Information Security [ETCS-401]

Dr. A K Yadav
Amity School of Engineering and Technology
(affiliated to GGSIPU, Delhi)
akyadav1@amity.edu
akyadav@akyadav.in
www.akyadav.in
+91 9911375598

February 15, 2021

Introduction

- What is Information?
- Why it is so important?
- What is Information Security?
- How can we secure information?

What is Information?

- Dictionary Definition: *facts provided or learned about something or someone*
- Information is prompt that has meaning in some context for its receiver and/or sender.
- Information has become a great and inexhaustible resource in national development.
- To live effectively is to live with authentic and adequate information.
- It is also used by government and civics bodies in formulation of good policies
- Good information is essential for effective operation and decision making at all levels in businesses.
- Identifies and illustrates the different kinds of information by the complex internal and external communication links of a typical R&D department.

Why it is so important?

- Over the last few years, the IT security threat landscape has changed significantly.
- Traditional malware threats hit an apparent wall in 2005
- However new threats (bots, spam, phishing) have stepped in.
- Unauthorized access (malware, spyware) limits our ability to protect the confidentiality of the data
- Malicious programs can alter the data values, destroying the integrity of the data
- Denial of Service (DoS) attacks can shut down a server and/or network, making the system unavailable.
- Efforts to correct costs corporations time and money!
- There were on average over 20 million phishing attempts per day.

- USA organizations alone more than 10 billion USD spam cost in 2004, including lost productivity and the additional equipment, software, and manpower needed to combat the problem.
- Regulatory Issues for different countries
- Loss of corporate confidential information (financials, personnel)

What is Information Security?

- Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.
- Deals with several different "trust" aspects of information and its protection
- Three widely accepted elements or areas of focus:
  - Confidentiality
  - Integrity
  - Availability (Recoverability)
- Includes Physical Security as well as Electronic

How can we secure information?

- Security Assessment
  - Identify areas of risk
  - Identify potential for security breaches, collapses
  - Identify steps to mitigate
- Security Application
  - Expert knowledge (train, hire, other)
  - Multi-layered Approach (there is no single solution)
  - Policies and Procedures
- Security Awareness
  - Not just for the geeks
  - Security Training at all levels (external and/or internal)
  - Continuing education and awareness – not a one-time shot
  - Make it part of the culture

Key Points

- Objective of Information Security is ***Confidentiality, Integrity, Availability***
- Protect your systems and your data
- Threats are numerous, evolving, and their impact is costly
- Security should be applied in layers and at every layer
- Security Awareness at all levels must be maintained
- Failure to Secure is an Opportunity to Fail

History of Information Security

- The need for computer security arose during World War II when the first mainframe computers were developed and used to aid computations for communication code breaking messages from enemy cryptographic devices like the Enigma.
- Multiple levels of security were implemented to protect these devices and the missions they served.
- This required new processes as well as tried-and-true methods needed to maintain data confidentiality.
- Access to sensitive military locations was controlled by means of badges, keys, and the facial recognition of authorized personnel by security guards.
- The growing need to maintain national security eventually led to more complex and technologically sophisticated computer security safeguards.

- During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes.
- The primary threats to security were physical theft of equipment, spying against products of the systems, and destroy.
- One of the first documented security problems that fell outside these categories occurred in the early 1960s
- when a systems administrator was working on a MOTD (message of the day) file while another administrator was editing the password file.
- A software glitch mixed the two files, and the entire password file was printed on every output file.
- **The 1960s**
- Advanced Research Procurement Agency (ARPA) began to examine feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception

- **The 1970s and 80s**
- ARPANET grew in popularity as did its potential for misuse
- Fundamental problems with ARPANET security were identified
  - No safety procedures for dial-up connections to ARPANET
  - Non-existent user identification and authorization to system

- Late 1970s: microprocessor expanded computing capabilities and security threats
- Information security began with Rand Report R-609 (paper that started the study of computer security)
- Scope of computer security grew from physical security to include:
  - Safety of data
  - Limiting unauthorized access to data
  - Involvement of personnel from multiple levels of an organization

- **The 1990s**
- Networks of computers became more common; so too did the need to interconnect networks
- Internet became first manifestation of a global network of networks
- In early Internet deployments, security was treated as a low priority

- **The Present**
- The Internet brings millions of computer networks into communication with each other—many of them unsecured
- Ability to secure a computer's data influenced by the security of every computer to which it is connected

Distributed Information System and its Importance

- A set of information systems physically distributed over multiple sites, which are connected with some kind of communication network
- Distributed processing is a technique for implementing a single logical set of processing functions across a number of physical devices, so that each performs some part of the total processing required.
- Distributed processing is often accompanied by the formation of a distributed database.
- A distributed database exists when the data elements stored at multiple locations are interrelated, or if a process (program execution) at one location requires access to data stored at another location

- They can communicate and coordinate with each other by passing messages to one another
- **Importance**
  - Scalable
  - More efficient
  - More reliable

Role of Internet and Web Services

- **Role of Internet:–**
  - The internet is a universal technology platform that allows any computer to communicate with any other computer in the world.
  - 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.
- **Web services in Information System:–**
  - A web service is any piece of software that makes itself available over the internet and uses a standardized XML messaging system.
  - XML is used to encode all communications to a web service.
  - For example, a client invokes a web service by sending an XML message, then waits for a corresponding XML response.

- Web services play a complementary and dominate role in building global information system for today's dynamic business world.
- Web services are self contained, modular applications that can be describe, published, located and invoked over a network.
- Web services performs functions using ranging from simple requests to complicated business processes.
- The idea of web services is to leverage the advantage of the web as a platform to apply it to the services themselves, not just to the static information.
- Web 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 product.
- Web services have been proven to give a strong return on investors and make computer based information system more adaptable.

- They also help bring productivity, flexibility,and low maintenance cost in the development of information system by integrating components from various third party vendor's product.

- **Benefits of web services for developing information security:-**
  - Web services tools are available for most computer system, including mainframes and packaged applications.
  - This means that not only the existing application can be retained, but also the existing knowledge of staff can be applied and extended using web services for business integration.
  - Web services are adaptable and can handle changes more readily than other integration solutions, because they use structured text as message format.
  - IT managers now have the ability to exchange data between most application, on most computers in a consistent and standard way.

Threats and attacks

- Information systems are frequently exposed to various types of threats which can cause different types of damages that might lead to significant financial losses.
- Information security damages can range from small losses to entire information system destruction.
- The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system.
- Organizations are struggling to understand what the threats to their information assets are and how to obtain the necessary means to combat them which continues to pose a challenge.
- A Threat is a possible security violation that might exploit the vulnerability of a system or asset.

- Attack is an deliberate unauthorized action on a system or asset.
- Attack can be classified as active and passive attack.
- An active attack attempts to alter system resources or affect their operation.
- A passive attack attempts to learn or make use of information from the system but does not affect system resources
- An attack will have a motive and will follow a method when opportunity arise.

Classification of Threats

Threats broadly can be classified into two categories:

1. Based on attacks techniques
2. Based on threats impacts

Classification based on attacks techniques

- **The three orthogonal dimensional model**
  Three dimensional model that subdivides threat space into subspaces according to three orthogonal dimensions labelled *motivation, localization and agent*:
  - Threat agent is an actor that imposes the threat on a specific asset of the system which is represented by three classes: *human, technological, force majeure*.
  - Threat motivation represents the cause of the creation of the threat and it is reorganized into two classes: *deliberate and accidental threat*
  - Threat localization represents the origin of threats, either *internal or external*.

- **Hybrid model for threat classification**
  A hybrid model for information system security threat classification named the information system security threat cube classification model or C3 model. They consider three main criteria:
  - Security threat frequency: It shows the frequency of security threat occurrence.
  - Area of security threat activity: It represents the domain that is being affected by the threat like physical security, personnel security, communication and data security, and operational security.
  - Security threat source: It gives types of the threat's source.
- **Information Security Threats Classification Pyramid model**
  A classification method for deliberate security threats in a hybrid model that you named Information Security Threats Classification Pyramid. It classifies deliberate threats based on three factors:

- Attackers prior knowledge about the system: It represents how much the attacker knows about the system in terms of system hardware, software, employees and users knowledge.
- Criticality of the area: It represents the criticality of parts of the system which might be affected by the threat.
- Loss: It represents all losses that can occur in the system or to the organization (privacy, integrity etc.)

Classification based on threats impacts
STRIDE Model

- Microsoft developed a classification method, called STRIDE, which is applied on the network, host, and application.
- STRIDE allows characterizing known threats according to the goals and purposes of the attacks (or motivation of the attacker).

- The STRIDE acronym is formed from the first letter of each of the following categories:
  Spoofing identity, **T**ampering with data, **R**epudiation, **I**nformation disclosure, **D**enial of service and **E**levation of privilege
- It is a goal-based approach, where an attempt is made to get inside the mind of the attacker by rating the threats against.

ISO model

The ISO standard (ISO 7498-2) has listed five major security threats impacts and services as a reference model:

- Destruction of information and/or other resources
- Corruption or modification of information
- Theft, removal or loss of information and/or other resources,
- Disclosure of information
- Interruption of services.

Different threats to Information Security

- Malware
- Internet bot
- Adware
- Spyware
- Spam
- Phishing
- Key Loggers
- Viruses
- Worms
- Trojan horses
- Ransomware

Malware

- Hostile, intrusive, or annoying software or program code ("malicious" + "software")
- Includes computer viruses, worms, trojan horses, bots, spyware, adware, etc
- Software is considered malware based on the intent of the creator rather than any particular features

Internet bot

- also known as web robots, are automated internet applications controlled by software agents
- These bots interact with network services intended for people, carrying out monotonous tasks and behaving in a human-like manner (i.e., computer game bot)
- Bots can gather information, reply to queries, provide entertainment, and serve commercial purposes.
- Botnet - a network of "zombie" computers used to do automated tasks such as spamming or reversing spamming

Adware

- Advertising-supported software is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.
- Adware is software integrated into or bundled with a program, typically as a way to recover programming development costs through advertising income

Spyware

- A broad category of software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user
- In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet
- Spyware can collect many different types of information about a user:
  - Records the types of websites a user visits
  - Records what is typed by the user to intercept passwords or credit card numbers
  - Used to launch "pop up" advertisements
- Many legitimate companies incorporate forms of spyware into their software for purposes of advertisement(Adware)

Spam

- Spamming is the abuse of electronic messaging systems to send unsolicited, undesired bulk messages
- Spam media includes:
  - e-mail spam (most widely recognized form)
  - instant messaging spam
  - Usenet newsgroup spam
  - Web search engine spam
  - spam in blogs
  - mobile phone messaging spam

Phishing

- A criminal activity using social engineering techniques.
- An attempt to acquire sensitive data, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication.
- Typically carried out using email or an instant message

Key Loggers

- Keystroke logging (often called keylogging) is a diagnostic used in software development that captures the user's keystrokes
  - Useful to determine sources of error in computer programs
  - Used to measure employee productivity on certain clerical tasks
- Highly useful for law enforcement and espionage
  - Obtain passwords or encryption keys and thus bypassing other security measures
- Widely available on the internet and can be used by anyone for the same purposes
- Can be achieved by both hardware and software means
- Hardware key loggers are commercially available devices which come in three types:
  - Inline devices that are attached to the keyboard cable
  - Devices installed inside standard keyboards

- Keyboards that contain the key logger already built-in

- Writing software applications for keylogging is trivial, and like any computer program can be distributed as malware (virus, trojan, etc.)

Viruses

- A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions
- It can self-replicate, inserting itself onto other programs or files, infecting them in the process

Worms

- A computer worm is a type of malware that spreads copies of itself from computer to computer.
- A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.
- The primary difference between a virus and a worm is that viruses must be triggered by the activation of their host; whereas worms are stand-alone malicious programs that can self-replicate and propagate independently as soon as they have breached the system

Trojan Horse

- A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer.
- A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.
- A Trojan acts like a bona fide application or file to trick you
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.
- Trojans must spread through user interaction such as opening an email attachment or downloading and running a file from the Internet

Ransomware

- Ransomware is a type of malicious software designed to block access to a computer system or computer files until a sum of money is paid.
- Most ransomware variants encrypt the files on the affected computer, making them inaccessible, and demand a ransom payment to restore access

Tutorial 1

1. Among the fundamental challenges in information security are confidentiality, integrity, and availability, or CIA. Define each of these terms.
2. Give a concrete example where confidentiality is more important than integrity.
3. Give a concrete example where integrity is more important than confidentiality.
4. Give a concrete example where availability is the overriding concern.
5. From a bank's perspective, which is usually more important, the integrity of its customer's data or the confidentiality of the data? From the perspective of the bank's customers, which is more important?

6. Discuss a significant World War II event where broken Enigma messages played a major role.

Assessing Damages

- A risk analysis needs to be a part of every security effort.
- It should analyze and categorize the assets that need to be protected and the risks that need to be avoided
- It should facilitate the identification and prioritization of protective elements.
- It can also provide a means to measure the effectiveness of the overall security architecture, by tracking those risks and their associated mitigation over time to observe trends.
- How formal and extensive should your risk analysis be?
- That really depends on the needs of your organization and the audience for the information.
- In a larger, well structured environment, a more detailed risk analysis may be needed.

- Military and high-risk environments may also merit a greater level of diligence and detail.
- On the other side, a small office environment, like that of a dentist or lawyer, may not require a deep analysis.
- In any case, there must be at least some definition of what the security program is intended to defend
- Not proper analysis may focus on the wrong priorities or overlook important assets (leaving them exposed) and threats (failing to defend against them)
- Formal definition of risk is the probability of an undesired event exploiting a vulnerability to cause an undesired result to an asset.
- $Risk$ = Probability of occurance xCost of Asset Damage

- A quantitative approach to risk analysis will take into account actual values — the estimated probability or likelihood of a problem occurring along with the actual cost of loss or compromise of the assets in question.
- One commonly used approach to assigning cost to risks is
  Annualized Loss(ALE) =
  Single Loss(SLE)xAnnualized Rate(ARO)
  where ALE is *annualized loss expectancy*, SLE is *single loss expectancy*, and ARO is *annualized rate of occurrence*
- Problems with the ALE approach.

Security in Mobile

- Many mobile devices such as smartphones and tablets are typically designed from a consumer perspective.
- They're meant to be user friendly, and they typically come with a built-in security model as part of the operating system to protect the user from a variety of threats.
- They are productivity-focused first; and security is only a secondary consideration.
- They do have some built-in security features
- Today we will first look at the key risks associated with mobile devices, both to the devices themselves as well as to the applications that run on those devices
- A clear understanding of the risks is necessary before you can determine the appropriate countermeasures.

Mobile Device Risks

Security risks that affect mobile devices fall into two categories:

- **Device risks** which are based on the fact that today's smartphones and tablets are a new breed of powerful computer with capabilities of local and cloud-based storage Enterprise organizations have less control over these than they do with more traditional, well-understood desktop and laptop computers.
- **Application risks** which originate from third-party apps installed by end users.
  These apps often can access corporate data, store it on the device, and upload it outside the corporate perimeter.

Device Risks

- Smartphones and tablets are basically computers
- They are susceptible to the same threats as computers
- These threats can exploit vulnerabilities in the underlying operating system to cause data loss and theft, changes to settings, denial of service, intrusions into protected internal networks etc.
- Malware can infect smartphones and tablets just like computers
- Malware can form the platform on which attackers can perform network intrusions and data theft

- A compromised mobile device will be an excellent tool for breaking into a network and stealing data, especially if it is not perceived as a significant threat within an organization and not protected as well as a computer system. -The followings are the other threats against mobile devices:

- Data Storage
- Weak Passwords
- Wi-Fi Hijacking
- Open Hotspots
- Baseband Hacking
- Bluetooth Snooping and Fuzzing

Data Storage

- Modern smartphones, cameras, and tablets contain large amounts of flash memory and are accessible via USB, allowing data thieves to copy files.
- Mobile devices have so much storage capacity that they can be used to steal all the data in many organizations.
- Data storage on mobile devices makes it so easy to bulk-download huge amounts of data
- These devices can pose a significant risk to an organization's data
- It is hard to detect hidden stolen data
- The on-board memory storage on mobile devices allows them to be mounted as a storage device on any computer.
- They can be used to copy data, which can then be stolen or misused.

- Once the data gets on the mobile device, it is much hard for organizations to control.
- Data can also be stolen or misused through e-mail attachments and other applications.

Weak Passwords

- Any computing platform provides access to data and resources based on end-user credentials involving a password
- Mobile devices provide a path of attack to any resource if the attacker can guess or intercept the user's password.
- This is especially significant for e-mail because getting into a smartphone or tablet and reading e-mail is relatively easy if you have the password or PIN.

Wi-Fi Hijacking

- Wi-Fi hijacking is done by malicious attackers through the use of free Wi-Fi hotspots set up in public places where end users get the free wireless eg airports, coffee shops, parks, and railways stations etc.
- These hotspots are often monitored by attackers looking to harvest personal information, financial data, and passwords.

Open Hotspots

- Mobile devices can be used to tether a computer or otherwise act as a wireless network
- Computers around them can use to access the Internet just like a regular Wi-Fi or Bluetooth access point.
- Attackers nearby could also connect to the hotspots without the user's knowledge
- They can fire attacks against the local network and its devices

Baseband Hacking

- Smartphones contain both networking and voice capabilities, the network can be used to compromise the voice function.
- Cellular calls can be intercepted by a network attacker who compromises the smartphone.
- These attacks may exploit vulnerabilities in the underlying hardware of the smartphone, such as the hardware and firmware used by iPhone and Android devices.
- These attacks use the smartphone's baseband processor to over turn it into a listening device that allows the intruder to listen the conversations, even when a call is not in progress, by using the built-in microphone.

Bluetooth Snooping and Fuzzing

- Most end users leave their Bluetooth device PINs set at the default PIN
- They are nearly always set to 0000 or 1234
- Even advanced technical specialists may not know how to change these codes without a lot of research.
- As a result, an attacker can easily pair with a phone or a device and use that connection to steal or intercept data or listen your calls
- A type of attack known as “fuzzing” can be performed via Bluetooth pairing.
- A fuzzing attack can send invalid data to cause abnormal behaviour such as crashing, privilege escalation, and intrusions that can implant malware.

Application risks

- Third-party apps for mobile devices are written by people you don't know and in environments you can't control
- You have no visibility into their process, development lifecycle, or quality control
- Anybody can upload an app to an application store.
- These apps can be malicious, or they can intentionally or unintentionally compromise the security policies and standards that have been established within your organization.
- The following are the risks associated with these apps:

- Trojaned Apps
- Hidden Malicious URLs
- Phishing
- Smishing
- War Texting

Trojaned Apps

- Just as with PCs, useful applications can be infected with malware.
- They can be either realistic-looking apps that compromise the mobile device directly
- They can be actual apps that contain hidden code that may take control over the phone at a later time.
- In March 2011, a malware outbreak involving a Trojan called DroidDream took place because the Trojan was hidden in dozens of apps
- Some of these apps were legitimate and productive and available in the authorized Google Play store.

Hidden Malicious URLs

- URL-shortening or redirection is a common method of including a link in a message or web page without filling the screen with complicated location information.
- This makes seeing the end point location impossible until the user clicks the link to find out where it goes.
- In addition, the link text that appears on the screen may be different from the actual link embedded inside page code, especially in e-mail messages.
- Attackers can use this technique to send people to malicious web sites.
- On mobile devices, it can be very difficult to validate links before visiting them, unlike on computers where hovering the pointer over the link text shows the actual link location.

Phishing

- Phishing on mobile devices represents exactly the same risk as with computers.
- Phishing uses the classic technique of sending e-mail containing a malicious attachment or web link along with some fake but realistic-looking message to trick the end user into opening the attachment or link.
- This technique is used to steal personal information such as bank account numbers, credit card numbers, or usernames and passwords.

Smishing

- Similar to phishing, smishing uses SMS text messages to lure unsuspecting end users into calling a voice number to give personal information.
- These text messages contain a realistic seeming and urgent request to confirm details for security reasons or to confirm a purchase, refund, or payment.

War Texting

- Modern automobiles have become computerized, networked, interconnected, and interoperable with smartphones
- Attacks against the smartphone can give attackers the ability to remotely start, unlock, track, or operate a vehicle associated with the compromised smartphone
- These attacks have been given nick name as war texting.

Tutorial 2

1. When you want to authenticate yourself to your computer, most likely you type in your username and password. The username is considered public knowledge, so it is the password that authenticates you. Your password is something you know.
   - 1.1 It is also possible to authenticate based on something you are, that is, a physical characteristic. Such a characteristic is known as a biometric. Give an example of biometric-based authentication.
   - 1.2 It is also possible to authenticate based on something you have, that is, something in your possession. Give an example of authentication based on something you have.

1.3 Two-factor authentication requires that two of the three authentications methods (something you know, something you have, something you are) be used. Give an example from everyday life where two-factor authentication is used. Which two of the three are used?

2. How effective is the CAPTCHA? How user-friendly is the CAPTCHA?
3. Why do you hate CAPTCHAs?
4. Malware is software that is intentionally malicious, in the sense that it is designed to do damage or break the security of a system. Malware comes in many familiar varieties, including viruses, worms, and Trojans.
   - 4.1 Has your computer ever been infected with malware? If so, what did the malware do and how did you get rid of the problem? If not, why have you been so lucky?
   - 4.2 In the past, most malware was designed to annoy users. Today, it is often claimed that most malware is written for profit. How could malware possibly be profitable?

5. What is war dialling and war driving? What is war carting?
6. Suppose that we have a computer that can test 2^{40} keys each second.
   - 6.1 What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{88}?
   - 6.2 What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{112}?
   - 6.3 What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{256}?

Mobile Device Security

- Built-in Security Features
- Mobile Device Passwords
  - Password length
  - Password complexity
  - Screen-lock grace period
  - Password history
  - Password age
  - Number of allowed failed login attempts
- Encryption
- Mobile Device Management (MDM) With MDM solutions, organizations can perform the following activities:
  - Device provisioning and configuration
  - Software distribution
  - Encryption and password management
  - Remote wipe and lock
  - Policy enforcement

- Policy Management
  - Password settings:
    Password required, password complexity, password length, password lifetime, number of passwords remembered, number of password failures before lock, number of password failures before the device is wiped
  - Services disabled:
    POP and IMAP messaging and SMS and MMS messaging
  - Functions disabled:
    Removable storage, camera, Wi-Fi networking, infrared, Bluetooth
  - Access disabled:
    Access to ActiveSync
  - Applications to block:
    Blocking the execution of individual apps
  - Privilege of applications:
    Running apps under regular user or privileged account
  - Roles:
    Removing privileged role permission for the user

- Installation restrictions:
  Blocking unsigned installations and blocking unsigned themes
- Encryption:
  Device encryption, files excluded from encryption, storage device
- Mobile VPN settings:
  Various location and encryption settings
- Software distribution settings:
  Various settings to manage required applications that must be installed on the device
- Certificates:
  Removing unmanaged certificates (card) encryption

- Security Management: Security management controls provided by MDM solutions include enforcement of authentication, application controls, and encryption.
- Software Management: Software management options provide control over deploying, managing, updating, deleting, and blocking applications on mobile devices.

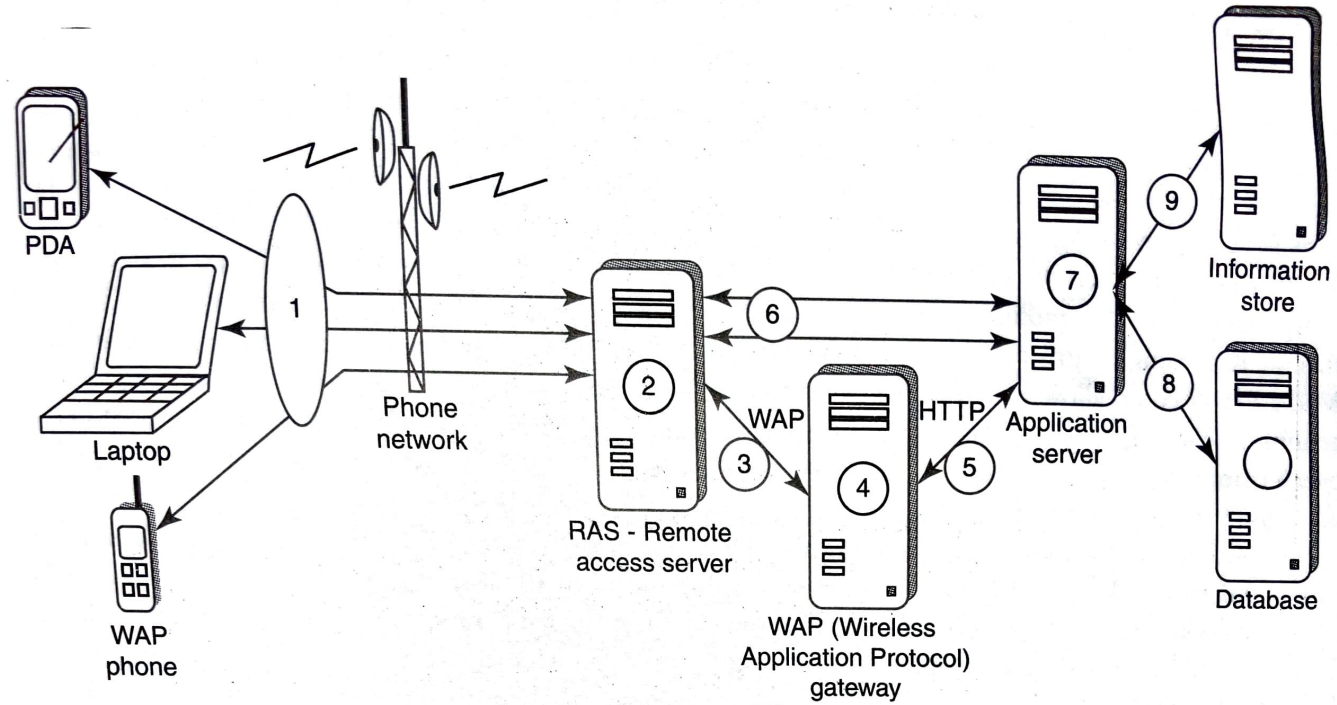
- Inventory Management : Asset management capabilities include tracking of devices, owners, and applications along with remote support.
- Remote Provisioning and Deprovisioning: Devices can be set up automatically when new users join the organization's device pool, and they can be remotely wiped (full or selective) upon termination.
- Messaging Control: MDM solutions provide secure channels and control over features of standard office productivity tools by restricting and enforcing settings for e-mail, calendar, contacts, notes, and tasks.
- Data Loss Prevention (DLP)

Authentication Service Security

There are two components of security in mobile computing:
Security of Device
Security of Networks

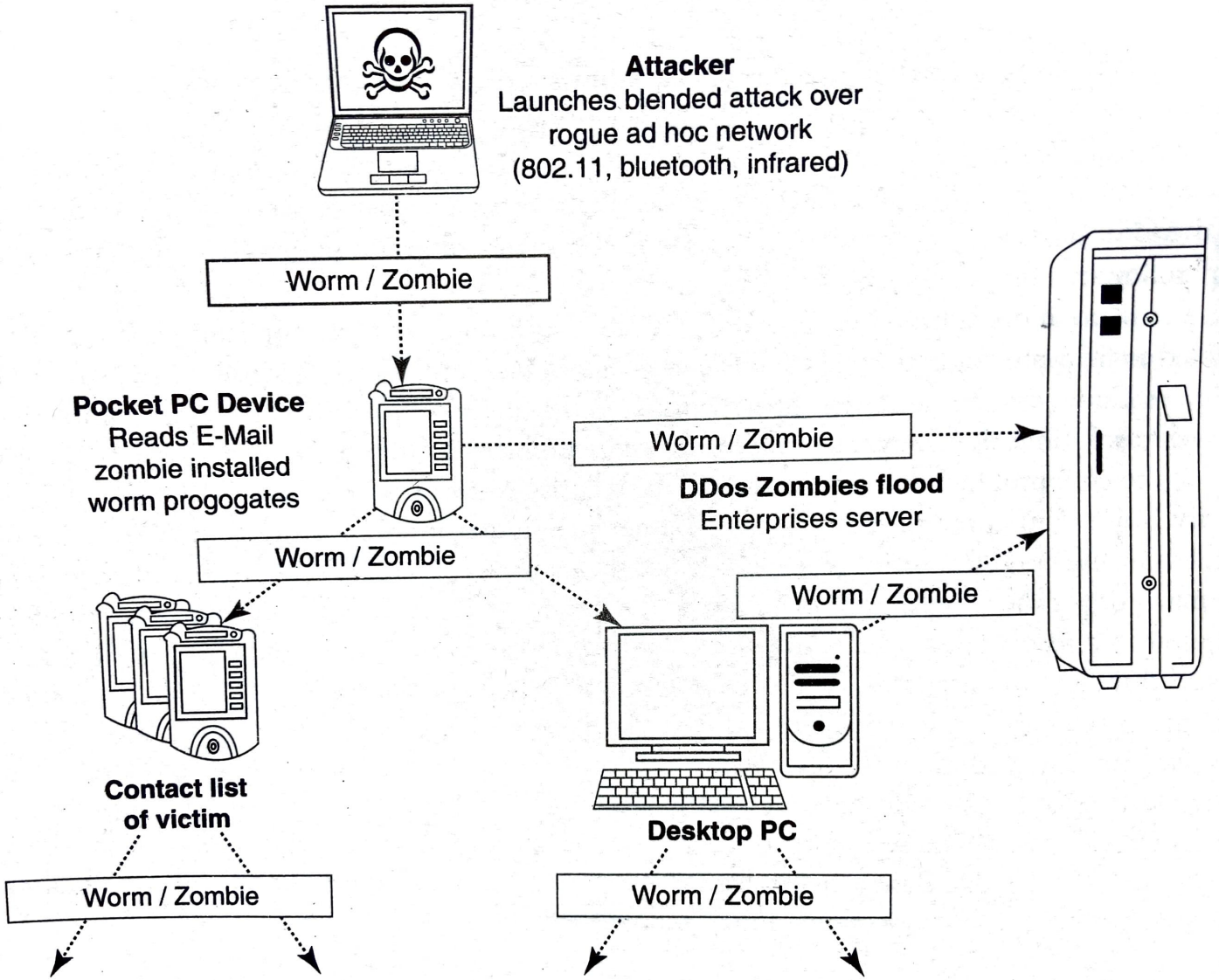
- Cryptographic Security for Mobile Devices
- Lightweight Directory Access Protocol (LDAP) Security for Hand-held Mobile Computing Devices
- Remote Access Service (RAS) Security for Mobile Devices
- Media Player Control Security

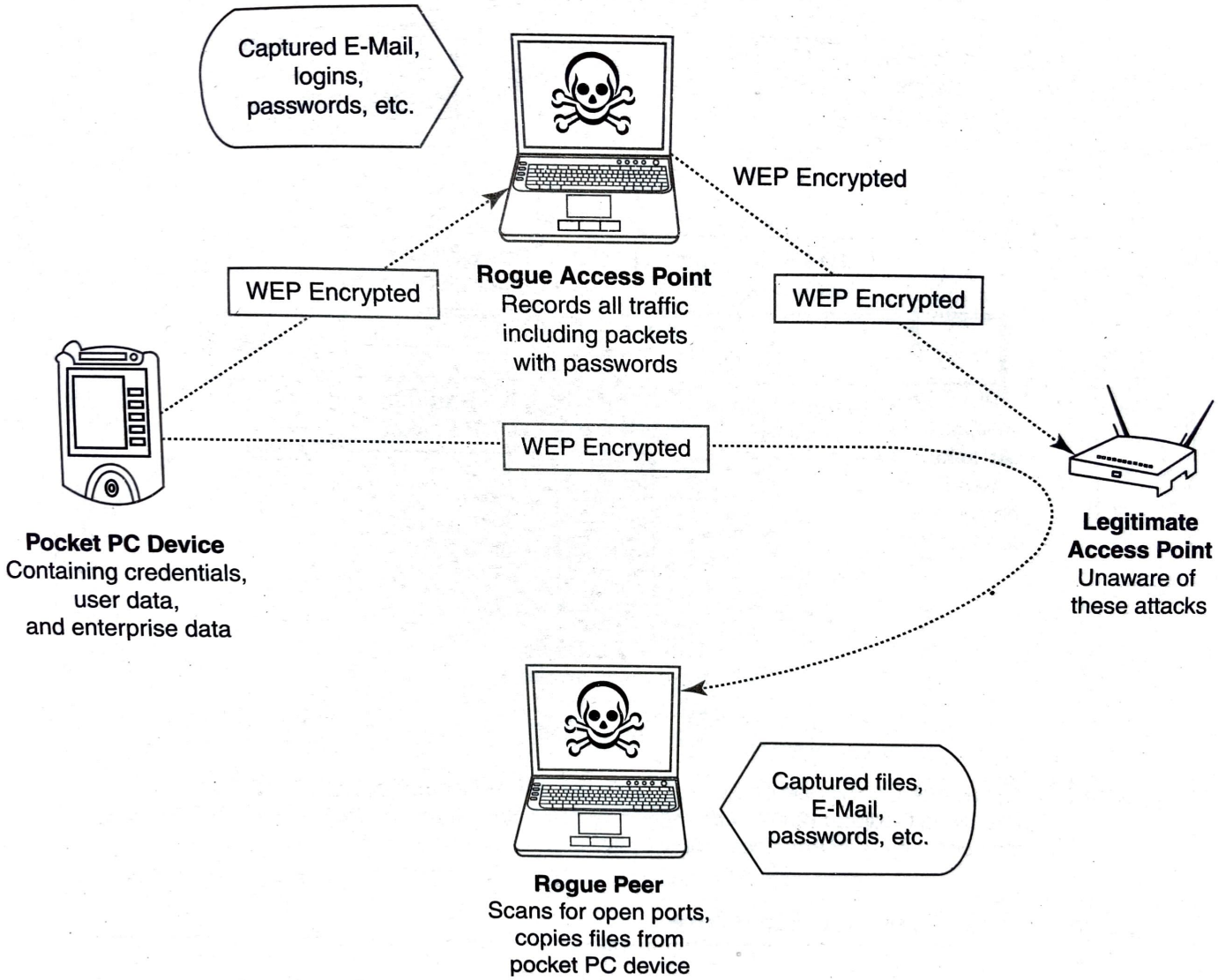
Networking API Security for Mobile Computing Applications

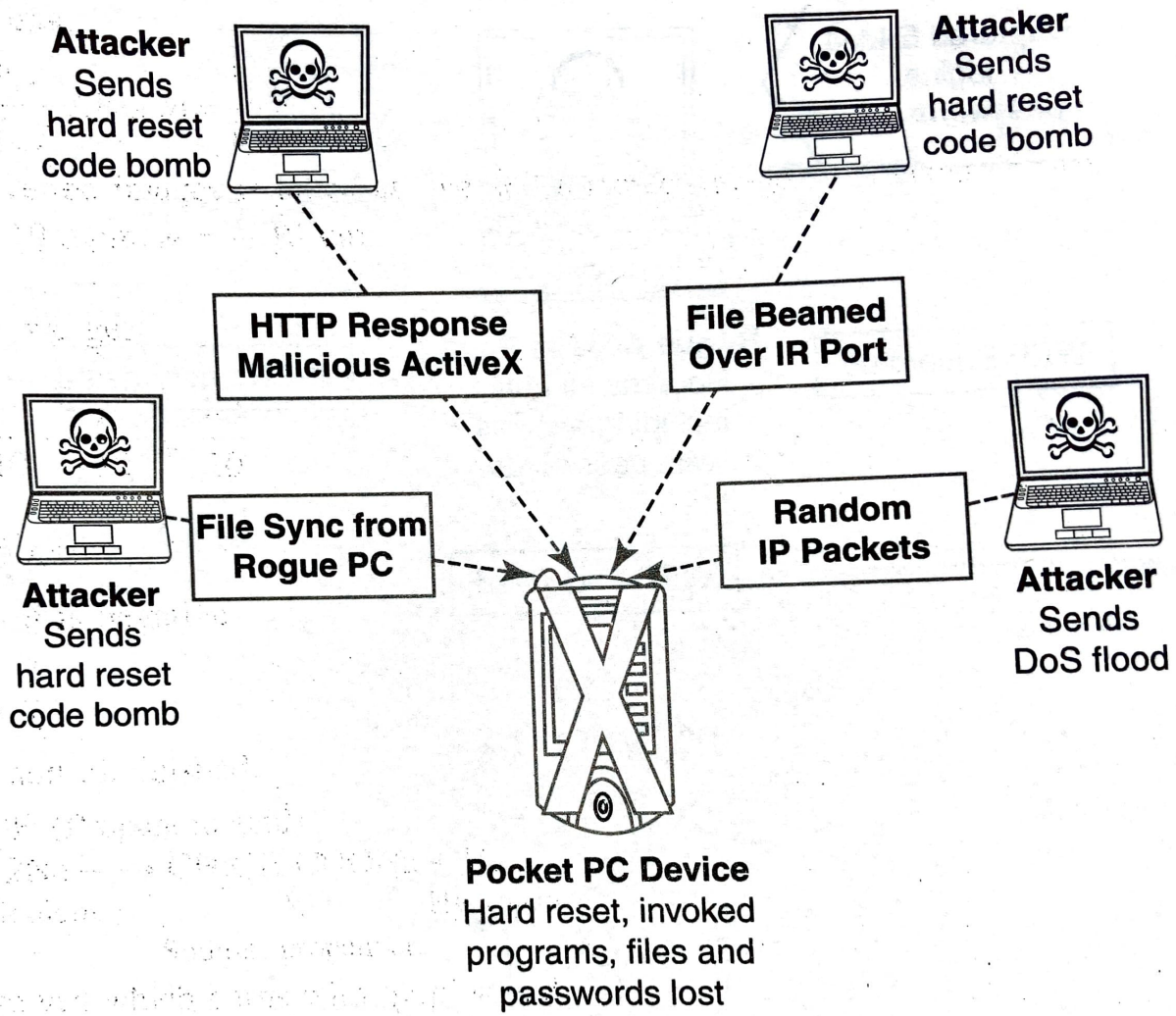


Attacks on Mobile/Cell Phones

- Mobile Phone Theft
- Mobile Viruses
- Mishing
- Vishing
- Smishing
- Hacking Bluetooth

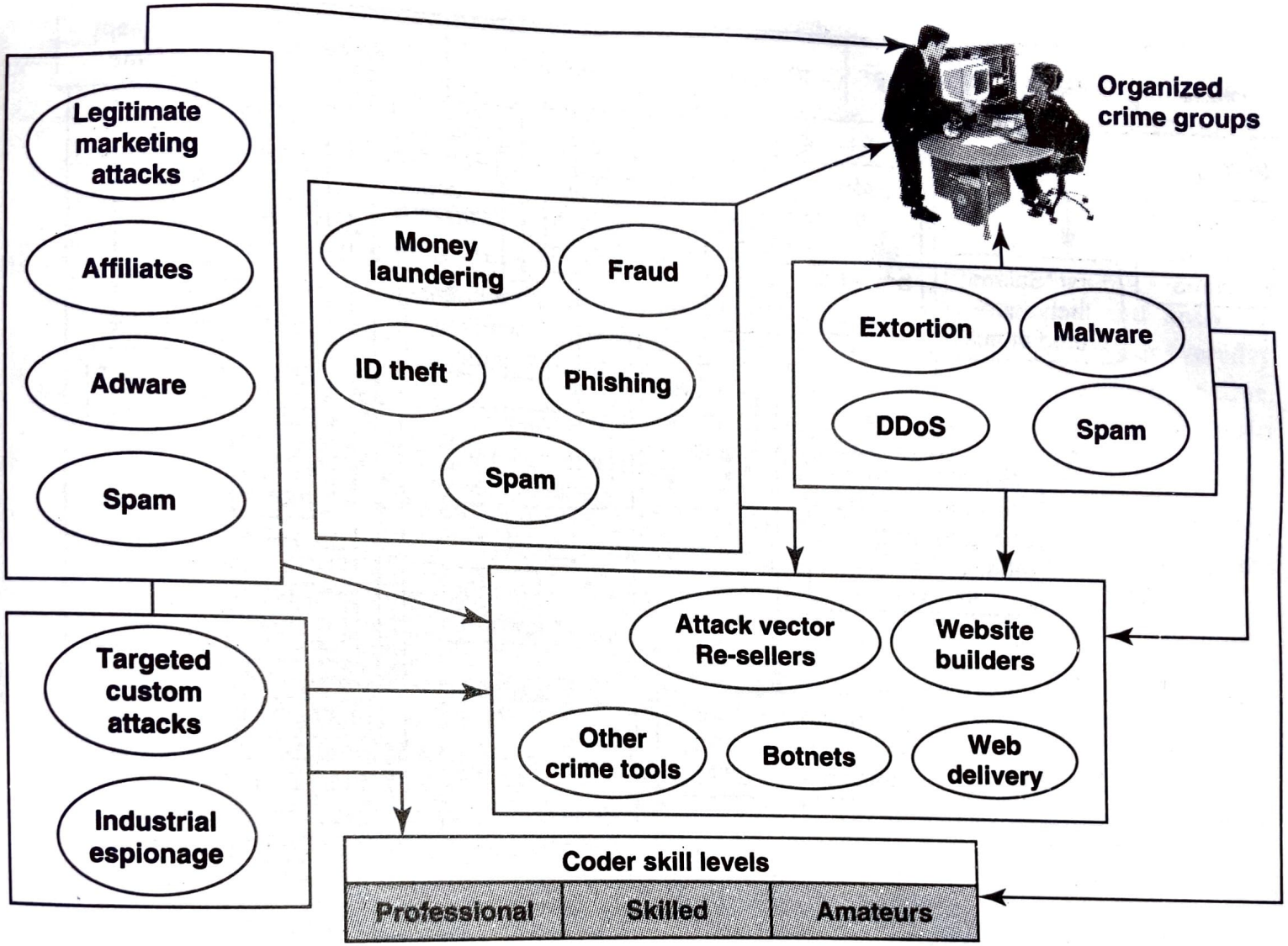

Attacker
Launches blended attack over
rogue ad hoc network
(802.11, bluetooth, infrared)
Worm / Zombie
Pocket PC Device
Reads E-Mail
zombie installed
worm progogates
Worm / Zombie
Worm / Zombie
DDos Zombies flood
Enterprises server
Worm / Zombie
Contact list
of victim
Desktop PC
Worm / Zombie
Worm / Zombie


Captured E-Mail, logins, passwords, etc.
WEP Encrypted
Rogue Access Point
Records all traffic including packets with passwords
WEP Encrypted
WEP Encrypted
WEP Encrypted
Pocket PC Device
Containing credentials, user data, and enterprise data
Legitimate Access Point
Unaware of these attacks
Captured files, E-Mail, passwords, etc.
Rogue Peer
Scans for open ports, copies files from pocket PC device


Attacker
Sends
hard reset
code bomb
Attacker
Sends
hard reset
code bomb
HTTP Response
Malicious ActiveX
File Beamed
Over IR Port
Attacker
Sends
hard reset
code bomb
File Sync from
Rogue PC
Random
IP Packets
Attacker
Sends
DoS flood
Pocket PC Device
Hard reset, invoked
programs, files and
passwords lost

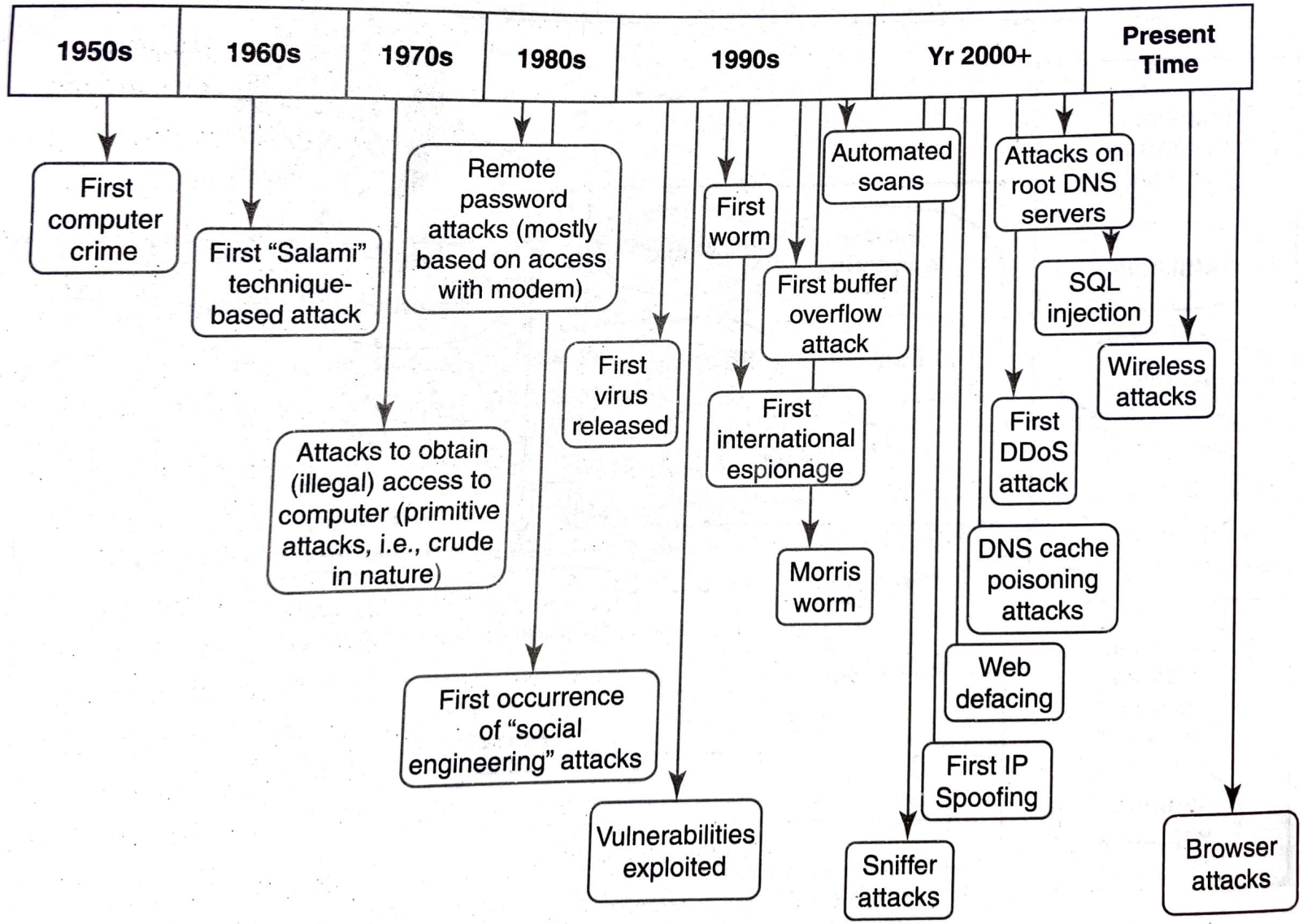
Security Implication for organizations

- Security Breach
- Personal Information
- Insider Threat
- Three type of Insider
  - Malicious Insider
  - Careless Insider
  - Tricked Insider
- Example Heartland Payment System
- Example BlueCross BlueShield
- Physical Security is very Important
- Insider threats can not be ignored


Organized crime groups
Legitimate marketing attacks
Affiliates
Adware
Spam
Money laundering
Fraud
ID theft
Phishing
Spam
Extortion
Malware
DDoS
Spam
Attack vector Re-sellers
Website builders
Other crime tools
Botnets
Web delivery
Targeted custom attacks
Industrial espionage
Coder skill levels
Professional
Skilled
Amateurs

Privacy has the four key dimension:

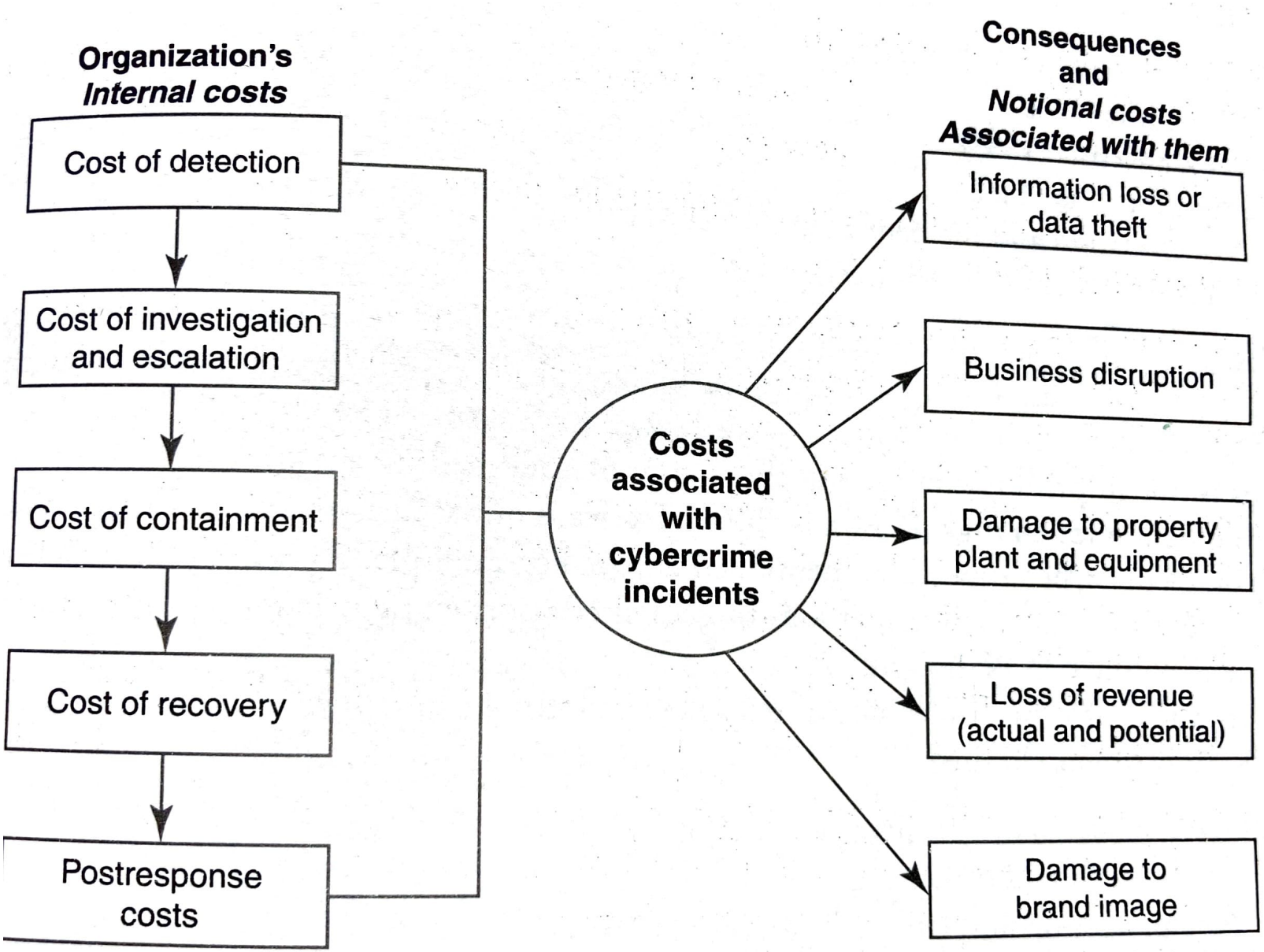
- Informational/data privacy
- Personal privacy
- Communication privacy
- Territorial privacy


1950s
1960s
1970s
1980s
1990s
Yr 2000+
Present Time
First computer crime
First "Salami" technique-based attack
Attacks to obtain (illegal) access to computer (primitive attacks, i.e., crude in nature)
Remote password attacks (mostly based on access with modem)
First occurrence of "social engineering" attacks
First virus released
Vulnerabilities exploited
First worm
First buffer overflow attack
First international espionage
Morris worm
Automated scans
Sniffer attacks
Attacks on root DNS servers
SQL injection
First DDoS attack
DNS cache poisoning attacks
Web defacing
First IP Spoofing
Wireless attacks
Browser attacks

The key challenges from emerging new information threats:

- Industrial espionage
- IP based blocking
- IP based cloaking
- Cyber Terrorism
- Confidential information leakage

Cost of Cybercrimes and IPR issues



Lesson to learn

- Endpoint protection
- Secure coding
- HR checks
- Access controls
- Importance of the security governance

Laptops Security

- Physical security
  - Cables and hard-wired locks
  - Laptop Safes
  - Motion sensors and alarms
  - Warning labels and stamps
  - Other measures
- Logical security
  - Protecting from malicious programs/attackers/ social engineering
  - Avoiding weak passwords/ open access
  - Monitoring application security and scanning vulnerabilities
  - Ensuring that unencrypted data/ unprotected file system do not pose threats
  - Proper handing of removable drives/ storage mediums/ unnecessary ports

- Password protection through appropriate passwords rules and use of strong passwords
- Locking down unwanted ports and devices
- Regularly installing security patches and updates
- Installing antivirus software/firewals/intrusion detection system
- Encrypting critical file systems
- Other countermeasures

Basic Principles of Information Security

- Confidentiality
- Integrity
- Availability
- Additional Concepts
  - Donn B. Parker proposed a set of six elements, known as the Parkerian Hexad, or the six atomic elements of information, which includes *Control (or Physical Possession), Authenticity, and Utility*.
  - Other principles that have been proposed include *Accountability, Non-Repudiation, and Legality*.
  - The U.S. Department of Defence defined "Five Pillars of Information Assurance," which include *Authenticity and Non-Repudiation* along with the *CIA triad*.

- The Organization for Economic Co-operation and Development (OECD) published guidelines that added *Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment*.
- U.S. National Institute of Standards and Technology Special Publication 800-27, Revision A, proposes a total of 33 principles for securing technology systems.
- There are many ways to categorize security principles, and the CIA triad is the most simplistic of them all.

- The best-known attributes of security defined in the preceding models and others like them include :
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
  - Accuracy
  - Authenticity
  - Awareness

- Completeness
- Consistency
- Control
- Democracy
- Ethics
- Legality
- Non-repudiation
- Ownership
- Physical Possession
- Reassessment
- Relevance
- Response
- Responsibility
- Risk Assessment
- Security Design and Implementation
- Security Management
- Timeliness
- Utility

Tutorial 3

1. What kind of attacks are possible on mobile/cell phones? Explain with example.
2. Explain the countermeasures to be practised for possible attacks on mobile/cell phones.
3. What kind of cyber security measures an organization should have to take in case of portable storage devices? Prepare security guidelines which can be implemented in an organization.
4. Explain the various measures for protection of laptops through physical and logical control measures.
5. What is security breach? Explain the impact it has on an organization.

6. What are Personal Information (PI) and Sensitive Personal Information (SPI)? Explain with appropriate examples.
7. What is meant by "insider threat"? How does it affects an organization?
8. Are information security and cyber security two independent domains? Explain your answer with example to support your rationale.
9. What are four dimensions of privacy? Do they all relate to data security? Justify your answer with suitable example.
10. What are some key challenges to organization discussed in the last classes?

Information Classification

Information must be classified according to its intended audience and be handled accordingly. Every piece of information must be classified into one of the following categories:

- **Personal**: Information not owned by the organization, belonging to private individuals
- **Public**: Information intended for distribution to and viewing by the general public
- **Confidential**: Information for use by employees, contractors, and business partners only
- **Proprietary**: Intellectual property of the organization to be handled only by authorized parties
- **Secret**: Information for use only by designated individuals with a need to know

Roles

- Information Authority Roles and Responsibilities
  - Ensure that does not put information at risk
  - Assign classification standard values to information
  - Implement Information Handling Standards
  - Information Classification and Handling Standard
  - Implement an information retention schedule following the Information Retention and Disposition Standard
  - Submit the Information Security Risk Inventory and Self-Assessment Report to the Information Security Officer (ISO) yearly
  - Work with the ISO, information custodian/steward, and other authorized individuals
  - Perform information security duties as required by other standards and practices, policies, executive orders, memoranda, etc.
  - Establish written procedures granting and revoking access privileges

- Ensure that those with access to the information understand their responsibilities for collecting, using, retaining, and disposing of the information only in appropriate ways.
- Monitor usage of the information.

- Information Custodian / Steward Roles and Responsibilities
  - Access and protection of information and the file systems are in compliance with all applicable information security policies and the authorized directives of the information authority.
  - Ensure that any electronic systems have all appropriate security features installed.
  - Work with the ISO, information authority, and other authorized individuals on the investigation and mitigation of information security incidents/breaches affecting the integrity and confidentiality of the information.
  - Perform information security duties as required by organization standards and practices, policies, executive orders, and memoranda.

- Review access request to and use of information stored in the data warehouse, determine appropriate access, and authorize or deny the request under their authority.

- Information User Roles and Responsibilities
  - Don't put your information at risk
  - Perform information security duties as required by standards and practices, policies, executive orders, memoranda, etc., as appropriate.

Privacy of Data

- Data privacy or information privacy is a branch of data security concerned with the proper handling of data

Concepts in Internet and World Wide Web

- What is Internet?
- How is it works?
- What is world wide web?
- What is the Protocol in general?
  - Protocols are the set of rules that are followed in some particular interaction.
- What are the Network Protocols?
  - Network protocols are the set of rules followed in networked communication systems
- What is the Security Protocols?
  - Security protocols are the communication rules followed in security applications

- What is the Authentication Protocols?
  - Authentication Protocols are the set of communication rules followed in security applications over a network to authenticate humans to a machines or the security of the message to authenticate the humans
- MAC Addresses, IP Addresses, and ARP
  - 48 bits, 32 bits/128 bits
- TCP/IP and OSI Model
- Ports and TCP/IP

IPv4/IPv6

<table>
<tr><th>Layer No</th><th>TCP/IP Model</th><th>OSI Model</th><th>Layer No</th></tr>
<tr><td rowspan="3">5</td><td rowspan="3">Application data</td><td>Application layer</td><td>7</td></tr>
<tr><td>Presentation layer</td><td>6</td></tr>
<tr><td>Session layer</td><td>5</td></tr>
<tr><td>4</td><td>TCP</td><td>Transport layer</td><td>4</td></tr>
<tr><td>3</td><td>IP</td><td>Network layer</td><td>3</td></tr>
<tr><td rowspan="3">2</td><td rowspan="3">Media Access Control</td><td>Data-link layer:</td><td rowspan="3">2</td></tr>
<tr><td>Media Access Control</td></tr>
<tr><td>Logical Link Control</td></tr>
<tr><td>1</td><td>Physical layer</td><td>Physical layer</td><td>1</td></tr>
</table>

Tutorial 4

1. What is Information Classification? How can you classify information?
2. What is the role and responsibilities of Information custodian?
3. If your were a owner of an organization, what actions you were taken to secure information of your user?
4. Supreme Court of India limited use of Aadhaar in some scheme of Indian government and in some scheme the court permitted. Why? Explain your view.
5. What is MAC address and IP address?
6. Explain ARP poisoning with example.
7. What do you mean by Protocols? Give example of some day to day life protocols and some example of security and authentication network protocols.

8. What is the role of ports in Internet? List some port number with their services.
9. Explain protocols and applications of the layers of network models.
10. What is the difference between TCP and UDP protocols? On which layer of OSI model they work?

Functions of various networking components

- Hub
- Switches
- Bridges
- Routers
- Gateway

Hub

- Hubs were dumb devices used to solve the most basic connectivity issue: how to connect more than two devices together.
- They transmitted packets between devices connected to them
- They retransmit each and every packet received on one port out through all of its other ports without storing or remembering any information about the hosts connected to them.
- This created scalability problems for legacy half-duplex Ethernet networks
- As the number of connected devices and volume of network communications increased, collisions became more frequent, degrading performance.

- A collision occurs when two devices transmit a packet onto the network at almost the exact same moment, causing them to overlap and thus destroying them.
- When this happens, each device must detect the collision and then retransmit their packet
- As more devices are attached to the same hub, and more hubs are interconnected, the chance that two nodes transmit at the same time increases, and collisions became more frequent.
- In addition, as the size of the network increases, the distance and time a packet is in transit over the network also increases, making collisions even more likely.
- So it is necessary to keep the size of such networks very small to achieve acceptable levels of performance.
- For this reason, hubs are rarely used in enterprise network environments.

Switches

- Switches were developed to overcome the performance shortcomings of hubs.
- It operate at layer two of the OSI model
- Switches are more intelligent devices that learn the various MAC addresses of connected devices and transmit packets only to the devices they are addressed to
- Since each packet is not rebroadcast to every connected device, the likelihood that two packets will collide is significantly reduced.
- In addition, switches provide a security benefit by reducing the ability to monitor or "sniff" another workstation's traffic.
- With a hub, every workstation would see all traffic on that hub; with a switch, every workstation sees only its own traffic.

- A switched network cannot absolutely eliminate the ability to sniff traffic.
- An attacker can trick a local network segment into sending it another device's traffic with an attack known as ARP poisoning.
- ARP poisoning works by fake replies to ARP broadcasts.
- For example, suppose malicious workstation Attacker wishes to monitor the traffic of workstation Victim, another host on the local switched network segment.
- To accomplish this, Attacker would broadcast an ARP packet onto the network containing Victim's IP address but Attacker's MAC address.
- Any workstation that receives this broadcast would update its ARP tables and thereafter would send all of Victim's traffic to Attacker.

- This ARP packet is commonly called a complimentary ARP and is used to announce a new workstation attaching to the network.
- To avoid alerting Victim that something is wrong, Attacker would immediately forward any packets received for Victim to Victim.
- Otherwise Victim would soon wonder why network communications weren't working.
- The most severe form of this attack is where the Victim is the local router interface.
- In this situation, Attacker would receive and monitor all traffic entering and leaving the local segment
- To reduce a network's exposure to ARP poisoning attacks, segregate sensitive hosts between layer three devices or use virtual LAN (VLAN) functionality on switches.

- For highly sensitive hosts, administrators may wish to statically define important MAC entries, such as the default gateway.
- Statically defined MAC entries will take precedence over MAC entries that are learned via ARP.
- Statically defining ARP entries carries a high administrative burden and does not scale well, but can protect small networks that require high security.

Routers

Bridges

- A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments.
- Bridges is different from router.
- Router allows multiple networks to communicate independently and yet remain separate
- Bridges connects two separate networks as if they were a single network
- In the OSI model, bridges work on data link layer
- Bridges are also used to interconnect two LANs that are operating two different networking protocols.
- For example, LAN A could be an Ethernet LAN and LAN B could be a token ring.

Gateways

- The basic difference between gateways and router is that gateways communicate using more than one protocol to connect a bunch of networks.
- They can operate at any of the seven layers of the OSI model
- The term gateway can also loosely refer to a computer or computer program configured to perform the tasks of a gateway, such as a default gateway or router
- A network gateway provides interoperability between networks and contains devices, such as protocol translators, impedance matchers, rate converters, fault isolators, or signal translators.
- A network gateway requires the establishment of mutually acceptable administrative procedures between the networks using the gateway

Modulation Techniques

- Modulation is the process of changing one or more properties of a called the carrier signal that is periodic waveform, with a modulating signal that typically contains information to be transmitted
- The main work of modulation is to convert data into electrical signals optimized for transmission.
- Amplitude Modulation (AM) and Frequency Modulation (FM) are the very famous modulation techniques used for transmitting the signals in radio broadcasting.
- Modulation techniques are roughly divided into four types:
  - Analog modulation
  - Digital modulation
  - Pulse modulation
  - Spread spectrum method

Need for security

- Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
- Information can take many forms, such as electronic and physical.
- For many organisations, information is their most important asset, so protecting it is crucial.
- Information security performs four important roles:
  - Protects the organisation's ability to function.
  - Enables the safe operation of applications implemented on the organisation's IT systems.
  - Protects the data the organisation collects and uses.
  - Safeguards the technology the organisation uses.
- The basics of information security could be explained by 5W of information security.

- What is Information Security?
- Why do you need Information Security?
- Who is responsible for Information Security?
- When is the right time to address Information Security?
- Where does Information Security apply?

- As we know information security is all about protecting the confidentiality, integrity and availability of information.
- To answer why we need security, answer the following questions:
  - Do you have information that needs to be kept confidential (secret)?
  - Do you have information that needs to be accurate?
  - Do you have information that must be available when you need it?
- If you answered yes to any of these questions, then you have a need for information security.

- We need information security to reduce the risk of unauthorized information disclosure, modification, and destruction.
- We need information security to reduce risk to a level that is acceptable to the business (management).
- We need information security to improve the way we do business.

Legal, Ethical and Professional Issues in Information Security

- The fixed moral attitudes or customs of a particular group are known as cultural mores
- Ethics are socially acceptable behaviours.
- Laws are rules that mandate or prohibit certain behaviour in society
- Ethics are based on cultural mores
- Laws are inherited or drawn from ethics
- The members of a society create rules to balance the individual rights to self-determination against the needs of the society as a whole are called laws.
- The key difference between laws and ethics is that laws carry the authority of a governing body, and ethics do not.

- Some ethical standards are universal.
- For example, murder, theft, assault, and set to fire or are actions that deviate from ethical and legal codes throughout the world.

Types of Law

- Civil law
- Criminal law
- Tort law
- Private law
- Public Law
- Other Indian law
  - RTI
  - RTE
  - Common civil code
  - Consumer right protection law
  - Religious law

Different types of laws

- Indian Information Technology Act 2000.
- Block the access of Online Child Sexual Abuse Materials(CSAM)
- Indian Penal Code 1860
- Code of Criminal Procedure 1973 (CrPC)
- Indian Evidence Act, 1872
- Computer Fraud and Abuse Act of 1986 (CFA Act)
- National Information Infrastructure Protection Act of 1996
- USA Patriot Act of 2001
- Telecommunications Deregulation and Competition Act of 1996
- Communications Decency Act of 1996 (CDA)
- Computer Security Act of 1987

Tutorial 5

1. What are the different networking devices?
2. On which layer of OSI model, the above networking devices operate?
3. What is the role of router in Information Security?
4. What are the differences between Switch and Bridge?
5. What are the differences between Router and Gateways?
6. Why do we need Information Security?
7. Define Cultural mores, Ethics and Laws. Explain with some real life example.
8. What is the difference between Ethics and Laws. Give some example of ethics which is not laws and some example of ethics which is not acceptable as per laws.

9. What are the different laws for Information Security?
10. Give some example of ethical difference between different cultures.

Laws of Interest to Information Security Professionals

- Privacy
  - The issue of privacy has become one of the hottest topics in information
  - Privacy is a "state of being free from unsanctioned intrusion"
  - The ability to collect information on an individual, combine facts from separate sources, and merge it with other information has resulted in databases of information that were previously impossible to set up
  - The aggregation of data from multiple sources permits unethical organizations to build databases of facts with frightening capabilities
- Privacy of Customer Information
  - Privacy of Customer Information Section of Common Carrier Regulations
  - Federal Privacy Act of 1974
  - The Electronic Communications Privacy Act of 1986

- The Health Insurance Portability & Accountability Act Of 1996 (HIPAA) also known as the Kennedy-Kassebaum Act
- The Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999

+ Export and Espionage Laws
  - Economic Espionage Act (EEA) of 1996
  - Security and Freedom Through Encryption Act of 1997 (SAFE)
+ Copyright Law
  - Intellectual property is recognized as a protected asset
  - US copyright law extends this right to the published word, including electronic formats
  - Fair use of copyrighted materials includes
    * Use to support news reporting, teaching, scholarship, and a number of other related permissions
    * The purpose of the use has to be for educational or library purposes, not for profit, and should not be excessive
  - With proper acknowledgement, permissible to include portions of others work as reference
+ Freedom of Information Act of 1966 (FOIA)

- The Freedom of Information Act provides any person with the right to request access to federal agency records or information, not determined to be of national security
- US Government agencies are required to disclose any requested information on receipt of a written request
- There are exceptions for information that is protected from disclosure, and the Act does not apply to state or local government agencies or to private businesses or individuals, although many states have their own version of the FOIA
- In addition to the national and international restrictions placed on an organization in the use of computer technology, each state or locality may have a number of laws and regulations that impact operations
- It is the responsibility of the information security professional to understand state laws and regulations and insure the organization's security policies and procedures comply with those laws and regulations

International Laws and Legal Bodies

- European Council Cyber-Crime Convention;
  - To create an international task force to oversee a range of security functions associated with Internet activities,
  - To standardize technology laws across international borders
  - It also attempts to improve the effectiveness of international investigations into breaches of technology law
  - This convention is well received by advocates of intellectual property rights with its emphasis on copyright infringement prosecution
- Digital Millennium Copyright Act (DMCA)
  - The Digital Millennium Copyright Act (DMCA) is the US version of an international effort to reduce the impact of copyright, trademark, and privacy infringement
  - The European Union Directive 95/46/EC increases protection of individuals with regard to the processing of personal data and limits the free movement of such data

    * The United Kingdom has already implemented a version of this directive called the Database Right

- United Nations Charter
    * To some degree the United Nations Charter provides provisions for information security during Information Warfare
    * Information Warfare (IW) involves the use of information technology to conduct offensive operations as part of an organized and lawful military operation by a sovereign state
    * IW is a relatively new application of warfare, although the military has been conducting electronic warfare and counter-warfare operations for decades, jamming, intercepting, and spoofing enemy communications

Policy Versus Law

- Most organizations develop and formalize a body of expectations called policy
- Policies function in an organization like laws
- For a policy to become enforceable, it must be:
  * Distributed to all individuals who are expected to comply with it
  * Readily available for employee reference
  * Easily understood with multi-language translations and translations for visually impaired, or literacy-impaired employees
  * Acknowledged by the employee, usually by means of a signed consent form
- Only when all conditions are met, does the organization have a reasonable expectation of effective policy

Ethical Concepts in Information Security

- Cultural Differences in Ethical Concepts
  - Differences in cultures cause problems in determining what is ethical and what is not ethical
  - Studies of ethical sensitivity to computer use reveal different nationalities have different perspectives
  - Difficulties arise when one nationality's ethical behaviour contradicts that of another national group
- Ethics and Education
  - Employees must be trained and kept aware of a number of topics related to information security, not the least of which is the expected behaviours of an ethical employee
  - This is especially important in areas of information security, as many employees may not have the formal technical training to understand that their behaviour is unethical or even illegal
  - Proper ethical and legal training is vital to creating an informed, well prepared, and low-risk system user

- Deterrence to Unethical and Illegal Behaviour
  * Deterrence - preventing an illegal or unethical activity
  * Laws, policies, and technical controls are all examples of deterrents
  * Laws and policies only deter if three conditions are present:
    - Fear of penalty
    - Probability of being caught
    - Probability of penalty being administered

Codes of Ethics and Professional Organizations

- A number of professional organizations have established codes of conduct or codes of ethics that members are expected to follow.
- Codes of ethics can have a positive effect on people's judgement regarding computer use.
- Unfortunately, many employers do not encourage their employees to join these professional organizations.
- Employees who have earned some level of certification or professional accreditation can be deterred from ethical lapses by the threat of loss of accreditation or certification due to a violation of a code of conduct.
- Loss of certification or accreditation can dramatically reduce marketability and earning power.

- It is the responsibility of security professionals to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society.
- It is likewise the organization's responsibility to develop, disseminate, and enforce its policies.
- Ten Computer Ethics from the Computer Ethics Institute
  1. We should not use a computer to harm other people.
  2. We should not interfere with other people's computer work.
  3. We should not snoop around in other people's computer files.
  4. We should not use a computer to steal.
  5. We should not use a computer to bear false witness.
  6. We should not copy or use proprietary software for which we have not paid.
  7. We should not use other people's computer resources without authorization or proper compensation.
  8. We should not appropriate other people's intellectual output.

9. We should think about the social consequences of the program we are writing or the system we are designing.
10. We should always use a computer in ways that ensure consideration and respect for our fellow humans.

Risk Management

- Risk management is the process of identifying risk, assessing its relative magnitude, and taking steps to reduce it to an acceptable level. It involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of an organization's assets.
- Risk Identification: The recognition, enumeration, and documentation of risks to an organization's information assets.
  - Identify, Inventory, & Categorize Assets
  - Classify, Value, & Prioritize Assets
  - Identify & Prioritize Threats
  - Specify Asset Vulnerabilities
- Risk Assessment: A determination of the extent to which an organization's information assets are exposed to risk
  - Determine Loss Frequency (Likelihood)

- Evaluate Loss Magnitude (Impact)
- Calculate Risk
- Assess Risk Acceptability

- Risk Control: The application of controls that reduce the risks to an organization's information assets to an acceptable level
  - Select Control Strategies
  - Justify Controls
  - Implement, Monitor, & Assess Controls

Security Threats to E-Commerce

1. Financial frauds
   - Credit Card Fraud
   - Fake Return & Refund Fraud
2. Phishing
3. Spamming
4. DOS & DDoS Attacks
5. Malware
6. SQL Injection
7. Cross-Site Scripting (XSS)
8. Bots
9. Brute force
10. Man in The Middle
11. e-Skimming

How to protect from the E-Commerce Threats

- HTTPS and SSL certificates
- Anti-malware and Anti-virus software
- Secure Your Servers and Admin Panels
- Secure Payment Gateway
- Deploying Firewall
- Educating Your Staff and Clients
- Employ Multi-Layer Security
- E-Commerce Security Plug-ins
- Backup Your Data
- Stay Updated
- Keep an eye on Malicious Activity

Virtual Organization

- A virtual organization is a group of people from different organizations who form a virtual company, either in leased facilities or through 100-percent telecommuting arrangements.
- When the job is done, the organization is either redirected or dissolved.
- These organizations rely almost exclusively on remote computing and telecommuting, but they are rare and therefore are not well documented or studied

Business Transactions on Web

- Banking
- Online Shopping
- Insurance
- Online Marketing / Advertisement
- Online Tour and Travelling
- Online Bill payments

E Governance

- Government to Citizen (G2C)
- Government to Employees (G2E)
- Government to Business (G2B)
- Government to Government (G2G)

Electronic Data Interchange (EDI)

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.
In EDI, paper documents are replaced with electronic documents such as pdf, word documents, spreadsheets, etc

- EDI Documents
  - Invoices
  - Purchase orders
  - Shipping Requests
  - Acknowledgement
  - Business Correspondence letters
  - Financial information letters
- How it works?
- Pros and Cons

Concepts in Electronics payment systems

- An e-payment system is a way of making transactions or paying for goods and services through an electronic medium, without the use of cheques or cash.
- It is also called an electronic payment system or online payment system

* E Cash / Digital Cash
* Virtual Credit/Debit Card
* Wallet /E-Money
* Electronic Fund Transfer (EFT)
* Credit Card
* Debit Card
* Prepaid / Cash Card
* Smart Card

Digital Forensics

- Involve the preservation, identification, extraction, documentation, and interpretation of computer media for evidential and root cause analysis.
- **Digital Malfeasance:** A crime against or using digital media, computer technology, or related components; in other words, a computer is the source of the crime or the object of it
- **Evidential Material (EM):** Also known as "items of potential evidential value," any information that could potentially support an organization's legal or policy-based case against a suspect

- **Forensics:** The coherent application of methodical investigatory techniques to present evidence of crimes in a court or similar setting. Forensics allows investigators to determine what happened by examining the results of an event - criminal, natural, intentional, or accidental.

Digital forensics can be used for two key purposes:

1. **To investigate allegations of digital malfeasance.** Such an investigation requires digital forensics to gather, analyse, and report the findings. This is the primary mission of law enforcement in investigating crimes that involve computer technologies or on-line information

2. **To perform root-cause analysis.**
   If an incident occurs and the organization suspects an attack was successful, digital forensics can be used to examine the path and methodology used to gain unauthorized access, and to determine how pervasive and successful the attack was. This type of analysis is used primarily by incident response teams to examine their equipment after an incident.

The organization must choose one of two approaches when employing digital forensics:

1. **Protect and forget**
   This approach, also known as patch and proceed, focuses on the defence of data and the systems that house, use, and transmit it. An investigation that takes this approach focuses on the detection and analysis of events to determine how they happened and to prevent reoccurrence. Once the current event is over, who caused it or why is almost immaterial.

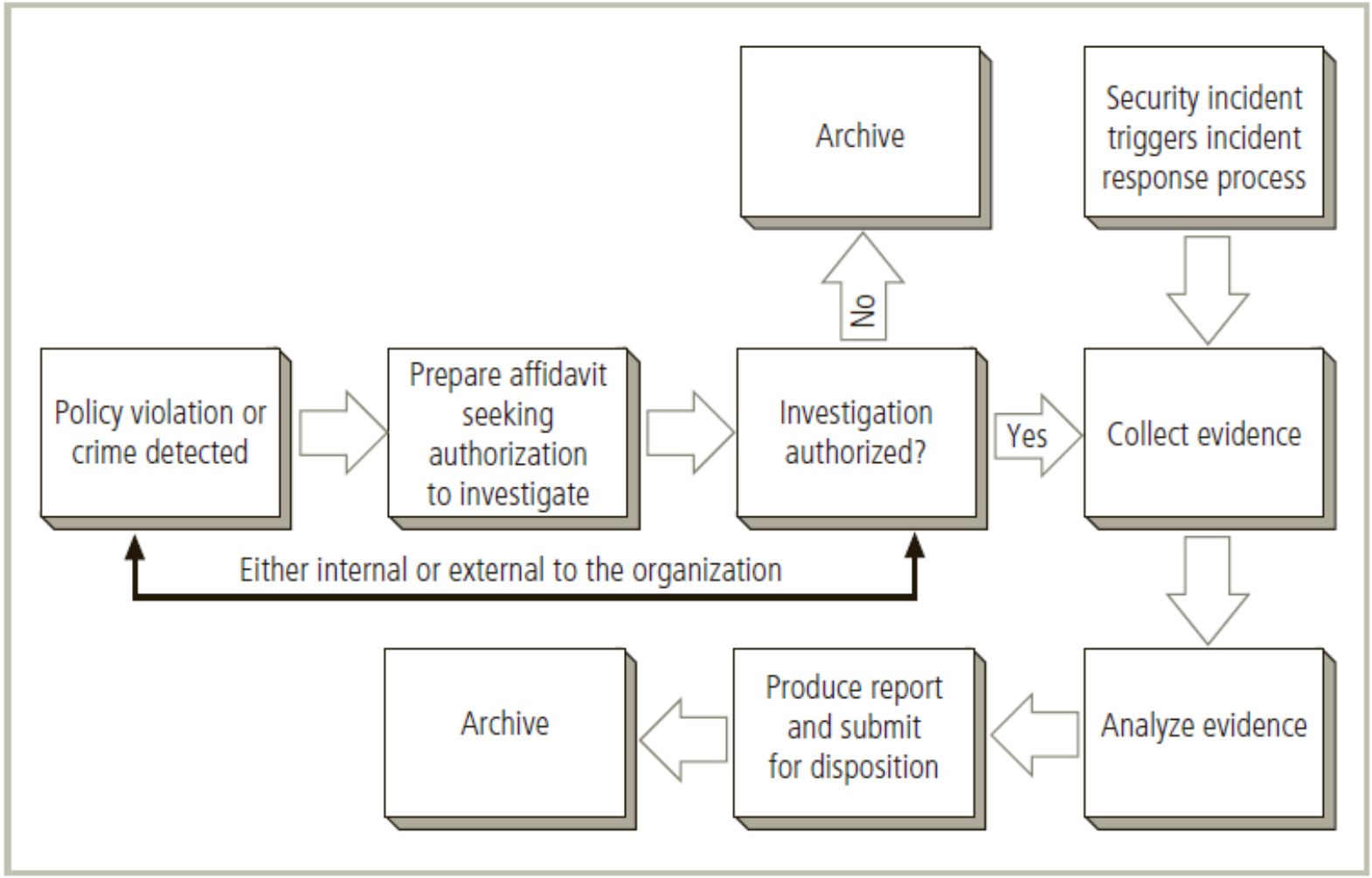
2. **Apprehend and prosecute**
   This approach, also known as pursue and prosecute, focuses on the identification and apprehension of responsible parties, with additional attention to the collection and preservation of potential EM that might support administrative or criminal prosecution. This approach requires much more attention to detail to prevent contamination of evidence that might hinder prosecution

An organization might find it impossible to retain enough data to successfully handle even administrative penalties, but it should certainly adopt the latter approach if it wants to pursue formal administrative penalties, especially if the employee is likely to challenge them.

Digital Evidence Handling

All investigations follow the same basic methodology

1. Identify relevant evidential material (EM)
2. Acquire (seize) the evidence without alteration or damage
3. Take steps to assure that the evidence is verifiable authentic at every step and is unchanged from the time it was seized
4. Analyse the data without risking modification or unauthorized access
5. Report the findings to the proper authority


Archive
Security incident triggers incident response process
No
Policy violation or crime detected
Prepare affidavit seeking authorization to investigate
Investigation authorized?
Yes
Collect evidence
Either internal or external to the organization
Archive
Produce report and submit for disposition
Analyze evidence

Type of Digital Forensics

- **Media forensics**
  Media Forensics is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from the digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.
- **Cyber/Computer forensics**
  Cyber forensics is the acquisition, preservation, and analysis of electronically stored information in such a way that ensures its admissibility for use as evidence, exhibits, or demonstratives in a court of law

- **Software forensics**
  Software forensics is a branch of science that investigates computer software text codes and binary codes in cases involving patent infringement or theft and can be used to support evidence for legal disputes over intellectual property, patents, and trademarks
- **Mobile forensics**
  Mobile forensics process aims to recover digital evidence or relevant data from a mobile device in a way that will preserve the evidence in a forensically sound condition.

Tutorial 6

1. List some International Laws and Legal Bodies for Information Security. Explain in brief.
2. What is the difference or relationship between Policy and Law?
3. How can you stop unethical and illegal Behaviour?
4. Explain some Codes of Ethics for any Professional Organizations.
5. What are the three steps of Risk Management? Explain in detail.
6. What are the Security Threats to E-Commerce?
7. How can you protect yourself from the E-Commerce Threats?
8. What are the different Business Transactions taking place on web?

9. What are the different electronic payment system are used now a days?
10. What do you mean by Digital Forensics? What are the different types of Digital Forensics?

Revision and Doubt Session

Any doubt?

Tutorial 7 (Mid Term Exam Solutions)

1. 1.1 Among the fundamental challenges in information security are confidentiality, integrity, and availability, or CIA. Define each of these terms. (5)

   1.2 What are the three steps of Risk Management? Explain in detail. (5)

2. 2.1 Malware is software that is intentionally malicious, in the sense that it is designed to do damage or break the security of a system. Malware comes in many familiar varieties, including viruses, worms, and Trojans.

   2.1.1 Has your computer ever been infected with malware? If so, what did the malware do and how did you get rid of the problem? If not, why have you been so lucky?

   2.1.2 In the past, most malware was designed to annoy users. Today, it is often claimed that most malware is written for profit. How could malware possibly be profitable?

(5)

2.2 Suppose that we have a computer that can test 2^{40} keys each second.

2.2.1 What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{88}?

2.2.2 What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{256}?

(5)

3. 3.1 What kind of attacks are possible on mobile/cell phones? Explain the countermeasures to be practised for possible attacks on mobile/cell phones. (5)

3.2 What are the different networking devices? On which layer of OSI model, these networking devices operate? (5)

4. 4.1 From a bank's perspective, which is usually more important, the integrity of its customer's data or the confidentiality of the data? From the perspective of the bank's customers, which is more important? (5)

4.2 Explain ARP poisoning with example. (5)

Physical Security

- Building and Campus Security
  - Room Access Based on Job Function
  - Physical Security for Laptops
  - Position of Computer Monitors
  - Badges on the Organization's Premises
  - Temporary Badges
  - Guards for Private Areas
  - Badge Checking
  - Tailgating
  - Employee Responsibility for Security
  - Security Policy Enforcement
- Data Center Security
  - Physical Security for Critical Systems
  - Security Zones
  - Non-Employee Access to Corporate Systems
  - Asset Tags

- Equipment Entrance Pass
- Equipment Exit Pass
- Access Authorization
- Access from Inside
- Employee Access Lifetime
- Inactive Access Badges
- New Access Requests
- Production Staff Access
- Access Monitoring
- Access via Secure Area
- Buddy System
- Three-Badge Access Requirement
- Biometric Authentication
- Room Access Based on Job Function

- Health and Safety
  - Search of Personal Property
  - Tailgating
  - Security Drills

Disaster and Controls

- Fire
- Flood
- Burglary
- Theft
- Vandalism
- Terrorism

Access Control-Biometrics

- Biometric systems include the use of facial recognition and identification, retinal scans, iris scans, fingerprints, hand geometry, voice recognition, lip movement, and keystroke analysis.
- Biometric devices are commonly used today to provide authentication for access to computer systems and buildings, and even to permit pulling a trigger on a gun.
- The algorithm for comparison may differ, but a body part is examined and a number of unique points are mapped for comparison with stored mappings in a database.
- If the mappings match, the individual is authenticated.
- The process depends on two things:
- first, that the body part examined can be said to be unique

- Second, that the system can be tuned to require enough information to establish a unique identity and not result in a false rejection, while not requiring so little information as to provide false positives.
- All of the biometrics currently in use have been established because they represent characteristics that are unique to individuals.
- The relative accuracy of each system is judged by the number of false rejections and false positives that it generates.

Tutorial 8

1. Why physical security of a system is important?
2. How can we insure physical security of information?

Factors in Biometrics Systems

- Does the individual user interact with the biometric system in a 'supervised' or an 'unsupervised' way?
- Is the user ID claimed before interacting with the biometric system?
- What are the requirements of the biometrics in terms of accuracy, enrolment and response time?
- What is the user motivation for complying with the biometric system?
- Is the cost of data/material that are protected through biometric systems worth the deployment cost?
- What are the other 'non-biometrics' technologies that compete with or complement the biometric technologies?

Benefits

- Traditionally, passwords and ID cards have been used to restrict access to secure systems but these methods can easily be breached and are unreliable.
- Biometrics cannot be borrowed, stolen or forgotten and forging one is practically impossible.
- Biometrics is an alternative to using passwords for authentication in logical or technical access control.
- Biometrics is based on the third type of authentication mechanism – something you are.
- As a quick recall noted that biometrics is defined as an automated means of identifying or authenticating the ID of a living person based on physiological or behavioral characteristics.

- In biometrics, identification is a 'one-to-many' search of an individual's characteristics from a database of stored images.
- Authentication in biometrics is a 'one-to-one' search to verify a claim to an ID made by a person.
- Biometrics is used for identification in physical controls and for authentication in logical controls.
- In the domain of physical security passwords and PINs are the most frequently used authentication techniques for controlling access.
- In higher security applications, hand-held tokens are used instead of passwords.
- However, passwords, PINs and tokens have a number of problems that raise questions about their suitability for modern security access control applications, particularly high security applications such as access to defence systems or medical data systems.

- Biometrics provides a number of benefits compared to the traditional methods:
  1. Increased level of security.
  2. Greater convenience.
  3. Higher level of accountability.
  4. Fraud detection and fraud deterrence.

Criteria for selection of biometrics

- Biometrics is a physical or biological feature or attribute that can be measured.
- It can be used as a means of proving that you are who you claim to be, or as a means of proving without revealing your ID that you have a certain right or a password.
- We also know that the crucial difference is that the biometrics is something that is part of you, rather than something you know or can carry with you.
- Examples of physiological biometric features include height, weight, body odor, the shape of the hand, the pattern of veins, retina or iris, the face and the patterns on the skin of thumbs or fingers (fingerprints).

- Examples of behavioral biometrics are voice patterns, signature and keystroke sequences and gait (the body movement while walking).
- While it is sometimes argued that DNA should not be classified as a biometrics because it is not externally observable, it is still considered a biometrics by most subject experts, in so far as it is a body feature that can be used for identification and verification purposes.
- Most biometric applications are based on certain biometric information.
- Although biometric features include various subsets of body characteristics, not all such subsets are suitable for identification purposes.

The evaluation whether a particular body characteristic is suitable for biometrics use can be done on the seven criteria, also known as the 'seven pillars'.

Characteristics	Meaning
Universality	All human beings have the same physical characteristics – such as fingers, iris, face and DNA – which can be used for identification. Thus, under this pillar of wisdom, every person should have the characteristic. People who are mute or without a fingerprint will need to be accommodated in some way.
Distinctiveness/ uniqueness	For humans, these characteristics are unique, and thus constitute a distinguishing feature. Generally, no two people have identical characteristics. However, identical twins are hard to distinguish.
Permanence/ persistence	These characteristics remain persistent, that is, largely unchanged throughout a person's life.

Availability/ collectability	A person's unique physical characteristics need to be collected in a reasonably easy fashion for quick identification.
Performance	The degree of accuracy of identification must be quite high before the system can be operational.
Acceptability	Applications will not be successful if the public offers strong and continuous resistance to biometrics. Thus, the general public must accept the sample collection routines. Non-intrusive methods are more acceptable.
Resistance to circumvention	To provide added security, a system needs to be harder to circumvent than existing ID management systems. In other words, the technology/technique used should be difficult to deceive.

Each of the various biometric techniques that exist has its own limitations.

Technique Name	Strength	Factors to consider for system implementation

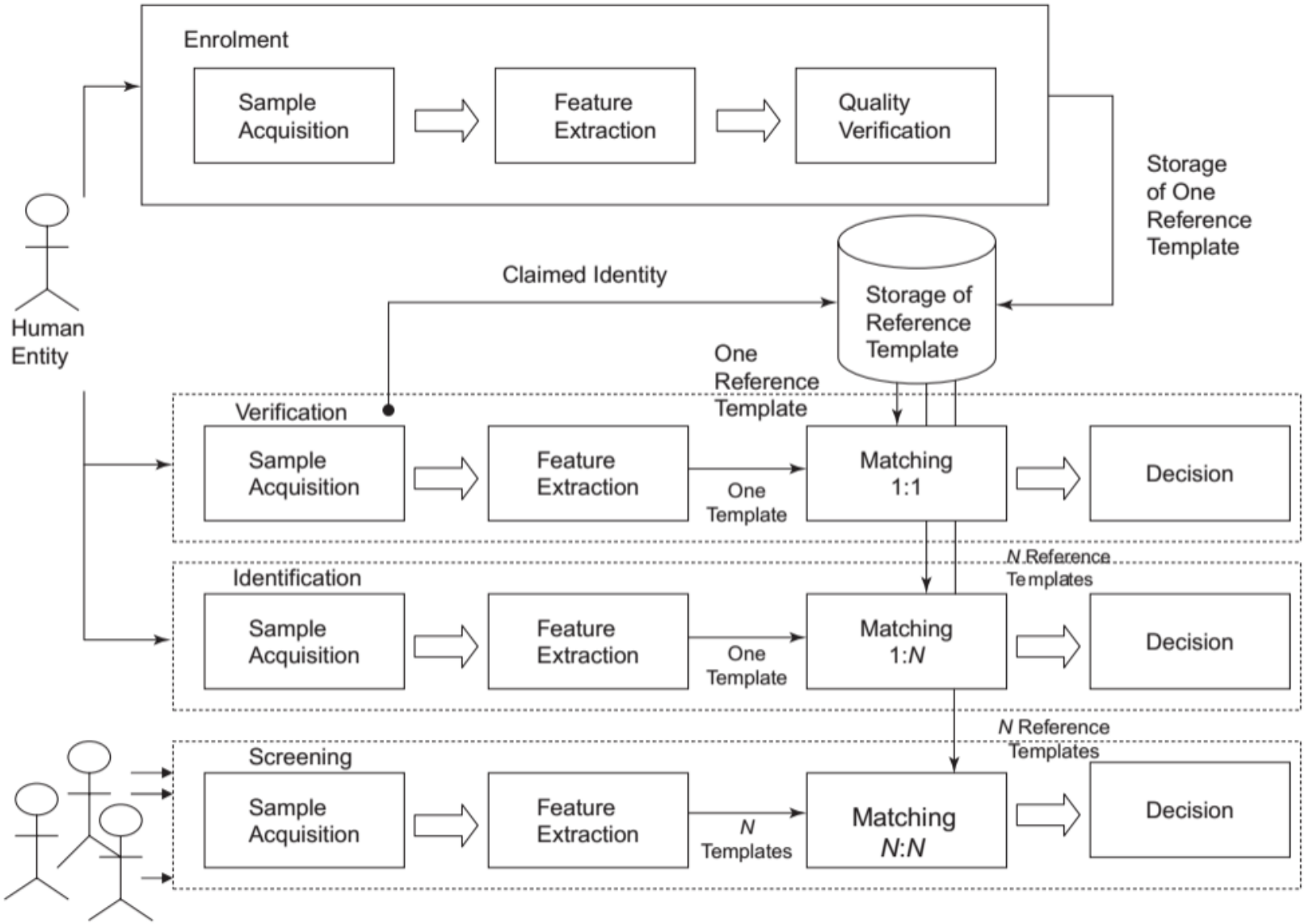
Fingerprint recognition	1. The technology/technique is used widely (not infested with social connotations) 2. Well proven technology/technique capable of providing high accuracy rate, that is, low false rejection rate 3. Multiple fingers can be enrolled thereby providing	1. Impact from perception of law enforcement agencies and forensic users 2. Impaired or damage fingers may fail to support minutiae extraction from the finger impression taken 3. May require additional software and hardware 4. May need

Design Issues in Biometric Systems

A generic biometric system goes through following six basic steps as depicted. The last two steps are used only during the recognition phase.

1. **Sample acquisition:** In this first step, the biometric data must be collected using an appropriate sensor, for example, an image capture in the case of iris recognition or a saliva sample in the case of DNA.
2. **Feature extraction:** This step performs the transformation from the sample into the template. In general, the template is numeric data. (This step can be omitted if full images are used.)
3. **Quality verification:** This step establishes a reference image or template by repeating the first two operations as many times as needed so as to ensure that the system has captured and recognized the data correctly.

4. **Storage of reference template:** This step registers the reference template. Several storage media are possible and the choice depends on the requirements of the application.
5. **Matching:** This step compares the real-time input data from an individual with the reference template(s) or image(s).
6. **Decision:** This step uses the result of the matching step to declare a result, in accordance with application-dependent criteria (e.g., decision threshold) – for example, for a verification task, the result would say whether the user claiming an ID should be authenticated.


Enrolment
Sample Acquisition
Feature Extraction
Quality Verification
Storage of One Reference Template
Claimed Identity
Storage of Reference Template
Human Entity
One Reference Template
Verification
Sample Acquisition
Feature Extraction
One Template
Matching 1:1
Decision
N Reference Templates
Identification
Sample Acquisition
Feature Extraction
One Template
Matching 1:N
Decision
N Reference Templates
Screening
Sample Acquisition
Feature Extraction
N Templates
Matching N:N
Decision

Design Issues in Biometric Systems

Biometric systems, by their very nature, are complex systems with responsive decision-making involved in terms of physical access controls. The two most critical issues that designers of biometric systems face are briefly explained below

- **Storage and protection of the template:**
  As shown in the above biometric systems have to scan, store/retrieve a template and match.
  It is important to note that depending on the design of the system, the match can be performed in different locations: on the processor that is used to acquire the biometric sample data, on a local PC or a remote server or on a portable medium such as a smart card equipped with a strong enough processor.
  In addition, the reference template may be stored on the same three media leaving us with five different combinations and resulting in five different levels of 'trust'.

Also, there can be three different modes of protection that may be used for the template: no protection, data encryption or digital signature.
This means that there can be 15 possible configurations.
Each use of combination has its own advantages and disadvantages;
The choice of the combination is clearly application dependent based on risk and requirements analysis.

- **Accuracy of biometric system steps:**
  The evaluation of a biometric system has to be based on the evaluation of all components: the recognition system performance, the communication interface, the matching and decision step and other key factors such as ease of use, acquisition speed and processing speed.
  The performance of a biometric system ultimately depends on the accuracy of the end decision only.

Biometric Measurement Issues

Measuring the accuracy of biometric systems is important.
Accuracy estimates depend very much on the quality of the test data that are used.
Poor quality data will degrade the accuracy estimates.
Biometric systems accuracy can be measured through three key metrics:

1. Failure to enroll (user cannot register in the system)
2. False match (impostor breaks in)
3. False non-match (a valid user locked out)

Interoperability Issues

- Exchange and extension of data
- Standards for information exchange
- Security and Misuse of data

Economic and Social Aspects

Economic implications of biometrics

- **Optimal ID concept:**
  The economic importance of ID is growing in a digital society, but the strongest ID protection is not necessarily the optimal one.
- **Demands for stronger identification create negative implications:**
  ID errors and abuse may become less frequent, but when they happen, they could potentially be more dangerous. For example, 'ID theft' may become less frequent but more severe and with wider social effect.

- **Interoperability is vital for market operation:**
  There is a serious danger that the biometric identification market and markets that depend on ID may fragment into clusters that will not interoperate, thus becoming vulnerable to monopolization or dominance by a few players.
- **Open competition threatened by biometric-related IPRs:**
  The unregulated exploitation of IPRs to aspects of biometrics can significantly reduce competition in biometrics and/or distort development, direction and speed of uptake.
- **Markets will be shaped by public-sector uptake:**
  The use of biometrics in electronic government (e-government) initiatives and associated large-scale public procurement could be key levers to ensure open and competitive markets, and rapid and socially productive innovation.

Social implications of biometrics:

- **Clarity of purpose:**
  'Function creep' is an important concern, that is, the technology and processes introduced for one purpose will be extended to other purposes that were not discussed or agreed upon at the time of their implementation. Thus, it is important to be clear about what the needs of the application are and how biometrics will be able to achieve them.
- **Interoperability and equivalence of performance and process:**
  This is not only a technical issue. Process equivalence (e.g., backup procedures that are the same everywhere) is extremely important as it impacts system performance, especially where biometrics are used in international situations (e.g., border control IS).

- **Human factors engineering, usability and social exclusion:**
  Human factors such as age, ethnicity, gender, diseases or disabilities (including natural ageing) ought to be studied on a case-by-case basis so as to minimize the possibility of social exclusion of a small but significant part of the population. Research on the usability and the user-friendliness of biometrics in real life is still in progress.
- **Element of trust:**
  People may temporarily accept to trade-in parts of their personal freedom in exchange for a more secure world. But when government control is perceived as excessive, disproportionate and/or 'too efficient', an erosion of trust can appear that will be in the interest of neither governments nor citizens.

Tutorial 9

1. Explain the role of access control, authentication and user identification in the context of security.
2. If a certain human physiological characteristic is to be used in biometrics, it has to satisfy certain criteria. Explain these criteria.
3. Explain how matching and enrolment processes work in biometrics and what purposes they serve together.
4. What are the key success factors for biometric systems to work? Illustrate with examples wherever possible.
5. Explain the basic steps involved in the process flow of any biometric systems.
6. What are the relative advantages and disadvantages of biometrics?

7. What are the criteria used while selecting a biometric characteristics to design a biometric system?
8. Present your understanding about the critical technical issues in a biometric system design.
9. Is the issue of data protection related with biometrics? Explain with suitable arguments.
10. Using the Internet resources, find out details of at least four finger recognition systems or devices and do comparative feature analysis.

Legal Challenges

- **Enabling legal environment:**
  The existing legal environment (privacy and data protection) is flexible in that it is an 'enabling' legislation legitimizing the de facto commercial use of personal data. Data protection rules regulate the use of biometrics but they lack normative content and ethical debate.
- **Opacity/transparency rules required:**
  Data protection (transparency rules) does not specify what the limits of use and abuse of biometrics are. Opacity (privacy) rules may prohibit use in cases where there is the need to guarantee against outside steering or disproportionate power balances.

- **Fundamental concerns arising with wider implications:**
  As biometrics is diffused in society, some concerns are gaining importance – concerns about power accumulation, further use of existing data, specific threats related to the use of biometrics by the public sector, and the failure to protect individuals from their inclination to trade their own privacy with what seems to be a very low-cost convenience.
- **Use of biometrics in law enforcement:**
  It is imperative that biometric evidence be regulated when presented as an evidence in courts of law so as to protect suspects adequately (e.g., being heard and right to counter-expertise).

Legal Framework for Information Security

Security Metrics

Information Security Vs Privacy

- When you think of security issues related to the Internet, images of malicious hackers and troublesome viruses are often the first things to come to mind.
- Privacy is a security issue, as well.
- However, the two are not identical.
- Privacy is a security issue, but security issues are not necessarily privacy issues.
- Privacy is regarded as a fundamental right for humans.
- At first glance, you might think they are the same issue, but they are not.
- Privacy is a subset of security.
- If your privacy is compromised, then certainly your security has been compromised, but it does not necessarily work both ways.

- Consider the following examples: in December 1999, a computer hacker obtained the credit card numbers of thousands of people from CD Universe's website.
- This is a privacy issue in that the personal financial data of many people were taken without their permission.
- It is also a security issue, obviously, because that information was obtained illegally by snooping around CD Universe's computers.
- Now let us say you are at work, and you receive an e-mail in your Outlook e-mail program with an attachment that reads: 'Here is that document you asked for? don't show anyone else'.
- You have just been sent the infamous Melissa virus, which began making the Internet rounds in March 1999.
- If you open the attachment, the virus will automatically be forwarded to the first 50 people in your Outlook address book.

- This is a security issue because the virus has taken over your program that is Outlook to execute an unwanted task.

Tutorial 10

1.

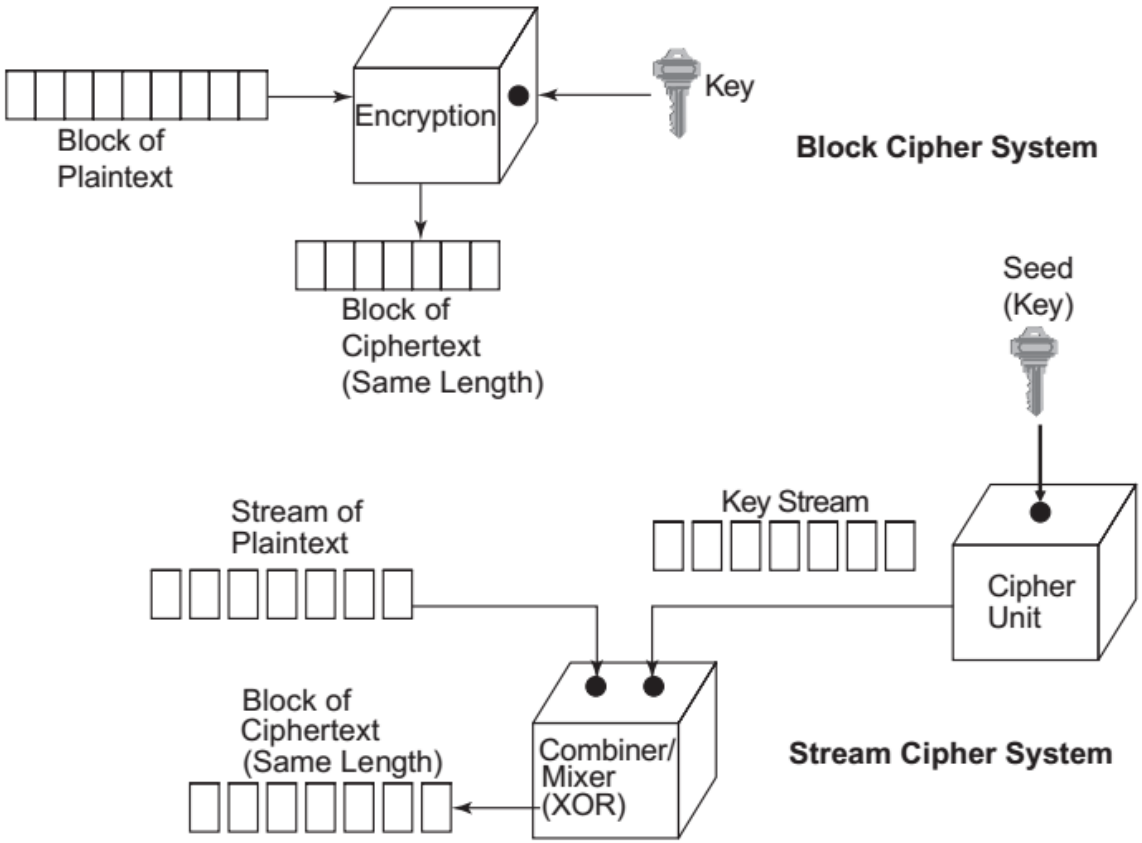
Model of Cryptographic Systems

The terminology of cryptography includes the following key terms:

- Cryptology is the science and art of secret communications.
- Cryptography is the set of methods used to ensure the secrecy and/or authenticity of messages.
- Cryptanalysis is the set of methods used to break a cipher system and/or forge coded signals so that they will be accepted as authentic.
- Plaintext is the original, understandable message.
- Cipher is a method or algorithm to transform a plain text into something that is difficult to understand.
- Ciphertext is the result of the application of the cipher to the plaintext, that is, the unintelligible or scrambled form of the message.

- Cryptographic key is some additional secret information used in conjunction with the cipher algorithm to perform the cryptographic process.
- Encryption/encipherment is the process of converting the intelligible message (the plaintext) back to its unintelligible form (the ciphertext).
- Decryption/decipherment is the process of converting the unintelligible message (the ciphertext) back to its intelligible form (the plaintext).
- Secure channel is a pathway between the sender and the receiver of a message that can be guaranteed to be safe, that is, free from any illicit observation or modification of messages carried out on it by any third party.
- Cryptovirology is known as the younger evil sibling of Cryptography. It is a field devoted to the study of using cryptography for designing powerful malicious software.

- There are many types of 'ciphers'.
  - Transformation Cipher
  - Substitution Cipher
  - Block Cipher
  - Stream Cipher



Issues in Documents Security

- At any given time, a business may have files including customer credit card information, employee social security numbers, business bank account information, or proprietary information
- These files could be readily accessible to both employees and customers, depending on where you keep them and how vigilant you and your employees are at keeping them secure.
- Most businesses have both physical documents and digital documents.
- These documents may include employee forms, like health information or financial information for your business, such as credit card numbers or contract information.

- If they aren't properly secured, these documents and files put your business, your employees, and your customers at risk of identity theft or credit card fraud, losing valuable information.
- Here are some of the most common document security issues and actionable tips on how to fix those issues.
- **Unsecured documents are easy to steal**
  Important documents need to be locked in a file cabinet. While a determined thief might be able to break a lock, a casual or opportunistic thief will likely move on. Make it a policy for anyone with important files to put them away in a locked cabinet or desk drawer whenever they aren't using them.

- **Too many people have access to sensitive information**
  You do need some sensitive information, such as payroll records and emergency contact information for employees, but that doesn't mean everyone needs access to it. Limit access just to those who need the information to complete their job responsibilities.
- **Computers are at risk**
  Digital information is just as vulnerable as hard copies if you leave your computer unlocked. If your employees use company computers or personal devices with company information, require them to lock their computers. For that matter, antivirus software and system updates are an important and easy part of securing devices. There's no good reason to skip out on those.

- **Physical data is easily destroyed**
  It only takes one fire or one flood to wipe out years of important business documents. In 2017, for instance, tech company Hewlett-Packard lost "more than 100 boxes" of "correspondence, speeches, and other items" from the company's founders in the Santa Rosa, California, wildfires. Use a fire and waterproof file cabinet to secure your documents.
- **Too many documents are on file**
  When you no longer need a document, it's time to shred it. Don't leave documents with confidential information in recycling bins, in the trash, or on a desk to take care of later. This goes for hard drives, too. Unless you physically destroy it, a good hacker could still pull information from it.

- **Networks are unsecured**
  Almost every business is at risk of an online data breach or cyber attack. CNN Tech reports that a 2017 cyber attack resulted in some British hospitals temporarily closing, and schools in Montana closed for three days when a hacker group stole the personal information of students and teachers. While there are a lot of ways to secure your network, one of the easiest is to simply ensure you have a firewall in place and require a password for access.
- **Records aren't backed up**
  There are plenty of ways to lose critical data. Whether it's user error, technical malfunction, or hacking, if you don't regularly back up your data, it's at risk. In many cases, you can automate backups, so you don't even have to think about it. In a worst-case scenario, even if a hacker does steal and hold your information for ransom, you have a copy, so you at least know what is at risk.

- **There is no disaster plan in place**
  Every business needs a disaster plan. You probably have a fire escape plan, a panic button in case of police emergencies, and maybe even an evacuation plan if you live in areas prone to natural disasters. But do you have a plan in place for document theft? Business, employee, and customer information is at risk no matter how diligent you are at locking file cabinets or securing your network. It's unfortunate but true.
- **The security camera is poorly placed**
  Properly positioned security cameras are a theft deterrent by themselves, but even if you are the victim of an on-location data theft (or any other crime), good security cameras may help police identify and locate the criminal. Business security systems don't need to be expensive to be effective.

- **Hire a security expert**
  If you truly want to limit your business exposure to theft, hire a security expert to audit your business. This goes for both physical security, such as illegal entries, and cyber security, such as hacking. When you know where the holes are in your defences, you can take steps to make your business documents even more secure.

Depending on your preparation and response, document security issues can make or break your business. Take the steps necessary to reduce risk and secure critical information. It will only help your business in the long run.

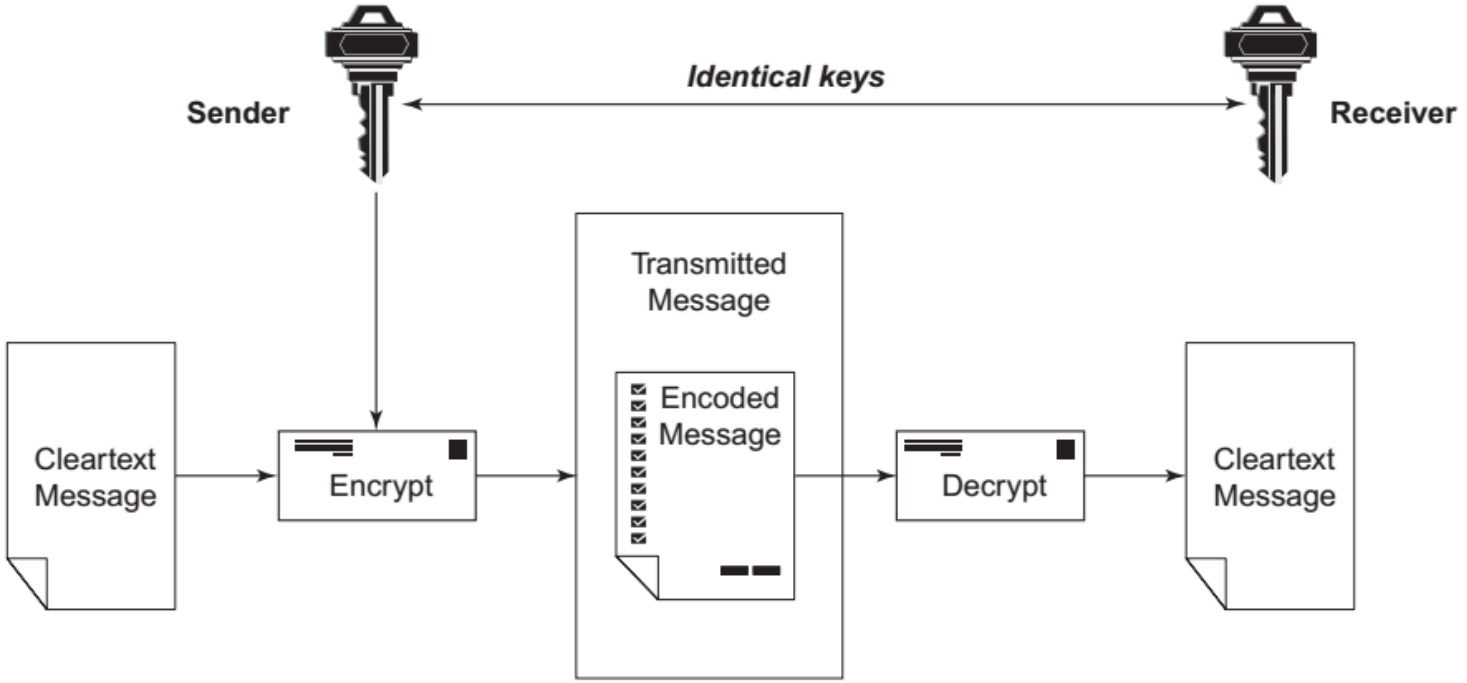
System of Keys

True strength of the confidentiality service may depend on a number of variables associated with the encryption function listed as follows:

- The security protocol or application used to invoke the encryption function;
- The trust in the platform executing the protocol or application;
- The cryptographic algorithm;
- The length of the key(s) used for encryption/decryption;
- The protocol used to manage/generate those keys
- The storage of the secret keys.

The strength of a cryptographic system usually increases as the key length increases. This is because a longer key length implies a larger number of possible keys. A 128-bit encryption has become the common practice; any key length less than 64 bits is no longer considered to be secure.
Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system

- **Private/symmetric key:**
  A private or symmetric key is a secret key that is shared between the sender and the receiver of the message. This key is usually the only key that can decipher the message



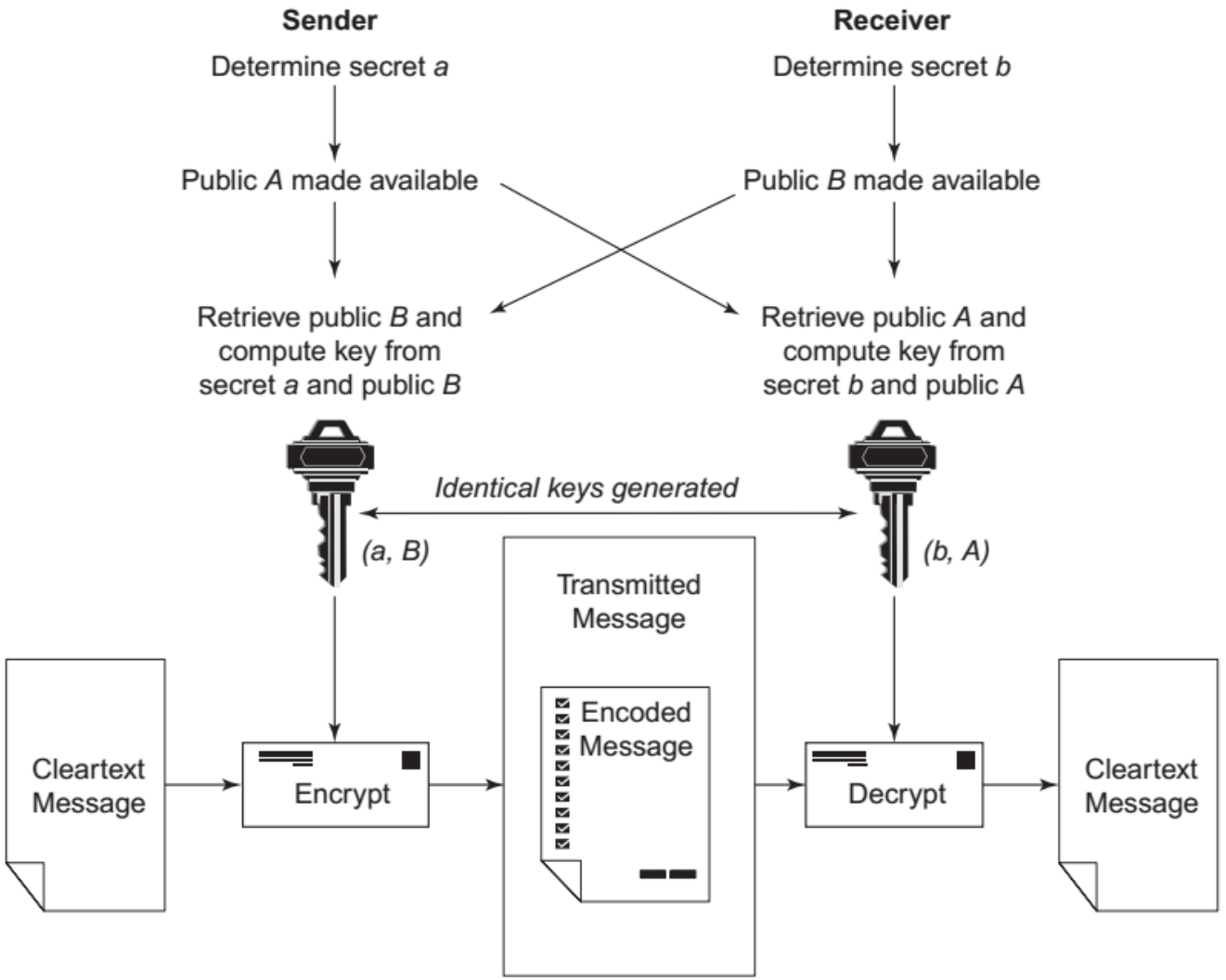
- **Public/asymmetric key:**
  A public or asymmetric key is the one that is made publicly available and can be used to encrypt data that only the holder of the uniquely and mathematically related private key can decrypt

- **Data/session key:**
  This is a symmetric key, which may or may not be random or reused. It is used for encrypting data. Often, this key is negotiated using standard protocols or sent in a protected manner using a secret public or private key.
- **Key encrypting key:**
  These are the keys that are used to protect data encrypting keys. These keys are usually used only for key updates and not data encryption.

Public Key Cryptography

- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
- Each receiver possesses a unique decryption key, generally referred to as his private key.
- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver.
- Encryption algorithm is complex enough to prohibit attacker from deducing the plain text from the cipher text and the encryption (public) key.

- Private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key.



Key Management

- **Key generation:** This involves the selection of the number that is going to be used to tailor an encryption mechanism to a particular use. The use may be a sender and receiver pair, a domain, an application, a device or a data object. The key must be chosen in such a way that it is not predictable and that knowledge of it is not leaked in the process. Keys must be chosen randomly and in addition, they must not be disclosed at the time of the selection.
- **Distribution:** Key distribution is the process of getting a key from the point of its generation to the point of its intended use. This problem is more difficult in symmetric key algorithms where it is necessary to protect the key from disclosure in the process. This step must be performed in a channel separate from the one that the traffic moves in.

- **Installation:** Key installation is the process of getting the key into the storage of the device or process that uses it. If this step involves manual operations, then such operations might result in leaking information about the key, key transcription errors or it might be so cumbersome as to discourage its use.
- **Storage:** Keys need to be protected and the integrity of the storage mechanism itself is important. For example, the mechanism may be designed so that once the key is installed, it cannot be observed from outside the encryption machine itself. Some key-storage devices are designed to self-destruct when subjected to forces that might disclose the key or there are evidences that the key device is being tampered with. As another approach, the key may be stored in an encrypted form so that knowledge of the stored form does not disclose information about the behaviour of the device under the key.

- **Change:** This is about ending the use of one key and beginning that of another. This is determined by convention or protocol. Historical practices show that information about the key is prone to leakage during the key-change time. The longer the key is in use and the more traffic that is encrypted under it, the higher are the chances for its discovery and therefore more the traffic that will be compromised. This shows that there is value to key-changing practices.
- **Control:** Controlling the key means the ability to exercise a directing or restraining influence over its content or use. For example, selecting which key from a set of keys is to be used for a particular application or party is a part of key control. Ensuring that a key which is intended for encrypting keys cannot be used for data is a part of key control. Key control is essential to the proper functioning of a key management system.

Digital Signature

- Digital signature is a term used to describe a long numeric code that is uniquely assigned to one person.
- It has nothing to do with a real signature.
- The purpose of a digital signature is to be used in encryption systems.
- A digital signature is issued to an individual by a Certificate Authority (CA).
- This is a group or an organization responsible for maintenance and safekeeping of digital signatures.
- Because of their length, no one actually remembers or even knows his/her digital signatures.
- An individual's digital signature will normally reside on his/her computer, or can be stored on a card or on pen drives.

- When someone wishes to encrypt an e-document, they will use a password or PIN that in turn allows the digital signature to be used.
- Although secure once encrypted, digital signatures are only as safe as is the medium where they reside.
- Anyone obtaining access to your password, PIN or computer can potentially make unauthorized use of your digital signature.
- The use of a digital signature does not guarantee the ID of the originator.

Applications of Digital Signature

- Authentication
- Integrity Check
- Non-repudiation

Fingerprints

- Digital signatures create a virtual fingerprint that is unique to a person or entity and are used to identify users and protect information in digital messages or documents.
- A message digest is a fingerprint or a unique summary that can uniquely identify the message.

Tutorial 11

1. Explain the meaning of various key terms associated with cryptography.
2. Explain the concept of ciphers. What are the various types of ciphers that exist?
3. What is the difference between block cipher and stream cipher systems?
4. Explain the role of cryptography in information systems security.
5. With a suitable illustration, explain the working of digital signatures. What is a message digest?
6. What is the role of a trusted certificate in message authentication? Explain how it is useful in e-commerce?

7. Why is key management essential? Discuss the various functions under key management.
8. With suitable diagrams, explain the working of symmetric and asymmetric encryption methods.
9. Compare private- and public-key methods in terms of their relative advantages and disadvantages.
10. How do you place steganography in the context of cryptography? Explain how (digital) watermarking is related to steganography.
11. Explain the scientific principle on which the concept of quantum cryptography is based.

Firewalls

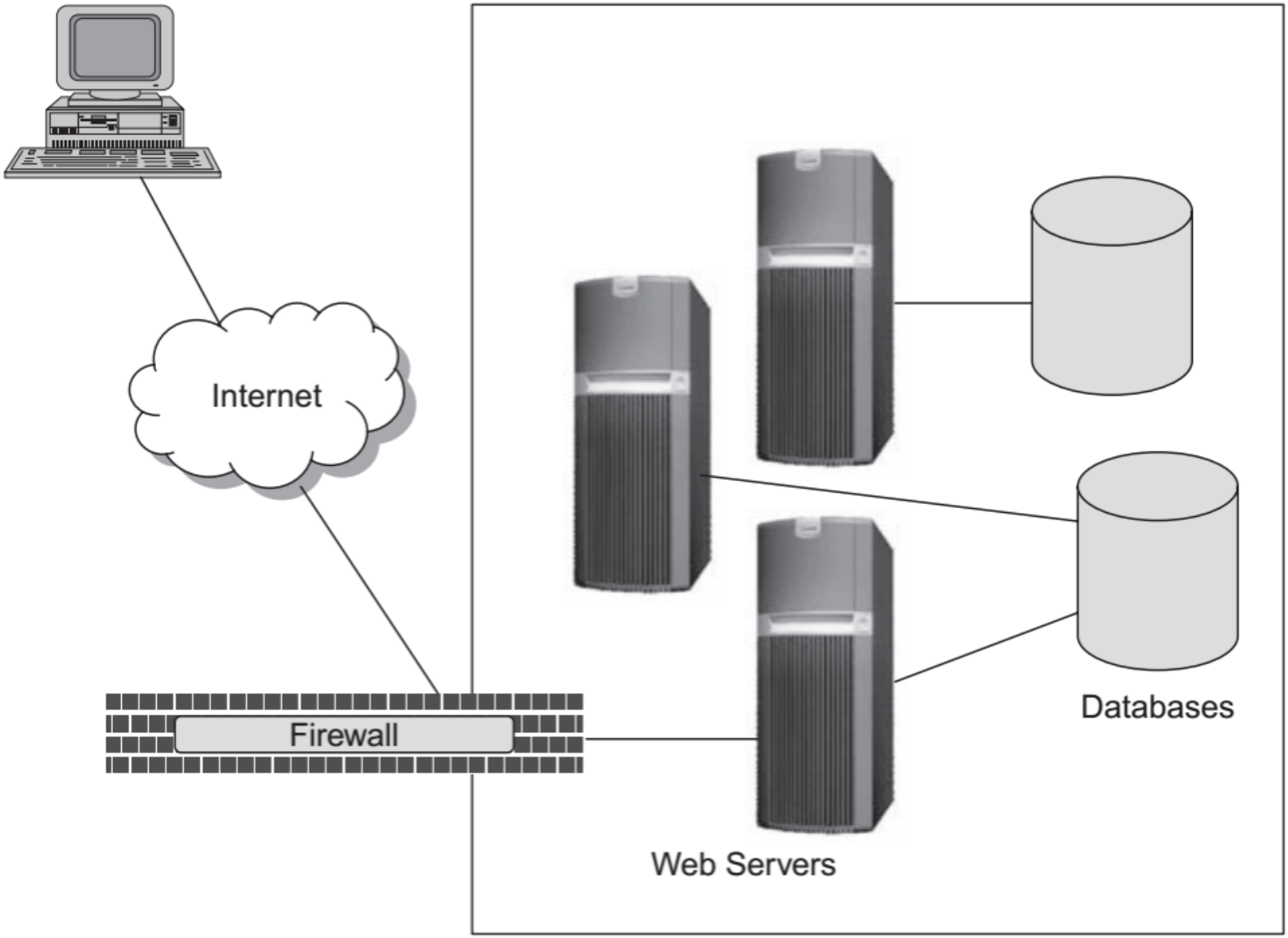
- Firewall is not simply a router, a host system or a collection of systems that provide security to a network. It is important to understand that a firewall is an 'approach' to security.
- It helps organizations to implement a larger security policy that defines the services and access to be permitted.
- Basically, a firewall is a barrier to keep destructive forces away from your property/assets.
- In fact, that is why it is called a firewall. Its job is similar to a physical firewall that keeps a fire from spreading from one area to another.
- We have mentioned threats to information systems assets, especially those that reside on the corporate networks and the Internet. In previous discussion we have already explained hackers and threats from them.

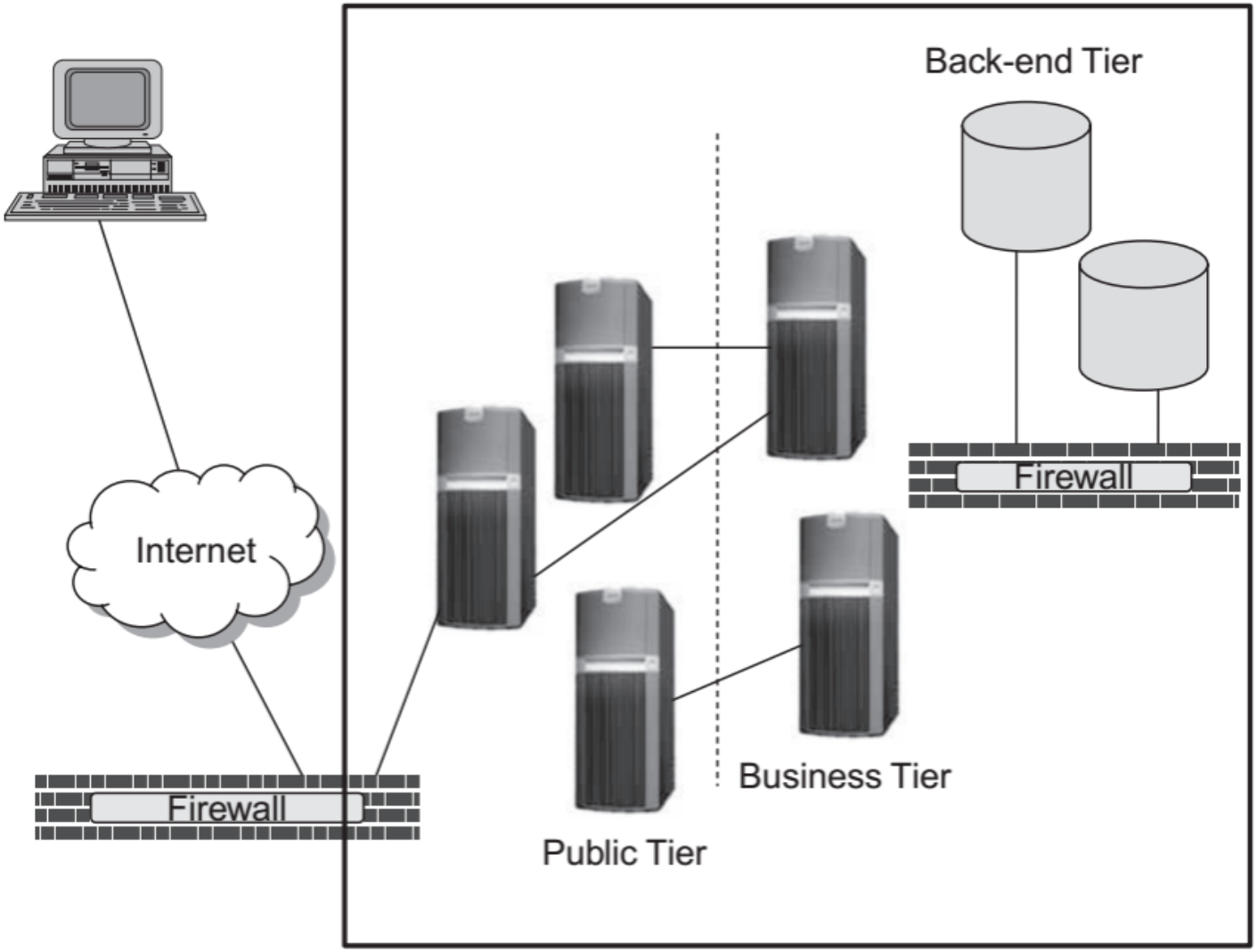
- Firewalls protect the network from unauthorized use by attackers.
- Basically, any device that can control network traffic for security reasons can be called a firewall.
- Firewalls are used to restrict access from one network to another network.
- Most organizations use firewalls to restrict access into their network from Internet users.
- As an internal usage, firewalls may also be used to restrict one internal network segment from accessing another internal segment, for example, the finance department of a company may not want the production department to access their network for the sake of information confidentiality.
- Thus, computer firewalls (made of software and/or hardware) are there to protect computers against unauthorized access. They also prevent rogue programs from gaining access to the Internet.

- A key point is that in addition to antivirus and privacy software, a firewall is a part of total system security.
- Firewalls also log intruders attempts to access the computer network, providing important information, such as date/time, IP address of intruder and method of attack. This information helps in the identification of the intruder.
- Firewalls are hardware and software combinations that block intruders from access to an intranet while still allowing people on the intranet to access the resources of the Internet.
- Depending on how secure a site needs to be, and how much time, money and resources can be spent, there are many kinds of firewalls that can be built.
- Most of them, though, are built using only a few elements. Servers and routers are the primary components of firewalls.

- Firewalls can be deployed in many ways. A perimeter firewall, also known as the gateway firewall, is placed between the Internet connection device and the local area network (LAN) hardware such as switches, computers or printers.
- Some hardware routers have firewalls, if you are considering buying a router to connect two or more computers look for the one with a firewall built in. These types of routers provide firewall security to a number of computers through a single Internet connection. They also lower your costs for protecting all the machines in your network.

- Two typical deployment scenarios for firewalls, that is, firewalls in a two-tier network architecture and firewalls in a three-tier network architecture

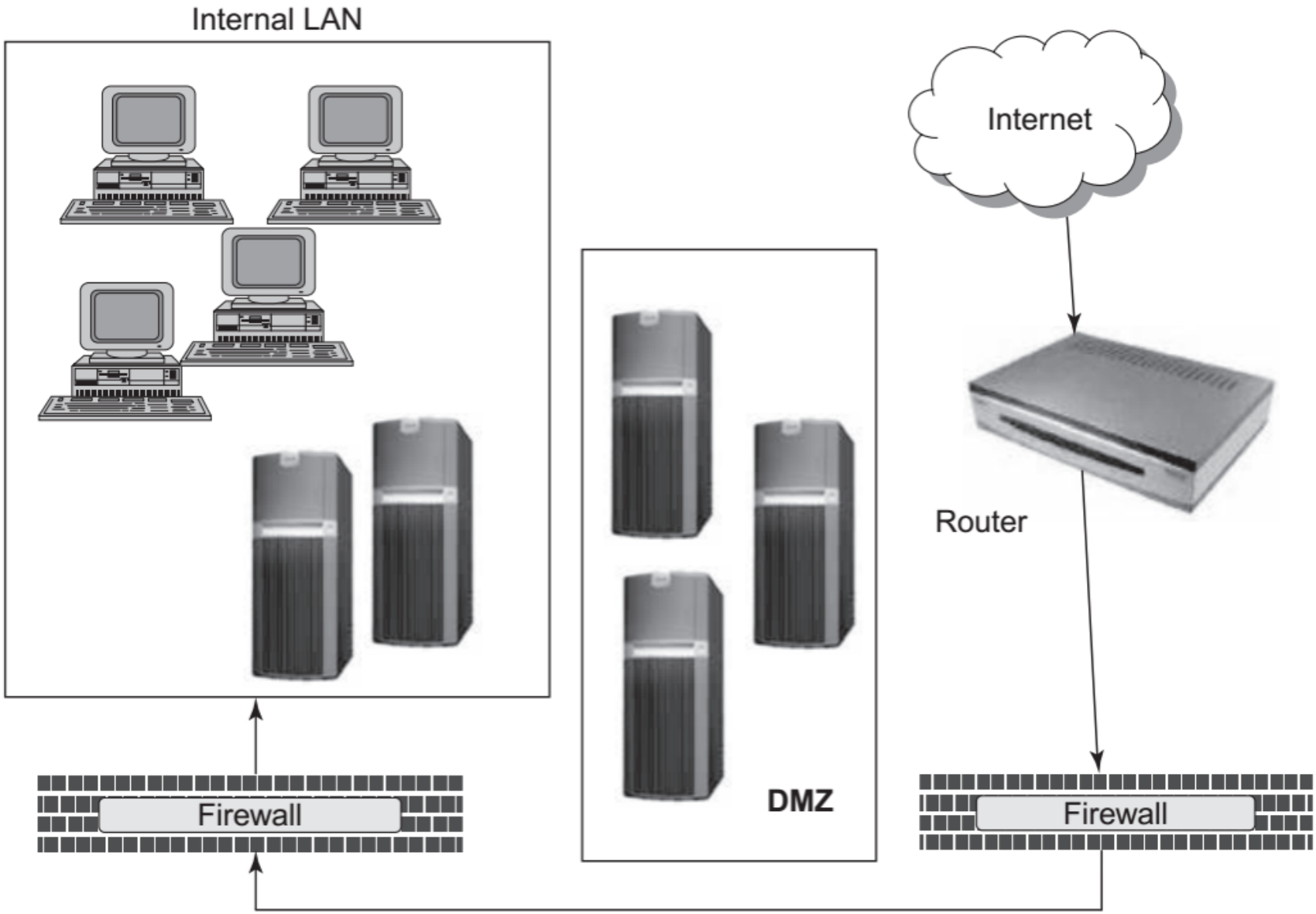

Internet
Firewall
Databases
Web Servers



- There are many advantages in deploying firewalls in this manner;

- The first firewall supports a particular security policy and provides the first line of defence
- The first tier of web servers only accepts specific requests, can authorize individuals before accepting certain types of requests and can dictate which entities can place requests to the next tiers.
- The middle tier can provide security at the component level. The idea in such two-tier architecture is that no request should be made from the Internet directly to the back-end databases.

- **Demilitarized Zone** The area separated between the two firewalls is called the 'DMZ'.


Internal LAN
Internet
Router
Firewall
DMZ
Firewall

- Basically, a DMZ is a subnetwork that is located neither inside the internal network nor outside as part of the Internet.
- Technically, a demilitarized area is any area where access is controlled, but not prevented by firewall technology.

Design and Implementation Issues

- There are a number of basic design issues that should be addressed by the security professional who has been given the responsibility of designing, specifying and implementing or overseeing the installation of a firewall.
- The first and most important decision reflects the policy of how your company or organization wants to operate the system
- The second important question is: What level of monitoring, redundancy and control is desired by the organization?
- The third issue in firewall design architecture and implementation is of financial nature. It is important to try to quantify any proposed solutions in terms of how much it will cost either to buy or to implement. Firewall products range from highend to low-end values.

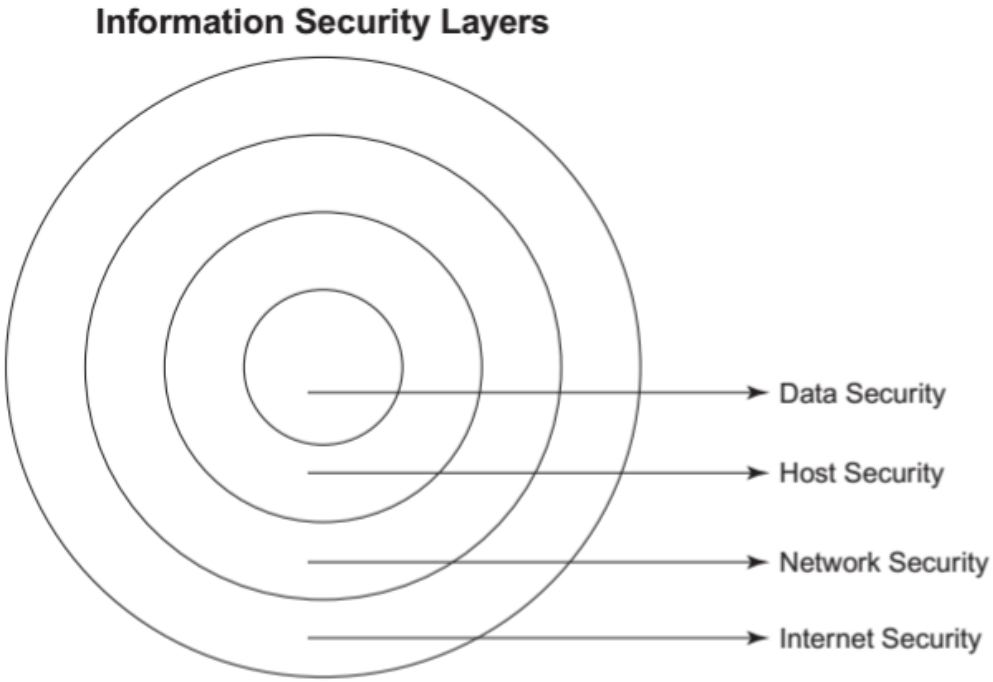
- There are other challenges on the technical side as well; there are a couple of decisions to make, based on the fact that for all practical purposes, what we are talking about is a static traffic routing service placed between the network service provider's router and the organization's internal network.
- The traffic routing service may be implemented at an IP level via screening rules in a router, or at an application level via proxy gateways and services.
- The decision to make is whether to place an exposed stripped-down machine on the outside network to run proxy services for telnet, FTP, news, etc. or whether to set up a screening router as a filter, permitting communication with one or more internal machines.

- There are benefits and drawbacks to both approaches, with the proxy machine providing a greater level of audit and, potentially, security in return for an increased cost in configuration and a decrease in the level of service that may be provided.
- The trade-off between ease-of-use and security is always a challenge to handle for organizations.

Network Security Basic Concepts

- Network security is the fundamental defence to safeguard the collaborative enterprise.
- As the convergence of corporate networks gains pace, security issues for the computer networks become a top concern for the business enterprises.
- The complexity of ensuring a reliable network security is viewed as the single most critical barrier to the successful implementation of net-centric information systems
- The network security is the first line of defence.

- Peripheral defences play an important role and so there is a need to establish perimeter security for protecting the network



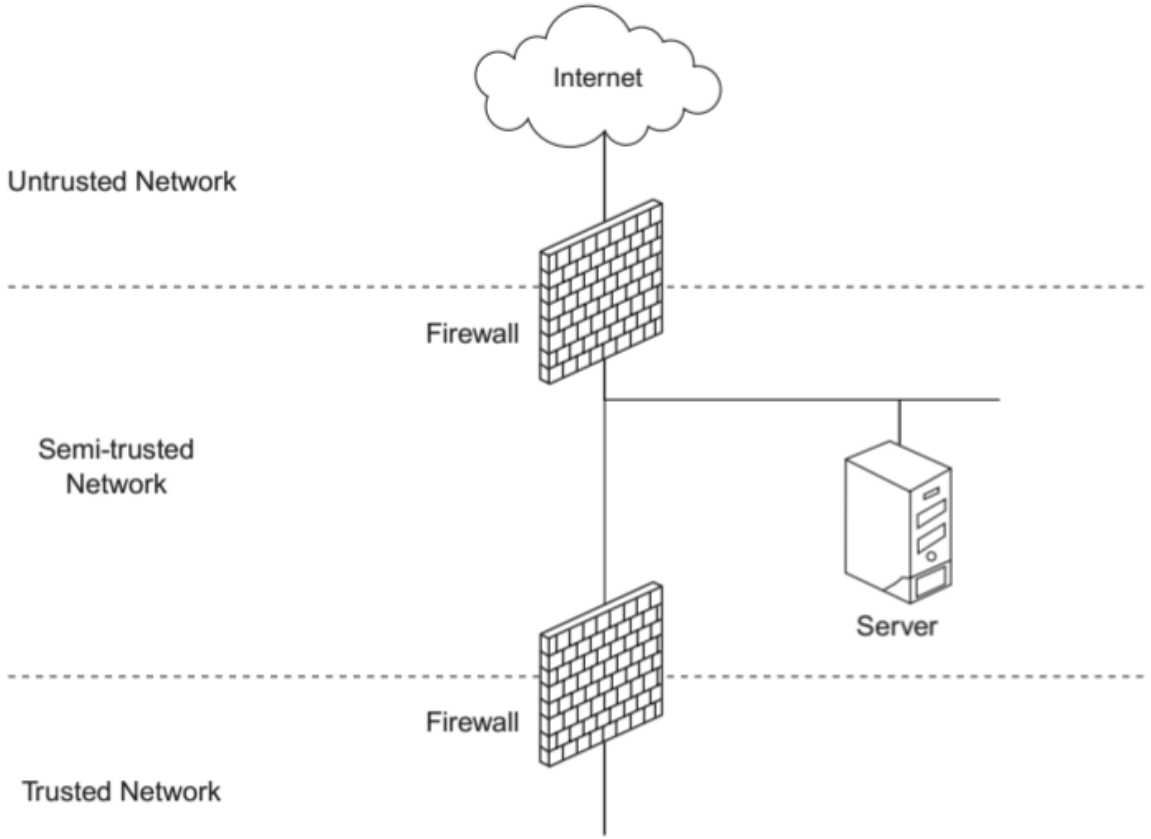
- **Computer Security**
  The concepts of network security are related to the security of the computers and other related terms.
- Therefore, it is important to explain these terms.

- Emission security(Emsec) refers to preventing a system being attacked using compromising emanations, that is, conducted or radiated electromagnetic signals.
- There are many aspects of Emsec.
- Military and defence organizations are greatly concerned with 'tempest defenses', which prevent the stray radio frequency (RF) emitted by computers and other electronics equipments, from being picked up by a person and used to reconstruct the data being processed; though this requires extremely complex technical skills in the person attempting it, it is not impossible.
- Apart from defence and military organizations, smart card industry is also concerned with power analysis, in which a computation being performed by a smart card – such as a digital signature – is observed by measuring the electric current drawn by the central processing unit (CPU) of a computer and the measurement results are used to reconstruct the key.

- Although people often undermine the importance of Emsec, it is not something to be ignored.
- Credit card-related frauds are notorious and people can lose a large amount of money.
- Communications security and Emsec were adequate, in the earlier days, when messages were by teletype.
- Eventually, computers came on the scene in a big way and most of the information assets of the organizations became easier to use and more and more people got to access them with interactive sessions.
- Thus, information on the systems became accessible to almost everybody as long as they had access to them. This is when the need for computer security was realized.
- **Network Security**
  As computer systems evolved further and computers got linked through networks, another problem arose, that of lack of network understanding.

- New security problems occur when computers are networked together. Issues such as various types of networks, encryption standards, emissions control, etc. come up in the domain of network security.
- This gave rise to the concept of network security. Network security means different things to different people.
- It is a complex and rapidly evolving field. Basically, network security is used to control access to network resources and services.
- There are three elements of network security that are used to create many different concepts and security mechanisms: cryptography, secure network protocols and applications and access control mechanisms.
- Authentication, integrity and confidentiality and non-repudiation are the basic properties that are expected from a network service provider.

- Network security is required because networks are subject to various attacks by hackers
- **Trusted and Untrusted Networks**
  This is a way of classifying networks in terms of levels of security. When a network manager creates a network security policy, each network that makes up the topology must be classified as one of the following three types of networks 1. trusted network; 2. semi-trusted network; 3. untrusted network.



- **Trusted Networks**
  Trusted networks are the networks inside your network security perimeter. These networks are the ones that organizations need to protect.

- A network administrator employed in an organization administers the computers that comprise these networks, and the organization controls their security measures.
- When a firewall server is set up, the network administrator must explicitly identify the type of networks that are attached to the firewall server through network adapter cards.
- After the initial configuration, the trusted networks include the firewall server and all networks behind it.
- One exception to the general rule mentioned above is the inclusion of VPNs, which are trusted networks that transmit data across an untrusted network infrastructure.
- The network packets that originate on a VPN are considered to originate from within your internal perimeter network.
- **Semi-Trusted Networks** These are the networks dedicated to your use, but not under your physical control e.g., the Internet.

- These are also referred to as the demilitarized zone (DMZ).
- Under the scenario of semi-trusted networks, access is allowed to some database materials and electronic mail (e-mail).
- Semi-trusted networks may include domain name system (DNS), proxy and modem servers.
- However, they are not for confidential or proprietary information.
- **Untrusted Networks** Untrusted networks are the networks that are known to be outside an organization's security perimeter.
- Essentially, they are any network where you do not know the routing of messages (e.g., the Internet or similar).
- They are untrusted because they are outside an organization's control. There is no control over the administration or security policies for these sites.

- They are the private, shared networks from which you are trying to protect your network.
- However, individuals and organizations may still need and want to communicate with these networks although they are untrusted.
- When you set up the firewall server, you explicitly identify the untrusted networks from which that firewall can accept requests. Untrusted networks are outside the security perimeter and are external to the firewall server.
- **Unknown Networks** These networks are neither trusted nor untrusted. By default, all non-trusted networks are considered unknown networks. Unknown networks can be identified below the Internet node and more specialized policies need to be applied to those untrusted networks

Dimensions

- A network is two or more devices connected together in such a way as to allow them to exchange information.
- The networks need not be only computer networks; there are other forms of networks as well – networks that carry voice, radio or television (TV) signals.
- When an organization's network is connected to the Internet, you are physically connecting the corporate network to more than 50,000 unknown networks and all their users.
- Although such connections open the door to many useful applications and provide great opportunities for information sharing, most private networks contain some information that should not be shared with outside users on the Internet.

- Thus, the preoccupation of network security professionals is protecting confidential information and protecting the corporate network to maintain internal network system integrity under the threat of attacks.
- Network intrusion is the most common security issue. The other issues for network security are:

1. attacks against network assets, that is, information and physical assets accessible through the network
2. network perimeter threats
3. security of the network router
4. security of wireless networks
5. host security
6. World Wide Web (WWW) security
7. intrusion detection systems (IDSs)
8. operating systems (OSs) security

- There is always some risk because not all Internet users are involved in lawful activities.
- There are two key questions behind most security issues in a networked environment:
- The first one is how to protect confidential information from those who do not explicitly need to access it,
- Other one is how the network and its resources can be protected from malicious users and accidents that originate outside the network.

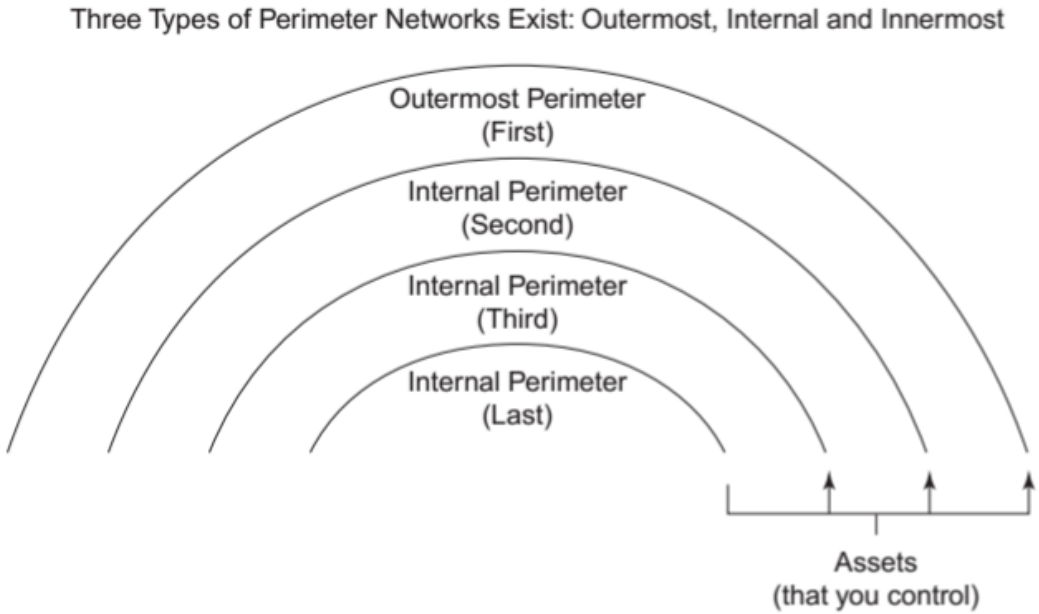
Tutorial 12

1. Explain what firewalls are and why do organizations need them.
2. Explain various approaches to the deployment of firewalls. Why is the concept of 'demilitarized zone' so important?
3. What is the role played by a proxy server?
4. What are the different types of firewall configurations that you are aware of? Explain how they function.
5. Explain the role of routers and intrusion detection systems in the context of firewalls.
6. Discuss key design and implementation issues for firewalls. Explain the critical role of firewall policies that the organizations must consider.

Perimeter for Network Protection

- What is meant by the term ‘perimeter’.
- The ‘perimeter’ represents the point at which external traffic gains initial access to the network as well as the point through which internal traffic will traverse the Internet.
- The purpose of perimeter security layers is to protect against hackers trying to penetrate the network, DoS and sophisticated attacks at the application level or other hybrid methods of attacks.
- It is critical to deploy multiple security layers at the perimeter so that if an attack gets through the first layer, supporting layers will stop the attack.

- There are three types of perimeter networks: the outermost perimeter, internal perimeters and the innermost perimeter as shown in the below Figure.



- The multiple internal perimeters are relative to a particular asset, such as the internal perimeter that is just inside the firewall server.

- The outermost perimeter network identifies the separation point between the assets that organizations control and the assets that are not controlled; usually, this point is the router that is used to separate the network from other networks.
- Internal perimeter networks represent additional boundaries where other security mechanisms are in place, such as Internet firewalls and filtering routers.
- Given the nature of perimeter networks and perimeter security, it becomes important to consider certain factors while designing it.
- In many cases, perimeter security represents the greatest assortment of security layers and may include VPN, DoS, firewall and intrusion protection.

- With several different security technologies being deployed at the perimeter, it will be important to consider how they will be controlled – a centralized, policy-based management solution will usually provide the ability to unify the perimeter security decisions.
- A key requirement at the perimeter, through which all Internet-bound traffic passes, is to control the websites that employees may visit to protect the company from litigation and the network from inadvertent downloads of viruses, malware or Trojans through web filtering.
- To understand why organizations frequently suffer network intrusions and how these can be avoided, it is important to first gain a high-level understanding of the different types of vulnerabilities that hackers seek when casing a network.
- When hackers attack networks, they always look to exploit the vulnerabilities in the networks, most often so because the networks are not adequately protected.

- The categories of vulnerabilities that hackers typically search for are the following:
  - Inadequate border protection
  - Remote access servers (RASs) with weak access controls
  - Application servers with well-known exploits
  - Misconfigured systems and systems with default configurations

Security Perimeter Design Considerations

- **Be aware of the enemy:**
  Organizations must know the potential attackers or intruders. However, it must be noted that even security measures can never make it impossible for a user to perform unauthorized tasks with a computer system; they can only make it harder. The goal is to make sure that the network security controls are beyond the attacker's ability or motivation.
- **Consider network security costs:**
  Security measures usually reduce convenience, especially for sophisticated users. It is important to realize that security matters can delay work and can create expensive administrative and educational overhead. When designing security measures, organizations need to understand their costs and must consider those costs against the potential benefits. To do that, the organizations must understand the

costs of the measures themselves and the costs and likelihood of security breaches.

- **Make justifiable assumptions supported by business case:** Organizations might assume that their network is not tapped, that attackers know less than security professionals employed by them, that they are using standard software or that a locked room is safe. The assumptions should be examined and justified. Any hidden assumption is a potential security hole.
- **Work with a limited number of secrets:** Most security is based on secrets. Passwords and encryption keys are secrets. Although the secrets are not all that secret. The most important part of keeping secrets is in knowing the areas that need protection. The larger the number of secrets, the harder it will be to keep them all. Security systems should be designed so that only a limited number of secrets need to be kept.

- **Lax behavior of humans:**
  Many security procedures fail because their designers do not observe or predict how users will react to them. For example, because passwords can be difficult to remember, automatically generated nonsense passwords often are written on the undersides of keyboards.
- **User education is always critical:**
  If your security measures interfere with an essential use of the system, those measures will be resisted and perhaps bypassed. To get compliance, organizations must make sure that users can get their work done. The users must understand and accept the need for security.

- **User awareness and training on security:**
  Any user can compromise the system security, at least to some degree. For instance, passwords can often be found simply by calling legitimate users on the telephone, claiming to be a system administrator and asking for them. The users should be taught never to release passwords or other secrets over unsecured telephone lines.
- **Understand your weaknesses:**
  Every security system has vulnerabilities. You should understand your system's weak points and know how they could be exploited. You should also know the areas that present the greatest danger and should prevent access to them immediately. Understanding the weak points is the first step toward turning them into secure areas.

- **Limit the scope of access:**
  Organizations should create appropriate barriers in their network system so that if intruders access one part of the system, they do not automatically have access to the rest of the system. The security of a system is only as good as the weakest security level of any single host in the system.
- **Understand the environment:**
  A good understanding of how the overall system normally functions always helps. Organizations need to know what is expected and what is unexpected security incidents. Network security professionals in the organizations must be familiar with how network devices and tools can be used for detecting security problems. Adequate security alertness must exist to notice unusual events to catch intruders before they can damage the system. Security auditing tools can help detect those unusual events.

- **Limit your trust:**
  Trust as in network security is a good element of operations as long it works! Organizations should carefully select the software on which they can rely. The security system should not have to rely on the assumption that all software is bug-free. A cardinal rule is that even the third-party ready software packages and tools must be tested.
- **Physical security to be treated as important:**
  Physical access to a computer or a router usually gives a sufficiently sophisticated user total control over that computer. Physical access to a network link usually allows a person to tap that link, jam it or inject traffic into it. It makes no sense to install complicated software security measures when access to the hardware is not controlled. Thus, to protect the network assets and components, physical security always remains an important link in the security chain.

- **Adopt a pervasive perspective on security:**
  Security of the network system gets affected by almost any change that is made in the system. This is especially true when new services are created, new networks components are added, etc. Administrators, programmers and users should consider the security implications of every change they make.

Network Attacks

- Intruders attempt to attack networks to gain hold of the information resources on the network.
- Network intruders come in three forms –
  masquerader - an individual who is authorized to use a computer;
  misfeasor - a legitimate user who misuses his/her privileges;
  clandestine user - an individual who seizes supervisory control of the system and uses it to suppress audit information.
- Conceptually, network attacks can be classified as:
  1. Interruption: Denying service to authorized users. These are attacks on system availability.
  2. Interception: Unauthorized user obtaining access to a service. Thus, this is an attack on confidentiality.
  3. Modification: Unauthorized access and tampering with data. This is an attack on integrity.

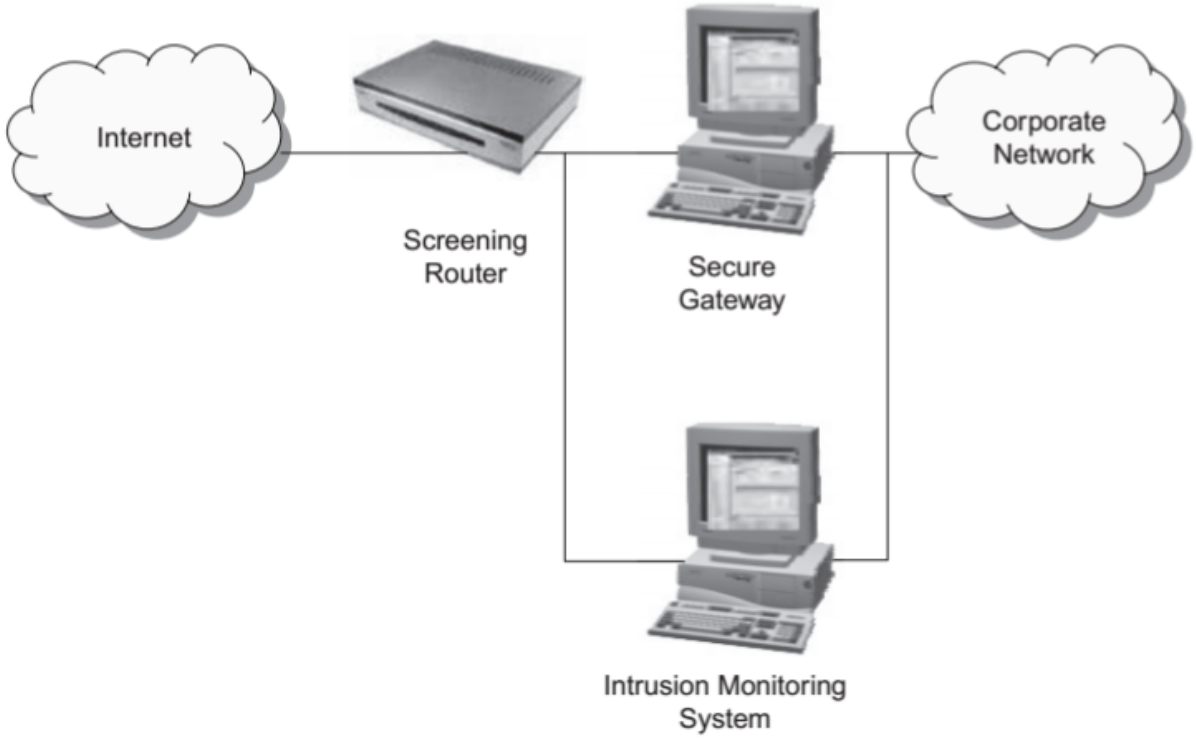
4. Fabrication: Counterfeit data. This is an attack on authenticity.

- The other way of classifying network attacks is passive versus active attacks.
- Passive attacks mean that only the message transfer is monitored: unauthorized public release of a confidential message or using a message to determine the type of communications.
- Active attacks mean that the message is intercepted, modified or otherwise manipulated.
- Masquerading is where attacker pretends to be someone else, replay means that messages are recorded and used to produce an authorized effect, message modification means that the message has been altered and denial of service (DoS) prevents valid users from accessing a service.

- Technically speaking, the following are the five common methods of attack that present opportunities to compromise the information on the network:
  1. Password attacks
  2. Network packet sniffers
  3. Internet protocol (IP) spoofing and DoS
  4. Distribution of sensitive internal information to external sources
  5. Man-in-the-middle attacks.

Need of Intrusion Monitoring and Detection

- Having understood how an attacker hacks the network and obtains an illicit access to an organization's data or data of employees placed on the network, let us summarize why intrusion monitoring and detection is necessary.
- The incorporation of monitoring and detection of possible threats to the networks provides the corporations with the ability to ensure the following:
  - **Protected information assets are not accessed by unauthorized entities:**
    Organizations must identify the location of various types of information and know where the development of protected technologies takes place. By installing an IDS within the corporate network, one can offer protection to that information without the need for a secure gateway as shown in the below Fig.



- **The ability to monitor network traffic without impact to the network:**
  A secure gateway is intrusive. All the data packets must pass through it before they can be transmitted to the remote network. An intrusion monitoring system is passive in the sense that it listen on the network and takes appropriate action with the packets as shown in the above Fig.

- **Actively respond to attacks on systems:**
  If implemented properly, intrusion monitoring systems have the ability to perform specific actions when an event takes place. Those actions range from notification to automatic reconfiguration of a device and blocking the connection at the network level.
- **Security professionals are able to understand the attacks on the networks and build systems to resist those attacks:**
  Reviewing the information captured by the intrusion monitoring system can assist in the development of better tools, practices and processes to improve the level of Information Security and decrease the risk of loss.
- **Security metrics get generated:**
  As in any program, good-quality metrics are required to report on the operational aspects of IT systems. Good detection methods help generate metrics around attempts to penetrate the organizational network

Intrusion Detection

- An IDS inspects all inbound and outbound network activities.
- It can be set up to identify any suspicious network activity patterns that may indicate a network or system attack.
- Unusual patterns that are known to generally attack networks can signify someone attempting to break into the network system or trying to compromise the system.
- The IDS can be hardware or software-based security service that monitors and analyses system events for the purpose of finding and providing real-time or near real-time warning of events that are identified by the network configuration to be attempts to access system resources in an unauthorized manner.
- Typically the monitoring and warning is done by examining the network vulnerability scans.

- There are a number of good network vulnerability tools available in the market.
- Essentially network ports are scanned to assess if any potential vulnerabilities can be seen.
- There are two popular approaches available currently to intrusion detection methodology: knowledge-based IDSs and behaviour-based IDSs.
- Knowledge-based IDSs are more common than behaviour-based IDSs.
- Knowledge-based IDS use a database of previous attacks and known system vulnerabilities to look for current attempts to exploit their vulnerabilities and trigger an alarm if a vulnerability is found.
- On the other hand, behaviour-based IDSs take a dynamic approach in the sense that they detect deviations from the learned patterns of user behaviour.

- An alarm is triggered when any activity that is considered outside of normal system use takes place.
- These types of systems are more sophisticated but less common than the knowledge-based IDS.
- The relative advantages and disadvantages of both approaches are summarized in below Table:

Knowledge-based intrusion detection	Behaviour-based intrusion detection
Advantages: 1. False alarm rates are low, that is, intrusion triggers are more reliable 2. Intrusion alarms are standardized and are clear for security personnel to understand	1. The systems can dynamically adapt to new or unique vulnerabilities 2. Systems are not dependent on specific operating systems such as in the case of knowledge-based systems

Disadvantages:	
1. Systems place high demands on resources; knowledge databases need continuous maintenance and updates	1. False alarm rates are high; this can create high data noise, at times making the systems unusable
2. New or unique attacks may go unnoticed if they happen not to be captured in the network attack history database	2. The activity and behaviour of the users on the network may not be static enough to warrant an effective implementation of this type of system

- **Categories of Intrusion Detection System**
  There are many ways in which an IDS can be categorized depending on its use as follows:
  1. **Misuse detection:** Here, the IDS analyses the information it gathers and compares it to the databases of attack signatures. To be effective, this type of IDS depends on the attacks that have already been documented. Like virus detection systems, software for misuse detection is only as good as the databases of attack signatures that it can use to compare packets.
  2. **Anomaly detection:** In this type of detection system, a baseline is established. It consists of things such as the network's traffic load state, breakdown, protocol and typical packet size. With anomaly detection, sensors monitor network segments to compare their present state against the baseline in order to identify anomalies.

3. **Network-based IDS (NIDS):** NIDSs monitor network traffic and uncover possible attacks or suspicious activities. In an NIDS, the IDS sensors evaluate the individual packets that are flowing through the network. The NIDS detects malicious packets that are designed by an attacker to be overlooked by the simplistic filtering rule of many firewalls. However there is a problem with an NIDS – it will not detect attacks against a host made by an intruder who is logged in at the host's terminal.
4. **Host-based IDS (HIDS):** HIDSs can be installed on individual workstations and/or servers to watch for an inappropriate or anomalous activity and insider attacks. They are usually used to make sure that the users do not accidentally delete system files, reconfigure important settings or put the system at risk in any other way. In an HIDS, the IDS examines the activity on each individual computer node or host. The kinds of items that are evaluated include modifications to important system files, abnormal or excessive

central processing unit (CPU) activity and misuse of root or administrative rights.

5. **Passive IDS:** In a passive system, the IDS detects a potential security breach, logs the information and signals and alerts. Here, no direct action is taken by the system.
6. **Reactive IDS:** In a reactive system, the IDS can respond in several ways to the suspicious activity such as by logging a user off the system, closing down the connection or even reprogramming the firewall to block network traffic from the suspected malicious source.

- **Characteristics of a Good Intrusion Detection System**
  We can see that an IDS needs to address several issues in the interest of the security of the networks, a modern-day bastion of information systems (IS). There are many mechanisms for deploying the IDSs. However, regardless of the mechanisms on which they are based, the following are essential:

1. **Uptime:** Smooth and continuous running with minimal human intervention. It should run in the background. The internal working should get examined from outside, so it is not a black box.
2. **Fault tolerance:** This is needed for sustaining a system crash. Its knowledge base should not require a rebuild from restart.
3. **Robustness:** The IDS must be robust, that is, difficult to sabotage. The system should be self-healing in the sense that it should be able to monitor itself for suspicious network activities that might signify attempts to weaken the detection mechanism or shut it off.
4. **Performance:** This is always a critical concern. Without a good performance, an IDS will not get effectively used.
5. **Easy configurable:** Configuration of the IDS should be easy. This is important because every system has a different usage pattern, and the defence mechanism should adapt easily to these patterns.

6. **Easy adaptability:** Given the constantly changing network environment in today's business dynamics, the IDS should be like a chameleon in its ability to adapt to the changing environment. At the same time, it should stay current with the system as it changes, that is, new applications added, upgrades and any other modifications. In other words, the IDS must adapt to the changes of the system.
7. **Built-in defence mechanism:** An IDS must have built-in defence mechanisms, and the environment around it should be hardened to make it difficult to fool, that is, minimum opportunity for generating false alarm or assurance on the positives, that is, a trigger is generated only in genuine situations.

Tutorial 13

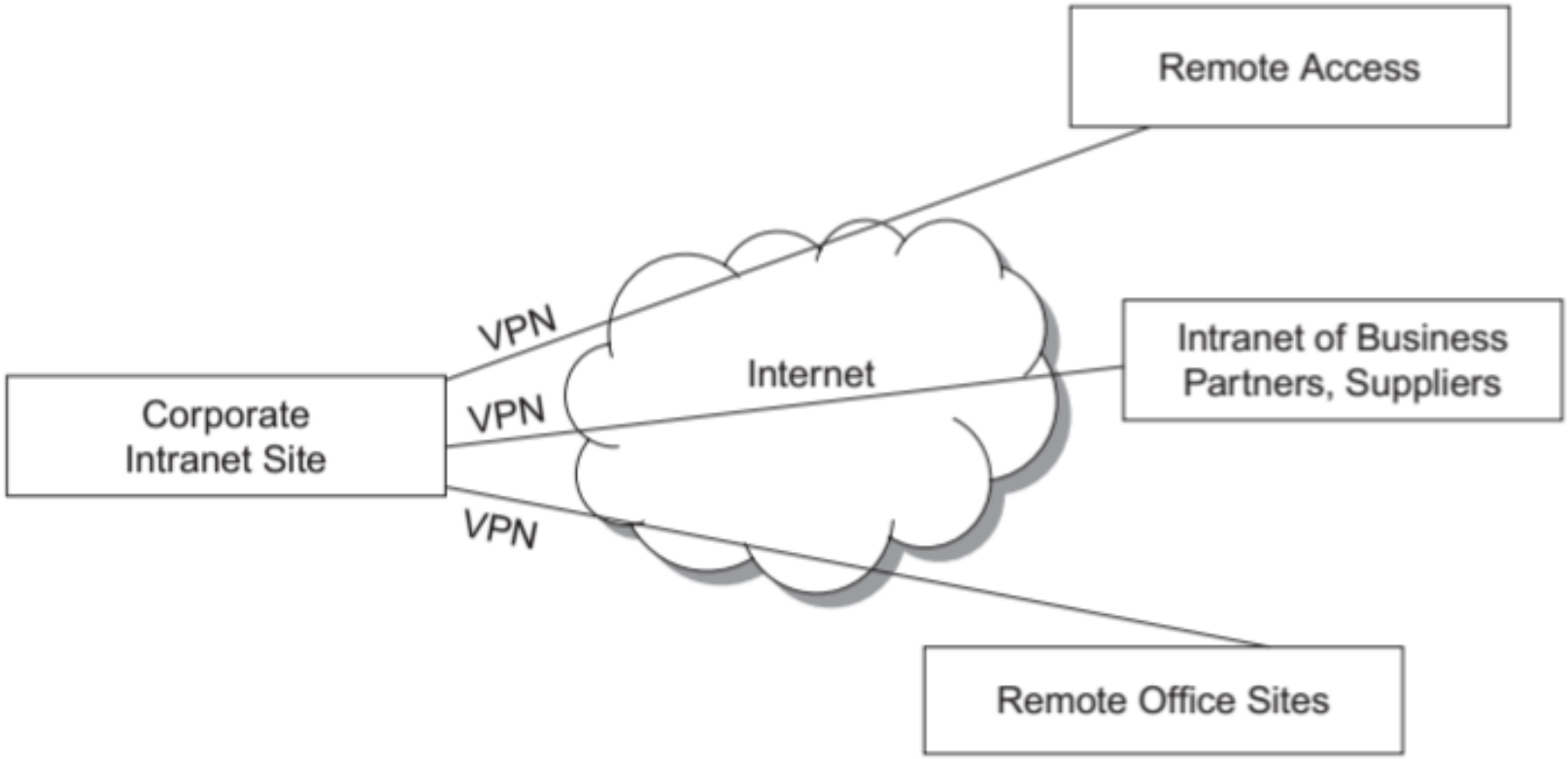
1. Explain how network security matters in the modern digital world in which today's extended enterprises operate.
2. Explain the concept of network trust.
3. What are the three main types of networks that must be considered when defining a security policy?
4. Explain the various methods of attack on a network.
5. Why is security perimeter an important concept? Explain with suitable examples. What considerations should be made in the design of perimeter security?
6. What is an intrusion detection system? Explain the need for having an intrusion detection system in place.

7. Explain the various stages followed by intruders to attack networks.
8. What are the two most well-known conceptual approaches to the design of intrusion detection systems? Compare them in terms of their relative advantages and disadvantages.
9. What are the various categories of intrusion detection systems?
10. What are the characteristics of a good intrusion detection system?
11. Why do organizations perform network penetration tests?
12. Do routers play a role in intrusion detection? Explain.
13. What can organizations do to ensure security of their network routers? Explain with examples.
14. Describe the challenges faced by the intrusion detection systems.
15. What care needs to be taken while implementing intrusion detection systems in organizations?

What is Virtual Private Networks

- VPN is a network of virtual circuits that carries private traffic through public or shared networks such as the Internet or those provided by network service providers.
- VPNs allow a trusted network to communicate with another trusted network over untrusted/public networks such as the Internet.
- VPNs are used primarily to extend an enterprise's internal private network that is intranet across untrusted/public networks.

- They provide the capability to securely convey information across the public network into the corporate network.

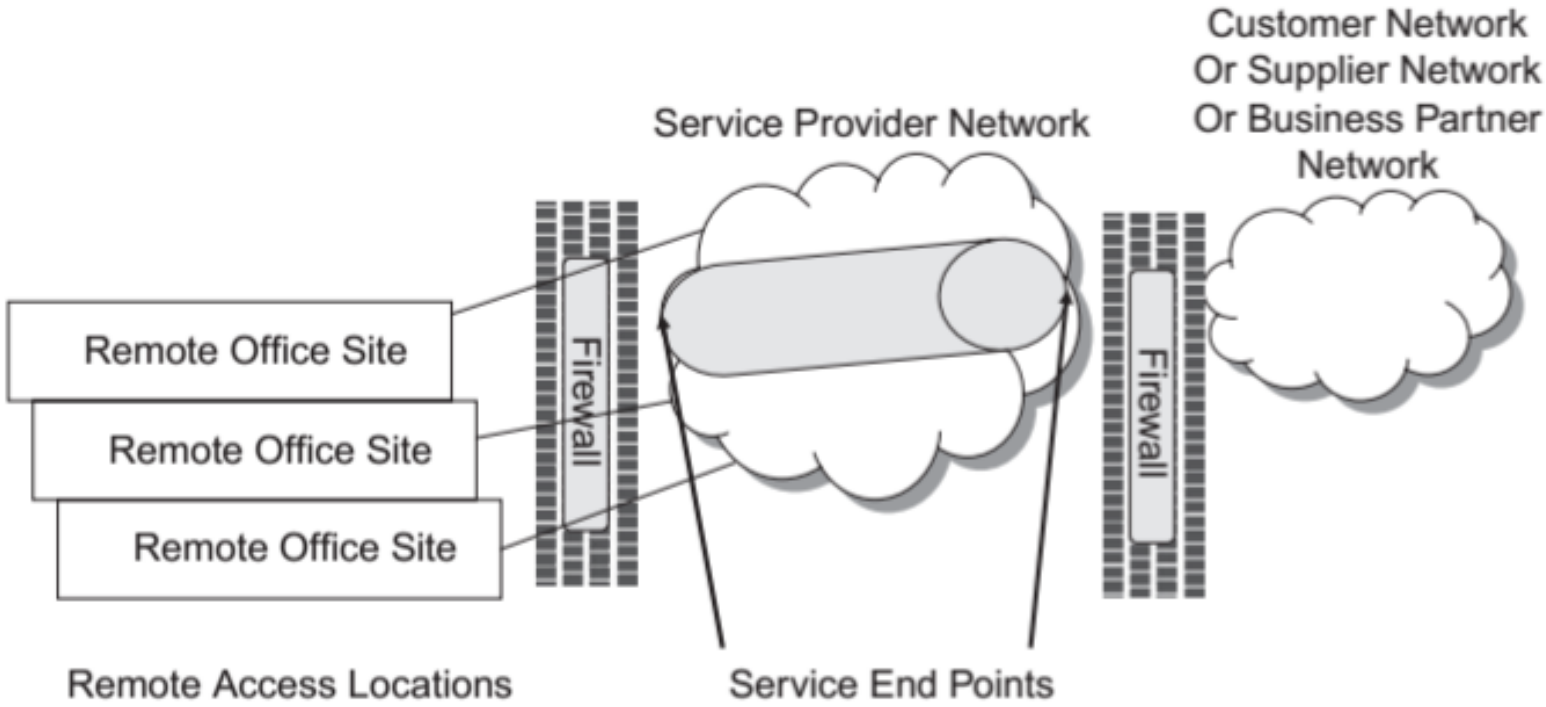


Virtual Private Networks-Need

- With an increasing use of the Internet and a growth in the number of mobile workers, many organizations have moved to VPNs.
- VPNs have become popular because they offer many of the advantages of private networks with a lower cost.
- A well-designed VPN can provide many benefits listed below:
  1. Extends geographic connectivity
  2. Improves security
  3. Reduces operational costs versus a traditional WAN
  4. Reduces transit time and transportation costs for remote users
  5. Improves productivity
  6. Simplifies network topology
  7. Provides global networking opportunities
  8. Provides telecommuter support
  9. Provides a broadband networking compatibility
  10. Provides a faster return on investment than a traditional WAN.

- VPNs have several characteristics:
  - traffic is encrypted to prevent eavesdropping
  - remote site is authenticated
  - multiple protocols are supported
  - connection is point to point
- When two secure networks each protected by a firewall establish a VPN between them, the firewalls at each end of the network encrypt and authenticate the traffic that passes between them

- Same way when a VPN is established between a remote client and a firewall, the traffic between them is encrypted and authenticated.



- Using a VPN, the exchange of data is controlled, secure and validated.
- VPNs provide a secure communication across the Internet.

- Client-to-firewall VPNs allow remote users to have a private and secure communication even when the traffic travels over the Internet.
- However VPNs also introduce a whole new set of security issues and risks for an organization. But with a proper security architecture design, VPNs can offer a number of advantages to the organizations

Use of Tunnelling with VPN

- The word tunnel occurs invariably in the discussion of a VPN and hence it is important to understand it.
- A tunnel is a means of forwarding data across a network from one node to another, as if the two nodes were directly connected.
- This is achieved by encapsulating the data – an extra header is added to the data sent by the transmitting end of the tunnel, and the data are forwarded by intermediate nodes based on this outer header without looking at the contents of the original packet.
- There can be two types of VPNs: secure VPN (SVPN) and trusted VPN

- SVPN uses cryptographic tunneling protocols to provide the necessary confidentiality (preventing snooping), sender authentication (preventing identity spoofing) and message integrity (preventing message alteration) to achieve the privacy intended.
- When properly chosen, implemented and used, such techniques can provide secure communications over unsecured networks.
- A trusted VPN does not use cryptographic tunneling; instead, it relies on the security of a single provider's network to protect the traffic.
- Tunneling is an important concept with respect to VPNs
- Tunneling is the transmission of data intended for use only within a private, usually corporate network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network.

- Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units so that the private network protocol information appears to the public network as data.
- Tunneling allows the use of the Internet, which is a public network, to convey data on behalf of a private network.
- Thus VPN is a group of one or more secure IP tunnels.

Authentication Mechanisms

- A VPN involves two entities: the protected or inside network which provides physical and administrative security to protect the transmission and a less trustworthy that is untrusted, outside network or segment usually through the Internet.
- Generally a firewall sits between a remote user's workstation or client and the host network or server.
- As the user's client establishes the communication with the firewall, the client may pass authentication data to an authentication service inside the perimeter.
- A known trusted person, sometimes only when using trusted devices, can be provided with appropriate security privileges to access resources not available to general users.

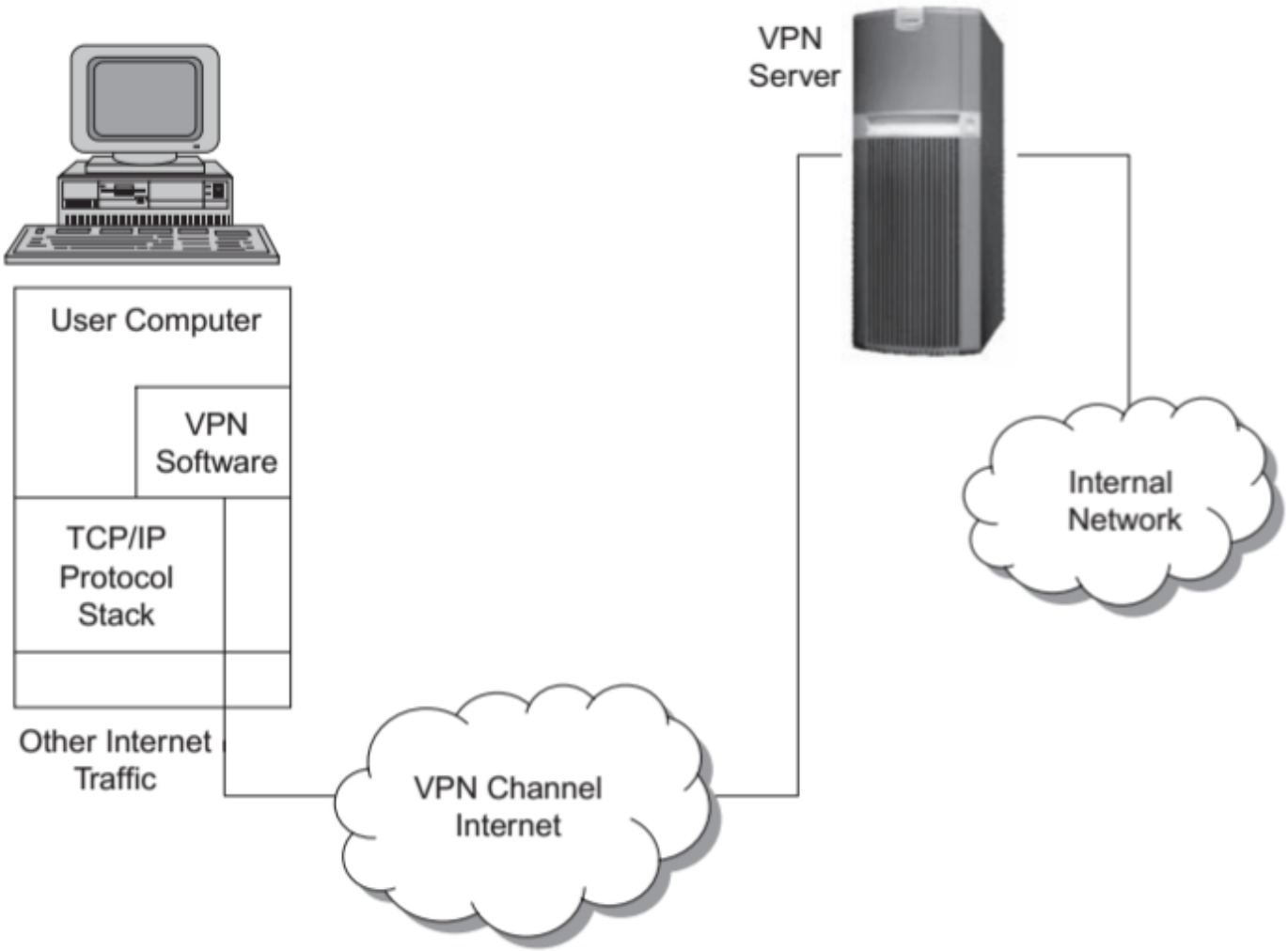
- For better security, many VPN client programs can be configured to require that all IP traffic must pass through the tunnel while the VPN is active.
- From the users perspective, this means that while the VPN client is active, all access outside their employer's secure network must pass through the same firewall as would be the case while physically connected to the office Ethernet.
- This reduces the risk that an attacker might gain access to the secured network by attacking the employee's laptop: to other computers on the employee's home network, or on the public Internet, it is as though the machine running the VPN client simply does not exist.
- Such security is important because other computers, local to the network on which the client computer is operating, may be untrusted or partially trusted.

- Even with an organization's internal network that is protected from the outside Internet by a firewall, people who share it may be simultaneously working for different employers over their respective VPN connections from the shared internal network.
- Each employer would therefore want to ensure that their proprietary data are kept secure, even if another computer in the local network gets infected with malware.
- If a travelling employee uses a VPN client from a wifi access point in a public place, such security is even more important.
- However the use of internetwork packet exchange (IPX)/sequenced packet exchange (SPX) is one way for the users to be able to access local resources.

Types of VPNs and their Usage

- There are many ways to set up a VPN. The most popular approaches are user VPNs used for remote access and site-to-site VPN to communicate with other offices.
- The difference between them is the way the two types are used, not because of the way traffic is segregated by each type.
- **Remote Access VPN or User VPN**

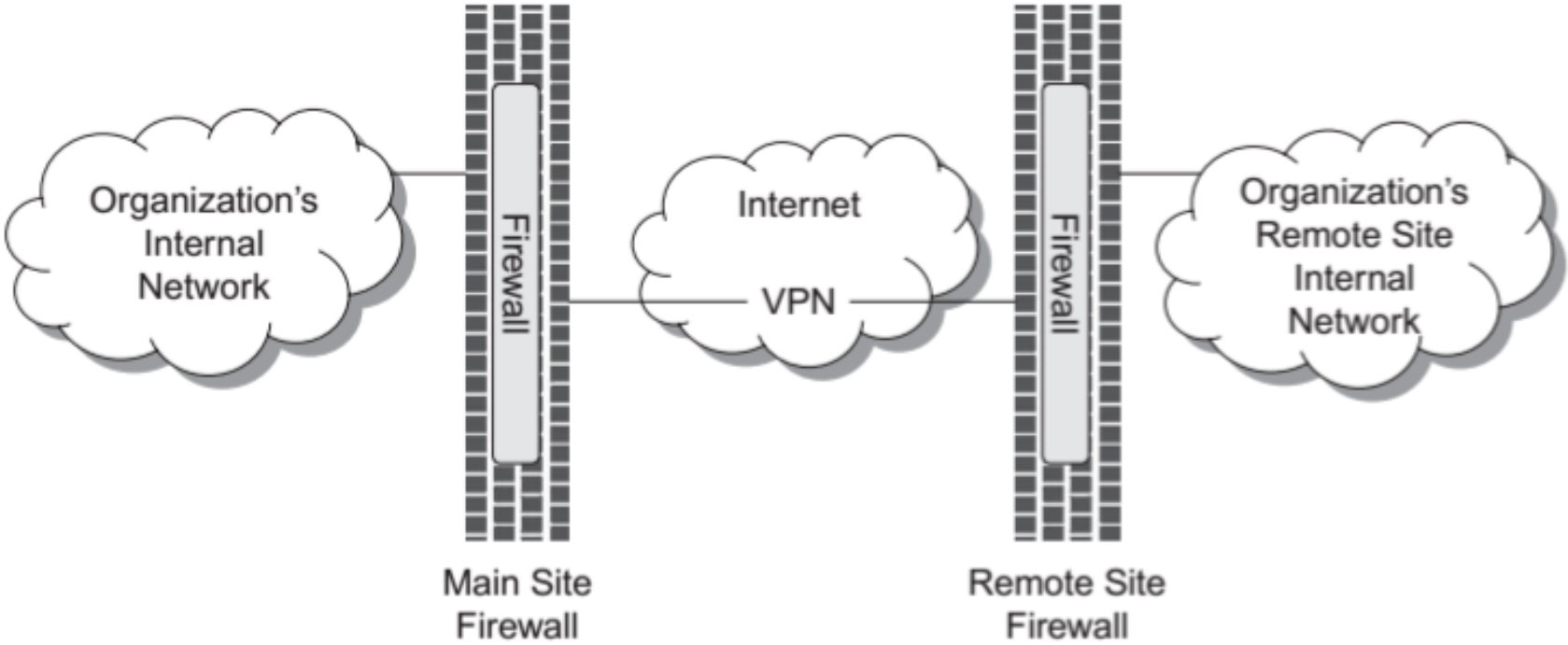
- Let us understand this with a simple example. Remote access VPN/user VPN configuration is shown in Figure



- As we can see, a remote access VPN or a user VPN is a VPN between an individual user machine and an organization site or network.
- It is used by employees who travel and yet wish to connect to their organization's network or by employees who work from home.
- The VPN server may be the organization's firewall or may be a separate VPN server.
- In this type of VPN, the user connects to the Internet via a local ISP dial-up, digital subscriber line (DSL) or cable modem and initiates a VPN to the organization site via the Internet.
- Obviously, the network speed will be slower because the limiting factor will be the user's Internet connection.

- A remote access VPN offers two primary benefits: mobile employees, that is, those employees who frequently travel for work and can have access to e-mails, information assets on an organization's network and other internal systems wherever they are without the need for expensive long-distance calls to dial-up servers.
- Employees who work from home can have the same access to network services as employees who work from the organization facilities without the requirements for expensive leased lines.
- **Site-to-Site VPN**
- This is also known as the intranet site-to-site VPN.
- It is useful when an organization may not have a need for 'go-any-where-dial-up access' to the network, but instead wants satellite offices, perhaps even in other countries, to be able to communicate and share data with offices in other countries and the home office.

- Site-to-site VPN setup is illustrated in below Figure



- An organization with small remote offices can create a virtual network that connects all remote offices to the central site or even with each other at a significantly reduced cost.

- A site-to-site VPN can be thought of as a virtual chain with removable links, with the various anchor points being the satellite and home offices.
- Using the Internet, a satellite office can initiate their encryption security to put the connecting link in place, making a connection between their LAN and the head quarter's LAN.
- Site-to-site VPNs can be one of the following two types:
  1. **Intranet-based VPN:** If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect one LAN to another LAN.
  2. **Extranet-based VPN:** When a company has a close relationship with another company then they can build an extranet VPN that connects LAN to LAN and that allows all of the various companies to work in a shared environment.

VPN Technologies and Architecture

Configurations for Virtual Private Networks

-

Security Concerns in VPN

Tutorial 14

1. Using suitable diagram(s) explain what virtual private networks are and why do organizations need them.
2. Explain the crucial role of VPNs in today's net-centric digital enterprises.
3. In the context of security, how do tunnelling protocols work for VPNs? Why is authentication important?
4. What are the business scenarios under which different kinds of VPNs get used?
5. What are the various VPN technologies available today? Explain.
6. Describe the various well-known VPN architectures as discussed in the due course.

7. In the light of what you have learned, provide a comprehensive view of parameters that put forth the strong need for VPN security.

Thank you

Please send your feedback or any queries to **akyadav1@amity.edu**
You can contact me on **+91 9911375598**