky since a security breach could result in total data or business loss, and consequently could cost many times more to recover.

The implementation of a security policy should invariably cover all parameters of security such as physical access to the server, method of storage and disposal of confidential documents, including access to the network and Internet usage.

2.4.8 Multiple Layers of Intranet Security

Security requirements vary from organisation to organisation. They also vary on the content that the organisation's intend to place on their servers. While for certain intranets simple security solutions are enough, for many organisations solution could be in the form of implementing more than a firewall or multi-layered security architecture.

A company can implement a wide range of security models but the most useful ones are those that are organised in multiple levels. Implementation of a multi-layered or multi-tiered scheme is easier and flexible than using all or no security approach in which a user allows either total access or provides a total denial.

In addition, not just to access, security methods also protect information from accidental or intentional modification, manipulation or destruction. Most security experts opine that a security breach is more likely to come from within a company's own staff rather than from outside. These may be frustrated employees, or enthusiasts who are after the thrill of breaking the code.

Most commercial servers use a powerful operating system as base that provides good methods of file-system security. Some servers require additional software to control access to server resources and files. The immediately next higher level is the software tool that monitors the system logs, serious looking out for any suspicious activity. When any intrusion is detected, the software generates an alert message. The response could be spontaneous and automatic, with an option to generate the alert message manually. The history recorded in the server logs is used to assess damage and for planning restoration from the damage.

Use of firewalls and proper alarm systems can act as complement to above security measures, which can be added to network routers to detect or block potential threats. These devices help in filtering, detecting and then permitting the user requests and have tendency to scan the IP packets for blocking suspicious behaviour or patterns. A proxy server also helps a lot since it hides the real IP addresses of users requesting resources outside the firewall.

Finally, the software run outside the firewall tries all known security tricks of hackers, thus scanning for vulnerability points. The security implementation also should be supplemented with regular process audits by an independent security expert.

2.4.9 SOCKS

As it is well known, each type of network security protects data at a different layer of the OSI model. Built-in at each layer lies the protocol that filters, scans and checks the access. These protocols are usually easily configurable.

SOCKS is an open, industry-standard protocol advanced by the Authenticated Firewall Traversal working group of the IETF (Internet Engineering Task Force). It defines a protocol, which allows TCP applications to access firewalls in a secure and controlled manner, gaining authenticated access through that server to an external network. It can be straightaway used to construct a firewall on a TCP/IP based server.

SOCKS is a networking middleware: a circuit-level gateway, acting as a proxy and is placed at the session layer to mediate client/server connections. It can be used to connect or establish connections between two hosts and perform transactions on an Intranet or the Internet. Since it functions at the lower layer than application layer, it is clearly application-independent.

There are a number of products based on SOCKS specifications such as Auto SOCKS available in the market. The latest version is SOCKS 5, which is backward compatible with previous versions as well as supporting key features such as authentication, encryption, the UDP protocol, DNS and IP addressing.

The main problem with SOCKS is that it lacks transparency to software developers and users.

Implementation requires a change to all existing client-based software so that all of them use the SOCKS libraries. This process of changing the client code is known as "socksifying". This could be extremely cumbersome since it is also expected that at both sides similar level of programming should be available since the entire process takes place at the sessions layer (i.e., at the level of routers).

SOCKS combine powerful features of circuit-level proxies without the programming overhead of traditional application-level firewalls. A number of companies, including IBM, DEC, Cyberguard, etc. have commercial firewall products deploying the SOCKS protocol.

2.5 ADVICE FROM SECURITY EXPERTS

Intentional hacking helps in maintaining better security: Several companies employ professionals as security specialists whose basic job is to detect and cover loopholes in the security systems of the company. It would be highly astonishing to ask why would a company pay someone to hack its Intranet system. The answer would be obvious, that they intend to improve the security of its Intranet as well as to identify where from the possible risks can crop in. It should always be remembered that majority of the threats come from inside the company.

Good resources: Books such as "Intranet Security: Stories from the Trenches" by Linda McCarthy, which also happens to be her first book, could prove to be a bible to the current day security specialists.

Qualifications of security professionals: For the security professionals, it is essential that they have adequate freedom to check the security measures and enforce them and simultaneously they should also know how to use it effectively. It is also essential that they do not have a striking ego. Egoistic personalities can be very harmful to the security systems; the firewall experts, security managers, etc., should be bound by the sense of responsibility, trust, loyalty and above all cool nature in tackling complex security issues.

Firewall configuration makes all the difference: The greatest blunder that any company make is to just install a firewall and think that they have ensured perfect security. While firewalls protect from outside threats, it requires updating from time to time. Poor firewall configuration has been considered the cause of the biggest security breaches that took place in the recent past.

Lot of care required while programming: It is a common and well-known saying that many developers of "secure systems" leave a "back door" way for themselves so that they can get into the system bypassing the secure front door.

The big problem is that often the companies owning the web servers or Intranets have so many contractors and newly recruited programmers writing critical code who do not know the intricacies of the system security. The code never being reviewed causes the greatest concern.

Security risks present on the networks: Lots of risks are present everywhere on Internet as well as on Intranet, if it is not known what is being done. Every day a number of servers get connected to the global community but it is less than one percent companies who serious thinks about the security issues. A study of security of web servers reveal that out of 2,000 high-profile web servers consisting of various kinds such as commerce servers, banks, industries, government and so on, only three companies noticed the breaches.

Routine security audits are essential: It is essential that regular security audits are conducted to find out physically which computer is connected and permits access to which networks. Also, the profiles, browser permissions, certification, passwords, location of the computer in the network layout plan, firewall configuration, etc. for each computer and user on the Intranet has to be carefully studied during the audits. There are a number of other issues that cannot be dealt with directly such as integrity of the persons within the organisation. It is essential that they be requested to fill up a questionnaire or they are interviewed briefly about the security measures using indirect questions.

Example of security audit as case study: Linda narrates one of her experience about a security audit. She was performing a spot audit where she was checking certain systems. It was noticed that there could be systems that was not even part of the audit. The exact location on the network layout plan was found out and it was noticed that it had an extra connection to it but she could not make out by the network map where the connection lead to. Consequently, she decided to audit that system and found that it was connected to the Internet, to that company's Intranet as well as to a customer network. Still ahead, it was found that a hacker had broken into the system and replaced the system files and put them back in proper place. Nobody in the company even knew that the system had been broken into and only two people knew that it was even connected to the Internet.

☞ Check Your Progress 1

1) The Open House resembles to an ____________where users do not require any special authentication to view the information.

2) ______________, a system that establishes a hierarchy of authority for the issuance & authentication of certificates and users presenting them.

3) ISP stands for _________________.

4) A firewall is a system, or group of systems that enforce an ________.

5) The _____________establish a connection to a remote system on behalf of specific applications.

2.6 SUMMARY

As everyone is moving forward into the world of Internet commerce, it is important to remember that there have always been barriers to any kind of commerce. Earlier there were troubles with pirates, bank robbers and dacoits in the past, everyone with swords and guns; and now there is a new community preparing fast called the modern-day "electronic gangsters" or simply, the hackers.

It is to be always remembered while going for a security system that the security technology proposed to be implemented should be inexpensive, easy to implement, and transparent to end users.

Whatever the risks, business practices must continue to evolve. In order to move forward, it must accept some of those risks, while doing the utmost to minimize risks, as far as possible, are humanly and technologically possible.

Finally, it is advisable that instead of just one security solution, the company intending to implement one should think of a combination of security measures as people do in their lives by using security latches, closed circuit televisions, etc. in addition to the conventional locks and burglar alarms.

2.7 SOLUTIONS/ANSWERS

Check Your Progress 1

1) Unprotected website
2) Public Key Infrastructure
3) Internet Service Provide
4) Access Control Policy
5) Application Level Gateways

2.8 FURTHER READINGS

1) *The Elements of Intranet Style* by Eric Brown, Cyberpress (Publisher).

2) David Linthicum's *Guide to Client/Server and Intranet Development* by David S.Linthicum, John Wiley & Sons.

3) *Building your Intranet with Windows NT 4.0* by Stephen A.Thomas, John Wiley & Sons.

Reference Websites

1) http://intranetjournal.com
2) http://idm.internet.com
3) http://www.cio.com/forums/intranet
4) http://www.gooddocuments.com