17.5 DIGITAL SIGNATURE

In today's commercial environment, establishing a framework for the authentication of computer-based information requires familiarity from both the legal advisor and computer security fields. Combining these two disciplines is not an easy task. The historical legal concept of 'signature' is defined as any mark made with the intention of authenticating the marked document. In a digital setting, this concept of "signature" may well include markings as digitised images of paper signatures.

To understand the concept of digital signature in a better way, we must first know the legal implications of digital signature. A signature is not part of the substance of a transaction, but is a representation. Signing serves the following general purposes:

- **Evidence**: A signature authenticates writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.
- **Ceremony**: The act of signing a document calls to the signer's attention the legal significance of the signer's act, and thereby helps prevent inconsiderate engagements.
- **Approval**: In certain contexts defined by law or custom, a signature expresses the signer's approval or authorisation of the writing, or the signer's intention that it has legal effect.
- **Efficiency and Logistics**: A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document.

Although the basic nature of transactions has not changed, the cyber law has only begun to adapt new technology. The legal and business communities must develop rules and practices, which use new technology to achieve and surpass the effects historically expected from paper forms. To achieve the basic purposes of signatures outlined above, a signature must have the following attributes:

- **Signer Authentication**: A signature should indicate who signed a document, message or record, and should be difficult for another person to produce without authorisation.
- **Document Authentication**: A signature should identify what is signed, making it impracticable to falsify or alter either the signed matter or the signature without detection.

17.5.1 How Digital Signature is Used

Digital signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use public key cryptography technique, which employs an *algorithm* using two different but mathematically related *keys*; one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form. Computer equipment and software utilising two such keys are often collectively termed an 'asymmetric cryptosystem'.

The complementary keys of an asymmetric cryptosystem for digital signatures are arbitrarily termed the private key, which is known only to the signer and is used to create the digital signature, and the public key, which is ordinarily more widely known and is used by a relying party to verify the digital signature. If many people need to verify the signer's digital signatures, the public key must be available or distributed to all of them. Although the keys of the pair are mathematically related, if the asymmetric cryptosystem has been designed and implemented securely it is computationally infeasible to derive the private key from the knowledge of the public key. Thus, many people may know the public key of a given signer and use it to verify that signer's signatures; they cannot discover the signer's private key and use it to forge digital signatures.

Another fundamental process, termed as hash function, is used in both creating and verifying a digital signature. A hash function is an algorithm, which creates a digital representation in the form of a hash value of a standard length, which is usually much smaller than the message but nevertheless, substantially unique to it. Thus, use of digital signatures usually involves two processes, one performed by the signer and the other by the receiver of the digital signature. These are:

- **Digital signature creation**, which uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.
- **Digital signature verification**, the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

To have a clear understanding of how digital signature is applied, let us consider an example. Suppose Mr. A wants to send his signed message to Mr. B through Internet, he can use the public key cryptosystem to provide digital signatures. Mr. A uses his own private key to create a digital signature and Mr. B will use A's public key to verify this digital signature. On the digital signature creation side, Mr. A creates digital signature using his private key. This process makes message in encrypted form and results as signed message. The signed message is then send through the Internet to Mr. B.

On the digital signature verification side, Mr. B receives the message, together with the digital signature from the Internet. Mr. B gets a copy of Mr. A public key and verify the signature by A's public key. This process results in the decryption of the message with A's public key. If the result after decryption is the same as the transmitted message, Mr. B can believe that the message has really come from Mr. A. This is because only Mr. A holds his private key, which is needed to generate the digital signature.

Note that if the message or the digital signature is modified during the transmission, Mr. B will not find the decrypted form of digital signature to match with the message, then Mr. B can conclude that either the message transmission is tampered, or the message is not generated by Mr. A.

17.6 FIREWALL

The ongoing occurrences of incidents pertaining to network security caused a great concern to the people, using computers as their medium to exchange data across the country. A need was felt for a method of controlling the traffic, which allows access of information to computers. Organisations required an application that could protect and isolate their internal systems from the Internet. This application is called *Firewall*. Simply put, a firewall prevents certain outside connections from entering into the network. It traps inbound or outbound packets, analyses them, and then permits access or discards them.

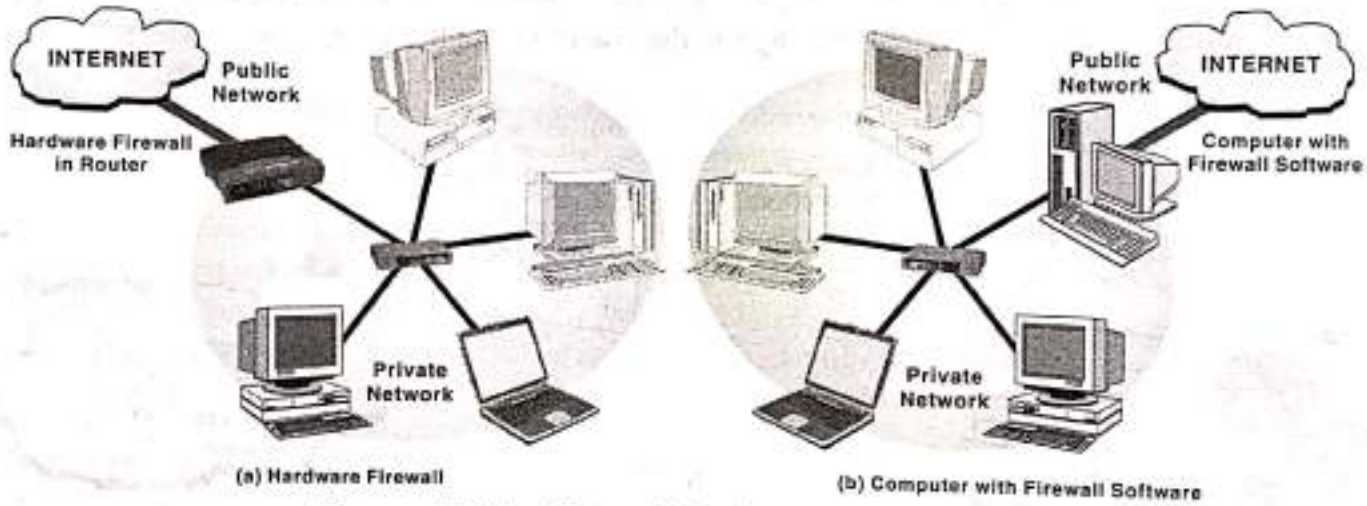

Figure 17.13 *Firewall Software and Hardware*

THINGS TO REMEMBER

Firewall

Firewall makes decisions on whether or not data should be allowed to pass based upon a security policy. For each packet of data, the firewall compares known components of the packet to a security rule set and decides if the packet should be allowed to pass. In addition, Firewall has security rules that involve altering the packet in some basic way before passing the data. With a sensible security policy and a security rule set designed to implement that policy, a firewall is used in protecting local area networks from attacks.

Generally, Firewall system comprises a software, embedded in a router, computer, host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be a threat from hosts outside the subnet. It serves as the gatekeeper between an untrusted network (Internet) and the more trusted internal networks. If a remote user tries to access the internal networks without going through the firewall, its effectiveness is diluted. For example, if a travelling manager has an office computer that he or she can dial into while travelling, and his or her computer is on the protected internal network, then an attacker who can dial into that computer has circumvented the firewall. Similarly, if a user has a dial-up Internet account, and sometimes connects to the

Internet from his or her office computer, he or she opens an unsecured connection to the Internet that circumvents the firewall.

17.6.1 How Firewall Works

To understand the working of firewall, consider an example where an organisation is having hundreds of computers on the network. In addition, the organisation will have one or more connections to the Internet lines. Now, without a firewall in place, all the computers are directly accessible to anyone on the Internet. A person who knows what other people are doing can probe those computers, try to make FTP (file transfer protocol) connections to them, or telnet connections and so on. If one employee makes a mistake and leaves a security hole, hackers can get to the machine and exploit that hole.

With a firewall in place, the network landscape becomes much different. An organisation will place a firewall at every connection to the Internet (for example, at every T1 line coming into the company). The Firewall can implement security rules. For example, one of the security rules that out of the 300 computers inside an organisation, only one is permitted to receive public FTP traffic or allowing FTP connections only to that one computer and prevent them on the others. A company can set up rules like this for FTP servers, Web servers, Telnet servers and so on. In addition, an organisation can have control on how employees connect to websites, whether files are allowed to leave the company over the network and so on. Firewall provides incredible control over how people use the network. It provides protection against the following:

- Blocking unwanted traffic.
- Direct incoming traffic to more trustworthy internal systems.
- Hide vulnerable systems, which cannot be secured from the Internet.
- Log traffic to and from the private network.
- Hide information like system names, network topology, network device types, and internal user ID's from the Internet.
- Provide more robust authentication than standard applications.

One can also customise firewalls according to the specific needs. This means that one can add or remove filters based on several conditions:

- **IP Addresses:** IP addresses are 32-bit numbers, normally expressed as four 'octets' between the periods. It is a unique address assigned on the Internet. A typical IP address looks like this: 135.27.84.129. If a certain IP address outside the company is reading too many files from a server, the firewall can block all traffic to or from that IP address.
- **Domain Names:** As numeric strings are hard to remember, which make up an IP address, all servers on the Internet also have human-readable names, called domain names. For example, it is easier for us to remember www.itlesl.com than 134.26.56.161. An organisation might block all access to certain domain names or allow access only to specific domain names.
- **Ports:** Server machine, which makes services available to the Internet, uses numbered ports. For each service that is available on the server, a corresponding port number is assigned. For example, if a server machine is running a web (HTTP) server, the web server would typically be available on Port 80. A firewall can be configured to block Port 80 on all machines.
- **Specific Words and Phrases:** Firewall can be made to configure by sniffing (search through) each packet of information for an exact match of the text listed in the filter. For example, a user can instruct the firewall to block any packet with the word "ADWARE" in it.

17.6.2 Types of Firewall

A firewall intercepts the data between the Internet and the computer. All data traffic passes through it, and it allows only authorised data to pass into the corporate network. Firewalls are typically implemented using one of the three primary architectures: *packet filtering, application-level gateway, and circuit-level gateway.*

Packet filtering Packet filtering is the most basic firewall protection technique used in an organisation. It operates at the network layer to examine incoming and outgoing packets and apply a fixed set of rules to the packets to determine whether they will be allowed to pass. The packet filter firewall is typically very fast because it does not examine any of the data in the packet. It simply examines the IP packet header, the source and destination IP addresses, and the port combinations, then it applies filtering rules. For example, it is easy to filter out all packets destined for Port 80, which might be the port for a web server. The administrator may decide that Port 80 is off limits except for specific IP subnets, and a packet filter would suffice for this. Packet filtering is fast, flexible, transparent (no changes are required at the client) and cheap. This type of filter is commonly used in small to medium businesses that require control over users to use the Internet.

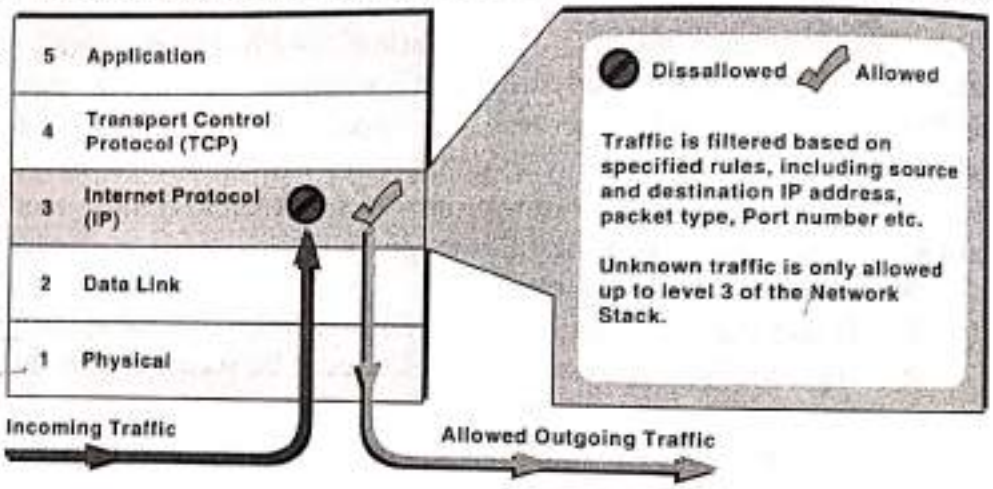

Figure 17.14 *Packet Filtering Firewall*

Application-level gateway An application-level gateway firewall uses server programs (called proxies), which run on the firewall. These proxies take requests from the external network, examine them, and forward the legitimate requests to the internal host computer. This type of firewall supports functions such as user authentication and logging. As this type of firewall is considered the most secure type, it provides a number of advantages to the medium-high risk web sites:

- The firewall can be configured as the only host address that is visible to the outside network, requiring all connections to and from the internal network to go through the firewall.
- The use of proxies for different services prevents direct access to services on the internal network, protecting the enterprise against insecure or misconfigured internal hosts.
- Strong user authentication can be enforced with application gateways.
- Proxies can provide detailed logging at the application level.

This type of firewall requires every client program to be set up as a proxy. In addition, the firewall must have a proxy in it for each type of protocol that can be used. This can cause a delay in implementing new protocols if the firewall does not support it. The penalties paid for this additional level of security are performance and flexibility. Proxy server firewalls have large processor and memory requirements in order to support many simultaneous users, and introduction of new Internet applications and protocols can often involve significant delays while new proxies are developed to support them. True proxy servers are undoubtedly the safest, but impose an overhead in heavily loaded networks.

Firewall working on application-level gateways technique requires a proxy for each service (such as FTP, and HTTP), which is compatible to it. When a service is required that is not supported by a proxy, an organisation has three possible choices to perform:

- Deny the service until the firewall vendor has developed a secure proxy.
- Develop a custom proxy.
- Pass the service through the firewall.

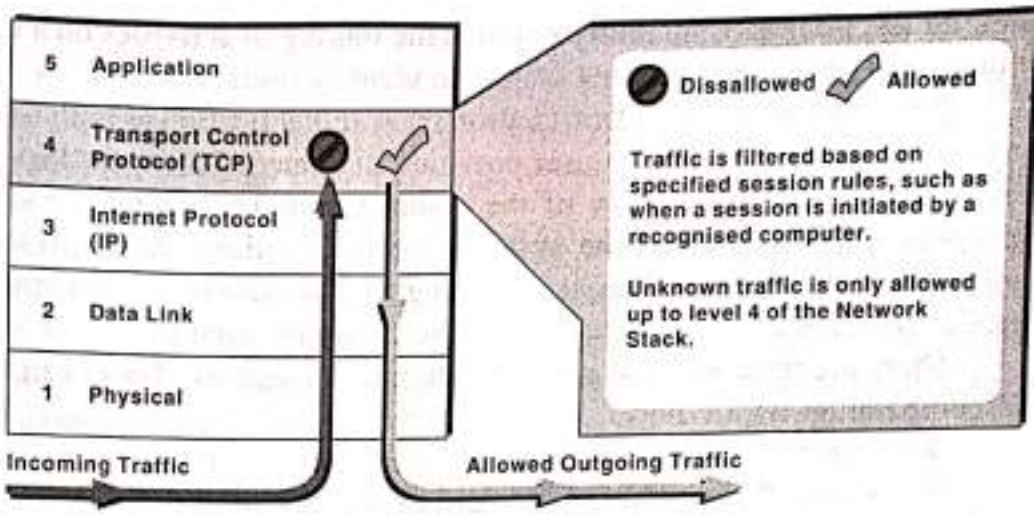

Figure 17.15 *Application-Level Gateway Firewall*

Circuit-level gateway In the circuit-level firewall, all connections are monitored and only those connections that are found to be valid are allowed to pass through the firewall. This generally means that a client behind the firewall can initiate any type of session, but clients outside the firewall cannot see or connect to a machine protected by the firewall. Stateful inspections usually occur at the network layer, thus making it fast and preventing suspicious packets from travelling up the protocol stack. Unlike static packet filtering technique, stateful inspection makes its decisions based on all the data in the packet (corresponding to all the levels of the OSI model).

Using this information, firewall builds dynamic state tables and then uses these tables to keep track of the connections, which go through it. Rather than allowing all packets that meet the rule set's requirements to pass, it allows only those packets, which are part of a valid, established connection. A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users.

17.7 USERS IDENTIFICATION AND AUTHENTICATION

Identification and authentication (I&A) is another line of defence against the unauthorised people from entering into a computer system. I&A is a critical building block of computer security as it forms the basis for most types of access control and for establishing user's accountability. Such access control often requires a system to identify and differentiate among different users. For example, access control is often based on least privilege, which refers to granting of accesses to only those users who are required to perform

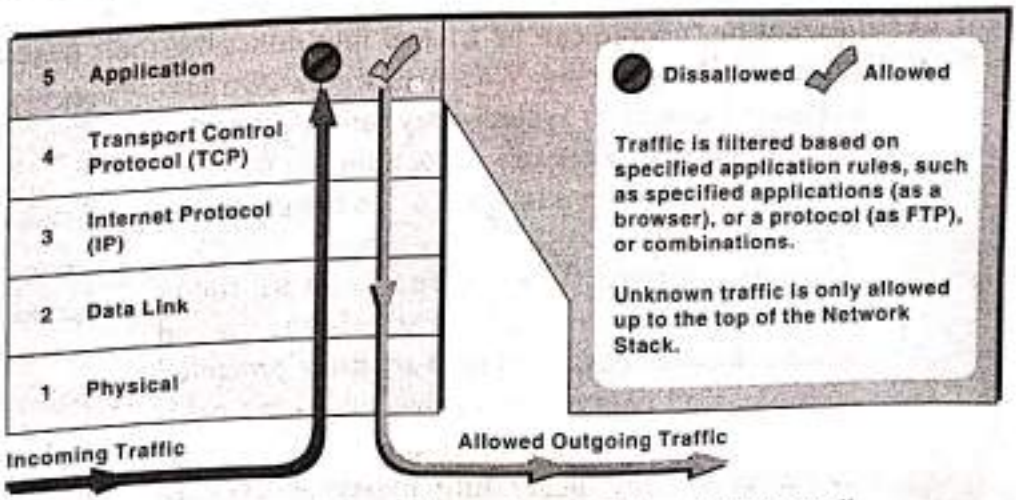

Figure 17.16 *Circuit-Level Gateway Firewall*

their duties. User accountability requires the linking of activities on a computer system to specific individuals and, therefore, requires system to identify users.

Often people confuse identification from authentication as both have similar aspects. *Identification* is the means through which a user provides a claimed identity to the system. Where as, *authentication* refers to establishing validity of the claim. Computer systems make use of data authentication for recognising people, which the systems receive. Authentication presents several challenges: such as collecting authentication data, transmitting the data securely, and identifying the same person who was earlier authenticated and is still using the computer system.

There are three ways of authenticating users identity. These can be done either by using alone or in combination with others:

- **Users Requirement** (password, PIN, cryptographic key).
- **Users Possessions** (ATM card or smart card).
- **Users Biometric** (voice pattern, handwriting dynamics, fingerprint).

These means give strong authentication, however, there are certain problems associated with these. If people want to pretend to be someone else on a computer system, they can guess or learn an individual's password; they can also steal or fabricate tokens.

17.7.1 Users Requirement

The most common form of information and authentication is the combination of a user ID and password. This technique is based solely on user requirement. In general, password systems work by requiring the users to enter a user ID and password (personal identification number). The system compares the password to a previously stored password for that user ID. If there is a match, the user is authenticated and granted access. This type of security access has been successfully providing security to computer systems for a long time. They are integrated into many operating systems, and users and system administrators are familiar with them. When properly managed in a controlled environment, they can provide effective security. However, this technique is dependent upon keeping passwords secret. Unfortunately, there are many ways that the secret key may be divulged.

- **Finding Passwords**: If users create own passwords, he may tend to make it easy to remember. On the other hand, assigned passwords may be difficult to remember, so users are more likely to write them down. Many computer systems are equipped with administrative accounts that have preset passwords. Because these passwords are standard, they are easily 'guessed'.
- **Giving Passwords**: Users may share their passwords with a co-worker in order to share files. In addition, people can be tricked into divulging their passwords.
- **Electronic Monitoring**: When passwords are transmitted to a computer system, they can be electronically monitored. This can happen on the network used to transmit the password or on the computer system itself.
- **Accessing Password File**: If the password file is not protected by strong access controls, the file can be downloaded. Password files are often protected with one-way encryption so that plain-text passwords are not available to system administrators or hackers (if they successfully bypass access controls).

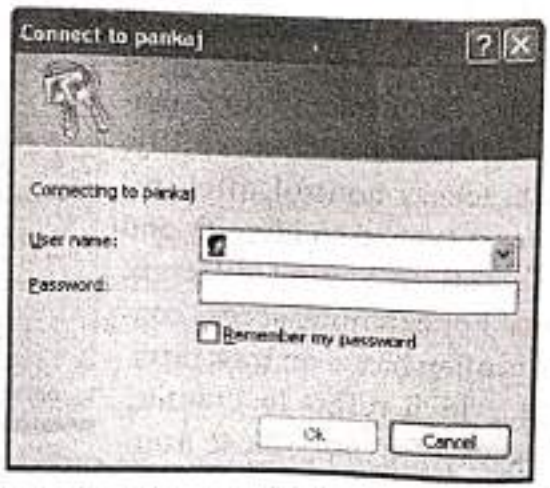

Figure 17.17 *User ID and Password*

17.7.2 Users Possessions

Although some techniques are based solely on users' requirements, most of the techniques are based on what the users possess. This combination provides significantly stronger security than individual's techniques. This technique uses *tokens* system. Such tokens are divided into two categories: *memory tokens* and *smart tokens*.

Memory tokens Memory tokens are meant for storing information. It requires special reader/writer devices for writing and reading of data to and from the tokens. The most common type of memory token is a magnetic strip card, in which a thin stripe of magnetic material is affixed to the surface of a card (for example, as on the back of credit cards). A common application of memory tokens for authentication to computer systems is the automatic teller machine (ATM) card.

Memory tokens when used with PINs provide significantly more security than passwords. In addition, memory cards are inexpensive to produce. A hacker must have both a valid token and the corresponding PIN to pretend to be someone else. This is much more difficult than obtaining a valid password and user ID combination. Tokens can be used in support of log generation without the need for the employee to key in a user ID for each transaction or other logged event since the token can be scanned repeatedly. If the token is required for physical entry and exit, then people will be forced to remove the token when they leave the computer. This can help maintain authentication. However, this method also has certain limitations, although sophisticated technical attacks are possible against memory token systems, most of the problems associated with them relate to their cost, administration, token loss, user dissatisfaction, and the compromise of PINs. Most of the techniques for increasing the security of memory token systems relate to the protection of PINs.

Figure 17.18 *Memory Token*

Smart tokens A smart token is the functionality expansion of memory token, incorporating one or more integrated circuits into the token itself. When used for authentication, a smart token is another example of authentication based on users possession category. A smart token requires a user to provide something the user knows (PIN or password) in order to "unlock" the smart token for use. Smart tokens offer great flexibility and are used to solve different authentication problems. The benefits of smart tokens vary, for the type it is used. In general, they provide greater security than memory cards. It can solve the problem of electronic monitoring even if the authentication is done across an open network by using one-time passwords.

However, like memory tokens, most of the problems associated with smart tokens relate to their cost, the administration of the system, and user dissatisfaction. Smart tokens are generally less vulnerable to the compromise of PINs because authentication usually takes place on the card. Moreover, smart tokens cost more than memory cards and are more complex, particularly challenge-response calculators.

Figure 17.19 *Smart Token*

17.7.3 Biometrics Technique

Biometric authentication technologies use the unique characteristics (or attributes) of an individual to authenticate the person's identity. These include physiological attributes (such as fingerprints, hand geometry, or retina patterns) or behavioural attributes (such as voice patterns and hand-written signatures). Biometric authentication technologies based upon these attributes have been developed for computer log in applications. Biometric authentication is technically complex and expensive, and user acceptance can be difficult.

Biometric systems provide an increased level of security for computer systems, but the technology is still new as compared to memory tokens or smart tokens. Biometric authentication devices provide imperfection, resulting from technical difficulties in measuring and profiling physical attributes as well as from the somewhat variable nature of physical attributes. These may change, depending on various conditions. For example, a person's speech pattern may change under stressful conditions or when suffering from a sore throat or cold. Due to their relatively high cost, biometric systems are typically used with other authentication means in environments requiring high security.

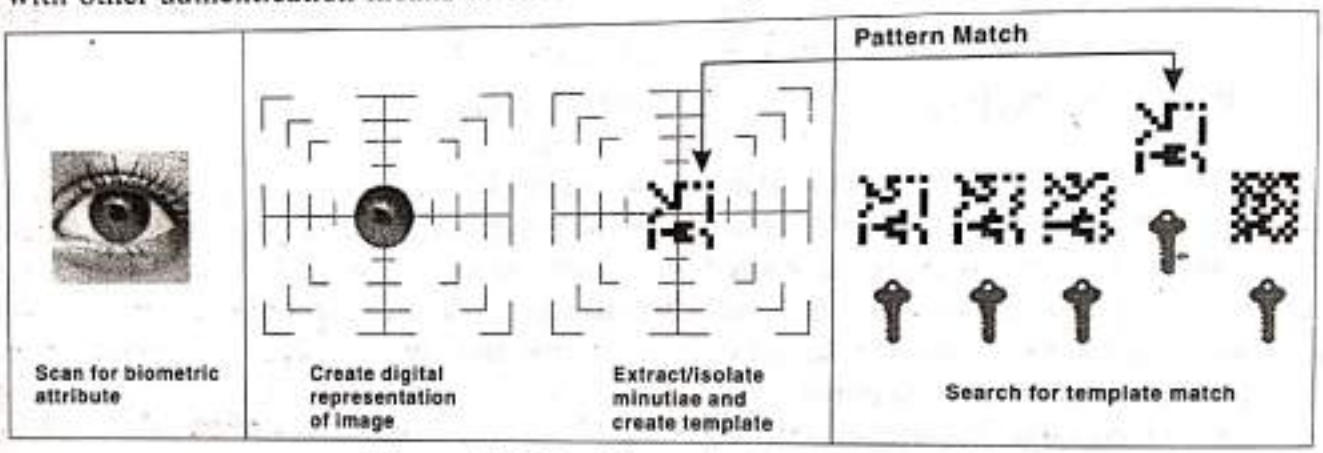

Figure 17.20 *Biometric Techniques*

17.8 SECURITY AWARENESS AND POLICIES

In today's computing environment, everyone in an organisation has access to system resources and, therefore, has the potential to cause harm. Each computer on networks is potentially a door in which access to other computers on the network is possible. Therefore, a need for security awareness and training is required to implement computer security in an organisation. Computer security awareness and training is an issue that affects all computer users, whether they use a personal computer or terminals connected to the mainframe computer.

17.8.1 Awareness

The main purpose behind security awareness is to enhance security by improving awareness of the need to protect system resources, developing skills, and knowledge so that computer users can perform their jobs more securely and build knowledge needed for design, implement, or operate security programs for organisations and systems. Awareness is used to reinforce the fact that security supports the mission of the organisation by protecting valuable resources. In addition, it is also used to remind people of basic security practices, such as logging off a computer system or locking doors.

To spread awareness of computer security, various teaching methods are deployed, such as video tapes, newsletters, posters, bulletin boards, briefings, short reminder notices at log-on, discussions, and lectures. Awareness is often incorporated into security training and is used to change employees

attitudes. However, employees often regard computer security as an obstacle to productivity. To help motivate employees, it must be emphasised how security, from a broader perspective, contributes to productivity. The consequences of poor security must be explained, while avoiding the fear and intimidation that employees often associate with security.

Providing training is also an awareness activity, which teach skills to the people that enable them to perform their jobs in a more secure manner. This includes teaching people what they should do and how they should (or can) do it. Training addresses many levels, from basic security practices to more advanced or specialised skills. It can be specific to one computer system or generic enough to address all systems. Many personnel's need advanced or specialised training rather than just basic security practices. For example, managers may need to understand security consequences and costs so that they can take the security factor into their decisions. There are different ways to identify individuals or groups who need specialised or advanced training. One method is to look at job categories, such as executives, functional managers, or technology providers.

A security-training program normally includes training classes, either strictly devoted to security or as added special sections or modules within existing training classes. Training is either computer or lecture-based, and may include hands on practice and case studies.

17.8.2 Security Policy

A security policy is a formal statement of the rules for people who are given access to an organisation's technology. When developing a security policy, care must be taken to identify and understand relevant and valid issues. Mostly, resources are wasted on reacting to a high-profile hoax call while a serious issue goes unnoticed. When evaluating the effectiveness of a particular security policy, the resources being protected must be analysed, the information stored in today's computer ranges from public domain material such as telephone numbers to highly sensitive data, for example, an individual's genome. It is not practical nor is it possible to firmly secure all this information. The goal is to protect information in line with its relative value and importance to the business process. A security policy should focus on allowing employees to access only the resources he or she needs to perform their job function. Those who need to see information and only individuals who need to modify information should be allowed.

The main purpose of security policy is to inform users, staff, and managers of their obligatory requirements for protecting technology and information assets. The policy should specify the mechanisms through which these requirements can be met.

Security Policy

THINGS TO REMEMBER

The important characteristics of security policy are as follows:

- It must be implementable through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods.
- It must be enforceable with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible.
- It must clearly define the areas of responsibility for the users, administrators, and management.