

Unit 1

Why the Study of subject "Information Security"?

Today's computing environment is far different, more distributed, and as such, much more complex to manage. Business information is dispersed, as local area networks and departmental systems have replaced the monolithic mainframe. Further, the emphasis on the computer and resident information has given way to an emphasis on ensuring continuity of the processes that keep the business running. Risk management and business continuity planning, therefore, must become critical components of business operations. In order for managers to make informed decisions about whether to assume, avoid or transfer risk, and implement cost-effective security solutions, it is essential to adopt a methodology that addresses the issues in terms of cost and benefit.

In the budding Information Age, the technology of information storage, processing, transfer, and access has exploded, leaving efforts to secure that information effectively in a never-ending catch-up mode. For the risks potentially associated with information and information technology (IT) to be identified and managed cost-effectively, it is essential that the process of analyzing and assessing risk is well understood by all parties and executed on a timely basis. This chapter is written with the objective of illuminating the process and the issues of risk analysis and assessment.

Information System

An **information system** (IS) is any combination of information technology and people's activities using that technology to support operations, management, and decision-making. In a very broad sense, the term *information system* is frequently used to refer to the interaction between people, algorithmic processes, data and technology. In this sense, the term is used to refer not only to the information and communication technology (ICT) an organization uses, but also to the way in which people interact with this technology in support of business processes. Some make a clear distinction between information systems, ICT, and business processes. Information systems are distinct from information technology in that an information system is typically seen as having an ICT component. Information systems are also different from business processes. Information systems help to control the performance of business processes.

Alter argues for an information system as a special type of work system. A work system is a system in which humans and/or machines perform work using resources (including ICT) to produce specific products and/or services for customers. An information system is a work system whose activities are devoted to processing (capturing, transmitting, storing, retrieving, manipulating and displaying) information. **Beynon-Davies** defines an information system as an example of a system concerned with the manipulation of signs. An information system is a type of socio-technical system. An information system is a mediating construct between actions and technology. Alter argues for an information system as a special type of work system. An information system is a work system whose activities are devoted to processing information. Information systems are the primary focus of study for the information systems discipline and for organizational informatics.

History of Information System

The history of **information systems** coincides with the history of computer science that began long before the modern discipline of computer science emerged in the twentieth century. Regarding the circulation of information and ideas, numerous legacy information systems still exist today that are continuously updated to promote ethnographic approaches, to ensure data integrity, and to improve the social effectiveness & efficiency of the whole process i.e. capturing, transmitting, storing, retrieving, manipulating and displaying of information. In general, information systems are focused upon processing information within organizations, especially within business enterprises, and sharing the benefits with modern society. Before the concept of management information systems was created, computer scientists were just programmers creating applications for science and math calculations. As computer usage evolved in fields of business and data management, software applications were needed to process nonscientific data. A field of study would be needed to bridge the gap between computer programmers and the business world to create information-based applications for business and networks. Then evaluation may be understood briefly by following Table.

Year	Main activities	Skills required
1970s	<p>Mainframe computers were used Computers and data were centralized Systems were tied to a few business functions: payroll, inventory, billing</p> <p>Main focus was to automate existing processes</p>	Programming in COBOL
1980s	<p>PCs and LANs are installed Departments set up own computer systems End-user computing with Word Processors and Spreadsheets makes departments less dependent on the IT department</p> <p>Main focus is automating existing processes</p>	PC support, basic networking
1990s	<p>Wide Area Networks (WANs) become corporate standards Senior management looks for system integration and data integration. No more stand-alone systems.</p> <p>Main focus is central control and corporate learning</p>	Network support, systems integration, database administration
2000s	<p>Wide Area Networks expand via the Internet to include global enterprises and business partners – supply chain and distribution Senior management looks for data sharing across systems.</p> <p>Main focus is efficiencies and speed in inventory, manufacturing, distribution</p>	Network support, systems integration

Need of Distributed Information System

In 1952, the evolving punch card system created by IBM would change the way government, business and education would perceive the way that data was to be processed. Punch cards allowed mainframes to read and extract data from computers by reading hole punches. Programmers wrote programs on a mainframe for punch card operations in which the punch card would be read into the program by a card reader to update a database. The database could be a business application, a scientific application or any application. Business applications were difficult for computer scientists because many didn't have a background in business. The programmers usually had to call in business people and write down notes of how business managers and executives wanted the computer to process information. The computer programmer usually wrote the program without understanding of business concepts at all. In the late 1950s and 1960s, computers would start to integrate into other areas of society. Accounting, retail sales, transportation and media services would benefit from the advent and use of computers. There was still a language barrier between programmers and business people who wanted certain applications developed for their business or operation. That would begin to change in 1970.

Need of Management Information Systems

With the advent of computer programs for business applications, it became apparent that the communication gap that existed between computer programmers and business people had to be solved. Business people wanted programmers to come up with the ultimate solution for their problems and programmers had a hard time explaining to management what was possible and what was not, technically, possible. The solution was to design a course of study which merged information technology, business and computer programming. This field was called, Management Information Systems (MIS). The idea was to create a workforce who could bridge the communication and technical gaps between management and computer programmers. The first courses were taught in as business courses in select colleges in America. The courses started off as electives in the area of business. As the 1970s closed, colleges and business schools would create full four-year programs designed for studies in the field of information systems.

Management Information System Networks

From 1980 to the present, there has been an explosion of technology in the field of information systems. The integration of the personal computer (PC) into the workplace and homes has made information readily available to all people. The creation of wide area networks, the Internet and distributed processing have changed the way people obtain information. The concept of Management Information Systems has expanded to include data mining (databases of archived information), data retrieval sciences (critical business data stored on microchips) and technology used in everyday devices such as cell phones, wireless devices that require the passage of important data as well as integrated software for common functions. The world is living in the Age of Information. Computers have assisted countries into transforming themselves from the industrial revolution into the information age by merging concepts through various management information system applications.

The Open Systems Interconnection Model

The OSI is a product of the Open Systems Interconnection effort at the International Organization for Standardization. It is a way of sub-dividing a communications system into smaller parts called layers. A layer is a collection of conceptually similar functions that provide services to the layer above it and receives services from the layer below it. On each layer an *instance* provides services to the instances at the layer above and requests service from the layer below.

For example, a layer that provides error-free communications, across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of the path. Conceptually two instances at one layer are connected by a horizontal protocol connection on that layer. Lately the OSI model has been taught using a Mnemonic, (such as "All People Seem To Need Data Processing" 7 to 1) to help in understanding the complex model, such are from layer 1 to 7, and going from layer 7 to 1:

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption
		5. Session	Interhost communication
	Segments	4. Transport	End-to-end connections and reliability, Flow control
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

Physical Layer

The Physical Layer defines the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a transmission medium, such as a copper or optical cable. This includes the layout of pins, voltages, cable specifications, hubs, repeaters, network adapters, host bus adapters .

To understand the function of the Physical Layer, contrast it with the functions of the Data Link Layer. Think of the Physical Layer as concerned primarily with the

interaction of a single device with a medium, whereas the Data Link Layer is concerned more with the interactions of multiple devices. The major functions and services performed by the Physical Layer are:

- Establishment and termination of a connection to a communications medium.
- Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.
- Modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling such as copper and optical fiber or over a radio link.

Data Link Layer

The Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer. Originally, this layer was intended for point-to-point and point-to-multipoint media, characteristic of wide area media in the telephone system. The Data Link Layer provides high-speed local area networking over existing wires (power lines, phone lines and coaxial cables), includes both error correction and flow control by means of a selective repeat Sliding Window Protocol.

All Physical Layer bits are not necessarily to go into frames, as some of these bits are purely intended for Physical Layer functions. For example, every fifth bit of the FDDI bit stream is not used by the Layer. Data link layer arranges bits for both WAN and LAN service, from the Physical Layer, into logical sequences called frames.

Network Layer

The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer. The Network Layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer—sending data throughout the extended network and making the Internet connection possible. Network Layer provides logical addressing scheme in which values are chosen by the network engineer. In this scheme, IPv4 and IPv6 would have to be classed with X.25 as Subnet Access protocols because they carry interface addresses rather than node addresses. Network Layer services includes routing protocols, multicast group management, Network Layer information and Network Layer address assignment. The Network Layer could have at least 3 sub-layers:

- 1. Sub-Network Access** - It considers protocols and deal with the interface to networks, such as X.25;
- 2. Sub-Network Dependent Convergence** - when it is necessary to bring the level of a transit network up to the level of networks on either side;
- 3. Sub-Network Independent Convergence** - which handles transfer across multiple networks.

Transport Layer

The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The Transport Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state and connection oriented. This means that the Transport Layer can keep track of the segments and retransmit those that fail. The Transport layer also provides the acknowledgement of the successful data transmission and if no error free data was transferred then sends the next data.

Perhaps an easy way to visualize the Transport Layer is to compare it with a Post Office, which deals with the dispatch and classification of mail and parcels sent. Do remember, however, that a post office manages the outer envelope of mail. Higher layers may have the equivalent of double envelopes, such as cryptographic presentation services that can be read by the addressee only. All the tunneling protocols operate at the Transport Layer, such as carrying non-IP protocols.

Session Layer

The Session Layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes check-pointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session check-pointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls.

Presentation Layer

The Presentation Layer establishes a context between Application Layer entities, in which the higher-layer entities can use different syntax and semantics, as long as the presentation service understands both and the mapping between them. The presentation service data units are then encapsulated into Session Protocol data units, and moved down the stack. This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

Application Layer

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. When

identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network or the requested communication exists. Some examples of application layer implementations include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and X.400 Mail.

Transmission Control Protocol (TCP)

In May, 1974, the Institute of Electrical and Electronic Engineers (IEEE) published a paper entitled "A Protocol for Packet Network Interconnection. The paper's authors, Vinton G. Cerf and Bob Kahn, described an internetworking protocol for sharing resources using packet-switching among the nodes. A central control component of this model was the Transmission Control Program that incorporated both connection-oriented links and datagram services between hosts. The monolithic Transmission Control Program was later divided into a modular architecture consisting of the Transmission Control Protocol at the connection-oriented layer and the Internet Protocol at the internetworking (datagram) layer. The model became known informally as TCP/IP, although formally it was henceforth called the Internet Protocol Suite.

The **Transmission Control Protocol (TCP)** is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite, complementing the Internet Protocol (IP) and therefore the entire suite is commonly referred to as TCP/IP. TCP provides the service of exchanging data reliably directly between two network hosts, whereas IP handles addressing and routing message across one or more networks. In particular, TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. TCP is the protocol that major Internet applications rely on, such as the World Wide Web, e-mail, and file transfer. Other applications, that do not require reliable data stream service, use a sister protocol, the User Datagram Protocol (UDP) which provides a datagram service, which emphasizes reduced latency over reliability.

TCP provides a communication service at an intermediate level between an application program and the Internet Protocol (IP). That is, when an application program desires to send a large chunk of data across the Internet using IP, instead of breaking the data into IP-sized pieces and issuing a series of IP requests, the software can issue a single request to TCP and let TCP handle the IP details. IP works by exchanging pieces of information called packets. A packet is a sequence of bytes and consists of a header followed by a *body*. The header describes the packet's destination and, optionally, the routers to use for forwarding until it arrives at its final destination. The body contains the data IP is transmitting. Due to network congestion, traffic load balancing, or other unpredictable network behavior, IP packets can be lost, duplicated, or delivered out of order. TCP detects these problems, requests retransmission of lost packets, rearranges out-of-order packets, and even helps minimize network congestion to reduce the occurrence of the other problems. Once the TCP receiver has finally reassembled a perfect copy of the data originally transmitted, it passes that datagram to the application program. Thus, TCP abstracts the application's communication from the underlying networking details. TCP is optimized for accurate delivery rather than timely delivery, and therefore, TCP sometimes incurs relatively long delays (in the order of seconds) while waiting for

out-of-order messages or retransmissions of lost messages. It is not particularly suitable for real-time applications such as Voice over IP. For such applications, protocols like the Real-time Transport Protocol (RTP) running over the User Datagram Protocol (UDP) are usually recommended instead.

TCP is a reliable stream delivery service that guarantees delivery of a data stream sent from one host to another without duplication or losing data. Since packet transfer is not reliable, a technique known as positive acknowledgment with retransmission is used to guarantee reliability of packet transfers. This fundamental technique requires the receiver to respond with an acknowledgment message as it receives the data. The sender keeps a record of each packet it sends, and waits for acknowledgment before sending the next packet. The sender also keeps a timer from when the packet was sent, and retransmits a packet if the timer expires. The timer is needed in case a packet gets lost or corrupted. When an HTML file is sent from a Web server, the TCP software layer of that server divides the sequence of bytes of the file into segments and forwards them individually to the IP software layer (Internet Layer). The Internet Layer encapsulates each TCP segment into an IP packet by adding a header that includes (among other data) the destination IP address. Even though every packet has the same destination address, they can be routed on different paths through the network. When the client program on the destination computer receives them, the TCP layer (Transport Layer) reassembles the individual segments and ensures they are correctly ordered and error free as it streams them to an application.

Internet Protocol Version 4 (IPv4)

Internet Protocol version 4 (IPv4) is the fourth revision in the development of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet. IPv4 is still by far the most widely deployed Internet Layer protocol. As of 2010, IPv6 deployment is still in its infancy. IPv4 is a connectionless protocol for use on packet-switched Link Layer networks e.g., Ethernet. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing, or avoid duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol e.g., Transmission Control Protocol.

Internet Protocol, version 4 of IP was the first that was widely used in modern TCP/IP. *IPv4*, as it is sometimes called to differentiate it from the newer IPv6, is the Internet Protocol version in use on the Internet today, and an implementation of the protocol is running on hundreds of millions of computers. It provides the basic datagram delivery capabilities upon which all of TCP/IP functions. There are four main subsections in IPV4, which represent the four main functions of IP. The first subsection provides a comprehensive discussion of IP addressing. The second discusses how data is encoded and formatted into IP datagrams for transmission. The third describes datagram size issues and how fragmentation and reassembly are used to convey large datagrams over networks.

The last subsection covers matters related to the delivery and routing of IP datagrams. After the four main subsections I conclude our look at IPv4 with an overview of IP multicasting, which is used for delivering a single datagram to more than one recipient

IP Header Fields

- **1. Version** - The version is a binary number that is four bits long. It indicates which version of IP is being used. Currently we are using IP version four, although IP version six will soon make an impact on the networking world.
- **2. IHL (Internet Header Length)** - The IHL simply measures the length of the IP header in 32-bit words. The minimum header length is five 32-bit words.
- **3. Type of Service** - This field is for specifying special routing information. This field in particular relates to Quality of Service technologies quite well. Essentially, the purpose of this 8-bit field is to prioritize datagram that are waiting to pass through a router.
- **4. Total Length** - This 16-bit field includes the length of the IP datagram. This length includes the IP header and also the data itself.
- **5. Identification** - This is a 16-bit field that acts as a means of organizing chunks of data. If a message is too large to fit in one data packet, it is split up and all of its child packets are given the same identification number. This is handy to ensure data is rebuilt on the receiving end properly.
- **6. Flags** - This field signifies fragmentation options- such as whether or not fragments are allowed. The Flags field also has capability to tell the receiving source that more fragments are on the way, if enabled. This is done with the MF flag, also known as the more fragments flag.

4 Bits	8 Bits	16 Bits	24 Bits
Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source IP Address			
Destination IP Address			
IP Options			Padding
Data			

- **7. Fragment Offset** - This is a 13-bit field that assigns a number value to each fragment. The receiving computer will then use these numbers to reassemble the data correctly. Obviously this is only applicable if fragments are allowed.
- **8. Time to Live** - This is often known as TTL. It is a field that indicates how many hops a data packet should go through before it is discarded. Every successful pass through a router, known as a hop, decrements this field by one. When it reaches zero, it is discarded.
- **9. Protocol** - This 8-bit field indicates which protocol should be used to receive the data. Some of the more popular protocols such as TCP and UDP are identified by the numbers 6 and 17 respectively.

- **10. Header Checksum** - This 16-bit field holds a calculated value that is used to verify that the header is still valid. Each time a packet travels through a router this value is recalculated to ensure the header is still indeed valid.
- **11. Destination IP Address** - This 32-bit field holds the IP address of the receiving computer. It is used to route the packet and to make sure that only the computer with the IP address in this field obtains the packets.
- **12. Source IP Address** - This 32-bit field holds the IP address of the sending computer. It is used to verify correct delivery, and will also be the return address in case an error occurs.
- **13. IP Options** - This field can hold a fair number of optional settings. These settings are primarily used for testing and security purposes. Although clever settings such as keeping timestamp data from each router hop may seem handy, it will actually degrade speed more often than not.
- **14. Padding** - Since the IP options field varies in length depending on the configuration, we need to have this field set to occupy left over bits. This is because the header needs to be ended after a 32-bit word: no more, no less.
- **15. Data** - This is fairly self explanatory- it is simply the data that is being sent.

The above diagram should be reviewed until a firm grasp is held on the concept of an IP header. If you feel you have the concepts down well enough, it's time to move onto routing the data!

Internet Protocol Version 6 (IPv6)

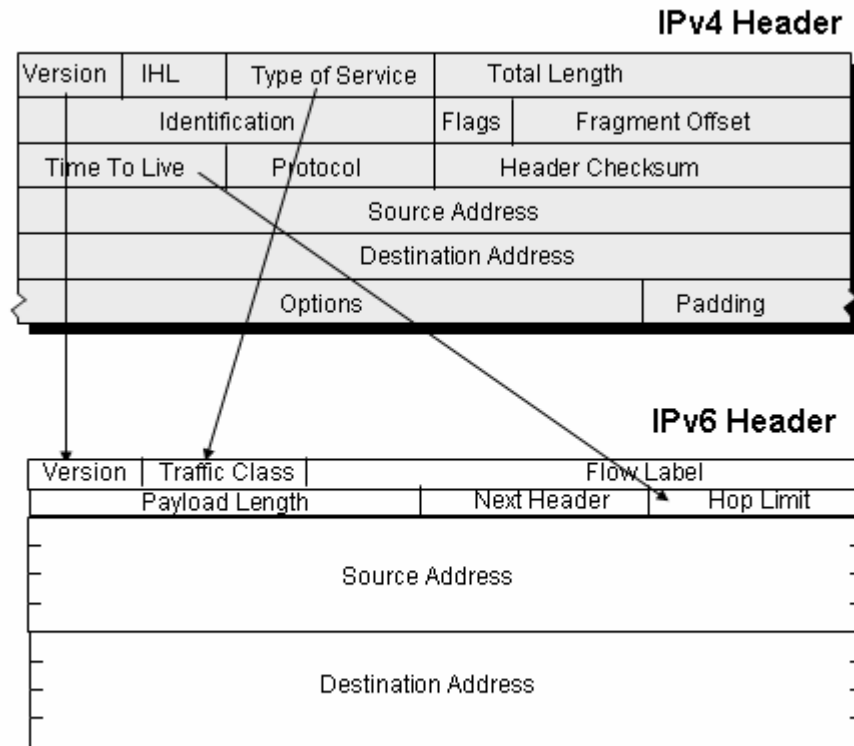
The Internet is now way too big for coordinated flag days. The transition of IPv6 into a mainstream deployed technology for the global Internet will take some years, and for many there is still a lingering doubt that will happen at all. The effort that has led to the specification of IPv6 is by no means a recently started initiative. A workshop hosted by the then Internet Activities Board (IAB) in January 1991 identified the two major scaling issues for the Internet: a sharply increasing rate of consumption of address space and a similar unconstrained growth of the inter-domain routing table. The conclusion reached at the time was that "if we assume that the internet architecture will continue in use indefinitely then we need additional [address] flexibility".

In 1994 the IETF Next Generation protocol design team defined the core IPv6 protocol. The essential characteristic of the protocol was that of an evolutionary refinement of the version 4 protocol, rather than a revolutionary departure from V4 to an entirely different architectural approach.

IPv6 Changes

The major strength of the IPv6 protocol is the use of fixed length 128 bit address fields. Other packet header changes include the dropping of the fragmentation control fields from the IP header, dropping the header checksum and length, and altering the structure of packet options within the header and adding a flow label. But it is the extended address length that is the critical change with IPv6. A 128 bit address field allows an addressable range of 2 to the 128th power, and 2 to the power of 128 is an exceptionally large number. On the other hand if we are talking about a world that is currently capable of manufacturing more than a billion silicon chips every year, and recognizing that even a 10-3 density ration would be a real

achievement, then maybe its not all that large a number after all. There is not doubt that such a protocol has the ability to encompass a network that spans billions of devices, which is a network attribute that is looking more and more necessary in the coming years.



Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4, the first publicly used implementation, which is still in dominant use currently. It is an Internet Layer protocol for packet-switched internetworks. The main driving force for the redesign of Internet Protocol is the foreseeable IPv4 address exhaustion. IPv6 is specified by the Internet Engineering Task Force (IETF) and described in Internet standard document RFC 2460, which was published in December 1998. IPv6 has a vastly larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits. The new address space thus supports 2^{128} (about 3.4×10^{38}) addresses. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

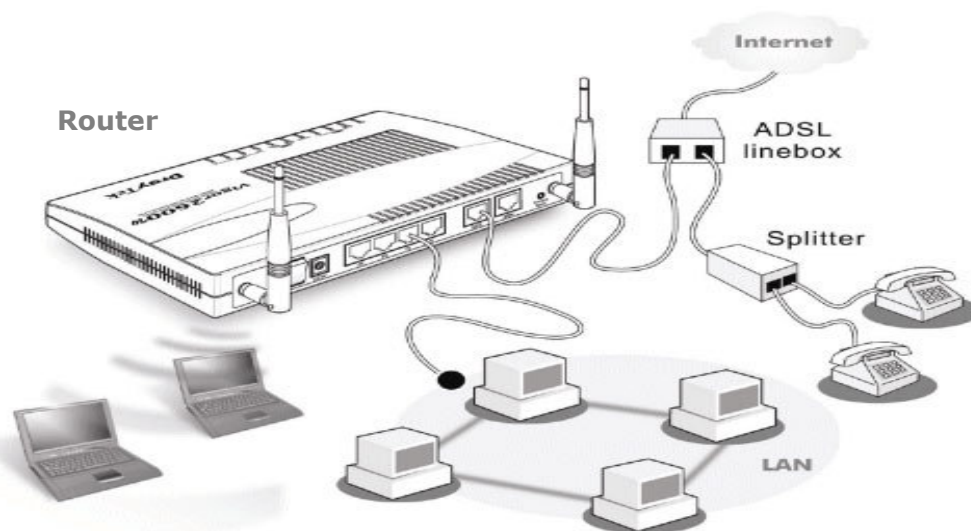
IPv6 also implements new features that simplify aspects of address assignment (stateless address autoconfiguration) and network renumbering (prefix and router announcements) when changing Internet connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from Link Layer media addressing information (MAC address). Network

security is integrated into the design of the IPv6 architecture. Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread optional deployment first in IPv4 (into which it was back-engineered). The IPv6 specifications mandate IPsec implementation as a fundamental interoperability requirement.

Routers

A **router** is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks. In packet-switched networks such as the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each point-of-presence on the Internet. A router is often included as part of a network switch

A router is a networking device whose software and hardware are customized to the tasks of routing and forwarding information. A router has two or more network interfaces, which may be to different physical types of network (such as copper cables, fiber, or wireless) or different network standards. Each network interface is a specialized device that converts electric signals from one form to another. Routers connect two or more logical subnets, which do not share a common network address. The subnets in the router do not necessarily map one-to-one to the physical interfaces of the router. The term "**layer 3 switching**" is used often interchangeably with the term "**routing**". The term **switching** is generally used to refer to data forwarding between two network devices that share a common network address. This is also called layer 2 switching or LAN switching.



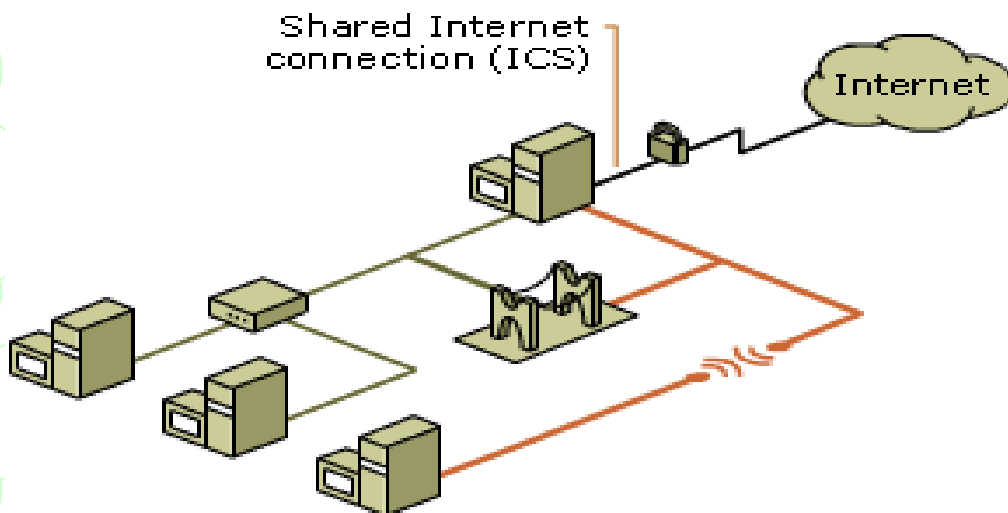
Conceptually, a router operates in two sub-systems.

- **Control plane:** where a router builds a table (called routing table) as how a packet should be forwarded through which interface, by using either statically configured statements (called static routes) or by exchanging information with other routers in the network through a dynamical routing protocol.
- **Forwarding plane:** where the router actually forwards traffic (called packets in IP) from ingress (incoming) interfaces to an egress (outgoing) interface that is appropriate for the destination address that the packet carries with it, by following rules derived from the routing table that has been built in the control plane.

For pure Internet Protocol (IP) forwarding function, a router is designed to minimize the state information on individual packets. A router does not look into the actual data contents that the packet carries, but only at the layer 3 addresses to make a forwarding decision, plus optionally other information in the header. Forwarding decisions can involve decisions at layers other than the IP internetwork layer or OSI layer 3. A function that forwards based on data link layer, or OSI layer 2, information is properly called a bridge or switch. This function is referred to as layer 2 switching, as the addresses it uses to forward the traffic are layer 2 addresses in the OSI layer model.

Bridges

A **bridge** device filters data traffic at a network boundary. Bridges reduce the amount of traffic on a LAN by dividing it into two segments. Bridges operate at the data link layer (Layer 2) of the OSI model. Bridges inspect incoming traffic and decide whether to forward or discard it. An Ethernet bridge, for example, inspects each incoming Ethernet frame - including the source and destination MAC addresses, and sometimes the frame size - in making individual forwarding decisions.



A bridge reads the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets. Bridges can be programmed to reject packets from particular

networks. Bridging occurs at the data link layer of the OSI model, which means the bridge cannot read IP addresses, but only the outermost hardware address of the packet. In our case the bridge can read the Ethernet data which gives the hardware address of the destination address, not the IP address. Bridges forward all broadcast messages. Only a special bridge called a translation bridge will allow two networks of different architectures to be connected. Bridges do not normally allow connection of networks with different architectures. The hardware address is also called the MAC (media access control) address. To determine the network segment a MAC address belongs to, bridges use one of:

- Transparent Bridging - They build a table of addresses (bridging table) as they receive packets. If the address is not in the bridging table, the packet is forwarded to all segments other than the one it came from. This type of bridge is used on Ethernet networks.
- Source route bridging - The source computer provides path information inside the packet. This is used on Token Ring networks

The Network Bridge feature that is available with Windows XP; Windows Server 2003, Standard Edition; and Windows Server 2003, Enterprise Edition allows you to connect LAN segments simply by clicking the **Bridge Connections** menu command. No configuration is required, and you do not need to purchase additional hardware, such as routers or bridges. Network Bridge automates the configuration that is required to route traffic between multi-segment networks that consist of a single type of media or mixed media.

Gateway

A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes, while the nodes that connect the networks in between are gateways. For example, the computers that control traffic between company networks or the computers used by internet service providers (ISPs) to connect users to the internet are gateway nodes. In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

On an IP network, clients should automatically send IP packets with a destination outside a given subnet mask to a network gateway. A subnet mask defines the IP range of a network. For example, if a network has a base IP address of 192.168.0.0 and has a subnet mask of 255.255.255.0, then any data going to an IP address outside of 192.168.0.X will be sent to that network's gateway. While forwarding an IP packet to another network, the gateway might or might not perform Network Address Translation. A gateway is an essential feature of most routers, although other devices (such as any PC or server) can function as a gateway.

A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Most gateways operate at the application layer, but can operate at the network or session layer of the OSI model.

Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model. To confuse issues, when talking about a router that is used to interface to another network, the word gateway is often used. In a communications network, a network node equipped for interfacing with another network that uses different protocols. A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks. A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions. Gateways, also called protocol converters, can operate at any layer of the OSI model.

Ethernet Hub

A network hub is a fairly unsophisticated broadcast device. Hubs do not manage any of the traffic that comes through them, and any packet entering any port is broadcast out on all other ports. Since every packet is being sent out through all other ports, packet collisions result—which greatly impedes the smooth flow of traffic. Most hubs detect typical problems, such as excessive collisions and jabbering on individual ports, and *partition* the port, disconnecting it from the shared medium. Thus, hub-based Ethernet is generally more robust than coaxial cable-based Ethernet (e.g. 10BASE2, thinnet), where a misbehaving device can adversely affect the entire collision domain. Even if not partitioned automatically, a hub makes troubleshooting easier because status lights can indicate the possible problem source or, as a last resort, devices can be disconnected from a hub one at a time much more easily than a coaxial cable. They also remove the need to *troubleshoot* faults on a huge cable with multiple taps. An **Ethernet hub, active hub, network hub, repeater hub, hub** or **concentrator** is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiparty repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.



Switches

A **network switch** or **switching hub** is a computer networking device that connects network segments. The term commonly refers to a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches. The term **network switch** does not generally encompass unintelligent or passive network devices such as hubs and repeaters.

The network switch, packet switch (or just switch) plays an integral part in most Ethernet local area networks or LANs. Mid-to-large sized LANs contain a number of linked managed switches. Small office/home office (SOHO) applications typically use a single switch or an all-purpose converged device such as a gateway access to small office/home broadband services such as DSL router or cable Wi-Fi router. In most of these cases, the end-user device contains a router and components that interface to the particular physical broadband technology, as in Linksys 8-port and 48-port devices. User devices may also include a telephone interface for VoIP. Switches may operate at one or more OSI layers, including physical, data link, network, or transport (i.e., end-to-end). A device that operates simultaneously at more than one of these layers is known as a multilayer switch.

Mobile Internet Protocol (Mobile IP)

Mobile IP (or **IP mobility**) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. **Mobile IPv6**, the IP mobility implementation for the next generation of the Internet Protocol, IPv6, is described in RFC 3775. The Mobile IP protocol allows location-independent routing of IP datagrams on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from its home network, a mobile node is associated with a *care-of* address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its *home agent*. Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagrams to the mobile node through the *tunnel*.

Mobile IP provides an efficient, scalable mechanism for roaming within the Internet. Using Mobile IP, nodes may change their point-of-attachment to the Internet without changing their home IP address. This allows them to maintain transport and higher-layer connections while roaming. Node mobility is realized without the need to propagate host-specific routes throughout the Internet routing fabric.

Applications

Mobile IP is most often found in wired and wireless environments where users need to carry their mobile devices across multiple LAN subnets. Examples of use are in roaming between overlapping wireless systems, e.g., IP over WLAN, WiMAX etc. Currently, Mobile IP is not required within cellular systems such as 3G, to provide transparency when Internet users migrate between cellular towers, since these systems provide their own data link layer handover and roaming mechanisms. However, it is often used in 3G systems to allow seamless IP mobility between different Packet Data Serving Node (PDSN) domains. In many applications (e.g., VPN, VoIP), sudden changes in network connectivity and IP address can cause problems. A mobile node can have two addresses - a permanent home address and a care-of address (CoA), which is associated with the network the mobile node is visiting. Two kinds of entities comprise a Mobile IP implementation:

- A *home agent* stores information about mobile nodes whose permanent home address is in the home agent's network.
- A *foreign agent* stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP.

A node wanting to communicate with the mobile node uses the permanent home address of the mobile node as the destination address to send packets to. Because the home address logically belongs to the network associated with the home agent, normal IP routing mechanisms forward these packets to the home agent. Instead of forwarding these packets to a destination that is physically in the same network as the home agent, the home agent redirects these packets towards the foreign agent through an IP tunnel by encapsulating the datagram with a new IP header using the care of address of the mobile node.

When acting as transmitter, a mobile node sends packets directly to the other communicating node through the foreign agent, without sending the packets through the home agent, using its permanent home address as the source address for the IP packets. This is known as triangular routing. If needed, the foreign agent could employ *reverse tunneling* by tunneling the mobile node's packets to the home agent, which in turn forwards them to the communicating node. This is needed in networks whose gateway routers have ingress filtering enabled and hence the source IP address of the mobile host would need to belong to the subnet of the foreign network or else the packets will be discarded by the router.

The Mobile IP protocol defines the following:

- an authenticated registration procedure by which a mobile node informs its home agent(s) of its care-of-address(es);
- an extension to ICMP Router Discovery, which allows mobile nodes to discover prospective home agents and foreign agents; and
- the rules for routing packets to and from mobile nodes, including the specification of one mandatory tunneling mechanism and several optional tunneling mechanisms.

Research and Development

Enhancements to the Mobile IP technique, such as Mobile IPv6 and Hierarchical Mobile IPv6 (HMIPv6) are being developed to improve mobile communications in certain circumstances by making the processes more secure and more efficient. Researchers create support for mobile networking without requiring any pre-deployed infrastructure as it currently is required by MIP. One such example is Interactive Protocol for Mobile Networking (IPMN) which promises supporting mobility on a regular IP network just from the network edges by intelligent signalling between IP at end-points and application layer module with improved quality of service.

Researchers are also working to create support for mobile networking between entire subnets with support from Mobile IPv6. One such example is Network Mobility (NEMO) Network Mobility Basic Support Protocol by the IETF Network Mobility Working Group which supports mobility for entire Mobile Networks that move and to attach to different points in the Internet. The protocol is an extension of Mobile IPv6 and allows session continuity for every node in the Mobile Network as the network moves.

Changes in IPv6 for Mobile IPv6

- A set of mobility options to include in mobility messages
- A new Home Address option for the Destination Options header
- A new Type 2 Routing header
- New Internet Control Message Protocol for IPv6 (ICMPv6) messages to discover the set of home agents and to obtain the prefix of the home link
- Changes to router discovery messages and options and additional Neighbor Discovery options

Cellular Network

A **cellular network** is a radio network distributed over land areas called cells, each served by at least one fixed-location transceiver known as a cell site or base station. When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission. Cellular networks offer a number of advantages over alternative solutions:

- increased capacity
- reduced power use
- larger coverage area
- reduced interference from other signals

An example of a simple non-telephone cellular system is an old taxi driver's radio system where the taxi company has several transmitters based around a city that can communicate directly with each taxi. The most common example of a cellular network is a mobile phone (cell phone) network. A mobile phone is a portable telephone which receives or makes calls through a cell site (base station), or transmitting tower. Radio waves are used to transfer signals to and from the cell phone. Modern mobile phone networks use cells because radio frequencies are a limited, shared resource. Cell-sites and handsets change frequency under computer control and use low power transmitters so that a limited number of radio frequencies can be simultaneously used by many callers with less interference. A cellular network is used by the mobile phone operator to achieve both coverage and capacity for their subscribers. Large geographic areas are split into smaller cells to avoid line-of-sight signal loss and to support a large number of active phones in that area. All of the cell sites are connected to telephone exchanges (or switches) , which in turn connect to the public telephone network. In cities, each cell site may have a range of up to approximately ½ mile, while in rural areas, the range could be as much as 5 miles. It is possible that in clear open areas, a user may receive signals from a cell site 25 miles away. Almost all mobile phones use cellular technology, including GSM, CDMA.

CDMA Architecture

CDMA network deployment and subscriber growth have developed considerable momentum, and data services are now available from a number of carriers. Currently, these carriers use circuit-switched technology operating at 14.4 Kbps. As with GSM, CDMA requires a handset that specifically supports data. Connect the phone to a laptop, and the phone operates just like a modem, enabling you to establish dial-up connections to the Internet, your corporate remote access server (RAS), and so on. WAP-based microbrowser applications are also being made available. Another service for CDMA networks is called QuickNet Connect. By eliminating conventional modem connections, this service allows fast connections (of approximately five seconds) to the Internet. See Figure 3. To the user, the carrier appears like an ISP offering dial-up Internet service.

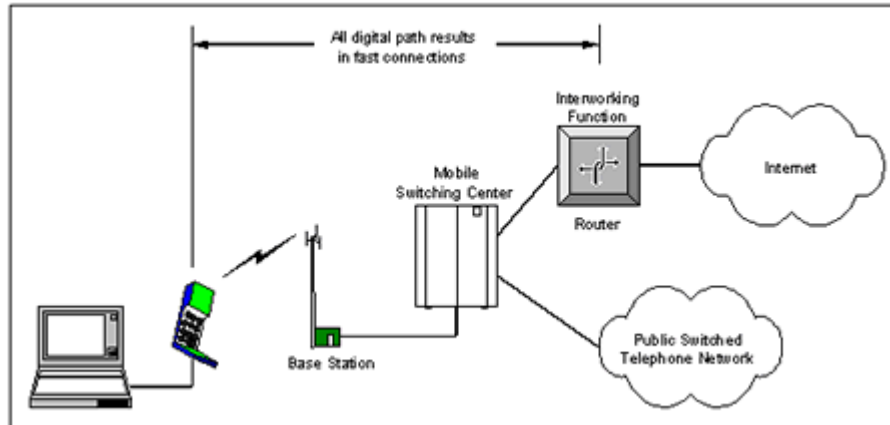


Figure 3: QuickNet Connect for CDMA

Today's CDMA service is based on the IS-95A standard. A refinement of this standard, IS-95B, allows up to eight channels to be combined for packet-data rates as high as 64 Kbps. Japanese CDMA carriers, IDO and DDI, are planning on deploying this higher-speed service by early 2000. Beyond IS-95B, CDMA evolves into 3G technology in a standard called CDMA2000. CDMA2000 comes in two phases. The first, with a specification already completed, is 1XRTT, while the next phase is 3XRTT. The 1X and 3X refer to the number of 1.25 MHz wide radio carrier channels used, and RTT refers to radio-transmission technology. CDMA2000 includes numerous improvements over IS-95A, including more sophisticated power control, new modulation on the reverse channels, and improved data encoding methods. The result is significantly higher capacity for the same amount of spectrum, and indoor data rates up to 2Mbps that meet the IMT-2000 requirements. The full-blown 3XRTT implementation of CDMA requires a 5MHz spectrum commitment for both forward and reverse links. However, 1XRTT can be used in existing CDMA channels since it uses the same 1.25 MHz bandwidth.

A CDMA network consists of the following components:

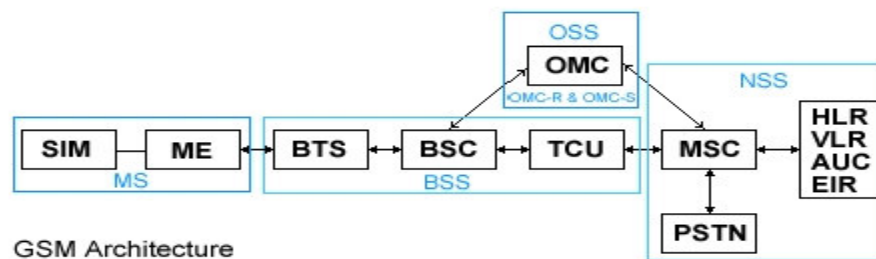
- **Mobile station.** The CDMA mobile station (or mobile phone) communicates with other parts of the system through the base-station system.
- **Base station (BS).** The base station (BS) handles the radio interface to the mobile station. The base station is the radio equipment (transceivers and antennas)
- **Base station controller (BSC).** The BSC provides the control functions and physical links between the MSC and BTS. It provides functions such as handover, cell configuration data and control of RF power levels in base transceiver stations. A number of BSCs are served by a MSC.
- **Mobile switching center (MSC).** The MSC performs the telephony switching functions of the system. It also performs such functions as toll ticketing, network interfacing, common channel signalling, and others.
- **Home location register (HLR).** The HLR database is used for storage and management of subscriptions. The home location register stores permanent data about subscribers, including a subscriber's service profile, location information,

and activity status.

- *Visitor location register (VLR)*. The VLR database contains temporary information about subscribers that is needed by the mobile services switching center (MSC) in order to service visiting subscribers. When a mobile station roams into a new mobile services switching center (MSC) area, the visitor location register (VLR) connected to that MSC will request data about the mobile station from the HLR, reducing the need for interrogation of the home location register (HLR).
- *Authentication center (AC)*. The AC provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call. The authentication center (AUC) also protects network operators from fraud.
- *Operation and administration (OAM)*. The OAM is the functional entity from which the network operator monitors and controls the system. The purpose of operation and support system is to offer support for centralized, regional, and local operational and maintenance activities that are required for CDMA.

GSM Architecture

The GSM (Global System for Mobile Communication) Architecture consists of three major sub-systems. These are Base Station Sub-System (BSS) that provides the air interface for Mobile Stations (MS), Network Sub-System (NSS) that connects calls between users, and Operation Sub-System (OSS) that allows remote monitoring and management of network.



GSM Architecture

SIM - Subscriber Identity Module

ME - Mobile Equipment

BTS - Base Transceiver Station

BSC - Base Station Controller

TCU - Transcoder Unit

MSC - Mobile Switching Centre

PSTN - Public Switched Telephone Network

HLR - Home Location Register

VLR - Visitor Location Register

AUC - Authentication Centre

EIR - Equipment Identity Register

OMC-R - OMC devoted to BSS

OMC - Operations & Maintenance Centre

OMC-S - OMC devoted to NSS

Unit 2

Principals of Information Security

Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Confidentiality is necessary but not sufficient for maintaining the privacy of the people whose personal information a system holds.

Integrity

In information security, integrity means that data cannot be modified without authorization. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on. There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mis-type someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

Authenticity

In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation

Information Classification

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification. The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

The type of information security classification labels selected and used will depend on the nature of the organization, with examples being:

- ❖ In the business sector, labels such as: **Public, Sensitive, Private, Confidential.**
- ❖ In the government sector, labels such as: **Unclassified, Sensitive But Unclassified, Restricted, Confidential, Secret, Top Secret.**

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification a particular information asset has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place.

Electronic Commerce

Electronic commerce, commonly known as **e-commerce** or **e-business** consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks. The amount of trade conducted electronically has grown extraordinarily with widespread Internet usage. The use of commerce is conducted in this way; spurring and drawing on innovations in electronic funds transfer, Internet marketing, online transaction processing, electronic data interchange (EDI) and automated data collection systems. Modern electronic commerce typically uses the World Wide Web at least at some point in the transaction's lifecycle, although it can encompass a wider range of technologies such as e-mail as well.

B2B Electronic commerce that is conducted between businesses is referred to as business-to-business or B2B. B2B can be open to all interested parties (e.g. commodity exchange) or limited to specific, pre-qualified participants (private electronic market).

B2C Electronic commerce that is conducted between businesses and consumers, on the other hand, is referred to as business-to-consumer or B2C. This is the type of electronic commerce conducted by companies such as Amazon.com.

Online shopping is a form of electronic commerce where the buyer is directly online to the seller's computer usually via the internet. If an intermediary is present, then the sale and purchase transaction is called electronic commerce such as eBay.com. Electronic commerce is generally considered to be the sales aspect of e-business. It also consists of the exchange of data to facilitate the financing and payment aspects of the business transactions.

Electronic Government

Electronic government or e-Government (also known as **digital government**, **online government**) is creating a comfortable, transparent, and cheap interaction between government and citizens (G2C – government to citizens), government and business enterprises (G2B –government to business enterprises) and relationship between governments (G2G – inter-agency relationship). There are four domains of **e-government** namely, governance, information and communication technology (ICT), business process re-engineering (BPR) and e-citizen.

Definitions of e-Government and e-Governance abound in literature. Definitions for e-Government and e-Governance range from the working definitions like “the ability for anyone visiting the city website to communicate and/or interact with the city via the Internet in any way more sophisticated than a simple email letter to the generic city (or webmaster) email address provided at the site” to “the use of technology to enhance the access to and delivery of government services to benefit citizens, business partners and employees”. Focus of these definitions range from those focusing on Information and communication technologies (ICTs) to those focusing on ICT-enabled government and governance transformation. Some examples of such definitions include:

- ❖ The use of ICTs, and particularly the Internet, as a tool to achieve better government.
- ❖ The use of information and communication technologies in all facets of the operations of a government organization.
- ❖ The continuous optimization of service delivery, constituency participation and governance by transforming internal and external relationships through technology, the Internet and new media.

Whilst e-Government has traditionally been understood as being centered on the operations of government, e-Governance is understood to extend the scope by including citizen engagement and participation in governance. As such, following in line with the OECD definition of e-Government, e-Governance can be defined as the use of ICTs as a tool to achieve better governance.

Electronic Data Interchange

Electronic Data Interchange is the means of transferring of data between different parties using networks, such as VANs or the Internet. As more and more companies get connected to the Internet, EDI is becoming increasingly important as an easy mechanism for companies to buy, sell, and trade information. EDI can be formally defined as '**The transfer of structured data, by agreed message standards, from one computer system to another without human intervention**'. The National Institute of Standards and Technology in a 1996 publication defines Electronic Data Interchange as "the computer-to-computer interchange of strictly formatted messages that represent documents other than monetary instruments. EDI implies a sequence of messages between two parties, either of whom may serve as originator or recipient. The formatted data representing the documents may be transmitted from originator to recipient via telecommunications or physically transported on electronic storage media. In EDI, the usual processing of received messages is by computer only.

EDI Standards

The EDI standard says which pieces of information are mandatory for a particular document, which pieces are optional and give the rules for the structure of the document. The standards are like building codes. Just as two kitchens can be built "to code" but look completely different, two EDI documents can follow the same standard and contain different sets of information. For example a food company may indicate a product's expiration date while a clothing manufacturer would choose to send color and size information. The EDI standards were designed to be independent of communication and software technologies. EDI can be transmitted using any methodology agreed to by the sender and recipient. This includes a variety of technologies, including modem FTP, E-mail, HTTP etc. It is important to differentiate between the EDI documents and the methods for transmitting the.

EDI documents generally contain the same information that would normally be found in a paper document used for the same organizational function. However, EDI is not confined to just business data related to trade but encompasses all fields such as medicine (e.g., patient records and laboratory results), transport (e.g., container and modal information), engineering and construction, etc may also cover in the scope of EDI. There are four major sets of **EDI standards**:

- ❖ The UN-recommended UN/EDIFACT is the only international standard and is predominant outside of North America.
- ❖ The US standard ANSI ASC X12 (X12) is predominant in North America.
- ❖ The TRADACOMS standard developed by the ANA (Article Numbering Association) is predominant in the UK retail industry.
- ❖ The ODETTE standard used within the European automotive industry

All of these standards first appeared in the early to mid 1980s. The standards prescribe the formats, character sets, and data elements used in the exchange of business documents and forms. Many business transactions are formatted in XML and transported over the Internet using the HTTP Web protocol. The complete **X12 Document List** includes all major business documents, including purchase orders (called "ORDERS" in UN/EDIFACT and an "850" in X12) and invoices (called "INVOIC" in UN/EDIFACT and an "810" in X12).

EDI and E-Commerce Gateway in India (ICENET)

The Indian Customs and Excise NETWORK (ICENET) are proposed to be set up between EC / EDI (Electronic Commerce / Electronic Data Interchange) gateway and the Customs nodes. The network would cater to all traffic between the gateway and the nodes, which would primarily be related to transactions, as well as inter node data, which would be in the nature of messaging and database queries. ICENET has been designed as a redundant terrestrial network with VSAT backup where necessary (Jaipur, Ludhiana, Petrapole, Raxaul & Haldia). VSATs would be operational using ICENET and would be provided by Customs. The backbone of ICENET would be E1 lines of 2.048 Mbps or higher bandwidth to be leased from the Department of Telecommunications, Government of India. The E1 lines would terminate at the cluster locations in the metropolitan cities of Delhi, Mumbai, Calcutta and Chennai from where leased lines of smaller bandwidth (64/128 Kbps) would be used to connect the Customs nodes to the cluster locations. The selected vendor would be responsible for setting up ICENET on a turnkey basis (including interfacing with all other agencies such as the Department of Telecommunications) and managing the network for a period of three years from the date of commissioning

It is now proposed to extend EDI services to all trading partners by setting up the Customs gateway, which would handle all transactions centrally and route it to the concerned Customs Commissionerate over ICENET. Tenders are called to propose a complete solution on a turnkey basis comprising hardware, software and networking arrangements. The selected vendor would be required to customize the solution to suit the needs of ICES and maintain the system on a continuing basis for an initial period of three years. For this purpose, the vendor would be required to work in close association with domain experts from the Customs department. The proposed Customs gateway will enable data interchange partners to transmit messages (including lodging of documents) to the Customs computer system and also receive messages from it, in any format. The messages could be based on international messaging standards such as UN/EDIFACT or in the form of ASCII files. The department proposes to enable the users to send/receive messages through web based forms, email attachments of File Transfer Protocol (FTP) over the Internet. The proposed solution will be versatile enough to receive, transmit and process messages in any of these modes or a variant or combination thereof, and enable seamless conversion into ICES formats

Electronic Payment System

Electronic Payment is a financial exchange that takes place online between buyers and sellers. The content of this exchange is usually some form of digital financial instrument (such as encrypted credit card numbers, electronic cheques or digital cash) that is backed by a bank or an intermediary, or by a legal tender. The various factors that have led the financial institutions to make use of electronic payments are:

Decreasing technology cost: The technology used in the networks is decreasing day by day, which is evident from the fact that computers are now dirt-cheap and Internet is becoming free almost everywhere in the world.

Reduced operational and processing cost: Due to reduced technology cost the processing cost of various commerce activities becomes very less. A very simple reason to prove this is the fact that in electronic transactions we save both paper and time.

There are numerous different payments systems available for online merchants. These include the traditional credit, debit and charge card but also new technologies such as digital wallets, e-cash, mobile payment and e-checks. Another form of payment system is allowing a 3rd party to complete the online transaction for you. These companies are called Payment Service Providers (PSP); a good example is Paypal or WorldPay

Electronic Tokens

An electronic token is a digital analog of various forms of payment backed by a bank or financial institution. There are two types of tokens:

Real Time: (or Pre-paid tokens) - These are exchanged between buyer and seller, their users pre-pay for tokens that serve as currency. Transactions are settled with the exchange of these tokens. Examples of these are DigiCash, Debit Cards, Electronic purse etc.

Post Paid Tokens: These are used with fund transfer instructions between the buyer and seller. Examples are Electronic cheques, Credit card data etc.

Electronic or Digital Cash:

Digital cash is based on cryptographic systems called "Digital Signatures" similar to the signatures used by banks on paper cheques to authenticate a customer. Purchase of digital cash from an online currency server (or bank) involves 2 steps:

- ❖ Establishment of an account in this step we are given a unique digital number which also becomes our digital signature. As it is a number known only to the customer and the bank, forgery, which may be done in paper cheques, becomes very difficult.
- ❖ Maintenance of sufficient money in the account is required to back any purchase. This combines computerized convenience with security and privacy that improve upon paper cash.

There are following properties of Digital Cash

- ❖ **Must have a monetary value:** It must be backed by cash (currency), bank authorized credit or a bank certified cashier's check.
- ❖ **Must be interoperable or exchangeable:** As payment for other digital cash, paper cash, goods or services, lines of credit, bank notes or obligations, electronic benefit transfers and the like.
- ❖ **Must be storable and retrievable:** Cash could be stored on a remote computer's memory, in smart cards, or on other easily transported standard or special purpose devices. Remote storage or retrieval would allow users to exchange digital cash from home or office or while traveling.
- ❖ **Should not be easy to copy or tamper with while it is being exchanged.** This is achieved by using the following technologies; these are nothing but new and very efficient versions of the old art of cryptography.

Electronic Cheques

The electronic cheques are modeled on paper checks, except that they are initiated electronically. They use digital signatures for signing and endorsing and require the use of digital certificates to authenticate the payer, the payer's bank and bank account. They are delivered either by direct transmission using telephone lines or by public networks such as the Internet.

Benefits of electronic Cheques:

- Well suited for clearing micro payments. Conventional cryptography of e-cheques makes them easier to process than systems based on public key cryptography (like digital cash).
- They can serve corporate markets. Firms can use them in more cost-effective manner.
- They create float and the availability of float is an important requirement of Commerce

Credit and Debit Cards

Over the years, credit cards have become one of the most common forms of payment for e-commerce transactions. In North America almost 90% of online B2C transactions were made with this payment type. Turban et al. goes on to explain that it would be difficult for an online retailer to operate without supporting credit and debit cards due to its widespread use. Increased security measures such as the use of the card verification number (CVN) which detects fraud by comparing the verification number on the printed on the signature strip on the back of the card with the information on file with the cardholder's issuing bank. Also online merchants have to comply with stringent rules stipulated by the credit and debit card issuers (**Visa and MasterCard**) this means that merchants must have security protocol and procedures in place to ensure transactions are more secure. This can also include having a certificate from an authorized certification authority (CA) who provides PKI infrastructure for securing credit and debit card transactions.

Despite this widespread use in North America, there are still a large number of countries such as China, India and Pakistan that have some problems to overcome in regard to credit card security. In the meantime, the use of smartcards has become extremely popular. There are following limitations of Debit and Credit Cards:

- ❖ They are identification cards owned by the issuer & restricted to one user i.e. cannot be given away.
- ❖ They are not legal tender
- ❖ Their usage requires an account relationship and authorization system.

Smart Card

A Smartcard is similar to a credit card; however it contains an embedded 8-bit microprocessor and uses electronic cash which transfers from the consumers' card to the sellers' device. A popular smartcard initiative is the VISA Smartcard. Using the VISA Smartcard you can transfer electronic cash to your card from your bank account, and you can then use your card at various retailers and on the internet.

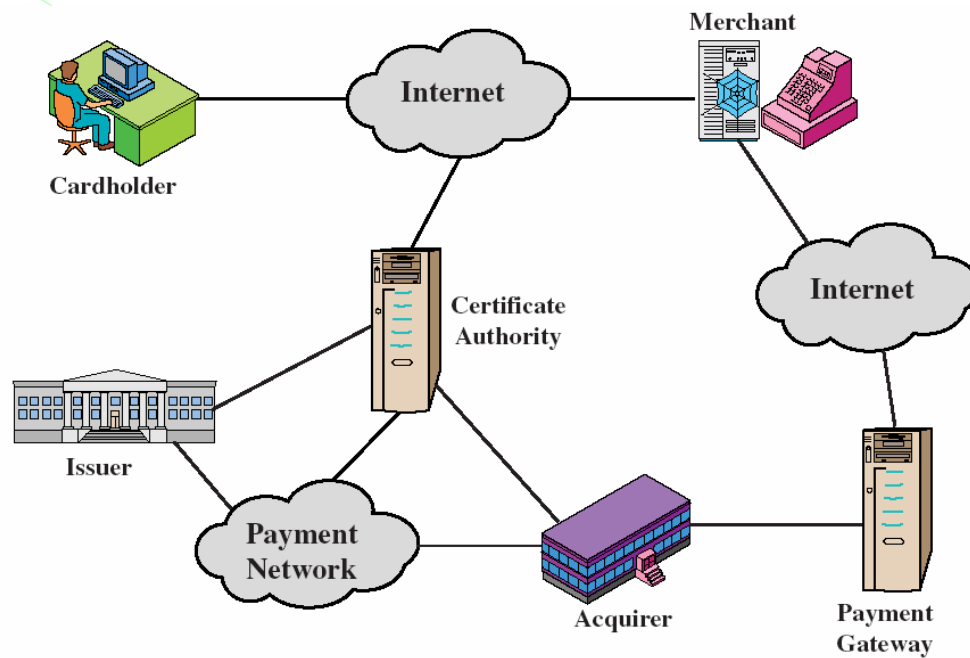
Secure Electronic Transaction (SET) Protocol

*SET was developed by **SETco**, led by VISA and MasterCard (and involving other companies such as GTE, IBM, Microsoft, Netscape, RSA and VeriSign) starting in 1996. SET was based on X.509 certificates with several extensions. The first version was finalised in May 1997 and a pilot test was announced in July 1998.*

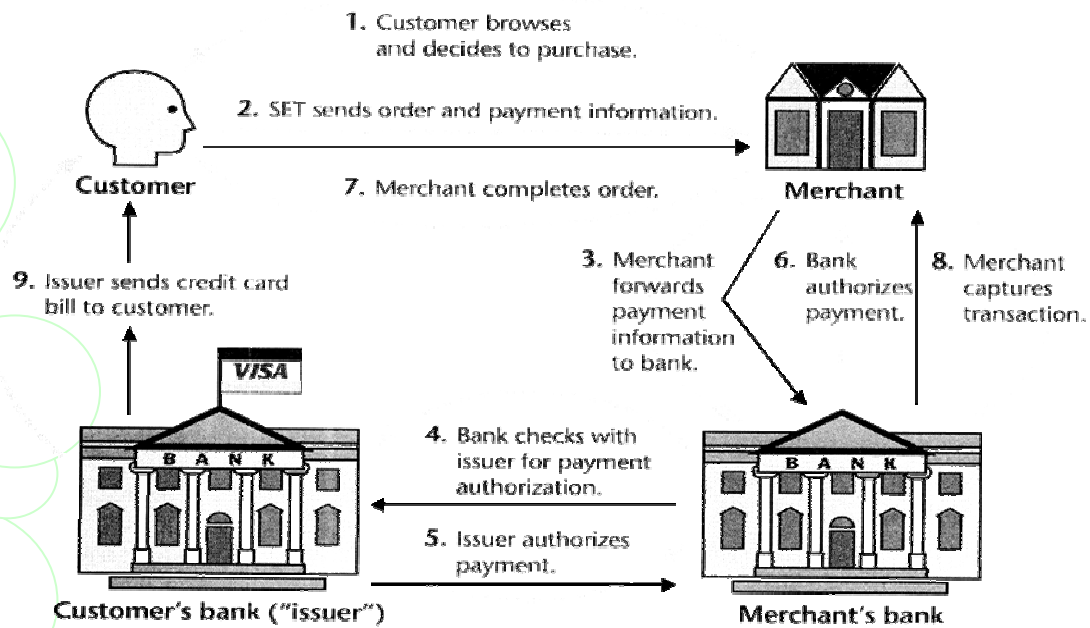
SET Protocol is a standard protocol for securing credit card transactions over insecure networks, specifically, the Internet. SET was not itself a payment system, but rather a set of security protocols and formats that enable users to employ the existing credit card payment infrastructure on an open network in a secure fashion. However, it failed to gain traction. VISA now promotes the 3-D secure scheme. SET allowed parties to cryptographically identify themselves to each other and exchange information securely. SET used a blinding algorithm that, in effect, would have let merchants substitute a certificate for a user's credit-card number. If SET were used, the merchant itself would never have had to know the credit-card numbers being sent from the buyer, which would have provided verified good payment but protected customers and credit companies from fraud. SET was intended to become the de facto standard of payment method on the Internet between the merchants, the buyers, and the credit-card companies. Network effect - need to install client software (an e-wallet). It has following key features.

- ❖ **Confidentiality:** All messages are encrypted
- ❖ **Trust:** All parties must have digital certificates
- ❖ **Privacy:** information made available only when and where necessary
- ❖ Developed by **Visa and MasterCard**
- ❖ Designed to **protect credit card transactions**

Parties in SET



SET Transaction



- ❖ The customer sends order and payment information to the merchant.
- ❖ The merchant requests payment authorization from the payment gateway prior to shipment.
- ❖ The merchant confirms order to the customer.
- ❖ The merchant provides the goods or service to the customer.
- ❖ The merchant requests payment from the payment gateway.
- ❖ The customer opens an account with a card issuer. Such as MasterCard, Visa.
- ❖ The customer receives a X.509 V3 certificate signed by a bank using X.509 V3 standards.
- ❖ A merchant who accepts a certain brand of card must possess two X.509 V3 certificates, one for signing & one for key exchange
- ❖ The customer places an order for a product or service with a merchant.
- ❖ The merchant sends a copy of its certificate for verification

Electronic Bill Presentment and Payment

Electronic bill presentment and payment (EBPP) is a fairly new technique that allows consumers to view and pay bills electronically. There are a significant number of bills that consumers pay on a regular basis, which include: power bills, water, oil, internet, phone service, mortgages, car payments etc. EBPP systems send bills from service providers to individual consumers via the internet. The systems also enable payments to be made by consumers, given that the amount that appears on the e-bill is correct.

The biggest difference between EBPP systems and the traditional method of bill payment is that of technology. Rather than receiving a bill through the mail, writing out and sending a check, consumers receive their bills in an email, or are prompted to visit a website to view and pay their bills.

Three broad models of EBPP have emerged. These are:

1. Consolidation, where numerous bills for any one recipient are made available at one Web site, most commonly the recipient's bank. In some countries, such as Australia, New Zealand and Canada, the postal service also operates a consolidation service. The actual task of consolidation is sometimes performed by a third party and fed to the Web sites where consumers receive the bills. The principal attraction of consolidation is that consumers can receive and pay numerous bills at the one location, thus minimizing the number of login IDs and passwords they must remember and maintain.
2. Biller Direct, where the bills produced by an organization are made available through that organization's Web site. This model works well if the recipient has reasons to visit the biller's Web site other than to receive their bills. In the freight industry, for example, customers will visit a carrier's Web site to track items in transit, so it is reasonably convenient to receive and pay freight bills at the same site.
3. Direct email delivery, where the bills are emailed to the customer's In Box. This model most closely imitates the analog postal service. It is convenient, because almost everyone has email and the customer has to do nothing except use email in order to receive a bill. Email delivery is proving especially popular in the B2B market in many countries.

CyberCash, Inc. (www.cybercash.com)

www.cybercash.com is an internet payment service for electronic commerce, headquartered in Reston, Virginia. It was founded in August 1994 by Daniel C. Lynch (who served as chairman), William N. Melton (who served as president and CEO, and later chairman), Steve Crocker (Chief Technology Officer), and Bruce G. Wilson. The company initially provided an electronic wallet software to consumers and provided software to merchants to accept credit card payments. Later they also offered "CyberCoin", a micropayment system modeled after the NetBill research project at Carnegie Mellon University, which they later licensed. Despite a trial with ESPN.com, CyberCoin never took off, and the focus remained on providing software for consumers and merchants to process credit card payments.

NetBill (www.netbill.org)

NetBill is a business model set of protocols, and software implementation for commerce in information goods and other network-delivered services. It has very low transaction costs for micro-payments (around 1 cent for a 10 cent item), protects the privacy of the transaction, and is highly scalable. While NetBill will enable a market economy in information, it is still expected that there will be an active exchange of free information

Unit 3

Information Security Controls

Security is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of service. Because certain computer security controls inhibit productivity, security is typically a compromise toward which security practitioners, system users, and system operations and administrative personnel work to achieve a satisfactory balance between security and productivity. Controls for providing information security can be physical, technical, or administrative. These three categories of controls can be further classified as either preventive or detective. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred.

Three other types of controls supplement preventive and detective controls. They are usually described as deterrent, corrective, and recovery. Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to not violate security. Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation. Execution of corrective controls could result in changes to existing physical, technical, and administrative controls. Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation.

Deterrent, corrective, and recovery controls are considered to be special cases within the major categories of physical, technical, and administrative controls; they do not clearly belong in either preventive or detective categories. For example, it could be argued that deterrence is a form of prevention because it can cause an intruder to turn away; however, deterrence also involves detecting violations, which may be what the intruder fears most. Corrective controls, on the other hand, are not preventive or detective, but they are clearly linked with technical controls when antiviral software eradicates a virus or with administrative controls when backup procedures enable restoring a damaged data base. Finally, recovery controls are neither preventive nor detective but are included in administrative controls as disaster recovery or contingency plans.

Physical Controls

Physical security is the use of locks, security guards, badges, alarms, and similar measures to control access to computers, related equipment (including utilities), and the processing facility itself. In addition, measures are required for protecting computers, related equipment, and their contents from espionage, theft, and destruction or damage by accident, fire, or natural disaster (e.g., floods and earthquakes)

Preventive Physical Controls

Preventive physical controls are employed to prevent unauthorized personnel from entering computing facilities (i.e., locations housing computing resources, supporting utilities, computer hard copy, and input data media) and to help protect against natural disasters. Examples of these controls include:

- **Backup files and documentation.**
- **Fences.**
- **Security guards.**
- **Badge systems.**
- **Double door systems.**
- **Locks and keys.**
- **Backup power.**
- **Biometric access controls.**
- **Site selection.**
- **Fire extinguishers.**

Backup Files and Documentation

Should an accident or intruder destroy active data files or documentation, it is essential that backup copies be readily available. Backup files should be stored far enough away from the active data or documentation to avoid destruction by the same incident that destroyed the original. Backup material should be stored in a secure location constructed of noncombustible materials, including two-hour-rated fire walls. Backups of sensitive information should have the same level of protection as the active files of this information; it is senseless to provide tight security for data on the system but lax security for the same data in a backup location.

Fences

Although fences around the perimeter of the building do not provide much protection against a determined intruder, they do establish a formal no trespassing line and can dissuade the simply curious person. Fences should have alarms or should be under continuous surveillance by guards, dogs, or TV monitors.

Security Guards

Security guards are often stationed at the entrances of facilities to intercept intruders and ensure that only authorized persons are allowed to enter. Guards are effective in inspecting packages or other hand-carried items to ensure that only authorized, properly described articles are taken into or out of the facility. The effectiveness of stationary guards can be greatly enhanced if the building is wired with appropriate electronic detectors with alarms or other warning indicators terminating at the guard station.

Badge Systems

Physical access to computing areas can be effectively controlled using a badge system. With this method of control, employees and visitors must wear appropriate badges whenever they are in access-controlled areas. Badge-reading systems programmed to allow entrance only to authorized persons can then easily identify intruders.

Double Door Systems

Double door systems can be used at entrances to restricted areas (e.g., computing facilities) to force people to identify themselves to the guard before they can be released into the secured area. Double doors are an excellent way to prevent intruders from following closely behind authorized persons and slipping into restricted areas.

Locks and Keys

Locks and keys are commonly used for controlling access to restricted areas. Because it is difficult to control copying of keys, many installations use cipher locks (i.e., combination locks containing buttons that open the lock when pushed in the proper sequence). With cipher locks, care must be taken to conceal which buttons are being pushed to avoid a compromise of the combination.

Backup Power

Backup power is necessary to ensure that computer services are in a constant state of readiness and to help avoid damage to equipment if normal power is lost. For short periods of power loss, backup power is usually provided by batteries. In areas susceptible to outages of more than 15–30 min., diesel generators are usually recommended.

Biometric Access Controls

Biometric identification is a more sophisticated method of controlling access to computing facilities than badge readers, but the two methods operate in much the same way. Biometrics used for identification includes fingerprints, handprints, voice patterns, signature samples, and retinal scans. Because biometrics cannot be lost, stolen, or shared, they provide a higher level of security than badges. Biometric identification is recommended for high-security, low-traffic entrance control.

Site Selection

The site for the building that houses the computing facilities should be carefully chosen to avoid obvious risks. For example, wooded areas can pose a fire hazard, areas on or adjacent to an earthquake fault can be dangerous and sites located in a flood plain are susceptible to water damage. In addition, locations under an aircraft approach or departure route are risky, and locations adjacent to railroad tracks can be susceptible to vibrations that can precipitate equipment problems.

Fire Extinguishers

The control of fire is important to prevent an emergency from turning into a disaster that seriously interrupts data processing. Computing facilities should be located far from potential fire sources (e.g., kitchens or cafeterias) and should be constructed of noncombustible materials. Furnishings should also be noncombustible. It is important that appropriate types of fire extinguishers be conveniently located for easy access. Employees must be trained in the proper use of fire extinguishers and in the procedures to follow should a fire break out. Automatic sprinklers are essential in computer rooms and surrounding spaces and when expensive equipment is located on raised floors. Sprinklers are usually specified by insurance companies for the protection of any computer room that contains combustible materials.

However, the risk of water damage to computing equipment is often greater than the risk of fire damage. Therefore, carbon dioxide extinguishing systems were developed; these systems flood an area threatened by fire with carbon dioxide, which suppresses fire by removing oxygen from the air. Although carbon dioxide does not cause water damage, it is potentially lethal to people in the area and is now used only in unattended areas.

Detective Physical Controls

Detective physical controls warn protective services personnel that physical security measures are being violated. Examples of these controls include:

- Motion detectors.
- Smoke and fire detectors.
- Closed-circuit television monitors.
- Sensors and alarms.

Motion Detectors

In computing facilities that usually do not have people in them, motion detectors are useful for calling attention to potential intrusions. Motion detectors must be constantly monitored by guards.

Fire and Smoke Detectors

Fire and smoke detectors should be strategically located to provide early warning of a fire. All fire detection equipment should be tested periodically to ensure that it is in working condition.

Closed-Circuit Television Monitors

Closed-circuit televisions can be used to monitor the activities in computing areas where users or operators are frequently absent. This method helps detect individuals behaving suspiciously.

Sensors and Alarms

Sensors and alarms monitor the environment surrounding the equipment to ensure that air and cooling water temperatures remain within the levels specified by equipment design. If proper conditions are not maintained, the alarms summon operations and maintenance personnel to correct the situation before a business interruption occurs.

Technical Controls

Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.

Preventive Technical Controls

Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:

- **Access control software**
- **Antivirus software**
- **Passwords**
- **Smart cards**
- **Encryption**
- **Dial-up access control and callback systems**

Access Control Software

The purpose of access control software is to control sharing of data and programs between users. In many computer systems, access to data and programs is implemented by access control lists that designate which users are allowed access. Access control software provides the ability to control access to the system by establishing that only registered users with an authorized log-on ID and password can gain access to the computer system.

Antivirus Software

Viruses have reached epidemic proportions throughout the micro-computing world and can cause processing disruptions and loss of data as well as significant loss of productivity while cleanup is conducted. In addition, new viruses are emerging at an ever-increasing rate — currently about one every 48 hours. It is recommended that antivirus software be installed on all microcomputers to detect, identify, isolate, and eradicate viruses. This software must be updated frequently to help fight new viruses. In addition, to help ensure that viruses are intercepted as early as possible, antivirus software should be kept active on a system, not used intermittently at the discretion of users.

Passwords

Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system. Fixed passwords that are used for a defined period of time are often easy for hackers to compromise; therefore, great care must be exercised to ensure that these passwords do not appear in any dictionary. Fixed passwords are often used to control access to specific data bases. In this use, however, all persons who have authorized access to the data base use the same password; therefore, no accountability can be achieved.

Currently, dynamic or one-time passwords, which are different for each log-on, are preferred over fixed passwords. Dynamic passwords are created by a token that is programmed to generate passwords randomly.

Smart Cards

Smart cards are usually about the size of a credit card and contain a chip with logic functions and information that can be read at a remote terminal to identify a specific user's privileges. Smart cards now carry prerecorded, usually encrypted access control information that is compared with data that the user provides (e.g., a personal ID number or biometric data) to verify authorization to access the computer or network.

Encryption

Encryption is defined as the transformation of plaintext (i.e., readable data) into cipher text (i.e., unreadable data) by cryptographic techniques. Encryption is currently considered to be the only sure way of protecting data from disclosure during network transmissions. Encryption can be implemented with either hardware or software. Software-based encryption is the least expensive method and is suitable for applications involving low-volume transmissions; the use of software for large volumes of data results in an unacceptable increase in processing costs. Because there is no overhead associated with hardware encryption, this method is preferred when large volumes of data are involved.

Dial-Up Access Control and Callback Systems

Dial-up access to a computer system increases the risk of intrusion by hackers. In networks that contain personal computers or are connected to other networks, it is difficult to determine whether dial-up access is available or not because of the ease with which a modem can be added to a personal computer to turn it into a dial-up access point. Known dial-up access points should be controlled so that only authorized dial-up users can get through. Currently, the best dial-up access controls use a microcomputer to intercept calls, verify the identity of the caller (using a dynamic password mechanism), and switch the user to authorized computing resources as requested. Previously, call-back systems intercepted dial-up callers, verified their authorization and called them back at their registered number, which at first proved effective; however, sophisticated hackers have learned how to defeat this control using call-forwarding techniques.

Detective Technical Controls

Detective technical controls warn personnel of violations or attempted violations of preventive technical controls. Examples of these include audit trails and intrusion detection expert systems, which are discussed in the following sections.

Audit Trails

An audit trail is a record of system activities that enables the reconstruction and examination of the sequence of events of a transaction, from its inception to output of final results. Violation reports present significant, security-oriented events that may indicate either actual or attempted policy transgressions reflected in the audit trail. Violation reports should be frequently and regularly reviewed by security officers and data base owners to identify and investigate successful or unsuccessful unauthorized accesses.

Intrusion Detection Systems

These expert systems track users (on the basis of their personal profiles) while they are using the system to determine whether their current activities are consistent with an established norm. If not, the user's session can be terminated or a security officer can be called to investigate. Intrusion detection can be especially effective in cases in which intruders are pretending to be authorized users or when authorized users are involved in unauthorized activities.

Administrative Controls

Administrative, or personnel, security consists of management constraints, operational procedures, accountability procedures, and supplemental administrative controls established to provide an acceptable level of protection for computing resources. In addition, administrative controls include procedures established to ensure that all personnel who have access to computing resources have the required authorizations and appropriate security clearances.

Preventive Administrative Controls

Preventive administrative controls are personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of computing data and programs. Examples of preventive administrative controls include:

- Security awareness and technical training.
- Separation of duties.
- Procedures for recruiting and terminating employees.
- Security policies and procedures.
- Supervision.
- Disaster recovery, contingency, and emergency plans.
- User registration for computer access.

Security Awareness and Technical Training

Security awareness training is a preventive measure that helps users to understand the benefits of security practices. If employees do not understand the need for the controls being imposed, they may eventually circumvent them and thereby weaken the security program or render it ineffective. Technical training in the form of emergency and fire drills for operations personnel can ensure that proper action will be taken to prevent such events from escalating into disasters.

Separation of Duties

This administrative control separates a process into component parts, with different users responsible for different parts of the process. Judicious separation of duties prevents one individual from obtaining control of an entire process and forces collusion with others in order to manipulate the process for personal gain.

Recruitment and Termination Procedures

Appropriate recruitment procedures can prevent the hiring of people who are likely to violate security policies. A thorough background investigation should be conducted, including checking on the applicant's criminal history and references. Although this does not necessarily screen individuals for honesty and integrity, it can help identify areas that should be investigated further.

Three types of references should be obtained: (1) employment, (2) character, and (3) credit. Employment references can help estimate an individual's competence to perform, or be trained to perform, the tasks required on the job. Character references can help determine such qualities as trustworthiness, reliability, and ability to get along with others. Credit references can indicate a person's financial habits, which in turn can be an indication of maturity and willingness to assume responsibility for one's own actions.

In addition, certain procedures should be followed when any employee leaves the company, regardless of the conditions of termination. Any employee being involuntarily terminated should be asked to leave the premises immediately upon notification, to prevent further access to computing resources. Voluntary terminations may be handled differently, depending on the judgment of the employee's supervisors, to enable the employee to complete work in process or train a replacement.

All authorizations that have been granted to an employee should be revoked upon departure. If the departing employee has the authority to grant authorizations to others, these other authorizations should also be reviewed. All keys, badges, and other devices used to gain access to premises, information, or equipment should be retrieved from the departing employee. The combinations of all locks known to a departing employee should be changed immediately. In addition, the employee's log-on IDs and passwords should be canceled, and the related active and backup files should be either deleted or reassigned to a replacement employee.

Any special conditions to the termination (e.g., denial of the right to use certain information) should be reviewed with the departing employee; in addition, a document stating these conditions should be signed by the employee. All terminations should be routed through the computer security representative for the facility where the terminated employee works to ensure that all information system access authority has been revoked.

Security Policies and Procedures

Appropriate policies and procedures are key to the establishment of an effective information security program. Policies and procedures should reflect the general policies of the organization as regards the protection of information and computing resources. Policies should cover the use of computing resources, marking of sensitive information, movement of computing resources outside the facility, introduction of personal computing equipment and media into the facility, disposal of sensitive waste, and computer and data security incident reporting. Enforcement of these policies is essential to their effectiveness.

Supervision

Often, an alert supervisor is the first person to notice a change in an employee's attitude. Early signs of job dissatisfaction or personal distress should prompt supervisors to consider subtly moving the employee out of a critical or sensitive position.

Supervisors must be thoroughly familiar with the policies and procedures related to the responsibilities of their department. Supervisors should require that their staff members comply with pertinent policies and procedures and should observe the effectiveness of these guidelines. If the objectives of the policies and procedures can be accomplished more effectively, the supervisor should recommend appropriate improvements. Job assignments should be reviewed regularly to ensure that an appropriate separation of duties is maintained, that employees in sensitive positions are occasionally removed from a complete processing cycle without prior announcement, and that critical or sensitive jobs are rotated periodically among qualified personnel.

Disaster Recovery, Contingency, and Emergency Plans

The disaster recovery plan is a document containing procedures for emergency response, extended backup operations, and recovery should a computer installation experience a partial or total loss of computing resources or physical facilities (or of access to such facilities). The primary objective of this plan, used in conjunction with the contingency plans, is to provide reasonable assurance that a computing installation can recover from disasters, continue to process critical applications in a degraded mode, and return to a normal mode of operation within a reasonable time. A key part of disaster recovery planning is to provide for processing at an alternative site during the time that the original facility is unavailable.

Contingency and emergency plans establish recovery procedures that address specific threats. These plans help prevent minor incidents from escalating into disasters. For example, a contingency plan might provide a set of procedures that defines the condition and response required to return a computing capability to nominal operation; an emergency plan might be a specific procedure for shutting down equipment in the event of a fire or for evacuating a facility in the event of an earthquake.

User Registration for Computer Access

Formal user registration ensures that all users are properly authorized for system and service access. In addition, it provides the opportunity to acquaint users with their responsibilities for the security of computing resources and to obtain their agreement to comply with related policies and procedures.

Detective Administrative Controls

Detective administrative controls are used to determine how well security policies and procedures are complied with, to detect fraud, and to avoid employing persons that represent an unacceptable security risk. This type of control includes:

- Security reviews and audits.
- Performance evaluations.
- Required vacations.
- Background investigations.
- Rotation of duties.

Security Reviews and Audits

Reviews and audits can identify instances in which policies and procedures are not being followed satisfactorily. Management involvement in correcting deficiencies can be a significant factor in obtaining user support for the computer security program.

Performance Evaluations

Regularly conducted performance evaluations are an important element in encouraging quality performance. In addition, they can be an effective forum for reinforcing management's support of information security principles.

Required Vacations

Tense employees are more likely to have accidents or make errors and omissions while performing their duties. Vacations contribute to the health of employees by relieving the tensions and anxieties that typically develop from long periods of work. In addition, if all employees in critical or sensitive positions are forced to take vacations, there will be less opportunity for an employee to set up a fraudulent scheme that depends on the employee's presence (e.g., to maintain the fraud's continuity or secrecy). Even if the employee's presence is not necessary to the scheme, required vacations can be a deterrent to embezzlement because the employee may fear discovery during his or her absence.

Background Investigations

Background investigations may disclose past performances that might indicate the potential risks of future performance. Background investigations should be conducted on all employees being considered for promotion or transfer into a position of trust; such investigations should be completed before the employee is actually placed in a sensitive position. Job applicants being considered for sensitive positions should also be investigated for potential problems. Companies involved in government-classified projects should conduct these investigations while obtaining the required security clearance for the employee.

Rotation of Duties

Like required vacations, rotation of duties (i.e., moving employees from one job to another at random intervals) helps deter fraud. An additional benefit is that as a result of rotating duties, employees are cross-trained to perform each other's functions in case of illness, vacation, or termination.

Biometrics

"Biometrics is the automated identification, or verification of human identity through the measurement of repeatable physiological, or behavioral characteristics".

"Biometrics is the development of statistical and mathematical methods applicable to data analysis problems in the biological sciences."

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). For our use, biometrics refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics, such as fingerprints, irises, voice patterns, facial patterns, and hand measurements, for identification and verification purposes.

Biometrics comprises methods for uniquely recognizing humans based upon one or more physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. Biometric characteristics can be divided in two main classes

Physiological are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, which has largely replaced retina, etc.

Behavioral are related to the behavior of a person. Examples include, but are not limited to typing rhythm, and voice. Some researchers have coined the term **behaviometrics** for this class of biometrics. A biometric system can operate in the following two modes:

1. **Verification** – A one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be. Can be done in conjunction with a smart card, username or ID number. **Verification** refers to the 'one to one' comparison between a sample and another to ask the question, 'are you who you say you are.' The majority of access control applications utilize verification techniques, rather than attempting searches of databases, which could compromise accuracy and raise costs.
2. **Identification** – A one to many comparison of the captured biometric against a biometric database in attempt to identify an unknown individual. The identification only succeeds in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. In general terms **identification** means the search of a biometric sample against a database of other samples in order to ascertain whether the donor is already contained in, or new to the database

The first time an individual uses a biometric system is called an *enrollment*. During the enrollment, biometric information from an individual is stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Such systems themselves be secure if the biometric system is to be robust.

The **first block** (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an **image acquisition system**, but it can change according to the characteristics desired.

The **second block** performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc.

In the **third block** necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a *template*. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the filesize and to protect the identity of the enrollee

If enrollment is being performed, the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area).

Working Principle of Biometrics

Biometric devices consist of a reader or scanning device, software that converts the gathered information into digital form, and a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data in the database. All Biometric authentications require comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login)

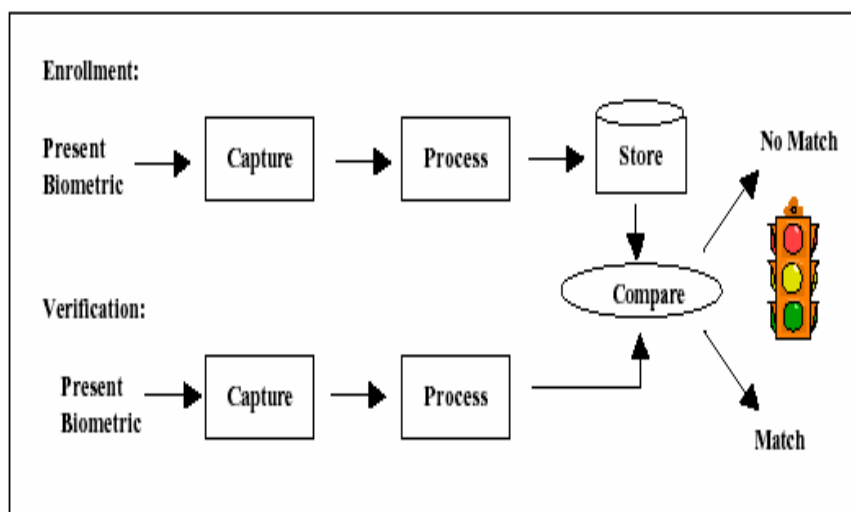


Figure 1 Enrollment and Verification Technique

During **Enrollment**, as shown in the picture above, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison. Biometric recognition can be used in **Identification** mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching.

A system can also be used in **Verification** mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple glance at a camera is enough to authenticate the user.

Issues and concerns

Privacy and discrimination Data obtained during biometric enrollment could be used in ways the enrolled individual does not consent to.

Danger to owners of secured items When thieves cannot get access to secure properties, there is a chance that the thieves will destroy the means of biometrics object of the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. For example, in 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car.

Cancelable biometrics One advantage of passwords over biometrics is that they can be re-issued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone's face is compromised from a database, they cannot cancel or reissue it. Cancelable biometrics is a way in which to incorporate protection and the replacement features into biometrics. **Governments are unlikely to disclose full capabilities of biometric deployments**

Certain members of the civilian community are worried about how biometric data is used. Unfortunately, full disclosure may not be forth coming to the civilian community. To quote the Report of the (United States) Defense Science Board Task Force on Defense Biometric.

Indian Scenario

India is undertaking an ambitious mega project (the Multipurpose National Identity Card) to provide a unique identification number to each of its 1.25 billion people. The Identification number will be stored in central databases. Consisting the biometric information of the individual. If implemented, this would be the biggest implementation of the Biometrics in the world. India's Home Minister, P Chidambaram, described the process as "the biggest exercise... since humankind came into existence". The government will then use the information to issue identity cards. Officials in India will spend one year classifying India's population according to demographics indicators. The physical count will begin on February 2011

Key Issues Factors for Selection of a Biometrics System

1. Accuracy
2. Throughput Rate
3. Acceptability by Users
4. Uniqueness of Biometrics Organ and Action
5. Reliability of Biometrics
6. Data Storage Requirements
7. Enrollment Time
8. Data collection and interoperability
9. Requirement about Subject and System Contacts
10. Medical , legal and social issues

There are following types of biometric system each has its on advantage and disadvantage.

1. Fingerprint Biometrics

The tip of the finger is a small area from which to take measurements, and ridge patterns can be affected by cuts, dirt, or even wear and tear. Acquiring high-quality images of distinctive fingerprint ridges and minutiae is complicated task. People with no or few minutia points (surgeons as they often wash their hands with strong detergents, builders, people with special skin conditions) cannot enroll or use the system. Results can also be confused by false minutia points due to low-quality enrollment, imaging, or fingerprint ridge detail.

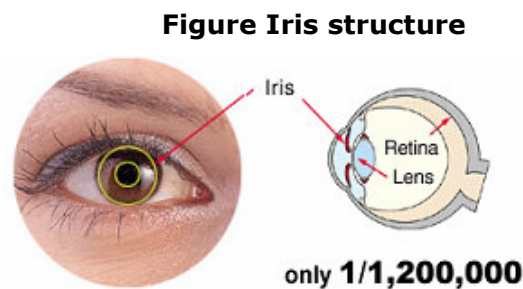
There is some controversy over the uniqueness of fingerprints. The quality of partial prints is however the limiting factor. **As the number of defining points of the fingerprint becomes smaller, the degree of certainty of identity declines.** There have been a few well-documented cases of people being wrongly accused on the basis of partial fingerprints.

Benefits of fingerprint biometric systems

- Easy to use
- Cheap
- Small size
- Low power
- Non-intrusive

2. Iris Biometrics

Iris is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupils. The iris of the eye has a unique pattern, from eye to eye and person to person. An iris scan will analyze over 200 points of the iris, such as rings, furrows, freckles, the corona and will compare it to a previously recorded template. Glasses, contact lenses, and even eye surgery does not change the characteristics of the iris. To prevent an image / photo of the iris from being used instead of a real "live" eye, iris scanning systems will vary the light and check that the pupil dilates or contracts.



Benefits of Iris Biometrics

- **Highly accurate:** There is no known case of a false acceptance for iris recognition
- **Not intrusive and hygienic** - no physical contact required

3. Retina Biometrics

The blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person. Retina scans require that the person removes their glasses, place their eye close to the scanner, stare at a specific point, and remain still, and focus on a specified location for approximately 10 to 15 seconds while the scan is completed. A retinal scan involves the use of a low-intensity coherent light source, which is projected onto the retina to illuminate the blood vessels which are then photographed and analyzed. A coupler is used to read the blood vessel patterns. A retina scan cannot be faked as it is currently impossible to forge a human retina. A retinal scan has an error rate of 1 in 10,000,000, compared to fingerprint identification error being sometimes as high as 1 in 500.

Benefits of retina biometric systems

- Highly accurate

Weaknesses of retina biometric systems

- The user must hold still while the scan is taking place
- Enrollment and scanning are intrusive and slow.

4. Face Recognition Biometrics

Biometric facial recognition systems will measure and analyze the overall structure, shape and proportions of the face: Distance between the eyes, nose, mouth, and jaw edges; upper outlines of the eye sockets, the sides of the mouth, the location of the nose and eyes, the area surrounding the cheekbones. At enrolment, several pictures are taken of the user's face, with slightly different angles and facial expressions, to allow for more accurate matching. For verification and identification, the user stands in front of the camera for a few seconds, and the scan is compared with the template previously recorded. To prevent an image / photo of the face or a mask from being used, face biometric systems will require the user to smile, blink, or nod their head. Also, facial thermography can be used to record the heat of the face (which won't be affected by a mask).

Benefits of face biometric systems

It can be done from a distance, even without the user being aware of it (for instance when scanning the entrance to a bank or a high security area).

Weaknesses of face biometric systems

Face biometric systems are more suited for authentication in comparison to identification purposes, as it is easy to change the proportion of one's face by wearing a mask, a nose extension, etc. User perceptions / civil liberty: Most people are uncomfortable with having their picture taken.

5. Voice biometrics

Our voices are unique to each person (including twins), and cannot be exactly replicated. Speech includes two components: a physiological component (the voice tract) and a behavioral component (the accent). It is almost impossible to **imitate** anyone's voice perfectly. Voice recognition systems can discriminate between two very similar voices, including twins. The voiceprint generated upon enrolment is characterized by the vocal tract, which is a unique physiological trait. During enrollment, the user is prompted to repeat a short passphrase or a sequence of numbers. Voice recognition can utilize various audio capture device (microphones, telephones and PC microphones). The performance of voice recognition systems may vary depending on the quality of the audio signal. To prevent the risk of unauthorized access via tape recordings, the user is asked to repeat random phrases.

Benefits of voice biometric systems

- Ability to use existing telephones
- Can be automated, and coupled with speech recognition systems
- Low perceived invasiveness

Weaknesses of voice biometric systems:

Possibility of High false and non-matching rates for authentic user

6. DNA biometrics

Humans have 23 pairs of chromosomes containing their DNA blueprint. One member of each chromosomal pair comes from their mother, the other comes from their father. Every cell in a human body contains a copy of this DNA. The large majority of DNA does not differ from person to person, but 0.10 percent of a person's entire genome would be unique to each individual. This represents 3 million base pairs of DNA.

Genes make up 5 percent of the human genome. **The other 95 percent are non-coding sequences, (which used to be called junk DNA).** In non-coding regions there are identical repeat sequences of DNA, which can be repeated anywhere from one to 30 times in a row. These regions are called variable number tandem repeats (VNTRs). For any given VNTR loci in an individual's DNA, there will be a certain number of repeats. The higher number of loci are analyzed, the smaller the probability to find two unrelated individuals with the same DNA profile.

The main steps to create a DNA profile are: isolate the DNA (from a sample such as blood, saliva, hair, or tissue).

- Cut the DNA up into shorter fragments containing known VNTR areas.
- Sort the DNA fragments by size, and compare the DNA fragments in different samples.

Benefits of DNA biometric systems

Accurate: the chance of 2 individuals sharing the same DNA profile is less than one in a hundred billion with 26 different bands studied.

Weaknesses of DNA biometric systems

A physical sample must be taken, while other biometric systems only use an image or a recording

-
-
-
-
-
-
-
-

ISO 27001

The ISO 27001 standard was published in October 2005, essentially replacing the old BS7799-2 standard. It is the specification for ISMS, an Information Security Management System. BS7799 itself was a long standing standard, first published in the nineties as a code of practice. As this matured, a second part emerged to cover management systems. It is this against which certification is granted. Today in excess of a thousand certificates are in place, across the world. ISO 27001 enhanced the content of BS7799-2 and harmonized it with other standards. A scheme has been introduced by various certification bodies for conversion from BS7799 certification to ISO27001 certification.

The objective of the standard itself is to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System". Regarding its adoption, this should be a strategic decision. Further, "The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the process employed and the size and structure of the organization". The standard defines its 'process approach' as "The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management".

Information Security Management System

ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard.

Most organizations have a number of information security controls. Without an ISMS however, the controls tend to be somewhat disorganized and disjointed, having been implemented often as point solutions to specific situations or simply as a matter of convention. Maturity models typically refer to this stage as "ad hoc". The security controls in operation typically address certain aspects of IT or data security, specifically, leaving non-IT information assets (such as paperwork and proprietary knowledge) less well protected on the whole. Business continuity planning and physical security, for examples, may be managed quite independently of IT or information security while Human Resources practices may make little reference to the need to define and assign information security roles and responsibilities throughout the organization.

ISO/IEC 27001 requires that management:

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities and impacts;
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and

- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

While other sets of information security controls may potentially be used within an ISO/IEC 27001 ISMS as well as, or even instead of, ISO/IEC 27002 (the Code of Practice for Information Security Management), these two standards are normally used together in practice. Annex A to ISO/IEC 27001 succinctly lists the information security controls from ISO/IEC 27002, while ISO/IEC 27002 provides additional information and implementation advice on the controls.

Organizations that implement a suite of information security controls in accordance with ISO/IEC 27002 are simultaneously likely to meet many of the requirements of ISO/IEC 27001, but may lack some of the overarching management system elements. The converse is also true, in other words, an ISO/IEC 27001 compliance certificate provides assurance that the management system for information security is in place, but says little about the absolute state of information security within the organization. Technical security controls such as antivirus and firewalls are not normally audited in ISO/IEC 27001 certification audits: the organization is essentially *presumed* to have adopted all necessary information security controls since the overall ISMS is in place and is deemed adequate by satisfying the requirements of ISO/IEC 27001. Furthermore, management determines the scope of the ISMS for certification purposes and may limit it to, say, a single business unit or location. The ISO/IEC 27001 certificate does not necessarily mean the remainder of the organization, outside the scoped area, has an adequate approach to information security management.

ISMS Certificate

ISMS may be certified compliant with ISO/IEC 27001 by a number of Accredited Registrars worldwide. Certification against any of the recognized national variants of ISO/IEC 27001 (e.g. JIS Q 27001, the Japanese version) by an accredited certification body is functionally equivalent to certification against ISO/IEC 27001 itself. In some countries, the bodies that verify conformity of management systems to specified standards are called "certification bodies", in others they are commonly referred to as "registration bodies", "assessment and registration bodies", "certification/ registration bodies", and sometimes "registrars".

The ISO/IEC 27001 certification, like other ISO management system certifications, usually involves a three-stage audit process:

- **Stage 1** is a preliminary, informal review of the ISMS, for example checking the existence and completeness of key documentation such as the organization's information security policy, Statement of Applicability (SoA) and Risk Treatment Plan (RTP). This stage serves to familiarize the auditors with the organization and vice versa.
- **Stage 2** is a more detailed and formal compliance audit, independently testing the ISMS against the requirements specified in ISO/IEC 27001. The auditors will seek evidence to confirm that the management system has been properly designed and implemented, and is in fact in operation (for example by confirming that a security committee or similar management body meets

regularly to oversee the ISMS). Certification audits are usually conducted by ISO/IEC 27001 Lead Auditors. Passing this stage results in the ISMS being certified compliant with ISO/IEC 27001.

- **Stage 3** involves follow-up reviews or audits to confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic re-assessment audits to confirm that the ISMS continues to operate as specified and intended. These should happen at least annually but (by agreement with management) are often conducted more frequently, particularly while the ISMS are still maturing.

The ISO/IEC 27000-series standards provide good practice guidance on designing, implementing and auditing Information Security Management Systems to protect the confidentiality, integrity and availability of the information on which we all depend. There are Ten ISO27k standards are published so far:

- ISO/IEC 27000 overview & vocabulary
- ISO/IEC 27001 formal ISMS specification
- ISO/IEC 27002 infosec controls guide
- ISO/IEC 27003 implementation guide
- ISO/IEC 27004 infosec metrics
- ISO/IEC 27005 infosec risk management
- ISO/IEC 27006 ISMS certification guide
- ISO/IEC 27011 ISO27k for telecomms
- ISO/IEC 27033-1 network security
- ISO 27799 ISO27k for healthcare

Systems Security Engineering Capability Maturity Model (SSE-CMM)

The Systems Security Engineering Capability Maturity Model (SSE-CMM) describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The SSE-CMM does not prescribe a particular process or sequence, but captures practices generally observed in industry. The model is a standard metric for security engineering practices covering:

1. **The entire life cycle**, including development, operation, maintenance, and decommissioning activities:
2. **The whole organization**, including management, organizational, and engineering activities:
3. **Concurrent interactions with other disciplines**, such as system, software, hardware, human factors, and test engineering; system management, operation, and maintenance:
4. **Interactions with other organizations**, including acquisition, system management, certification, accreditation, and evaluation.

The SSE-CMM Model Description provides an overall description of the principles and architecture upon which the SSE-CMM is based, an executive overview of the model, suggestions for appropriate use of the model, the practices included in the model, and a description of the attributes of the model. It also includes the requirements used to develop the model. The SSE-CMM Appraisal Method describes the process and tools for evaluating an organization's security engineering capability against the SSE-CMM.

The SSE-CMM was developed to advance security engineering as a defined, mature, and measurable discipline. It describes the characteristics essential to the success of an organization's security engineering process, and is applicable to all security engineering organizations including government, commercial and academic. Its acceptance as ISO/IEC 21827 makes it the first formal standard of this scale dedicated to security engineering practices. The SSE-CMM establishes a framework for measuring and improving performance in the application of security engineering principles. It is a tool for engineering organizations to evaluate their security engineering practices and define improvements to them.

The SSE-CMM describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. There are following features of SSE-CMM model:

- Tool for engineering organizations to evaluate security engineering practices and define improvements to them.
- Standard mechanism for customers to evaluate a provider's security engineering capability.
- Basis for security engineering evaluation organization (e.g., system certifiers and product evaluators) to establish organization capability-based confidences (as an ingredient to system or project security assurance).
- The SSE-CMM addresses security engineering activities that span the entire trusted product or secure system life cycle, including concept definition, requirements analysis, design, development, integration, installation, operations, maintenance, and decommissioning.

- The SSE-CMM applies secure product developers, secure system developers and integrators, and organizations that provide security services and security engineering.
- The SSE-CMM applies to all types and sizes of security engineering organizations, such a commercial, government, and academic.

Appraisals

The SSE-CMM is structured to support a wide variety of improvement activities, including self-administered appraisals, or internal appraisals augmented by expert "facilitators" from inside or outside the organization. Although it is primarily intended for internal process improvement, the SSE-CMM can also be used to evaluate a potential vendor's capability to perform its security engineering process.

Guidance for SSE-CMM Appraisal Services

The SSO is currently developing an Appraiser Certification Program based on recommendations made previously by the SSE-CMM Project to ensure that these services are provided in a qualified and highly professional manner. The following qualifications were defined: The SSE-CMM appraisal team should include no more than one member who has not previously participated on a prior CMM appraisal. Each member of the appraisal team should fully meet at least one of the following criteria and collectively the appraisal team should meet al of the criteria:

- Active membership in an SSE-CMM Project Working Group
- 10 years security engineering experience
- 2 years process improvement experience
- Training or experience in some form of CMM appraisal, preferably SSE-CMM

SSE-CMM appraisal team facilitators should meet most of the above criteria, and ideally should have facilitated a previous SSE-CMM appraisal.

Security Metrics

At a high-level, metrics are quantifiable measurements of some aspect of a system or enterprise. For an entity (system, product, or other) for which security is a meaningful concept, there are some identifiable attributes that collectively characterize the security of that entity. Further, a security metric (or combination of security metrics) is a quantitative measure of how much of that attribute the entity possesses. A security metric can be built from lower-level physical measures. Security metrics focus on the actions (and results of those actions) that organizations take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defenses are breached. They are useful to senior management, decision makers, users, administrators, or other stakeholders who face a difficult and complex set of questions regarding security, such as:

- How much money/resources should be spent on security?
- Which system components or other aspects should be targeted first?
- How can the system be effectively configured?

- How much improvement is gained by security expenditures, including improvements to security processes?
- How do we measure the improvements?
- Are we reducing our exposure?

Metrics and the SSE-CMM

With regard to the use of the SSE-CMM, the following types of metrics are being identified and studied:

Process Metrics - Specific metrics that could serve as quantitative or qualitative evidence of the level of maturity for a particular SSE-CMM process area or could serve as a binary indication of the presence or absence of a mature process.

Security Metrics - A measurable attribute of the result of an SSE-CMM security engineering process that could serve as evidence of its effectiveness. A security metric may be objective or subjective, and quantitative or qualitative.

The first type of metric provides information about the processes themselves. The second type of metric provides information on the results of those processes and what they can tell the stakeholder about how effective use of the processes has been in achieving an acceptable security outcome. These metrics categories tailor their own metrics program to measure their progress against security objectives. Accompanying guidance is also being provided.

Information security vs. Privacy