# INFORMATION SECURITY

| | L | T/P | C |
|---|---|---|---|
| **Paper Code: ETCS-401** | **L** | **T/P** | **C** |
| **Paper: Information Security** | **3** | **0** | **3** |

**INSTRUCTIONS TO PAPER SETTERS: MAXIMUM MARKS: 75**

1. Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 25 marks.

2. Apart from Question No. 1, rest of the paper shall consist of four units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be of 12.5 marks.

*Objective: To understand the basic concepts of web threats, legal ethical and professional issues of information security.*

### UNIT- I

**Information and Security:**

**Information Systems:** Recent History, Distributed Information System and its Importance, Role of Internet and Web Services, Threats and attacks, Classification of Threats and Assessing Damages Security in Mobile and Wireless Computing- Security Challenges in Mobile Devices, authentication Service Security, Security Implication for organizations, Laptops Security. Basic Principles of Information Security, Confidentiality, Integrity Availability and other terms in Information Security, Information Classification and their Roles, Privacy of Data.

**[T1, T2][No. of hrs. 12]**

### UNIT-II

**Networks and E-Security:**

**Concepts in Internet and World Wide Web:** Brief review of Internet Protocols-TCP/IP, IPV4, IPV6. **Functions of various networking components:** Routers, bridges, switches, hub, gateway and Modulation Techniques. Need for security, Legal, Ethical and Professional Issues in Information Security, Risk Management, 11 Security Threats to E-Commerce, Virtual Organization, Business Transactions on Web, E Governance and EDI, Concepts in Electronics payment systems, E Cash, Credit/Debit Cards,

**Digital forensics including digital evidence handling:** Media forensics, Cyber forensics, Software forensics, Mobile forensics.

**[T1, T2][No. of hrs. 11]**

### UNIT-III

**Physical Security and Bio-metrics as Security:**

**Physical Security:** Needs, Disaster and Controls, Basic Tenets of Physical Security and Physical Entry Controls, Access Control- Biometrics, Factors in Biometrics Systems, Benefits, Criteria for selection of biometrics, Design Issues in Biometric Systems, Interoperability Issues, Economic and Social Aspects, Legal Challenges Framework for Information Security, Security Metrics, Information Security Vs Privacy

**[T1, T2][No. of hrs. 11]**

### UNIT-IV

**Network Cryptography:**

Model of Cryptographic Systems, Issues in Documents Security, System of Keys, Public Key Cryptography, Digital Signature, Requirement of Digital Signature System, Finger Prints, Firewalls, Design and Implementation Issues,

**Policies Network Security:** Basic Concepts, Dimensions, Perimeter for Network Protection, Network Attacks, Need of Intrusion Monitoring and Detection, Intrusion Detection Virtual Private Networks- Need, Use of Tunnelling with VPN, Authentication Mechanisms, Types of VPNs and their Usage, Security Concerns in VPN

**[T1, T2][No. of hrs. 10]**

**Text Books:**

[T1] Godbole," Information Systems Security", Wiley
[T2] Merkov, Breithaupt," Information Security", Pearson Education

**References:**

[R1] Yadav, "Foundations of Information Technology", New Age, Delhi
[R2] Schou, Shoemaker, “Information Assurance for the Enterprise", Tata McGraw Hill
[R3] Furnell, "Computer Insecurity", Springer
[R4] http://www.iiitd.edu.in/~gauravg/

# Unit I

# Information and Security

## Information Systems

Information system, an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products. Business firms and other organizations rely on information systems to carry out and manage their operations, interact with their customers and suppliers, and compete in the marketplace. Information systems are used to run interorganizational supply chains and electronic markets. For instance, corporations use information systems to process financial accounts, to manage their human resources, and to reach their potential customers with online promotions. Many major companies are built entirely around information systems. These include eBay, a largely auction marketplace; Amazon, an expanding electronic mall and provider of cloud computing services; Alibaba, a business-to-business e-marketplace; and Google, a search engine company that derives most of its revenue from keyword advertising on Internet searches. Governments deploy information systems to provide services cost-effectively to citizens. Digital goods—such as electronic books, video products, and software—and online services, such as gaming and social networking, are delivered with information systems. Individuals rely on information systems, generally Internet-based, for conducting much of their personal lives: for socializing, study, shopping, banking, and entertainment. As major new technologies for recording and processing information were invented over the millennia, new capabilities appeared, and people became empowered.

### Components of Information Systems

The main components of information systems are computer hardware and software, telecommunications, databases and data warehouses, human resources, and procedures. The hardware, software, and telecommunications constitute information technology (IT), which is now ingrained in the operations and management of organizations.

1. Computer hardware

Today throughout the world even the smallest firms, as well as many households, own or lease computers. Individuals may own multiple computers in the form of smartphones, tablets, and other wearable devices. Large organizations typically employ distributed computer systems, from powerful parallel-processing servers located in data centres to widely dispersed personal computers and mobile devices, integrated into the organizational information systems. Sensors are becoming ever more widely distributed throughout the physical and biological environment to gather data and, in many cases, to effect control via devices known as actuators. Together with the peripheral equipment—such as magnetic or solid-state storage disks, input-output devices, and telecommunications gear—these constitute the hardware of information systems. The cost of hardware has steadily and rapidly decreased, while processing speed and storage capacity have increased vastly. This development has been occurring under Moore's law: the power of the microprocessors at the heart of computing devices has been doubling approximately every 18 to 24 months. However, hardware's use of electric power and its environmental impact are concerns being addressed by designers. Increasingly, computer and storage services are delivered from the cloud—from shared facilities accessed over telecommunications networks.

2. Computer software

Computer software falls into two broad classes: system software and application software. The principal system software is the operating system. It manages the hardware, data and program files, and other system resources and provides means for the user to control the computer, generally via a graphical user interface (GUI). Application software is programs designed to handle specific tasks for users. Smartphone apps became a common way for individuals to access information systems. Other examples include general-purpose application suites with their spreadsheet and word-processing programs, as well as "vertical" applications that serve a specific industry segment—for instance, an application that schedules, routes, and tracks package deliveries for an overnight carrier. Larger firms use licensed applications developed and maintained by specialized software companies, customizing them to meet their specific needs, and develop other applications in-house or on an outsourced basis. Companies may also use applications delivered as software-as-a-service (SaaS) from the cloud over the Web. Proprietary software, available from and supported by its vendors, is being challenged by open-source software available on the Web for free use and modification under a license that protects its future availability.

3. Telecommunications

Telecommunications are used to connect, or network, computer systems and portable and wearable devices and to transmit information. Connections are established via wired or wireless media. Wired technologies include coaxial cable and fiber optics. Wireless technologies, predominantly based on the transmission of microwaves and radio waves, support mobile computing. Pervasive information systems have arisen with the computing devices embedded in many different physical objects. For example, sensors such as radio frequency identification devices (RFIDs) can be attached to products moving through the supply chain to enable the tracking of their location and the monitoring of their condition. Wireless sensor networks that are integrated into the Internet can produce massive amounts of data that can be used in seeking higher productivity or in monitoring the environment. Various computer network configurations are possible, depending on the needs of an organization. Local area networks (LANs) join computers at a particular site, such as an office building or an academic campus. Metropolitan area networks (MANs) cover a limited densely populated area and are the electronic infrastructure of "smart cities." Wide area networks (WANs) connect widely distributed data centres, frequently run by different organizations. Peer-to-peer networks, without a centralized control, enable broad sharing of content. The Internet is a network of networks, connecting billions of computers located on every continent. Through networking, users gain access to information resources, such as large databases, and to other individuals, such as coworkers, clients, friends, or people who share their professional or private interests. Internet-type services can be provided within an organization and for its exclusive use by various intranets that are accessible through a browser; for example, an intranet may be deployed as an access portal to a shared corporate document base. To connect with business partners over the Internet in a private and secure manner, extranets are established as so-called virtual private networks (VPNs) by encrypting the messages.

4. Databases and Data Warehouses

Many information systems are primarily delivery vehicles for data stored in databases. A database is a collection of interrelated data organized so that individual records or groups of records can be retrieved to satisfy various criteria. Typical examples of databases include employee records and product catalogs. Databases support the operations and management functions of an enterprise. Data warehouses contain the archival data, collected over time, that can be mined for information in order to develop and market new products, serve the existing customers better, or reach out to potential new customers. Anyone who has ever purchased something with a credit card—in person, by mail order, or over the Web—is included within such data collections. Massive collection and processing of the quantitative, or structured, data, as well as of the textual data often gathered on the Web, has developed into a broad initiative known as "big data." Many benefits can arise from decisions based on the facts reflected by big data. Examples include evidence-based medicine, economy of resources as a result of avoiding waste, and recommendations of new products (such as books or movies) based on a user's interests. Big data enables innovative business models. For example, a commercial firm collects the prices of goods by crowdsourcing (collecting from numerous independent individuals) via smartphones around the world. The aggregated data supplies early information on price movements, enabling more responsive decision making than was previously possible.

5. Human resources and procedures

Qualified people are a vital component of any information system. Technical personnel include development and operations managers, business analysts, systems analysts and designers, database administrators, programmers, computer security specialists, and computer operators. In addition, all workers in an organization must be trained to utilize the capabilities of information systems as fully as possible. Billions of people around the world are learning about information systems as they use the Web. Procedures for using, operating, and maintaining an information system are part of its documentation. For example, procedures need to be established to run a payroll program, including when to run it, who is authorized to run it, and who has access to the output. In the autonomous computing initiative, data centres are increasingly run automatically, with the procedures embedded in the software that controls those centers.

## Recent History

The invention of the printing press by Johannes Gutenberg in the mid-15th century and the invention of a mechanical calculator by Blaise Pascal in the 17th century are but two examples. These inventions led to a profound revolution in the ability to record, process, disseminate, and reach for information and knowledge. This led, in turn, to even deeper changes in individual lives, business organization, and human governance. The first large-scale mechanical information system was Herman Hollerith's census tabulator. Invented in time to process the 1890 U.S. census, Hollerith's machine represented a major step in automation, as well as an inspiration to develop computerized information systems.

One of the first computers used for such information processing was the UNIVAC I, installed at the U.S. Bureau of the Census in 1951 for administrative use and at General Electric in 1954 for commercial use. Beginning in the late 1970s, personal computers brought some of the advantages of information systems to small businesses and to individuals. Early in the same decade the Internet began its expansion as the global network of networks. In 1991 the World Wide Web, invented by Tim Berners-Lee as a means to access the interlinked information stored in the globally dispersed computers connected by the Internet, began operation and became the principal service delivered on the network. The global penetration of the Internet and the Web has enabled access to information and other resources and facilitated the forming of relationships among people and organizations on an unprecedented scale. The progress of electronic commerce over the Internet has resulted in a dramatic growth in digital interpersonal communications (via e-mail and social networks), distribution of products (software, music, e-books, and movies), and business transactions (buying, selling, and advertising on the Web). With the worldwide spread of smartphones, tablets, laptops, and other computer-based mobile devices, all of which are connected by wireless communication networks, information systems have been extended to support mobility as the natural human condition. As information systems enabled more diverse human activities, they exerted a profound influence over society. These systems quickened the pace of daily activities, enabled people to develop and maintain new and often more-rewarding relationships, affected the structure and mix of organizations, changed the type of products bought, and influenced the nature of work. Information and knowledge became vital economic resources. Yet, along with new opportunities, the dependence on information systems brought new threats. Intensive industry innovation and academic research continually develop new opportunities while aiming to contain the threats. After an installed system is handed over to its users and operations personnel, it will almost invariably be modified extensively over its useful life in a process known as system maintenance. A large system will typically be used and maintained for some 5 to 10 years or even longer. Most maintenance is to adjust the system to the organization's changing needs and to new equipment and other software, but inevitably some maintenance involves correcting design errors and exterminating software “bugs” as they are discovered.

# Distributed Information Systems and Its Importance

In light of recent technological changes and advancements, distributed systems are becoming more popular. Many top companies have created complex distributed systems to handle billions of requests and upgrade without downtime. Distributed designs may seem daunting and hard to build, but they are becoming more essential in 2021 to accommodate scaling at exponential rates. When beginning a build, it is important to leave room for a basic, high-availability, and scalable distributed system.

What is a distributed system?

At a basic level, a distributed system is a collection of computers that work together to form a single computer for the end-user. All these distributed machines have one shared state and operate concurrently. They are able to fail independently without damaging the whole system, much like micro services. These interdependent, autonomous computers are linked by a network to share information, communicate, and exchange information easily.

Distributed systems must have a shared network to connect its components, which could be connected using an IP address or even physical cables. Unlike traditional databases, which are stored on a single machine, in a distributed system, a user must be able to communicate with any machine without knowing it is only one machine. Most applications today use some form of a distributed database and must account for their homogenous or heterogeneous nature. In a homogenous distributed database, each system shares a data model and database management system and data model. Generally, these are easier to manage by adding nodes. On the other hand, heterogeneous databases make it possible to have multiple data models or varied database management systems using gateways to translate data between nodes.

Generally, there are three kinds of distributed computing systems with the following goals:

Distributed Information Systems: distribute information across different servers via multiple communication models

Distributed Pervasive Systems: use embedded computer devices (i.e. ECG monitors, sensors, mobile devices)

Distributed Computing Systems: computers in a network communicate via message passing

Decentralized vs distributed

There is quite a bit of debate on the difference between decentralized vs distributed systems. Decentralized is essentially distributed on a technical level, but usually a decentralized system is not owned by a single source.

It is harder to manage a decentralized system, as you cannot manage all the participants, unlike a distributed, single course design where one team/company owns all the nodes.

## Benefits of a distributed system

Distributed systems can be challenging to deploy and maintain, but there are many benefits to this design.

- Scaling: A distributed system allows you to scale horizontally so you can account for more traffic.
- Modular growth: There is almost no cap on how much you can scale.
- Fault tolerance: Distributed systems are more fault tolerant than a single machine.
- Cost effective: The initial cost is higher than a traditional system, but because of their scalability, they quickly become more cost effective
- Low latency: Users can have a node in multiple locations, so traffic will hit the closet node
- Efficiency: Distributed systems break complex data into smaller pieces
- Parallelism: Distributed systems can be designed for parallelism, where multiple processors divide up a complex problem into pieces

Scalability is the biggest benefit of distributed systems. Horizontal scaling means adding more servers into your pool of resources. Vertical scaling means scaling by adding more power (CPU, RAM, Storage, etc.) to your existing servers.

Horizontal-scaling is easier to scale dynamically, and vertical-scaling is limited to the capacity of a single server. Good examples of horizontal scaling are Cassandra and MongoDB. They make it easy to scale horizontally by adding more machines. An example of vertical scaling is MySQL, as you scale by switching from smaller to bigger machines.

**Design issues with distributed systems**

While there are many benefits to distributed systems, it's also important to note the design issues that can arise. We've summarized the main design considerations below.

- Failure Handling: Failure handling can be difficult with distributed systems because some components fail while others continue to function. This can often serve as an advantage to prevent large-scale failures, but it also lead to more complexity when it comes to troubleshooting and debugging.
- Concurrency: A common issue occurs when several clients attempt to access a shared resource simultaneously. You must ensure that all resources are safe in a concurrent environment.
- Security issues: Data security and sharing have increased risks in distributed computer systems. The network has to be secured, and users must be able to safely access replicated data across multiple locations.
- Higher initial infrastructure costs: The initial deployment cost of a distributed system can be higher than a single system. This pricing includes basic network setup issues, such as transmission, high load, and loss of information.

Distributed systems aren't easy to get up and running, and often this powerful technology is too *"overkill"* for many systems. There are many challenges distributing data that ensures various requirements under unexpected circumstances.

Similarly, bugs are harder to detect in systems that are spread across multiple locations.

**Examples of distributed systems**

Distributed systems are used in all kinds of things, everything from electronic banking systems to sensor networks to multiplayer online games. Many organizations utilize distributed systems to power content delivery network services. In the healthcare industry, distributed systems are being used for storing and accessing and telemedicine. In finance and commerce, many online shopping sites use distributed systems for online payments or information dissemination systems in financial trading.

Distributed systems are also used for transport in technologies like GPS, route finding systems, and traffic management systems. Cellular networks are also examples of distributed network systems due to their base station.

Google utilizes a complex, sophisticated distributed system infrastructure for its search capabilities. Some say it is the most complex distributed system out there currently.

## Global Information Systems: Role of Internet and Web Services

The Internet, one of the most marvelous inventions of this century, in fact, a "killer application, is the international network of networks. The Internet is a universal technology platform that allows computer to communicate with any other computer in the world. Furthermore, one of the advantages of the Internet is that nobody really 'owns it. It is a global collection of networks, both big and small. These networks connect together in many different ways to form the single entity that we know as the Internet. In fact, the very name comes from this idea of interconnected networks as shown in figure 1.1.

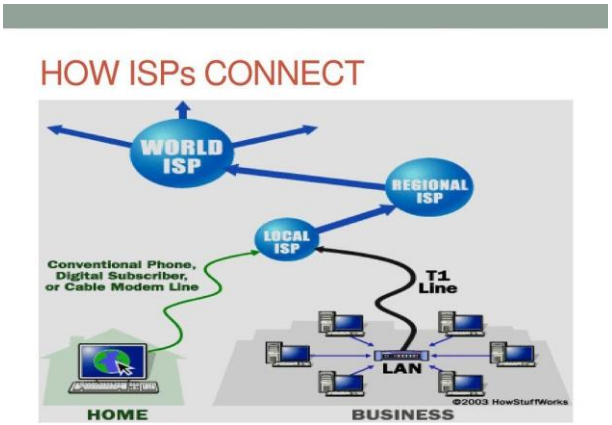


Figure 1.1 The Internet

The Internet has become so well-meshed in the day-to-day working of the knowledge workers that its contribution is acknowledged by everybody. Although the Internet, indeed, has brought the world closer in a way, this very ‘free' and 'autonomous nature of the Internet does have some implications for the security of IS. In this section, we focus on the contribution of web services to modern IS in the global. The Internet has revolutionized communication and thereby its contribution to information sharing. With access to a computer and an appropriate connection, anyone can interact with others worldwide. However, the web is designed to exchange unstructured information: while people can read web pages and understand their meaning, computers cannot. If corporations want to conduct business over the web, humans have to be involved unless there is a way for computers to communicate on their own. This is where web services come in. They make it possible for companies to do business through their computer systems exploiting the Internet infrastructure.

Web services play a complementary and dominant role in building global IS for today's dynamic business world. IBM's definition of web services states that "Web Services are self-contained, modular applications that can be described, published, located and invoked over a network, generally, the World Wide Web (WWW). Companies send and receive a great deal of information, by automating even a small part. However, one of the greatest benefits from web services comes from links between companies, where extended processes between companies can be automated. This is very much essential in the paradigm of today's 'extended enterprise concept’.

Web services perform functions ranging from simple requests to complicated business processes. Once a web service is developed, other applications and other web services can discover and invoke the deployed service through universal description, discovery and integration (UDDI). The idea of web services is to leverage the advantages of the web as a platform to apply it to the services themselves, not just to the static information. "Services refer to components and the services offered that can be used to build larger application services. Web services make it easier to build service-based architectures without the applications being locked-in to a particular software vendor's products.

Web services have been proven to give a strong return on investment (ROI) and make computer-based IS more adaptable. They also help bring productivity, flexibility and low maintenance cost in the development of IS by integrating components from various third-party vendors (another avenue for implementing appropriate security measures in the IS). Web services make information available from computer systems to other applications using well-defined standards.

Benefits of web services for developing IS of global nature are as follows:

1. Web services tools are available for most computer systems, including mainframes and packaged applications. This means that not only the existing applications can be retained, but also the existing knowledge of staff can be applied and extended using web services for business integration.
2. Web services are adaptable and can handle changes more readily than other integration solutions, because they use structured test as their message format. Therefore, because the cost of maintenance is reduced, the overall cost of a web services system also reduces.
3. IT managers now have the ability to exchange data between most applications, on most computers, in a consistent and standard way. Tools and further standards are therefore emerging to build composite applications that can model and manage business processes around these business-level components
4. If necessary, an alternative application can be used to provide web services without changing the overall effect of the system. This gives significant flexibility in the choice of a supplier. This aspect is particularly important in the consideration of outsourcing security services.

## Information Systems Security: Threats and Attacks

In Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.
**Threat** –Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

The IS Security Threats can be classified as follows:

1. **Human Error** (inadvertent disclosure of confidential information).
2. **Computer abuse or crime** ( when a person intends to be malicious and starts stealing information from sites, or cause damage to a computer or computer network)
3. **Natural and Political Disasters** (Natural calamities, wars and riots)
4. **Failure of Hardware or Software** (server malfunctioning, Software errors)

**Security Threats related to Computer Crime or Abuse (Cyber Crime):**

**1. Hacking/ Impersonation**

In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the 'hacking') are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. They're usually technology buffs who have expert-level skills in one particular software program or language. As for motives, there could be several, but the most common are pretty simple and can be explained by a human tendency such as greed, fame, power, etc. Some people do it purely to show-off their expertise – ranging from relatively harmless activities such as modifying software (and even hardware) to carry out tasks that are outside the creator's intent, others just want to cause destruction.

Greed and sometimes voyeuristic tendencies may cause a hacker to break into systems to steal personal banking information, a corporation's financial data, etc. They also try and modify systems so that they can execute tasks at their whims. Hackers displaying such destructive conduct are also called "Crackers" at times. They are also called "Black Hat" hackers .On the other hand, there are those who develop an interest in computer hacking just out of intellectual curiosity. Some companies hire these computer enthusiasts to find flaws in their security systems and help fix them. Referred to as "White Hat" hackers, these guys are against the abuse of computer systems. They attempt to break into network systems purely to alert the owners of flaws. It's not always altruistic, though, because many do this for fame as well, in order to land jobs with top companies, or just to be termed as security experts. “Grey Hat” is another term used to refer to hacking activities that are a cross between black and white hacking. Some of the most famous computer geniuses were once hackers who went on to use their skills for constructive technological development. Dennis Ritchie and Ken Thompson, the creators of the UNIX operating system were two of them. Shawn Fanning, the developer of Napster, Mark Zuckerberg of Facebook, and many more are also examples. Some of the Hacking Techniques are:

a. **SQL Injections:**

An SQL injection is a technique that allows hackers to play upon the security vulnerabilities of the software that runs a web site. It can be used to attack any type of unprotected or improperly protected SQL database. This process involves entering portions of SQL code into a web form entry field – most commonly usernames and passwords – to give the hacker further access to the site backend, or to a particular user’s account. When you enter logon information into sign-in fields, this information is typically converted to an SQL command. This command checks the data you’ve entered against the relevant table in the database. If your input data matches the data in the table, you’re granted access, if not, you get the kind of error you would have seen when you put in a wrong password. An SQL injection is usually an additional command that when inserted into the web form, tries to change the content of the database to reflect a successful login. It can also be used to retrieve information such as credit card numbers or passwords from unprotected sites.

b. **Theft of FTP Passwords:**

This is another very common way to tamper with web sites. FTP password hacking takes advantage of the fact that many webmasters store their website login information on their poorly protected PCs. The thief searches the victim’s system for FTP login details, and then relays them to his own remote computer. He then logs into the web site via the remote computer and modifies the web pages as he or she pleases.

**c. Cross-site scripting:**

Also known as XSS (formerly CSS, but renamed due to confusion with cascading style sheets), is a very easy way of circumventing a security system. Cross-site scripting is a hard-to-find loophole in a web site, making it vulnerable to attack. In a typical XSS attack, the hacker infects a web page with a malicious client-side script or program. When you visit this web page, the script is automatically downloaded to your browser and executed. Typically, attackers inject HTML, JavaScript, VBScript, ActiveX or Flash into a vulnerable application to deceive you and gather confidential information. If you want to protect your PC from malicious hackers, investing in a good firewall should be first and foremost.

### 2. Virus dissemination

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. “Worms” unlike viruses don’t need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term “worm” is sometimes used to mean self-replicating “malware” (Malicious software). These terms are often used interchangeably in the context of the hybrid viruses/worms that dominate. The current virus scenario. “Trojan horses” are different from viruses in their manner of propagation.

They masquerade as a legitimate file, such as an email attachment from a supposed friend with a very believable name, and don't disseminate themselves. The user can also unknowingly install a Trojan-infected program via drive-by downloads when visiting a website, playing online games or using internet-driven applications. A Trojan horse can cause damage similar to other viruses, such as steal information or hamper/disrupt the functioning of computer systems. Computer viruses usually spread via removable media or the internet. A flash disk, CD-ROM, magnetic tape or other storage device that has been in an infected computer infects all future computers in which it's used. Your computer can also contract viruses from sinister email attachments, rogue web sites or infected software. And these disseminate to every other computer on your network. All computer viruses cause direct or indirect economic damages. Based on this, there are two categories of viruses:

1) Those that only disseminate and don't cause intentional damage

2) Those which are programmed to cause damage.

However, even by disseminating, they take up plenty of memory space, and time and resources that are spent on the clean-up job. Direct economic damages are caused when viruses alter the information during digital transmission. Considerable expenses are incurred by individuals, firms and authorities for developing and implementing the anti-virus tools to protect computer systems.

**3. Logic bombs**

A logic bomb, also known as "slag code", is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as "time-bombs". For example, the infamous "Friday the 13th" virus which attacked the host systems only on specific dates; it "exploded" (duplicated itself) every Friday that happened to be the thirteenth of a month, thus causing system slowdowns.

Logic bombs are usually employed by disgruntled employees working in the IT sector. You may have heard of "disgruntled employee syndrome" wherein angry employees who've been fired use logic bombs to delete the databases of their employers, stultify the network for a while or even do insider trading. Triggers associated with the execution of logic bombs can be a specific date and time, a missing entry from a database or not putting in a command at the usual time, meaning the person doesn't work there anymore. Most logic bombs stay only in the network they were employed in. So in most cases, they're an insider job. This makes them easier to design and execute than a virus. It doesn't need to replicate; which is a more complex job. To keep your network protected from the logic bombs, you need constant monitoring of the data and efficient anti-virus software on each of the computers in the network. There's another use for the type of action carried out in a logic bomb "explosion" – to make restricted software trials. The embedded piece of code destroys the software after a defined period of time or renders it unusable until the user pays for its further use. Although this piece of code uses the same technique as a logic bomb, it has a non-destructive, non-malicious and user-transparent use, and is not typically referred to as one.

**4. Denial-of-Service attack**

A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it. Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. DoS attacks violate the acceptable use policies of virtually all internet service providers. Another variation to a denial-of-service attack is known as a "Distributed Denial of Service" (DDoS) attack wherein a number of geographically widespread perpetrators flood the network traffic. Denial-of-Service attacks typically target high profile web site servers belonging to banks and credit card payment gateways. Websites of companies such as Amazon, CNN, Yahoo, Twitter and eBay are not spared either.

**5. Phishing**

This is a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing. People receive email containing links to legitimate appearing websites. The malware would have installed itself on your computer and stolen private information. Cyber-criminals use social engineering to trick you into downloading malware off the internet or make you fill in your personal information under false pretenses. A phishing scam in an email message can be evaded by keeping certain things in mind. Look for spelling mistakes in the text. Cyber-criminals are not known for their grammar and spelling. Fake threat messages saying "Your email account will be closed if you don't reply to this email" are sent to the users to trick them by threatening that their security has been compromised. Attackers use the names and logos of well-known web sites to deceive you. The graphics and the web addresses used in the email are strikingly similar to the legitimate ones, but they lead you to phony sites. Not all phishing is done via email or web sites. Vishing (voice phishing) involves calls to victims using fake identity fooling them into considering the call to be from a trusted organization. They may claim to be from a bank asking you to dial a number (provided by VoIP service and owned by attacker) and enter their account details.

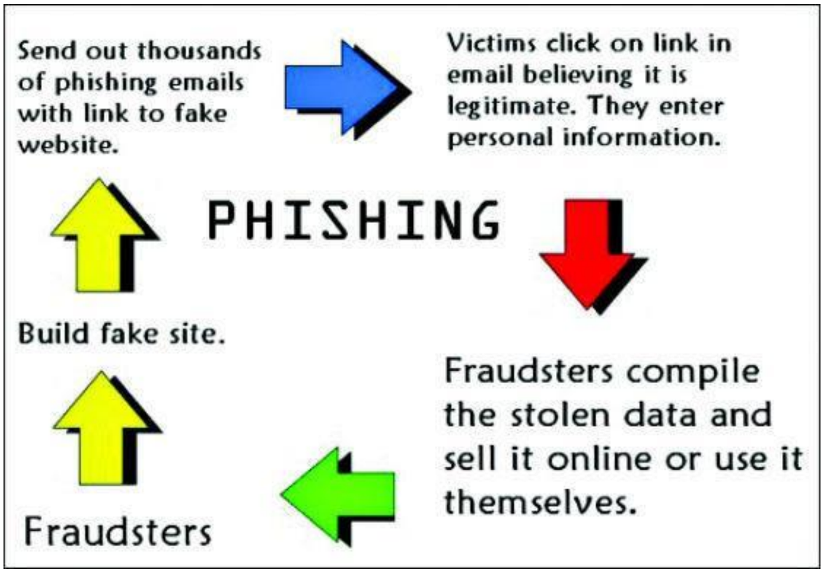

Send out thousands of phishing emails with link to fake website.
Victims click on link in email believing it is legitimate. They enter personal information.
PHISHING
Build fake site.
Fraudsters compile the stolen data and sell it online or use it themselves.
Fraudsters

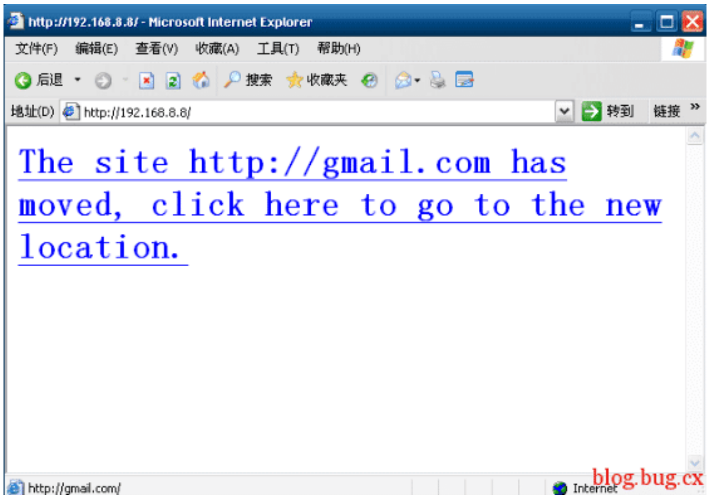
Figure 1.2 Phishing

**6. Email bombing and spamming**

Email bombing is characterized by an abuser sending huge volumes of email to a target address resulting in victim's email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters. Email bombing is commonly carried out using bonnets (private internet connected computers whose security has been compromised by malware and under the attacker's control) as a DDoS attack. This type of attack is more difficult to control due to multiple source addresses and the bots which are programmed to send different messages to defeat spam filters. "Spamming" is a variant of email bombing. Here unsolicited bulk messages are sent to a large number of users, indiscriminately. Opening links given in spam mails may lead you to phishing web sites hosting malware. Spam mail may also have infected files as attachments. Email spamming worsens when the recipient replies to the email causing all the original addressees to receive the reply. Spammers collect email addresses from customer lists, newsgroups, chat-rooms, web sites and viruses which harvest users' address books, and sell them to other spammers as well. A large amount of spam is sent to invalid email addresses. Email filters cleaning out spam mail. Sending spam violates the acceptable use policy (AUP) of almost all internet service providers. If your system suddenly becomes sluggish (email loads slowly or doesn't appear to be sent or received), the reason may be that your mailer is processing a large number of messages. Unfortunately, at this time, there's no way to completely prevent email bombing and spam mails as it's impossible to predict the origin of the next attack. However, what you can do is identify the source of the spam mails and have your router configured to block any incoming packets from that address.

### 7. Web jacking

Web jacking derives its name from "hijacking". Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests. Cases have been reported where the attacker has asked for ransom, and even posted obscene material on the site. The web jacking method attack may be used to create a clone of the web site, and present the victim with the new link saying that the site has moved. Unlike usual phishing methods, when you hover your cursor over the link provided, the URL presented will be the original one, and not the attacker's site. But when you click on the new link, it opens and is quickly replaced with the malicious web server. The name on the address bar will be slightly different from the original website that can trick the user into thinking it's a legitimate site. For example, "gmail" may direct you to "gmai1". Notice the one in place of 'L'. It can be easily overlooked.


The site http://gmail.com has moved, click here to go to the new location.

http://192.168.8.8/ - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退
搜索
收藏夹
地址(D) http://192.168.8.8/
转到
链接
http://gmail.com/
Internet
blog.bug.cx

Figure 1.3 Web Jacking

Web jacking can also be done by sending a counterfeit message to the registrar controlling the domain name registration, under a false identity asking him to connect a domain name to the webjacker's IP address, thus sending unsuspecting consumers who enter that particular domain name to a website controlled by the webjacker. The purpose of this attack is to try to harvest the credentials, usernames, passwords and account numbers of users by using a fake web page with a valid link which opens when the user is redirected to it after opening the legitimate site.

**8. Cyber stalking**

Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn't physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It's an invasion of one's online privacy. Cyber stalking uses the internet or any other electronic means and is different from offline stalking, but is usually accompanied by it. Most victims of this crime are women who are stalked by men and children who are stalked by adult predators and pedophiles. Cyber stalkers thrive on inexperienced web users who are not well aware of netiquette and the rules of internet safety. Cyber stalkers harass their victims via email, chat rooms, web sites, discussion forums and open publishing web sites (e.g. blogs). The availability of free email / web site space and the anonymity provided by chat rooms and forums has contributed to the increase of cyber stalking incidents. Everyone has an online presence nowadays, and it's really easy to do a Google search and get one's name, alias, contact number and address, contributing to the menace that is cyber stalking. As the internet is increasingly becoming an integral part of our personal and professional lives, stalkers can take advantage of the ease of communications and the availability of personal information only a few mouse clicks away. In addition, the anonymous and non-confrontational nature of internet communications further tosses away any disincentives in the way of cyber stalking. Cyber stalking is done in two primary ways:

a. **Internet Stalking:** Here the stalker harasses the victim via the internet. Unsolicited email is the most common way of threatening someone, and the stalker may even send obscene content and viruses by email. However, viruses and unsolicited telemarketing email alone do not constitute cyber stalking. But if email is sent repeatedly in an attempt to intimidate the recipient, they may be considered as stalking. Internet stalking is not limited to email; stalkers can more comprehensively use the internet to harass the victims. Any other cyber-crime that we've already read about, if done with an intention to threaten, harass, or slander the victim may amount to cyber stalking.

b. **Computer Stalking:** The more technologically advanced stalkers apply their computer skills to assist them with the crime. They gain unauthorized control of the victim's computer by exploiting the working of the internet and the Windows operating system. Though this is usually done by proficient and computer savvy stalkers, instructions on how to accomplish this are easily available on the internet.

Cyber stalking has now spread its wings to social networking. With the increased use of social media such as Facebook, Twitter, Flickr and YouTube, your profile, photos, and status updates are up for the world to see. Your online presence provides enough information for you to become a potential victim of stalking without even being aware of the risk. With the "check-ins", the "life-events", apps which access your personal information and the need to put up just about everything that you're doing and where you're doing it, one doesn't really leave anything for the stalkers to figure out for themselves. Social networking technology provides a social and collaborative platform for internet users to interact, express their thoughts and share almost everything about their lives. Though it promotes socialization amongst people, along the way it contributes to the rise of internet violations.

**9. Data diddling**

Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that’s programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

This is one of the simplest methods of committing a computer-related crime, because even a computer amateur can do it. Despite this being an effortless task, it can have detrimental effects. For example, a person responsible for accounting may change data about themselves or a friend or relative showing that they’re paid in full. By altering or failing to enter the information, they’re able to steal from the enterprise. Other examples include forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements. Electricity boards in India have been victims of data diddling by computer criminals when private parties were computerizing their systems.

### 10. Identity Theft and Credit Card Fraud

Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name. The imposter may also use your identity to commit other crimes. “Credit card fraud” is a wide ranging term for crimes involving identity theft where the criminal uses your credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is your pre-approved card falling into someone else’s hands. He/she can use it to buy anything until you report to the authorities and get your card blocked. The only security measure on credit card purchases is the signature on the receipt but that can very easily be forged. However, in some countries the merchant may even ask you for an ID or a PIN. Some credit card companies have software to estimate the probability of fraud. If an unusually large transaction is made, the issuer may even call you to verify. Often people forget to collect their copy of the credit card receipt after eating at restaurants or elsewhere when they pay by credit card. These receipts have your credit card number and your signature for anyone to see and use. With only this information, someone can make purchases online or by phone. You won’t notice it until you get your monthly statement, which is why you should carefully study your statements. Make sure the website is trustworthy and secure when shopping online. Some hackers may get a hold of your credit card number by employing phishing techniques. Sometimes a tiny padlock icon appears on the left screen corner of the address bar on your browser which provides a higher level of security for data transmission. If you click on it, it will also tell you the encryption software it uses.

### 11. Salami slicing attack

A “salami slicing attack” or “salami fraud” is a technique by which cyber-criminals steal money or resources a bit at a time so that there’s no noticeable difference in overall size. The perpetrator gets away with these little pieces from a large number of resources and thus accumulates a considerable amount over a period of time. The essence of this method is the failure to detect the misappropriation. The most classic approach is “collect-the-roundoff” technique. Most calculations are carried out in a particular currency are rounded off up to the nearest number about half the time and down the rest of the time. If a programmer decides to collect these excess fractions of rupees to a separate account, no net loss to the system seems apparent. This is done by carefully transferring the funds into the perpetrator’s account. Attackers insert a program into the system to automatically carry out the task. Logic bombs may also be employed by unsatisfied greedy employees who exploit their know-how of the network and/or privileged access to the system. In this technique, the criminal programs the arithmetic calculators to automatically modify data, such as in interest calculations. Stealing money electronically is the most common use of the salami slicing technique, but it’s not restricted to money laundering. The salami technique can also be applied to gather little bits of information over a period of time to deduce an overall picture of an organization. This act of distributed information gathering may be against an individual or an organization. Data can be collected from web sites, advertisements, documents collected from trash cans, and the like, gradually building up a whole database of factual.

Intelligence about the target. Since the amount of misappropriation is just below the threshold of perception, we need to be more vigilant. Careful examination of our assets, transactions and every other dealing including sharing of confidential information with others might help reduce the chances of an attack by this method.

**12. Software Piracy**

Thanks to the internet and torrents, you can find almost any movie, software or song from any origin for free. Internet piracy is an integral part of our lives which knowingly or unknowingly we all contribute to. This way, the profits of the resource developers are being cut down. It's not just about using someone else's intellectual property illegally but also passing it on to your friends further reducing the revenue they deserve.

Software piracy is the unauthorized use and distribution of computer software. Software developers work hard to develop these programs and piracy curbs their ability to generate enough revenue to sustain application development. This affects the whole global economy as funds are relayed from other sectors which results in less investment in marketing and research.

The following constitute software piracy:

- Loading unlicensed software on your PC
- Using single-licensed software on multiple computers
- Using a key generator to circumvent copy protection
- Distributing a licensed or unlicensed ("cracked") version of software over the internet and offline

"Cloning" is another threat. It happens when someone copies the idea behind your software and writes his own code. Since ideas are not copy protected across borders all the time, this isn't strictly illegal. A software "crack" is an illegally obtained version of the software which works its way around the encoded copy prevention. Users of pirated software may use a key generator to generate a "serial" number which unlocks an evaluation version of the software, thus defeating the copy protection. Software cracking and using unauthorized keys are illegal acts of copyright infringement. Using pirated material comes with its own risks. The pirated software may contain Trojans, viruses, worms and other malware, since pirates will often infect software with malicious code. Users of pirated software may be punished by the law for illegal use of copyrighted material.

**13. Others**

So far we've discussed the dedicated methods of committing cybercrimes. In a nutshell, any offence committed using electronic means such as net extortion, cyber bullying, child pornography and internet fraud is termed as cybercrime. The internet is a huge breeding ground for pornography, which has often been subject to censorship on grounds of obscenity. But what may be considered obscene in India might not be considered so in other countries.

Since every country has a different legal stand on this subject matter, pornography is rampant online. However, according to the Indian Constitution, largely, pornography falls under the category of obscenity and is punishable by law. Child pornography is a serious offence, and can attract the harshest punishments provided for by law. Pedophiles lurk in chat rooms to lure children. The internet allows long-term victimization of such children, because the pictures once put up, spread like wild-fire, and may never get taken down completely. Internet crimes against children are a matter of grave concern, and are being addressed by the authorities, but this problem has no easy solution.

**Types of Attacks:**

**Software attacks** – Software Attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently.

**Malware-** Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or a anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

1. Infection Methods
2. Malware Actions

Malware on the basis of Infection Method are following:

2. **Virus –** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.

3. **Worms –** Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will for example consume hard disk space thus slowing down the computer.

4. **Trojan –** The Concept of Trojan is completely different from the viruses and worms. The name Trojan derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside. Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed. They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, and Remote Access Trojans etc.

5. **Bots –**: Bots can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need of human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called Botnet.

**Malware on the basis of Actions:**

1. **Adware –** Adware is not exactly malicious but they do breach privacy of the users. They display ads on computer's desktop or inside individual programs. They come attached with free to use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.

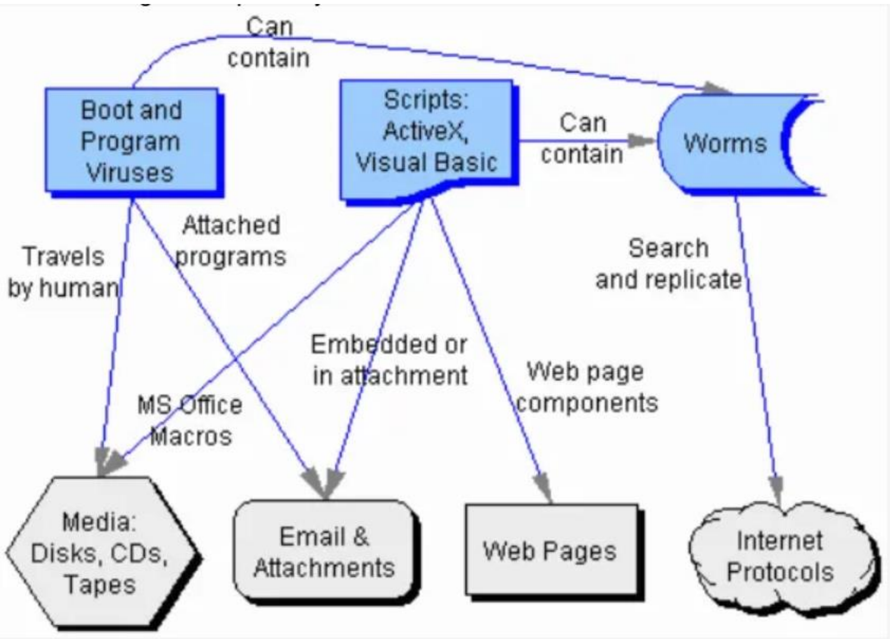
2. **Spyware –** It is a program or we can say a software that monitors your activities on computer and reveal collected information to interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they installs themselves and sits silently to avoid detection. One of the most common example of spyware is KEYLOGGER. The basic job of key logger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.

3. **Ransomware –** It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.

4. **Scareware –** It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.

5. **Rootkits –** are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.

6. **Zombies –** They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.



A simple diagram to show how malware can propogate

Figure 1.4 Malware Propagation

**Classification of Thefts:**

- **Theft of intellectual property** means violation of intellectual property rights like copyrights, patents etc.

- **Identity theft** means to act someone else to obtain person's personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.

- **Theft of equipment and information** is increasing these days due to the mobile nature of devices and increasing information capacity.

- **Sabotage** means destroying company's website to cause loss of confidence on part of its customer.

- **Information extortion** means theft of company's property or information to receive payment in exchange. For example ransomware may lock victims file making them inaccessible thus forcing victim to make payment in exchange. Only after payment victim's files will be unlocked.

These are the old generation attacks that continue these days also with advancement every year. Apart from these there are many other threats. Below is the brief description of these new generation threats.

- **Technology with weak security –** With the advancement in technology, with every passing day a new gadget is being released in the market. But very few are fully secured and follow Information Security principles. Since the market is very competitive Security factor is compromised to make device more up to date. This leads to theft of data/ information from the devices
- **Social media attacks –** in these cyber criminals identify and infect a cluster of websites that persons of a particular organization visit, to steal information.
- **Mobile Malware –**There is a saying when there is connectivity to Internet there will be danger to Security. Same goes to Mobile phones where gaming applications are designed to lure customer to download the game and unintentionally they will install malware or virus in the device.
- **Outdated Security Software –** With new threats emerging every day, updating in security software is a pre requisite to have a fully secured environment.
- **Corporate data on personal devices –** These days every organization follows a rule BYOD. BYOD means bring your own device like Laptops, Tablets to the workplace. Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.
- **Social Engineering –**It is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install malicious software- that will give them control of your computer. For example email or message from your friend that was probably not sent by your friend. Criminal can access your friend's device and then by accessing the contact list he can send infected email and message to all contacts. Since the message/ email is from a known person recipient will definitely check the link or attachment in the message, thus unintentionally infecting the computer.

## Classification of Threats and Accessing damages:

Security in any organization is managed through the security policies, security architectures and security procedures/ processes. The security managers need to know explicitly about the assets of their organizations, vulnerability of their Information System to different threats and their potential damage. Threats consists of the following properties:

1. Asset: Asset is something of value to the organization( information in electronic or physical form, software, hardware, people with unique expertise etc)
2. Actor: Actor is capable to violate the Security Requirements- Confidentiality, Integrity, Availability (CIA)

3. Motive: It indicates that whether the actor's intentions are deliberate or accidental.
4. Access:  how the asset will be accessed by the actor.

The major categories of Damages resulting from threats to the IS are:

1. Destruction of information or other resources.
2. Corruption or Modification of information.
3. Theft, Removal or loss of information and other resources.
4. Disclosure of information.
5. Modification of important or sensitive information.
6. Interruption of access to important information, software, applications or services.

Each threat and vulnerability must be related to one or more of the organizational assets requiring protection. Thus, prior to assessing damages (caused by security incidents), we need to identify assets. Typically, there are five categories of logical and physical assets:

1. Information: documented (paper or electronic) data or intellectual property used to meet the mission of an organization.

2. Software: software applications and services that process, store or transmit information.

3. Hardware: IT physical devices considering their replacement costs.

4. People: the people in an organization who possess skills, competencies, knowledge and experience that are difficult to replace.

5. Systems: Is that process and store information (conceptually, a system is a combination of information, software and hardware assets. In computer networking terms, any host, client or server also can be considered a system).

Another way of grouping the threats is to put them together in groups based on some common themes suggested as follows:

1. Human actors using network access: The threats in this category are network-based threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.

2. Human actors using physical access: The threats in this category are physical threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.

3. System problems: The threats in this category are problems with an organization's IT systems. Examples include hardware defects, software defects, unavailability of related enterprise systems, viruses, malicious code and other system-related problems.

4. Other Problems: Problems that are outside the organization's control. (Natural Disaster)

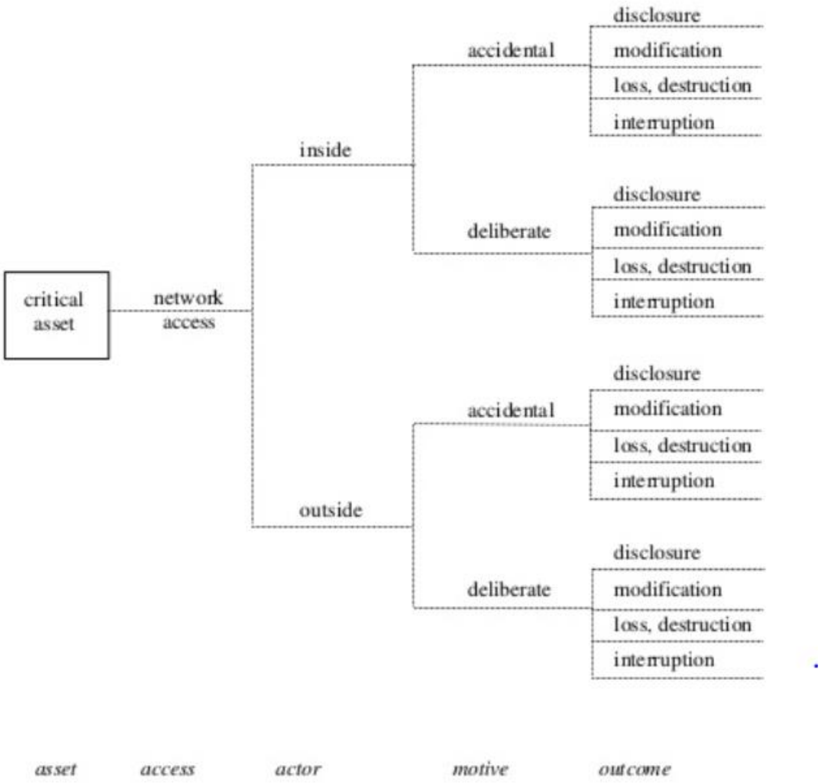


**Figure 1.5 Generic Threat Profile**

Organizational Assets are evaluated using various suitable units of measurements like monitory value of the assets but always we can’t use the monitory value as in case of information we have to assess the damages in relative ways like sensitivity or importance of the information to organization. The immediate costs and losses of assets can be measured by the following:

1. Productivity: (number of employees impacted) x (hours wasted) (burdened hourly rate). Note that burdened hourly rate could be the notional cost of the employees-for example, billing rate of the employees to the customer or in terms of their outgoing cost to the employing organization (salary of the employees).

2. Revenue: direct loss and lost future revenues.

3. Financial performance: credit rating and stock price.

4. Other expenses: equipment rental, overtime costs, extra shipping costs, travel expenses, etc.

Hidden costs are difficult to handle. Consider the example of a DoS attack (this situation was illustrated in Box 2.1) where the damaged reputation of the company can have a negative impact on the relationship of the company with its customers, suppliers, financial markets, banks and business partners. These hidden costs are extremely difficult to quantify and measure. The bottom line is that the cost of an information system security incident in a company has to be measured in terms of the impact on its business; hence, identical incidents in two different companies can have different costs. To evaluate these costs and measure the impact of a security incident on a company, organizations need a systematic approach and a comprehensive risk management system.

**Other terms in Information Security**

**Access Control System**

Physical, procedural and/or electronic mechanism that ensures that only those who are authorized to view, update, and/or delete data can access that data.

**Authorization**

The process of giving someone permission to do or have something; a system administrator defines which users are allowed access to the system and what privileges are allowed for each user.

**Confidentiality**

Confidentiality is an attribute of information. Confidential information is sensitive, contractually protected, or information whose loss, corruption, or unauthorized disclosure could be harmful or prejudicial.

**Data Custodians**

As defined in the UA Information Systems Security Policy, individuals who have been officially designated as being accountable for protecting the confidentiality of specific data that is transmitted, used, or stored on a system or systems within a department, college, school, or administrative unit of the UA and certain affiliated organizations.

**Encryption**

The process of turning readable text into unreadable (cipher) text, which requires the use of a decipher key to render it readable.

**Ownership**

This term signifies decision-making authority and accountability for a given scope of control.

**Personally Identifiable Information**

Personally identifiable information is defined as data or other information that is tied to, or which otherwise identifies, an individual or provides information about an individual in a way that is reasonably likely to enable identification of a specific person and make personal information about them known.

Personal information includes, but is not limited to, information regarding a person's home or other personal address, social security number, driver's license, marital status, financial information, credit card numbers, bank account numbers, parental status, sexual orientation, race, religion, political affiliation, personal assets, medical conditions, medical records or test results, home or other personal phone numbers, non-university address, employee number, personnel or student records, and information related to the UA Affirmative Action Policy.

**Principle of Least Privilege**

Access privileges for any user should be limited to only what they need to have to be able to complete their assigned duties or functions, and nothing beyond these privileges.

**Principle of Separation of Duties**

Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse or other harm.

**Privacy**

An individual right to be left alone; to withdraw from the influences of his or her environment; to be secluded, not annoyed, and not intruded upon; to be protected against the misuse or abuse of something legally owned by an individual or normally considered by society to be his or her property.

**Record**

Recorded information, regardless of medium or characteristics, made or received by the university that is evidence of its operations, and has value requiring its retention for a specific period of time. for example

"Record means any document, paper, book, letter, drawing, map, plat, photo, photographic file, motion picture film, microfilm, microphotograph, exhibit, magnetic or paper tape, punched card, electronic record, or other document of any other material, regardless of physical form or characteristic, developed or received under law or in connection with the transaction of official business and preserved or appropriate for preservation by an agency or a political subdivision, as evidence of the organization, function, policies, decisions, procedures, operations, or other activities of the state or political subdivision or because of the informational value in them; the term does not include library and museum material developed or acquired and preserved solely for reference, historical, or exhibition purposes, extra copies of documents preserved solely for convenience of reference, or stocks of publications and processed documents."

**Security**

An attribute of information systems practices that includes specific policy-based, procedural, and technical mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services and the confidentiality of sensitive information.

**Sensitive Information**

A general term for any information that requires access controls and other control measures to meet legal, policy and/or ethical requirements.

**System**

A network, computer, software package, or other entity for which there can be security concerns.

**System(s) Owners**

As defined in the UA Information Systems Security Policy, individuals within the UA community who are accountable for the budget, management, and use of one or more electronic information systems or electronic applications that support UA business, client services, educational, or research activities that are associated or hosted by the UA.

**Users**

Any individual that has been granted access and privileges to UA computing and network services, applications, resources, and information.

## Security in Mobile and Wireless Computing

In the recent years, the use of laptops, personal digital assistants (PDAs) and mobile phones has grown from the limited user communities to widespread desktop replacement and broad deployment. The complexity of managing these devices outside the walls of the office is something that the information technology (IT) departments in the organizations need to address. Remote connection has extended from fixed location dial-in to wireless-on-the-move, and smart handheld devices such as PDAs have become networked, converging series on the move, and smart handheld devices such as PDAs have become networked, converging with mobile phones. Furthermore, the maturation of the PDA and advancements in cellular phone technology have converged into a new category of mobile phone device: the smart phones combine the best aspect of mobile and wireless technologies and blend them into a useful business tool. While IT department of organisations as yet are not swapping employees' company-provided PDAs (as the case may be) for the smart phones, many users may bring these devices from home and use them in the office. Research in Motions' (RIM) Blackberry Wireless Handheld is an alternate technology. According to RIM report, there are approximately 10.000 corporations that use the Blackberry enterprise server and client/server software for data communication between corporate Blackberry devices and other mail systems. Thus, the larger and more diverse community of mobile users and their devices increases the demands on the IT function to secure the device, data and connection to the network, keeping control of the corporate assets, while at the same time supporting mobile user productivity Clearly, these technological developments present a new set of security challenges to the global organizations

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now there is a long list of options ranging from high-end PDAs with integrated wireless modems down to small phones with wireless web-browsing capabilities. Even the simplest of handheld devices provide enough competing power to run small applications, play games, music and make voice calls. A key driver for the growth of mobile solutions for business is the proliferation of handheld devices in the enterprise. As more personal devices find their way into the enterprise, corporations are realizing security threats that come along with the benefits achieved with mobile solutions. Since the term 'mobile device' includes many products, a clear distinction among the key terms mobile computing, wireless computing and handheld devices is provided. Wireless refers to the method of transferring information between a computing device, such as a PDA, and a data source, such as an agency database server, without a physical connection. Not all wireless communication technologies are mobile. For example, lasers are used in wireless data transfer between buildings, but cannot be used in mobile communications at this time. Mobile simply describes a computing device that is not restricted desktop, that is not tethered.

Mobile computing does not necessarily require wireless communication. In fact, it may not require communication between devices at all. Thus, while 'wireless is a subset of 'mobile', in most cases, an application can be mobile without being wireless, Smart handhelds are defined as handheld or pocket-size devices that connect to a wireless or cellular network, and can have software installed on them. This includes networked PDAs and smart phones as shown in fig. 1.

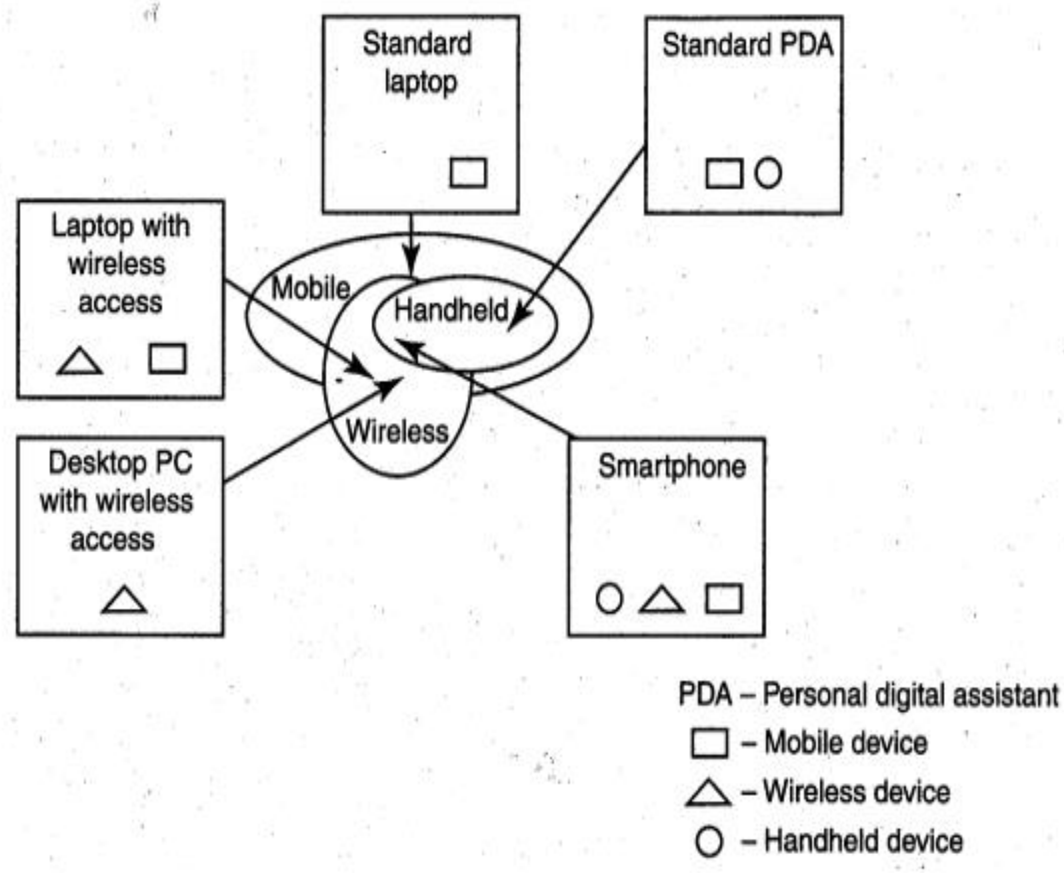


Figure 1.6 Mobile, Wireless and Handheld devices

## Security Challenges in Mobile Devices

Mobility brings two main challenges to the information systems security: on the handheld devices, information is being taken outside of the physically controlled environment, and remote access back to the protected environment is being granted. Perceptions of the organizations to these security challenges are important in devising appropriate security operating procedure.

As the number of mobile device user increases, two challenges are presented; one at the device level-called 'Micro Challenges' and another one at the organizational level-called 'Macro Challenges'.

Some well-known technical challenges in mobile security are:

- Managing the registry setting and configurations
- Authentication service security
- Cryptography security
- Lightweight directory access protocol (LDAP) security

- Remote access server (RAS) security
- Media player control security
- Networking application program interface (API) security

**Registry Settings for Mobile Devices**

Let us understand the issue of registry settings on mobile devices through an example: Microsoft ActiveSync Lent for synchronization with Windows-powered personal computers (PC) and Microsoft Outlook ActiveSync acts as the gateway between Windows-powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music videos and applications from a user's desktop to his/her device. In addition to synchronizing with a PC ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their email, calendar, notes and contacts updated wirelessly when they are away from their PCs. In this context, registry setting becomes an important issue given the case with which various applications allow a free flow of information.

Thus, establishing trusted groups through appropriate registry settings becomes crucial. One of the most prevalent areas where this attention to security is applicable is within group policy'. Group policy is one of the operations that are performed by Windows Active Directory. As a supporting point, consider the following within the past two years, Microsoft has doubled the number of group policy settings that it ships with the operating system (OS). There are now nearly 1,700 settings in a standard group policy. The emphasis on most of the group policy settings is security.

There is one more dimension to mobile device security new mobile applications are constantly being provided to help protect against spyware, viruses, worms, malware and other malicious codes that run through the networks and the Internet. Microsoft and other companies are trying to develop solutions as fast as they can, but the core problem is still not being addressed. According to the experts, the core problem to many of the mobile security issues on a Windows platform is that the baseline security is not configured properly When you get a computer installed or use a mobile device for the first time, it may not be 100% secure. Even if users go through every Control Panel setting and group policy option, they may not get the computer to the desired baseline security. For example, the only way to get a Windows computer to a security level that will be near bulletproof is to make additional registry changes that are not exposed through any interface. There are many ways to get these registry changes completed on every computer in the enterprise, but some are certainly more efficient than the others.

Naive users may think that for solving the problem of mobile device security there are not many registry settings to tackle. The reality of the overall problem becomes prevalent settings to you start researching and investigating the abundance of ‘registry hacks’ that are discussed in Microsoft Knowledge Base articles.

## Authentication Service Security

There are two components of security in mobile computing security of devices and security in networks. A secure network access involves the manual authentication between the device and the base stations or web servers. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No malicious node can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in the security of mobile devices. Some eminent kinds of attacks to which mobile devices are subjected to are: push attacks, pull attacks and crash attacks. These attacks are shown diagrammatically in fig. 1.7, fig. 1.8 and fig. 1.9 respectively.

Authentication services security is important given the typical attacks on mobile devices through the wireless networks: denial of service (DoS) attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking. Security measures in this scenario come from wireless application protocols (WAPs), use of virtual private networks (VPNs), media access control (MAC) address filtering and development in 802x standards.

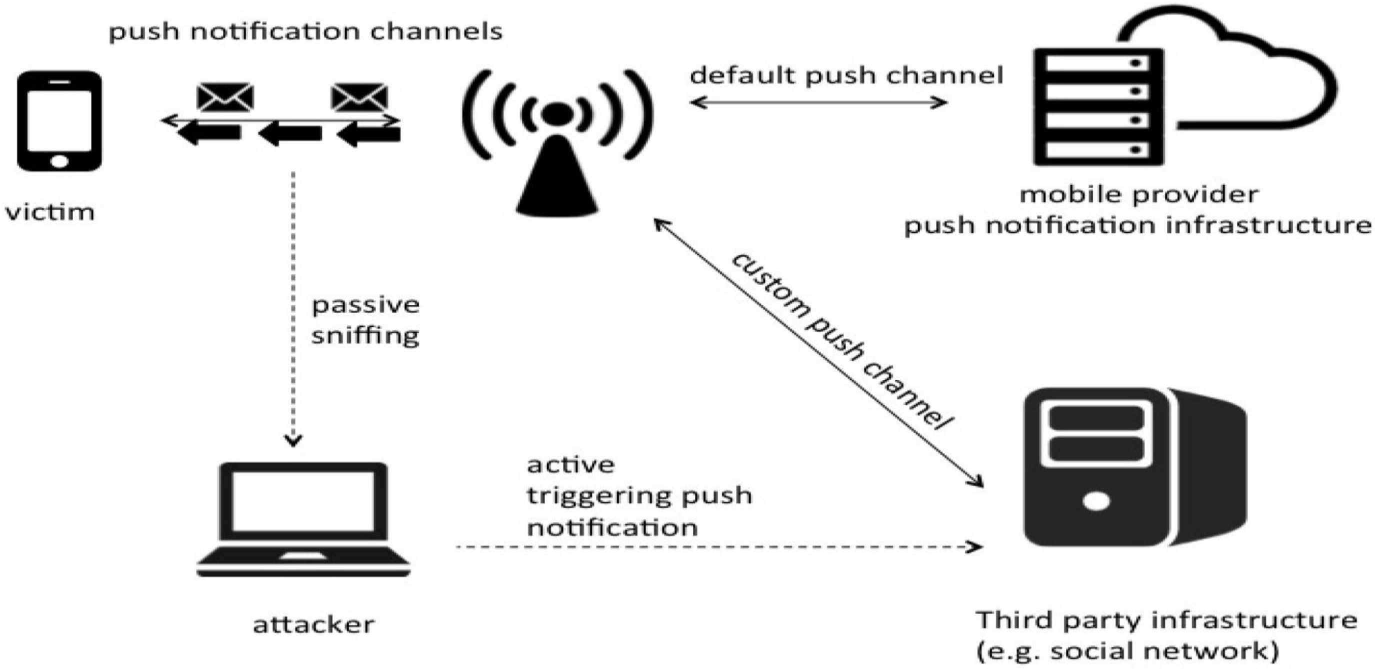


Figure 1.7 Push attack on mobile devices

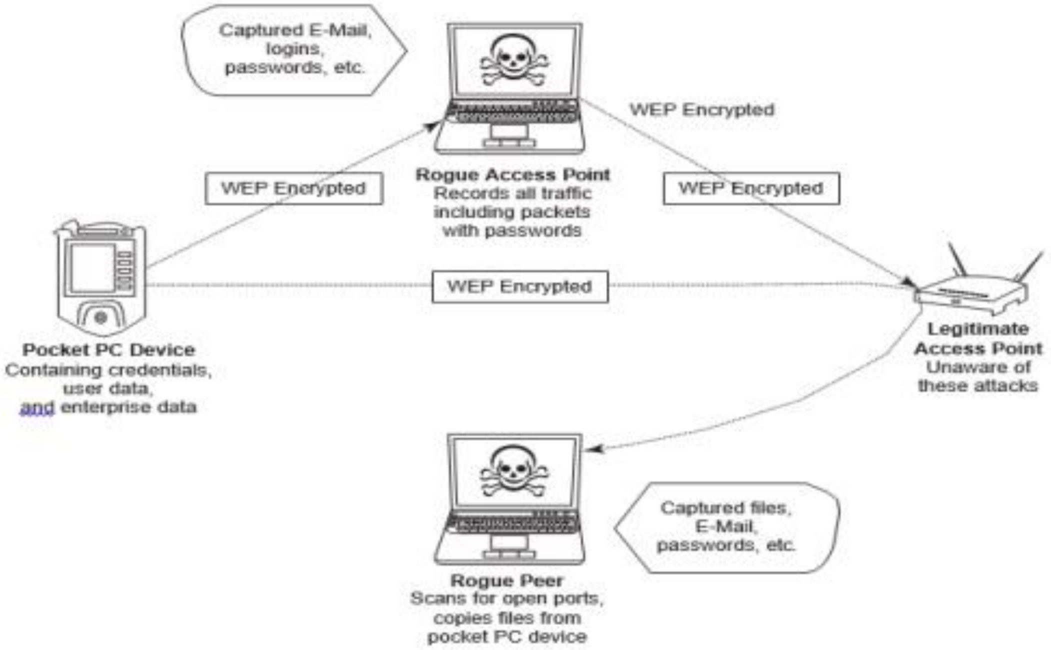


Figure 1.8 Pull attack on mobile devices

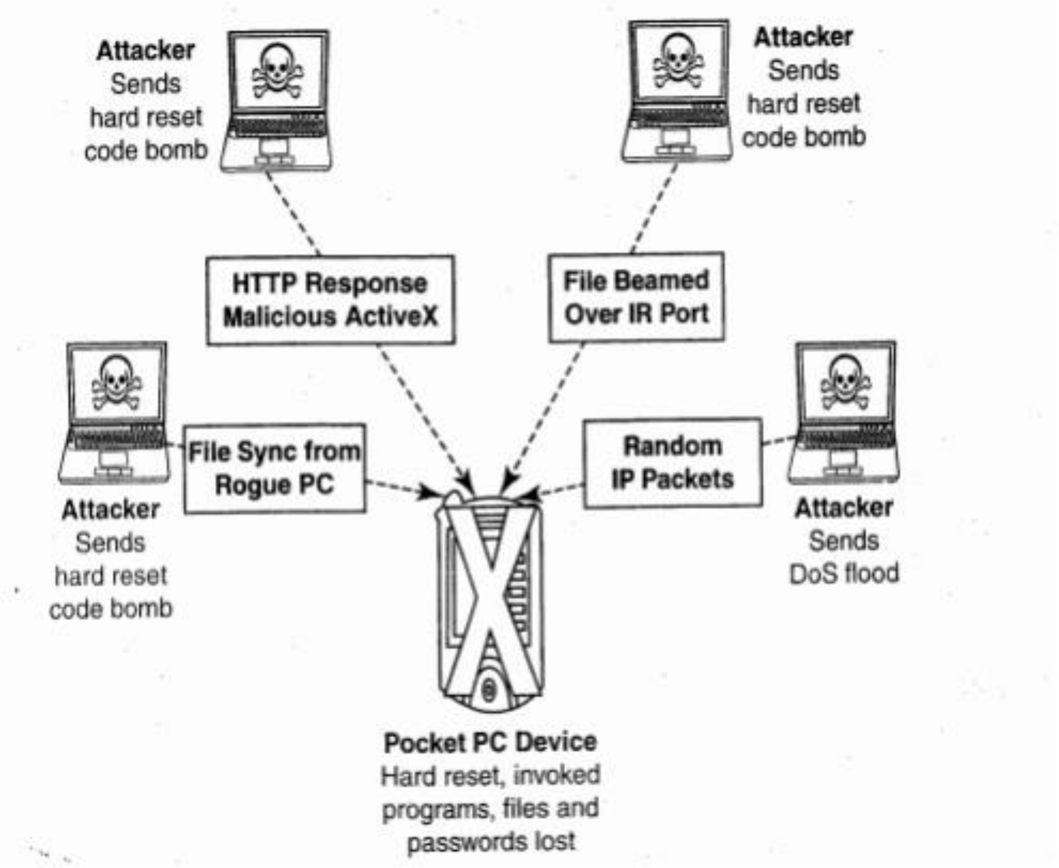


Figure 1.9 Crack attack on mobile devices

**Cryptographic Security for Mobile Devices**

There is a technique known as cryptographically generated addresses (CGA). CGA are Internet protocol version 6 (IPv6) addresses where up to 64 address bits are generated by hashing the address owner's public key. The address owner uses the corresponding private key to assert address ownership and to sign messages sent from the address without a public-key infrastructure (PKI) or other security infrastructure. Deployment of PKI provides many benefits for users to secure their financial transactions initiated from mobile devices. The CGA-based authentication can be used to protect IP-layer signaling protocols including neighbor discovery (as in context-aware mobile computing applications) and mobility protocols. It can be used for key exchange in opportunistic Internet protocol security. Palms (devices that can be held in one's palm) are one of the common handheld devices used in mobile computing. Cryptographic security controls are deployed on these devices. For example, the Cryptographic Provider Manager (CPM) in Palm OS 5 is a system-wide suite of cryptographic services for securing data and resources on a palm-powered device. The CPM extends encryption services to any application written to take advantage of these capabilities, allowing the encryption of only selected data or of all data and resources on the device.

**LDAP Security for Handheld Mobile Computing Devices**

LDAP is a software protocol for enabling anyone to locate organizations, individuals and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet. In a network, a directory tells you where in the network an entity is located. LDAP is a lightweight' (smaller amount of code) version of directory access protocol (DAP). LDAP is lighter because in its initial version it did not include security features. It originated at the University of Michigan and has been endorsed by at least 40 companies. Centralized directories such as LDAP make revoking permissions quick and easy.

**RAS Security for mobile devices**

RAS is an important consideration for protecting the business-sensitive data that may reside on the employees' mobile devices. In addition to bring vulnerable to unauthorized access on their own, mobile devices also provide a route into the systems with which they connect. By using a mobile device to appear as a registered user to these systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways. This is shown in fig. 5.

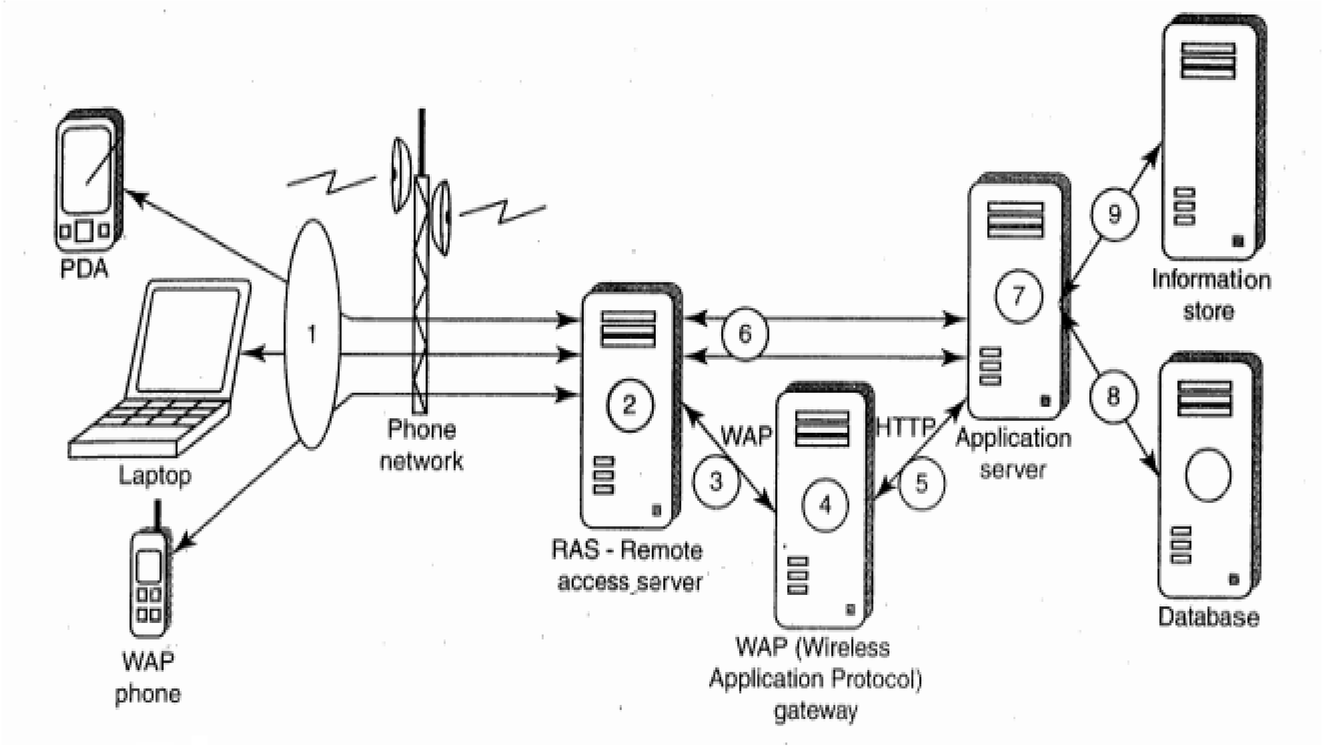


Figure 1.10 Communication from mobile client to organization information store

Another threat comes from the practice of port scanning. First, crackers use a domain name system (DNS) serve to locate the IP address of a connected computer (either the mobile device itself or a gateway server to which it connects). A domain is a collection of sites that are related in some sense Then they scan the ports on this known IP address, working their way through its main control protocol (TCP)/user datagram protocol (UDP) sack to see what communication ports are unprotected by firewalls. For instance, file transfer protocol (FTP) transmissions are typically assigned to port 21. If this port is left unprotected, it can be misused by hackers.

Protecting against port scanning requires software that traps unauthorized incoming packets, thereby preventing a mobile device from revealing its existence and ID. A personal firewall on a pocket PC or smart phone device can be an effective protective screen against this form of attack for the users connecting through a direct Internet or RAS connection. For situations where all connections to the corporate network pass through a gateway, placing the personal firewall on the gateway itself could be the simplest solution, because it avoids the need to place a personal firewall on each mobile device. In either case, deploying secure access methods that implement strong authentication keys will provide an additional protection.

### Media Player Control Security

It is quite common to expect them embracing the mobile handheld devices as a means for information access, remote working and entertainment! Music and video are the two important aspects in the day-to-day aspects for the young generation. Given this, it is easy to appreciate how this can be a source for security breaches. Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the music gateways.

There are many examples to show how a media player can turn out to be a source of threat to information held on mobile devices. For example, in the year 2002, Microsoft Corporation warned about this (visit the URL quoted in the Further Reading section about this news item). According to this news item, Microsoft had warned people that a series of flaws in its Windows Media Player could allow a malicious hacker hijack people's computer systems and perform a variety of actions. According to this warning from Microsoft, in the most severe exploit of a flaw, a hacker could take over a computer system and perform any task the computer's owner is allowed to do, such as opening files or accessing certain parts of a network.

### Networking API Security for Mobile Computing Applications

With the advent of electronic commerce (e-commerce) and its further off-shoot into m-commerce, online payments are becoming a common phenomenon with the payment gateways accessed remotely and possibly wirelessly. Further, with the advent of web services and their use in mobile computing applications, the API becomes an important consideration. Operators and handset developers are increasingly motivated to create even more advanced features for mobile phones, such as one that would enable a phone to double as a credit card and a digital television (TV) player, but they have to ensure that the users and devices are adequately protected from the external threats.

Already, there are organizations announcing the development of various APIs to enable software and hardware developers to write single applications that can be used to target multiple security platforms present in a range of devices such as mobile phones, portable media players, set-top boxes and home gateways.

Most of these developments are targeted specifically at securing a range of embedded and consumer products, including those running OS such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile (the last three are the most commonly used OS for mobile devices). Technological developments such as these provide the ability to significantly improve the security of a wide range of consumer as well as mobile devices. Providing a common software framework and APIs will become an important enabler of new and higher value services.

## Security Implications for Organizations

Managing Diversity and Proliferation of Handheld Devices:

In the previous sections, we talked about the micro-issues of purely technical nature in mobile device security. In this section, we focus on the macro-issues at the organizational level. Given the threats to information systems through usage of mobile devices, the organizations need to establish security practices at a level appropriate to their security objectives, subject to legal and other external constraints. Some organizations will implement security procedures and tools extensively, while others will place more value on cost and convenience. Whatever approaches an organization chooses, it is important that the policy-making effort starts with the commitment from a Chief Executive Officer (CEO), president or director who takes security seriously and communicates that throughout, an organization. The best security technology features are worthless if there is no organization policy or automated enforcement to ensure that they are actually used. In some cases, for example, senior executives have been given special access rights to the corporate network which can circumvent standard security procedures.

Security is always a primary concern; even then, at times, there is still some short-sightedness. Most organizations fail to see the long-term significance of keeping track of who owns what kind of mobile devices. Mobile devices of employees should be registered in corporate asset register irrespective of whether the devices have been provided by the organization or not. In addition, close monitoring of these devices is required in terms of their usage. When an employee leaves, it is important to remove his/her logical as well as physical access to corporate resources because employees (for malicious or other reasons) could be using their mobile devices to connect into the corporate networks. Thus, mobile devices which belong to the company should be returned to the IT department and, at the very least, deactivated and cleansed.

Here is an interesting illustration on this point, unlike laptops, which owing to their cost are generally provided as a corporate item requiring significant sign-off and approvals, many handhelds can be squeezed under approval limits or be purchased the individual. Their usage often falls outside the range of the IT department's scope of control.

Thus another factor in security complications with mobile devices is their falling cost. Until a few ago, mobile devices were considered an office supply item instead of a powerful computing platform. Early handhelds were expensive and specialized, so they were deployed only for specific applications, but more general-purpose models are now available at a relatively low cost, often bundled with a tariff for wireless connection. So, many organizations did not have policies concerning the usage of mobile/wireless devices at work/ connected with work. Nowadays, because modern handheld devices for mobile computing are at times, good productivity tools, they cannot be precluded from use by employees, contractors and other business entities. Given this, it is important for the device management teams to also include user awareness education; thus they get encouraged to take some personal responsibility for the physical security of their devices.

Threats through Lost and Stolen Devices:

This is a new emerging issue for InfoSec. Often mobile handheld devices are lost while people are on the move. Lost mobile devices are becoming even a larger security risk to corporations. A report based on a survey of London's 24,000 licensed cab drivers quotes that 2,900 laptops 1,300 PDAs and over 62,000 mobile phones were left in London in cabs in the year 2001. Today this figure could be far larger given the greatly increased sales and usage of mobile devices.

The security threat under this scenario is scary; owing to a general lack of security in mobile devices, it is often not the value of the handheld device that is important but rather the content that, if lost or stolen, can para company a serious risk of sabotage, exploitations or damage to its professional integrity as most of the times, the mobile handheld devices are provided by the organization. Most of these lost devices have wireless access to a corporate network and potentially very little security, making them Even if the weak link and a major headache for security administrators. Even if these lost devices are personal, the issue is no less serious given the resulting privacy exposures. Garner Group had predicted that by 2003 there will be over one billion mobile devices in use globally. This shows that the popularity of mobile devices is increasing at a rapid rate, but people have not been educated about the importance of securing them. The picture is indeed scary; mobile users are in an even worse position now because they are far more reliant on their mobile devices to store large amounts of sensitive information with very few concerned about hacking it up or protecting it.

Protecting Data on Lost Devices:

For protecting data that are stored persistently on a device, there are two precautions the individuals can take to prevent disclosure of the data stored on a mobile device: encrypting sensitive data and encrypting the entire file system (this may be useful when using data outside of a database, such as in a spreadsheet). Data that are stored on hard disks, in persistent memory or on removable flash cards (whether they are in are out of the device) should be protected. There are many third-party solutions/tools available to protect data on the lost devices in several ways, including encrypting the servers where a database file is residing. There are solutions using which individuals can enforce a self-destruct policy to destroy privileged data on a lost device or create a database action to delete the data on a user's device using a suitable tool.

A key point here is that the organizations should have a clear policy on how to respond to the loss or theft of a device, whether it is data storage, a PDA or a laptop. There should be a method for the device owner to quickly report the loss, and device owners should be aware of this method. Writing the emergency contact information on the device itself is unlikely to be very helpful.

Educating the Laptop Users:

Often, it so happens that corporate laptop users could be putting their company's networks at risk by downloading non-work-related software capable of spreading viruses and spyware. This is because the software assets on laptops become more complex as more applications are used on an increasingly sophisticated OS with diverse connectivity options. A number of surveys conducted worldwide support this. Some are described below.

According to year 2004 finding, through one survey, some 86% of employees with laptops admitted to installing software onto their machines when outside of the office, with many using their laptops to access peer-to-peer websites and download illegal music files and movies. As per one survey of 500 European business laptop users, malicious code, such as spyware and viruses, is infecting laptops and consequently business networks when they are reconnected to the corporate systems.

## LAPTOP SECURITY

The price of computing technology is steadily decreasing; devices such as the laptops have become common in use. Although laptops, like other mobile devices, enhance the business functions and provide mobile access to information anytime and anywhere, they also pose a large threat as they a portable. Wireless capability in these devices has also raised security concerns.

According to the computer security industry and insurance company statistics, thefts of laptops have always been a major concern. Criminals are targeting laptop systems that are expensive as they could fetch a quick profit in the black market. Very few laptop thieves are actually interested in the information that is present in the laptop. Most laptops contain personal and corporate information which could be sensitive. Such information can be misused if found by a malicious user. It is a common belief of senior executive that the information stored on their laptops is only useful for them and would be of any interest to others. Owing to this belief, most senior executives in an organization feel that it is not necessary to protect the information stored on these laptops.

### Physical Security Countermeasures

Cables and hardwired locks: Securing with cables and locks, specially designed for laptops, is the most efficient and ideal solution to safeguard any mobile device. Kensington cables are one of the most popular brands in laptop security cables. These cables are made of aircraft-grade steel thus making these cables 40% stronger than any other national security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. However, cables do not ensure full proof security as the fixed item to which the laptop was attached can be dismantled or smashed. Laptops can also be kept in some kind of safe. In addition, laptops can be protected by security cables Motion sensors and alarms: Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once activated, these devices can be used to track missing laptops in crowded places. Also available are security PCMCIA cards that act as a motion detector an alarm system, and also have the capability to lockdown the laptop if the laptop is moved out of the designated range. They also secure the passwords and encryption keys and prevent access to the OS. These cards have batteries which keep them powered on even when the system is shutdown. Warning labels and stamps can also be used: Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft.

**DATA PROTECTION**

Laptop/computer's security is the responsibility of the user, whether it is a personally-owned or university/office-assigned laptop. Due to its unique vulnerabilities, it is imperative to take special precautions when using restricted data with your laptop. To the fullest extent possible, laptop users should be diligent about safeguarding restricted data from unnecessary exposure due to theft or loss.

**Data Protection Recommendations**

1. Protecting from malicious programs/hackers/social engineering;

2. Avoiding weak passwords/open access;

3. Monitoring application security and scanning for vulnerabilities,

4. Ensuring that unencrypted data/unprotected file systems do not pose threats

5. Proper handling of removable drives/storage mediums/unnecessary ports:

6. Password protection through appropriate passwords rules and use of strong passwords:

7. Locking down unwanted ports/devices;

8. Regularly installing security patches and updates;

9. Installing antivirus software/firewalls/intrusion detection systems (IDSS);

10. Encrypting critical

11. File systems; other countermeasure choosing a secure OS which has been tested for quite some time and which has a high security incorporated into it, registering the laptop with the laptop manufacturer to track down the laptop in case of theft, disabling unnecessary user accounts and renaming the administrator account, disabling display of the last logged in username in the login dialog box, backing up data on a regular basis.

**Remote Data Destruction**

In the unfortunate event that a laptop is ever lost or stolen, a remote data destruction product can help secure restricted data by allowing the user to remotely and securely delete all data stored on the machine.

## Basic Principles of Information Security

### Introduction

Many of the topics information technology students study in school carry directly from the classroom to the workplace. For example, new programming and systems analysis and design skills can often be applied on new systems-development projects as companies espouse cloud computing and mobile infrastructures that access internal systems.

Security is a little different. Although their technical skills are certainly important, the best security specialists combine their practical knowledge of computers and networks with general theories about security, technology, and human nature. These concepts, some borrowed from other fields, such as military defense, often take years of (sometimes painful) professional experience to learn. With a conceptual and principled view of information security, you can analyze a security need in the right frame of reference or context so you can balance the needs of permitting access against the risk of allowing such access. No two systems or situations are identical, and no cookbooks can specify how to solve certain security problems. Instead, you must rely on principle-based analysis and decision making.

This chapter introduces these key information security principles, concepts, and durable “truths.”

**Principle 1: There Is No Such Thing as Absolute Security**

In 2003, the art collection of the Whitworth Gallery in Manchester, England, included three famous paintings by Van Gogh, Picasso, and Gauguin. Valued at more than $7 million, the paintings were protected by closed-circuit television (CCTV), a series of alarm systems, and 24-hour rolling patrols. Yet in late April 2003, thieves broke into the museum, evaded the layered security system, and made off with the three masterpieces. Several days later, investigators discovered the paintings in a nearby public restroom along with a note from the thieves saying, “The intention was not to steal, only to highlight the woeful security.”

The burglars’ lesson translates to the information security arena and illustrates the first principle of information security (IS): Given enough time, tools, skills, and inclination, a malicious person can break through any security measure. This principle applies to the physical world as well and is best illustrated with an analogy of safes or vaults that businesses commonly use to protect their assets. Safes are rated according to their resistance to attacks using a scale that describes how long it could take a burglar to open them. They are divided into categories based on the level of protection they can deliver and the testing they undergo. Four common classes of safe ratings are B-Rate, C-Rate, UL TL-15, and UL TL-30:

- **B-Rate:** B-Rate is a catchall rating for any box with a lock on it. This rating describes the thickness of the steel used to make the lockbox. No actual testing is performed to gain this rating.

- **C-Rate:** This is defined as a variably thick steel box with a 1-inch-thick door and a lock. No tests are conducted to provide this rating, either.

- **UL TL-15:** Safes with an Underwriters Laboratory (UL) TL-15 rating have passed standardized tests as defined in UL Standard 687 using tools and an expert group of safe-testing engineers. The UL TL-15 label requires that the safe be constructed of 1-inch solid steel or equivalent. The label means that the safe has been tested for a net working time of 15 minutes using “common hand tools, drills, punches hammers, and pressure applying devices.” *Networking time* means that when the tool comes off the safe, the clock stops. Engineers exercise more than 50 different types of attacks that have proven effective for safecracking.

- **UL TL-30:** UL TL-30 testing is essentially the same as the TL-15 testing, except for the networking time. Testers get 30 minutes and a few more tools to help them gain access. Testing engineers usually have a safe’s manufacturing blueprints and can disassemble the safe before the test begins to see how it works.

## Confidentiality

*Confidentiality is sometimes referred to as the* ***principle of least privilege, meaning that users should be given only enough privilege to perform their duties, and no more****. Some other synonyms for confidentiality you might encounter include privacy, secrecy, and discretion.*

“Security Architecture and Design,” security testing of hardware and software systems employs many of the same concepts of safe testing, using computers and custom-developed testing software instead of tools and torches. The outcomes of this testing are the same, though: As with software, no safe is burglar proof; security measures simply buy time. Of course, buying time is a powerful tool. Resisting attacks long enough provides the opportunity to catch the attacker in the act and to quickly recover from the incident. This leads to the second principle.

FYI: Confidentiality Models

Confidentiality models are primarily intended to ensure that no unauthorized access to information is permitted and that accidental disclosure of sensitive information is not possible. Common confidentiality controls are user IDs and passwords.

## Confidentiality, Integrity, and Availability

**Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability**

All information security measures try to address at least one of three goals:

- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorized use

These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs. Information security professionals who create policies and procedures (often referred to as governance models) must consider each goal when creating a plan to protect a computer system.

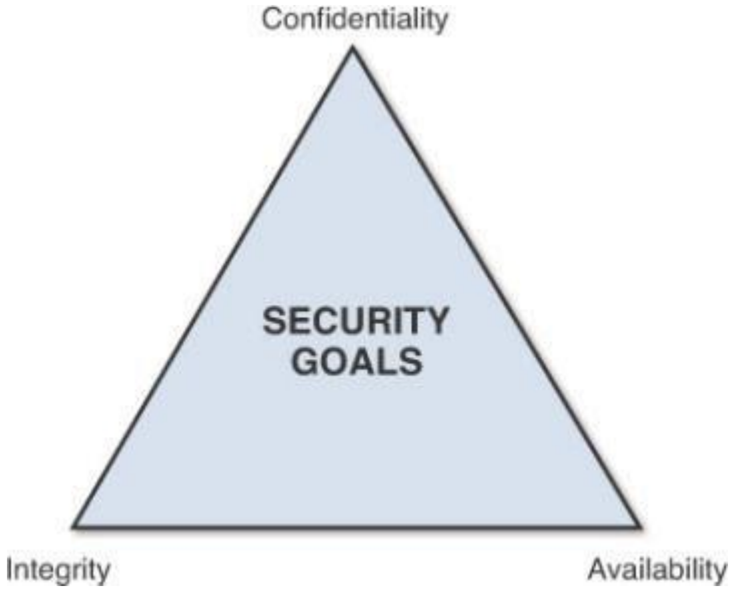


Figure 1.11The CIA triad.

The principle of information security protection of confidentiality, integrity, and availability cannot be overemphasized: This is central to all studies and practices in IS. You’ll often see the term *CIA triad* to illustrate the overall goals for IS throughout the research, guidance, and practices you encounter.

**Integrity Models**

Integrity models keep data pure and trustworthy by protecting system data from intentional or accidental changes. Integrity models have three goals:

- Prevent unauthorized users from making modifications to data or programs
- Prevent authorized users from making improper or unauthorized modifications
- Maintain internal and external consistency of data and programs

An example of integrity checks is balancing a batch of transactions to make sure that all the information is present and accurately accounted for.

**Availability Models**

Availability models keep data and resources available for authorized use, especially during emergencies or disasters. Information security professionals usually address three common challenges to availability:

- Denial of service (DoS) due to intentional attacks or because of undiscovered flaws in implementation (for example, a program written by a programmer who is unaware of a flaw that could crash the program if a certain unexpected input is encountered)
- Loss of information system capabilities because of natural disasters (fires, floods, storms, or earthquakes) or human actions (bombs or strikes)
- Equipment failures during normal use

Some activities that preserve confidentiality, integrity, and/or availability are granting access only to authorized personnel, applying encryption to information that will be sent over the Internet or stored on digital media, periodically testing computer system security to uncover new vulnerabilities, building software defensively, and developing a disaster recovery plan to ensure that the business can continue to exist in the event of a disaster or loss of access by personnel.

**Principle 3: Defense in Depth as Strategy**

A bank would never leave its assets inside an unguarded safe alone. Typically, access to the safe requires passing through layers of protection that might include human guards and locked doors with special access controls. Furthermore, the room where the safe resides could be monitored by closed-circuit television, motion sensors, and alarm systems that can quickly detect unusual activity. The sound of an alarm might trigger the doors to automatically lock, the police to be notified, or the room to fill with tear gas.

Layered security, as in the previous example, is known as defense in depth. This security is implemented in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response. Defense in depth also seeks to offset the weaknesses of one security layer by the strengths of two or more layers.

In the information security world, defense in depth requires layering security devices in a series that protects, detects, and responds to attacks on systems. For example, a typical Internet-attached network designed with security in mind includes routers, firewalls, and intrusion detection systems (IDS) to protect the network from would-be intruders;

employs traffic analyzers and real-time human monitors who watch for anomalies as the network is being used to detect any breach in the layers of protection; and relies on automated mechanisms to turn off access or remove the system from the network in response to the detection of an intruder.

Finally, the security of each of these mechanisms must be thoroughly tested before deployment to ensure that the integrated system is suitable for normal operations. After all, a chain is only as good as its weakest link.

In Practice: Phishing for Dollars

Phishing is another good example of how easily intelligent people can be duped into breaching security. Phishing is a dangerous Internet scam, and is becoming increasingly dangerous as targets are selected using data available from social media and enable a malicious person to build a profile of the target to better convince him the scam is real. A phishing scam typically operates as follows:

- The victim receives an official-looking email message purporting to come from a trusted source, such as an online banking site, PayPal, eBay, or other service where money is exchanged, moved, or managed.
- The email tells the user that his or her account needs updating immediately or will be suspended within a certain number of days.
- The email contains a URL (link) and instructs the user to click on the link to access the account and update the information. The link text appears as though it will take the user to the expected site. However, the link is actually a link to the attacker's site, which is made to look exactly like the site the user expects to see.
- At the spoofed site, the user enters his or her credentials (ID and password) and clicks Submit.
- The site returns an innocuous message, such as "We're sorry—we're unable to process your transaction at this time," and the user is none the wiser.
- At this point, the victim's credentials are stored on the attacker's site or sent via email to the perpetrator, where they can be used to log in to the *real* banking or exchange site and empty the account before the user knows what happened.

Phishing and resultant ID theft and monetary losses are on the increase and will begin to slow only after the cycle is broken through awareness and education. Protect yourself by taking the following steps:

- Look for telltale signs of fraud: Instead of addressing you by name, a phishing email addresses you as "User" or by your email address; a legitimate message from legitimate companies uses your name as they know it.
- Do not click on links embedded in unsolicited finance-related email messages. A link might look legitimate, but when you click on it, you could be redirected to the site of a phisher. If you believe that your account is in jeopardy, type in the known URL of the site in a new browser window and look for messages from the provider after you're logged in.
- Check with your provider for messages related to phishing scams that the company is aware of. Your bank or other financial services provider wants to make sure you don't fall victim and will often take significant measures to educate users on how to prevent problems.

### Principle 4: When Left on Their Own, People Tend to Make the Worst Security Decisions

The primary reason identity theft, viruses, worms, and stolen passwords are so common is that people are easily duped into giving up the secrets technologies use to secure systems. Organizers of Infosecurity Europe, Britain’s biggest information technology security exhibition, sent researchers to London’s Waterloo Station to ask commuters to hand over their office computer passwords in exchange for a free pen. Three-quarters of respondents revealed the information immediately, and an additional 15 percent did so after some gentle probing. Study after study like this one shows how little it takes to convince someone to give up their credentials in exchange for trivial or worthless goods.

**Principle 5: Computer Security Depends on Two Types of Requirements: Functional and Assurance**

Functional requirements describe what a system *should* do. Assurance requirements describe how functional requirements should be implemented and tested. Both sets of requirements are needed to answer the following questions:

- Does the system do the right things (behave as promised)?
- Does the system do the right things in the right way?

These are the same questions that others in noncomputer industries face with verification and validation. Verification is the process of confirming that one or more predetermined requirements or specifications are met. Validation then determines the correctness or quality of the mechanisms used to meet the needs. In other words, you can develop software that addresses a need, but it might contain flaws that could compromise data when placed in the hands of a malicious user.

Consider car safety testing as an example. Verification testing for seat belt functions might include conducting stress tests on the fabric, testing the locking mechanisms, and making certain the belt will fit the intended application, thus completing the functional tests. Validation, or assurance testing, might then include crashing the car with crash-test dummies inside to “prove” that the seat belt is indeed safe when used under normal conditions and that it can survive under harsh conditions.

With software, you need both verification and validation answers to gain confidence in products before launching them into a wild, hostile environment such as the Internet. Most of today’s commercial off-the-shelf (COTS) software and systems stop at the first step, verification, without bothering to test for obvious security vulnerabilities in the final product. Developers of software generally lack the wherewithal and motivation needed to try to break their own software. More often, developers test that the software meets the specifications in each function that is present but usually do not try to find ways to circumvent the software and make it fail. You learn more about security testing of software in Chapter 5.

**Principle 6: Security through Obscurity is Not an Answer**

Many people in the information security industry believe that if malicious attackers don’t know how software is secured, security is better. Although this might seem logical, it’s actually untrue. Security through obscurity means that hiding the details of the security mechanisms is sufficient to secure the system alone. An example of security through obscurity might involve closely guarding the written specifications for security functions and preventing all but the most trusted people from seeing it. Obscuring security leads to a false sense of security, which is often more dangerous than not addressing security at all.

If the security of a system is maintained by keeping the implementation of the system a secret, the entire system collapses when the first person discovers how the security mechanism works—and someone is always determined to discover these secrets. The better bet is to make sure no one mechanism is responsible for the security of the entire system. Again, this is defense in depth in everything related to protecting data and resources.

In Chapter 11, “Cryptography,” you’ll see how this principle applies and why it makes no sense to keep an algorithm for cryptography secret when the security of the system should rely on the cryptographic keys used to protect data or authenticate a user. You can also see this in action with the open-source movement: Anyone can gain access to program (source) code, analyze it for security problems, and then share with the community improvements that eliminate vulnerabilities and/or improve the overall security through simplification (see Principle 9).

**Principle 7: Security = Risk Management**

It’s critical to understand that spending more on securing an asset than the intrinsic value of the asset is a waste of resources. For example, buying a $500 safe to protect $200 worth of jewelry makes no practical sense. The same is true when protecting electronic assets. All security work is a careful balance between the level of risk and the expected reward of expending a given amount of resources. Security is concerned not with eliminating all threats within a system or facility, but with eliminating known threats and minimizing losses if an attacker succeeds in exploiting vulnerability. Risk analysis and risk management are central themes to securing information systems. When risks are well understood, three outcomes are possible:

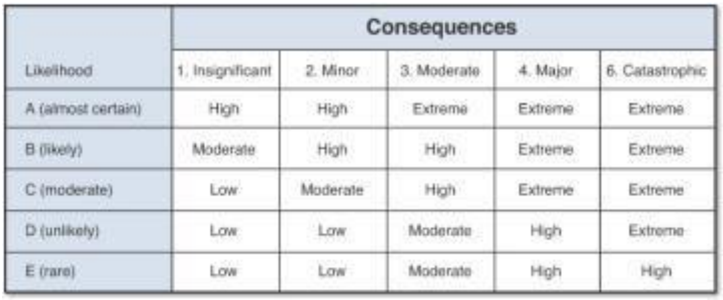
- The risks are mitigated (countered).
- Insurance is acquired against the losses that would occur if a system were compromised.
- The risks are accepted and the consequences are managed.

Risk assessment and risk analysis are concerned with placing an economic value on assets to best determine appropriate countermeasures that protect them from losses.

The simplest form of determining the degree of a risk involves looking at two factors:

- What is the consequence of a loss?
- What is the likelihood that this loss will occur?

Figure 1.12 illustrates a matrix you can use to determine the degree of a risk based on these factors.



|  | Consequences |  |  |  |  |
|---|---|---|---|---|---|
| Likelihood | 1. Insignificant | 2. Minor | 3. Moderate | 4. Major | 6. Catastrophic |
| A (almost certain) | High | High | Extreme | Extreme | Extreme |
| B (likely) | Moderate | High | High | Extreme | Extreme |
| C (moderate) | Low | Moderate | High | Extreme | Extreme |
| D (unlikely) | Low | Low | Moderate | High | Extreme |
| E (rare) | Low | Low | Moderate | High | High |

Figure 1.12 Consequences/likelihood matrix for risk analysis.

After determining a risk rating, one of the following actions could be required:

- **Extreme risk:** Immediate action is required.

- **High risk:** Senior management's attention is needed.
- **Moderate risk:** Management responsibility must be specified.
- **Low risk:** Management is handled by routine procedures.

In the real world, risk management is more complicated than simply making a human judgment call based on intuition or previous experience with a similar situation. Recall that every system has unique security issues and considerations, so it's imperative to understand the specific nature of data the system will maintain, what hardware and software will be used to deploy the system, and the security skills of the development teams. Determining the likelihood of a risk coming to life requires understanding a few more terms and concepts:

- Vulnerability
- Exploit
- Attacker

Vulnerability refers to a known problem within a system or program. A common example in InfoSec is called the buffer overflow or buffer overrun vulnerability. Programmers tend to be trusting and not worry about who will attack their programs, but instead worry about who will use their programs legitimately. One feature of most programs is the capability for a user to "input" information or requests. The program instructions (source code) then contain an "area" in memory (buffer) for these inputs and act upon them when told to do so. Sometimes the programmer doesn't check to see if the input is proper or innocuous. A malicious user, however, might take advantage of this weakness and overload the input area with more information than it can handle, crashing or disabling the program. This is called buffer overflow, and it can permit a malicious user to gain control over the system. This common vulnerability with software must be addressed when developing systems. Chapter 13, "Software Development Security," covers this in greater detail.

An exploit is a program or "cookbook" on how to take advantage of a specific vulnerability. It might be a program that a hacker can download over the Internet and then use to search for systems that contain the vulnerability it's designed to exploit. It might also be a series of documented steps on how to exploit the vulnerability after an attacker finds a system that contains it.

An attacker, then, is the link between a vulnerability and an exploit. The attacker has two characteristics: skill and will. Attackers either are skilled in the art of attacking systems or have access to tools that do the work for them. They have the will to perform attacks on systems they do not own and usually care little about the consequences of their actions.

In applying these concepts to risk analysis, the IS practitioner must anticipate who might want to attack the system, how capable the attacker might be, how available the exploits to a vulnerability are, and which systems have the vulnerability present.

Risk analysis and risk management are specialized areas of study and practice, and the IS professionals who concentrate in these areas must be skilled and current in their techniques. You can find more on risk management in Chapter 4, "Governance and Risk Management."

### Principle 8: The Three Types of Security Controls Are Preventative, Detective, and Responsive

Controls (such as documented processes) and countermeasures (such as firewalls) must be implemented as one or more of these previous types, or the controls are not there for the purposes of security. Shown in another triad, the principle of defense in depth dictates that a security mechanism serve a purpose by preventing a compromise, detecting that a compromise or compromise attempt is underway, or responding to a compromise while it's happening or after it has been discovered.

Referring to the example of the bank vault in Principle 3, access to a bank's safe or vault requires passing through layers of protection that might include human guards and locked doors with special access controls (prevention). In the room where the safe resides, closed-circuit televisions, motion sensors, and alarm systems quickly detect any unusual activity (detection). The sound of an alarm could trigger the doors to automatically lock, the police to be notified, or the room to fill with tear gas (response).

These controls are the basic toolkit for the security practitioner who mixes and matches them to carry out the objectives of confidentiality, integrity, and/or availability by using people, processes, or technology (see Principle 11) to bring them to life.

In Practice: How People, Process, and Technology Work in Harmony

To illustrate how people, process, and technology work together to secure systems, let's take a look a how the security department grants access to users for performing their duties. The process, called user access request, is initiated when a new user is brought into the company or switches department or role within the company. The user access request form is initially completed by the user and approved by the manager.

When the user access request is approved, it's routed to information security access coordinators to process using the documented procedures for granting access. After access is granted and the process for sharing the user's ID and password is followed, the system's technical access control system takes over. It protects the system from unauthorized access by requiring a user ID and password, and it prevents password guessing from an unauthorized person by limiting the number of attempts to three before locking the account from further access attempts.

In Practice: To Disclose or Not to Disclose—That Is the Question!

Having specific knowledge of a security vulnerability gives administrators the knowledge to properly defend their systems from related exploits. The ethical question is, how should that valuable information be disseminated to the good guys while keeping it away from the bad guys? The simple truth is, you can't really do this. Hackers tend to communicate among themselves far better than professional security practitioners ever could. Hackers know about most vulnerabilities long before the general public gets wind of them. By the time the general public is made aware, the hacker community has already developed a workable exploit and disseminated it far and wide to take advantage of the flaw before it can be patched or closed down.

Because of this, open disclosure benefits the general public far more than is acknowledged by the critics who claim that it gives the bad guys the same information.

Here's the bottom line: If you uncover an obvious problem, raise your hand and let someone who can do something about it know. If you see something, say something. You'll sleep better at night!

### Principle 9: Complexity Is the Enemy of Security

The more complex a system gets, the harder it is to secure. With too many "moving parts" or interfaces between programs and other systems, the system or interfaces become difficult to secure while still permitting them to operate as intended. You learn in Chapter 5 how complexity can easily get in the way of comprehensive testing of security mechanisms.

**Principle 10: Fear, Uncertainty, and Doubt Do Not Work in Selling Security**

At one time, "scaring" management into spending resources on security to avoid the unthinkable was effective. The tactic of fear, uncertainty, and doubt (FUD) no longer works: Information security and IT management is too mature. **Now IS managers must justify all investments in security using techniques of the trade. Although this makes the job of information security practitioners more difficult, it also makes them more valuable because of management's need to understand what is being protected and why.** When spending resources can be justified with good, solid business rationale, security requests are rarely denied.

**Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility**

As described in Principle 3, "Defense in Depth as Strategy," the information security practitioner needs a series of countermeasures and controls to implement an effective security system. One such control might be dual control, a practice borrowed from the military. The U.S. Department of Defense uses a dual control protocol to secure the nation's nuclear arsenal. This means that at least two on-site people must agree to launch a nuclear weapon. If one person were in control, he or she could make an error in judgment or act maliciously for whatever reason. But with dual control, one person acts as a countermeasure to the other: Chances are less likely that both people will make an error in judgment or act maliciously. Likewise, no one person in an organization should have the ability to control or close down a security activity. This is commonly referred to as separation of duties.

Process controls are implemented to ensure that different people can perform the same operations exactly in the same way each time. Processes are documented as procedures on how to carry out an activity related to security. The process of configuring a server operating system for secure operations is documented as one or more procedures that security administrators use and can be verified as done correctly.

Just as the information security professional might establish process controls to make sure that a single person cannot gain complete control over a system, you should never place all your faith in technology. Technology can fail, and without people to notice and fix technical problems, computer systems would stall permanently. An example of this type of waste is installing an expensive firewall system (a network perimeter security device that blocks traffic) and then turning around and opening all the ports that are intended to block certain traffic from entering the network.

**People, process, and technology controls** are essential elements of several areas of practice in information technology (IT) security, including operations security, applications development security, physical security, and cryptography. These three pillars of security are often depicted as a three-legged stool (see Figure 1.13).

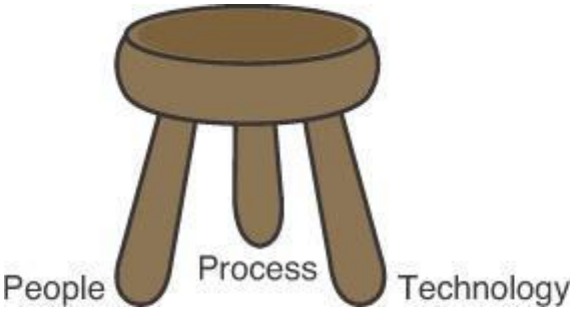


Figure 1.13 The people, process, and technology triad.

**Principle 12: Open Disclosure of Vulnerabilities Is Good for Security!**

A raging and often heated debate within the security community and software developing centers concerns whether to let users know about a problem before a fix or patch can be developed and distributed. Principle 6 tells us that security through obscurity is not an answer: Keeping a given vulnerability secret from users and from the software developer can only lead to a false sense of security. Users have a right to know about defects in the products they purchase, just as they have a right to know about automobile recalls because of defects. The need to know trumps the need to keep secrets, to give users the right to protect themselves.

## Information Classification and their Roles

An information classification process is a business decision process. Information is an asset of the organization, and managers have been charged with protecting and accounting for proper use of all assets. There are many reasons why any organization classifies the information. The main reason for classification is that all the information does not have the same level of importance. They are important for organization but at every level information has separate value. Information classification is the process of identifying and assigning predetermined levels of sensitivity to different types of information.

The benefits of information classification are as follows -

- The information classification helps to protect sensitive information.
- It helps identify which information is most sensitive or vital to an organization.
- Helps in fulfilling requirements toward regulatory compliance or legal mandates.
- Helps to Identify which information is most useful for the organization
- Helps in identifying which Protection applies to which information.
- It supports the Confidentiality, Integrity and Availability (CIA) in relation with data.

A classification level must be assigned to information when that information is determined to be classified. A classification level indicates the relative importance of classified information and thereby determines the specific requirements applicable to that information. Clearly defined classification levels are essential to an effective classification system.

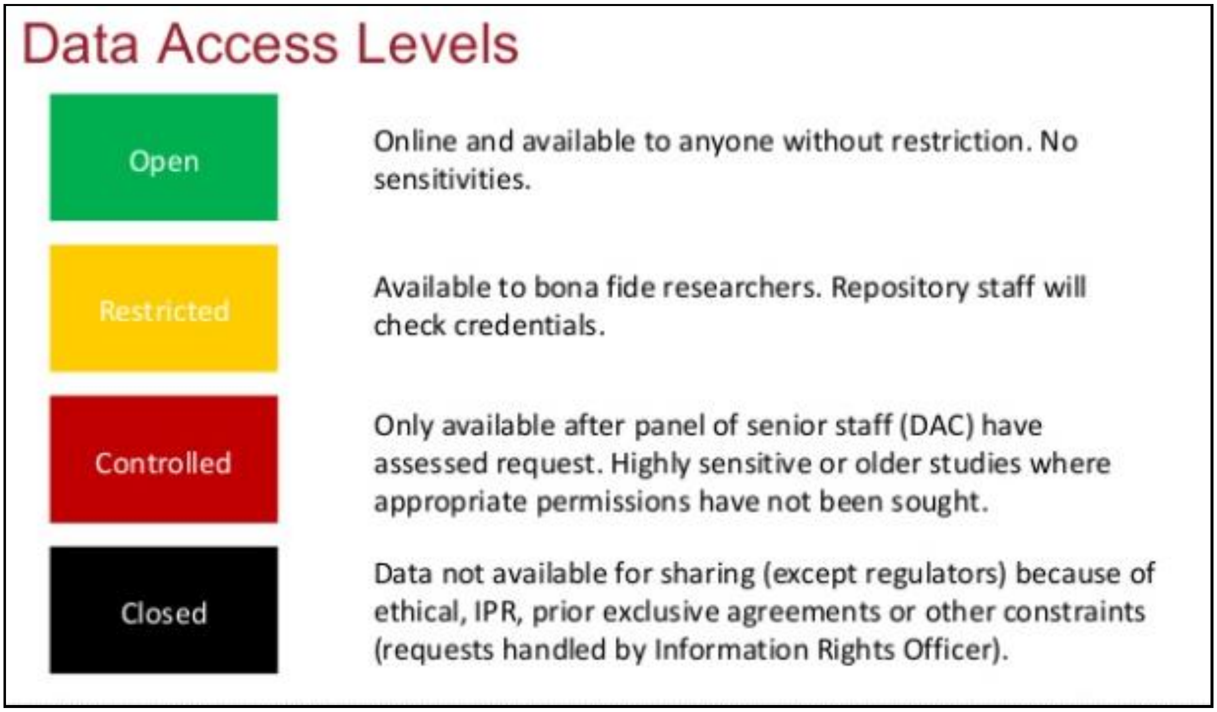
Several scheme for levels of data/ information classification, ranging from lowest to highest level of sensitivity:

1. Unclassified
2. Sensitive but unclassified
3. Confidentiality
4. Secret
5. Top secret

Some of the information classification in case of private organizations are as follows

1. Public
2. Sensitive
3. Private

The figure 1.14 represents the different data/information access levels used in information security programs.



## Data Access Levels

| | |
|---|---|
| Open | Online and available to anyone without restriction. No sensitivities. |
| Restricted | Available to bona fide researchers. Repository staff will check credentials. |
| Controlled | Only available after panel of senior staff (DAC) have assessed request. Highly sensitive or older studies where appropriate permissions have not been sought. |
| Closed | Data not available for sharing (except regulators) because of ethical, IPR, prior exclusive agreements or other constraints (requests handled by Information Rights Officer). |

Figure 1.14 Data/Information access levels

For example

**Example (a)** National Security Information (hereinafter "classified information") shall be classified at one of the following three levels:

> (1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.
>
> (2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.
>
> (3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

The appropriate classification level would be expected to usually be determined by the information disclosure risks because those risks largely determine the magnitude of the net damage that could be caused by such disclosure. Generally, the benefits of information disclosure are expected to be on the order of magnitude of the confidential level of damage. Therefore, the difficult balancing situations will usually occur when information disclosure damage is at the confidential level because then the benefits and risks are expected to be about equal. When information disclosure risks are at the serious or extremely grave levels associated with Secret or Top Secret information, respectively, then the classification levels would usually be expected to be determined solely by those damages. It would be rare that the information disclosure benefits would approximate those significantly higher serious or extremely grave damage levels.

**Example (b)** In case of International Service Provider a total five categories are used in classifying information. These are

1) **Top Secret**-Information that, if disclosed, could cause severe impact to the company's competitive advantage or business strategies.

2) **Confidential**-Information that, if disclosed, could violate the privacy of individuals, reduce competitive advantage, or damage the company.

3) **Restricted**-Information that is available to a specific subset of the employee population when conducting company business.

4) **Internal Use**-Information that is intended for use by all employees when conducting company business.

5) **Public**-Information that has been made available to the public through authorized company channels.

**Information Classification: Various Roles**

From the security perspective, the roles and responsibilities of all participants in the information classification program must be clearly defined. The roles that owner, custodian and user play in information classification are described along with their responsibilities.

**Role**

1. **Owner**

An information owner may be an executive or manager of an organization. An owner is different from a custodian. The owner has final corporate responsibility of data protection, and under the concept of due care, the owner may be liable for negligence because of the failure to protect this data.

**Responsibilities**

This person is responsible for the information asset(s) that must be protected. In particular, the responsibilities of an information owner include the following:

1. Making the original decision as to what level of classification the information requires based on the business needs for the protection of the data

2 reviewing the classification assignments periodically and making alterations as the business needs change

3 delegating the responsibility of the data protection duties to the custodian.

**2. Custodian**

An information custodian is the delegated personnel.

**Responsibilities**

The duties may include

1. Running regular backups and routinely testing the validity of the backup data
2. Performing data restoration from the backups when necessary.
3. Additionally duties of the custodian, may include being the administrator of the classification scheme.

**3. User**

An end user is considered to be an operator, responsible for protecting the information by its owner. Managers, executives and supervisory staff are also considered as users.

**Responsibilities**

The duties/ responsibilities may include

1. Users must follow the operating procedure guidelines as defined in organization security policy.
2. Users must take care to preserve the information security during their work.
3. Must prevent open view from occurring.
4. Users must use the company's computing resources only for company purposes, and not for personal use.

## Privacy of Data

Data privacy, also called information privacy, is the aspect of information technology (IT) that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties. The challenge of data privacy is to utilize data while protecting individual's privacy preferences and their personally identifiable information. The fields of computer security, data security, and information security design and utilize software, hardware, and human resources to address this issue. Since the laws and regulations related to Privacy and Data Protection are constantly changing, it is important to keep abreast of any changes in the law and to continually reassess compliance with data privacy and security regulations. Within academia, Institutional Review Boards function to assure that adequate measures are taken to insure both the privacy and confidentiality of human subjects in research. As heterogeneous information systems with differing privacy rules are interconnected and information is shared, policy appliances will be required to reconcile, enforce, and monitor an increasing amount of privacy policy rules (and laws). There are two categories of technology to address privacy protection in commercial IT systems: communication and enforcement.

Policy communication

P3P – The Platform for Privacy Preferences. P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.

Policy enforcement

XACML – The Extensible Access Control Markup Language together with its Privacy Profile is a standard for expressing privacy policies in a machine-readable language which a software system can use to enforce the policy in enterprise IT systems.

EPAL – The Enterprise Privacy Authorization Language is very similar to XACML, but is not yet a standard.

WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message. Protecting privacy on the internet On the internet many users give away a lot of information about themselves: unencrypted e-mails can be read by the administrators of an e-mail server, if the connection is not encrypted (no HTTPS), and also the internet service provider and other parties sniffing the network traffic of that connection are able to know the contents. The same applies to any kind of traffic generated on the Internet, including web browsing, instant messaging, and others. In order not to give away too much personal information, e-mails can be encrypted and browsing of web pages as well as other online activities can be done traceless via anonymizers, or by open source distributed anonymizers, so-called mix networks. Well known open-source mix nets include I2P – The Anonymous Network and Tor. Improving privacy through individualization Computer privacy can be improved through individualization. Currently security messages are designed for the "average user", i.e. the same message for everyone. Researchers have posited that individualized messages and security "nudges", crafted based on users' individual differences and personality traits, can be used to further improve each person's compliance with computer security and privacy.

# UNIT II

# Networks and E-Security

**Internet Protocol:** The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying data grams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

Historically, IP was the connectionless datagram service in the original *Transmission Control Program* introduced by Vint Cerf and Bob Kahn in 1974; the other being the connection-oriented Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6).

## What is Internet Protocol (IP)?

IP (short for Internet Protocol) specifies the technical format of packets and the addressing scheme for computers to communicate over a network. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself can be compared to something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

## TCP/IP

Short for **Transmission Control Protocol/Internet Protocol**, **TCP/IP** is a set of rules (protocols) governing communications among all computers on the Internet. More specifically, TCP/IP dictates how information should be packaged (turned into bundles of information called packets), sent, and received, as well as how to get to its destination. TCP/IP was developed in 1978 and driven by Bob Kahn and Vint Cerf**.**

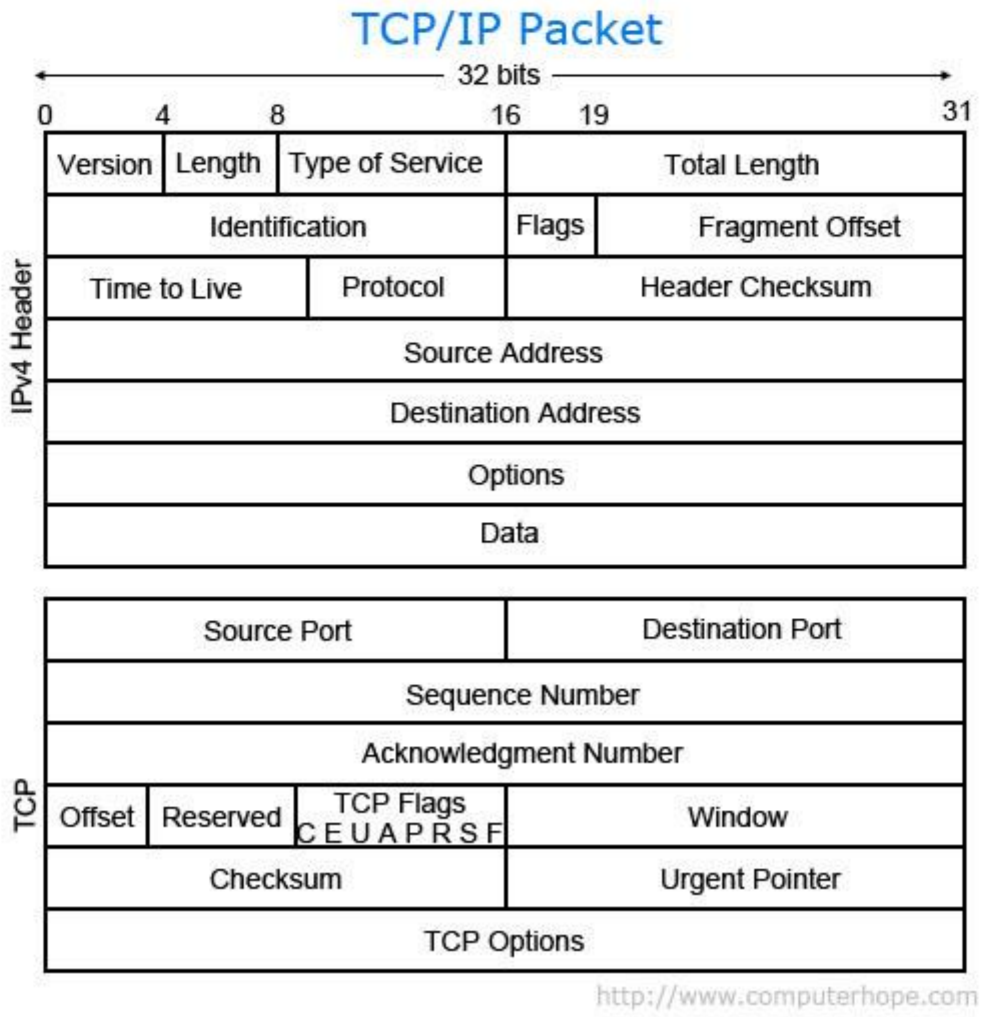


**Figure 2.1. TCP/IP Header**

### How does TCP/IP work?

As the name implies, TCP/IP is a combination of two separate protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). The Internet Protocol standard dictates the logistics of packets sent out over networks; it tells packets where to go and how to get there. IP has a method that lets any computer on the Internet forward a packet to another computer that is one or more intervals closer to the packet's recipient. You can think of it like workers in a line passing boulders from a quarry to a mining cart.

The Transmission Control Protocol is responsible for ensuring the reliable transmission of data across Internet-connected networks. TCP checks packets for errors and submits requests for re-transmissions if any are found.

### Three of the most common TCP/IP protocols

- **HTTP** - Used between a web client and a web server, for *non-secure* data transmissions. A web client (i.e. Internet browser on a computer) sends a request to a web server to view a web page. The web server receives that request and sends the web page information back to the web client.

- **HTTPS** - Used between a web client and a web server, for *secure* data transmissions. Often used for sending credit card transaction data or other private data from a web client (i.e. Internet browser on a computer) to a web server.
- **FTP** - Used between two or more computers. One computer sends data to or receives data from another computer directly.

**Domain names and TCP/IP addresses**

The TCP/IP address for a website or web server is typically not easy to remember. To remedy this issue, a domain name is used instead. For example, **45.79.151.23** is the IP address for the Computer Hope website and **computerhope.com** is the domain name. Using this method, instead of a set of numbers, makes it much easier for users to remember Computer Hope's web address.

## Internet Protocol Versions

There are currently two version of Internet Protocol (IP): ***IPv4*** and a new version called ***IPv6.*** IPv6 is an evolutionary upgrade to the Internet Protocol. IPv6 will coexist with the older IPv4 for some time.

**What is IPv4 -- Internet Protocol Version 4?**

IPv4 (*Internet **P**rotocol **V**ersion **4***) is the fourth revision of the Internet Protocol (IP) used to to identify devices on anetwork through an addressing system. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks *(see RFC:791*).

IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bitaddress scheme allowing for a total of 2^32 addresses (just over 4 billion addresses). With the growth of the Internet it is expected that the number of unused IPv4 addresses will eventually run out because every device -- including computers, smartphones and game consoles -- that connects to the Internet requires an address.

A new Internet addressing system Internet Protocol version 6 (IPv6) is being deployed to fulfill the need for more Internet addresses.

**What is IPv6 -- Internet Protocol Version 6?**

IPv6 (*Internet **P**rotocol **V**ersion **6***) is also called IPng (*Internet **P**rotocol **n**ext **g**eneration*) and it is the newest version of the Internet Protocol (IP) reviewed in the IETF standards committees to replace the current version of IPv4 (Internet Protocol Version 4).

IPv6 is the successor to Internet Protocol Version 4 (IPv4). It was designed as an evolutionary upgrade to the Internet Protocol and will, in fact, coexist with the older IPv4 for some time. IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted.

IPv6 is often referred to as the "next generation" Internet standard and has been under development now since the mid-1990s. IPv6 was born out of concern that the demand for IP addresses would exceed the available supply.

While increasing the pool of addresses is one of the most often-talked about benefit of IPv6, there are other important technological changes in IPv6 that will improve the IP protocol:

- No more NAT (Network Address Translation)
- Auto-configuration
- No more private address collisions
- Better multicast routing
- Simpler header format
- Simplified, more efficient routing
- True quality of service (QoS), also called "flow labeling"
- Built-in authentication and privacy support
- Flexible options and extensions
- Easier administration (say good-bye to DHCP)

The following table lists the important differences between IPv4 and IPv6.

**Table 1.1 IPV4 vs IPV6**

| IPv4 | IPv6 |
|---|---|
| **IPv4 addresses** are 32 bit length. | **IPv6 addresses** are 128 bit length. |
| **IPv4 addresses** are **binary numbers** represented in decimals. | **IPv6 addresses** are **binary numbers** represented in **hexadecimals**. |
| **IPSec** support is only optional. | Inbuilt **IPSec** support. |
| **Fragmentation** is done by sender and forwarding routers. | **Fragmentation** is done only by sender. |
| No packet flow identification. | Packet flow identification is available within the **IPv6 header** using the **Flow Label** field. |
| **Checksum field** is available in **IPv4 header** | No checksum field in **IPv6 header**. |
| **Options fields** are available in **IPv4 header**. | No option fields, but **IPv6 Extension headers** are available. |
| Address Resolution Protocol (ARP) is available to mapIPv4 addresses to MAC addresses. | **Address Resolution Protocol (ARP)** is replaced with a function of**Neighbor Discovery Protocol (NDP)**. |

| | |
|---|---|
| Internet Group Management Protocol (IGMP) is used to manage multicast group membership. | IGMP is replaced with Multicast Listener Discovery (MLD) messages. |
| **Broadcast messages** are available. | **Broadcast messages** are not available. Instead a link-local scope "All nodes" **multicast IPv6 address** (FF02::1) is used for broadcast similar functionality. |
| Manual configuration (Static) of **IPv4 addresses** or DHCP (Dynamic configuration) is required to configure **IPv4 addresses**. | Auto-configuration of addresses is available. |

## FUNCTIONS OF VARIOUS NETWORKING COMPONENTS

Computer networks share common devices, functions, and features including servers, clients, transmission media, shared data, shared printers and other hardware and software resources, network interface card(NIC), local operating system(LOS), and the network operating system (NOS).

To function, any network must contain four components: (1) transmission media (cables or radio waves) to connect and establish communication between nodes, (2) network adapters that allow the nodes on the network to communicate, (3) network navigation devices (such as routers and switches) that move data around the network, and (4) software that allows the network to run.

### Connecting Devices - Hub, Repeater, Switch, Bridge, Router, Gateway

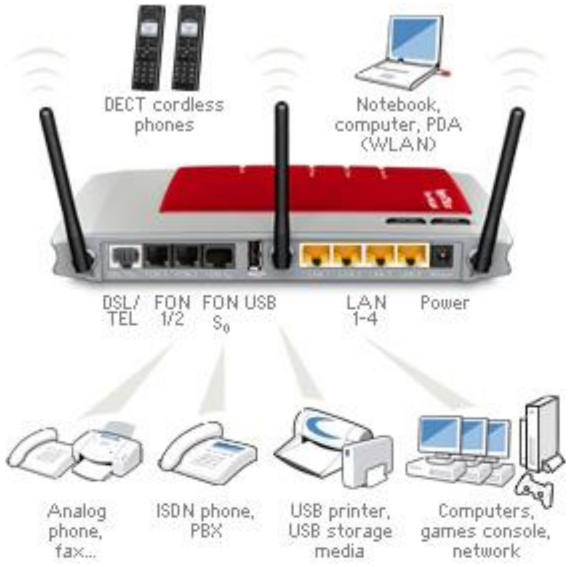


**Figure 1.2 . Switches**

To understand what connecting devices are, it is important to know about Backbone Networks. Backbone Network is a means of connecting 2 LAN's. It provides a transmission channel for packets from being transmitted from one LAN to the other. The individual LAN's are connected to the Backbone Network by using some types of devices such as Hubs, Repeaters, Switches, Bridges, Routers and Gateways.

Although these terms sound familiar, not many of us know the purpose of using these devices difference between these devices. Hence, it is very important to know the basic function of these devices in order to decide upon the device that is to be used for a particular purpose.

**Hub**

A hub works in the physical layer of the OSI model. It is basically a non-intelligent device, and has no decision making capability. What a Hub basically does is take the input data from one of the ports and broadcast the information to all the other ports connected to the network.

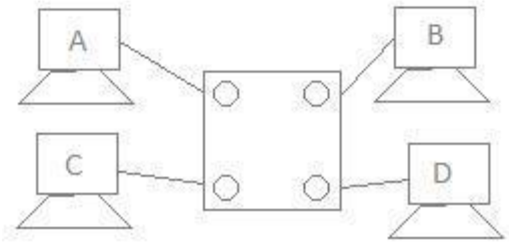


**Figure 1.3: Four port network**

To demonstrate its working, consider a 4 port network as shown in Fig 1. There are 4 computers connected to the 4 ports. Suppose, if Computer A wants to send some data to Computer B using a Hub, then, Computer A broadcasts the data on the network, and Computer B, being connected to the network, has access to the data. But, in this case all the other ports connected to the network has access to the data that is being transmitted by Computer A. This happens because, the Hub works in the Physical Layer and hence it does not know about the MAC addresses of the ports connected to the network. So, there is a lack of security in the Hub.

**Figure 1.4: USB Hub**

The picture shows a USB Hub, wherein the data is fed into the input port and is broadcasted to all the other 4 ports. The Network Hubs are outdated and are out of the market.

## Repeater

A repeater is a device similar to the Hub, but has additional features. It also works in the Physical layer. The repeaters are used in places where amplification of input signal is necessary. But, the kind of amplification done by the repeater is different from the regular amplification by amplifiers. The regular amplifies everything fed into it. That means, if the input signal has noise induced into it, both the desired signal and noise signal are together amplified. But, in the case of a repeater, it regenerates the input signal, and amplifies only the desirable signal. Hence, the noise component of the signal is eliminated.

**Figure 1.5 . Repeater**

The repeaters are necessary since, during the transmission of the signals over long distances, the signal has attenuation, delay distortions and noise, which lead in loss of data. Hence, in order to prevent this, the regenerative repeaters are used. Hence, the repeater regenerates the faded signal. In addition, it has all the features of a Hub. One common problem between the repeaters and the Hubs are that only one transmission can take place on the network at a particular time. If multiple devices transmit data simultaneously, there will be data collision.

### Switch

A switch is an intelligent device that works in the data link layer. The term intelligent refers to the decision making capacity of the Switch. Since it works in the Data link layer, it has knowledge of the MAC addresses of the ports in the network.

**Figure 1.6 . Switch**

Hence, in the Fig 1, if data has to be sent from Computer A to Computer B, then, the data is transferred to the Computer B only, and not to any other computers connected on the network. Hence, it establishes a link between the sender and the receiver based on the MAC addresses. This also means that when data is being sent from A to B, Computer C can establish a link with Computer D and communication can take place between them. So, simultaneous data transfer is possible in a switch. Also, Hub divides bandwidth, but a Switch does not.It is also to be noted that a switch is a secure device, because it sends information only to the desired destinations, and also certain security features such as firewalls can be implemented in the Switches.

### Bridge

A bridge is also a device which works in the Data Link Layer, but is more primitive when compared to a switch. Initial bridges were used to connect only 2 LAN's, but the most recent ones perform similar operation as the switches. It also works on the principle of transfer of information using the MAC addresses of the ports.

**Figure 1.7. Bridge**

It can be noted is that the normal ADSL modem can be connected via bridging also. The only difference is that, when bridging is used, each time the device has to be connected to the internet, it has to dial to the internet and establish a connection. Also, a bridge alone cannot be used to connect to the internet, because, the bridge works in the Data Link Layer, and has no knowledge of the IP Addresses, which are used in the Internet.

### Router

Any computer can be connected to the internet via MODEM, which performs the MODulation and the DEModulation operations. But, when there are more than one computer at home or in an organization, and you have a single internet connection, you need a Router. Router is a device which is used when multiple devices need to connect to the Internet using the same IP.

Any Internet Service Provider (ISP) provides a single IP, and especially for personal use, the IP address is assigned dynamically. This is done because, suppose, an ISP has 1000 IP addresses, it does not mean that it has 1000 customers. An ISP assumes that not all devices will be connected to the internet at the same time. Hence, when a user wants to access the internet, any IP address from the pool of IP addresses from the ISP will be assigned to connect the user to the internet.

**Figure 1.8. Router**

Hence, the router does the job of connecting multiple devices in a LAN to the internet using the same IP address. Since the router works in the Network Layer, it does forwarding on the basis of IP addresses.The WiFi routers that are commonly used now are the IEEE 802.11 b/g standard router, which is explained below.

## IEEE 802.11

IEEE 802.11 is a standard for WiFi. There are several different technologies/ generations that have been implemented. As mentioned, the recent modems are IEEE 802.11 b/g modems. The word b/g has the meaning as follows:

An IEEE 802.11 b standard uses 2.4GHz band and has a maximum transfer rate of 11 Mbps, while the IEEE 802.11 g standard uses 2.4 GHz band and has maximum transfer rate of 54 Mbps. Thus the b/g modem refers to a dual bandwidth modem, which is compatible with both the b and g standards. The standards are mainly differentiated based on the distance and speed of data transfer.The more recent IEEE 802.11 N standard has the capability to provide speeds of over 100 Mbps. It basically uses multiple wireless signals and antennas, and has increased signal intensity in order to be able to provide network for greater distances. It employs MIMO technology, wherein spatial encoding is used. The spatial pre-coding is done at the transmitter and the post-coding is done at the receiver. Recently, Reliance

Communications was in news for implementing MIMO technology to improve its 3G data transfer speeds.

**Brouter**

Brouter (Bridging Router) is a device which has two functions. Brouter acts as a router for known protocols (known by the router and those on the network) and hence works in the network layer. For data packets with unknown protocols, it acts as a bridge by connecting two different networks which is the function of a bridge - and this works in the data-link layer.

**Gateway**

The Gateway devices work in the Transport layer and above, where the different network technologies are implemented. A gateway is necessary when there are different technologies implemented by the different LAN's which are to be connected together.

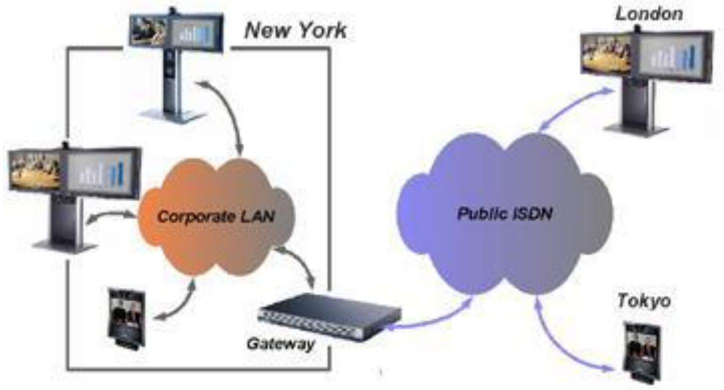


**Figure 1.9. Gateway function**

The Figure 1.9 shows the working of a gateway. Consider 2 networks, say in New York, and a network in London. If data has to be sent from one place to another, we need to ensure that the network technologies that are being used by both the networks are the same. If not, we need to use a Gateway.

In the more common example, we use a telephone network and internet networks, which works on different technologies. The telephone network follows the ISDN, and the Internet follows the IP. Here, 2 different technologies are being used. In this case, the router fails to work, since the router cannot understand the functionalities of both the networks. Hence, we require a Gateway, which acts as a translator in communicating between the 2 networks.

## MODULATION TECHNIQUES

Modulation is a process of changing the characteristics of the wave to be transmitted by superimposing the message signal on the high-frequency signal. In this process video, voice and other data signals modify high-frequency signals – also known as the carrier wave. This carrier wave can be DC or AC or pulse chain depending on the application used. Usually, a high-frequency sine wave is used as a carrier wave signal.

These modulation techniques are classified into two major types: analog and digital or pulse modulation. Prior to discussing further the different types of modulation techniques, let us understand the importance of modulation.

**Need for modulation**

- In the modulation technique, the message signal frequency is raised to a range so that it is more useful for transmission. The following points describe modulation's importance in the communication system.
- In signal transmission, the signals from various sources are transmitted through a common channel simultaneously by using multiplexers. If these signals are transmitted simultaneously with a certain bandwidth, they cause interference. To overcome this, speech signals are modulated to various carrier frequencies in order for the receiver to tune them to the desired bandwidth of his own choice within the range of transmission.
- Another technical reason is antenna size; the antenna size is inversely proportional to the frequency of the radiated signal. The order of the antenna aperture size is at least one by a tenth of the wavelength of the signal. Its size is not practicable if the signal is 5 kHz; therefore, raising frequency by modulating process will certainly reduce the height of the antenna.
- Modulation is important to transfer the signals over large distances since it is not possible to send low-frequency signals for longer distances.
- Similarly, modulation is also important to allocate more channels for users and to increase noise immunity.

**Working Principle of modulation**

Information can be added to the carrier by varying its amplitude, frequency, phase, polarization -- for optical signals -- and even quantum-level phenomena like spin.

Modulation is usually applied to electromagnetic signals: radio waves, lasers/optics and computer networks. Modulation can even be applied to a direct current -- which can be treated as a degenerate carrier wave with a fixed amplitude and frequency of 0 Hz -- mainly by turning it on and off, as in Morse code telegraphy or a digital current loop interface. The special case of no carrier -- a response message indicating an attached device is no longer connected to a remote system -- is called baseband modulation.

Modulation can also be applied to a low-frequency alternating current -- 50-60 Hz -- as with powerline networking.

## Types of modulation

The two types of modulation: analog and digital modulation techniques have already been discussed. In both the techniques, the baseband information is converted to Radio Frequency signals, but in analog modulation, these RF communication signals are a continuous range of values, whereas in digital modulation these are prearranged discrete states.

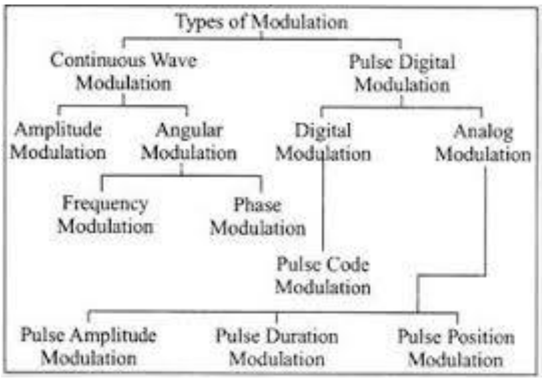


**Figure 1.10. Types of Modulation**

### Analog Modulation

In this modulation, a continuously varying sine wave is used as a carrier wave that modulates the message signal or data signal. The Sinusoidal wave's general function is shown in the figure below, in which, three parameters can be altered to get modulation – they are mainly amplitude, frequency, and phase, so the **types of analog modulation** are:

- Amplitude modulation (AM)
- Frequency modulation (FM)
- Phase modulation (PM)

In **amplitude modulation**, the amplitude of the carrier wave is varied in proportion to the message signal, and the other factors like frequency and phase remain constant. The modulated signal is shown in the below figure, and its spectrum consists of a lower frequency band, upper-frequency band, and carrier frequency components. This type of modulation requires greater bandwidth, more power. Filtering is very difficult in this modulation.

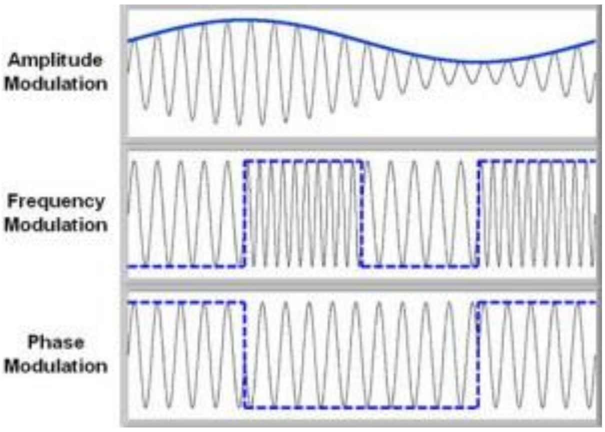


**Figure 1.11Types of Analog Modulation**

**Frequency modulation** (FM) varies the frequency of the carrier in proportion to the message or data signal while maintaining other parameters constant. The advantage of FM over AM is the greater suppression of noise at the expense of bandwidth in FM. It is used in applications like radio, radar, telemetry seismic prospecting, and so on. The efficiency and bandwidths depend on the modulation index and maximum modulating frequency.

In **phase modulation**, the carrier phase is varied in accordance with the data signal. In this type of modulation, when the phase is changed it also affects the frequency, so this modulation also comes under frequency modulation.

Analog modulation (AM, FM, and PM) is more sensitive to noise. If noise enters into a system, it persists and gets carried till the end receiver. Therefore, this drawback can be overcome by the digital modulation technique.

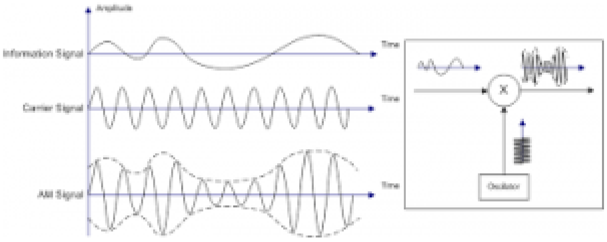


**Figure1.12 Amplitude Modulation**

## Digital Modulation

For better quality and efficient communication, the digital modulation technique is employed. The main advantages of digital modulation over analog modulation include permissible power, available bandwidth, and high noise immunity. In digital modulation, a message signal is converted from analog to digital message and then modulated by using a carrier wave.

The carrier wave is keyed or switched on and off to create pulses such that the signal is modulated. Similar to the analog, here the parameters like amplitude, frequency, and phase variation of the carrier wave decides the type of digital modulation.

The **types of digital modulation** are based on the type of signal and application used such as Amplitude Shift Keying, Frequency Shift Keying, Phase Shift Keying, Differential Phase Shift Keying, Quadrature Phase Shift Keying, Minimum Shift Keying, Gaussian Minimum Shift Keying, Orthogonal Frequency Division Multiplexing, etc., as shown in the figure.

Amplitude shift keying changes the amplitude of the carrier wave based on the baseband signal or message signal, which is in digital format. It is used for low-band requirements and is sensitive to noise.

In frequency-shift keying, the frequency of the carrier wave is varied for each symbol in the digital data. It needs larger bandwidths as shown in the figure. Similarly, the phase shift keying changes the phase of the carrier for each symbol and it is less sensitive to noise.

### Frequency Modulation

In order to create a frequency modulated wave, the frequency of the radio wave is varied in accordance with the amplitude of the input signal.

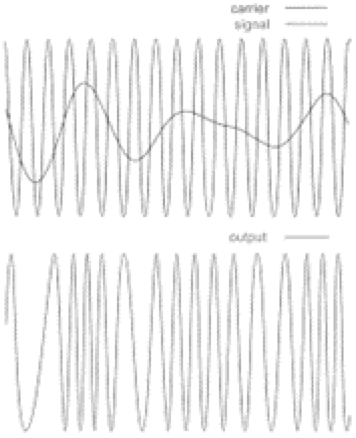


**Figure 1.13 Frequency Modulation**

When the audio wave is modulated with that of the radio frequency carrier signal, then the generated frequency signal will change its frequency level. The variation by which the wave moves upward and downward is to be noted. This is termed as deviation and is generally represented as kHz deviation.

As an instance, when the signal has a deviation of either + or – 3kHz, then it is represented as ±3kHz. This means that the carrier signal has up and downward deviation of 3kHz.

Broadcasting stations that need very high-frequency range in the frequency spectrum (in the range of 88.5 – 108 MHz), they need certainly a large amount of deviation which is nearly ±75 kHz. This is called wide-band frequency modulation. The signals in this range hold the ability to assist the high quality of transmissions, whereas they require higher bandwidth too. In general, 200kHz is permitted for every WBFM. And for narrowband FM, a deviation of ±3 kHz is enough.

While implementing an FM wave, it is more beneficial to know the effectivity range of the modulation. This stands as the parameter in stating factors such as knowing the type of signal whether wide band or narrow band FM signal. It also helps in making sure that the whole receivers or transmitters that are in the system are programmed to adapt to the standardized range of modulation as this shows an impact on the factors such as the channel spacing, bandwidth of the receiver, and others.

So, to signify the modulation level, modulation index and deviation ratio parameters are to be determined.

The different **types of frequency modulation** include the following.

**Narrow band FM**

- This is termed as the type of frequency modulation where the modulation index value is too minimal.
- When the modulation index value is < 0.3, then there will be an only carrier and corresponding sidebands having bandwidth as twice the modulating signal. So, $\beta \leq 0.3$ is called narrow band frequency modulation.
- The maximum range of modulating frequency is of 3 kHz
- The maximum frequency deviation value is 75 kHz

**Wide band FM**

- This is termed as the type of frequency modulation where the modulation index value is large.
- When the modulation index value is > 0.3, then there will be more than two sidebands having bandwidth as twice the modulating signal. When the modulation index value increases, then the number of sidebands gets increased. So, $\beta > 0.3$ is called narrow band frequency modulation.
- The maximum range of modulating frequencies is in between 30 Hz – 15 kHz
- The maximum frequency deviation value is 75 kHz

- This frequency modulation needs a higher bandwidth range which is almost 15 times ahead of the narrow band frequency modulation.

The other types of modulation techniques used in the communication system are:

- Binary phase shift keying
- Differential phase-shift keying
- Differential quadrature phase shift keying
- Offset quadrature phase shift keying
- Audio FSK
- Multi FSK
- Dual-tone FSK
- Minimum shift keying
- Gaussian minimum shift keying
- Trellis coded type of modulation

## Modulation and demodulation

Modulation is the process of encoding information in a transmitted signal, while demodulation is the process of extracting information from the transmitted signal. Many factors influence how faithfully the extracted information replicates the original input information. Electromagnetic interference can degrade signals and make the original signal impossible to extract. Demodulators typically include multiple stages of amplification and filtering in order to eliminate interference.

A device that performs both modulation and demodulation is called a modem -- a name created by combining the first letters of MOdulator and DEModulator.

A computer audio modem allows a computer to connect to another computer or to a data network over a regular analog phone line by using the data signal to modulate an analog audio tone. A modem at the far end demodulates the audio signal to recover the data stream. A cable modem uses network data to modulate the cable service carrier signal.

Sometimes a carrier signal can carry more than one modulating information stream. Multiplexing combines the streams onto a single carrier -- e.g., by encoding a fixed-duration segment of one, then of the next, for example, cycling through all the channels before returning to the first -- a process called time-division multiplexing (TDM). Another form is frequency-division multiplexing (FDM), where multiple carriers of different frequencies are used on the same medium.

In another form, wavelength-division multiplexing (WDM) modulates multiple laser wavelengths/frequencies on long-haul fiber links to increase the total available bandwidth.

Why use modulation in communications?

Multiple carriers of different frequencies can often be transmitted over a single media, with each carrier being modulated by an independent signal. For example, Wi-Fi uses individual channels to simultaneously transmit data to and from multiple clients.

A carrier signal is used to reduce the wavelength for efficient transmission and reception. Because the optimum antenna size is one-half or one-quarter of a wavelength, an audio frequency of 3000 Hz would need a wavelength of 100 km and a 25-kilometer antenna. Instead, using an FM carrier of 100 MHz, with a wavelength of 3 meters, the antenna would only need to be 80 cm long.

## Modulation and duty cycle

In wireless communications, the duty cycle is the proportion of time that the wireless network transmits RF signals. The duty cycle is thus an important factor in assessing the electromagnetic radiation to which a person is exposed. The actual duty cycle can vary, depending on the data load on the network and the network speed. So, the duty cycle can be affected by whether the network is being used for VoIP, streaming videos or videos, etc.

### Advantages of Various Types of Modulation

For transmission purposes, the size of the antenna has to be very large before the modulation technique was not proposed. The level of communication gets restricted as there will be no long-distance communications having zero levels of distortions.

So, with the development of modulation, there are many benefits of utilizing communication systems. And the advantaged of modulation are:

- The size of the antenna can be lessened
- There happens no kind of signal consolidation
- The range of communication is enhanced
- There will be the possibility of multiplexing
- One can adjust bandwidth as per the requirements

- The quality of reception gets increased
- Better performance and effectiveness

**Applications of Various Types of Modulation**

There is an extensive range of various modulation techniques and those are:

- Implemented in music mixing, and magnetic tape recording systems
- To track EEG monitoring for newly born children
- Used in telemetry
- Used in radar
- FM broadcasting techniques

## Need for Security, Business Needs, Threats, Attacks, Legal, Ethical and Professional Issues.

### Business Needs First

Information security performs four important functions for an organization:

1. Protects the organization's ability to function
2. Enables the safe operation of applications implemented on the organization's IT systems.
3. Protects the data the organization collects and uses.
4. Safeguards the technology assets in use at the organization.

**1. Protecting the functionality of an organization**

- Decision makers in organizations must set policy and operate their organizations in compliance with the complex, shifting legislation that controls the use of technology.

**2. Enabling the safe operation of applications**

- Organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications
- The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly those applications that serve as important elements of the infrastructure of the organization.

### 3. Protecting data that organizations collect & use

- Protecting data in motion
- Protecting data at rest
- Both are critical aspects of information security.
- The value of data motivates attackers to seal, sabotage, or corrupts it.
- It is essential for the protection of integrity and value of the organization’s data

### 4. Safeguarding Technology assets in organizations

- Must add secure infrastructure services based on the size and scope of the enterprise.
- Organizational growth could lead to the need for **public key infrastructure,** PKI, an integrated system of software, encryption methodologies.

## Threats

To protect an organization’s information, you must

1. Know yourself

(i.e) be familiar wit the information to be protected, and the systems that store, transport and process it.

2. Know the threats you face

To make sound decisions about information security, management must be informed about the various threats facing the organization, its application, data and information systems.

A threat is an object, person, or other entity, that represents a constant danger to an asset.

## Threats to Information Security

| Categories of threat | | Examples |
|---|---|---|
| Acts of human error or failure | -- | Accidents, employee mistakes |
| Compromises to intellectual property | -- | Piracy, copyright infringement |
| Deliberate acts of espionage or trespass | -- | Unauthorized access and/or/data collection |
| Deliberate acts of information extortion | -- | Blackmail or information disclosure |
| Deliberate acts of sabotage or vandalism | -- | Destruction of systems or information |
| Deliberate acts of theft | -- | Illegal confiscation of equipment or information |
| Deliberate software attacks | -- | Viruses, worms, macros, denial-of-service |
| Forces of nature | -- | Fire, flood, earthquake, lightning |
| Deviations in quality of service | -- | ISP, power , or WAN service providers |

| | | |
|---|---|---|
| Technical hardware failures or errors | -- | Equipment failure |
| Technical software failures or errors | -- | Bugs, code problems, unknown loopholes |
| Technological obsolescence | -- | Antiquated or outdated technologies |

## Threats

### 1. Acts of Human Error or Failure:

- Acts performed without intent or malicious purpose by an authorized user.
- because of in experience ,improper training,
- Making of incorrect assumptions.

One of the greatest threats to an organization’s information security is the organization’s own employees.

- Entry of erroneous data
- accidental deletion or modification of data
- storage of data in unprotected areas.
- Failure to protect information

can be prevented with  
- Training  
- Ongoing awareness activities  
-Verification by a second party  
- Many military applications have robust, dual- approval controls built in .

### 2. Compromises to Intellectual Property

- is defined as the ownership of ideas and control over the tangible or virtual representation of those ideas.
- Intellectual property includes trade secrets, copyrights, trademarks, and patents.
- Once intellectual property has been defined and properly identified, breaches to IP constitute a threat to the security of this information.
- Organization purchases or leases the IP of other organizations.
- Most Common IP breach is the unlawful use or duplication of software based intellectual property more commonly known as **software Piracy**.
- Software Piracy affects the world economy.
- U.S provides approximately 80% of world’s software.

In addition to the laws surrounding software piracy, two watch dog organizations investigate allegations of software abuse.

1. Software and Information Industry Association (SIIA)  
   (i.e)Software Publishers Association
2. Business Software Alliance (BSA)

- Another effort to combat (take action against) piracy is the online registration process.

**3. Deliberate Acts of Espionage or Trespass**

- Electronic and human activities that can breach the confidentiality of information.
- When an unauthorized individual's gain access to the information an organization is trying to protect is categorized as act of espionage or trespass.
- Attackers can use many different methods to access the information stored in an information system.

1. Competitive Intelligence[use web browser to get information from market research]
2. Industrial espionage(spying)
3. Shoulder Surfing(ATM)

**Trespass**

- Can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.
- Sound principles of authentication & authorization can help organizations protect valuable information and systems.
- **Hackers->** "People who use and create computer software to gain access to information illegally"
- There are generally two skill levels among hackers.
- **Expert Hackers**-> Masters of several programming languages, networking protocols, and operating systems .
- **Unskilled Hackers**

**4. Deliberate Acts of information Extortion (obtain by force or threat)**

- Possibility of an attacker or trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement not to disclose the information.

**5. Deliberate Acts of sabotage or Vandalism**

- Destroy an asset or
- Damage the image of organization
- Cyber terrorism-Cyber terrorists hack systems to conduct terrorist activities through network or internet pathways.

**6. Deliberate Acts of Theft**

- Illegal taking of another's property-- is a constant problem.
- Within an organization, property can be physical, electronic, or intellectual.
- Physical theft can be controlled by installation of alarm systems.

- Trained security professionals.
- Electronic theft control is under research.

**7. Deliberate Software Attacks**

- Because of **malicious code** or **malicious software** or sometimes **malware.**
- These software components are designed to damage, destroy or deny service to the target system.
- More common instances are

  Virus, Worms, Trojan horses, Logic bombs, Backdoors.
- "The British Internet Service Provider Cloudnine" be the first business "hacked out of existence"

**Virus**

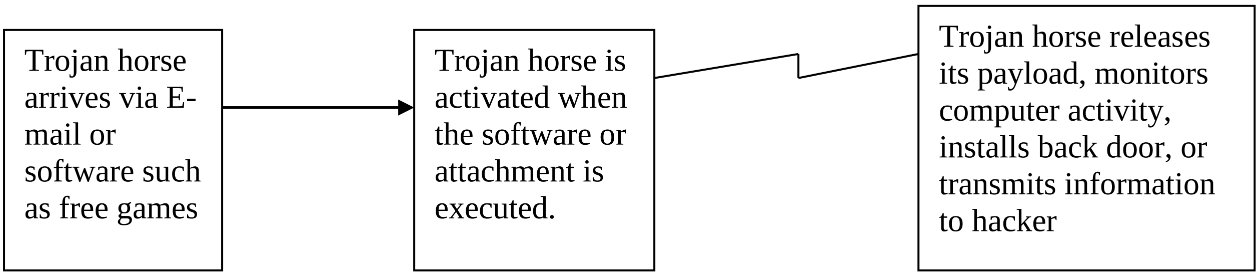
- Segments of code that performs malicious actions.
- Virus transmission is at the opening of Email attachment files.
- **Macro virus**-> Embedded in automatically executing macrocode common in word processors, spreadsheets and database applications.
- **Boot Virus**-> infects the key operating files located in the computer's boot sector.

**Worms**

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

**Trojan Horses**

- Are software programs that hide their true nature and reveal their designed behavior only when activated.


Trojan horse arrives via E-mail or software such as free games
Trojan horse is activated when the software or attachment is executed.
Trojan horse releases its payload, monitors computer activity, installs back door, or transmits information to hacker

## Trojan horse Attack

**Back Door or Trap Door**

- A Virus or Worm has a payload that installs a backdoor or trapdoor component in a system, which allows the attacker to access the system at will with special privileges.

Eg: Back Orifice

**Polymorphism**

- A **Polymorphic threat** is one that changes its apparent shape over time, making it undetectable by techniques that look for preconfigured signatures.
- These viruses and Worms actually evolve, changing their size, and appearance to elude detection by antivirus software programs.

**Virus & Worm Hoaxes**

**Types of Trojans**

- Data Sending Trojans
- Proxy Trojans
- FTP Trojans
- Security software disabler Trojans
- Denial of service attack Trojans(DOS)

**Virus**

A program or piece of code that be loaded on to your computer, without your knowledge and run against your wishes.

**Worm**

A program or algorithm that replicates itself over a computer network and usually performs malicious actions.

**Trojan Horse**

A destructive program that masquerade on beginning application, unlike viruses, Trojan horse do not replicate themselves.

**Blended threat**

Blended threats combine the characteristics of virus, worm, Trojan horses & malicious code with server and Internet Vulnerabilities.

**Antivirus Program**

A Utility that searches a hard disk for viruses and removes any that found.

## Forces of Nature

**Fire:** Structural fire that damages the building. Also encompasses smoke damage from a fire or water damage from sprinkles systems.

**Flood:** Can sometimes be mitigated with flood insurance and/or business interruption Insurance.

**Earthquake:** Can sometimes be mitigated with specific causality insurance and/or business interruption insurance, but is usually a separate policy.

**Lightning**: An Abrupt, discontinuous natural electric discharge in the atmosphere.

**Landslide/Mudslide**: The downward sliding of a mass of earth & rocks directly damaging all parts of the information systems.

**Tornado/Severe Windstorm:**

**Huricane/typhoon:**
**Tsunami:**
**Electrostatic Discharge (ESD):**
**Dust Contamination:**

Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage.

- They must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans, to limit losses in the face of these threats.

## Deviations in Quality of Service

- A product or service is not delivered to the organization as expected.
- The Organization’s information system depends on the successful operation of many interdependent support systems.
- It includes power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff & garbage haulers.
- This degradation of service is a form of **availability disruption.**

## Internet Service Issues

- Internet service Provider(ISP) failures can considerably undermine the availability of information.
- The web hosting services are usually arranged with an agreement providing minimum service levels known as a **Service level Agreement (SLA).**
- When a Service Provider fails to meet SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.

## Communications & Other Service Provider Issues

- Other utility services can affect the organizations are telephone, water, waste water, trash pickup, cable television, natural or propane gas, and custodial services.
- The loss of these services can impair the ability of an organization to function.
- For an example, if the waste water system fails, an organization might be prevented from allowing employees into the building.
- This would stop normal business operations.

## Power Irregularities

- Fluctuations due to power excesses.
- Power shortages &
- Power losses

This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment.

- When voltage levels **spike** (experience a momentary increase),or **surge** ( experience prolonged increase ), the extra voltage can severely damage or destroy equipment.
- The more expensive uninterruptible power supply (UPS) can protect against spikes and surges.

## Technical Hardware Failures or Errors

- Resulting in unreliable service or lack of availability
- Some errors are terminal, in that they result in unrecoverable loss of equipment.
- Some errors are intermittent, in that they resulting in faults that are not easily repeated.

## Technical software failures or errors

- This category involves threats that come from purchasing software with unknown, hidden faults.
- Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.

- These failures range from bugs to untested failure conditions.

### Technological obsolescence

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

### Man-in-the –Middle

- Otherwise called as **TCP hijacking attack**.
- An attacker monitors packets from the network, modifies them, and inserts them back into the network.
- This type of attack uses IP spoofing.
- It allows the attacker to change, delete, reroute, add, forge or divert data.
- TCP hijacking session, the spoofing involves the interception of an encryption key exchange.

### SPAM

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

### Mail Bombing

- Another form of E-mail attack that is also a DOS called a **mail bomb**.
- Attacker routes large quantities of e-mail to the target.
- The target of the attack receives unmanageably large volumes of unsolicited e-mail.
- By sending large e-mails, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.
- The target e-mail address is buried under thousands or even millions of unwanted e-mails.

### Sniffers

- A **sniffer** is a program or device that can monitor data traveling over a network.
- Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere.
- Sniffer often works on TCP/IP networks, where they are sometimes called **"packet Sniffers".**

## Social Engineering

- It is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.
- An attacker gets more information by calling others in the company and asserting his/her authority by mentioning chief's name.

## Buffer Overflow

- A buffer overflow is an application error that occurs when more data is sent to a buffer than it can handle.
- Attacker can make the target system execute instructions.

## Timing Attack

- Works by exploring the contents of a web browser's cache.
- These attacks allow a Web designer to create a malicious form of cookie, that is stored on the client's system.
- The cookie could allow the designer to collect information on how to access password- protected sites.

## Attacks

- An attack is an act of or action that takes advantage of a vulnerability to compromise a controlled system.
- It is accomplished by a **threat agent** that damages or steals an organization's information or physical asset.
- **Vulnerability** is an identified weakness in a controlled system, where controls are not present or are no longer effective.
- Attacks exist when a specific act or action comes into play and may cause a potential loss.

## Malicious code

- The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
- The state –of-the-art malicious code attack is the polymorphic or multivector, worm.
- These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

## Attack Replication Vectors

1. IP scan & attack
2. Web browsing

3. Virus
4. Unprotected shares
5. Mass mail
6. Simple Network Management Protocol(SNMP)

**1. IP scan & attack**

The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers.

**2. Web browsing**

If the infected system has write access to any Web pages, it makes all Web content files (.html,.asp,.cgi & others) infectious, so that users who browse to those pages become infected.

**3. Virus**

Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.

**4. Unprotected shares**

Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.

**5. Mass Mail**

By sending E-mail infections to addresses found in the address book, the infected machine infects many users, whose mail -reading programs also automatically run the program & infect other systems.

**6. Simple Network Management Protocol (SNMP)**

- By using the widely known and common passwords that were employed in early versions of this protocol, the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

**Hoaxes**

- A more devious approach to attacking the computer systems is the transmission of a virus hoax with a real virus attached.
- Even though these users are trying to avoid infection, they end up sending the attack on to their co-workers.

**Backdoors**

- Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door.
- Sometimes these entries are left behind by system designers or maintenance staff, and thus referred to as trap doors.
- A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

### Password Crack

- Attempting to reverse calculate a password is often called **cracking.**
- A password can be hashed using the same algorithm and compared to the hashed results, If they are same, the password has been cracked.
- The (SAM) Security Account Manager file contains the hashed representation of the user's password.

### Brute Force

- The application of computing & network resources to try every possible combination of options of a password is called a **Brute force attack.**
- This is often an attempt to repeatedly guess passwords to commonly used accounts, it is sometimes called a **password attack.**

### Dictionary

- This is another form of the brute force attack noted above for guessing passwords.
- The **dictionary attack** narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords instead of random combinations.

### Denial –of- Services(DOS) & Distributed Denial –of- Service(DDOS)

- The attacker sends a large number of connection or information requests to a target.
- This may result in the system crashing, or simply becoming unable to perform ordinary functions.
- DDOS is an attack in which a coordinated stream of requests is launched dagainst a target from many locations at the same.

### Spoofing

- It is a technique used to gain unauthorized access to computers, where in the intruder sends messages to a computer that has an IP address that indicates that the messages are coming from a trusted host.

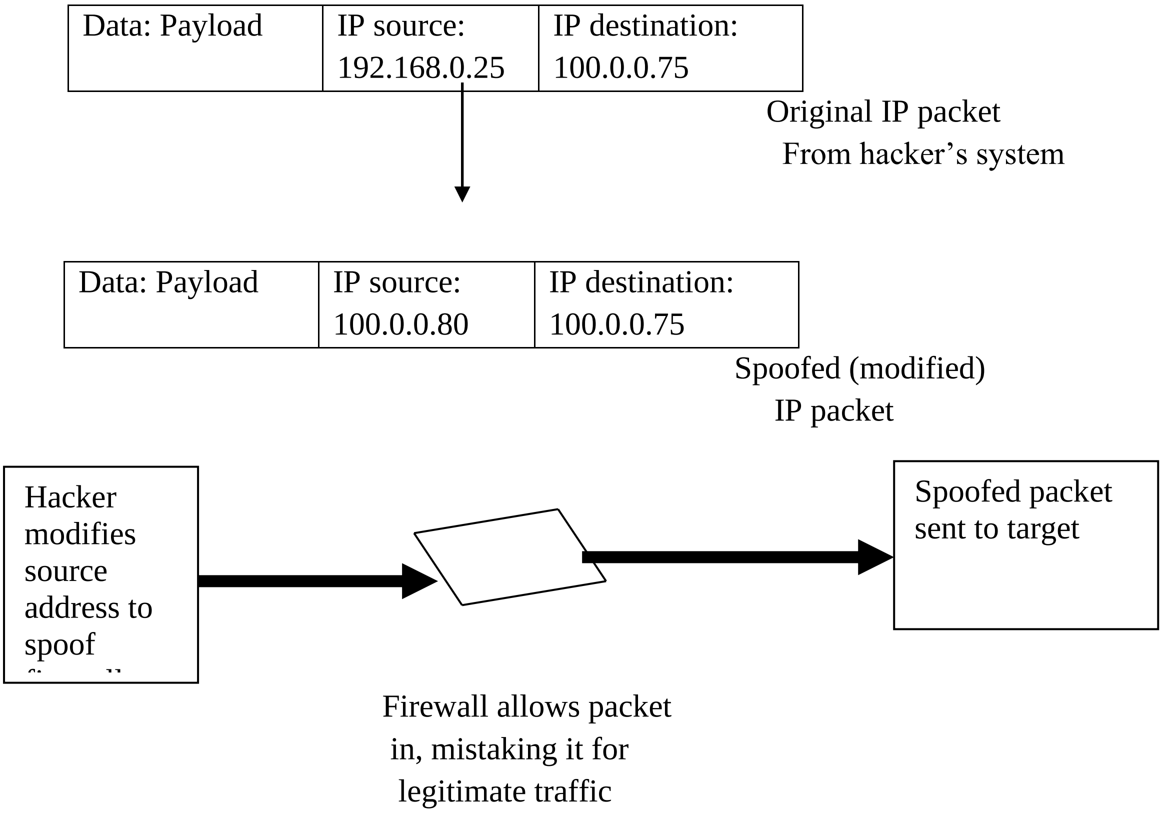

Data: Payload
IP source: 192.168.0.25
IP destination: 100.0.0.75
Original IP packet From hacker's system
Data: Payload
IP source: 100.0.0.80
IP destination: 100.0.0.75
Spoofed (modified) IP packet
Hacker modifies source address to spoof
Spoofed packet sent to target
Firewall allows packet in, mistaking it for legitimate traffic

**Figure 1.14 IP spoofing**

## Legal, Ethical, and Professional Issues in Information Security

Law and Ethics in Information Security

**Laws** are rules that mandate or prohibit certain behavior in society; they are drawn from **ethics**, which define socially acceptable behaviors. The key difference between laws and ethics is that laws carry the sanctions of a governing authority and ethics do not. Ethics in turn are based on **Cultural mores.**

**Table 1.2 Key U.S Laws of Interest to Information Security Professionals**

| ACT | SUBJECT | DATE | DESCRIPTION |
|---|---|---|---|
| Communications Act of 1934,updated by Telecommunications Deregulation & Competition Act | Telecommunications | 1934 | Regulates interstate and foreign Telecommunications. |
| Computer Fraud & Abuse Act | Threats to computers | 1986 | Defines and formalizes laws to counter threats |

| | | | |
|---|---|---|---|
| | | | from computer related acts and offenses. |
| Computer Security Act of 1987 | Federal Agency Information Security | 1987 | Requires all federal computer systems that contain classified information to have surety plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems. |
| Economic Espionage Act of 1996 | Trade secrets. | 1996 | Designed to prevent abuse of information gained by an individual working in one company and employed by another. |
| Electronic Communications Privacy Act of 1986 | Cryptography | 1986 | Also referred to as the Federal Wiretapping Act; regulates interception and disclosure of electronic information. |
| Federal Privacy Act of 1974 | Privacy | 1974 | Governs federal agency use of personal information. |
| Gramm-Leach-Bliley Act of 1999 | Banking | 1999 | Focuses on facilitating affiliation among banks, insurance and securities firms; it has significant impact on the privacy of personal information used by these industries. |
| Health Insurance Portability and Accountability Act | Health care privacy | 1996 | Regulates collection, storage, and transmission of sensitive personal health care information. |
| National Information | Criminal intent | 1996 | Categorized crimes based on defendant's |

| | | | |
|---|---|---|---|
| Infrastructure protection Act of 1996 | | | authority to access computer and criminal intent. |
| Sarbanes-Oxley Act of 2002 | Financial Reporting | 2002 | Affects how public organizations and accounting firms deal with corporate governance, financial disclosure, and the practice of public accounting. |
| Security and Freedom through Encryption Act of 1999 | Use and sale of software that uses or enables encryption. | 1999 | Clarifies use of encryption for people in the United states and permits all persons in the U.S. to buy or sell any encryption product and states that the government cannot require the use of any kind of key escrow system for encryption products. |
| U.S.A. Patriot Act of 2001 | Terrorism | 2001 | Defines stiffer penalties for prosecution of terrorist crimes. |

## RISK MANAGEMENT

**Definition:**

The formal process of identifying and controlling the risks facing an organization is called risk management. It is the probability of an undesired event causing damage to an asset. There are three steps

1. Risk Identification.
2. Risk Assessment
3. Risk Control

**Risk Identification**: It is the process of examining and documenting the security posture of an organization’s information technology and the risk it faces.

**Risk Assessment**: It is the documentation of the results of risk identification.

**Risk Control**: It is the process of applying controls to reduce the risks to an organization's data and information systems.

To keep up with the competition, organizations must design and create safe environments in which business process and procedures can function.

These environments must maintain Confidentiality & Privacy and assure the integrity of organizational data-objectives that are met through the application of the principles of risk management.

**Components of Risk Management**

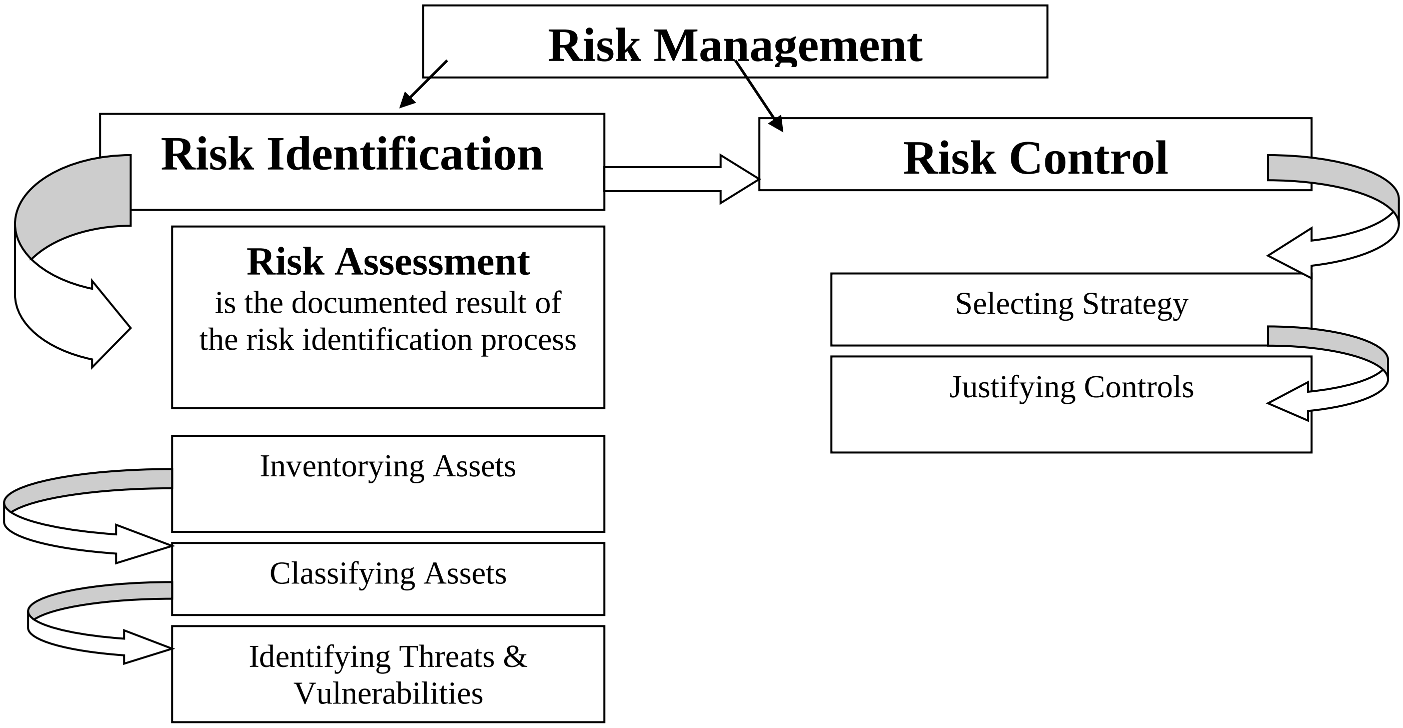


**Figure 1.15 Risk Management**

**An Overview of Risk Management**

Over 2,400 years ago by Chinese General Sun Tzu said

"1.If you know the enemy & know yourself, you need not fear the result of a hundred battles.

2. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

3. If you know neither the enemy nor yourself, you will succumb in every battle"

**Know Yourself**

- Identify, Examine & Understand the information systems.
- To protect assets, you must understand what they are? How they add value to the organization, and to which vulnerabilities they are susceptible.

- The policies, Education and training programs, and technologies that protect information must be carefully maintained and administered to ensure that they are still effective.

**Know the Enemy**

- Identifying, Examining & Understanding the threats facing the organization.

**The Roles of the Communities of Interest**

- It is the responsibility of each community of interest to manage the risks that organization encounters.

**Information Security**

- Understand the threats and attacks that introduce risk into the organization.
- Take a leadership role in addressing risk.

**Management & Users**

- Management must ensure that sufficient resource are allocated to the information security & Information technology groups to meet the security needs of the organization.
- Users work with the systems and the data and are therefore well positioned to understand the value of the information assets.

**Information Technology**

- Must build secure systems and operate them safely.

Three communities of interest are also responsible for the following

- Evaluating the risk controls.
- Determining which control options are cost effective.
- Acquiring or installing the needed controls.
- Overseeing that the controls remain effective.

**Important Risk Factors of information Security are**

i. Understand the threats and attacks that introduce risk into the organization.
ii. Taking asset inventory.
iii. Verify the threats and vulnerabilities that have been identified as dangerous to the asset inventory, as well as the current controls and mitigation strategies.
iv. Review the cost effectiveness of various risk control measures.

**Risk Identification**

- IT professionals to know their organization’s information assets through identifying, classifying and prioritizing them.
- Assets are the targets of various threats and threat agents, and the goal is to protect the assets from the threats.
- Once the organizational assets have been identified, a threat identification process is undertaken and the circumstances and settings of each information asset are examined to identify vulnerabilities.
- When vulnerabilities are found, controls are identified and assessed as to their capability to limit possible losses in the eventuality of attack.

- The process of Risk Identification begins with the identification of the organization's information assets and an assessment of their value.

**Asset Identification & Valuation**

- Includes all the elements of an organization's system, such as people, procedures, data and information, software, hardware, and networking elements.
- Then, you classify and categorize the assets, adding details.

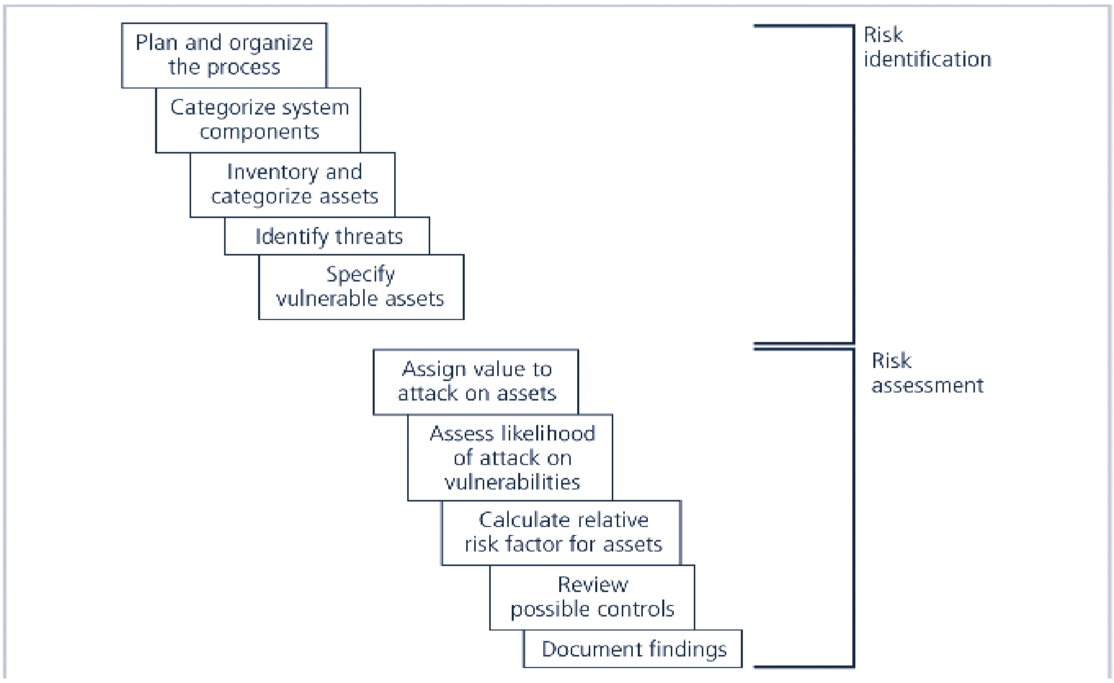

Plan and organize the process
Categorize system components
Inventory and categorize assets
Identify threats
Specify vulnerable assets
Assign value to attack on assets
Assess likelihood of attack on vulnerabilities
Calculate relative risk factor for assets
Review possible controls
Document findings
Risk identification
Risk assessment

**Figure 1.16 Risk Identification and Control**

## Security Threats to E-Commerce

Security is an essential part of any transaction that takes place over the internet. Customer will lose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe e-payments/transactions −

- **Confidential** − Information should not be accessible to unauthorized person. It should not be intercepted during transmission.
- **Integrity** − Information should not be altered during its transmission over the network.
- **Availability** − Information should be available wherever and whenever requirement within time limit specified.

- **Authenticity** − There should be a mechanism to authenticate user before giving him/her access to required information.

- **Non-Repudiabiity** − It is protection against denial of order or denial of payment. Once a sender sends a message, the sender should not able to deny sending the message. Similary the receipient of message should not be able to deny receipt.

- **Encryption** − Information should be encrypted and decrypted only by authorized user.

- **Auditability** − Data should be recorded in such a way that it can be audited for integrity requirements.

Measures to ensure Security are following −

- **Encryption** − It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and specified receiver only can decrypt the data using the same or different secret code.

- **Digital Signature** − Digital signature ensures the authenticity of the information. A digital signature is a e-signature authentic authenticated through encryption and password.

- **Security Certificates** − Security certificate is unique digital id used to verify identity of an individual website or user.

## Virtual Organization

This new form of organization, i.e., ‘virtual organization’ emerged in 1990 and is also known as digital organization, network organization or modular organization. Simply speaking, a virtual organization is a network of cooperation made possible by, what is called ICT, i.e. Information and Communication Technology, which is flexible and comes to meet the dynamics of the market.

Alternatively speaking, the virtual organization is a social network in which all the horizontal and vertical boundaries are removed. In this sense, it is a boundary less organization. It consists of individual’s working out of physically dispersed work places, or even individuals working from mobile devices and not tied to any particular workspace. The ICT is the backbone of virtual organization.

It is the ICT that coordinates the activities, combines the workers’ skills and resources with an objective to achieve the common goal set by a virtual organization. Managers in these organizations coordinate and control external relations with the help of computer network links. The virtual form of organization is increasing in India also. Nike, Reebok, Puma, Dell Computers, HLL, etc., are the prominent companies working virtually.

While considering the issue of flexibility, organizations may have several options like flexi-time, part-time work, job-sharing, and home-based working. Here, one of the most important issues involved is attaining flexibility to respond to changes – both internal and external – is determining the extent of control or the amount of autonomy the virtual organizations will impose on their members.

This is because of the paradox of flexibility itself. That is: while an organization must possess some procedures that enhance its flexibility to avoid the state of rigidity, on the one hand, and simultaneously also have some stability to avoid chaos, on the other.

Characteristics:

A virtual organization has the following characteristics:

1. Flat organization
2. Dynamic
3. Informal communication
4. Power flexibility
5. Multi-disciplinary (virtual) teams
6. Vague organizational boundaries
7. Goal orientation
8. Customer orientation
9. Home-work
10. Absence of apparent structure
11. Sharing of information
12. Staffed by knowledge workers.

In fact, this list of the characteristics of virtual organization is not an exhaustive one but illustrative only. One can add more characteristics to this list.

**Types of virtual organizations:**

Depending on the degree or spectrum of virtuality, virtual organizations can be classified into three broad types as follows**:**

1. Telecommuters
2. Outsourcing employees/competencies
3. Completely virtual

A brief description of these follows in turn.

1. **Telecommuters:**

These companies have employees who work from their homes. They interact with the workplace via personal computers connected with a modem to the phone lines. Examples of companies using some form of telecommuting are Dow Chemicals, Xerox, Coherent Technologies Inc., etc.

2. **Outsourcing Employees/Competencies:**

These companies are characterized by the outsourcing of all/most core competencies. Areas for outsourcing include marketing and sales, human resources, finance, research and development, engineering, manufacturing, information system, etc. In such case, virtual organization does its own on one or two core areas of competence but with excellence. For example, Nike performs in product design and marketing very well and relies on outsources for information technology as a means for maintaining inter-organizational coordination.

3. **Completely Virtual:**

These companies metaphorically described as companies without walls that are tightly linked to a large network of suppliers, distributors, retailers and customers as well as to strategic and joint venture partners. Atlanta Committee for the Olympic Games (ACOG) in 1996 and the development efforts of the PC by the IBM are the examples of completely virtual organizations.

## Business Transaction over Web

When you conduct business over the Internet, you are engaging in a robust and complex system with which you can purchase items for yourself or your business from the comfort of your own home. By familiarizing yourself with how Internet transactions work and what to look out for, you can make safe purchases and enjoy the many benefits of e-commerce.

## E-Commerce

You engage in electronic commerce when you purchase a product or service from a vendor's website instead of from a physical, brick-and-mortar store. There are two primary types of e-commerce -- B2B and B2C. You are engaging in B2B, or business-to-business e-commerce when you buy products or services for your own business. B2C, or business-to-customer, is far more common; it occurs when you buy products online for yourself. Additionally, there are two types of online stores. These are "Pure Click" and "Brick and Click." The first denotes an online operation that has no physical store, and the second refers to an online operation that has at least one physical store.

## The Process

When you do business over the Internet, you put a complex chain of events into motion. First, you land on the vendor's website and are presented with its catalog of items. You read descriptions and compare prices. When you find the item you want, you click a button to signify that you would like to purchase it. In the background, software that the vendor has installed to its site keeps a running tally of all the items that you select. This is known as "shopping cart" software. When you have finished shopping, you click the "Check Out" button. The site redirects you to a page where the shopping cart software presents you with your grand total. You then enter your name, address, birth date and credit or debit card number to complete the transaction.

### Payment Methods

Typically, you must use either a credit or debit card to purchase items online. There are exceptions to this. There are sites that will accept checks, money orders or electronic wallets, such as PayPal. When you pay with a credit or debit card, note that the information you provide must match the information that the issuing bank has on file. If it does not, the bank will not approve the transaction. This safeguard exists to prevent unauthorized use of your cards.

### Consumer Information Security and Concerns

When you pay for items online with a credit or debit card, you are transmitting the card's number, its expiration date and -- often -- the three-digit security number on its backside. Fortunately, all this information is routed through a secure channel that encrypts the data and requires the recipient to enter the correct key to decrypt it. This technology is called "Secure Sockets Layer Encryption." Sites that utilize this countermeasure will typically display an official certification seal, such as "VeriSign."

### E Governance and EDI

Electronic governance or e-governance is the application of information and communication technology (ICT) for delivering government services, exchange of information communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back office processes and interactions within the entire government framework.Through e-governance, government services will be made available to citizens in a convenient, efficient and transparent manner. The three main target groups that can be distinguished in governance concepts are government, citizens and businesses/interest groups. In e-governance there are no distinct boundaries.
Generally four basic models are available – government-to-citizen (customer), government-to-employees, government-to-government and government-to-business.

**EDI** stands for Electronic Data Exchange. EDI is an electronic way of transferring business documents in an organization internally between its various departments or externally with suppliers, customers or any subsidiaries etc. In EDI, paper documents are replaced with electronic documents like word documents, spreadsheets etc.

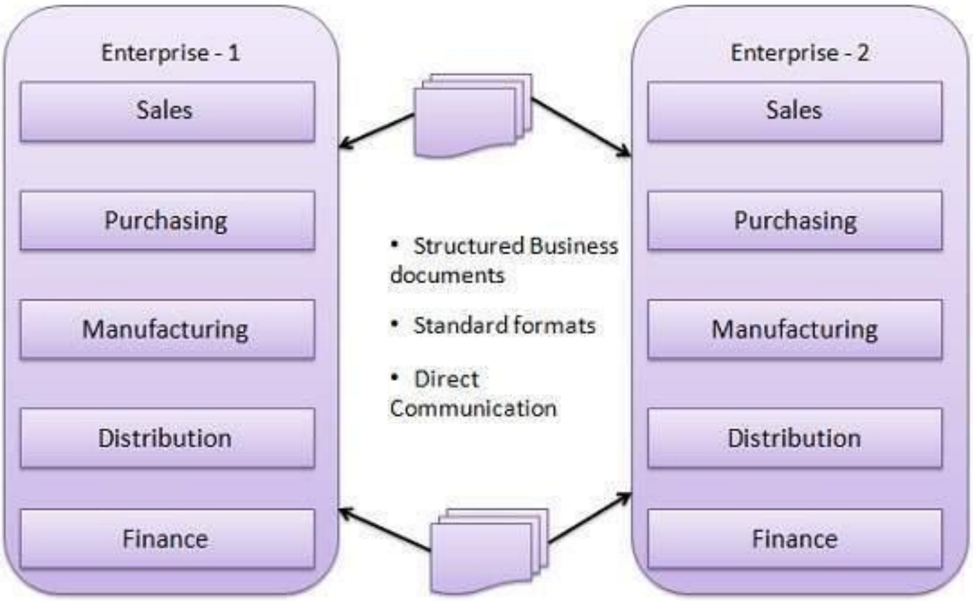


**Figure 1.17 EDI**

**EDI Documents-**

Following are few important documents used in EDI −

Invoices

Purchase orders

Shipping Requests

Acknowledgement

Business Correspondence letters

Financial information letters

Steps in an EDI System

Following are the steps in an EDI System.

A program generates the file which contains the processed document.

The document is converted into an agreed standard format.

The file containing the document is send electronically on network.

The trading partner receives the file.

An acknowledgement document is generated and sent to the originating organization.

**Advantages of an EDI System**

Following are the advantages of an EDI System.

**Reduction in data entry errors.** − Chances of errors are much less being use of computer in data entry.

**Shorter processing life cycle** − as orders can be processed as soon as they are entered into the system. This reduced the processing time of the transfer documents.

**Electronic form of data** − It is quite easy to transfer or share data being in electronic format.

**Reduction in paperwork** − As lot of paper documents are replaced with electronic documents there is huge reduction in paperwork.

**Cost Effective** − As time is saved and orders are processed very effectively, EDI proves to be highly cost effective.
**Standard Means of communication** − EDI enforces standards on the content of data and its format which leads to clearer communication.

## Electronic Payment Systems (Digital Payment)

Electronic Payment Systems or Digital payment is a way of payment which is made through digital modes. In digital payments, payer and payee both use digital modes to send and receive money. It is also called electronic payment as electronic payment as it involves paperless monetary transactions methods. No hard cash is involved in digital payments. All the transactions in digital payments are completed online. It is an instant and convenient way to make payments. E-Commerce or Electronics Commerce sites use electronic payment. Electronic payment has revolutionized the business processing by reducing paper work, transaction costs, labour cost. All the transactions in digital payments are completed online. It is an instant and convenient way to make payments. Being user friendly and less time consuming than manual processing, helps business organization to expand its market reach / expansion. Some of the modes of electronic payments are following.
Credit Card
Debit Card
Smart Card
E-Money
Electronic Fund Transfer (EFT)

### Credit Card

Payment using credit card is one of most common mode of electronic payment. Credit card is small plastic card with a unique number attached with an account. It has also a magnetic strip embedded in it which is used to read credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle. Following are the actors in the credit card system.
The card holder - Customer
The merchant - seller of product who can accept credit card payments.
The card issuer bank - card holder's bank
The acquirer bank - the merchant's bank
The card brand - for example, visa or master-card.

### Credit card payment process

| Step | Description |
|---|---|
| Step 1 | Bank issues and activates a credit card to customer on his/her request. |
| Step 2 | Customer presents credit card information to merchant site or to merchant from whom he/she want to purchase a product/service. |
| Step 3 | Merchant validates customer's identity by asking for approval from card brand company. |
| Step 4 | Card brand company authenticates the credit card and paid the transaction by credit. Merchant keeps the sales slip. |
| Step 5 | Merchant submits the sales slip to acquirer banks and gets the service chargers paid to him/her. |
| Step 6 | Acquirer bank requests the card brand company to clear the credit amount and gets the payment. |
| Step 7 | Now card brand company asks to clear amount from the issuer bank and amount gets transferred to card brand company. |

### Debit Card

Debit card, like credit card is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between debit card and credit card is that in case of payment through debit card, amount gets deducted from card's bank account immediately and there should be sufficient balance in bank account for the transaction to get completed. Whereas in case of credit card there is no such compulsion. Debit cards free customer to carry cash, cheques and even merchants accepts debit card more readily. Having restriction on amount being in bank account also helps customer to keep a check on his/her spending.

### Smart Card

Smart card is again similar to credit card and debit card in appearance but it has a small microprocessor chip embedded in it. It has the capacity to store customer work related/personal information. Smart card is also used to store money which is reduced as per usage.

Smart card can be accessed only using a PIN of customer. Smart cards are secure as they stores information in encrypted format and are less expensive/provides faster processing. Mondex and Visa Cash cards are examples of smart cards.

**E-Money**

E-Money transactions refer to situation where payment is done over the network and amount gets transferred from one financial body to another financial body without any involvement of a middleman. E-money transactions are faster, convenient and save a lot of time.

Online payments done via credit card, debit card or smart card are examples of e-money transactions. Another popular example is e-cash. In case of e-cash, both customer and merchant both have to sign up with the bank or company issuing e-cash.

**Electronic Fund Transfer**

It is a very popular electronic payment method to transfer money from one bank account to another bank account. Accounts can be in same bank or different bank. Fund transfer can be done using ATM (Automated Teller Machine) or using computer.

Now a day, internet based EFT is getting popularity. In this case, customer uses website provided by the bank. Customer logins to the bank's website and registers another bank account. He/she then places a request to transfer certain amount to that account. Customer's bank transfers amount to other account if it is in same bank otherwise transfer request is forwarded to ACH (Automated Clearing House) to transfer amount to other account and amount is deducted from customer's account. Once amount is transferred to other account, customer is notified of the fund transfer by the bank.

**Electronic Cash (Ecash)**

An anonymous electronic cash system; equivalent to "cash" or "printed bank notes" except that it is transferred through networks with bits of information, in essence it is just another representation of monetary value; anonymity is preserved through public key cryptography, digital signatures, and blind signatures.

How it is used:

Ecash is used over the Internet, email, or personal computer to other workstations in the form of secured payments of "cash" that is virtually untraceable to the user. It is backed by real currency from real banks.

The way ecash works is similar to that of electronic fund transfers done between banks. The user first must have an ecash software program and an ecash bank account from which ecash can be withdrawn or deposited. The user withdraws the ecash from the account onto her computer and spends it in the Internet without being traced or having personal information available to other parties that are involved in the process. The recipients of the ecash send the money to their bank account as with depositing "real" cash.

Other than making purchases on the Internet, ecash can also be found used in entertainment sites - on "gambling tables" in Internet casinos such as PAF Casino and Internet Casino. Ecash allows the exchange of money to be conducted in the same way as in real casinos.

**Relevance to business and electronic commerce:**

Even though there are more than 25,000 companies conducting business on the Internet, consumers are still not that confident with having transaction done over the Internet. This is mostly due to a lack of a readily available and secure payment system. With credit cards, consumers are concerned with the security of their information and thus deterring them from directly making purchases from the Internet. With ecash, hopefully consumers will be more comfortable with transactions over the Internet as it is a one-time transaction that cannot be traced back to the user, whereas with credit cards, hackers can obtain information of the card holder and commit frauds.With the appearance of ecash, the need for commercial banks to be involved in electronic banking and to back the electronic currencies becomes more apparent. However, there remains a skeptical view about having monetary transactions done over the Internet as it is a fairly public domain where there is easy access. Thus increasing and promoting commercial bank's interest in the Internet and conducting business over the Internet is necessary in order to further the development of ecash and commerce in the Internet, as well as improving cryptography and security features of the systems.

While it is a grand idea to mimic the real world transactions with cash on the Internet through the use of an anonymous transaction system, at this moment it still poses a lot of logistics and legal problems and possible security hazards. There are still questions of the regulation of electronic money, how will the ecash be backed and redeemed, determining how much of money in the economy are circulated in ecash since the Internet covers such a vast area internationally. Moreover, with Internet business companies, how will taxes be applied to them when they conduct business all over the world?

Ecash is not completely anonymous as with hard cash since there is always the computer and the network, which can be traced. But do people really care about anonymity? Some people may want to track expenses if they're conducting businesses through the Internet. Also, there is the issue of possible criminal activity within the system by allowing criminals to spend illegal money easier if ecash is untraceable. The US Department of Treasury's Financial Crimes Enforcement Network provides some information on how it is addressing these issues.

Some Ecash providers:
eCashTechnologies
CyberCash
Mondex
Magex

## Credit/Debit Cards

Debit and credit cards offer more than a way to access money without having to carry around cash or a bulky checkbook. **Debit cards** are like digitized versions of checkbooks; they are linked to your bank account (usually a checking account), and money is debited (withdrawn) from the account as soon as the transaction occurs. **Credit cards** are different; they offer a line of credit (i.e., a loan) that is interest-free if the monthly credit card bill is paid on time. Instead of being connected to a personal bank account, a credit card is connected to the bank or financial institution that issued the card. So when you use a credit card, the issuer pays the merchant and you go into debt to the card issuer.

Most debit cards are free with a checking account at a bank or credit union. They can also be used to conveniently withdraw cash from ATMs. Credit cards have the advantage of rewards programs but such cards often require an annual fee to use. Financial responsibility is a big factor in credit card use; it is easy to overspend and then get buried in overwhelming credit card debt at a very high interest rates.

This comparison provides a detailed overview of what debit and credit cards are, their types, associated fees, and pros and cons.

### Comparison Chart

Credit Card versus Debit Card comparison chart

| | **Credit Card** | **Debit Card** |
|---|---|---|
| **About** | Credit cards are lines of credit. When you use a credit card, the issuer puts money toward the transaction. This is a loan you are expected to pay back in full (usually within 30 days), unless you want to be charged interest. | Any time you use a debit card to buy something, money is deducted from your account. With a debit card, you can really only spend the money you have available to you. |

| | | |
|---|---|---|
| **Connected To** | Not required to be connected to a checking account. | Checking or Savings Account |
| **Monthly Bills** | Yes | No |
| **Application Process** | Somewhat difficult, depending on one's credit score and other details. | Easy, with basically no barrier to receiving a debit card. |
| **Spending Limit** | The credit limit set by the credit issuer. Limits increase or stay the same over time as a borrower's creditworthiness changes. | However much is in the bank account connected to the card. |
| **Interest Charged** | If a credit card bill is not paid in full, interest is charged on outstanding balance. The interest rate is usually very high. | No interest is charged because no money is borrowed. |
| **Security** | Credit cards in the U.S. are not very secure in and of themselves because many still use dated card security technology. However, consumers are not held liable for this poor security. | A PIN makes them secure so long as no one steals the card number and PIN, and as long as you don't lose the card itself. If the card/info is stolen, debit cards are very insecure. |
| **Fraud Liability** | Low. Rarely held liable for fraudulent activity. If you are, you are only held liable for a maximum of $50. | High. If someone steals your card and makes purchases, that money is removed from your bank account. Investigating this damage takes time. The longer you wait to report the fraud, the more likely you will be held liable for your own losses. |
| **Credit History** | Responsible credit card usage and payment can improve one's credit rating. Credit cards typically report account activity to at least one of the three major credit bureaus on a monthly basis. | Does not affect credit history. |

| | | |
|---|---|---|
| **Overdraw Fees** | Low. Some credit card companies allow to overdraw amount over the maximum credit line with a fee. | High "overdraft" fees. Possible to overdraw amount over the account limit. |
| **PIN** | In the U.S., this is uncommon, but PINs are being phased in. | Usually |

## Digital Forensics

**Digital forensics** (sometimes known as **digital forensic science**) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Forensic investigators typically follow a standard set of procedures: After physically isolating the device in question to make sure it cannot be accidentally contaminated; investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, examine hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions or actual litigation.

Ethical hacking is not a part of digital hacking/forensics:

Digital security threats occur when the security of a digital/online account or file has been breached/hacked or threatened. Modern-day ethical hackers often start hacking for the challenge or to educate themselves on the vulnerabilities in IT security. These hackers are sometimes called "white-hat hackers". It's become increasingly common for companies large and small to employ their in- house IS Analysts to help combat hacking. IS Analysts typically have extensive training in technological and informational infrastructure, with ongoing responsibilities to keep it running securely.

Ethical hackers coming from this area of expertise also have knowledge in problem-solving strategies for security breaches, and can collect and analyse data to monitor and interpret weakness. We can expect them to possess deep knowledge of the latest infrastructure and hardware, from routers to memory storage, with the ability to establish security policies and best practices.

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil (as part of the electronic discovery process) courts. Forensics may also feature in the private sector; such as during internal corporate investigations or intrusion investigation (a specialist probe into the nature and extent of an unauthorized network intrusion).

Digital forensics can be divided into 5 parts:

**1. Identify:** All digital forensics starts with identification. Before doing anything else, it's important to identify where data is stored. In the old days, investigators found the data they needed in filing cabinets. Today, it's pretty much all electronic. Data is stored on the hard drives of computers and servers, flash drives, network equipment – you name it, there's data on it.

**2. Preserve:** Preservation is a crucial part of the digital forensics process, and it largely rests on the shoulders of investigators. Why is preservation so important? Because without integrity, a piece of evidence loses its value or "admissibility" in the court of law. That's why it's so important to ensure that the artefacts are unaltered and preserved in their original state.

**3. Recover:** In just about every case, there is some sort of recovery process. This can include recovering deleted files from normal OS processes, intentionally deleted files, password protected files and even damaged or corrupted files. There are many methods of recovering these artefacts.

**4. Analysis:** Analysis is the guts of the investigation. This is where all the expertise and elbow grease comes in. Again, the key here is to gather as many artefacts as possible, and there are often many artefacts to be found. In fact, any action performed on a computer can create up to five artefacts in different locations. A good example is a simple Google search. Whenever you search for something, it's not just logged in your browser history; there's also a coordinating registry artefact that points to that search. Depending on the configuration of your devices, this search may be present across every device you own. A device like Skype, for instance, will sync chat history across all devices. Using these various artefacts that all point to each other, we can really develop that clear picture we're after.

**5. Present:** Finally, once examination is complete, it's time to present the findings in the form of a case report. All that documentation that is recorded makes creating this report a hell of a lot easier in the end. And all of the information that is collected leads to some definitive conclusion.

The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved;

- computer forensics,
- network forensics,
- forensic data analysis and mobile device forensics.

The typical forensic process encompasses the seizure, forensic imaging (acquisition) and analysis of digital media and the production of a report into collected evidence as shown in fig.1.

**Seizure:**

Seizing mobile devices is covered by the same legal considerations as other digital media. Mobiles will often be recovered switched on; as the aim of seizure is to preserve evidence, the device will often be transported in the same state to avoid a shutdown, which would change files. In addition, the investigator or first responder would risk user lock activation.

As well as identifying direct evidence of a crime, digital forensics can be used to

- attribute evidence to specific suspects,
- confirm alibis or statements,
- determine intent,

identify sources (for example, in copyright cases), or authenticate documents.

**Acquisition:**

The second step in the forensic process is acquisition, in this case usually referring to retrieval of material from a device. Due to the proprietary nature of mobiles it is often not possible to acquire data with it powered down; most mobile device acquisition is performed live. With more advanced smartphones using advanced memory management, connecting it to a recharger and putting it into a faraday cage may not be good practice. The mobile device would recognize the network disconnection and therefore it would change its status information that can trigger the memory manager to write data. Most acquisition tools for mobile devices are commercial in nature and consist of a hardware and software component, often automated.

**Examination/analysis:**

As an increasing number of mobile devices use high-level file systems, similar to the file systems of computers, methods and tools can be taken over from hard disk forensics or only need slight changes. The FAT file system is generally used on NAND memory. A difference is the block size used, which is larger than 512 bytes for hard disks and depends on the used memory type, e.g., NOR type 64, 128, 256 and NAND memory 16, 128, 256, or 512 kilobyte.

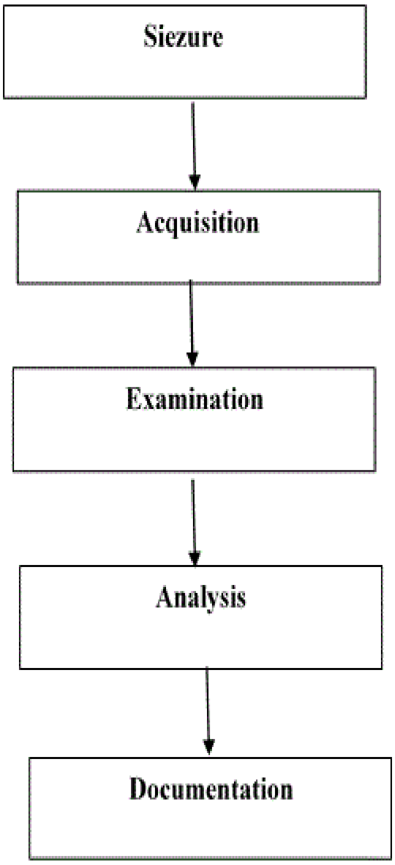


**Figure 1.18. Digital Forensic Process**

Investigations are much broader in scope than other areas of forensic analysis (where the usual aim is to provide answers to a series of simpler questions) often involving complex time-lines or hypotheses.

**Branches of Digital Forensics**

**Different branches of the digital forensics are as follows:**

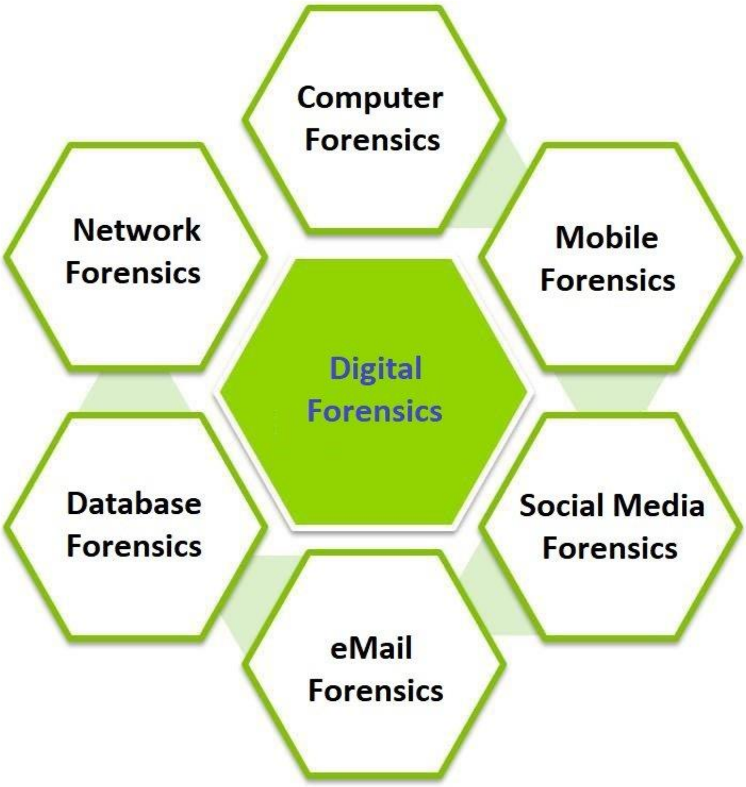


**Figure 1.19: Branches of Digital Forensics**

1. **Media Forensics**:

Media forensics is scientific study into the collection, analysis, interpretation, and presentation of audio, video, and image evidence obtained during the course of investigations and litigious proceedings.

2. **Cyber Forensics:**

Computer forensics (also known as cyber forensics) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Cybercrimes cover a broad spectrum, from email scams to downloading copyrighted works for distribution, and are fueled by a desire to profit from another person's intellectual property or private information. Cyber forensics can readily display a digital audit trail for analysis by experts or law enforcement. Developers often build program applications to combat and capture online criminals; these applications are the crux of cyber forensics. Cyber forensic techniques include:

- Cross-driven analysis that correlates data from multiple hard drives
- Live analysis, which obtains data acquisitions before a PC is shut down
- Deleted file recovery

Each of the above techniques is applied to cyber forensic investigations.

3. **Software Forensics:**

Software forensics is branch of science that investigates software source code or binary code to determine whether intellectual property infringement or theft occurred. It is the centrepiece of lawsuits, trials, and settlements when companies are in dispute over issues involving software patents, copyrights, and trade secrets. Software forensics tools can compare code to determine correlation, a measure that can be used to guide a software forensics expert.

Software forensics is especially important in patent and trade cases. In these cases, someone might have copied another person's code, but rewritten that code in a way to hide the theft. A digital forensic examiner may not have the tools or capabilities to prove a crime occurred.

The following common terms are important to understanding related to software forensics:

- IP address: A number that labels every computer attached to the internet

- Domain name system: Names for computers using the internet. These registered domains include the person's name and contact information.

- Hashing: Hashing is a way to map out the large amount of information on a computer. Some experts use hashing to determine whether someone has copied a file, although it's not always an effective method to prove theft. Hashing helps to find exact matches of code. If a programmer changes code with even one space, hashing can't conclusively determine if copyright infringement or theft exists.

- Source Code: The text form written by a computer programmer based on high-level instructions. Source code is always written in a computer programming language.

- Decompiled: Source code gets created to perform a process. Decompiling the process could open up the source code for interpretation and investigation. Often, information in a computer or in a file is lost in the decompiling process.

- Logging: Logging files tends to be informative for researchers. The problem is that too much logging uses up disk space or slows down a computer. Administrators must find a careful balance of logging information and saving space. Almost all operating systems record usage behaviors. Logging aids in determining who accessed a file and when the file was accessed. Computer files can also tell investigators what users do when they log into computers. Using the Perl programming language, a high-level computer programming language, investigators typically create their programs for log file analysis. Many of the current commercial products aren't adequate to cover the variety of log files that an investigator may experience.

- Network Surveillance: Networks refer to the way data travels between computers. To monitor networks, network administrators can use a special type of software and hardware. Data gets split into packets when it travels over networks. In software forensics, people in the field call watching networks packet sniffing with packet sniffers, network protocol analyzers, or network sniffers. Ethereal, which runs on UNIX and Windows, is the most widely available and free system for packet sniffing.

Past methods of software forensics includes code comparison included hashing, statistical analysis, text matching, and tokenization. These methods compared software code and produced a single measure indicating whether copying had occurred. However, these measures were not accurate enough to be admissible in court because the results were not accurate, the algorithms could be easily fooled by simple substitutions in the code, and the methods did not take into account the fact that code could be similar for reasons other than copying.

**Reasons to Use Software Forensics:**

Unfortunately, people use computers to cause harm. Below are some ways people have caused problems using computers-

- Viruses: People write computer codes that repeat themselves and cause damage.

- Worms: A programmer writes computer code to repeat and spread over networks causing damage.

- Logic Bombs: Logic bombs are timers that are usually attached to a virus or worm to activate the virus or worm at a certain time.

- Plagiarism: This term refers to intentionally copying someone else's work.

- Computer Fraud: This action involves using a computer for a crime.

- Trojan Horses: In computer terms, a Trojan horse is a program that looks like a safe program. These programs appear safe, but they cause harm.

## 4. Mobile Forensics:

Mobile device forensics is a sub-branch of digital forensics relating to recovery of digital evidence or data from a mobile device. It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms. Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data. Mobile devices are also useful for providing location information; either from inbuilt GPS/location tracking or via cell site logs, which track the devices within their range.

The phrase ‘mobile device’ usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability, including PDA devices, GPS devices and tablet computers.

The use of phones in crime was widely recognized for some years, but the forensic study of mobile devices is a relatively new field, dating from the early 2000s. A proliferation of phones (particularly smart phones) on the consumer market caused a demand for forensic examination of the devices, which could not be met by existing computer forensics techniques.

Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, SMS and MMS messages. Smartphone may additionally contain video, email, web browsing information, location information, and social networking messages and contacts.

There is growing need for mobile forensics due to several reasons and some of the prominent reasons are:

- Use of mobile phones to store and transmit personal and corporate information
- Use of mobile phones in online transactions
- Law enforcement, criminals and mobile phone devices

Mobile device forensics can be particularly challenging on a number of levels:

Evidential and technical challenges exist. For example, cell site analysis following from the use of mobile phone usage coverage, is not an exact science. Consequently, whilst it is possible to determine roughly the cell site zone from which a call was made or received, it is not yet possible to say with any degree of certainty, that a mobile phone call emanated from a specific location e.g. a residential address.

- To remain competitive, original equipment manufacturers frequently change mobile phone form factors, operating system file structures, data storage, services, peripherals, and even pin connectors and cables. As a result, forensic examiners must use a different forensic process compared to computer forensics.

- Storage capacity continues to grow thanks to demand for more powerful "mini computer" type devices.[4]
- Not only the types of data but also the way mobile devices are used constantly evolve.
- Hibernation behavior in which processes are suspended when the device is powered off or idle but at the same time, remaining active.

**Mobile forensic challenges**

- Hardware differences: As the mobile landscape is changing each passing day, it is critical for the examiner to adapt to all the challenges and remain updated on mobile device forensic techniques.

- Mobile operating systems: Unlike personal computers where Windows has dominated the market for years, mobile devices widely use more operating systems, including Apple's iOS, Google's Android, RIM's BlackBerry OS, Microsoft's Windows Mobile, HP's webOS, Nokia's Symbian OS, and many others.

- Mobile platform security features: Modern mobile platforms contain built-in security features to protect user data and privacy. These features act as a hurdle during the forensic acquisition and examination.

- Lack of resources: As mentioned earlier, with the growing number of mobile phones, the tools required by a forensic examiner would also increase. Forensic acquisition accessories, such as USB cables, batteries, and chargers for different mobile phones, have to be maintained in order to acquire those devices.

- Generic state of the device: Even if a device appears to be in an off state, background processes may still run. For example, in most mobiles, the alarm clock still works even when the phone is switched off. A sudden transition from one state to another may result in the loss or modification of data.

- Anti-forensic techniques: Anti-forensic techniques, such as data hiding, data obfuscation, data forgery, and secure wiping, make investigations on digital media more difficult.

- Dynamic nature of evidence: Digital evidence may be easily altered either intentionally or unintentionally. For example, browsing an application on the phone might alter the data stored by that application on the device.

- Accidental reset: Mobile phones provide features to reset everything. Resetting the device accidentally while examining may result in the loss of data.

- Device alteration: The possible ways to alter devices may range from moving application data, renaming files, and modifying the manufacturer's operating system. In this case, the expertise of the suspect should be taken into account.

- Passcode recovery: If the device is protected with a passcode, the forensic examiner needs to gain access to the device without damaging the data on the device.

- Communication shielding: Mobile devices communicate over cellular networks, Wi-Fi networks, Bluetooth, and Infrared. As device communication might alter the device data, the possibility of further communication should be eliminated after seizing the device.

- Lack of availability of tools: There is a wide range of mobile devices. A single tool may not support all the devices or perform all the necessary functions, so a combination of tools needs to be used. Choosing the right tool for a particular phone might be difficult.

- Malicious programs: The device might contain malicious software or malware, such as a virus or a Trojan. Such malicious programs may attempt to spread over other devices over either a wired interface or a wireless one.

- Legal issues: Mobile devices might be involved in crimes, which can cross geographical boundaries. In order to tackle these multijurisdictional issues, the forensic examiner should be aware of the nature of the crime and the regional laws.

As a result of these challenges, a wide variety of tools exist to extract evidence from mobile devices; no one tool or method can acquire all the evidence from all devices. It is therefore recommended that forensic examiners, especially those wishing to qualify as expert witnesses in court, undergo extensive training in order to understand how each tool and method acquires evidence; how it maintains standards for forensic soundness; and how it meets legal requirements such as the Daubert standard or Frye standard.

### 5. **Network Forensics:**

Network forensics is concerned with the monitoring and analysis of computer network traffic, both local and WAN/internet, for the purposes of information gathering, evidence collection, or intrusion detection. Traffic is usually intercepted at the packet level, and either stored for later analysis or filtered in real-time. Unlike other areas of digital forensics network data is often volatile and rarely logged, making the discipline often reactionary

6. **Forensics Data Analysis:**

Forensic Data Analysis is a branch of digital forensics. It examines structured data with the aim to discover and analyse patterns of fraudulent activities resulting from financial crime.

7. **Database Forensics:**

Database forensics is a branch of digital forensics relating to the forensic study of databases and their metadata. Investigations use database contents, log files and in-RAM data to build a timeline or recover relevant information.

# Unit III

# Physical Security and Bio-metrics as Security

## Physical Security

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. While most of these are covered by insurance, physical security's prioritization of damage prevention avoids the time, money and resources lost because of these events.

The physical security framework is made up of three main components: access control, surveillance and testing. The success of an organization's physical security program can often be attributed to how well each of these components is implemented, improved and maintained.

### Access control

The key to maximizing one's physical security measures is to limit and control what people have access to sites, facilities and materials. Access control encompasses the measures taken to limit exposure of certain assets to authorized personnel only. Examples of these corporate barriers often include ID badges, keypads and security guards. However, these obstacles can vary greatly in terms of method, approach and cost.

The building is often the first line of defense for most physical security systems. Items such as fences, gates, walls and doors all act as physical deterrents to criminal entry. Additional locks, barbed wire, visible security measures and signs all reduce the number of casual attempts carried out by cybercriminals.

More sophisticated access controls involve a technology-supported approach. ID card scanners and near-field communication (NFC) ID cards are methods of physical authentication that security teams can use to verify the identities of individuals entering and exiting various facilities. Some Swedish companies have recently experimented with embedding NFC microchips below the skin of their employees -- making it extremely difficult to forge or replicate their credentials. Invasive devices like this, however, are much less popular among labor unions, given the degree of physical pain and bodily concern.

Using tactically placed obstacles, organizations can make it more difficult for attackers to access valuable assets and information. Similarly, these barriers increase the time it takes for threat actors to successfully carry out acts of thievery, vandalism or terrorism. The more obstacles that are in place, the more time organizations have to respond to physical security threats and contain them.

But criminals are not the only threat that access controls can minimize. Barriers such as walls and fences can also be used to harden buildings against environmental disasters, such as earthquakes, mudslides and floods. These risks are extremely location-dependent. Organizations that divert resources toward such hardening measures should balance the cost and benefit of their implementation prior to investment.

### Surveillance

This is one of the most important physical security components for both prevention and post-incident recovery. Surveillance, in this case, refers to the technology, personnel and resources that organizations use to monitor the activity of different real-world locations and facilities. These examples can include patrol guards, heat sensors and notification systems.

The most common type of surveillance is closed circuit television (CCTV) cameras that record the activity of a combination of areas. The benefit of these surveillance cameras is that they are as valuable in capturing criminal behavior as they are in preventing it. Threat actors who see a CCTV camera are less inclined to break in or vandalize a building out of fear of having their identity recorded. Similarly, if a particular asset or piece of equipment is stolen, surveillance can provide the visual evidence one needs to identify the culprit and their tactics.

### Testing

Physical security is a preventative measure and incident response tool. Disaster recovery (DR) plans, for example, center on the quality of one's physical security protocols -- how well a company identifies, responds to and contains a threat. The only way to ensure that such DR policies and procedures will be effective when the time comes is to implement active testing.

Testing is increasingly important, especially when it comes to the unity of an organization. Fire drills are a necessary activity for schools and buildings because they help to coordinate large groups, as well as their method of response. These policy tests should be conducted on a regular basis to practice role assignments and responsibilities and minimize the likelihood of mistakes.

Physical security is pretty much exactly what it sounds like; it is the systems used to secure physical space and assets. Physical security encompasses the things employees and guests actually physically touch and the people themselves. Do the right people have access? Are unauthorized people prevented from getting access? The idea of focusing on workplace security is to lessen the probability of physical harm coming to people, property and information. While your network security protects data from being accessed remotely, data is just as likely to be compromised in a physical way. Organizations of all shapes and sizes need to consider their physical security. From the largest to the smallest, they all have something to protect. The primary assets organizations are protecting are: Property, People ad Data.

## Needs

At its core, physical security is about keeping your facilities, people and assets safe from real-world threats. It includes physical deterrence, detection of intruders, and responding to those threats.

While it could be from environmental events, the term is usually applied to keeping people – whether external actors or potential insider threats – from accessing areas or assets they shouldn’t. It could be keeping the public at large out of your HQ, on-site third parties from areas where sensitive work goes on, or your workers from mission-critical areas such as the server room.

Physical attacks could be breaking into a secure data center, sneaking into restricted areas of a building, or using terminals they have no business accessing. Attackers could steal or damage important IT assets such as servers or storage media, gain access to important terminals for mission critical applications, steal information via USB, or upload malware onto your systems.

Rigorous controls at the outermost perimeter should be able to keep out external threats, while internal measures around access should be able to reduce the likelihood of internal attackers (or at least flag unusual behavior).

One of the most common errors a company makes when approaching physical security, according to David Kennedy, CEO of penetration testing firm TrustedSec, is to focus on the front door. “They'll put all of the security in the front door; surveillance cameras, security guards, badge access, but what they don't focus on is the entire building of the whole.”

Smoking areas, on-site gym entrances, and even loading bays may be left unguarded, unmonitored and insecure, he says. Turnstiles or similar barriers that have movement sensors on the exits can also easily be opened by putting a hand through to the other side and waving it around.

While the cost of successful digital attacks keeps increasing, physical damage to your assets can be just as harmful. One notorious example of physical security failing saw a Chicago colocation site robbed four times in two years, with robbers taking 20 servers in the fourth break in.

As businesses become more dependent on the internet of things (IoT), so does the need for digital and physical security. IoT demands a significant amount of physical security to safeguard data, servers and networks. The rising interconnectedness of IoT has expanded the sphere of physical security. Virtual machines (VMs) and applications that run in the cloud, for example, are only as protected as their physical servers.

Whether organizations invest in first-party or third-party cloud computing services, these data centers need to be sufficiently protected using physical security measures to avoid severe data losses.

## Disaster and Controls

When a risk analysis or business impact assessment is performed, a list of all possible threats must be compiled. It does not matter whether the likelihood of any specific vulnerability is low or nonexistent (a tsunami in Ohio, for example); all possible threats must be compiled and examined. Many risk assessment methods and certification and accreditation processes have the practitioner compile these complete lists before making a determination as to their likelihood. The triad of confidentiality, integrity, and availability is at risk in the physical environment and must be protected.

Examples of risks to C.I.A. include:

- Interruptions in providing computer services (Availability)
- Physical damage (Availability)
- Unauthorized disclosure of information (Confidentiality)
- Loss of control over system (Integrity)
- Physical theft (Confidentiality, Integrity, and Availability)

Examples of threats to physical security are:

- Emergencies
    - Fire and smoke contaminants
    - Building collapse or explosion
    - Utility loss (electrical power, air conditioning, heating)
    - Water damage (pipe breakage)
    - Toxic materials release

- Natural disasters
    - Earth movement (such as earthquakes and mudslides)
    - Storm damage (such as snow, ice, and floods)

- Human intervention
    - Sabotage
    - Vandalism
    - War
    - Strikes

## Basic Tenets of Physical Security and Physical Entry Controls

Now for the power. In addition to the electrical wires hidden from prying human eyes, we should also ensure access to a stabilized energy source. In this way we prevent the risks associated with excess energy (breakdown, voltage spikes) or deficient (low voltage or current, no power). This can be done using the

UPS devices. Unregulated energy sources can also cause damage to electronic components, data loss, and faulty network connections.

### Physical Security Controls

Physical controls are the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material.
Examples of physical controls are:

- Closed-circuit surveillance cameras
- Motion or thermal alarm systems
- Security guards
- Picture IDs
- Locked and dead-bolted steel doors
- Biometrics (includes fingerprint, voice, face, iris, handwriting, and other automated methods used to recognize individuals)

### Physical Entry Controls

These are the secure areas that need to be protected by the appropriate entry controls to ensure only authorized personnel are allowed access. As a really basic example, only those employees who have been given the alarm access code and received a key can access the office. Examples include physical controls such as fences, locks, and alarm systems; technical controls such as antivirus software, firewalls, and IPSs; and administrative controls like separation of duties, data classification, and auditing. Physical entry control includes-:

- Password
- Passphrase
- Biometric
- Smart Card

Entry control systems consist of the hardware and procedures used to verify entry authorization. Methods of personnel entry authorization include credentials (such as badges), personal identification numbers (PIN), and automated biometric verification. Prohibited item detection typically occurs at entry points and is often interfaced with the entry control system. This paper discusses the above methods and examples of available hardware. An effective entry control system cannot be easily bypassed, allows observation by the response force (guards), protects guards, accommodates peak loads, performs personnel and material control, blocks passage until personnel and material control are complete, is under surveillance by the central alarm station, provides secondary inspection for those who cannot pass the automated inspection, and is designed for both entry and exit.

## Physical Access Control

Physical Access Control is the restriction of access to a certain building or space that often isn't enough protection in today's world. A locked door is a pretty good way to keep unwanted people out of a space, but how can you make sure the right people have access to your data? That's where logical access control comes in. While physical access control systems employ credentials like keycards, key fobs, or mobile credentials to restrict, allow and manage who can enter a space or building, logical access control takes security one step further by requiring identity authorization, and using processes like entry schedules and entry requirements to limit access.

In other words, there are two requirements to gain entry: something you have, and something you know. Something you have might be a keycard or fob, and something you know will be a more personal identifier that is harder for another person to obtain, like a PIN code, password, or facial ID.

Advanced physical access control systems, for example, will use this multi-factor authentication method by combining a physical barrier, like a gate, door or a turnstile, with a user authorization credential, like a password or biometric scan, to ensure only authorized individuals have access to high-security areas. Using a mobile credential for access can automatically incorporate the extra protection of logical access control. Your smartphone requires a password, fingerprint or FaceID to unlock, which makes it harder for would-be criminals to gain entry — they would need to have possession of the phone and be able to unlock it, just to get through the door. When it comes to protecting your data, using physical access control systems that employ multi-factor authentication is the first step in a comprehensive cybersecurity plan in the digital age.

Physical access control systems (PACS) are a type of physical security designed to restrict or allow access to a certain area or building. Often, PACS are installed in order to protect businesses and property from vandalism, theft, and trespassing, and are especially useful in facilities that require higher levels of security and protection. Unlike physical barriers like retaining walls, fences or strategic landscaping, physical access control procedures control who, how and when a person can gain entry. The following are the main components of a physical access control system:

Access point: The entrance point where the barrier is needed. Common physical access control examples of access points include security gates, turnstiles and door locks. A secure space can have a single access point, like an office inside a larger complex, or many access points.

Personal credentials: Most PACS require a user to have identifying credentials to enter a facility or access data. Physical access control examples of credentials include fobs and key card entry systems, encrypted badges, mobile credentials, PIN codes and passwords. Personal credentials tell the system who is trying to gain entry.

Readers and/or keypads: Stationed at the access point, readers send data from credentials to a control panel to authenticate the credential and request access authorization. If using a keypad or biometric reader (such a fingerprint scan, facial ID, or retina scan), users will enter their PIN or complete a scan prior to obtaining access.

Control panel: The PACS control panel receives the credential data from the reader and verifies if the credential is valid. If the credential data is approved, the control panel transmits authorization data to the access point via the access control server, and the door will unlock. If the credential data is not approved, the user will not be able to gain entry.

Access control server: The access control server stores user data, access privileges, and audit logs. Depending on your system, the server might be on-premises, or managed in the cloud. System maintenance and software updates should be performed regularly to protect the system from hacking and possible security breaches.

## Biometrics

For a quick biometrics definition: Biometrics are biological measurements — or physical characteristics — that can be used to identify individuals. For example, fingerprint mapping, facial recognition, and retina scans are all forms of biometric technology, but these are just the most recognized options.

Researchers claim the shape of an ear, the way someone sits and walks, unique body odors, the veins in one’s hands, and even facial contortions are other unique identifiers. These traits further define biometrics.

Three Types of Biometrics Security

While they can have other applications, biometrics have been often used in security, and you can mostly label biometrics into three groups:

- Biological biometrics
- Morphological biometrics
- Behavioral biometrics

**Biological biometrics** use traits at a genetic and molecular level. These may include features like DNA or your blood, which might be assessed through a sample of your body's fluids.

**Morphological biometrics** involve the structure of your body. More physical traits like your eye, fingerprint, or the shape of your face can be mapped for use with security scanners.

**Behavioral biometrics** are based on patterns unique to each person. How you walk, speak, or even type on a keyboard can be an indication of your identity if these patterns are tracked.

## Factors in Biometric Systems

The success of a biometric system often depends on choosing the right biometric modality, but it isn't easy. Careful research that includes rigorous comparisons of modality strengths and weaknesses is an important element to help select the right hardware. Factors to consider in the comparison may include: specifications, convenience, usability, acceptability, effectiveness, and budget.

There are many biometric modalities available including fingerprint, finger vein, facial recognition, iris, voice, signature, gait, and more. It's important to understand that not all biometric modalities have the ability to meet the requirements of every organization, it depends largely on the industry application context.

It's important to realize that there is not one biometric modality which is best for all conditions and implementations. Many factors must be taken into account when implementing a biometric device including location, security, acceptability, and ease of use. However, performance and cost may vary when taking into consideration deployment requirements and environment. At times deployments may require combining two biometric modalities (i.e. "multimodal" biometrics) to ensure optimal accuracy. Choosing the right modality is important to maximize the full benefits from a biometric system.

There are some important factors which should be considered before choosing a biometric modality. These include:

- Accuracy

Accuracy is one of the most important aspects to assess when choosing a biometric modality. It is based on several criteria including error rate, false acceptance rate (FAR), identification rate, false reject rate (FRR) and additional biometric system standards.

- Anti-spoofing capabilities

As biometric recognition systems become more widespread, more attention has been given to possible direct attacks, where potential intruders may gain access to the system by interacting with the system input device. Such attempts are commonly referred as spoofing attacks. Strong anti-spoofing protection is a must have capability for the right biometric modality.

- Acceptability

User acceptance is the linchpin of biometric identification management deployment success. Certain biometric modalities may have a stigma associated with them (e.g. – fingerprint biometrics and criminality) which can negatively impact user perception in certain cultures. Understanding which modalities are acceptable versus those that may cause user acceptance issues is important.

- Cost effectiveness

Cost is an important factor to consider when choosing the best and most effective biometric hardware modality. Depending on the underlying technology and hardware characteristics, certain modalities may be more cost effective than others. It’s important to recognize that an initial investment in biometrics can and is quite often recouped in a short amount of time to achieve fast return on investment (ROI).

- Hygiene

Contact dependent biometric hardware is an important factor to consider before making an investment. Many new deployments in industries that pay close attention to infection control prefer to use contactless biometric modalities for hygienic reasons.

## Benefits of Biometric Systems

Biometrics have offered a scalable solution to business owners who are now empowered to circumvent issues like undocumented access, ID swapping, manual badge checks, credential replacements and more. There have been many developments in the field of biometrics, which means things are more reliable and costs are down. Biometrics offer high level identification management security operations that have several advantages over traditional means and now they are available to you at lower costs.

### Accurate Identification

While traditional security systems are reliant on passwords, personal identification numbers (PINs) or smart cards, you can achieve a high level of accuracy with biometrics systems. If you have set up the system correctly, you can use biological characteristics like fingerprints and iris scans, which offer you unique and accurate identification methods. These features cannot be easily duplicated, which means only the authorized person gets access and you get high level of security.

### Accountability

Biometric log-ins mean a person can be directly connected to a particular action or an event. In other words, biometrics creates a clear, definable audit trail of transactions or activities. This is especially handy in case of security breaches because you know exactly who is responsible for it. As a result you get true and complete accountability, which cannot be duplicated.

### Easy and Safe for Use

The good thing about using biometrics for identificaiton is that modern systems are built and designed to be easy and safe to use. Biometrics technology gives you accurate results with minimal invasiveness as a simple scan or a photograph is usually all that’s required. Moreover the software and hardware can be easily used and you can have them installed without the need for excessive training.

### Time Saving

Biometric identification is extremely quick, which is another advantage it has over other traditional security methods. A person can be identified or rejected in a matter of seconds. For those business owners that understand the value of time management the use of this technology can only be beneficial to your office revenue by increasing productivity and reducing costs by eliminating fraud and waste.

## User Friendly Systems

You can have biometrics systems installed rather easily and after that, they do their job quickly, reliably and uniformly. You will need only a minimum amount of training to get the system operational and there is no need for expensive password administrators. If you use high quality systems, it will also mean your maintenance costs are reduced to minimize the expenses of maintaining an ongoing system.

## Security

Another advantage these systems have is that they can't be guessed or stolen; hence they will be a long term security solution for your company. The problem with efficient password systems is that there is often a sequence of numbers, letters, and symbols, which makes them difficult to remember on a regular basis. The problem with tokens is that they can be easily stolen or lost – both these traditional methods involve the risk of things being shared. As a result you can't ever be really sure as to who the real user is. However that won't be the case with biometric characteristics, and you won't have to deal with the problem of sharing, duplication, or fraud.

## Convenience

It's considered to be a convenient security solution because you don't have to remember passwords, or carry extra badges, documents, or ID cards. You are definitely saved the hassle of having to remember passwords frequently or changing cards and badges. People forget passwords and ID cards are lost, which can be a huge nuisance with traditional security methods.

## Versatility

There are different types of biometrics scanners available today and they can be used for various applications. They can be used by companies at security checkpoints including entrances, exits, doorways, and more.

Moreover you can make the most out of the biometric solutions to decide who can access certain systems and networks. Companies can also use them to monitor employee time and attendance, which raises accountability.

## Scalability

Biometrics systems can be quite flexible and easily scalable. You can use higher versions of sensors and security systems based on your requirements. At the lowest level you can use characteristics that are not very discriminative; however if you are looking for a higher level of security for large scale databases then you can use systems with more discriminable features, or multi-modal applications to increase identification accuracy.

## Return on Investment

It's definitely high because you can avoid fraud including "buddy punching," besides lowering payroll costs, accurate calculation of work hours, and reduced management time. While the security is improved you can also easily apply consistent policies and procedures at the same time. And all you have to think about is the initial cost of the biometric system.

You can benefit from biometrics systems to a great extent and do away with the need to remember passwords and combinations. Rather than remembering the password for a computer system or a combination to a safe, you can offer unique biometrics information and get access. The job will be done quickly, accurately, with a fast implementation schedule and minimal training.

## Criteria Selection of Biometric Techniques

There are many decision factors for selecting a particular biometric technology for a specific application.

a) Economic Feasibility or Cost - The cost of biometric system implementation has decreased recently; it is still a major barrier for many companies. Traditional authentication systems, such as passwords and PIN, require relatively little training, but this is not the case with the most commonly used biometric systems. Smooth operation of those systems requires training for both systems administrators and users

b) Risk Analysis - Error rates and the types of errors vary with the biometrics deployed and the circumstances of deployment. Certain types of errors, such as false matches, may pose fundamental risks to business security, while other types of errors may reduce productivity and increase costs. Businesses planning biometrics implementation will need to consider the acceptable error threshold.

c) Perception of Users - Users generally view behavior-based biometrics such as voice recognition and signature verification as less intrusive and less privacy-threatening than physiology-based biometrics.

d) Techno-Socio Feasibility - Organizations should focus on the user-technology interface and the conditions in the organizational environment that may influence the technology's performance. The organization should create awareness among the users how to use the techniques and should overcome the psychological factors as user fears about the technology. Organization has to also consider the privacy rights of users while implementing the biometric techniques.

e) Security - Biometric techniques should have high security standards if they will be implemented in high secure environment. The biometric techniques should be evaluated on the basis of their features, potential risk and area of application, and subjected to a comprehensive risk analysis.

f) User friendly and social acceptability - Biometric techniques should be robust and user friendly to use and they should function reliably for a long period of time. The techniques should not divide the society into two group i.e. digital and non digital society.

g) Legal Feasibility **-** Government has to form a regulatory statutory framework for the use of biometric techniques in various commercial applications. It should form a standard regulatory framework for use of these techniques in commercial applications or transactions. If required the framework has to be regulated and changed time to time.

h) Privacy - As biometric techniques rely on personal physical characteristics, an act has to be made to protect the individual's privacy data not to be used by other. A data protection law has to be created in order to protect the person's privacy data.

## Design Issues of Biometrics

While biometric systems can offer greater levels of security, various attacks exist to gain unauthorized access to a system that is protected by biometric authentication. The various issues of the biometric system are dealt here. System design issues Biometrics is invariably associated with security; hence the biometric system itself should be reasonably secure and trustworthy.

Some of the biometric security issues are :-

1) Rogue sensors and unauthorized acquisition of biometricϖ samples
2) Communications security between sensors, matchers andϖ biometric databases
3) Accuracy
4) Speed
5) Scalability
6) Resilience
7) Cost
8) Privacy

# Interoperability Issues

Interoperability is a factor to consider when designing almost any kind of system. It must ofcourse be considered when discussing data exchange between systems but must also be considered for evolving systems that retain and reuse data collected over time. In other words, even closed systems might have to interoperate with multiple generations and instantiations of themselves as they change over time. Interoperability also plays a role at the subsystem level, when systems are composed of vendor software or hardware. In the biometric system context, such components may include fingerprint matcher components, segmentation software, and minutiae detectors.

In general, standards help to promote interoperability. However, there are times when the use of a standard format in preference to a proprietary format can be detrimental and potentially limit functionality or flexibility. For biometric systems, sensor interoperability, discussed below, poses some specific challenges.

## Sensor Interoperability

Sensor interoperability refers to the compatibility between an enrolled biometric reference and a test sample, acquired using different sensors. In some systems, it is assumed that the two samples to be compared were acquired using the same sensor—or at least the same type and vintage of sensor. However, improvements in sensor technology and reduction in sensor costs means that enrollment and test samples are often obtained using different sensor types. This may also happen if a sensor manufacturer goes out of business and support is no longer available for a line of sensors. In a large, distributed system such as the FBI's Integrated Automated Fingerprint Identification System (IAFIS), remote sites use a variety of end-point systems and may collect samples using a variety of certified sensors. In short, it is possible in almost any biometric system that test samples will not be collected using the same sensor as used in enrollment. (In criminal justice systems, there is no known change in error rates when each booking site selects whichever certified scanning system it wants.) It has been observed that the matching performance drops when the reference and test samples for fingerprint, iris, and voice are acquired using different sensors rather than the same.

There are several reasons for this degradation in matching performance: (1) change in the sensor resolution and its operating behavior; (2) change in the sensor technology; (3) change in the user interface, and (4) changes in operational environment that have an impact on sensor performance. In the first case, while the underlying sensing technology remains the same—in, for example, an optical total internal reflection (TIR) fingerprint sensor—the image resolution (say from 300 by 300 to 500 by 500 pixels per inch) and/or the signal to noise ratio (SNR) of the sensor may change. In the second case, the two sensors providing reference and test samples may be based on completely different technologies (for example, one may be an optical TIR fingerprint sensor and one a capacitive solid state sensor). Of the factors listed, the second is more problematic because the change in sensor technology may decrease compatibility between enrolled references and test samples. There are multiple examples of different sensing technologies for a given modality. For example, sensors for fingerprints can be based on optical, capacitive, thermal, pressure, ultrasound, or multispectral technologies. Some touchless three-dimensional fingerprint sensors are being developed as well. Differences in how a user must interact with a sensor may introduce variations in sample coverage area and distortion. Similarly, two-dimensional images for face recognition can be captured in visible color, infrared, and thermal, as well as range (depth). Three-dimensional face images that capture the depth image are also being used for face recognition; these so-called range sensors capture a different face modality than the usual two-dimensional intensity or texture images captured by charge-coupled device (CCD) cameras.

Sensor interoperability is a major concern in large biometric installations, since it is expensive and time consuming to re-enroll a large number of subjects as the technology evolves and access to the subject population may become limited. In some cases, re-enrollment may be unavoidable and should be viewed as part of upgrading the infrastructure. To the extent possible, of course, representations of traits that perform well across existing and anticipated technologies are desirable.

### Human Interface Interoperability

One aspect of interoperability is the development of standardized human interfaces that would allow the data subject to know what to expect when interacting with a biometric system and how to control the recognition process. Although other technology interfaces such as are found in automatic teller machines, automobiles, televisions, and self-service gasoline pumps have a level of standardization that allows transferring experience gained with one system to other systems, little has been done in this area for biometrics, and these mass-market interfaces can confuse even experienced users on occasion. More standardized user interfaces coupled with broader human factors testing would contribute to greater maturity in all biometric applications.

## Economic Aspect

There are various ways to describe the economic factors affecting biometric development, adoption and use. Biometric technologies are strong recognition techniques and as such they influence the level of trust in economic transactions. In other words, they can help reduce fraud and thus help materialize the efficiency, development and equity gains of the information society. Their widespread deployment in the public sector can make recognition over the network easier, more secure and may bring down costs per secure transaction. Biometric solution in the cloud has an additional economic impact, unlike standard biometric solutions, because with the introduction of such cloud-based service we save more. Evidence to that is also the announcement of the Slovenian government to establish a national computing cloud with which it aims to cut costs by 45 million Euros. By moving services to the cloud there is no longer need to maintain multiple systems within companies or public institutions. There is also a new way of charging for services - pay-as-you-go. Furthermore, economic gains of cloud solutions result mainly from the following areas:

- Cost of power- Power Usage tends to be significantly lower in large facilities than in smaller one. That means big companies profit more than small one (regarding power usage).
- Infrastructure labour costs: Labour costs are significantly lower at any scale by automating many repetitive management's tasks. Larger facilities are able to lower them further than smaller ones.
- Security and reliability: Large cloud providers are often better able to bring deep expertise to bear on this problem than a typical corporate IT department, thus, actually making cloud systems more secure and reliable. Integration of biometrics introduces additional level of trust and increases security.
- Buying power: Operators of large data centres can get discount on hardware purchases over small buyers.

## Social Aspect

As with any technology, the developmental impact of biometric identification on society depends largely on the political, technological, and legal context in which it is used. Some cases suggest large returns on biometric identification in economic and social programs, with potential gains in efficiency, governance, and inclusion. One key conclusion is that identification services should become a standard element of development planning, including the delivery of social services. Rather than funding one-off applications, it is better to strengthen on-going gidentity management systems with multiple possible uses. Biometric services in the cloud provide exactly that possibility, since such system can be easily integrated into existing identity management systems.

There are certainly some particular social concerns related to biometrics, as there are with any particular tool or technology. From a social perspective, resistance to change to an unfamiliar technology could manifest itself in various ways. Systems of such complexity and infrastructural coherence must be deployed with a great caution. From this perspective, it is vital that additional research is carried out with the aim of examining the acceptability of such technologies at respective national levels and documenting clear contextual factors that are associated with cultural and broader social aspects that might be crucial for the acceptability of such systems, a fundamental element for their success. Biometric systems in the cloud assume and require an intimate relationship between people and technologies that collect and record the biological and behavioral characteristics of their bodies. The key social challenge surrounding biometrics is the seemingly irrevocable link between biometric traits and a persistent information record about a person. Unlike most other forms of recognition, biometric techniques are firmly tied to our physical bodies. Cost of failure in such systems is very high. If you lose a credit card, you can cancel it and get a new one. If a biometric trait is stolen, you've lost it for life. Any biometric system must be built to the highest levels of data including t you transmission that prevents interception, storage that prevents theft, and system-wide architecture to prevent both intrusion and compromise by corrupt or deceitful agents within the security organization. The tight link between personal records and biometrics can have both positive and negative consequences for individuals and for society at large. Convenience, improved security, and fraud reduction are some of the benefits often associated with the use of biometrics. These benefits may flow to particular individuals, corporations, and societies. All are sometimes realized only at the expense of others. Who benefits at whose expense and the relative balance between benefits and costs can influence the success of such biometric relative deployments.

Negative effects of identification using biometric methods should also be taken into account. Yet many common fears relate to identification more generally and are not specific to biometric technology. The most common fears are the risk of exclusion, threats to privacy and cos efficiency. A small percentage of the population cannot present suitable features to participate in certain biometric system. For example, when using fingerprint-based biometric system, it should be noted that some people have fingers that simply do not print well. Those who may have difficultly are infants, the elderly, and manual labourers, who are often already marginalized within society. Even if people with bad prints represent 1% of the population, this would mean massive inconvenience and suspicion for that minority. Because of that, it should always be possible to use an alternative. Taking multiple biometrics (multi-modality) can minimize this risk and almost guarantee identity. Still, there must be an alternative, such as the use of usernames and passwords in combination with secure certificates.

Second fact is that there will also be those who decline to participate on the basis of religious values, cultural norms, or even an aversion to the process. Religious beliefs about the body and personal characteristics or interpersonal contact (for example, taking photographs, touching or exposing parts of the body) may make a biometric system an unacceptable intrusion. Mandatory or strongly encouraged use of such a system may undermine religious authority and create de facto discrimination against certain groups whose members are not allowed to travel freely, take certain jobs, or obtain certain services without those violating their religious beliefs. Another category of people who may choose not to participate is concerned about misuse or compromise of the system or its data and its implications for privacy and personal liberty. Although a decision to participate or not may be an individual one, biometric systems can inadvertently affect groups whose shared characteristics make them less inclined to use the systems, assuming that participation is voluntary. Where use is mandatory even more consideration of these challenges may be needed [25]. By far the most significant negative is designed aspect of biometric systems is their potential to locate and track people physically. While many surveillance systems seek to locate and track, biometric systems present the greatest danger precisely because they promise extremely high accuracy. Whether a specific biometric system actually poses a risk of such tracking depends on how it is

The societal impact of biometric systems in the cloud will vary significantly depending on their type and purpose. The potential impacts on particular social groups and thus their receptions by these groups may also vary dramatically due to differences in how the group interprets the cultural beliefs, values, and specific behaviors. System performance may be degraded if social factors are not adequately taken into consideration. These factors are of two types: those that motivate and those that facilitate participant engagement with the system. As a rule, people's willingness to participate in a system and their commitment to it their understanding of its benefits. For example, a biometric system that allows convenie access to a worksite might be perceived as beneficial to individuals by relieving them of necessity to carry an identification card. On the other hand, a biometric system that tracks it depends on daytime movement of employees might be perceived as primarily beneficial to the employer and as undermining the employee's personal freedom. Participation may also be motivated by the possibility of negative consequences for nonparticipation - for instance restrictions on access to locations or services (perhaps entry to the United States), requirements to use a much lengthier process for a routine activity (for example to open a bank account), and even the threat of legal action (for example the requirement to enroll in a biometric system in order to maintain legal alien status). Nonparticipation may also subject individuals to social pressure and/or prevent them from joining some collective activities. At a basic level, biometrics with cloud computing can strengthen core identity systems like civil registries and national identification cards. Beyond these foundational applications, especially when combined with other advances in information and communications technology. It can also be leveraged for more functional purposes (voting, transfers or enabling financial access, health care systems, health insurance systems etc.) that facilitate access to rights and services, and strengthen public accountability. Relative to alternatives, biometric identification in the cloud can increase inclusion, privacy and efficiency, and may save greatly in the long run due to more automation and reduced fraud.

The implementation of biometric solution in the cloud could improve people's quality of life in terms of more secure authentication over multiple government and non-government services and applications, but there are also multiple social concerns that needs to be considered.

## Legal Challenges

As a future information security professional, you must understand the scope of an organization’s legal and ethical responsibilities. The information security professional plays an important role in an organization’s approach to managing liability for privacy and security risks. In the modern litigious societies of the world, sometimes laws are enforced in civil courts, where large damages can be awarded to plaintiffs who bring suits against organizations. Sometimes these damages are punitive—assessed as a deterrent. To minimize liability and reduce risks from electronic and physical threats, and to reduce all losses from legal action, information security practitioners must thoroughly understand the current legal environment, stay current with laws and regulations, and watch for new and emerging issues. By educating the management and employees of an organization on their legal and ethical obligations and the proper use of information technology and information security, security professionals can help keep an organization focused on its primary objectives.

### Law and Ethics in Information Security

In general, people elect to trade some aspects of personal freedom for social order. As Jean-Jacques Rousseau explains in The Social Contract, or Principles of Political Right, the rules the members of a society create to balance the individual rights to self-determination against the needs of the society as a whole are called laws. Laws are rules that mandate or prohibit. No distribution allowed without express authorization. 3 certain behavior; they are drawn from ethics, which define socially acceptable behaviors. The key difference between laws and ethics is that laws carry the authority of a governing body, and ethics do not. Ethics in turn are based on cultural mores: the fixed moral attitudes or customs of a particular group. Some ethical standards are universal. For example, murder, theft, assault, and arson are actions that deviate from ethical and legal codes throughout the world.

### Organizational Liability and the Need for Counsel

What if an organization does not demand or even encourage strong ethical behavior from its employees? What if an organization does not behave ethically? Even if there is no breach of criminal law, there can still be liability. Liability is the legal obligation of an entity that extends beyond criminal or contract law; it includes the legal obligation to make restitution, or to compensate for wrongs committed. The bottom line is that if an employee, acting with or without the authorization of the employer, performs an illegal or unethical act that causes some degree of harm, the employer can be held financially liable for that action. An organization increases its liability if it refuses to take measures known as due care. Due care standards are met when an organization makes sure that every employee knows what is acceptable or unacceptable behavior, and knows the consequences of illegal or unethical actions. Due diligence requires that an organization make a valid effort to protect others and continually maintains this level of effort. Given the Internet’s global reach, those who could be injured or wronged by an organization’s employees could be anywhere in the world. Under the U.S. legal system, any court can assert its authority over an individual or organization if it can establish jurisdiction—that is, the court’s right to hear a case if a wrong is committed in its territory or involves its citizenry. This is sometimes referred to as long arm jurisdiction—the long arm of the law extending across the country or around the world to draw an accused individual into its court systems. Trying a case in the injured party’s home area is usually favorable to the injured party.

### Policy Versus Law

Within an organization, information security professionals help maintain security via the establishment and enforcement of policies. These policies—guidelines that describe acceptable and unacceptable employee behaviors in the workplace—function as organizational laws, complete with penalties, judicial practices, and sanctions to require compliance. Because these policies function as laws, they must be crafted and implemented with the same care to ensure that they are complete, appropriate, and fairly applied to everyone in the workplace. The difference between a policy and a law, however, is that ignorance of a policy is an acceptable defense. Thus, for a policy to become enforceable, it must meet the following five criteria:

● Dissemination (distribution)—The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.

● Review (reading)—The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees. Common techniques include recordings of the policy in English and alternate languages.

● Comprehension (understanding)—The organization must be able to demonstrate that the employee understood the requirements and content of the policy. Common techniques include quizzes and other assessments. Legal, Ethical, and Professional Issues in Information Security 91 © Cengage Learning. All rights reserved. No distribution allowed without express authorization.

● Compliance (agreement)—The organization must be able to demonstrate that the employee agreed to comply with the policy through act or affirmation. Common techniques include logon banners, which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.

● Uniform enforcement—The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Only when all of these conditions are met can an organization penalize employees who violate the policy without fear of legal retribution.

### Types of Law

Civil law comprises a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizational entities and people. Criminal law addresses activities and conduct harmful to society, and is actively enforced by the state. Law can also be categorized as private or public. Private law encompasses family law, commercial law, and labor law, and regulates the relationship between individuals and organizations. Public law regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments. Public law includes criminal, administrative, and constitutional law.

## Framework for Information Security

The challenges of running an information security program can be overwhelming with so many areas to address -- from encryption, to application security to disaster recovery. The complication of compliance with regulatory requirements such as HIPAA, PCI DSS and Sarbanes-Oxley, to name a few, adds to the mix. How should security professionals organize and prioritize their efforts in order to build and maintain an information security program?

This is where IT security frameworks and standards can be helpful. To help manage the process, let's delve into what an information security framework is and discuss a few of the more popular frameworks and how they are used.

What is an IT security framework?

An IT security framework is a series of documented processes used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment. These frameworks are basically a blueprint for building an information security program to manage risk and reduce vulnerabilities. Information security pros can utilize these frameworks to define and prioritize the tasks required to build security into an organization.

Frameworks are often customized to solve specific information security problems, just like building blueprints are customized to meet their required specifications and use. Some frameworks were developed for specific industries, as well as different regulatory compliance goals. They also come in varying degrees of complexity and scale. You will find that there is a large amount of overlap in these frameworks in terms of general security concepts as each evolves.

## COBIT

Control Objectives for Information and Related Technology (COBIT) is a framework developed in the mid-90s by ISACA, an independent organization of IT governance professionals. ISACA currently offers the well-known Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) certifications. This framework started out primarily focused on reducing technical risks in organizations, but has evolved recently with COBIT 5 to also include alignment of IT with business-strategic goals. It is the most commonly used framework to achieve compliance with Sarbanes-Oxley rules.

## ISO 27000 series

The ISO 27000 series was developed by the International Standards Organization. It provides a very broad information security framework that can be applied to all types and sizes of organizations. It can be thought of as the information security equivalent of ISO 9000 quality standards for manufacturing, and even includes a similar certification process. It is broken up into different substandards based on the content. For example, ISO 27000 consists of an overview and vocabulary, while ISO 27001 defines the requirements for the program. ISO 27002, which was evolved from the British standard BS 7799, defines the operational steps necessary in an information security program.

Many more standards and best practices are documented in the ISO 27000 series. ISO 27799, for example, defines information security in healthcare, which could be useful for those companies requiring HIPAA compliance. New ISO 27000 standards are in the works to offer specific advice on cloud computing, storage security and digital evidence collection. ISO 27000 is broad and can be used for any industry, but the certification lends itself to cloud providers looking to demonstrate an active security program.

## NIST Special Publication 800-53

The U.S. National Institute of Standards and Technology (NIST) has been building an extensive collection of information security standards and best practices documentation. The NIST Special Publication 800 series was first published in 1990 and has grown to provide advice on just about every aspect of information security. Although not specifically an information security framework, other frameworks have evolved from the NIST SP 800-53 model. U.S. government agencies utilize NIST SP 800-53 to comply with the Federal Information Processing Standards' (FIPS) 200 requirements. Even though it is specific to government agencies, the NIST framework could be applied in any other industry and should not be overlooked by companies looking to build an information security program.

## NIST Special Publication 800-171

NIST SP 800-171 has gained in popularity in recent years due to the requirements set by the U.S. Department of Defence that mandated contractor compliance with the security framework by December 2017. Cyberattacks are occurring throughout the supply chain, and government contractors will find their systems and intellectual property a frequent target used to gain access into federal information systems. For the first time, manufacturers and their subcontractors now have to implement an IT security framework in order to bid on new business opportunities.

NIST SP 800-171 was a good choice for this requirement as the framework applies to smaller organizations as well. It is focused on the protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations, which aligns well with manufacturing or other industries not dealing with information systems or bound by other types of compliance. It may not be a good fit by itself for industries dealing with more sensitive information such as credit cards or Social Security data, but it is freely available and allows for the organization to self-certify using readily available documentation from NIST.

The controls included in the NIST SP 800-171 framework are directly related to NIST SP 800-53, but they are less detailed and more generalized. It is still possible to build a crosswalk between the two standards if an organization has to show compliance with NIST SP 800-53 using NIST SP 800-171 as the base. This allows a level of flexibility for smaller organizations that may grow over time as they need to show compliance with the additional controls included in NIST SP 800-53.

## NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity

The NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity is yet another framework option from NIST. It was recently developed under Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity" that was released in February 2013. This standard is different in that it was specifically developed to address U.S. critical infrastructure, including energy production, water supplies, food supplies, communications, healthcare delivery and transportation. These industries have all found themselves targeted by nation-state actors due to their strategic importance to the U.S. and must maintain a higher level of preparedness.

The NIST Cybersecurity Framework differs from the other NIST frameworks in that it focuses on risk analysis and risk management. The security controls included in this framework are based on the defined phases of risk management: identify, protect, detect, respond and recovery. These phases include the involvement of management, which is key to the success of any information security program. This structured process allows the NIST Cybersecurity Framework to be useful to a wider set of organizations with varying types of security requirements.

## CIS Controls (formerly the SANS Top 20)

The CIS Controls exist on the opposite spectrum from the NIST Cybersecurity Framework. This framework is a long listing of technical controls and best practice configurations that can be applied to any environment. It does not address risk analysis or risk management like the NIST Cybersecurity Framework, and is solely focused on hardening technical infrastructure to reduce risk and increase resiliency.

The CIS Controls are a welcome addition to the growing list of security frameworks because they provide direct operational advice. Information security frameworks can sometimes get caught up on the risk analysis treadmill but don't reduce overall organizational risk. The CIS Controls pair well with these existing risk management frameworks to help remediate identified risks. They are also a highly useful resource in IT departments that lack technical information security experience.

## HITRUST CSF

It is well known that the HITECH/HIPAA Security Rule has not been successful in preventing data breaches in healthcare. The original HIPAA compliance requirements were written in 1996 and set to apply to a broad set of technologies and organizations. More than 230 million people in the U.S. have had their data breached by a healthcare organization, according to the Department of Health and Human Services. The overly general requirements included HIPAA and the lack of operational direction as partly to blame for this situation. HITRUST CSF is attempting to pick up where HIPAA left off and improve security for healthcare providers and technology vendors. It combines requirements from almost every compliance regulation in existence, including the EU's GDPR. It includes both risk analysis and risk management frameworks, along with operational requirements to create a massive homogenous framework that could apply to almost any organization and not just those in healthcare.

HITRUST is a massive undertaking for any organization due to the heavy weighting given to documentation and processes. Many organizations end up scoping smaller areas of focus for HITRUST compliance as a result. The costs of obtaining and maintaining HITRUST certification adds to the level of effort required to adopt this framework as well. However, the fact that the certification is audited by a third party adds a level of validity similar to an ISO 27000 certification. Organizations that require this level of validation may be interested in the HITRUST CSF.

The beauty of any of these frameworks is that there is overlap between them so "crosswalks" can be built to show compliance with different regulatory standards. For example, ISO 27002 defines information security policy in section 5; COBIT defines it in the section "Plan and Organize;" Sarbanes-Oxley defines it as "Internal Environment;" HIPAA defines it as "Assigned Security Responsibility;" and PCI DSS defines it as "Maintain an Information Security Policy." By using a common framework like ISO 27000, a company can then use this crosswalk process to show compliance with multiple regulations such as HIPAA, Sarbanes-Oxley, PCI DSS and GLBA, to name a few.

IT security framework advice

The choice to use a particular IT security framework can be driven by multiple factors. The type of industry or compliance requirements could be deciding factors. Publicly traded companies will probably want to stick with COBIT in order to more readily comply with Sarbanes-Oxley. The ISO 27000 series is the magnum opus of information security frameworks with applicability in any industry, although the implementation process is long and involved. It is best used, however, where the company needs to market information security capabilities through the ISO 27000 certification. NIST SP 800-53 is the standard required by U.S. federal agencies but could also be used by any company to build a technology-specific information security plan. The HITRUST CSF integrates well with healthcare software or hardware vendors looking to provide validation of the security of their products. Any of them will help a security professional organize and manage an information security program. The only bad choice among these frameworks is not choosing any of them.

# Security Metrics

Information Security Metrics are powerful tools that every organization must use to measure and thereby improve performance of controls. Security Metrics can also provide important data points for an organization to ensure they prioritize between areas of focus and justify resource spend (time and money).

## 10 Cybersecurity Metrics to Be Monitor

Effective management of varying performance indices in information security can mean the difference between a practical and efficient project and a complete waste of money.
Although managers have been following KPIs for quite some time now, in information security, this is an uncommon and still developing practice to track cyber security metrics.
So, here are some suggestions for cybersecurity metrics that can and should be tracked to ensure the efficiency of your security projects.

1. Mean-Time-to-Detect and Mean-Time-to-Respond

Mean Time To Identify (MTTI) and Mean Time To Contain (MTTC) for US companies indicates that the Detect and Respond Phases are suffering. In fact, the MTTC in 2017 was 208 days and the MTTI was 52 days. At the same time, likelihood of incurring a mean breach cost of $2.25M is almost 28% over the next 24 months for U.S. companies. Poor performance in MTTI and MTTC is a huge contributor to breach costs. These should be your two most important KPIs when measuring information security. It’s also a good KPI for CISOs to measure and show their Board for long-term improvement. Everyone on the security team should prioritize improving these two KPIs.

2. Number of systems with known vulnerabilities

Knowing the number of vulnerable assets in your environment is a key cybersecurity metric to determining the risk that your business incurs. Managing updates and patches is a complex process, but very important to avoid loopholes that can be exploited in your environment. A vulnerability scan that includes all the assets will indicate what needs to be done to improve the security posture of your company. A vulnerability management program not a nicety, but a necessity.

3. Number of SSL certificates configured incorrectly

An SSL certificate is a small file that certifies the ownership of a cryptographic key to the website or company with which data is being exchanged, guaranteeing the authenticity of the transaction. Monitoring the security requirements for each certificate, as well as ensuring that they are properly configured on servers, prevents them from falling into the wrong hands and that your company's digital identity is not used to steal user information.

4. Volume of data transferred using the corporate network

If your employees have unrestricted access to the internet through the corporate network, monitoring the volume of traffic allows you to identify misuse of company resources. When downloading software, videos, movies and applications a user can leave the door open for botnets and malware to invade their environments, even more, if the downloads are from websites known to be dangerous.

5. Number of users with "super user" access level.

Best practices in information security management include full control of users' level of access to company resources, it is necessary for an employee to only access data, systems, and assets that are necessary to their work. Identifying the access levels of all network users allows you to adjust them as needed by blocking any super user or administrator that does not make sense.

6. Number of days to deactivate former employee credentials

By monitoring these cybersecurity metrics, you can define whether the Human Resources and IT teams are working in tune. In an ideal scenario, the access of users terminated from the company should be cancelled immediately. Keeping them active is a tremendous risk, as it leaks sensitive information and can lead to compromised devices.

7. Number of communication ports open during a period of time

As a general rule, avoid allowing inbound traffic for NetBIOS (UDP 137 and 138, TCP 135-139 and 445). Be observant of outbound SSL (TCP 443): a session that stays active for a long time could be an SSL VPN tunnel that allows bi-directional traffic. Any common ports for protocols that allow remote sessions, like TCP 22 (SSH), TCP 23 (telnet), TCP 3389 (RDP), and TCP 20 and 21 (FTP) should be monitored for a length of time.

8. Frequency of review of third party accesses

Often, IT managers grant access to third parties in their networks to complete a project or activity. It is important to monitor whether the access is cancelled at the end of service provisioning. Failure to do so endangers your environment if the third party decides to come back and extract data or carry out other malicious activity – for instance, they may come under the employ of a competitor. Possibly worse, if the 3rd party's network is breached, you could expose your network to the same threat.

9. Frequency of access to critical enterprise systems by third parties

Creating a mapping of critical systems for the company and knowing the users that access them are imperative in the security context. Monitoring attempts to access servers or applications that should not be targeted by unauthorized users may indicate misconduct and intentions to compromise your environment.

10. Percentage of business partners with effective cybersecurity policies

You must maintain strict control and monitor the cybersecurity metrics of the companies that provide services for your business. Giving access to your environments to this outsourced company can be a huge risk if it does not have effective policies for its safety in the first place. It is not too much to say that if your company invests in security but has third parties connected to your systems that do not, you have no security at all.

## Security Vs Privacy

Privacy is not security and security is not privacy, even if these words are erroneously interchanged all the time. Let me try to lay out the differences between the two.
Privacy is concerned with the collection and use of personal data. Security is concerned with protection of that personal data from unwanted intruders.

There are numerous privacy laws and well-established principles that dictate when a company can collect someone's personal data and how it can use that data. Whether you live in the EU, the US, or anywhere else, there's probably a privacy law or two that dictates when and how a company can collect your personal data.

Privacy is personal. It is the understanding between a customer and a company about what information will be collected and how it will be used. We give up personal data in exchange for services we want. For example, if I want to buy a book online, I understand that I have to provide the vendor my name, address, and credit card information so I can receive that book. I entrust my personal information with the understanding that the bookseller will not use my information for any other reason. It will maintain the privacy of my personal data.

Security is impersonal. Security is not concerned with what is collected or how it is used. Rather, security guards the personal data I provide to a vendor from those who shouldn't see it and ensures that when that data needs to be seen, it's in the right format and is accessible. More simply, security is a wall around the castle, and just as there can be many different walls around a castle, there can also be many different walls of security around my personal data. Security walls can include network protection, encryption, and authentication, to name just a few, and companies spend a lot of money on these walls.

Even though security and privacy are not the same, they *are* interdependent on one another. You can't have one without the other. It just doesn't make sense. If a company doesn't have security in place to protect my data, then its privacy policies will be meaningless because it won't be able to prevent the unauthorized access to my data. Conversely, if a company doesn't have a clear understanding of what data it collects and how it will use it, then it will be impossible to provide true security.

# UNIT-IV
# Network Cryptography

## Cryptography

Cryptography, which comes from the Greek work kryptos meaning ―hidden, is a process of making and using codes to secure the transmission of information.

Crypto analysis is the process of obtaining the original message (called plaintext) from an encrypted message (called the cipher ext) without knowing the algorithms and keys used to perform the encryption.

Encryption is the process of converting an original message into a form that is unreadable to unauthorized individuals-that is; to anyone without the tools to convert the encrypted message back to its original format.

Decryption is the process of converting the cipher text into a message that conveys readily understood meaning.

### Basic Encryption Definitions.

Encryption Definitions

**Algorithm**: An algorithm is the mathematical formula used to convert an unencrypted message into an encrypted message.

**Cipher**: Cipher text is the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components

### Packet Sniffers

- A network tool that collects copies of packets from the network and analyzes them.
- Can be used to eavesdrop on the network traffic

To use a packet sniffer legally, you must be:

- on a network that the organization owns
- under direct authorization of the owners of the network
- have knowledge and consent of the content creators (users)

### Content Filters

- Although technically not a firewall, a content filter is a software filter that allows administrators to restrict accessible content from within a network.
- The content filtering restricts Web sites with inappropriate content

### Trap and Trace

- Trace: determine the identity of someone using unauthorized access
- Better known as honey pots, they distract the attacker while notifying the Administrator.

## Model of Cryptographic System:

Cryptography is a process of making and using codes to secure the transmission of information. Cryptoanalysis is the process of obtaining the original message (called plaintext) from an encrypted message (called the cipher ext) without knowing the algorithms and keys used to perform the encryption.

Encryption is the process of converting an original message into a form that is unreadable to unauthorized individuals-that is to anyone without the tools to convert the encrypted message back to its original format.

Decryption is the process of converting the cipher text into a message that conveys readily understood meaning.

**Basic Encryption Definitions.**

Encryption Definitions

**Algorithm**: the mathematical formula used to convert an unencrypted message into an encrypted message.

**Cipher**: the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components

**Ciphertext or cryptogram**: the unintelligible encrypted or encoded message resulting from an encryption.

**Code**: the transformation of the larger components (words or phrases) of an unencrypted message into encrypted components.

**Cryptosystem:** the set of transformations necessary to convert an unencrypted message into an encrypted message.

**Decipher :** to decrypt or convert cipher text to plaintext.

**Encipher**: to encrypt or convert plaintext to cipher text.

**Key or cryptovariable**: the information used in conjunction with the algorithm to create cipher text from plaintext.

**Keyspace**: the entire range of values that can possibly be used to construct an individual key.

**Link encryption**: a series of encryptions and decryptions between a numbers of systems, whereby each node decrypts the message sent to it and then re-encrypts it using different keys and sends it to the next neighbor, until it reaches the final destination.

**Plaintext**: the original unencrypted message that is encrypted and results from successful decryption.

**Steganography**: the process of hiding messages in a picture or graphic. **Work factor**: the amount of effort (usually in hours) required to perform cryptanalysis on an encoded message.

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred as a **cipher system**.

Let us discuss a simple model of a cryptosystem that provides confidentiality to the information being transmitted. This basic model is depicted in the illustration below −

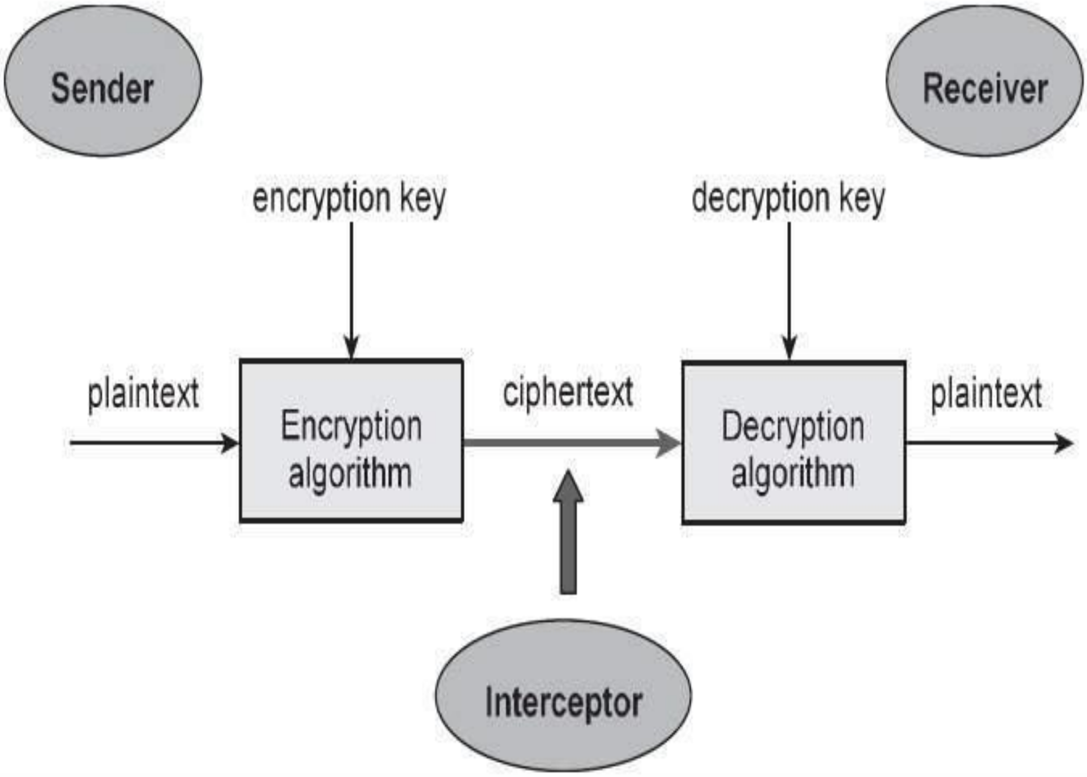


Figure 4.1 A typical Cryptographic System

The illustration in figure 4.1 shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data.

The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

## Components of a Cryptosystem

The various components of a basic cryptosystem are as follows −

- **Plaintext.** It is the data to be protected during transmission.

- **Encryption Algorithm.** It is a mathematical process that produces a cipher text for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a cipher text.

- **Cipher text.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The cipher text is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.

- **Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given cipher text and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.

- **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the cipher text.

- **Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the cipher text in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a **key space**.

An **interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the cipher text and may know the decryption algorithm. He, however, must never know the decryption key.

## Types of Cryptosystems

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system −

- Symmetric Key Encryption
- Asymmetric Key Encryption

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key.

1. **Symmetric Key Encryption**

The encryption process where **same keys are used for encrypting and decrypting** the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as **symmetric cryptography**. Symmetric cryptosystems are also sometimes referred to as **secret key cryptosystems**.

A few well-known examples of symmetric key encryption methods are − Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

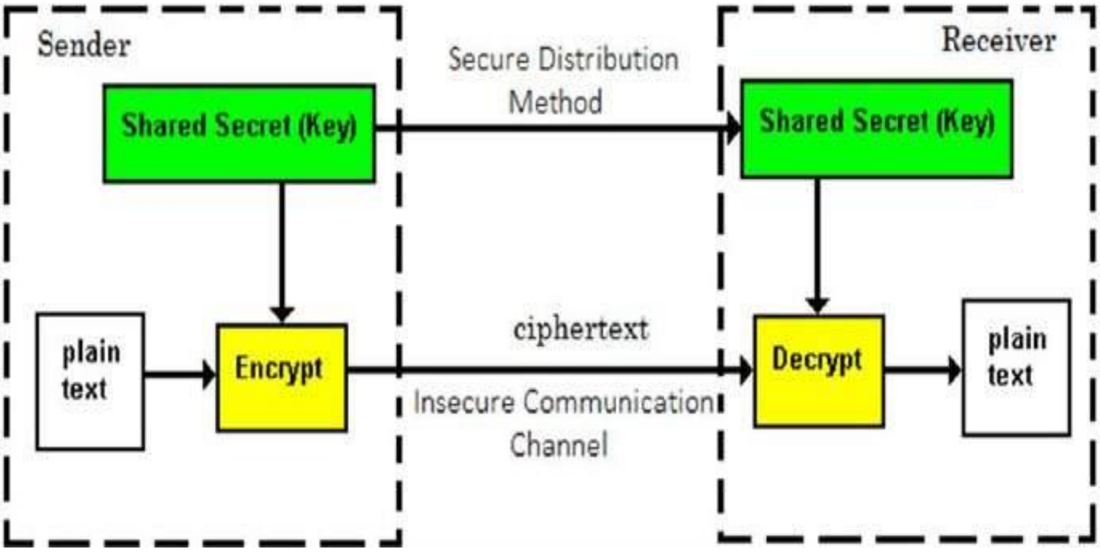


Figure 4.2 Symmetric Key Cyprography

Prior to 1970, all cryptosystems employed symmetric key encryption. Even today, its relevance is very high and it is being used extensively in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain advantages over asymmetric key encryption.

The salient features of cryptosystem based on symmetric key encryption are −

- Persons using symmetric key encryption must share a common key prior to exchange of information.
- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of **n** people, to enable two-party communication between any two persons, the number of keys required for group is **n × (n – 1)/2**.
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

## Challenge of Symmetric Key Cryptosystem

There are two restrictive challenges of employing symmetric key cryptography.

- **Key establishment** − Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.

- **Trust Issue** − Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver 'trust' each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

## Asymmetric Key Encryption

The encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible. The process is depicted in the following illustration −

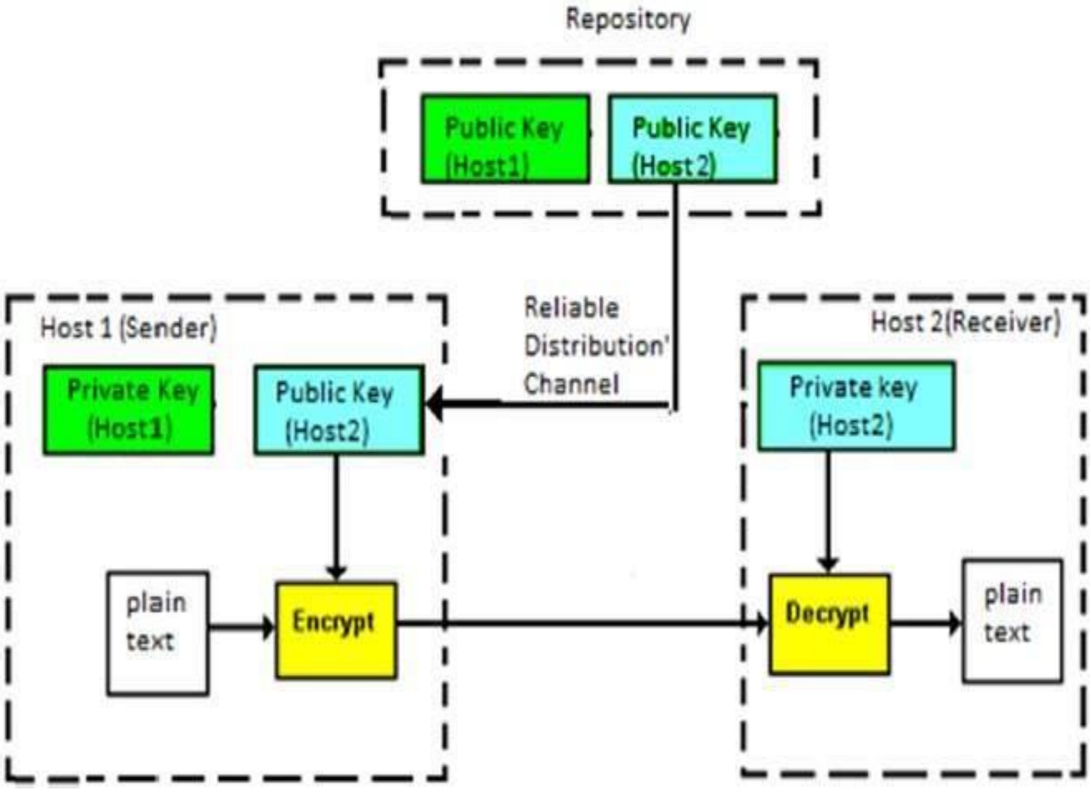


Figure 4.3 Asymmetric key cryptography

Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons. The salient features of this encryption scheme are as follows −

- Every user in this system needs to have a pair of dissimilar keys, **private key** and **public key**. These keys are mathematically related − when one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.

- It requires putting the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called **Public Key Encryption**.

- Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is strength of this scheme.

- When *Host1* needs to send data to *Host2*, he obtains the public key of*Host2* from repository, encrypts the data, and transmits.

- *Host2* uses his private key to extract the plaintext.

- Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.

- Processing power of computer system required to run asymmetric algorithm is higher.

Symmetric cryptosystems are a natural concept. In contrast, public-key cryptosystems are quite difficult to comprehend.

You may think, how can the encryption key and the decryption key are 'related', and yet it is impossible to determine the decryption key from the encryption key? The answer lies in the mathematical concepts. It is possible to design a cryptosystem whose keys have this property. The concept of public-key cryptography is relatively new. There are fewer public-key algorithms known than symmetric algorithms.

## Challenge of Public Key Cryptosystem

Public-key cryptosystems have one significant challenge − the user needs to trust that the public key that he is using in communications with a person really is the public key of that person and has not been spoofed by a malicious third party.

This is usually accomplished through a Public Key Infrastructure (PKI) consisting a trusted third party. The third party securely manages and attests to the authenticity of public keys. When the third party is requested to provide the public key for any communicating person X, they are trusted to provide the correct public key.

The third party satisfies itself about user identity by the process of attestation, notarization, or some other process − that X is the one and only, or globally unique, X. The most common method of making the verified public keys available is to embed them in a certificate which is digitally signed by the trusted third party.

### Relation between Encryption Schemes

A summary of basic key properties of two types of cryptosystems is given below –

| | **Symmetric Cryptosystems** | **Public Key Cryptosystems** |
|---|---|---|
| **Relation between Keys** | Same | Different, but mathematically related |
| Encryption Key | Symmetric | Public |

| | | |
|---|---|---|
| Decryption Key | Symmetric | Private |

Due to the advantages and disadvantage of both the systems, symmetric key and public-key cryptosystems are often used together in the practical information security systems.

## Issues in Document Security

Documents face threats of many kinds. Customer lists, sales-strategy reports, and detailed revenue statistics might fall into the hands of competitors. Confidential personal data given by customers and employees could be compromised leading to lawsuits. Identification details like bank-account login information or credit-card details might be stolen by thieves. Because of these possibilities in today's world, the issue of document security should be a top concern.

1. Security measures under a document management system seek to protect business data and business interests comply with legal requirements, such as protection of privacy, and prevent financial losses through ID theft and fraud.
2. Document security is generally ensured by restricting access to the documents. In a paper-based system, highly sensitive documents can be kept under lock and key for viewing by only top managers, for example.
3. It's practically impossible to ensure adequate security for documents under a paper-based system because keeping all documents under lock and key can affect business results. For example, decision makers might find that documents that provide decision-support information cannot be assembled quickly enough.
4. Electronic document management systems can improve things in a major way because access to particular folders and documents can be selectively restricted using electronic means. For example, employees can be categorized into different levels, and each level can have different access rights and permissions.
5. Access rights typically include viewing and editing privileges, i.e. some might be allowed to view a particular document but not modify it. Others might have full rights, including editing privileges. Users might also have to provide passwords to access the documents. This can theoretically prevent unauthorized persons from accessing documents at an employee's workstation.
6. As will be evident, permissions alone cannot provide full safeguards. An employee might not log out after accessing a document, and if that person leaves the workstation, someone else might then be able to view it. Training employees to follow best practices for security is a key element of overall document security.
7. It has been reported that most security lapses are due to employees, either through carelessness or dishonesty. It's very important to provide access rights strictly on a need-to-have basis, with each employee (including senior employees) being able to access only those documents that they require to complete their specific tasks.
8. Any document management system must maintain audit trails that keep track of who accessed which document and when, and what changes were made during each access. The trail must then be monitored by a responsible person for any unusual activities.
9. The existence of the Internet allows threats to come from external sources. Specific dangers from viruses and other malicious software, from hackers who can wipe out valuable business data, and from identity thieves have become far more serious today.
10. These external threats are guarded against through the installation of security software such as anti-virus and anti-spyware programs, implementation of firewalls and secure-access

mechanisms, such as SSL, and regular updates to operating systems and applications. Software developers typically issue patches to plug any possible security loopholes.

11. Authentication of documents is another key security precaution. Developments like electronic signatures can not only help senders sign outgoing documents, but also enable recipients to ensure that the documents they receive are indeed from who they claim to be, and that no alterations have occurred since it was authenticated.
12. Above all, regular reviews must be carried out to identify any security vulnerabilities, including practices like creating backups and implementing document retention and destruction policies. Documents that have exceeded their lifetimes must be shredded rather than left around.

As document security has become a vital concern, several helpful organizations have issued guidelines to help companies deal with these security issues. One such example is ISO 27002, a standard implemented by the International Standards Organization dealing specifically with information security. Implementing these policies and practices can help your organization improve the security of your documents and information.

## System of Keys

One of the most important aspects of any cryptographic system is key management; which is very difficult and, therefore, sometimes neglected.[1] A very common mistake is mixing different key types and reusing the same key for different purposes. An example with devastating consequences is the reuse of the same symmetric key for both symmetric authentication in CBC-MAC and symmetric data encryption in CBC encryption.

In a key management system each key should be labeled with one such type and that key should never be used for a different purpose. According to NIST SP 800-57 the following types of keys exist:

- **Private signature key**
  Private signature keys are the private keys of asymmetric (public) key pairs that are used by public key algorithms to generate digital signatures with possible long-term implications. When properly handled, private signature keys can be used to provide authentication, integrity and non-repudiation.
- **Public signature verification key**
  A public signature verification key is the public key of an asymmetric key pair that is used by a public key algorithm to verify digital signatures, either to authenticate a user's identity, to determine the integrity of the data, for non-repudiation, or a combination thereof.
- **Symmetric authentication key**
  Symmetric authentication keys are used with symmetric key algorithms to provide assurance of the integrity and source of messages, communication sessions, or stored data.
- **Private authentication key**
  A private authentication key is the private key of an asymmetric key pair that is used with a public key algorithm to provide assurance as to the integrity of information, and the identity of the originating entity or the source of messages, communication sessions, or stored data.
- **Public authentication key**
  A public authentication key is the public key of an asymmetric key pair that is used with a public key algorithm to determine the integrity of information and to authenticate the identity of entities, or the source of messages, communication sessions, or stored data.
- **Symmetric data encryption key**
  These keys are used with symmetric key algorithms to apply confidentiality protection to information.
- **Symmetric key wrapping key**
  Symmetric key wrapping keys are used to encrypt other keys using symmetric key algorithms. Key wrapping keys are also known as key encrypting keys.

- **Symmetric and asymmetric random number generation keys**
  These are keys used to generate random numbers.
- **Symmetric master key**
  A symmetric master key is used to derive other symmetric keys (e.g., data encryption keys, key wrapping keys, or authentication keys) using symmetric cryptographic methods.
- **Private key transport key**
  Private key transport keys are the private keys of asymmetric key pairs that are used to decrypt keys that have been encrypted with the associated public key using a public key algorithm. Key transport keys are usually used to establish keys (e.g., key wrapping keys, data encryption keys or MAC keys) and, optionally, other keying material (e.g. initialization vectors).
- **Public key transport key**
  Public key transport keys are the public keys of asymmetric key pairs that are used to encrypt keys using a public key algorithm. These keys are used to establish keys (e.g., key wrapping keys, data encryption keys or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors).
- **Symmetric key agreement key**
  These symmetric keys are used to establish keys (e.g., key wrapping keys, data encryption keys, or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors) using a symmetric key agreement algorithm.
- **Private static key agreement key**
  Private static key agreement keys are the private keys of asymmetric key pairs that are used to establish keys (e.g., key wrapping keys, data encryption keys, or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors).
- **Public static key agreement key**
  Public static key agreement keys are the public keys of asymmetric key pairs that are used to establish keys (e.g., key wrapping keys, data encryption keys, or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors).
- **Private ephemeral key agreement key**
  Private ephemeral key agreement keys are the private keys of asymmetric key pairs that are used only once to establish one or more keys (e.g., key wrapping keys, data encryption keys, or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors).
- **Public ephemeral key agreement key**
  Public ephemeral key agreement keys are the public keys of asymmetric key pairs that are used in a single key establishment transaction to establish one or more keys (e.g., key wrapping keys, data encryption keys, or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors).
- **Symmetric authorization key**
  Symmetric authorization keys are used to provide privileges to an entity using a symmetric cryptographic method. The authorization key is known by the entity responsible for monitoring and granting access privileges for authorized entities and by the entity seeking access to resources.
- **Private authorization key**
  A private authorization key is the private key of an asymmetric key pair that is used to provide privileges to an entity.
- **Public authorization key**
  A public authorization key is the public key of an asymmetric key pair that is used to verify privileges for an entity that knows the associated private authorization key.

# Public Key Cryptography

Public-key cryptography and related standards underlie the security features of many products such as signed and encrypted email, single sign-on, and Secure Sockets Layer (SSL) communications. This chapter covers the basic concepts of public-key cryptography.

A third party can intercept internet traffic, which passes information through intermediate computers:

- *Eavesdropping.* Information remains intact, but its privacy is compromised. For example, someone could gather credit card numbers, record a sensitive conversation, or intercept classified information.
- *Tampering.* Information in transit is changed or replaced and then sent to the recipient. For example, someone could alter an order for goods or change a person's resume.
- *Impersonation.* Information passes to a person who poses as the intended recipient. Impersonation can take two forms:
    1) *Spoofing.* A person can pretend to be someone else. For example, a person can pretend to have the email address **jdoe@example.net** or a computer can falsely identify itself as a site called **www.example.net**.
    2) *Misrepresentation.* A person or organization can misrepresent itself. For example, a site called **www.example.net** can purport to be an on-line furniture store when it really receives credit-card payments but never sends any goods.

*Public-key cryptography* provides protection against Internet-based attacks through:

- *Encryption and decryption* allow two communicating parties to disguise information they send to each other. The sender encrypts, or scrambles, information before sending it. The receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder.
- *Tamper detection* allows the recipient of information to verify that it has not been modified in transit. Any attempts to modify or substitute data are detected.
- *Authentication* allows the recipient of information to determine its origin by confirming the sender's identity.
- *Nonrepudiation* prevents the sender of information from claiming at a later date that the information was never sent.

## Encryption and Decryption

*Encryption* is the process of transforming information so it is unintelligible to anyone but the intended recipient.*Decryption* is the process of decoding encrypted information. A cryptographic algorithm, also called a *cipher*, is a mathematical function used for encryption or decryption. Usually, two related functions are used, one for encryption and the other for decryption.

With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, which is widely known, but on a number called a *key* that must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple. Decryption without the correct key is very difficult, if not impossible.

## Symmetric-Key Encryption

With symmetric-key encryption, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption, as shown in Figure 4.4, “Symmetric-Key Encryption”.

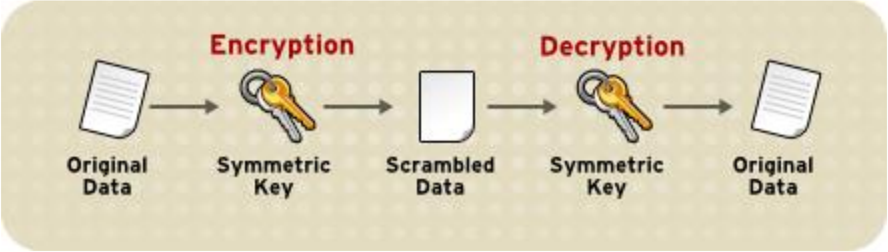


**Figure 4.4 Symmetric-Key Encryption**

Implementations of symmetric-key encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

Symmetric-key encryption is effective only if the symmetric key is kept secret by the two parties involved. If anyone else discovers the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key not only can decrypt messages sent with that key, but can encrypt new messages and send them as if they came from one of the legitimate parties using the key.

Symmetric-key encryption plays an important role in SSL communication, which is widely used for authentication, tamper detection, and encryption over TCP/IP networks. SSL also uses techniques of public-key encryption, which is described in the next section.

## Public-Key Encryption

Public-key encryption (also called asymmetric encryption) involves a pair of keys, a public key and a private key, associated with an entity. Each public key is published, and the corresponding private key is kept secret. (For more information about the way public keys are published, see Section 1.3, “Certificates and Authentication”.) Data encrypted with a public key can be decrypted only with the corresponding private key. Figure 4.5, “Public-Key Encryption” shows a simplified view of the way public-key encryption works.

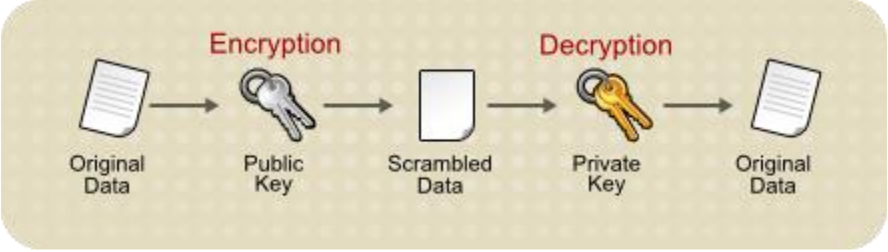


**Figure 4.5 Public-Key Encryption**

The scheme shown in Figure 4.5, “Public-Key Encryption” allows public keys to be freely distributed, while only authorized people are able to read data encrypted using this key. In general, to send encrypted data, the data is encrypted with that person's public key, and the person receiving the encrypted data decrypts it with the corresponding private key.

Compared with symmetric-key encryption, public-key encryption requires more processing and may not be feasible for encrypting and decrypting large amounts of data. However, it is possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL/TLS protocols.

The reverse of the scheme shown in Figure 4.5, “Public-Key Encryption” also works: data encrypted with a private key can be decrypted only with the corresponding public key. This is not a recommended practice to encrypt sensitive data, however, because it means that anyone with the public key, which is by definition published, could decrypt the data. Nevertheless, private-key encryption is useful because it means the private key can be used to sign data with a digital signature, an important requirement for electronic commerce and other commercial applications of cryptography. Client software such as Mozilla Firefox can then use the public key to confirm that the message was signed with the appropriate private key and that it has not been tampered with since being signed. “Digital Signatures” illustrates how this confirmation process works.

### Key Length and Encryption Strength

*Breaking* an encryption algorithm is basically finding the key to the access the encrypted data in plain text. For symmetric algorithms, breaking the algorithm usually means trying to determine the key used to encrypt the text. For a public key algorithm, breaking the algorithm usually means acquiring the shared secret information between two recipients.

One method of breaking a symmetric algorithm is to simply try every key within the full algorithm until the right key is found. For public key algorithms, since half of the key pair is publicly known, the other half (private key) can be derived using published, though complex, mathematical calculations. Manually finding the key to break an algorithm is called a brute force attack.

Breaking an algorithm introduces the risk of intercepting, or even impersonating and fraudulently verifying, private information.

The *key strength* of an algorithm is determined by finding the fastest method to break the algorithm and comparing it to a brute force attack.

For symmetric keys, encryption strength is often described in terms of the size or *length* of the keys used to perform the encryption: longer keys generally provide stronger encryption. Key length is measured in bits. For example, 128-bit keys with the RC4 symmetric-key cipher supported by SSL provide significantly better cryptographic protection than 40-bit keys used with the same cipher. The 128-bit RC4 encryption is 3 x $10^{26}$times stronger than 40-bit RC4 encryption.

An encryption key is considered full strength if the best known attack to break the key is no faster than a brute force attempt to test every key possibility.

Different types of algorithms — particularly public key algorithms — may require different key lengths to achieve the same level of encryption strength as a symmetric-key cipher. The RSA cipher can use only a subset of all possible values for a key of a given length, due to the nature of the mathematical problem on which it is based. Other ciphers, such as those used for symmetric-key encryption, can use all possible values for a key of a given length. More possible matching options mean more security.

Because it is relatively trivial to break an RSA key, an RSA public-key encryption cipher must have a very long key at least 1024 bits to be considered cryptographically strong. On the other hand, symmetric-key ciphers are reckoned to be equivalently strong using a much shorter key length, as little as 80 bits for most algorithms.

## Digital Signature

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

## Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration −

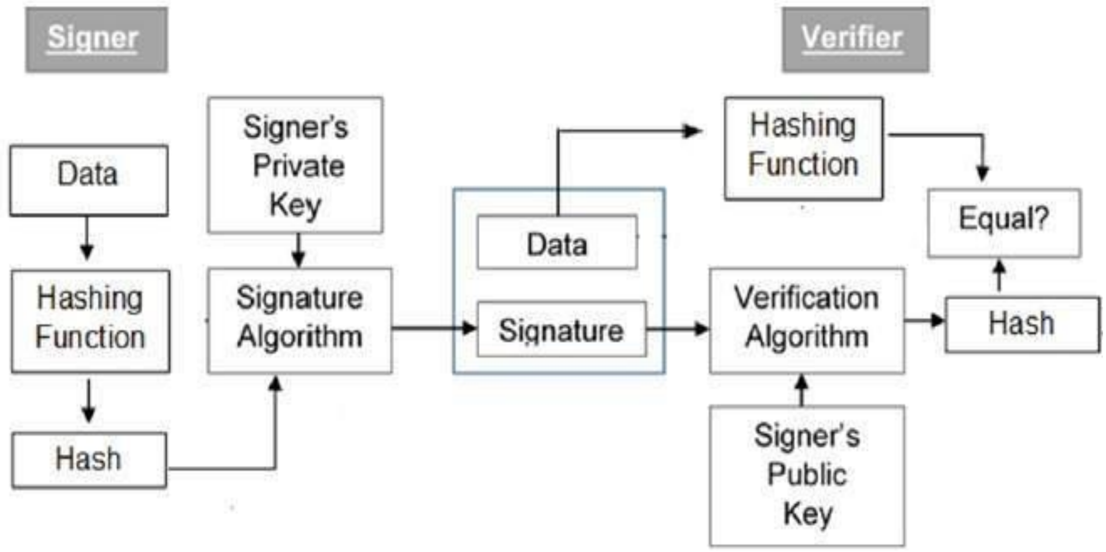


Figure 4.6 Digital Signature scheme

The following points explain the entire process in detail −

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence signing a hash is more efficient than signing the entire data.

## Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.

- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.

- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

## Encryption with Digital Signature

In many digital communications, it is desirable to exchange an encrypted message than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing PKC for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

This can archive by combining digital signatures with encryption scheme. Let us briefly discuss how to achieve this requirement. There are two possibilities, sign-then-encrypt and encrypt-then-sign.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration −

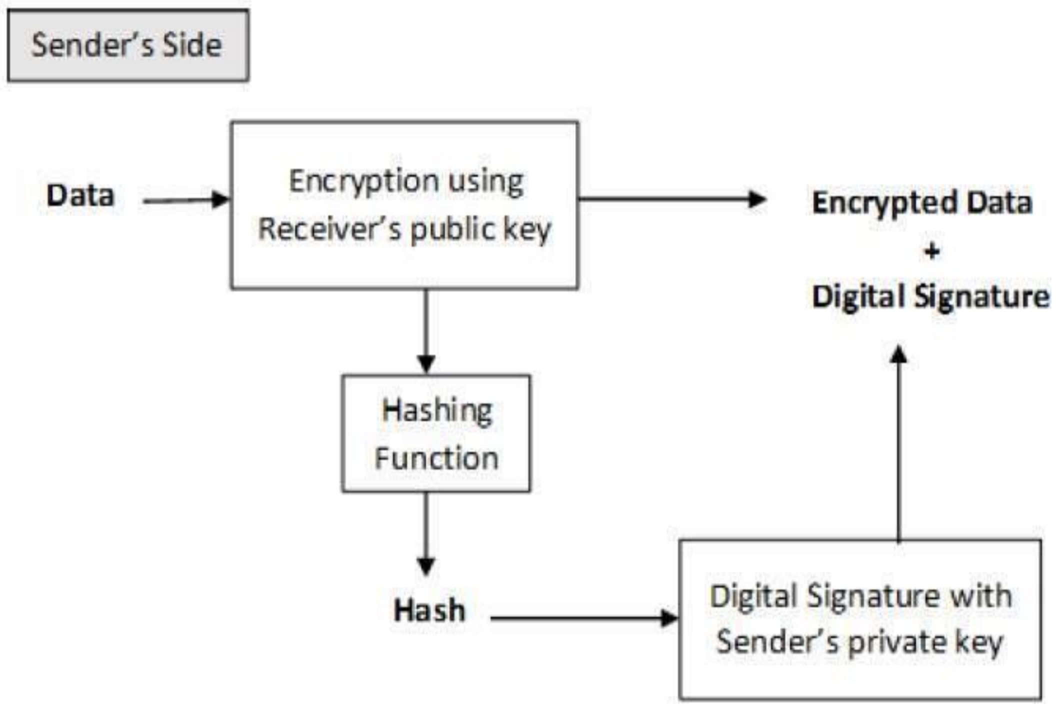

Sender's Side
Data
Encryption using Receiver's public key
Encrypted Data + Digital Signature
Hashing Function
Hash
Digital Signature with Sender's private key

Figure 4.7 Encryption with digital signature

The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.

## Finger Prints

### The History of Fingerprinting

Francis Galton published his book "Finger Prints" (1892) which stated:
· there are three types of fingerprint patterns
· prints are unique to each individual
· prints do not change over time
· A classification system that allowed the filing of many thousands of fingerprints was developed in 1891
· The first systematic and official use of fingerprints in the United States was in New York City for the Civil Service Commission in 1891.
· In 1924, the fingerprint records of the Bureau of Investigation and Leavenworth Prison merged to form identification records at the FBI. This is the largest collection of fingerprints in the world.

Fingerprints are made when oil from the body is mixed with other body sweat and dirt. When you then touch something, these adhere or stick to the surface of the object.

### Fingerprint Patterns

- Arch patterns have lines that start at one side of the print and then move toward the center of the print and leave on the other side of the print.
- Whorl patterns have a lot of circles that do not exit on either side of the print.
- Loop patterns have lines that start at one side of the print and then move toward the center of the print and leave on the same side of the print they started on.

### Types of fingerprints left at crime scenes

- visible prints are fingerprints that one can see with the naked eye

- latent prints are fingerprints that are invisible
- plastic prints are fingerprints that leave an impression on objects such as soap or wax.

**Methods used to obtain fingerprints**

- Ink pad or pencil smudge
- Dusting
- Impression
- fuming with super glue

## Fingerprint Principles

According to criminal investigators, fingerprints follow three fundamental principles:

1. A fingerprint is an **individual** characteristic; no two people have been found with the **exact** same fingerprint pattern.
2. A fingerprint **pattern** will remain **unchanged** for the **life** of an individual; however, the print itself may change due to permanent scars and skin diseases.
3. Fingerprints have general characteristic **ridge** patterns that allow them to be systematically identified.

## Fingerprint Classes

There are 3 specific classes for all fingerprints based upon their visual pattern: arches, loops, and whorls. Each group is divided into smaller groups as seen in the lists below.

1. **Arch:-** Plain arch and Tented arch
2. **Loop**:- Radial Loop and Ulnar loop
3. **Whorl:-** Plain whorl, Central pocket whorl, Double loop whorl and Accidental

# Firewalls

A firewall is any device that prevents a specific type of information from moving between the untrusted network outside and the trusted network inside There are five recognized generations of firewalls
The firewall may be:
1. a separate computer system
2. a service running on an existing router or server
3. a separate network containing a number of supporting devices

## Different generations of firewalls:

**First Generation**
Called packet filtering firewalls Examines every incoming packet header and selectively filters packets based on address, packet type, port request, and others factors The restrictions most commonly implemented are based on: IP source and destination address Direction (inbound or outbound)
**Second Generation**
TCP or UDP source and destination port-requests **Second Generation** Called application-level firewall or proxy server

- often a dedicated computer separate from the filtering router
- with this configuration the proxy server, rather than the Web server, is exposed to the outside world in the DMZ

- Additional filtering routers can be implemented behind the proxy server
- The primary disadvantage of application-level firewalls is that they are designed for a specific protocol and cannot easily be reconfigured to protect against attacks on protocols for which they are not designed

**Third Generation**

- Called stateful inspection firewalls
- Keeps track of each network connection established between internal and external systems using a state table which tracks the state and context of each packet in the conversation by recording which station sent what packet.
- These firewalls can track connectionless packet traffic such as UDP and remote procedure calls (RPC) traffic

**Fourth Generation**

While static filtering firewalls, such as first and third generation, allow entire sets of one type of packet to enter in response to authorized requests, a dynamic packet filtering firewall allows only a particular packet with a particular source, destination,and port address to enter through the firewall

□ It does this by understanding how the protocol functions, and opening and closing
―doors‖ in the firewall, based on the information contained in the packet header. In this manner, dynamic packet filters are an intermediate form, between traditional static packet filters and application proxies

**Fifth Generation**

- The final form of firewall is the kernel proxy, a specialized form that works under the Windows NT Executive, which is the kernel ofWindows NT
- It evaluates packets at multiple layers of the protocol stack, by checking security in the kernel as data is passed up and down the stack

**Firewalls are categorized by processing modes:-**

The five processing modes are

1) Packet filtering
2) Application gateways
3) Circuit gateways
4) MAC layer firewalls
5) Hybrids

**Packet-filtering Routers**

- Most organizations with an Internet connection have some form of a router as the interface at the perimeter between the organization‘s internal networks and the external service provider
- Many of these routers can be configured to filter packets that the organization does not allow into the network
- This is a simple but effective means to lower the organization‘s risk to external attack
- The drawback to this type of system includes a lack of auditing and strong authentication
- The complexity of the access control lists used to filter the packets can grow and degrade network performance
- Screened-Host Firewall Systems
    - Combine the packet-filtering router with a separate, dedicated firewall such as an application proxy server

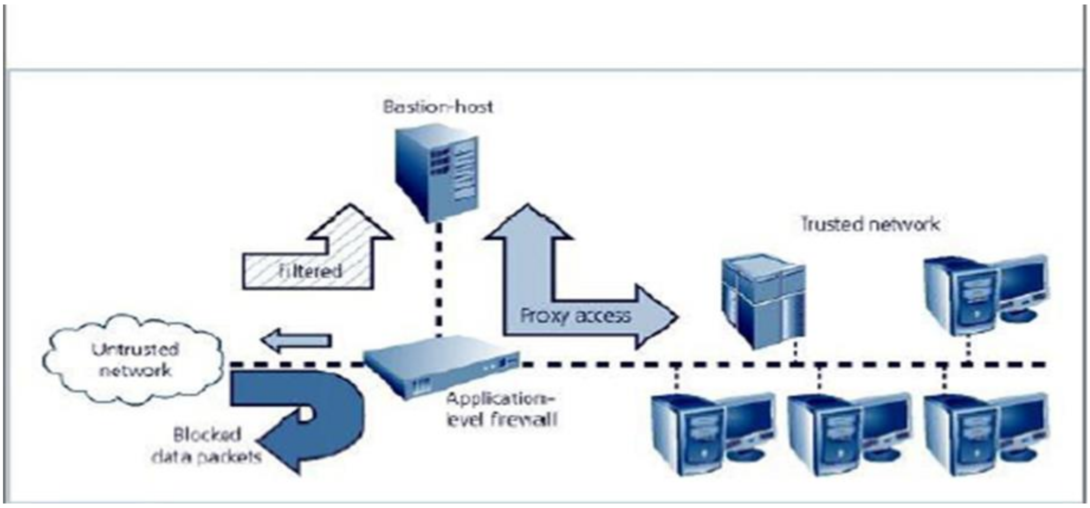


Figure 4.8 Screened Host Firewall

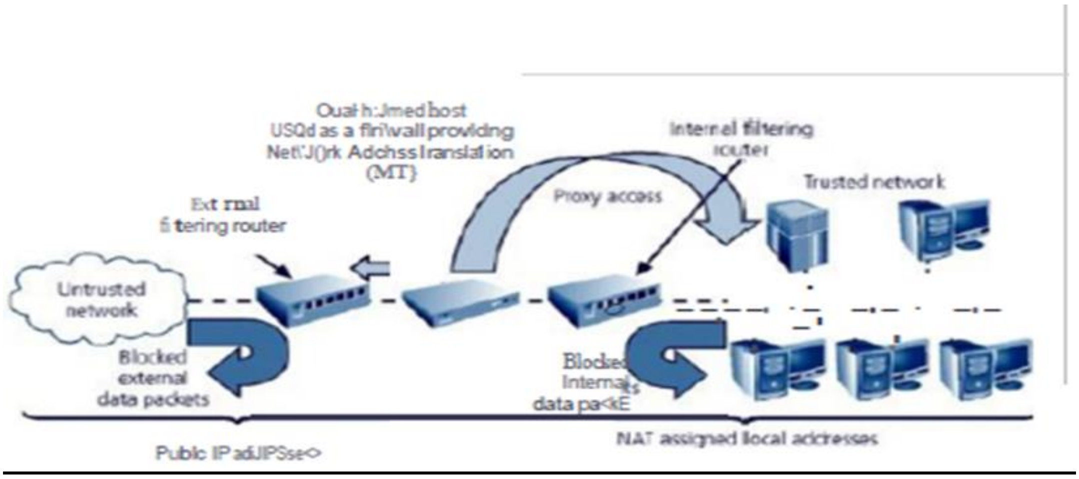

Ouai h:Jmed host USQd as a firi\wall providing Net\'J()rk Adchss lransla1 ion (MT}
Internal filtering router
Trusted network
Proxy access
Ext rnal fi tering router
Untrusted network
Blocked external data packets
Blocked Internal data pa<kEts
Public IP adJIPSse<>
NAT assigned llocal adclresses

Figure 4.9 Screened-Subnet Firewalls (with DMZ)

## Screened-Subnet Firewalls (with DMZ)

- Consists of two or more internal bastion-hosts, behind a packet-filtering router, with each host protecting the trusted network
- The first general model consists of two filtering routers, with one or more dual- homed bastion-host between them
- The second general model involves the connection from the outside or untrusted network going through this path:
- Through an external filtering router
- Into and then out of a routing firewall to the separate network segment known as the DMZ.

**The factors to be considered while selecting a right firewall**

Selecting the Right Firewall

- What type of firewall technology offers the right balance of protection features and cost for the needs of the organization?
- What features are included in the base price? What features are available at extra cost? Are all cost factors known?

- How easy is it to set up and configure the firewall? How accessible are staff technicians with the mastery to do it well?
- Can the candidate firewall adapt to the growing network in the target organization?

### What are Sock Servers?

- The SOCKS system is a proprietary circuit-level proxy server that places special .SOCKS client-side agents on each workstation
- Places the filtering requirements on the individual workstation, rather than on a single point of defense (and thus point of failure)
- This frees the entry router of filtering responsibilities, but then requires each
- A SOCKS system can require additional support and management resources to configure and manage possibly hundreds of individual clients, versus a single device or set of devices

## Design and Implementation Issues of Firewall

Firewall Recommended Practices:-

- All traffic from the trusted network is allowed out .The firewall device is always inaccessible directly from the public network. Allow Simple Mail Transport Protocol (SMTP) data to pass through your firewall, but insure it is all routed to a well-configured SMTP gateway to filter and route messaging traffic securely
- All Internet Control Message Protocol (ICMP) data should be denied
- Block telnet (terminal emulation) access to all internal servers from the public networks
- When Web services are offered outside the firewall, deny HTTP traffic from reaching your internal networks by using some form of proxy access or DMZ architecture

## Policies Network Security:

### Basic Concepts

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Types of Network Security Devices

- Active Devices

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

- Passive Devices

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

- Preventative Devices

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

- Unified Threat Management (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

## Dimensions

**Firewalls**

A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.

Firewalls are commonly used in private networks or intranets to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

**Hardware and Software Firewalls**

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available.

Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

**Antivirus**

An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, key loggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

**Content Filtering**

Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.

Content filtering can be divided into the following categories −

- Web filtering
- Screening of Web sites or pages
- E-mail filtering
- Screening of e-mail for spam
- Other objectionable content

**Intrusion Detection Systems**

Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.

Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. Intrusion detection systems can also perform the following actions −

- Correct Cyclic Redundancy Check (CRC) errors
- Prevent TCP sequencing issues
- Clean up unwanted transport and network layer options

## Perimeter for Network Protection

A network perimeter is the boundary between the private and locally managed-and-owned side of a network and the public and usually provider-managed side of a network. A perimeter is the fortified boundary of the network that might include the following aspects:

- Border routers
- Firewalls
- IDSs
- IPSs
- VPN devices
- Software architecture
- DMZs and screened subnets

Let's take a look at these perimeter components in closer detail.

**Border Routers**

Routers are the traffic cops of networks. They direct traffic into, out of, and within our networks. The border router is the last router you control before an untrusted network such as the Internet. Because all of an organization's Internet traffic goes through this router, it often functions as a network's first and last line of defense through initial and final filtering.

**Firewalls**

A firewall is a chokepoint device that has a set of rules specifying what traffic it will allow or deny to pass through it. A firewall typically picks up where the border router leaves off and makes a much more thorough pass at filtering traffic. Firewalls come in several different types, including static packet filters, stateful firewalls, and proxies. You might use a static packet filter such as a Cisco router to block easily identifiable "noise" on the Internet, a stateful firewall such as a Check Point FireWall-1 to control allowed services, or a proxy firewall such as Secure Computing's Sidewinder to control content. Although firewalls aren't perfect, they do block what we tell them to block and allow what we tell them to allow.

**Intrusion Detection Systems**

An IDS is like a burglar alarm system for your network that is used to detect and alert on malicious events. The system might comprise many different IDS sensors placed at strategic points in your network. Two basic types of IDS exist: network-based (NIDS), such as Snort or Cisco Secure IDS, and host-based (HIDS), such as Tripwire or ISS BlackICE. NIDS sensors monitor network traffic for suspicious activity. NIDS sensors often reside on subnets that are directly connected to the firewall, as well as at critical points on the internal network. HIDS sensors reside on and monitor individual hosts.

In general, IDS sensors watch for predefined signatures of malicious events, and they might perform statistical and anomaly analysis. When IDS sensors detect suspicious events, they can alert in several different ways, including email, paging, or simply logging the occurrence. IDS sensors can usually report to a central database that correlates their information to view the network from multiple points.

**Intrusion Prevention Systems**

An IPS is a system that automatically detects and thwarts computer attacks against protected resources. In contrast to a traditional IDS, which focuses on notifying the administrator of anomalies, an IPS strives to automatically defend the target without the administrator's direct involvement. Such protection may involve using signature-based or behavioral techniques to identify an attack and then blocking the malicious traffic or system call before it causes harm. In this respect, an IPS combines the functionality of a firewall and IDS to offer a solution that automatically blocks offending actions as soon as it detects an attack.

Some IPS products exist as standalone systems, such as TippingPoint's UnityOne device. Additionally, leading firewall and IDS vendors are incorporating IPS functionality into their existing products.

**Virtual Private Networks**

A VPN is a protected network session formed across an unprotected channel such as the Internet. Frequently, we reference a VPN in terms of the device on the perimeter that enables the encrypted session, such as Cisco VPN Concentrator. The intended use might be for business partners, road warriors, or telecommuters. A VPN allows an outside user to participate on the internal network as if connected directly to it. Many organizations have a false sense of security regarding their remote access just because they have a VPN. However, if an attacker compromises the machine of a legitimate user, a VPN can give that attacker an encrypted channel into your network. You might trust the security of your perimeter, but you have little control over your telecommuters' systems connecting from home, a hotel room, or an Internet café. Similar issues of trust and control arise with the security of nodes connected over a VPN from your business partner's network.

**Software Architecture**

Software architecture refers to applications that are hosted on the organization's network, and it defines how they are structured. For example, we might structure an e-commerce application by splitting it into three distinct tiers:

- The web front end that is responsible for how the application is presented to the user
- The application code that implements the business logic of the application
- The back-end databases that store underlying data for the application

Software architecture plays a significant role in the discussion of a security infrastructure because the primary purpose of the network's perimeter is to protect the application's data and services. When securing the application, you should ensure that the architecture of the software and the network is harmonious.

**De-Militarized Zones and Screened Subnets**

We typically use the terms DMZ and screened subnet in reference to a small network containing public services connected directly to and offered protection by the firewall or other filtering device. A DMZ and a screened subnet are slightly different, even though many people use the terms interchangeably. The term DMZ originated during the Korean War when a strip of land at the 38th parallel was off-limits militarily. A DMZ is an insecure area between secure areas. Just as the DMZ in Korea was in front of any defenses, the DMZ, when applied to networks, is located outside the firewall. A firewall or a comparable traffic-screening device protects a screened subnet that is directly connected to it. Remember this: A DMZ is in front of a firewall, whereas a screened subnet is behind a firewall.

A screened subnet is an isolated network that is connected to a dedicated interface of a firewall or another filtering device. The screened subnet is frequently used to segregate servers that need to be accessible from the Internet from systems that are used solely by the organization's internal users. The screened subnet typically hosts "public" services, including DNS, mail, and web. We would like to think these servers are bastion hosts. A bastion is a well-fortified position. When applied to hosts on a network, fortifying involves hardening the operating system and applications according to best practices. As attacks over time have shown, these servers are not always well fortified; in fact, they are sometimes vulnerable despite being protected by a firewall. We must take extra care fortifying these hosts because they are the target of the majority of attacks and can bring the attacker closer to accessing even more critical internal resources.

## Network Attacks

Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.

Your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place.

**Eavesdropping**

In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

**Data Modification**

After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if you do not require confidentiality for all communications, you do not want any of your messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.

**Identity Spoofing (IP Address Spoofing)**

Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.

After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data. The attacker can also conduct other types of attacks, as described in the following sections.

**Password-Based Attacks**

A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.

Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user.

When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.

After gaining access to your network with a valid account, an attacker can do any of the following:

- Obtain lists of valid user and computer names and network information.
- Modify server and network configurations, including access controls and routing tables.
- Modify, reroute, or delete your data.

**Denial-of-Service Attack**

Unlike a password-based attack, the denial-of-service attack prevents normal use of your computer or network by valid users.

After gaining access to your network, the attacker can do any of the following:

- Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

**Man-in-the-Middle Attack**

As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying as you to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section.

Compromised-Key Attack

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key.

An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

**Sniffer Attack**

A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key.

Using a sniffer, an attacker can do any of the following:

- Analyze your network and gain information to eventually cause your network to crash or to become corrupted.
- Read your communications.

**Application-Layer Attack**

An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

- Read, add, delete, or modify your data or operating system.
- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
- Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.
- Abnormally terminate your data applications or operating systems.
- Disable other security controls to enable future attacks.

## Need of Intrusion Monitoring and Detection

An IDS operates as either network-based, when the technology is focused on protecting network information assets, or host-based, when the technology is focused on protecting server or host information assets

IDSs use one of two detection methods, signature-based or statistical anomaly-based. Different types of IDSs

**a) Network-based IDS**

A network-based IDS (NIDS) resides on a computer or an appliance connected to a segment of an organization‘s network and monitors traffic on that network segment, looking for indications of ongoing or successful attacks.

**b) Host-based IDS**

A Host-based IDS (HIDS) works differently from a network-based version of IDS.

While a network-based-IDS resides on a network segment and monitors activities across that segment, a host-based IDS resides on a particular computer or server,known as the host and monitors activity only on that system. HIDs are also known as System Integrity Verifiers as they benchmark and monitor the status of key system files and detect when an intruder creates, modifies or deletes monitored files. A HIDs is also capable of monitoring system configuration databases, such as windows registries, in addition to stored configuration files like .ini, .cfg, and .dat files.

**c) Application-based IDS**

A refinement of Host-based IDs is the application-based IDS (AppIDS). Whereas the HIDs examines a single system for file modification, the application based IDs examines an application for abnormal incidents. It looks for anomalous occurrences such as users exceeding their authorization, invalid file executions etc.

**d) Signature-based IDS**

It is based on detection methods. A signature-based IDS (also called Knowledge- based IDs) examines data traffic in search of patterns that match known signatures – that is, preconfigured, predetermined attack patterns.

Many attacks have clear and distinct signatures such as

(i) foot printing and fingerprinting activities, have an attack pattern that includes the use of ICMP,DNS querying, and e-mail routing analysis

(ii) Exploits involve a specific attack sequence designed to take advantage of a vulnerability to gain access to a system

(iii) Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

**e) Statistical Anomaly-Based IDS(Also called Behavior-based IDS)**

This approach is used for detecting intrusions based on the frequency with which certain network activities takes place. Statistical Anomaly-Based IDS collects statistical summaries by observing traffic that is known to be normal. A baseline is established based on normal period. The Stats IDs periodically sample network activity, and using statistical methods compares the sampled network activity to the baseline. When the measured activities are outside the baseline parameters ,it is said to be exceeding the clipping level; at this point, the IDS will trigger an alert to notify the administrator.

**f) Log File Monitors (LFM)**

Log File Monitor (LFM) is an approach to IDS that is similar to NIDS. Using L Fm the system reviews the log files generated by servers, network devices, and when other IDSs. These systems look for patterns and signatures in the log files that may indicate an attack or intrusion is in process or has already succeeded.

**What are Honey Pots, Honey Nets, and Padded Cell Systems?**

A class of powerful security tools that go beyond routine intrusion detection is known variously as honey pots, honey nets and padded cell systems. Honey pots are decoy systems designed to lure potential attackers away from critical systems and encourage attacks against themselves. These systems are created for the sole purpose of deceiving potential attackers. In Industry they are known as decoys, lures, and fly-traps.

When a collection of honey pots connects several honey pot systems on a subnet, it may be called a honey net.

In sum, honey pots are designed to

i) Divert an attacker from accessing critical systems.

ii) Collect information about the attacker‘s activity

iii) Encourage the attacker to stay on the system long enough for administrators to document the event and, perhaps respond.

A Padded Cell is a honey pot that has been protected so that it cannot be easily compromised. In other words, a padded cell is a hardened honey spot.

The advantages and disadvantages of using honey pot or padded cell approach

Advantages:

- Attackers can be diverted to targets that they cannot damage.
- Administrators have time to decide how to respond to an attacker. Attacker’s action can be easily and extensively monitored

- Honey pots may be effective at catching insiders who are snooping around a network.

Disadvantages:

- The legal implication of using such devices are not well defined.
- Honey pots and Padded cells have not yet been shown to be generally useful security technologies.
- An expert attacker, once diverted into a decoy system, may become angry and launch a hostile attack against an organization‘s systems
- Admins and security managers will need a high level of expertise to use these systems.

**Scanning and Analysis Tools**

- Scanners, sniffers, and other analysis tools are useful to security administrators in enabling them to see what the attacker sees
- Scanner and analysis tools can find vulnerabilities in systems
- One of the preparatory parts of an attack is known as foot printing – collecting IP addresses and other useful data
- The next phase of pre-attack data gathering process is called fingerprinting – scanning all known addresses to make a network map of the target

How Scanning and Analysis tools are useful in enforcing Information Security?

Scanning and Analysis Tools

- Scanners, sniffers, and other analysis tools are useful to security administrators in enabling them to see what the attacker sees
- Scanner and analysis tools can find vulnerabilities in systems

One of the preparatory parts of an attack is known as foot printing – collecting IP addresses and other useful data

The next phase of pre-attack data gathering process is called fingerprinting –

Scanning all known addresses to make a network map of the target

## Intrusion detection

It’s a dire fact that while every enterprise has a firewall, most still suffer from network security problems. IT professionals are acutely aware of the need for additional protective technologies, and network equipment vendors are anxious to fill in the gap.

Intrusion Prevention Systems have been promoted as cost-effective ways to block malicious traffic, to detect and contain worm and virus threats, to serve as a network monitoring point, to assist in compliance requirements, and to act as a network sanitizing agent.

IDPSs are primarily focused on:

- Identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.
- Identifying problems with security policies
- Documenting existing threats.
- Deterring individuals from violating security policies.

In addition, all types of IDPSs perform the following:

Recording information related to observed events. Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.

Notifying security administrators of important observed events. This notification, known as an alert, may take the form of audible signals, e-mails, pager notifications, or log entries. A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.

Producing reports. Reports summarize the monitored events or provide details on particular events of interest.

An IDPS might also alter the settings for when certain alerts are triggered or what priority should be assigned to subsequent alerts after a particular threat is detected.

IPSs respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques:

The IPS stops the attack itself. Examples:

Terminate the network connection or user session that is being used for the attack. Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute. Block all access to the targeted host, service, application, or other resource.

The IPS changes the security environment. The IPS could change the configuration of other security controls to disrupt an attack. Such as reconfiguring a network device (e.g., firewall, router, switch) to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacks. Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities.

The IPS changes the attack's content. Some IPS technologies can remove or replace malicious portions of an attack to make it benign. An example is an IPS removing an infected file attachment from an e-mail and then permitting the cleaned email to reach its recipient.

Most IDPSs also offer features that compensate for the use of common evasion techniques. Evasion is modifying the format or timing of malicious activity so that its appearance changes but its effect is the same. Attackers use evasion techniques to try to prevent IDPSs from detecting their attacks.

For example: an attacker could encode text characters in a particular way, knowing that the target understands the encoding and hoping that any monitoring IDPSs do not. Most IDPSs can overcome common evasion techniques by duplicating special processing performed by the targets. If the IDPS can "see" the activity in the same way that the target would, then evasion techniques will generally be unsuccessful at hiding attacks.

## Virtual Private Network-Need, Use of Tunnelling with VPN.

Virtual private network technology is based on the idea of tunneling. VPN tunneling involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side.

For Internet-based VPNs, packets in one of several VPN protocols are encapsulated within Internet Protocol (IP) packets. VPN protocols also support authentication and encryption to keep the tunnels secure.

Types of VPN Tunneling

VPN supports two types of tunneling - voluntary and compulsory. Both types of tunneling are commonly used.

In voluntary tunneling, the VPN client manages connection setup. The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs). Then, the VPN client application creates the tunnel to a VPN server over this live connection.

In compulsory tunneling, the carrier network provider manages VPN connection setup. When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. From the client point of view, VPN connections are set up in just one step compared to the two-step procedure required for voluntary tunnels.

Compulsory VPN tunneling authenticates clients and associates them with specific VPN servers using logic built into the broker device. This network device is sometimes called the VPN Front End Processor (FEP), Network Access Server (NAS) or Point of Presence Server (POS). Compulsory tunneling hides the details of VPN server connectivity from the VPN clients and effectively transfers management control over the tunnels from clients to the ISP. In return, service providers must take on the additional burden of installing and maintaining FEP devices.

VPN Tunneling Protocols

Several computer network protocols have been implemented specifically for use with VPN tunnels. The three most popular VPN tunneling protocols listed below continue to compete with each other for acceptance in the industry. These protocols are generally incompatible with each other.

Point-to-Point Tunneling Protocol (PPTP)

Several corporations worked together to create the PPTP specification. People generally associate PPTP with Microsoft because nearly all flavors of Windows include built-in client support for this protocol. The initial releases of PPTP for Windows by Microsoft contained security features that some experts claimed were too weak for serious use. Microsoft continues to improve its PPTP support, though.

Layer Two Tunneling Protocol (L2TP)

The original competitor to PPTP for VPN tunneling was L2F, a protocol implemented primarily in Cisco products. In an attempt to improve on L2F, the best features of it and PPTP were combined to create a new standard called L2TP. Like PPTP, L2TP exists at the data link layer (Layer Two) in the OSI model -- thus the origin of its name.

Internet Protocol Security (IPsec)

IPsec is actually a collection of multiple related protocols. It can be used as a complete VPN protocol solution or simply as the encryption scheme within L2TP or PPTP. IPsec exists at the network layer (Layer Three) of the OSI model.

## Authentication Mechanisms

The VPN server can be configured to use either Windows or Remote Authentication Dial-In User Service (RADIUS) as an authentication provider. If Windows is selected as the authentication provider, the user credentials sent by users attempting VPN connections are authenticated using typical Windows authentication mechanisms, and the connection attempt is authorized using the VPN client’s user account properties and local remote access policies.

If RADIUS is selected and configured as the authentication provider on the VPN server, user credentials and parameters of the connection request are sent as RADIUS request messages to a RADIUS server.

The RADIUS server receives a user-connection request from the VPN server and authenticates and authorizes the connection attempt. In addition to a yes or no response to an authentication request, RADIUS can inform the VPN server of other applicable connection parameters for this user such as maximum session time, static IP address assignment, and so on.

RADIUS can respond to authentication requests based on its own user account database, or it can be a front end to another database server, such as a Structured Query Language (SQL) server or a Windows domain controller (DC). The DC can be located on the same computer as the RADIUS server or elsewhere. In addition, a RADIUS server can act as a proxy client to a remote RADIUS server.

The RADIUS protocol is described in RFC 2865 and RFC 2866 in the IETF RFC Database.

The VPN server can be configured to use either Windows or RADIUS as an accounting provider. If Windows is selected as the accounting provider, the accounting information accumulates on the VPN server for later analysis. Logging options can be specified from the properties of the Local File or SQL Server objects in the Remote Access Logging folder in the Routing and Remote Access snap-in. If RADIUS is selected, RADIUS accounting messages are sent to the RADIUS server for accumulation and later analysis.

Most RADIUS servers can be configured to place authentication request records into an audit file. A number of third parties have written billing and audit packages that read RADIUS accounting records and produce various useful reports. For more information about RADIUS accounting, see RFC 2866 in the IETF RFC Database.

The VPN server can be managed using industry-standard network management protocols and infrastructure. The computer acting as the VPN server can participate in a Simple Network Management Protocol (SNMP) environment as an SNMP agent if the Windows Server 2003 SNMP service is installed. The VPN server records management information in various object identifiers of the Internet

Management Information Base (MIB) II, which is installed with the Windows Server 2003 SNMP service. Objects in the Internet MIB II are documented in RFC 1213 in the IETF RFC Database.

## Types of VPNs and their Usage

Site-to-Site VPN

A site-to-site VPN allows two or more networks to be joined together. These networks use sophisticated encryption services to allow the connection to exist without hackers intercepting the traffic between the locations. Going back to our example, the connection between the branch office and its headquarters is an example of a site-to-site VPN. Users at both locations cannot tell that they are accessing network resources from another site because it is transparent to them.

Remote access VPN

A remote access VPN allows a user with a computer to access a private network. For example, I have a remote access VPN at my home that allows me to connect to my server, which stores all my music, documents from work, and photos of my family. I can access my VPN from my smart phone if I need something important.

## TYPES OF VPNs and their Usage

VPNs can be broadly categorized as follows:

1. A firewall-based VPN is one that is equipped with both firewall and VPN capabilities. This type of VPN makes use of the security mechanisms in firewalls to restrict access to an internal network. The features it provides include address translation, user authentication, real time alarms and extensive logging.
2. A hardware-based VPN offers high network throughput, better performance and more reliability, since there is no processor overhead. However, it is also more expensive.
3. A software-based VPN provides the most flexibility in how traffic is managed. This type is suitable when VPN endpoints are not controlled by the same party, and where different firewalls and routers are used. It can be used with hardware encryption accelerators to enhance performance. 4. An SSL VPN3 allows users to connect to VPN devices using a web browser. The SSL (Secure Sockets Layer) protocol or TLS (Transport Layer Security) protocol is used to encrypt traffic between the web browser and the SSL VPN device. One advantage of using SSL VPNs is ease of use, because all standard web browsers support the SSL protocol, therefore users do not need to do any software installation or configuration.

## VPN SECURITY CONSIDERATIONS

The following is general security advice for VPN deployment:

1. VPN connections can be strengthened by the use of firewalls.
2. An IDS / IPS (Intrusion Detection / Prevention System) is recommended in order to monitor attacks more effectively.
3. Anti-virus software should be installed on remote clients and network servers to prevent the spread of any virus / worm if either end is infected.
4. Unsecured or unmanaged systems with simple or no authentication should not be allowed to make VPN connections to the internal network.
5. Logging and auditing functions should be provided to record network connections, especially any unauthorized attempts at access. The log should be reviewed regularly.
6. Training should be given to network/security administrators and supporting staff, as well as to remote users, to ensure that they follow security best practices and policies during the implementation and ongoing use of the VPN.
7. Security policies and guidelines on the appropriate use of VPN and network support should be distributed to responsible parties to control and govern their use of the VPN.

8. Placing the VPN entry point in a Demilitarized Zone (DMZ) is recommended in order to protect the internal network.

9. It is advisable not to use split tunneling to access the Internet or any other insecure network simultaneously during a VPN connection. If split tunneling is VPN Security Page 20 of 23 used, a firewall and IDS should be used to detect and prevent any potential attack coming from insecure networks.

10. Unnecessary access to internal networks should be restricted and controlled.

## EXTRANET VPN SECURITY CONSIDERATIONS

The following are additional security considerations for extranet VPN deployment:

1. Strong user authentication mechanisms should be enforced.

2. The VPN entry point should be placed inside a DMZ to prevent partners from accessing the internal network.

3. Access rights should be granted on an as-needed basis. Only necessary resources should be available to external partners. Owners of these resources should review access permissions regularly.

## CLIENT SIDE VPN SECURITY CONSIDERATIONS

The following are general security considerations for VPN users:

1. Strong authentication is required when users are connecting dynamically from disparate, untrusted networks, for example:

a) By means of certificates and/or smart cards, or tokens: A smart card is used to store a user profile, encryption keys and algorithms. A PIN number is usually required to invoke the smart card. A token card provides a one-time password. When the user authenticates correctly on the token by entering the correct PIN number, VPN Security Page 21 of 23 the card will display a one-time passcode that will allow access to the network.

b) By means of add-on authentication system, like TACACS+, RADIUS. This kind of central authentication system contains a profile of all VPN users, controlling the access to the private network.

2. Personal firewalls should be installed and configured properly on client VPN machines to block unauthorized access to the client, ensuring it is safe from attack. Many of the more recent remote access VPN clients include personal firewalls. Some may also include other configuration checks, such as the client not being able to connect to the network if anti-virus software is not running, or if virus signatures are out of date.

3. The client machine should have anti-virus software installed, with up-to-date signatures, to detect and prevent virus infections. 4. The user should remain aware of the physical security of the machine, in particular when authentication information is stored on the machine. 5. All users should be educated on good Internet security practices. Access from home should be considered an insecure channel, as traffic is routed over the Internet.

## COMMON SECURITY FEATURES IN VPN PRODUCTS

The following are security features to look for when choosing a VPN product:

1. Support for strong authentication, e.g. TACACS+, RADIUS, smart cards / tokens.

2. Industry-proven strong encryption algorithms, with long key strength support to protect data confidentiality during transmission.

3. Support for anti-virus software, and intrusion detection / prevention features.

4. Strong default security for all administration / maintenance ports.

5. Digital certificate support, such as using certificates for site to site authentication

6. Address management support, such as the capability to assign a client address on the private network and ensuring all addresses are kept private.