UNIT 14 CYBER SECURITY, RISK MANAGEMENT,COMPLIANCE AND AUDIT

Objectives

After reading this unit you should be able to

- Understand the concept of cyber security governance,
- discuss about risk management and compliance
- Understand various types of security systems that are included in system Audit

Structure

14.1 INTRODUCTION

An effective cyber security governance is of paramount importance to successfully manage cyber security of an organization. It primarily deals with cyber security policies, the roles and responsibilities of individuals and overall risk appetite of the organization and the cyber security compliances, which are regulatory, contractual and even legal in nature. Hence, cyber security governance, risk management and compliance go hand in hand and are often represented as GRC trio.

The cyber security policy is followed by supporting framework, procedures and processes. The processes finally boil down to controls. Audit is a function which examines the adequacy of cyber security policy and effectiveness of the laid down controls and ensure that the defined controls are properly followed.

14.2 CYBER SECURITY GOVERNANCE

Cyber security governance provides a strategic view of how an organisation controls its security, including defining its risk appetite, building accountability frameworks, and establishing who is responsible for making decisions.

Cybersecurity governance involves process of establishing the architecture that ensures a company's security programs;

- align with business objectives,
- comply with regulations and standards (such as ISO and PCI security standards),
- defining roles and responsibilities at various levels in the organization and,
- achieve objectives for managing security risk and ensuring compliance.

The cyber security policy should be aligned with business objectives and business policy of the organization. This is the first and foremost requirement of cyber security policy. This is followed by defining roles and responsibilities of individuals in the organization and complying with the internal policies, regulations, contractual and legal obligations.

14.2.1 Six Principles of Cyber Security Governance

Cyber Security Governance in an organization is generally described by way of six principles. Let us have a look at them.

1. **First Principle: Building a culture of cyber resilience**

   Resilience is the ability of an organization to attain normalcy after an adverse incident. Cyber resilience is the ability of an organization to enable business acceleration (enterprise resiliency) by preparing for, responding to, and recovering from cyber threats. A cyber-resilient organization can adapt to known and unknown crises, threats, adversities, and challenges. The ultimate goal of cyber resiliency is to help an organization thrive in the face of adverse conditions.

2. **Second Principle: Establishing roles and responsibilities**

   Clearly defining an organisation's cyber security roles and responsibilities is an important step to achieve effective cyber security governance. This also includes adequately empowering the individuals to take decisions whenever needed. For instance, in case of an incident, well-documented crisis management plan clearly states who is responsible for which function while addressing the crisis.

3. **Third Principle: Holistic risk management**

   Effective cyber security risk management is a core aspect of governance and must be embedded within an organisation's overall risk framework. A separate section in this unit is exclusively dedicated to risk management and monitoring.

4. **Fourth Principle: Cyber security collaboration**

   This can be achieved by establishing a cyber security committee and a working group with representation from all the key stakeholders across the business.

5. **Fifth Principle: Set the direction of investment decisions.**

   Information security investments are intended to support organizational objectives. Security governance entails ensuring that information security is integrated with existing organization processes for capital and operational expenditure, for legal and regulatory compliance, and for risk reporting.

6. **Sixth Principle: Measuring resilience**

The effectiveness of cyber security activity should be accurately measured and reported. Measurement and reporting provide the basis for continuous improvement. Devising suitable KPIs (key performance indicators) and monitoring them on a continuous basis helps in this. For instance, as per the policy, if all the systems in the network should have up-to-date anti-malware, actual achievement may be 98% on any day-the KPI in this respect is 98%. Regular VAPT (vulnerability assessment and penetration tests) exercises also help in measuring some of the KPIs.

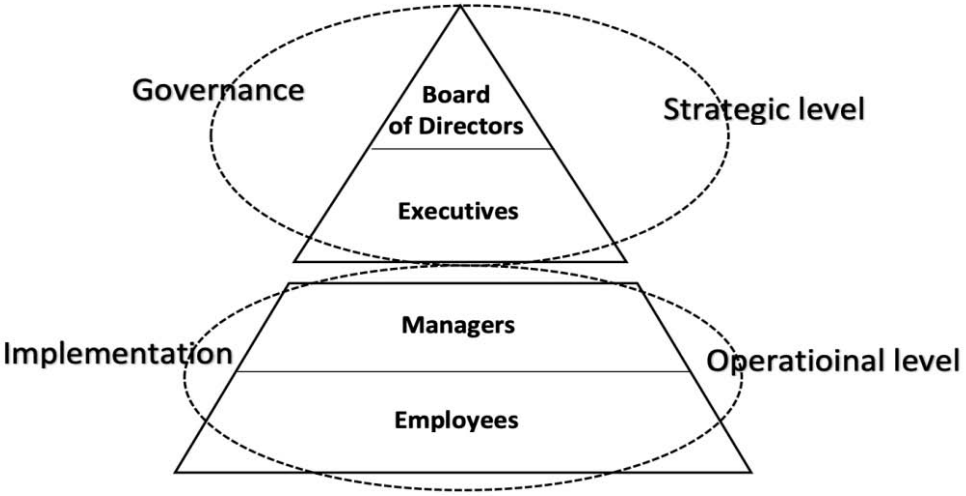
14.2.2 Cyber Security - Roles and Responsibilities

The top management or the Board is accountable for cyber security in an organization and the cyber security policy should be approved by the Board. Accountability is ultimate answerability, which is different from mere responsibility. For instance, when the IT Department is assigned with the job of implementing certain information security controls in a system, say Mobile Banking, they are just responsible for implementing so, whereas the accountability of ensuring the required controls are in place lies with the system or asset owner, i.e., the business owner of Mobile Banking. Whereas the accountability with respect to ensuring cyber security controls in a specific asset lies with the respective business owners, the accountability for overall information security of the organization always lies with the top management/the Board.

The information security policy is then followed by framework and procedures. The procedures are ensured by devising suitable cyber security controls. The adequacy and follow up of such controls is examined during the process of audit and the observations are reported to a Board level committee. This cycle ensures proper cyber security governance.

The Head of Information Security, who is generally called the Chief Information Security Officer (CISO), is responsible for finalising the information security policy upon consulting all the unit heads, Head of IT and other stake holders, which will be ultimately approved by the Board. The information security policy is then followed by framework and procedures. The procedures are ensured by devising suitable cyber security controls. So devised policy, framework, processes and controls are communicated to all the stakeholders in the organization. Subsequently, during the process of audit, the adequacy and practice of such controls is examined and the observations are reported to a Board level committee. This cycle ensures proper cyber security governance.

Figure 14.1 Cyber Security Governance Structure



CISO is also responsible for risk assessment, continuous risk monitoring, regulatory compliance and periodic security status report to the Board.

Three lines of defense: Apart from governance, there are three lines of defense in ensuring cyber security in an organization.

i. The first line of defense is the IT security team, and asset owners who actually ensure implementation of the required security controls in systems.

ii. The second line of defense is the CISO and his team who take care of the cyber security policy, risk management, compliance and periodical reporting of the security status to the Board.

iii. The third line of defense is Audit.

14.3 RISK MANAGEMENT

Risk management, in the context of information security, is the practice of minimising risks to organizational operations (e.g., mission, functions, image, and reputation), organizational assets and persons. Managing risk is one of the most important segments of information security. Risk management involves risk identification, risk analysis, risk evaluation and risk treatment.

14.3.1 Steps in Risk Management

There are four major steps involved in risk management of an organization. They are identification of risk, analysis of risk, evaluation of risk, response to risk and monitoring risk.

Identify

Identification of risks involves identifying vulnerabilities in each of the assets of organization and the threats that might exploit these vulnerabilities and the probability of such exploitation. The risk associated with each information asset is arrived at accordingly.

Analyse

Analyse the severity of each risk by assessing how likely it is to occur and how significant the impact might be if it does. This step considers financial risk, reputational risk, regulatory risk and operational risk. The combined impact of these risks is called Business Impact Analysis (BIA).

Evaluate

The step follows above-mentioned BIA exercise and involves evaluation of how each risk fits within the organization's risk appetite, which helps in prioritising the risks and finding respective ways to treat each risk.

Respond

This step involves making decision on how to respond to each risk. There are generally four options:

- **Treat (mitigate) the risk** – The risks that fall in this category are those which can be mitigated by taking suitable preventive measures and security controls and modifying the risk's likelihood and/or impact.
- **Tolerate (accept) the risk** – In the cost-benefit analysis, if the impact of risk is less than the benefit derived out of the asset, and if there are no ways to mitigate the risk, the organization may take a call to accept the risk.
- **Terminate (avoid) the risk** – As in above case, if there are now way to mitigate the risk and but the cost / impact of risk is far more than the benefit emanated from the asset, the organization may avoid the risk entirely by ending or completely changing the activity causing the risk.
- **Transfer (insure) the risk** – After managing the risk in the above three steps, there is generally left some residual risk which is left un-managed. Such risk may be shared with another party, usually by outsourcing or taking out insurance. Cyber insurance is one such example.

Monitor

Risk management is a never-ending process. Within this process, implemented security measures are monitored, and reviewed on a regular basis to ensure that they function as intended and that changes in the environment have rendered them ineffective. Business needs, vulnerabilities, and threats can all change over time.

Regular information system audits (IS audits) should be scheduled and conducted by an independent party, i.e. someone not responsible for the implementations or day-to-day management of Information Security. The role of IS Audit is discussed in the section 14.5.

14.3.2 Major Types of Cyber Security Risks faced by Banks

In Banks, data breaches generally result in following types of risks.

- **Financial Risk** – Banks being financial institutions, the data breaches often lead to financial risks. Money stolen by attacking payment systems

like ATM, SWIFT or the money demanded by attacker after a successful Ransomware attack or cost of failed operations during a DDoS attack, are some of the examples of financial risk.

- **Reputational Risk –** Trust of the customers that lost or reduced due to a data breach is reputational risk. For institutions like Banks, reputational risk is one of the risks of paramounce important as Banks business basically runs on trust.
- **Compliance Risk -** Non-compliance can be with Bank's own policies, mandatory requirements by regulators, viz., RBI and GoI and Legal and other Contractual obligations. Non-compliance with own policies may lead business loss and so with regulatory requirements may result in Regulator's wrath which may even lead to punitive measures. Legal and contractual non-compliances may lead to legal implications.
- **Operational risk** – This is the risk of losses caused by flawed or failed processes, policies, systems or events that disrupt business operations. Employee errors, criminal activity such as fraud, and physical events are among the factors that can trigger operational risk.
- **National Security Risk –** As banking is one of the critical systems of the nation's economy, a cyber security incident in any of the systemically important banks will also pose national security risk.

Activity 14.1

Explain the cyber security governance structure of your bank or any other organisation.

……

……

……

……

……

……

14.3.3 Business Impact Analysis (BIA)

It may be noted that the first four risks discussed above in section 14.3.2, i.e., financial risk, reputational risk, regulatory risk and operational risk, are considered in computation of business impact (BI) through the exercise of business impact analysis (BIA) for each asset. This is especially with respect to banking industry's systems. For instance, if an E-Mail system of a bank is down for a few hours on account of an incident, the incident's BI may be relatively lower compared to an incident causing disruption in Mobile banking or Internet Banking services. The BI will still be far more if the whole core banking system is disrupted, because all banking services will come to a grinding halt.

Information system Development

- An information system goes through a series of phases from conception to implementation.
  - This process is called the Software-Development Life-Cycle.
- Software-development life-cycle is used to facilitate the development of a large software product in a systematic, well-defined, and cost-effective way.

Secure information system development

- Secure information system are developed by integrating risk analysis and management activities at the start of the system development (SDLC) and continuing throughout.
- Security can be integrated into any (and ideally all) of these phases.
- In most organizations that use a variant of the waterfall model,
- security is included with the toll gate style mentioned previously, often at the end of each phase before moving to the next one.

Secure information system development

- Integrating security at the initial phase
- Integrity security at the Development Phase
- Integrity security at the Implementation Phase
- Integrity security at the Maintenance Phase
- Integrity security at the Disposal Phase

Integrating Security at Initial Phase

- Initial phase is where the decision is taken to develop a system.
- In this phase security consideration primarily involves business risk related to confidentiality, integrity and availability.
  - security is looked at more in terms of business risks with input from the information security office.
  - This phase include initiating project security planning, processes, assessing the business impact of an activity

Key security activities of Initial Phase

- Security must be implemented from Initial phase of business requirements in terms of confidentiality, integrity, and availability;
- Define the threats and possible security constraints for business.
- Determination of information categorization.
- Determination of any privacy requirements.

Integrating Security at Development Phase

- Development phase is where the shape of the information system is actually built.
- Primary security activities at development stage of system development include risk assessment, security control selection and documentation.
- Role of the Phase :
  - Security **architecture design preparation**,
  - security **control development**,
  - security **documentation and development**

Key security activities of development phase

- Conduct the risk assessment and use the results to supplement the baseline security controls;
  - Analyze security requirements;
  - Perform functional and security testing;
  - Prepare initial documents for system certification and accreditation; and
  - Design security architecture.

Integrating Security at Implementation Phase

- Implementation/Assessment is the third phase of the SDLC.
- During this phase, the system will be installed and evaluated in the organization's operational environment.

Key security activities of Implementation phase

- Integrate the information system into its environment;
- Plan and conduct system certification activities in synchronization with testing of security controls; and
- Complete system accreditation activities.

Integrating Security at Maintenance Phase

- In this phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced.
- The operational system is periodically assessed to determine how the system can be made more effective, secure, and efficient.
- Operations continue as long as the system can be effectively adapted to respond to an organization's needs while maintaining an agreed-upon risk level .

Key security activities of maintenance phase

- Conduct an operational readiness review;
- Manage the configuration of the system ;
- Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls; and
- Perform reauthorization as required.

Integrating security at the Disposal Phase

- Disposal phase is the final stage in the SDLC.
- where the legacy systems are replaced by newer systems.

Application development security

- Secure development of application is a practice to ensure that the code and processes that go into developing applications are as secure as possible. Secure development entails the utilization of several processes, including the implementation of a Security Development Lifecycle (SDL) and secure coding itself.
- Some of the primary issues to the secure development of applications are as follows
- Less trained/skilled developers
- Difficulty of finding the right information related to specific security measures for particular applications.

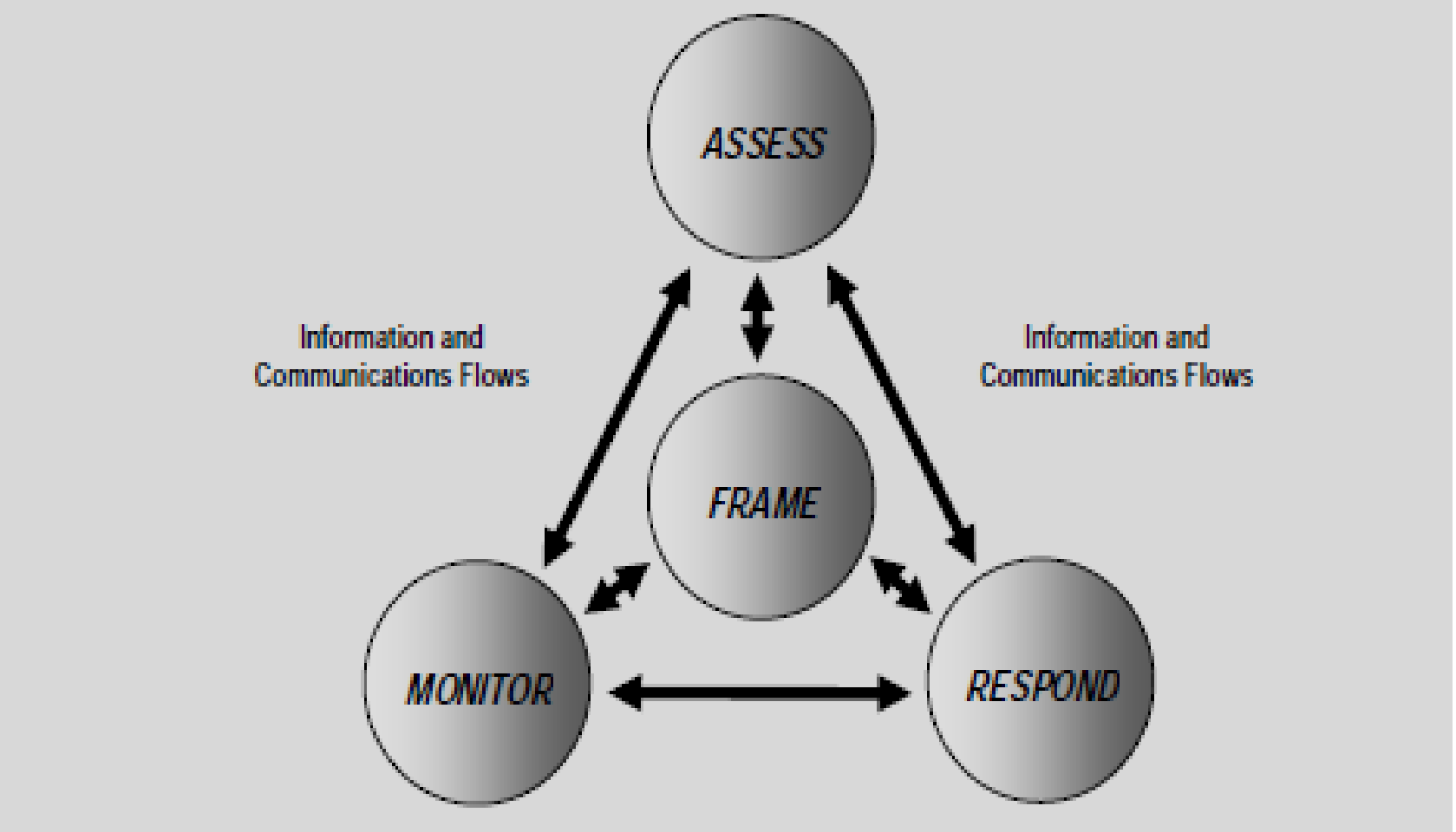
Information security Governance and Risk Management

- Information security needs to be governed and managed properly because **information has become one of the most critical business driver in recent years**.
- Information systems are the subject to serious threats that can have adverse effect on the organizational operations.

Risk Management

Risk management is the continuing process to identify, analyze, evaluate, and treat loss exposures and monitor risk control and financial resources to mitigate the adverse effects of loss.

Risk management Process



Risk management

- **Assessing:** assessment of risk means to analyze the level of risk and the level of security provided with our organization.

- **Framing:** Framing the risk means to sense the threat and inform all the related activities that execute in a sequential manner to be ready to control and avert a possible damage.
  - In this activity we analyze the possible risk associated with the security of information system and organization, and then try to define certain action for individual case.
- **Monitoring:** It involves continuously checking the information system and keeping an eye on other threat and vulnerability that maybe encountered by the organization.
  - It also helps in analyzing whether the system is continuously secure or not.
- **Responding:** Responding to risk means to take preventive or corrective measures so that system can kept protected from any kind of threats, whether internal or external.

Differences between Risk Management, Risk Assessment, and Risk Analysis

Risk Management

Risk management is the continuing process to identify, analyze, evaluate, and treat loss exposures and monitor risk control and financial resources to mitigate the adverse effects of loss.

Risk Assessment

Risk assessment includes processes and technologies that identify, evaluate, and report on risk-related concerns. the risk assessment process is a “key component” of the risk management process. it is primarily concerned with the Identification and Analysis phases.

Risk Analysis

Risk analysis can be considered the evaluation component of the broader risk assessment process, which determines the significance of the identified risk concerns.

Security architecture and Design

- Security Architecture and Design of a system means a bundle of following components:-hardware, software and operating system and how to use those component to design, architect, and evaluate secure computer systems

- Security Architecture and Design is a three-part domain.

1. The first part covers the **hardware and software** required to have a secure computer system
2. The second part covers the **logical models required to keep the system secure**
3. and the third part covers **evaluation models** that quantify how secure the system really is.

Secure System Design Concept

- **We can design a secure system by implementing software and hardware specifically and including following principles**

  - **Layering**
  - **Abstraction**
  - **Security domains**
  - **The ring model**
  - **Open-closed systems**

• Layering

- Layering separates hardware and software functionality into modular tiers.
- A generic list of security architecture layers is as follows :

1. Hardware (bottom layer)

2. Kernel and device drivers

3. Operating System

4. Applications (Top Layer)

- **Abstraction:** Abstraction hides unnecessary details from the user.
- Complexity is the enemy of security:
  - the more complex a process is, the less secure it is. That said, computers are tremendously complex machines.
- Abstraction provides a way to manage that complexity.
  - For example ,while music is being played from a file through the speaker of the computer system. The user is only concerned with playing of music just with click without knowing the internal working of music player.

- **Security Domains :** A security domain is the list of objects a subject is allowed to access.
  - With respect to kernels, two domains are user mode and kernel mode.

  - **Kernel mode (also known as supervisor mode)** is where the kernel lives, allowing low-level access to memory, CPU, disk, etc. It is the most trusted and powerful part of the system.

  - **User mode** is where user accounts and their processes live. The two domains are separated: an error or security lapse in user mode should not affect the kernel.

- **The Ring Model:**
- The ring model is a form of CPU hardware layering that separates and protects domains (such as kernel mode and user mode) from each other.
- Many CPUs, such as the Intel 86 family, have four rings, ranging from ring 0 (kernel) to ring 3.

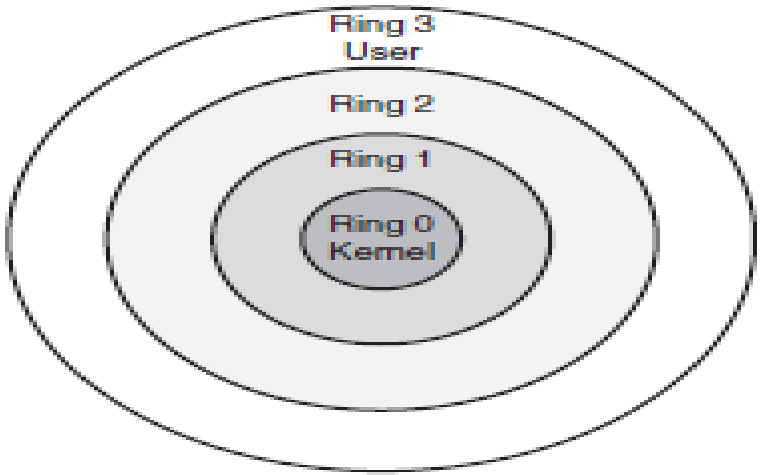
- The rings are (theoretically) used as follows:

  Ring 0: Kernel

  Ring 1: Other OS components that do not fit into ring 0

  Ring 2: Device drivers

  Ring 3: User applications

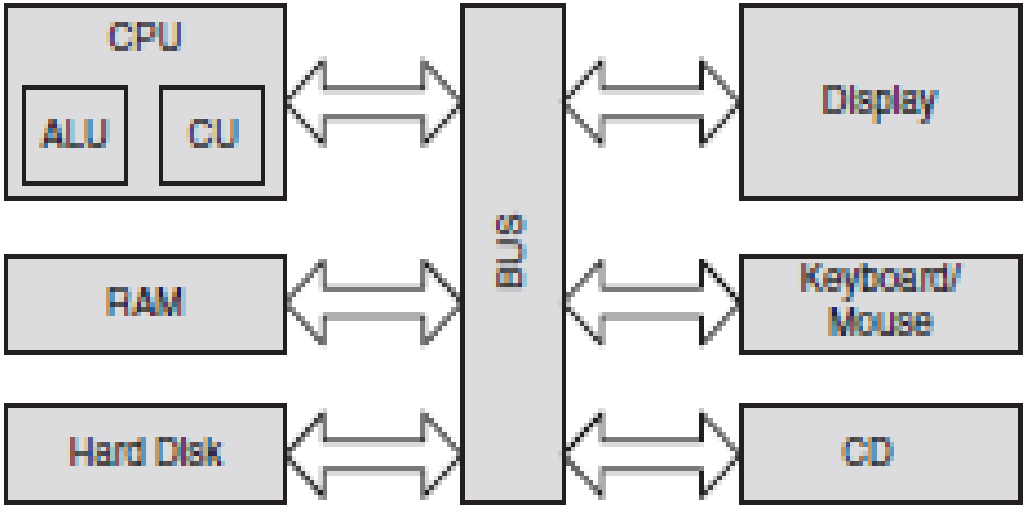


- **Open and Closed Systems:**
- **An open system** uses open hardware and standards, using standard components from a variety of vendors.
  - Ex - Assembled Desktop computer

- **Close systems-** only use proprietary hardware or software from specific vendor.
  - Ex- Branded Desktop (HP)

Secure hardware architecture

- Secure Hardware Architecture focuses on the physical computer hardware required to have a secure system.
- The hardware must provide confidentiality, integrity, and availability for processes, data, and users.



Security issues in 1.hardware, 2.data storage and 3.downloadable device

- Securing computer system means to protect all of its components that includes
  - hardware, software, storage devices, operating system and peripheral devices.
- Each component has its own vulnerability or weakness.
  - Hardware parts can be stolen and destroyed .
- Security of every component of the system is equally important.
  - We need to be able to control our computer system completely so that the information asset can be protected.

Security Issues in Hardware

- Hardware is the component on which the entire computer system is based this include processor, hard drive and monitor.
- Hardware mainly faces security issues related to stealing, destruction, gaining unauthorized access and breaking the security code of conduct.
  - Any breaking of code of conduct needs proper security measures such as placing the hardware with your controlled environment.

Counter Security Measures in hardware

To secure H/W from unauthorized access, following mechanism should be used-

- Biometric access control.
- Authentication token (entry via smart card).
- Radio Frequency Identification (RFID).
- Use VPN to provide complete security over internet.
- Use strong passwords.
- Provide limited access to the devices.

2. **Security Issues with Storage Devices**

- Data storage devices are used to save information.
- Devices such as compact disk(CD), digital versatile disk(DVD), memory cards, flash drives etc.

2. Security Issues with Storage Devices

- **The main issue faced by these devices is-**
  - **Loss and theft of data.**
  - **Improper disposal of data.**
  - **Introduction to malwares in your system.**
  - **Denial of data i.e., attack on availability of data.**

- **All these issues can be overcome by using following measures-**
  - **Making people aware of the various kinds of attacks.**
  - **Educating people regarding various cyber laws of the nation.**
  - **Making the people understandable the importance of security.**
  - **Implement certain policies and procedures that provide security for the storage devices and data.**

3. Security Issues with Downloadable (Peripheral) devices (PD)

- E.g. PD-USB: PDA, External Hard Drive
- Security Issues related to them are-
  - Stealing of data.
  - Destruction of data.
  - External attacks(virus etc.).
- Measures include:
  - Protection of data from theft/ manipulation
  - Protection of devices from being stolen or destroyed
  - Protection of environment from undesired access.

Physical Security of IT Assets

- An IT asset is a piece of software or hardware within an information technology environment.
- Tracking of IT assets within an IT asset management system can be crucial to the operational or financial success of an enterprise.
- IT assets are integral components of the organization's systems and network infrastructure.Security of data and asset is equally important.
- Physical security of our asset, especially the IT asset is also very important.
  - there are several issues that need to be countered in order to apply total security control.
- We may need to lock and other access control techniques to protect our asset from unwanted users.

Physical Security of IT Assets(Threats)

- **Threats for physical security are as follows:-**

(1) Physical access exposure to human beings : Organizations own employees are one of the main factors to cause physical security threats.

- Can be controlled through
  - strong authentication mechanism
  - restricted use of resources
  - restricted area and building
  - Proper standards for verification and validation of user identity.

(2) **Physical access exposure to natural disasters:-** Natural disasters may destroy your computer systems or all data storage systems and might interrupt your network.

- for example fire, lightening, or electronic interruption
- Can't be controlled, but recovery measures could be taken.

Physical Security of IT Assets(Measures)

- **Measures** to ensure physical security of IT assets-

(1)Physical access controls

- Through photo IDs, biometric authentication systems, entry logs, magnetic locks using electronic keycard, computer terminal locks.

(2)Electronic and visual surveillance systems

- Through closed circuit television(CCTV), RFID sensors
- CCTV cameras are also called the third eye because if human being missed noticing some people entering a restricted zone, these cameras could capture the event or photos.

(3) Intrusion Detection Systems(IDS):-

IDS is a way of dealing with unauthorized access to information system assets.

Backup Security Measures

- Following practices should be performed for maintaining proper data backup security-
  - Assigning responsibility, authority and accountability.
  - Assessing risks.
  - Developing data protection processes.
  - Communicating the processes to the concerning people.
  - Executing and testing the process.

1. Assign Accountability, Responsibility and Authority

- Make storage security a function of overall information security policies and architecture
- Divide duties where data is highly sensitive.
- ensure that the person authorizing access is not the person charged with responsibility for execution.

2. Assessing Risk

- Perform a Risk Analysis of the Entire Backup Process.
- Execute a Cost/Benefit Analysis on Backup Data Encryption
- Identify Sensitive Data.

3. Develop Data Protection Process

- Adopt a Multi-Layered Security Approach

. Authentication: Authorization: Encryption Auditing:

- Copy Your Backup Tapes

4. Communicating the processes to the concerning people

- it is important to ensure that the people responsible for carrying out its security are informed and trained.
- Security policies are the most important aspect of assigning accountability, responsibility and authority.

5. Executing and testing the process

- Once the end-to-end plan has been developed, defined and communicated to the appropriate people, it is time to begin execution and testing process.

Payment Systems

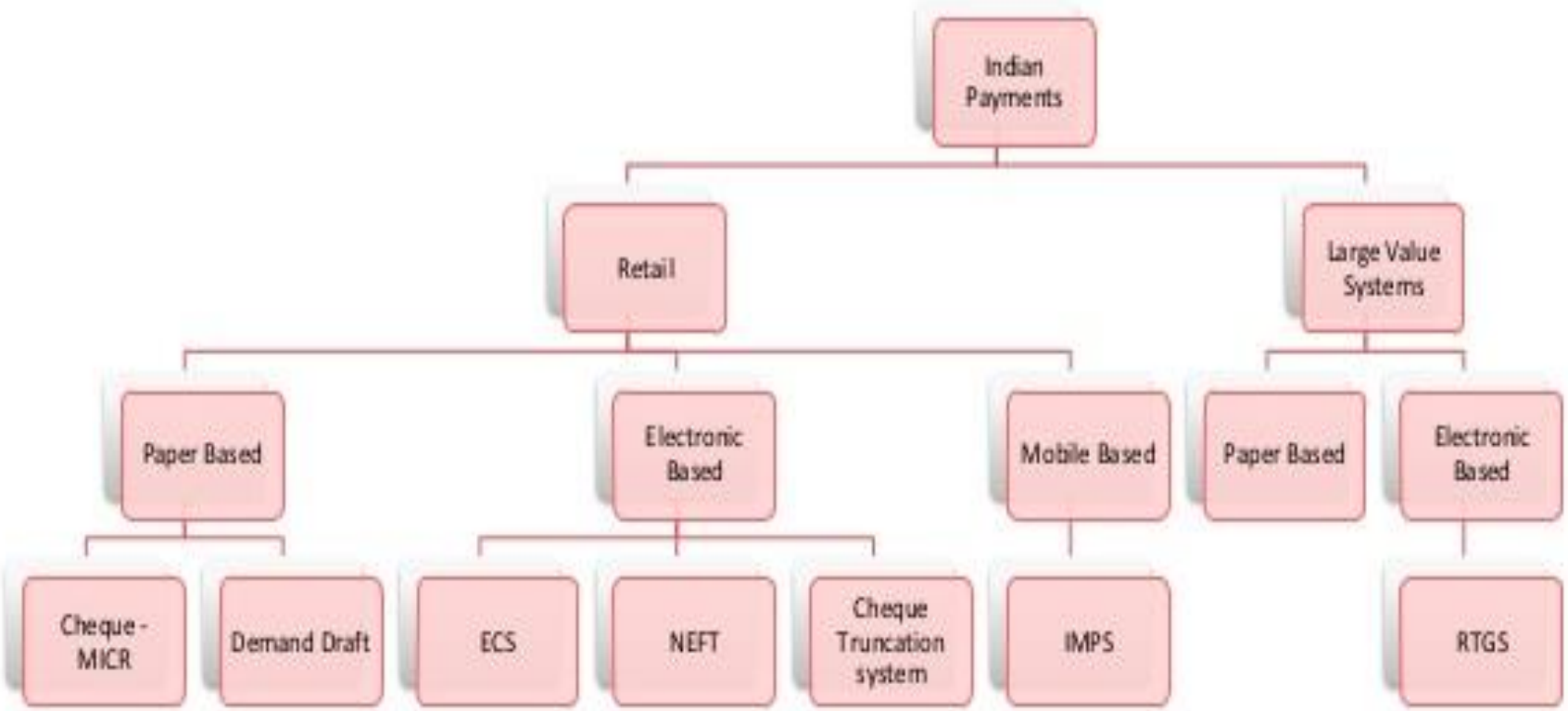
Definition:

- Financial system supporting transfer of funds from payers to payee/s.

Role:

- Payment systems to provide safe, efficient, affordable, easily accessible and robust payment services
- Payment systems help in the smooth flow of money in the economy thus increasing the liquidity in the hands of the customer enhancing his purchasing capacity
- Payment systems would also help minimize cases of fraud, use of counterfeit notes and black money

Classification



Electronic Clearing Service (ECS)

- It was introduced by RBI
- Provided an alternative method of effecting bulk transaction
- Avoided need for issuing and handling paper instrument
- User has to submit the mandate to the bank. (E.g.: MICR -Cancelled Cheque)
- No Transaction limit
- There are two types of ECS:
  - ECS – Debit - There is multiple debit from vast section of people and corresponding single credit entry. E.g.: Bill payment
  - ECS - Credit - Electronic fund transfer from one account to many transactions transfers. E.g.: Salary Payment

Real Time Gross Settlement (RTGS)

- Introduced by RBI in 2004
- RTGS systems are managed by RBI.Transfer anywhere within India.
- Funds for > Rs 2 lakh to be transferred through RTGS. Lower funds cannot be transferred . Upper Transaction limit set by individual bank.
- Payment instruction handled individually.
- Payment is final and irrevocable and the receiver can utilize the funds immediately
- RTGS Timings:
  - Weekdays : 9:15 AM to 4:15 PM
  - Saturday : 9:15 AM to 1:15 PM ; No settlement on Sundays and Holidays
- Service Charge applicable to customer
- Steps for Transaction : Register Payee & Transfer Funds

National Electronic Funds Transfer System (NEFT)

- It was launched by RBI in 2005
- It permits to transfer funds of lower value. Neither lower limit nor upper limit
- Transfer anywhere within India
- Operate on a deferred net settlement (DNS) basis which settles transactions in batches.
- NEFT Timings:
  - Weekdays: 12 times every hour from 8:00 AM to 7:00 PM
  - Saturday : 6 times every hour from 8:00 AM to 1:00 PM
  - No transfer on Sundays and Holidays
- Service Charge is applicable to the Customer
- Steps for Transaction : Register Payee & Transfer Funds

InterBank Mobile Payment Service (IMPS)

- Initiated by NPCI along with 4 Member banks – SBI, Bank of India, Union Bank of India and ICICI Bank
- Launched on 22nd November 2010
- Service available to Public
- To participate in IMPS, Banks should have approval from RBI
- Available with 54 Banks

IMPS™
INTER BANK MOBILE PAYMENT SERVICE

Objective of IMPS

- Make a Mobile as Channel
- Available – 24 X 7 X 365
- No more sharing of bank account details
- Instant
- Payment – Simple, convenient
- Time & cost saving
- Safe & Secure
- Immediate Confirmation
- Use existing payments infrastructure (existing ATM networks)

IMPS™
INTER BANK MOBILE PAYMENT SERVICE

Comparison with other payments

	IMPS	NEFT	RTGS
Time to Process	Instantaneous	Operates every one hour	Instantaneous
Availability	24 X 7 X 365	Available in working hours	Available in working hours
Restriction on Amount	Maximum 5 Lakh	Maximum 5 Lakh	> 2 Lakh Maximum 5 Lakh
Service Charge	Tiered Charges	Tiered Charges	Tiered Charges
Geographic spread	Supported by 54 Banks	78,000 enabled bank branches	78,000 enabled bank branches
Channels	Mobile – SMS, Mobile Applica USSD Internet	Internet, Branch	Internet, Branch
Reliability	Low due to Mobile Service	High	High

What is Unified Payment Interface ?

Objective of a unified payments system is to offer an architecture and a set of APIs on top of existing systems to facilitate online instant payments and financial inclusion.

Push & Pull Payments

- The payments can be both sender (payer) and receiver (payee) initiated and are carried out in a secure, convenient, and integrated fashion

Easy Instant Payments

- The unified payment system is expected to further propel easy instant payments via mobile, web, and other applications

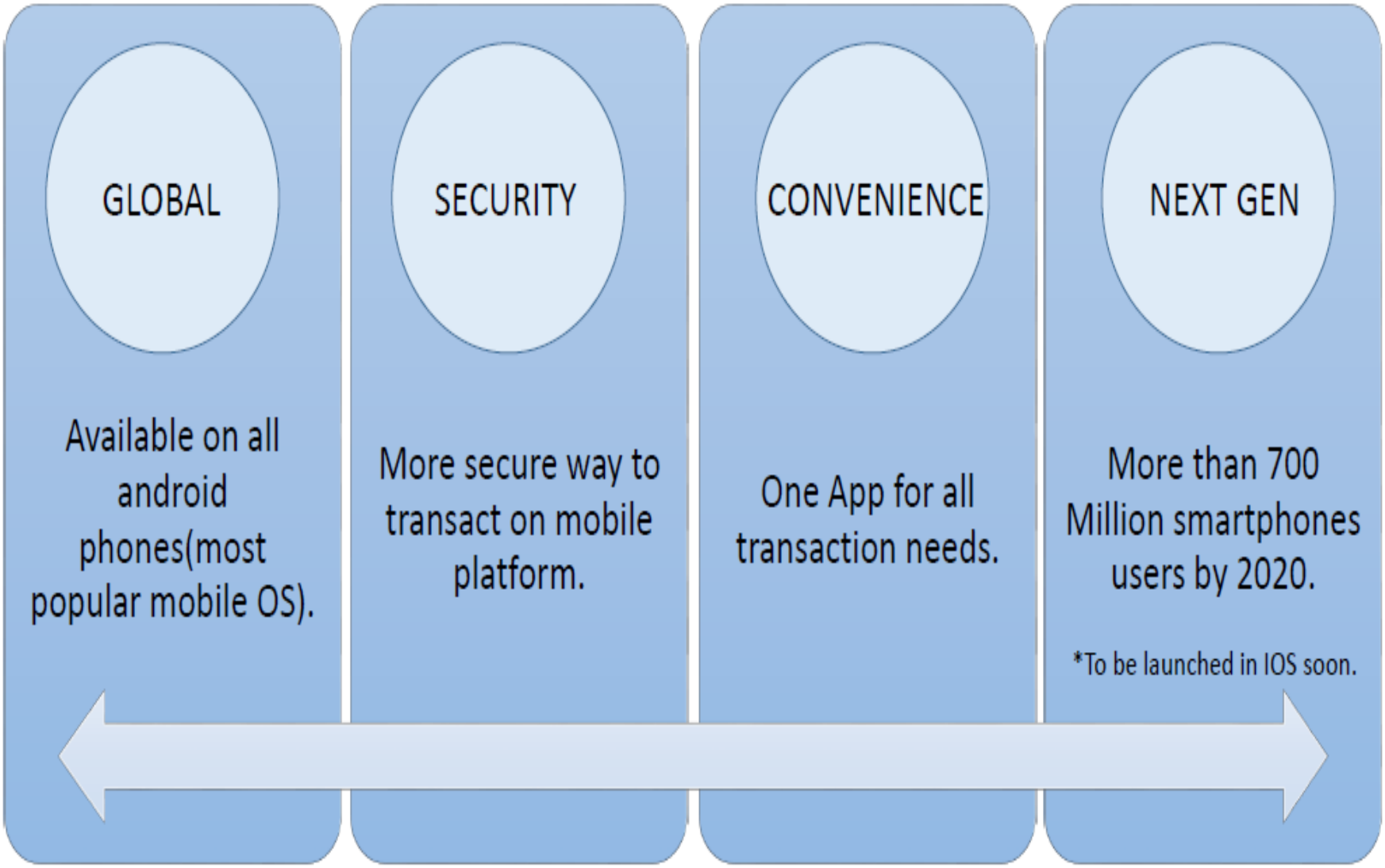
Scalable Architecture

- This next generation payment system provides an ecosystem driven scalable architecture and a set of APIs taking full advantage of mass adoption of smartphone

1 Click 2FA & Virtual address

- Virtual payment addresses, single click 2 factor authentication, Aadhaar integration, use of payer's smartphone for secure credential capture, etc. are some of the core features

Why UPI?


GLOBAL
Available on all android phones(most popular mobile OS).
SECURITY
More secure way to transact on mobile platform.
CONVENIENCE
One App for all transaction needs.
NEXT GEN
More than 700 Million smartphones users by 2020.
*To be launched in IOS soon.

Comparison Between Different Technique

BIOMETRIC	FINGERPRINT	FACE	HAND GEOMETRY	IRIS	VOICE
					
Barriers to universality	Dirt, Dryness	Hair, Glasses, Age	Hand Injury	Poor Lighting	Noise, Clouds
Distinctiveness	High	Low	Medium	High	Low
Performance	High	Medium	Medium	High	Low
Collectivity	Medium	High	High	Medium	Medium
Performance	High	Low	Medium	High	Low
Acceptability	Medium	High	Medium	Low	High
Potential for circumvention	Low	High	Medium	Low	High

[3]

Applications of Biometric System

- Criminal identification
- Internet banking
- Attendance system
- Airport, Bank security
- PC login security
- Prevents unauthorized access to private data
- Financial transaction management

Comparison of Electronic Payment Systems

	Online credit card payment	Electronic Cash	Electronic Checks	Smart Cards
Actual payment time	Paid later	Prepaid	Paid later	Prepaid
Transaction Information Transfer	Store & bank checks the status	Free transfer	Payment indication must be endorsed	Smart card of both parties make transfer
Online & offline transaction	Online	online	Offline allowed	Offline allowed
Bank A/C Involvement	Credit card a/c	No involvement	Bank a/c	Smart card a/c
Users	Any legitimate credit card users	Anyone	Anyone with bank a/c	Anyone with bank or credit card a/c
Party to which payment is made	Distributing bank	Store	Store	Store
Mobility	Yes	No	No	Yes

E-cash

- An e-commerce system that uses e-cash refers to a system in which money is only exchanged electronically.
- To use e-cash, link your personal bank account to other payee accounts.
- To make payments using your e-cash account, you can make a deposit to the other person's e-cash account if you have their banking information, or request a transfer to their bank account.

Cash Versus Credit Transactions

Cash Transaction	V's	Credit Transaction
Payment is made immediately		Payment is made at a later date
Buyer chooses goods to purchases		Credit is offered, payment is made later then the delivery of goods date or provision of the service date
Payment is made		
Receipt given by supplier to customer		

Differences between Risk Management, Risk Assessment, and Risk Analysis

Risk Management

Risk management is the continuing process to identify, analyze, evaluate, and treat loss exposures and monitor risk control and financial resources to mitigate the adverse effects of loss.

Risk Assessment

Risk assessment includes processes and technologies that identify, evaluate, and report on risk-related concerns. the risk assessment process is a “key component” of the risk management process. it is primarily concerned with the Identification and Analysis phases.

Risk Analysis

Risk analysis can be considered the evaluation component of the broader risk assessment process, which determines the significance of the identified risk concerns.

MALWARE VS ADWARE VS SPYWARE

MALWARE	ADWARE	SPYWARE
A software program that is intentionally created to cause damage to a computer, server or a computer network	A software program that generates revenues for a developer by automatically generating online advertisements in the user's interface	A software program that aims to gather information from users without their knowledge
Covers a range of malicious software	A type of malware	A type of malware
Can harm the computer in multiple ways depending on its type. It can destroy data and resources, cause configuration and network issues and many more	Provides profit to the developer by generating online advertisement on the user's interface	Tracks the activities and gathers information about the user without his knowledge

VIRUS VERSUS MALWARE

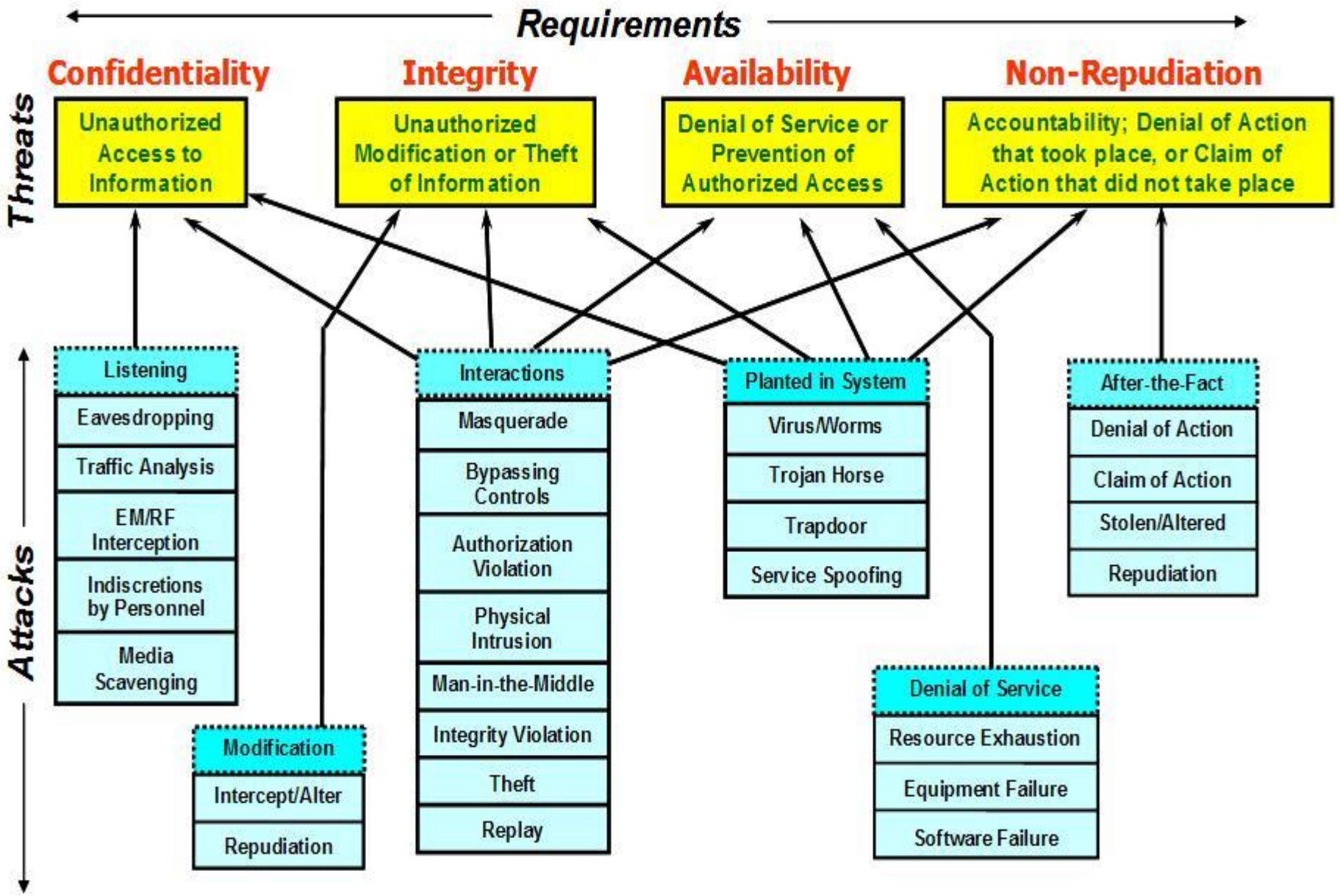
VIRUS	MALWARE
A software that is capable of copying itself and has a detrimental effect like corrupting the system or destroying data	A variety of hostile or intrusive software that harms a computer
There are no further classifications	Virus, spyware, worms, Trojans, ransomware, adware are types
McAfee antivirus plus, Kaspersky, Avira, Avast Pro are some anti-virus software	Malwarebytes, SpyBot Search and Destroy are some anti-malware software

Differences between cybersecurity and cybercrime

	Cybersecurity	Cybercrime
Types of crimes	Crimes where a computer network, software or hardware is the target (ransomware, viruses, worms, SQL injection, distributed denial of service attacks)	Crimes where the human or the human's data is the target (romance scams, cyberbullying, hate speech, sexting, child pornography trafficking, trolling)
Victims	Corporations and governments	Families and individuals
Academic programs	Computer science, computer engineering, information technology	Criminology, psychology, sociology
Intellectual focus	Applied science oriented – coding, networking and engineering strategies for making networks more secure	Basic science oriented – theoretical understandings of how and why crime is committed

Source: Roderick Graham

Security Requirements, Threats, and Attacks



Types of Malwares

- **Adware:**. The least dangerous and most lucrative Malware. Adware displays ads on your computer.
- **Spyware**:. Spyware is software that spies on you, tracking your internet activities in order to send advertising (Adware) back to your system.
- **Virus:** A virus is a contagious program or code that attaches itself to another piece of software, and then reproduces itself when that software is run. Most often this is spread by sharing software or files between computers.
- **Worm:** A program that replicates itself and destroys data and files on the computer. Worms work to “eat” the system operating files and data files until the drive is empty.
- **Trojan:** The most dangerous Malware. Trojans are written with the purpose of discovering your financial information, taking over your computer’s system resources, and in larger systems creating a “denial-of-service attack ” Denial-of-service attack: an attempt to make a machine or network resource unavailable to those attempting to reach it. Example: AOL, Yahoo or your business network becoming unavailable.

- **Rootkit:** It is the hardest of all Malware to detect and therefore to remove; many experts recommend completely wiping your hard drive and reinstalling everything from scratch. It is designed to permit the other information gathering Malware ~~in~~ to get the identity information from your computer without you realizing anything

- **Back doors:** Back doors are much the same as Trojans or worms, except that they open a "backdoor" onto a computer, providing a network connection for hackers or other Malware to enter or for viruses or SPAM to be sent.

- **Key loggers:** Records everything you type on your PC in order to glean your log-in names, passwords, and other sensitive information, and send it on to the source of the key logging program. Many times key loggers are used by corporations and parents to acquire computer usage information.

- **Ransom ware:** If you see this screen that warns you that you have been locked out of your computer until you pay for your cyber crimes. Your system is severely infected with a form of Malware called Ransom ware

- **Browser Hijacker:** This dangerous Malware will redirect your normal search activity and give you the results the developers want you to see. Its intention is to make money off your web surfing.

Access Control

Access Control domain covers mechanisms by which a system grants or revokes the right to access data or perform an action on an information system.

- File permissions, such as “create”, “read”, “edit”, or “delete” on a file server.
- Program permissions, such as the right to execute a program on an application server.
- Data right, such as the right to retrieve or update information in a database.

Access Control

- Access Control is the process or mechanism for giving the authority to access the specific resources, applications and system.
- Access control defines a set of conditions or criteria to access the system and its resources.
- There are three main accesses Control model first is *Mandatory access control model*, second is *Discretionary access control model* and third is *Role based access control models*.

Types of Access control

- **Mandatory access control (MAC) :**
- in this security policy users do not have the authority to override the policies and it totally controlled centrally by the security policy administrator.
- The security policy administrator defines the usage of resources and their access policy, which cannot be overridden by the end users, and the policy, will decide who has authority to access the particular programs and files.
- MAC is mostly used in a system where priority is based on confidentiality.

Types of Access control

- **Discretionary access control (DAC) :**
- This policy Contrast with Mandatory Access Control (MAC) which is determined by the system administrator while DAC policies are determined by the end user with permission.
- In DAC, user has the complete authority over the all resources it owns.
- and also determines the permissions for other users who have those resources and programs.

Types of Access control

- **Role-based access control (RBAC) :**
- This policy is very simple to use.
- In RBAC roles are assigned by the system administrator statically. In which access is controlled depending on the roles that the users have in a system.
- (RBAC) is mostly used to control the access to computer or network resources depending on the roles of individual users within an organization.
- Due to the static role assignment it does not have complexity. Therefore it needs the low attention for maintenance .

Difference between Authentication and authorization

Authentication is any process by which a system verifies the identity of a User who wishes to access it.

- Since Access Control is normally based on the identity of the User who requests access to a resource, Authentication is essential to effective Security.
- Authentication may be implemented using Credentials, each of which is composed of a User ID and Password. Alternately, Authentication may be implemented with Smart Cards, an Authentication Server or even a Public Key Infrastructure.

Authorization is the process of giving someone permission to do or have something.

- In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth).

Identification vs. Authentication

Identification	Authentication
Determine identity of the person	Determines if person is indeed who he claims to be
No identity claim M-1 mapping. Cost of computation $\propto$ #records of users.	Identity claim from the user 1-1 mapping. The cost of computation independent of #records
Captured biometric signatures from a set of known biometric feature stored in the system	Captured biometric signatures may be unknown to the system

Types of Authentication

SINGLE-FACTOR	TWO-STEP	TWO-FACTOR	MULTI FACTOR
Single process based on one category of factor	Additive process: Authenticate once with a single factor and then again with another single factor from the same category	Multiplicative process: Combination from the knowledge or inherence factor and the possession factor derives a stronger single credential than each independent credential	Multiplicative process: Combination of three or more, each from a separate category of factors, derives a stronger single credential than each independent factor
Includes the following factors: Knowledge factor: one thing you "know" ***or*** Inherence factor: one thing you "are"	Includes the following factors: Knowledge factor or inherence factor: one thing you "know" ***or*** "are" ***plus*** Knowledge factor or inherence factor: one thing you "know" ***or*** "are"	Includes the following factors: Knowledge and inherence factor: one thing you "know" ***or*** one thing you "are" ***plus*** Possession factor: one thing you "have"	Includes the following factors: Knowledge factor: one thing you "know" ***plus*** Inherence factor: one thing you "are" ***plus*** Possession factor: one thing you "have"
Examples: ▪ PIN ▪ Password ▪ Finger print ▪ Iris scan	Examples: ▪ Two physical keys ▪ Two passwords (user + one time only password via SMS, generator, email) ▪ Two forms of biometric identification	Examples: ▪ Password or biomarker with an identity card ▪ PIN, secret key or biomarker with a hardware token	Examples: ▪ Password and fingerprint and identity card ▪ PIN and iris scan and hardware token

What is CCTV Cameras ?

- CCTV Camera is an electronic devices, which can capture audio, video and images very sharply from 25 meters.
- It is an excellent product, that helps to provide security solutions for industrial & commercial buildings.
- It have facility to record high resolution audio & video.
- Now a day's CCTV Cameras is very popular and demanding product.

Components of CCTV System

- Analog System
  - Camera
  - DVR
  - Hard Disk for recording
  - Wiring – for Video - Coaxial or CAT 5(with video balun)
  - Wiring – for power (not required iv video balun is used)
  - Power Supply
  - Connector – BNC or RJ45 (in case of video balun)

Wireless CCTV systems

- Wireless CCTV systems are increasingly becoming a popular choice among CCTV buyers on account of the ease of installing such a system, lack of cabling requirements and assured mobility. The key advantages are:
- A wireless camera can be moved to other locations requiring observation while it is difficult to move a wired camera.
- Best suited for locations requiring temporary observation or in a temporary location.
- Wireless camera can be hidden to detect theft or pilferage
- Wireless recording and monitoring device need not be in the same line of sight allowing observation of any place from another remote location.
- Wireless systems are cost effective, re-deployable and portable.

At the same time, there are some disadvantages of wireless CCTV systems, which are listed below :-

- Wireless systems require a dedicated frequency to transmit signals from the camera to the receiving and recording station.
- Frequencies may be subject to various interruptions by use of electric motored products, air conditioning, fluorescent lighting or cordless telephones which affect the picture quality.
- Wireless camera may not provide the best picture quality as such systems are susceptible to picture distortion while wired cameras provide relatively better picture quality.
- Wireless CCTV cameras may need electric power which implies a wire runs through the camera though the video connection is wireless.
- Wireless systems require wireless technology-specific expertise to diagnose and fix break downs in the system.

Wired CCTV Systems

Wired CCTV systems connect the camera to the recording device and monitor with the help of standard coaxial cables or Unshielded Twisted Pair (UTP) cables or fiber optic cables.

The key advantages of wired CCTV systems are:

- Provides the best picture quality with zero interference
- The camera can be located hundreds of meters away from the recording or monitoring equipment.
- All sensors can be run from a single power supply

The key disadvantages are:

- Cabling and installing can be a tedious task, requiring help from experts
- Observation is fixed to a specific area and the camera cannot be easily moved to another location.

Overall, wireless cameras are relatively more expensive than traditional wired cameras. Wireless CCTV systems are a preferred choice in specific locations devoid of easy cabling facilities and for individuals requiring an easy-to-install solution. The wired CCTV system is a preferred choice when good picture quality and economy considerations gain precedence.

Camera Types

CCTV Cameras will normally be Monochrome only, Colour only & Colour/Mono and are available in a wide range housings.

- Fixed Box Camera & Lens – These are normally mounted internally on brackets or inside an externally rated housing. The camera comes with a separate lens which is interchangeable.
- Internal/External Dome Camera – These come with a built-in lens which can be fixed or varifocal type.
- External Bullet Camera - These come with a built-in lens which can be fixed or varifocal type and normally have built-in Infra Red LED to provide a monochrome image in low lighting conditions.
- Covert Camera – These are usually in the guise of an Intruder Alarm Motion Detector or a Smoke detector unit although other types are available and they are not readily identifiable as a CCTV Camera.
- Full Function Camera – A full function or Pan/Tilt/Zoom (PTZ) camera is a camera which can be controlled via the CCTV Recorder, Joystick or Network Connection. These cameras can be fully controlled to view various areas within a site and are especially useful on sites where there is an operator in control of the system at all times.

The difference between digital CCTV and analogue CCTV is all around the encoding of the signal. Here are the major differences:

Digital CCTV	Analogue CCTV
Store as many recordings, from as many cameras as you want. You're only limited by the size of the data storage on your computer or server.	You need to change the tape every day, and have the space to store the videos.
Image quality is superior and doesn't degrade over multiple copies or time, and it's cheap to copy data to CDs to pass information around.	When you copy or record over tapes the picture quality degrades, so you'll need to replace them.
Digital CCTV recorders, or DCRs record up to 100 images per second, and can record simultaneously from each camera	Analogue systems and VCR record from each camera in turn.
It's easy to sort through recorded data, and you can even connect to the digital CCTV system over the internet to check on recordings or look through the archive.	You will need to manually search through recordings to find the incident you want.

Difference between IP and CCTV Camera

- Analog CCTV systems connect to a DVR (digital video recorder) using coax cables and BNC connectors (not networked).
- IP Cameras connect directly to an existing Ethernet network. This connection could be wired or wireless and they can be accessed from anywhere.

Hybrid CCTV Systems

A Hybrid CCTV System can record and display IP Cameras and Analogue Cameras into the same Security Recorder.

This makes it possible to take full advantage of advanced features like video analytics, event controlled functionality, Megapixel Resolution and expansion via the existing LAN Network, whilst also connecting standard analogue (aging technology) CCTV Cameras.

Advantages of CCTV

- • CCTV surveillance cameras provide enhanced security with utmost clarity and with ease of access.
- • You can keep a track of production processes and other processes in industries and other production units.
- • They are a must for every retail stores, boutique, super markets and other shopping areas.
- • The CCTV surveillance systems are not easily damaged by dust, and severe climatic conditions.
- • During holidays they can be installed at your property thus they ensure the security of a home without making you worry anymore about your property when you are away.
- • For people who employ a babysitter at home, this CCTV system gives you utmost satisfaction about your concerns about your younger one at home while looked after by a baby sitter.
- • You can connect the CCTV surveillance system to your mobile phone and can easily access the live streaming of the recordings.

DISADVANTAGES OF CCTV CAMERA SYSTEM

- **Do Not Work Always**: CCTV camera system cannot monitor every area of your office or home at all times. Hence it cannot be considered as a foolproof method for crime prevention.

- **Privacy Concerns**: Invasion of privacy is the major issue when it comes to any security system device like the CCTV camera system. It lowers the employee morale and hampers productivity at times. Constant monitoring of every activity might put the workers ill at ease.

- **Initial Costs**: The initial costs incurred per camera are high. The installation may also increase the initial expenditure. It depends upon the complexity of the CCTV camera system as well.

Mustansiriyah University	Public-Key Cryptography	Class: Third Year
Engineering College	Asymmetric Cipher	Course name: Data Encryption
Computer Engineering Dep.	RSA Algorithm	Lecturer: Fatimah Al-Ubaidy

RSA Public-Key Cryptography

The RSA Algorithm: It is a public key cryptography algorithm, which was proposed by Diffie and Hellman. RSA can be used for key exchange, digital signatures and the encryption of small blocks of data.

- RSA is primarily used to encrypt the session key used for secret key encryption or the message's hash value (digital signature).
- RSA's mathematical hardness comes from the ease in calculating large numbers and the difficulty in finding the prime factors of those large numbers.
- To create an RSA public/private key pair, here are the basic steps:

1- Choose two prime numbers, p and q such that $p \neq q$.

2- Calculate the modulus, $n = p \times q$.

3- Calcuate $\phi(n) = (p - 1) \times (q - 1)$.

4- Select integer e such that gcd $(\phi(n), e) = 1$ and $1 < e < \phi(n)$. (* gcd is greater common divisor)

5- Calculate an integer d from the quotient $de \equiv 1 \pmod{\phi(n)} \Rightarrow de = 1 + k\,\phi(n) \Rightarrow$

$d = (1 + k\,\phi(n)) / e$

- To encrypt a message, M, with the public key (e, n), create the ciphertext, C, using the equation:

$C = M^e \bmod n$

- The receiver then decrypts the ciphertext with the private key (d, n) using the equation:

$M = C^d \bmod n$

RSA Public-Key Cryptography

The RSA Example

1. Select two prime numbers, p = 17 and q = 11.
2. Calculate n = p× q = 17 × 11 = 187.
3. Calculate $\phi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$.
4. Select e such that e is relatively prime to $\phi(n) = 160$ and less than $\phi(n)$; we choose e = 7.
5. Determine d such that $de \equiv 1 \pmod{160}$ and $d < 160$. $de = 1 + k\,\phi(n)$

The correct value is d = 23, because 23 × 7 = 161 = 1 + (1 × 160).
The resulting keys are public key PU = {7, 187} and private key PR = {23, 187}.

Given a plaintext input of M = 88. For encryption, we need to calculate $C = 88^7 \bmod 187$.
we can do this as follows.

$88^7 \bmod 187 = [(88^4 \bmod 187) * (88^2 \bmod 187) * (88^1 \bmod 187)] \bmod 187$
$88^1 \bmod 187 = 88$
$88^2 \bmod 187 = 7744 \bmod 187 = 77$
$88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$
$88^7 \bmod 187 = (88 * 77 * 132) \bmod 187 = 894{,}432 \bmod 187 = 11$

RSA Public-Key Cryptography

For decryption, we calculate $M = 11^{23} \bmod 187$:

$11^{23} \bmod 187 = [(11^1 \bmod 187) * (11^2 \bmod 187) * (11^4 \bmod 187) * (11^8 \bmod 187) * (11^8 \bmod 187)] \bmod 187$

$11^1 \bmod 187 = 11$

$11^2 \bmod 187 = 121$

$11^4 \bmod 187 = 14{,}641 \bmod 187 = 55$

$11^8 \bmod 187 = 214{,}358{,}881 \bmod 187 = 33$

$11^{23} \bmod 187 = (11 * 121 * 55 * 33 * 33) \bmod 187 = 79{,}720{,}245 \bmod 187 = 88$

In the preceding example shows, we can make use of a property of modular arithmetic:

$[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

As another example, suppose we wish to calculate $x^{11} \bmod n$ for some integers x and n. Observe that $x^{11} = x^{1+2+8} = (x)(x^2)(x^8)$.

Public-Key Cryptography

Applications for Public-Key Cryptosystems:

■ **Encryption/decryption:** The sender encrypts a message with the recipient's public key, and the recipient decrypts the message with the recipient's private key.

■ **Digital signature:** The sender "signs" a message with its private key.

■ **Key exchange:** Two sides cooperate to exchange a session key.

The security of RSA:

Five possible approaches to attacking the RSA algorithm are

■ **Brute force:** This involves trying all possible private keys.

■ **Mathematical attacks:** There are several approaches, all equivalent in effort to factoring the product of two primes.

■ **Timing attacks:** These depend on the running time of the decryption algorithm.

■ **Hardware fault-based attack:** This involves inducing hardware faults in the processor that is generating digital signatures.

■ **Chosen ciphertext attacks:** This type of attack exploits properties of the RSA algorithm.