Introduction

Unit: 1

Cyber Security

ANC0301

(B Tech III[rd] Sem)

Sujeet Singh Bhadouria

Assistant Professor

(CSE)

NIET, Gr. Noida

Faculty Profile

FACULTY PROFILE
Name of Faculty: Sujeet Singh Bhadouria

Designation & Department: Assistant Professor, CSE

Qualification: Ph.D (Pre-Submission) M.Tech

Experience: 10 Years of teaching experience

Area of Interest: Computer Network

Reviewer: IET Communications ISSN 1751-8644 (SCI & SCOPUS INDEX)
Research Publications:
International Journal 09
Paper Presentation 06
International Patent 01 (Granted)
National Patent 04

Evaluation Scheme

Sl. No.	Subject Codes	Subject Name	Periods			Evaluation Scheme				End Semester		Total	Credit
			L	T	P	CT	TA	TOTAL	PS	TE	PE		
WEEKS COMPULSORY INDUCTION PROGRAM													
1	AAS0301A	Engineering Mathematics-III	3	1	0	30	20	50		100		150	4
2	ACSE0306	Discrete Structures	3	0	0	30	20	50		100		150	3
3	ACSE0304	Digital Logic & Circuit Design	3	0	0	30	20	50		100		150	3
4	ACSE0301	Data Structures	3	1	0	30	20	50		100		150	4
5	ACSE0302	Object Oriented Techniques using Java	3	0	0	30	20	50		100		150	3
6	ACSE0305	Computer Organization & Architecture	3	0	0	30	20	50		100		150	3
7	ACSE0354	Digital Logic & Circuit Design Lab	0	0	2				25		25	50	1
8	ACSE0351	Data Structures Lab	0	0	2				25		25	50	1
9	ACSE0352	Object Oriented Techniques using Java Lab	0	0	2				25		25	50	1
10	ACSE0359	Internship Assessment-I	0	0	2				50			50	1
11	ANC0301/ ANC0302	Cyber Security*/ Environmental Science*(Non Credit)	2	0	0	30	20	50		50		100	0
12		MOOCs** (For B.Tech. Hons. Degree)											
		GRAND TOTAL										**1100**	**24**

Syllabus

Introduction:

Introduction to Information Systems: Types of Information Systems, Development of Information Systems, Need for Information Security, Threats to Information Systems, Information Assurance, Guidelines for Secure Password and WI-FI Security and social media and Windows Security, Security Risk Analysis and Risk Management.

Application Layer Security:

Data Security Considerations-Backups, Archival Storage and Disposal of Data, Security Technology-Firewall, Intrusion Detection, Access Control, Security Threats -Viruses, Worms, Trojan Horse, Bombs, Trapdoors, Spoofs, E-mail Viruses, Macro Viruses, Malicious Software, Network and Denial of Services Attack, Security, Threats to E-Commerce: Electronic Payment System, e- Cash, Issues with Credit/Debit Cards.

Syllabus

Secure System Development:

Application Development Security, Architecture & Design, Security Issues in Hardware: Data Storage and Downloadable Devices, Mobile Protection, Security Threats involving in social media, Physical Security of IT Assets, Access Control, CCTV and Intrusion Detection Systems, Backup Security Measures.

Cryptography and Network Security:

- Public key cryptography: RSA Public Key Crypto with implementation in Python, Digital Signature Hash Functions, Public Key Distribution.
- Symmetric key cryptography: DES (Data Encryption Standard), AES (Advanced Encryption Standard), Secure hash algorithm (SHA-1).
- Real World Protocols: Basic Terminologies, VPN, Email Security Certificates, Transport Layer Security, TLS, IP security, DNS Security.

Syllabus

Security Policy:

- Policy design Task, WWW Policies, Email based Policies, Policy Revaluation Process-Corporate Policies-Sample Security Policies, Publishing and Notification Requirement of the updated and new Policies.
- Recent trends in security.

Branch wise Applications

- There are many cyber security real-life examples where financial organizations like banks and social organizations, weather channels etc. have faced cyber-attacks and have lost valuable information and resources. To fix these problems, you'll need comprehensive cyber security awareness.

- According to KPMG, the annual compensation for cyber security heads ranges from 2 Cr to 4 Cr annually. The industry also reports a satisfaction level of 68%, making it a mentally and financially satisfying career for most.

Course Objective

Students will learn about :

- Security of Information system and Risk factors.
- Examine security threats and vulnerability in various scenarios.
- Understand concept of cryptography and encryption technique to protect the data from cyber-attack
- Provide protection for software and hardware.

Course Outcome

- After successful completion of this course student will be able to -

COURSE OUTCOME NO.	COURSE OUTCOMES	Bloom's Knowledge Level (KL)
CO1	Analyze the cyber security needs of an organization.	K4
CO2	Identify and examine software vulnerabilities and security solutions.	K1, K3
CO3	Comprehend IT Assets security (hardware and Software) and performance indicators.	K2
CO4	Measure the performance and encoding strategies of security systems.	K3, K5
CO5	Understand and apply cyber security methods and policies to enhance current scenario security.	K2, K3

Program Outcomes

1. Engineering knowledge
2. Problem analysis
3. Design/development of solutions
4. Conduct investigations of complex problems
5. Modern tool usage
6. The engineer and society
7. Environment and sustainability

Program Outcomes…(cont.)

8. Ethics
9. Individual and team work
10. Communication
11. Project management and finance
12. Life-long learning

CO-PO Mapping

CO-PO Mapping

PO No→ CO No.↓	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	2	1	2	-	-	-	1	2	1	2	2
CO2	2	2	2	2	2	1	-	1	2	1	2	2
CO3	2	2	1	2	2	-	-	1	2	1	2	2
CO4	2	2	1	2	2	1	-	1	2	1	2	2
CO5	2	2	1	2	2	-	-	1	2	1	2	2

*3= High *2= Medium *1=Low

Program Specific Outcomes

Program Specific Outcomes (PSOs) are what the students should be able to do at the time of graduation. The PSOs are program specific. PSOs are written by the department offering the program.

On successful completion of B. Tech. (CSE) Program, the Computer Science Engineering graduates will be able to:

PSO1 : Work as a software developer, database administrator, tester or networking engineer for providing solutions to the real world and industrial problems.

PSO2 : Apply core subjects of information technology related to data structure and algorithm, software engineering, web technology, operating system, database and networking to solve complex IT problems

PSO3 : Practice multi-disciplinary and modern computing techniques by lifelong learning to establish innovative career

PSO4 : Work in a team or individual to manage projects with ethical concern to be a successful employee or employer in IT industry.

CO-PSO Mapping

Program Specific Outcomes and Course Outcomes Mapping

CO	PSO1	PSO2	PSO3	PSO4
CO1	2	2	-	2
CO2	2	2	1	2
CO3	2	2	-	2
CO4	2	2	-	2
CO5	2	2	-	2

*3= High *2= Medium *1=Low

Program Educational Objectives

- The **Program Educational Objectives (PEOs)** of an engineering degree program are the statements that describe the expected achievements of graduates in their career, and what the graduates are expected to perform and achieve during the first few years after graduation.

PEO1: To have an excellent scientific and engineering breadth so as to comprehend, analyze, design and solve real-life problems using state-of-the-art technology.

PEO2: To lead a successful career in industries or to pursue higher studies or to understand entrepreneurial endeavors.

PEO3: To effectively bridge the gap between industry and academics through effective communication skill, professional attitude and a desire to learn.

Result Analysis

Faculty Name	Subject Name	Code	Result
Ms Ruchika Sharma	Cyber Security	ANC0301	100%

Question Paper Template

(SEM:…..SESSIONAL EXAMINATION –I)(2021-2022)

Subject Name: ……..

Time: 1.15Hours **Max. Marks:30**

General Instructions:

- All questions are compulsory. Answers should be brief and to the point.
- This Question paper consists of .....pages & ...5.....questions.
- It comprises of three Sections, A, B, and C. You are to attempt all the sections.
- Section A -Question No- 1 is objective type questions carrying 1 mark each, Question No- 2 is very short answer type carrying 2 mark each. You are expected to answer them as directed.
- Section B - Question No-3 is Short answer type questions carrying 5 marks each. You need to attempt any two out of three questions given.
- Section C -Question No. 4 &5are Long answer type (within unit choice) questions carrying 6marks each. You need to attempt any one part a. or b.
- Students are instructed to cross the blank sheets before handing over the answer sheet to the invigilator.
- No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.

		SECTION – A	[8]	
1.	Attempt all parts		(4×1=4)	CO
	a.		(1)	
	b.		(1)	
	c.		(1)	
	d.		(1)	
2.	Attempt all parts		(2×2=4)	CO
	a.		(2)	
	b.		(2)	

Question Paper Template

		SECTION – B		
3.	**Answer any two of the following-**		**[2×5=10]**	**CO**
	a.		**(5)**	
	b.		**(5)**	
	c.		**(5)**	
		SECTION – C		
4	**Answer any one of the following-(Any one can be applicative if applicable)**		**[2×6=12]**	**CO**
	a.	**Question-**	**(6)**	
	b.	**Question-**	**(6)**	
5.	**Answer any one of the following-**			
	a.		**(6)**	
	b.		**(6)**	

Prerequisite/Recap

- Basics recognition in the domain of Computer Science.
- Concept of network and operating system.
- Commands of programming language.

Introduction

- Modern life depends on online services, so having a better understanding of cyber security threats is vital.
- The course will improve your online safety in the context of the wider world, introducing concepts like malware, trojan virus, network security, cryptography, identity theft, and risk management.

1. https://www.javatpoint.com/cyber-security-introduction
2. https://www.edureka.co/blog/what-is-cybersecurity/
3. http://natoassociation.ca/a-short-introduction-to-cyber-security/

Content (Unit-1)

- Introduction to Information Systems
- Types of Information Systems
- Development of Information Systems
- Introduction to Information Security
- Need for Information Security
- Threats to Information Systems
- Information Assurance
- Cyber Security
- Guidelines for Secure Password and WI-FI Security and social media and Windows Security
- Security Risk Analysis and Risk management

Unit Objective

Topic	Objective
Information Systems	To Understand the information system , its Types and Development of Information Systems and also understanding of various threats to information system
Information Security	Develop an understanding of information security
Information Assurance	Develop an understanding of information assurance as practiced in computer operating systems

Objective of Topic

Topic	Objective
Cyber Security and Security Risk Analysis	Develop an understanding of security policies (confidentiality, integrity and availability), need of cyber security and security risk associated with it.

Topic Mapping with CO

Topic	CO
Introduction to Information Systems	CO1
Types of Information Systems	CO1
Development of Information Systems	CO1
Introduction to Information Security	CO1
Need for Information Security	CO1
Threats to Information Systems	CO1
Information Assurance	CO1
Cyber Security	CO1
Guidelines for Secure Password and WI-FI Security and social media and Windows Security	CO1
Security Risk Analysis and Risk management	CO1

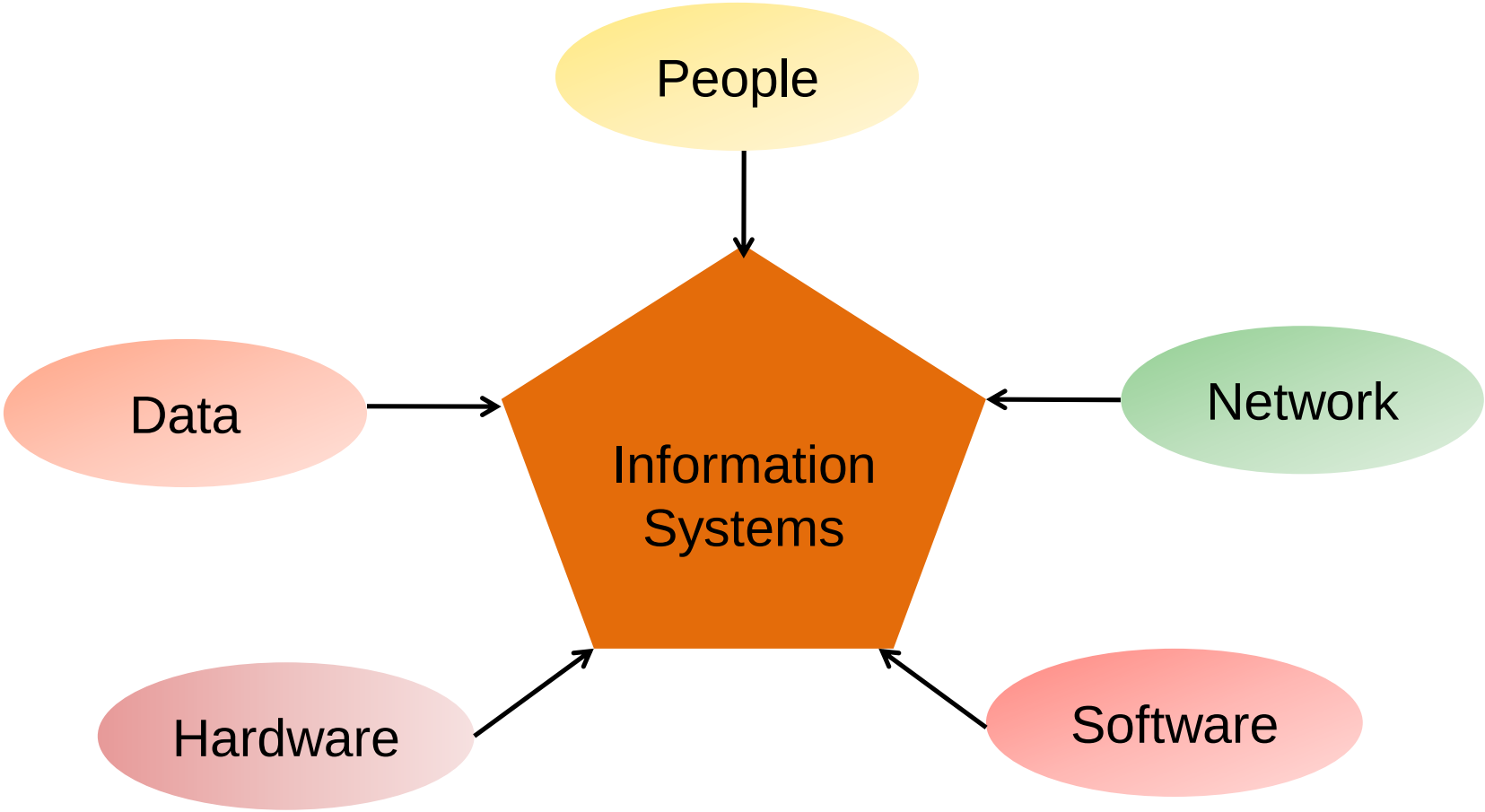
Introduction to Information Systems (CO1)

Information System

- Information System is made up of two terms, namely, Information and System.
- **Information** - Well-structured data with a specific meaning
- **System** - an arrangement that takes input and provides output after completing the required process.

"An arrangement that processes data and provides meaningful information."[1]

Information Systems Cont…



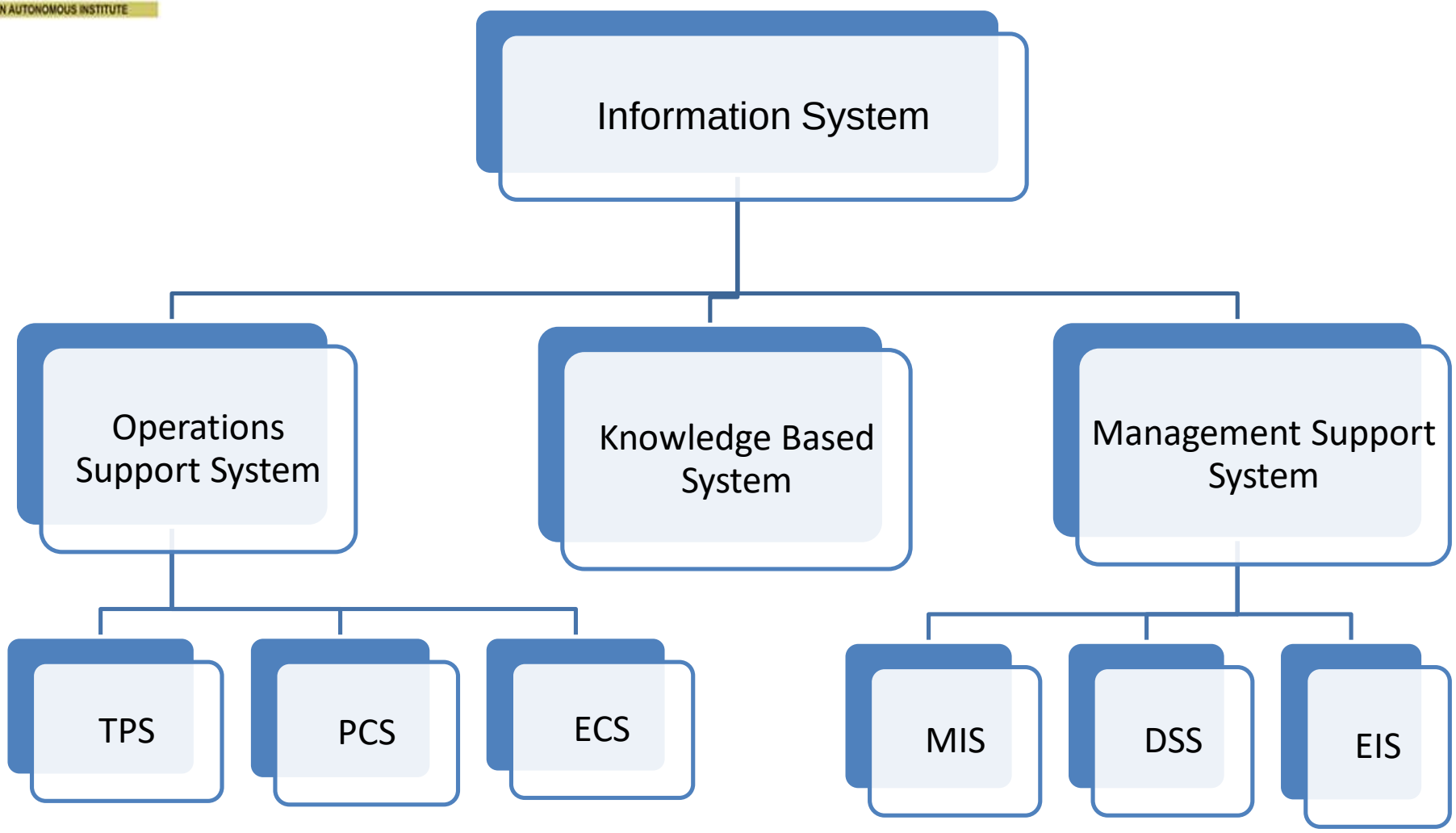
Information Systems Cont…

- An Information system contains software, hardware, data, people, and network.
- Processes and essential system elements are also considered as part of an Information System.
- An information system (IS) is an organized system for collecting, organizing, storing and communicating with the information.

Fundamental concepts in Information Systems

- Capture both internal data and external data of the organization and its environment.
- Stores the database items over an extensive period of time.
- Based on the user's need, specifications are deployed.
- The output of the Information systems varies on its type.

Types of Information System (CO1)



Operations Support Systems (OSS)

Support various business operations such as accounting and production.

A. Transaction processing system(TPS):

Helps in processing various business transactions and retrieving information from them.

Processing a transaction can be done in two ways -

- ✓ Batch Processing
- ✓ Online or Real-time processing.

- Batch Processing - transactions are stored over a period of time and then processed.
- Real-Time Processing – transactions are processed during their occurrences. For example, at retail stores, the cash receipts or card payments are registered and processed simultaneously.

Operations Support Systems (OSS)

B- Process Control System (PCS)

– Monitoring and controlling physical processes basically in production Industries.

Example-

- ✓Making day-to-day decisions
- ✓Controlling operational processes.

– This system **automates** the adjustment of a production process.

Operations Support Systems (OOS)

C- Enterprise collaboration system (ECS)

- Helps in sharing information among employees.
- A proper flow of information helps in **increasing the productivity** of an organization.
- Example of Tools used in ECS-
  - ✓ Mails
  - ✓ Video Conferencing
  - ✓ Group calendars

Knowledge-Based Systems

Provides information to **users** in different business areas when required.

- **Expert system:** Provides adequate **knowledge** and expert **advice** for making various managerial decisions.

  Expert System = Knowledge base + Software modules

- **Knowledge Management System (KMS):** For sharing knowledge, KMS uses a group of collaboration systems, such as the Intranet. Provides two types of knowledge-
  i. **Explicit knowledge** - Information that is documented, stored, and coded with the help of an Information System.
  ii. **Implicit/Tacit knowledge** - Information based on processes and procedures stored in the human mind.

Management Support Systems

MSS provides useful information to **managers** for **decision making** and **control**.

a) Management Information System (MIS): It generates information for monitoring performance and maintaining coordination.

Example- Production manager can check the report of cost and time of production.

Management Support Systems

b) Decision Support System (DSS):

Supports managerial decision making.
Example -Sales manager can set sales targets for the coming year by considering the existing market conditions.

c) Executive Information System (EIS) or Executive Support System (ESS) :

Provides critical information to the executive and top-level managers for for making strategic decisions.

Recap

Information System:

An arrangement that processes data and provides meaningful information.

Types of Information System

- Operations Support System
  - TPS
  - PCS
  - ECS
- Knowledge Based System
- Management Support System
  - MIS
  - DSS.

Development of IS (CO1)

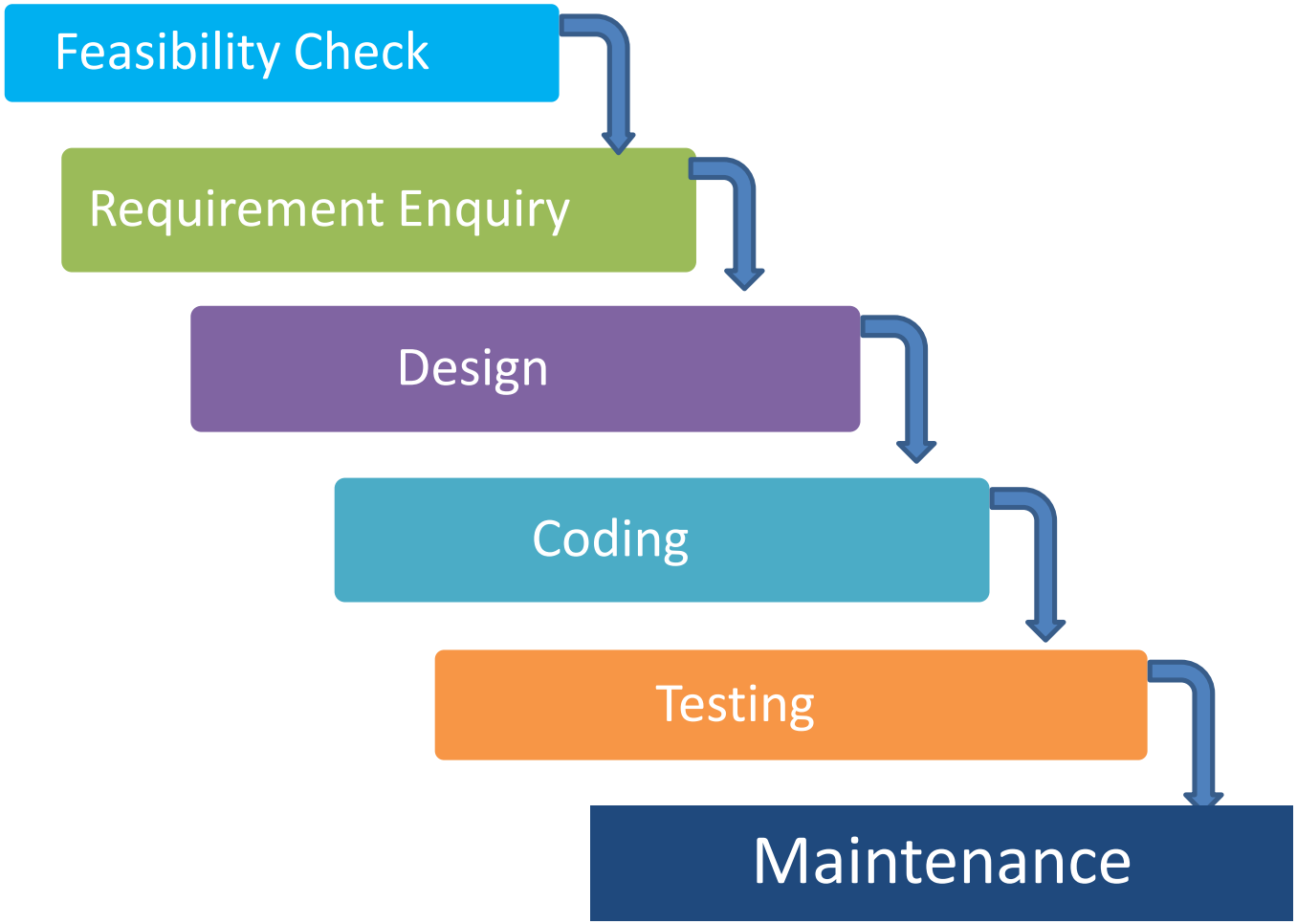
Development of IS, similar to the application development procedure.

The main approaches are listed as follows:

1. Waterfall model
2. Prototyping model
3. Evolutionary model
4. Spiral model
5. Incremental model

Waterfall model

This method is also called linear sequential model.



Stages of Waterfall Model

- **Feasibility check:** Technical and financial feasibility check about system development.
- **Requirement and specifications:** Gathering knowledge about the required system and developing the specifications needed.
- **Design:** Converting the requirements and specifications into a system model.
- **Coding:** Coding is the process of designing a bridge between the understanding of the user and the system. This is also called programming.
- **Testing:** Ensuring that the system performance is according to the user requirements. This is done after a system is set for use.
- **Maintenance:** Changes in the system after testing or use to correct the shortcomings or further requirements.

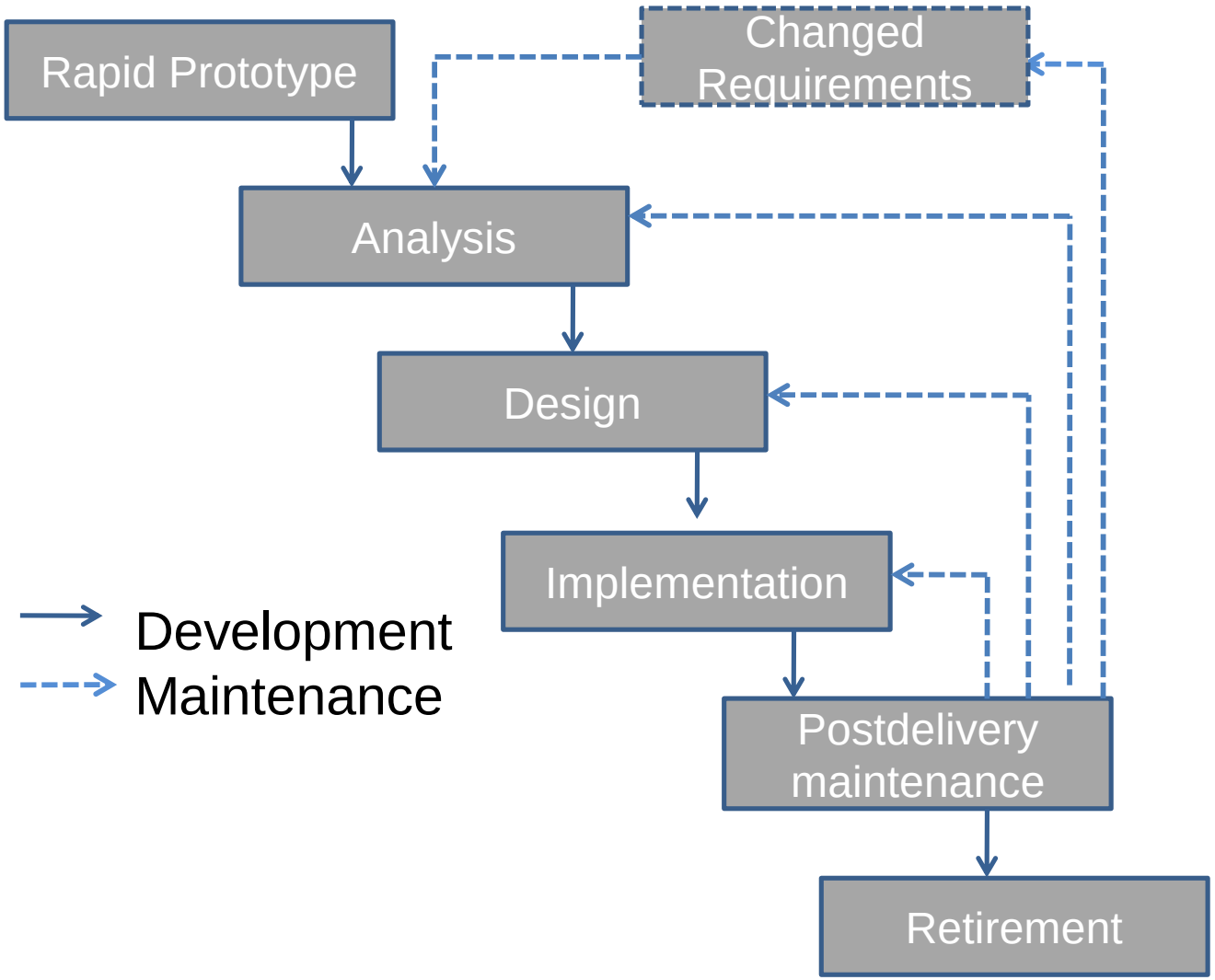
Drawbacks of Waterfall Model

- It approaches feasibility analysis before requirement analysis, which is not practical.
- It tests the system after implementing and designing; therefore, any change required after testing can be hard to be introduced.
- Any feedback to the previous process has not been approached.

Prototyping Model

- The prototype may be a usable program but is not suitable as the final software product.
- The code for the prototype is thrown away. However, experience gathered helps in developing the actual system.
- The development of a prototype might involve extra cost, but overall cost might turnout to be lower than that of an equivalent system developed using the waterfall model.

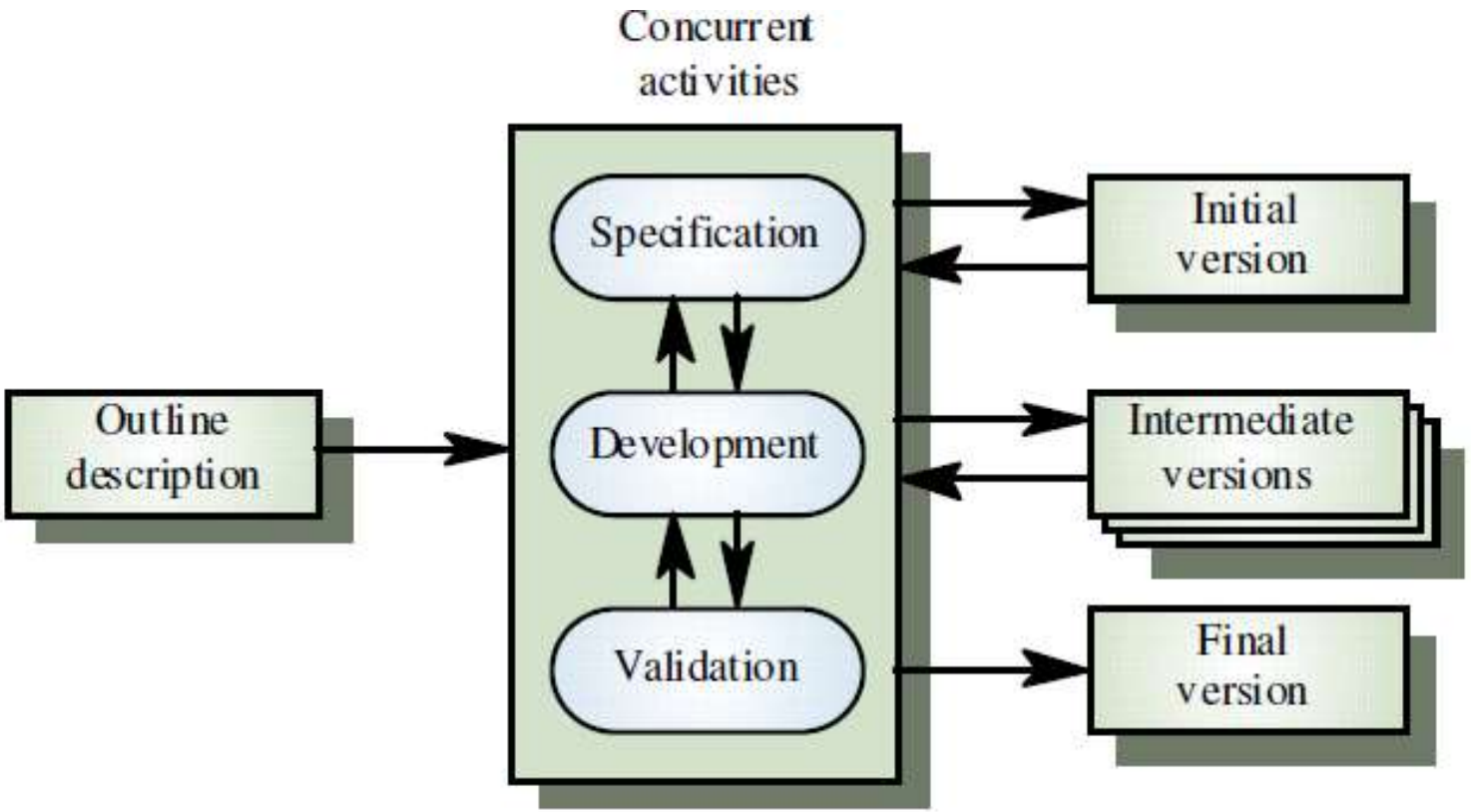
Prototyping Model



Evolutionary Model

- Evolutionary model approaches to improve the classic waterfall model by providing scope of feedback and improvement at every stage of the system development.
- Therefore, every stage should be taken as a separate evolutionary phase.
- This model is useful for complex projects where all functionality must be delivered at one time, but the requirements are unstable or not well understood at the beginning.

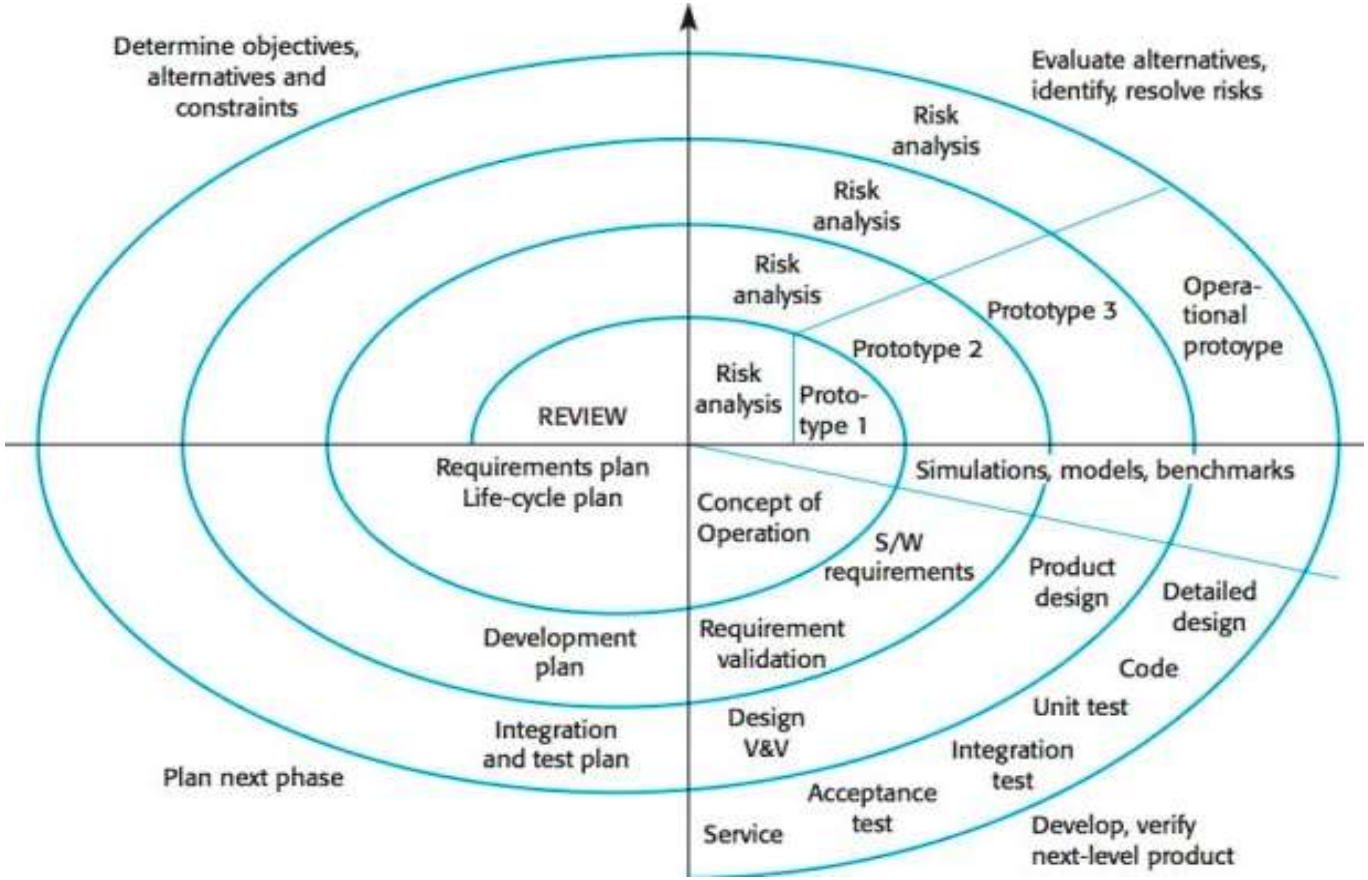
Evolutionary Model



Source: software engineering k k aggarwal

Spiral Model

- It is a combination of the features of the waterfall and prototype models.
- This idea was given by Boehm.



Source: Software engineering K K Aggarwal

Stages of Spiral Model

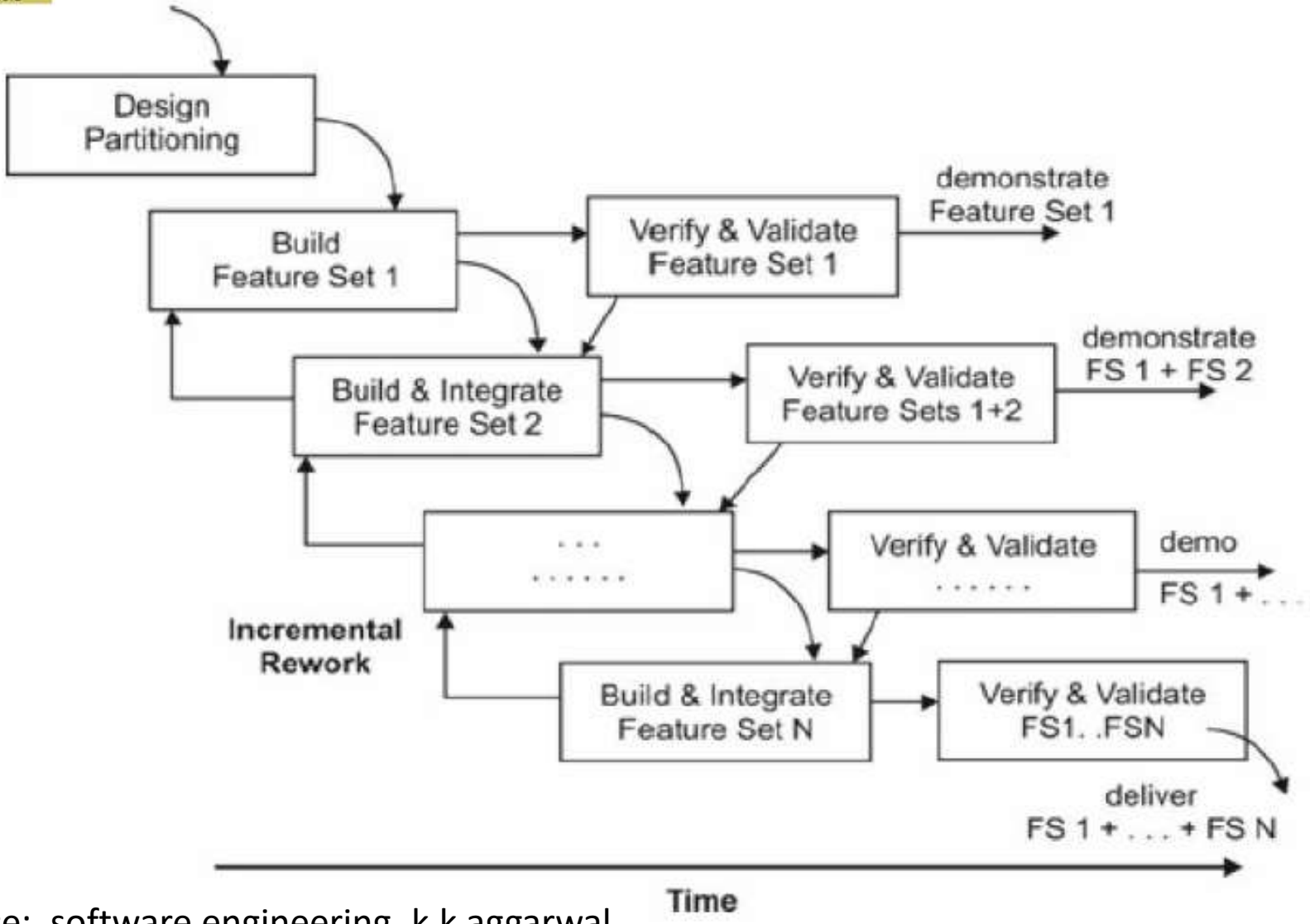
- **User/client communication:** Interaction with the client or users of the system to identify the requirements and specifications in the system
- **System planning:** Planning the system to be developed and preparing a rough draft and schedule of the development process
- **Risk analysis:** Identifying the problems in the plan and developing solutions to check them
- **Engineering:** Involves system hardware and software design, coding and testing the system
- **Construction and finalization:** Involves system building and testing to release it for use
- **System evaluation:** Evaluation by user or client to use the system.

Note- All these phases are repeated in the process of system development until users approve the system.

Incremental Model

- Incremental model approaches system development through various incremental steps, where every step tries to add more functions in the system development process.
- Each step of system development is a separate group of activities.
- This model can also be called Continuous Improvement Model.

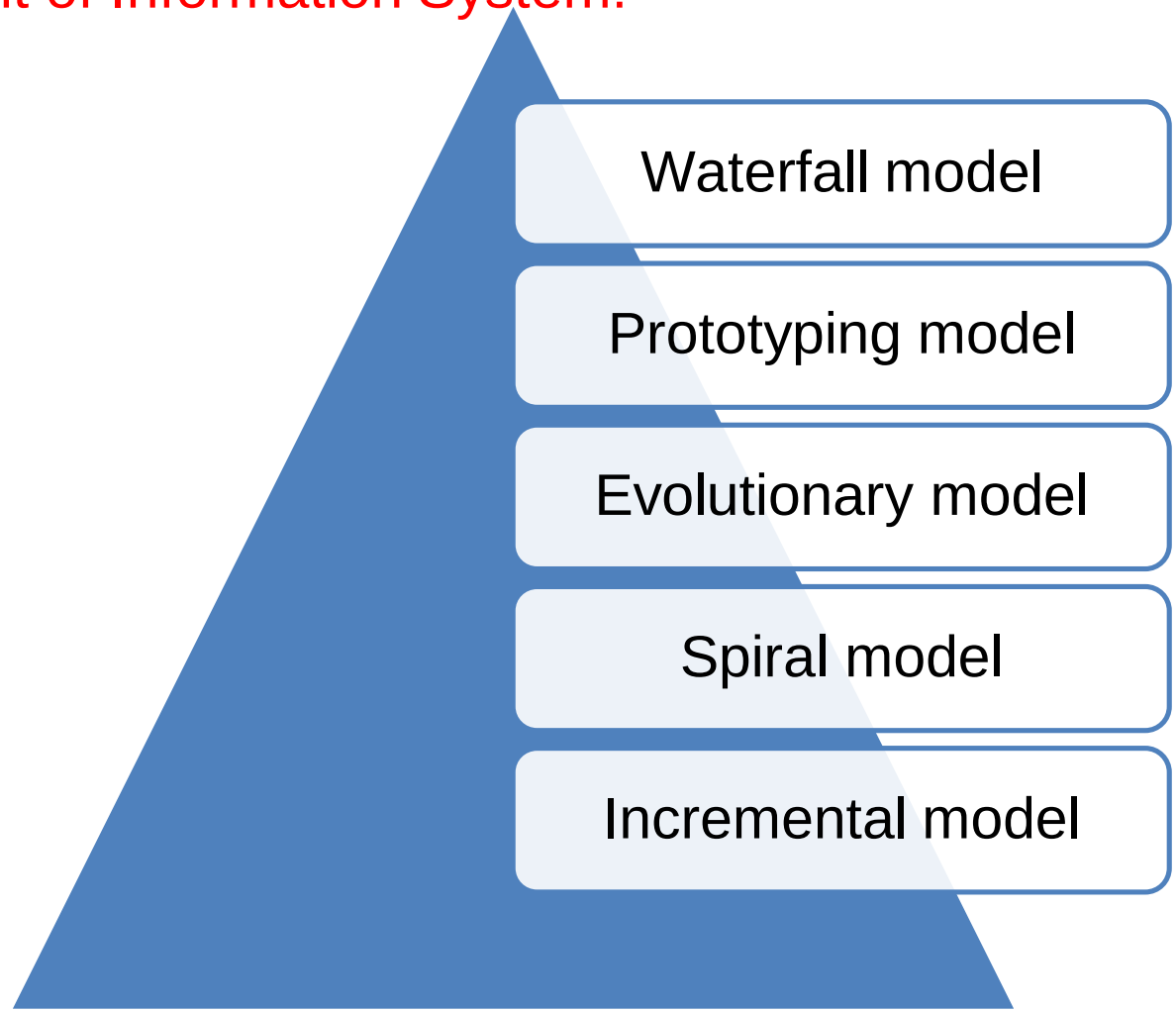
Incremental Model



Source: software engineering k k aggarwal

Recap

Development of Information System:



Introduction to Information Security (CO1)

- Information security refers to the protection of information.
- It is the process of securing, protecting, and safeguarding the information from an unauthorized access, use, and modification.
- Information is an important part of an organization or a business that requires more attention to preserve its integrity, privacy, and availability.

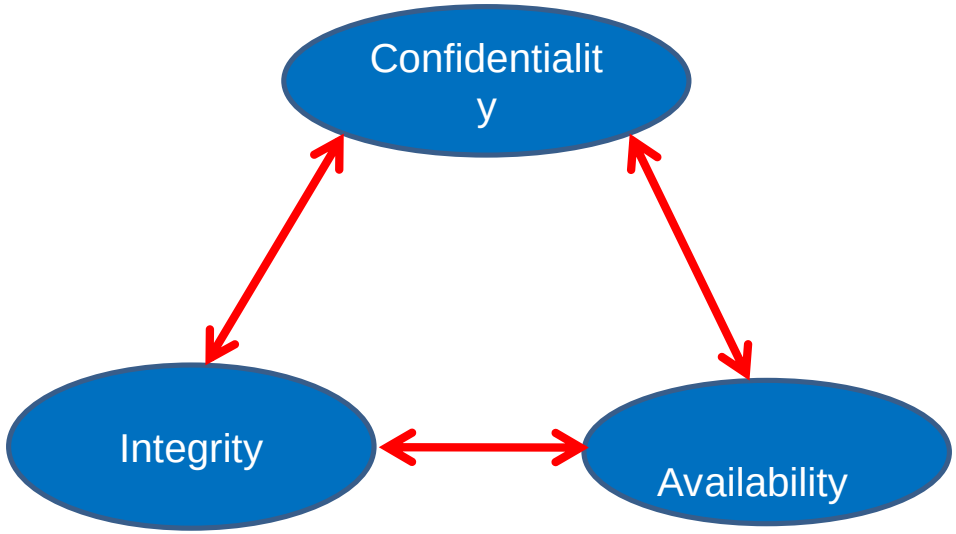
Goals of information security -

1. Confidentiality
2. Integrity
3. Availability

Source: Swayam

Introduction to Information Security

- Process of securing information from unauthorized access



Securing the information from unauthorized modification.

- On time
- Fault tolerance exists in the computer system or network
- Fair allocation of resources over the network
- Concurrency control management in database
- Deadlock management in database

Need for Information Security (CO1)

- To maintain proper security of information in an organization, we need to apply certain measures, policies, and procedures so that no harm is caused to the confidentiality, integrity, and availability of organizational information.

- Data breaches are become common
- Shrinking time from exposure to attack
- Epidemic of security vulnerabilities
- Phishing and spamming
- Zero day attack

Source: Swayam

Task to do

- **Compliance need-** PCI, SOX, HIPPA
- **Zero day attack**

A zero-day attack is a software-related attack that exploits a weakness that a vendor or developer was unaware of. The name comes from the number of days a software developer has known about the problem. The solution to fixing a zero-day attack is known as a software patch.

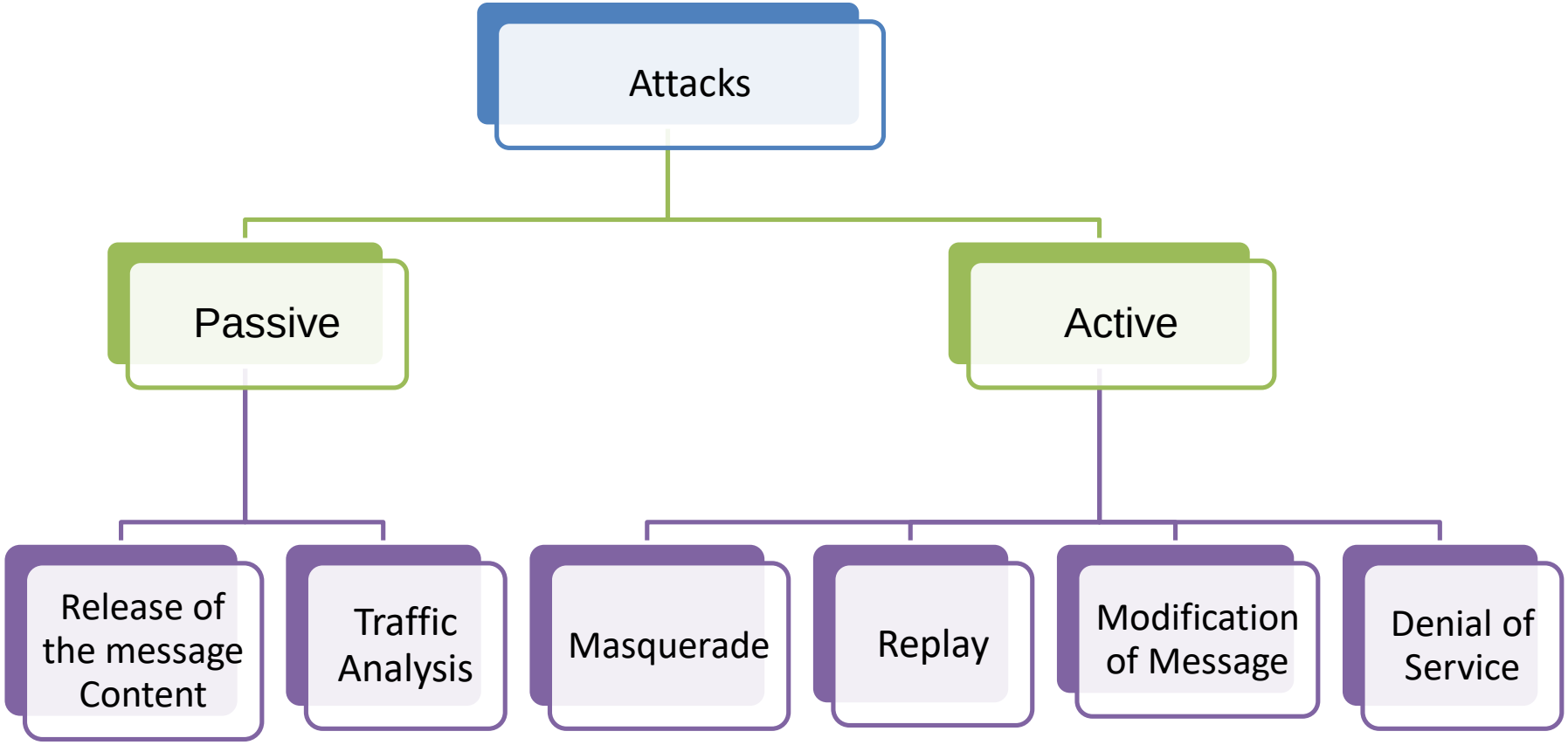
Threats to Information Systems (CO1)

- A threat is an illegal activity that can cause damages such as loss of information and data corruption to the network of an organization.
- The hardware and software components of a computer system are highly vulnerable to many threats.

Types of Threat	
Accidental threat	• occur due to exposure of confidential information and unauthorized modification in information. • occurrence is not dependent on any entity
Intentional threat	• It is performed by an entity to violate security of the computer system and network.

Attacks on the Network

- Attacks on the network can breach the security of data and resources over the network.

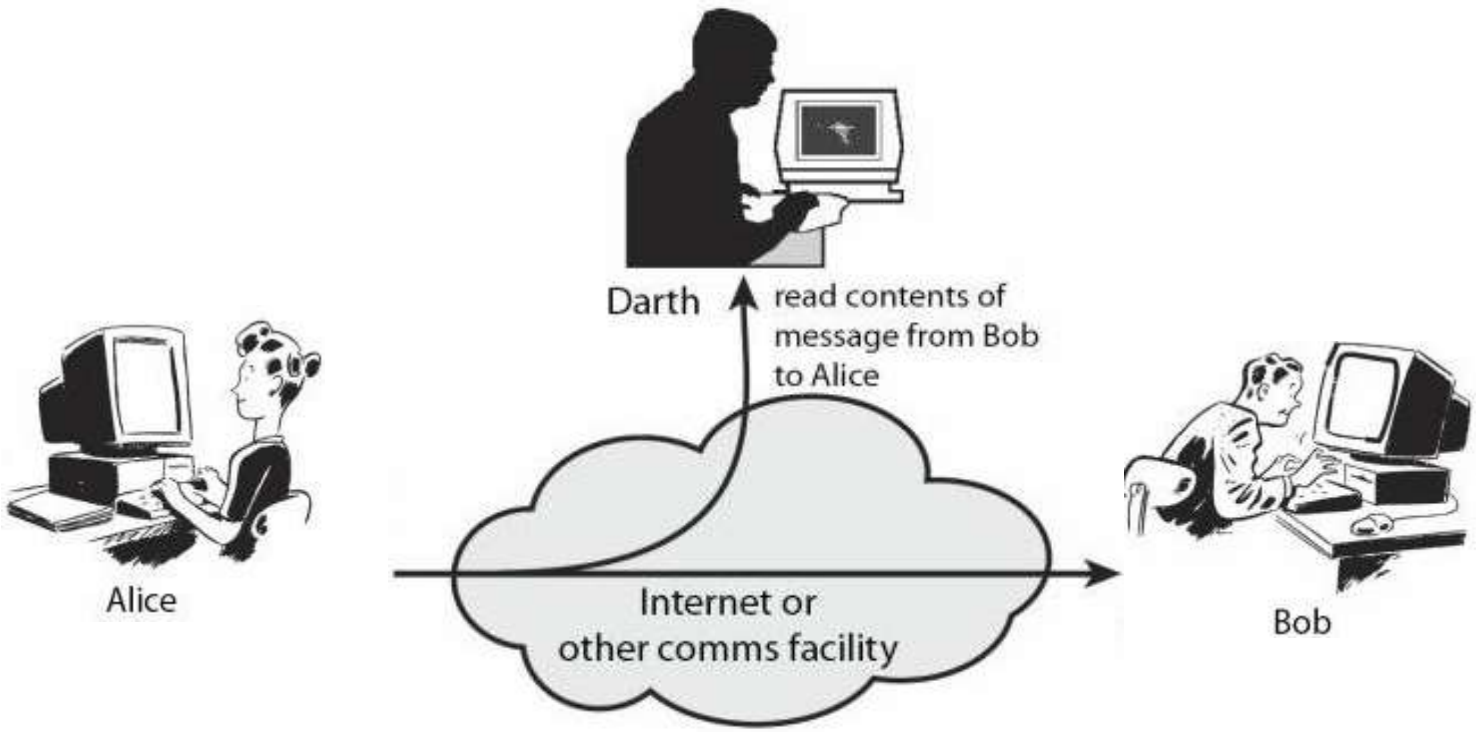


Passive Attack

- The attacker does not intend to cause any harm to the network.
- The attacker observes the information for which he/she does not have access rights.
- Only Monitors, analyzes, or observes the information available over the network.

Passive Attack

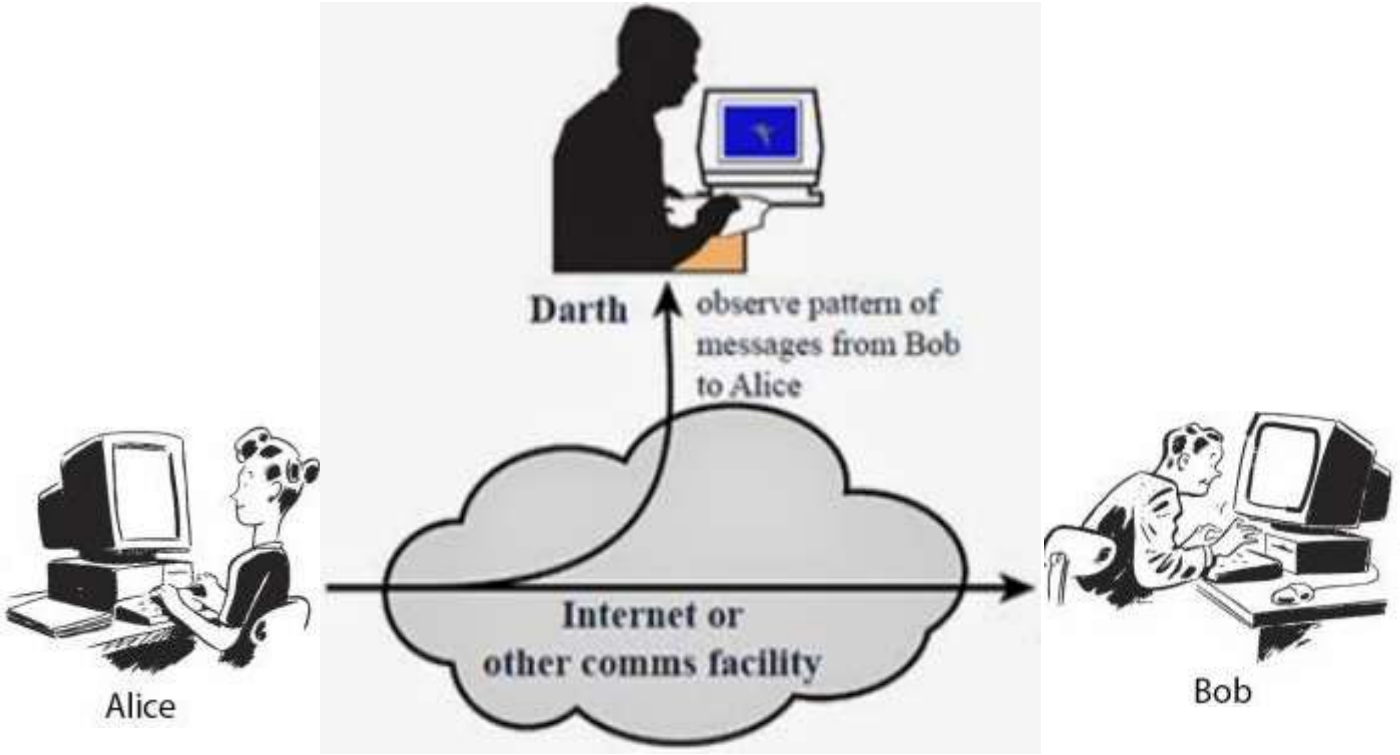
- **Release of the message Content**



Source: cryptography and network security william stallings

Passive Attack

- **Traffic Analysis**



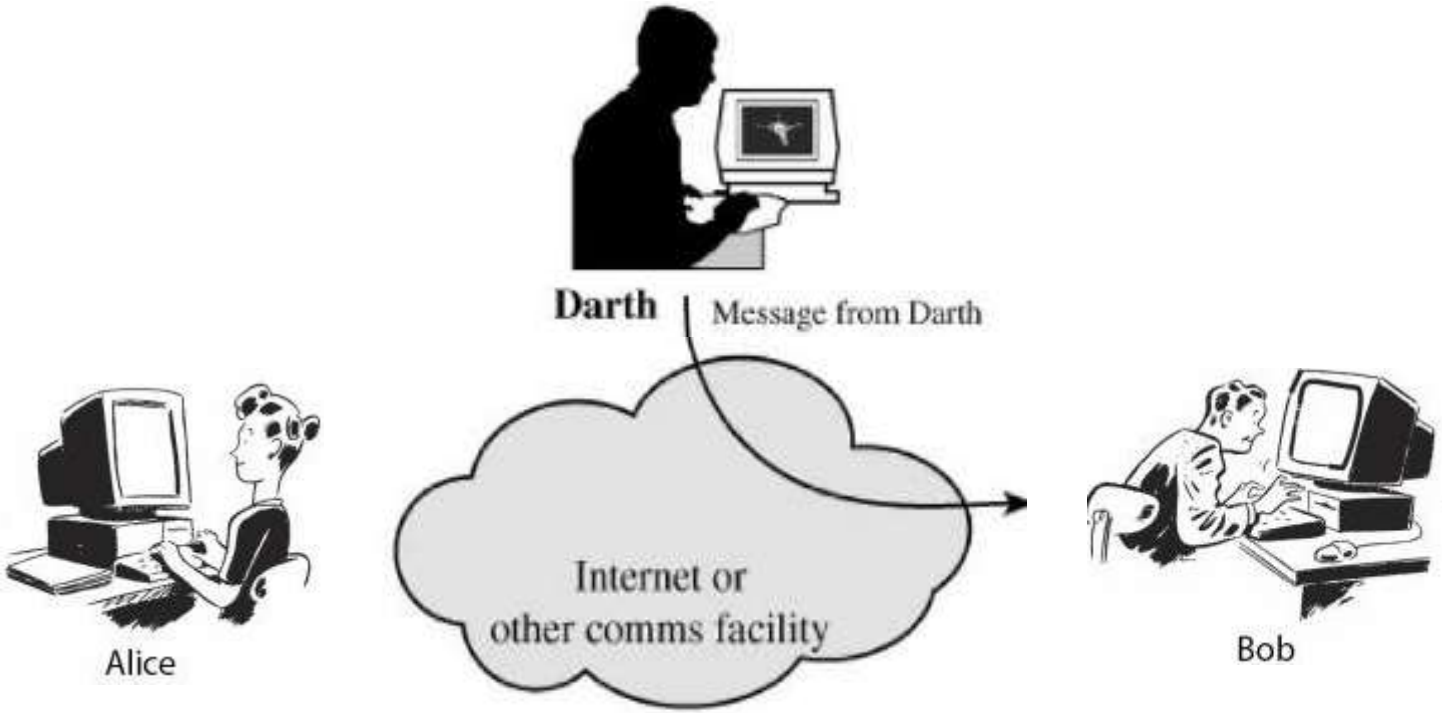
Source: cryptography and network security william stallings

Active Attack

- Intentions can be wrong.
- The attacker tries to steal information from the network.
- Attacker can create, delete, modify, and replace a message.

Active Attack

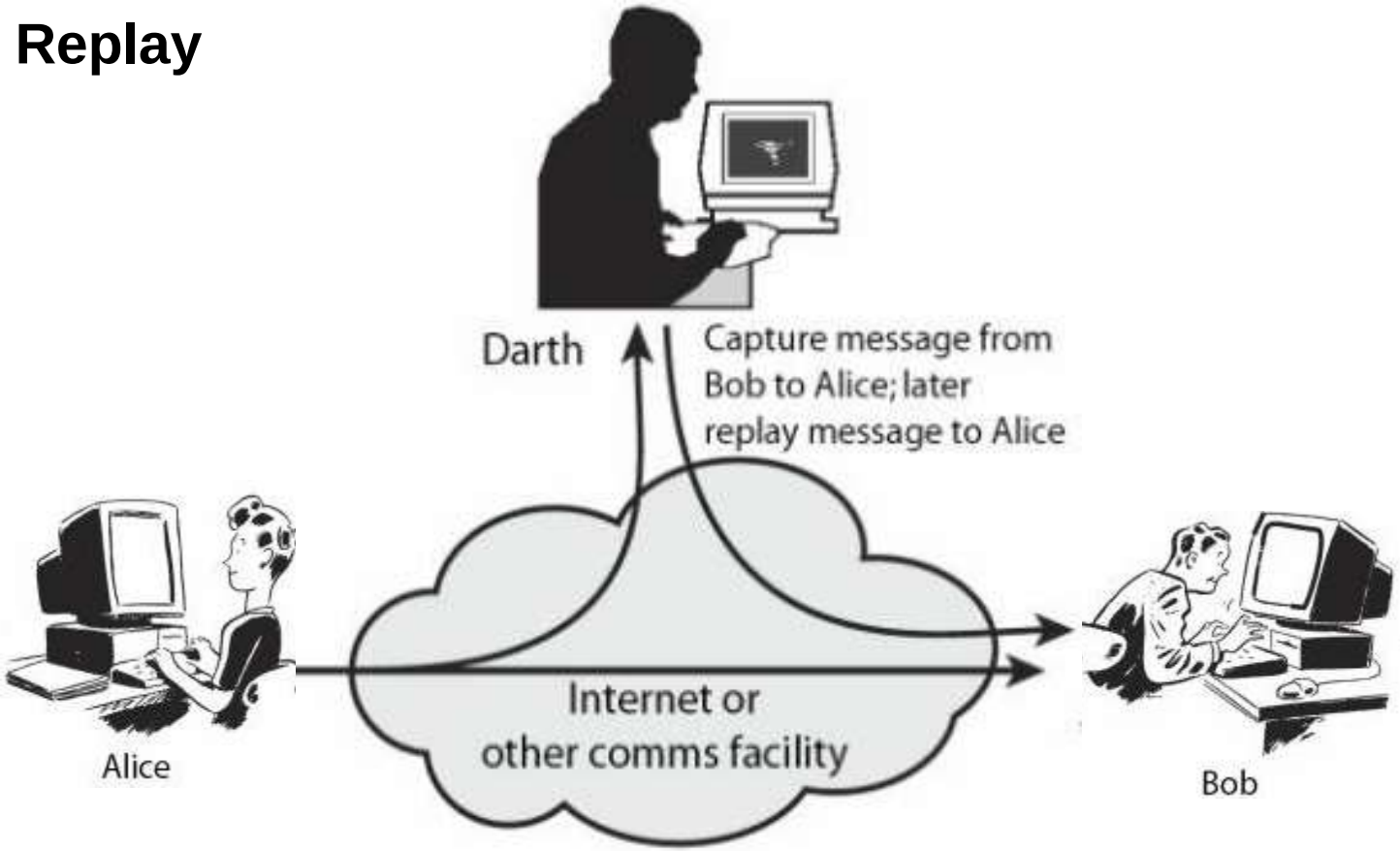
- **Masquerade**



Source: cryptography and network security william stallings

Active Attack

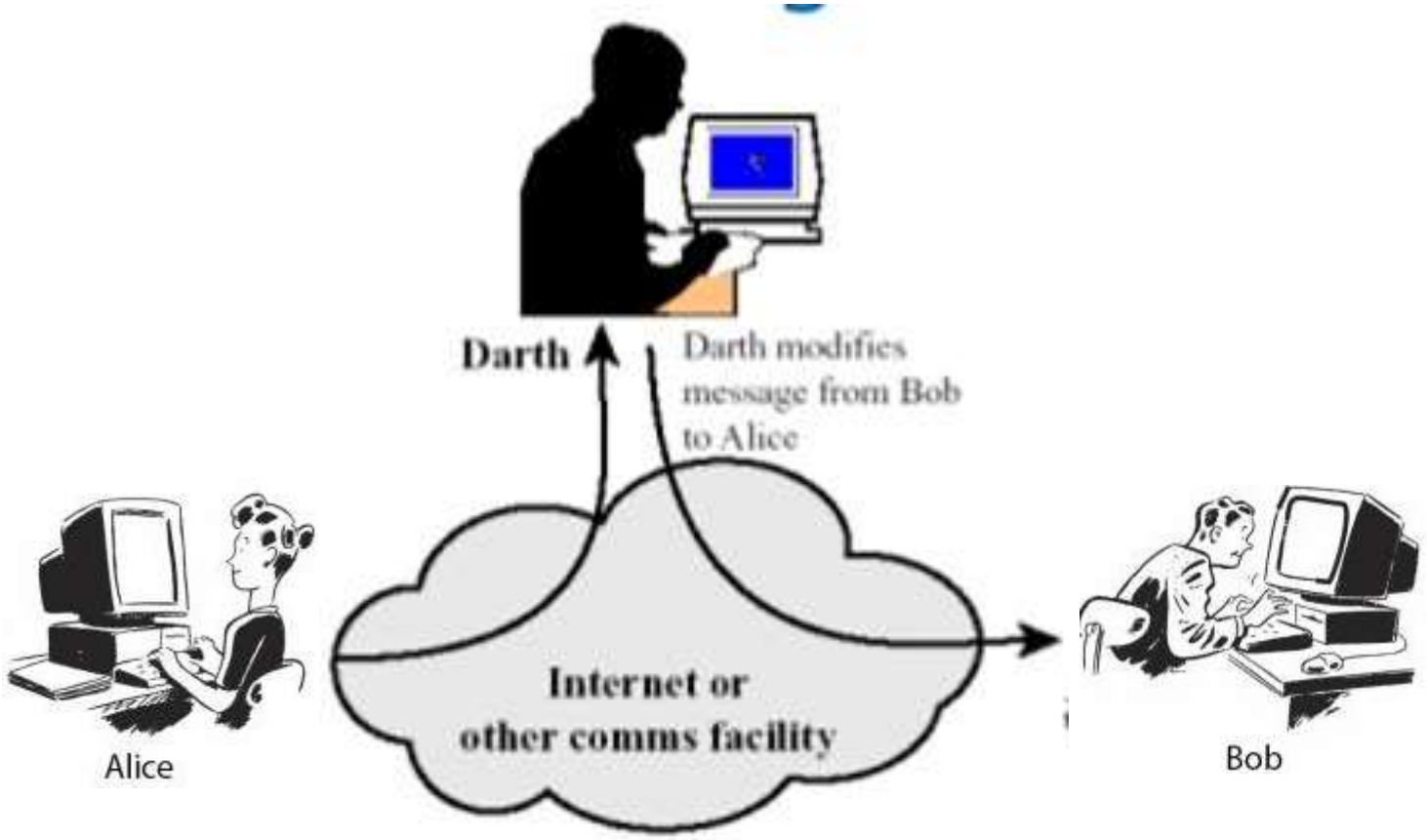
- **Replay**



Source: cryptography and network security william stallings

Active Attack

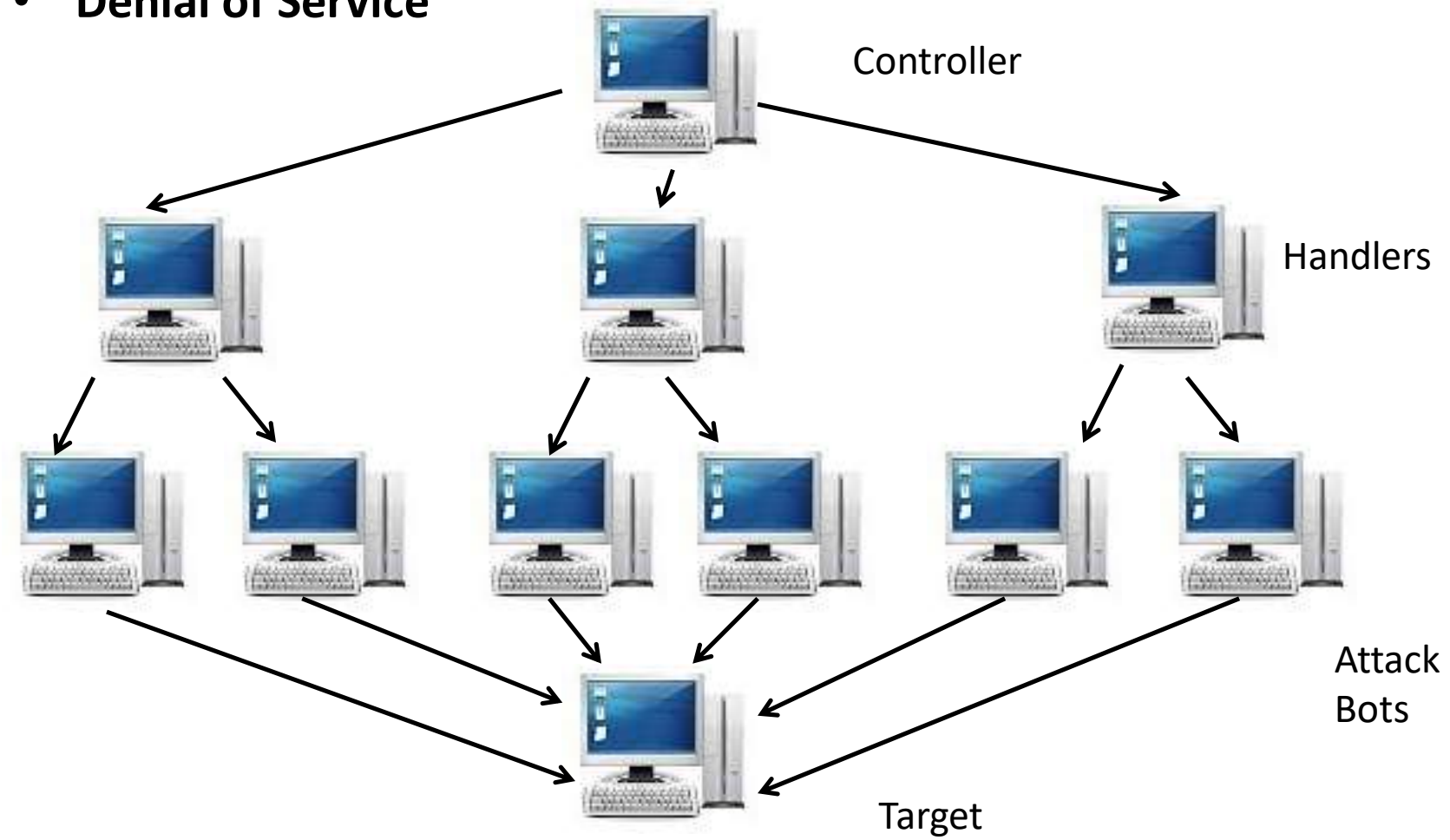
- **Modification of Message**



Source: cryptography and network security william stallings

Active Attack

- **Denial of Service**



Recap

Information Security:

- Confidentiality
- Integrity
- Availability
- **Attacks**
  - Passive
    - Release of the message Content
    - Traffic Analysis
  - Active
    - Masquerade
    - Replay
    - Modification of Message
    - Denial of Service

Information Assurance (IA) (C01)

- IA is defined as the set of measures applied to protect information systems and the information of an organization.
- It ensures availability, integrity, authentication, confidentiality, and non-repudiation of an organization's information and IS.

IA vs IS

Information Assurance	Information Security
• Focuses mainly on strategy	• Focuses primarily on tools and tactics
• Covers information management and protection in a larger domain	• Gives importance and priority to technology.
• Keeps focus on the overall risk management for the security of an organization	• Concentrates on applications and infrastructure developed to provide security and operations.

Information Security

- It protects information from unauthorized access
- Helps to avoid identity theft
- Promotes Information privacy
- Major techniques used are

  Identification, Authentication and authorization of users

- Cryptographic techniques

Source: Swayam

Network Security

- It identifies threats and stops them from entering or spreading into the network

- Network security components include:
  - •Anti-virus and anti-spyware
  - •Firewall
  - •Intrusion prevention systems (IPS)
  - •Virtual Private Networks (VPNs)

Source: Swayam

Security services

- Authentication– verifies the identity of the user
- Authorization– grants permission to authorized users
- Auditing– Increases the system competence
- Non-repudiation– The assurance that someone cannot deny the validity of something.

Guidelines for Secure Password and WI-FI Security

The following are general recommendations for creating a Strong Password:

- A Strong Password **should** -Be at least 8 characters in length
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- Have at least one numerical character (e.g. 0-9)
- Have at least one special character (e.g. ~!@#$%^&*()_-+=)
- A Strong Password **should not** -Spell a word or series of words that can be found in a standard dictionary
- Spell a word with a number added to the beginning and the end
- Be based on any personal information such as user id, family name, pet, birthday, etc.

Guidelines for WI-FI Security

How To Set Your Wi-Fi Security Protocols

1. Type your router's IP address in a web browser's search bar.
2. Enter your router's username and password.
3. Go to Wireless Security. This tab or page may be called something else in your router.
4. Select a security protocol.

- Here is a list of the security protocols ranked from the most secure to least secure:

1. WPAWPA2-PSK (TKIP/AES) – Most secure option, but not available on most routers
2. WPA2-PSK (AES) – Most secure option for most routers
3. WPA2-PSK (TKIP) – Still usable, minimal security
4. WPA-PSK (AES) – Still usable, minimal security
5. WPA-PSK (TKIP) – Not very secure
6. WEP 128 – Risky
7. WEP 64 – Highly risky
8. Open network or no passcode at all – No security

- WPA2 and AES are the best settings to secure your Wi-Fi connection from hackers. If hackers are able to breach your network, they could steal important information, like bank details, or even your identity.

Guidelines for Secure Password and WI-FI Security and social media and Windows Security

Social networking sites like Facebook and Twitter can be a great way to connect with friends. But there are some social networking safety tips you should always keep in mind.

- **Manage your privacy settings.** Learn about and use the privacy and security settings on your social networking sites. They help you control who sees what you post and manage your online experience in a positive way. You'll find some information about Facebook privacy settings at the bottom of this webpage.
- **Remember: once posted, always posted.** Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70% of job recruiters rejected candidates based on information they found online.
- **Build a positive online reputation.** Recent research also found that recruiters respond to a strong, positive personal brand online. So demonstrate your mastery of the environment and showcase your talents.

Guidelines for Secure Password and WI-FI Security and social media

- **Keep personal info personal.** Be careful how much personal info you provide on social networking sites. The more information you post, the easier it may be for someone to use that information to steal your identity, access your data, or commit other crimes such as stalking.
- **Protect your computer.** Security start with protecting your computer. Install Anitivirus. Keep your operating system, web browser, and other software current. You can use the Pitt Software Update Service to automatically download the latest security updates for Windows.
- **Know what action to take.** If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.
- **Use strong passwords.** Make sure that your password is at least eight characters long and consists of some combination of letters, numbers, and special characters (for example, +, @, #, or $).
- **Be cautious on social networking sites.** Even links that look they come from friends can sometimes contain harmful software or be part of a phishing attack. If you are at all suspicious, don't click it. Contact your friend to verify the validity of the link first.

Guidelines for Windows Security

1. Disable Windows 10 automatic login.
2. Set a password with your screensaver.
3. Turn on your firewall.
4. Disable remote access.
5. Enable or install antivirus protection tools.
6. Enable auto-updates for your operating system.
7. Set up file backups.
8. Turn on encryption.
9. Set up your user accounts.
10. Set up a password manager.

Contrasting Internet & Cyberspace

Cyberspace

- It is a symbolic and figurative space that exists within Internet
- It supports multitude of business, government and social interactions through information exchange

Internet

- The design of Internet results in a cyberspace built out of components
- It provides services designed to form more complex services

Security Risk Analysis(CO1)

- The entire process of maintaining organizational security involves assessment, analysis, and management of risks.
- Assessment is identification of any potential risks for a system.
- Analysis means **measuring the effects** that may be caused to the system and providing details to the management team for taking steps that will counter the most concerning issues.

Security Risk Analysis

- Management of risks is to take appropriate steps for removing system vulnerabilities. (Covered this in starting of unit)
- Risk analysis is a continuous process that requires you to constantly monitor the measures employed to maintain security of your systems at present.
- Keep calculating threats evaluating their further effects.
- It keeps the economy in check, that is, the cost of applied security measures never exceed the possible losses.

Risk analysis terminology

Assets	Everything that has some value and needs to be safeguarded
Threats:	possible danger to assets
Vulnerabilities:	any weakness/flaw in the system
Countermeasure:	Countermeasures are the devices or actions with an intent and capability to reduce system vulnerabilities.
Expected losses:	expected impacts of threats on an organization's assets
Impact:	It is usually categorized into four areas, namely, destruction, disclosure, modification, and Denial of Service (DoS).

Key Elements of Risk Analysis

- **Impact statement:** The impact statement describes the damages that may be caused by threats.
- **Effectiveness measure:** The effectiveness measure presents the calculated effectiveness of individual actions taken to counter the impact of threats.
- **Recommended counter measures:** The recommended countermeasures involve possible actions that are cost effective and maintain security of assets in a proper manner.

Risk Management

- **Cyber Services -** Cyber security is crucial. RCS methods keep you secure while identifying & eliminating threats from cyber criminals.

- **Investigation -** RCS knows how to perform discreet, effective, and fully legal investigations for both individuals and organizations.

- **Security Consulting -** RCS identifies and mitigates risks and vulnerabilities. If a problem arises, risk level is determined and action is taken.

- **Business Intelligence -** RCS business intelligence capabilities safeguard your assets & intellectual property from internal & external threats.

Faculty Video Links, Youtube & NPTEL Video Links and Online Courses Details

- https://youtu.be/BvWvFAS1iP0?list=PLUtfVcb-iqn834VGI9faVXGIGSDXZMGp8
- https://youtu.be/ooJSgsB5fIE
- https://youtu.be/tff_X0BMgfk
- https://youtu.be/fQ3ESFfvchg?list=PLUtfVcb-iqn834VGI9faVXGIGSDXZMGp8
- https://swayam.gov.in/nd2_cec20_cs09/preview
- https://www.youtube.com/watch?v=sdpxddDzXfE
- https://www.youtube.com/watch?v=0p3787JiFgQ
- https://www.youtube.com/watch?v=JdfmV2KW11I

Past Sessional Papers

Printed page: 2 Subject Code:ANC0301

Roll No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute)

Affiliated to Dr. A.P. J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow

Course : B.Tech Branch : CSE

Semester : III Sessional Examination : Second Year- (2021 - 2022)

Subject Name: Cyber Security

Time: 1.15Hours [SET- A] Max. Marks:30

General Instructions:

- This Question paper consists of .....pages & .....questions.It comprises of three Sections, A, B, and C
- Section A -Question No- 1 is objective type questions carrying 1 mark each, Question No- 2 is very short answer type carrying 2 mark each. You are expected to answer them as directed.
- Section B - Question No-3 is Short answer type questions carrying 5 marks each. Attempt any two out of three questions given.
- Section C -Question No. 4 &5are Long answer type (within unit choice) questions carrying 6marks each. Attempt any one part a or b.

		SECTION – A	[08Marks]	
1.	All questions are compulsory		(4×1=4)	
	a.	1. How many layers are there in OSI model? a. 4 b. 7 c. 3 d. 8	(1)	CO2
	b.	2. Data security considerations are? a. Backups b. Archival storage c. Disposal of data d. All	(1)	CO2
	c.	3. Full form of IDS? a. Invention detection system b. Illusion detection system c. Intrusion detection system d. None	(1)	CO2
	d.	4. Full form of VIRUS? a. Various Information Resource Under Support b. Very Information Resource Under Support c. Vital Information Resource Under Seize d. none	(1)	CO2

Past Sessional Papers

2.	All questions are compulsory		[2×2=4]	
	a.	Differentiate virus and worms?	(2)	CO2
	b.	Define zero day attack?	(2)	CO2
		SECTION – B	[10Marks]	
3.	Answer any two of the following-		[2×5=10]	
	a.	What is a firewall? Mention all types of Firewalls.	(5)	CO2
	b.	What is spoofing ? What are its different types?	(5)	CO2
	c.	What is e-commerce. Name some e -commerce site. How is payment done while the transaction of goods here?	(5)	CO2
		SECTION – C	[12Marks]	
4	Answer any one of the following-		[1×6=6]	
	a.	What is a Trojan horse in Network security and how it got its name?	(6)	CO2
	b.	Explain intrusion detection system?	(6)	CO2
5.	Answer any one of the following-		[1×6=6]	
	a.	Differentiate between Debit card and Credit card?	(6)	CO2
	b.	Explain the advantages and disadvantages of E-cash?	(6)	CO2

Past Sessional Papers

Printed page: 2 Subject Code: ANC0301

Roll No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute)

Affiliated to Dr. A.P. J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow

Course: B.Tech Branch: CSE

Semester: 3rd Sessional Examination: 2nd Sessional Year- (2021 – 2022)

Subject Name: Cyber Security

Time: 1.15Hours **[SET- B]** **Max. Marks: 30**

General Instructions:

- This Question paper consists of .....pages & .....questions.It comprises of three Sections, A, B, and C
- Section A -Question No- 1 is objective type questions carrying 1 mark each, Question No- 2 is very short answer type carrying 2 mark each. You are expected to answer them as directed.
- Section B - Question No-3 is Short answer type questions carrying 5 marks each. Attempt any two out of three questions given.
- Section C -Question No. 4 &5are Long answer type (within unit choice) questions carrying 6marks each. Attempt any one part a or b.

		SECTION – A	[08Marks]	
1.	All questions are compulsory		(4×1=4)	
	a.	1. How many layers are there in OSI model? a. 4 b. 7 c. 3 d. 8	(1)	CO2
	b.	2. Data security considerations are? a. Backups b. Archival storage c. Disposal of data d. All	(1)	CO2
	c.	3. Full form of IDS? a. Invention detection system b. Illusion detection system c. Intrusion detection system d. None	(1)	CO2
	d.	4. Full form of VIRUS? a. Various Information Resource Under Support b. Very Information Resource Under Support c. Vital Information Resource Under Seize d. none	(1)	CO2

Past Sessional Papers

2.	**All questions are compulsory**		(2×2=4)	
	a.	Define zero day attack.	(2)	CO2
	b.	Differentiate virus, worms, Trojan horse and logic bombs?	(2)	CO2
	SECTION – B		[10Marks]	
3.	**Answer any two of the following-**		(2×5=10)	
	a.	What is spoofing? Explain different types of spoofing?	(5)	CO2
	b.	Explain the working of IDS System with the help of the diagram.	(5)	CO2
	c.	Explain virtual private networks in detail?	(5)	CO2
	SECTION – C		[12Marks]	
4	**Answer any one of the following-**		(1×6=6)	
	a.	What is the data security consideration? Explain in this reference Data backup security, Data archival security and Data disposal consideration.	(6)	CO2
	b.	Discuss Electronic Payment System and its types. Explain the threats to E Commerce.	(6)	CO2
5.	**Answer any one of the following-**		(1×6=6)	
	a.	What is Firewall and explain the types of Firewall?	(6)	CO2
	b.	Differentiate between Debit card and Credit card?	(6)	CO2

Old Question Papers

Printed Pages:01 **Sub Code: RUC 501**

Paper Id: 199503 **Roll No.**

B TECH

(SEM V) THEORY EXAMINATION 2018-19

CYBER SECURITY

Time: 3 Hours ***Total Marks: 70***

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt *all* questions in brief. **2 x 7 = 14**

a. Write a short note on the Copyright Act?
b. What do you mean by physical Security for informationSystems?
c. Describe Intellectual Property Issues (IPR).
d. Write short notes on "Patent Law".
e. What do you mean by WWW policy?
f. Give small notes on Corporate Policy.
g. Differentiate between Cyber Security and Information Security.

SECTION B

2. Attempt any *three* of the following: **7 x 3 = 21**

a. What are the key differences between Symmetric and Asymmetric encryption?
b. Explain Information Security Governance in detail and process involved in the Risk Management?
c. Explain briefly about Application Development Security with guidelines.
d. Elaborate the term Access Control. What is include in authorization process for (File, Program, Data rights) and explain the all types of controls.
e. What do you understand by security structure (Architecture) and design?

Old Question Papers

SECTION C

3. Attempt any *one* part of the following: 7 x 1 = 7

(a) What do you mean by Intellectual Property? Describe various means using which Intellectual Property may be protected to an extent.

(b) Explain Confidentiality, Integrity and Availability in terms of cyber security.

4. Attempt any *one* part of the following: 7 x 1 = 7

(a) What are the approaches followed in developing Information System (IS)? Explain the difference between security and threats.

(b) What is the need of information Security also explain the term ISMS?

5. Attempt any *one* part of the following: 7 x 1 = 7

(a) Explain the role of Security in Internet and Web Services.

(b) What is Intrusion Detection System? Explain with Block Diagram.

6. Attempt any *one* part of the following: 7 x 1 = 7

(a) Explain in Detail about Secure Information System Development.

(b) Describe the working principle of CCTV.

7. Attempt any *one* part of the following: 7 x 1 = 7

(a) What are the Data Security Considerations? Explain in this reference Data Backup Security.

(b) What is Public Key Cryptography? Define its Advantage and Disadvantage.

Old Question Papers

Printed Pages : 1 Roll No. | | | | | | | | | | AUC002

COMMON TO ALL BRANCHES
THEORY EXAMINATION (SEM-IV) 2016-17
CYBER SECURITY

Time : 3 Hours *Max. Marks : 100*

Note : Be precise in your answer.

SECTION – A

1. Attempt all of the following questions: **10 x 2 = 20**

(a) What is CIA (Confidentiality, Integrity and Availability) trade?
(b) What are the threats to information system?
(c) What is System Development Life Cycle (SDLC)?
(d) Define the terms RTGS and NEFT.
(e) What do you mean by virus, worm and IP spoofing?
(f) How cyber security is different from computer security?
(g) State the difference between Risk Management and Risk Assessment.
(h) Explain briefly about disposal of data.
(i) Define IT asset and the security of IT Assets.
(j) What is the need of cyber laws in India?

Old Question Papers

SECTION – B

2. Attempt any five parts of the following question: 5 x 10 = 50

(a) What are biometric? How can a biometric be used for access control? Discuss the criteria for selection of biometrics.

(b) What is Intrusion Detection System (IDS)? Explain its type in detail.

(c) What are the backup security measures? Discuss its type.

(d) What are the basic fundamental principles of information security? Explain.

(e) Write a short note on CCTV and its applications.

(f) What is Electronic cash? How does cash based transaction system differ from credit card based transactions?

(g) What do you mean by Virtual Private Networks? Discuss authentication mechanism used in VPN.

(h) **Write a short note on:**

(i) Database Security (ii) Email Security (iii) Internet Security

SECTION – C

Attempt any two of the following questions: 2 x 15 = 30

3. What is Electronic Data Interchange (EDI)? What are the benefits of EDI? How can it be helpful in governance?

4. What is digital signature? What are the requirements of a digital signature system? List the security services provided by digital signature.

5. Explain the following in detail :

(i) Private Key cryptosystem and Public key cryptosystems.

(ii) Firewall.

Expected Questions for University Exam

1. Compare cyber security, information security, Information assurance.
2. Differentiate Cyber space and Internet.
3. Explain man-in-the –middle attack.
4. Explain scope of information assurance
5. What is decision support system
6. Explain the term vulnerability and threats. How these are related?

Recap

- Information Systems have become integral part of any systems

- Every fraction of a second, lot of information is exchanged and the strong information system framework support is necessary.

- Hence, this module has discussed about all the security measures, principles needed to preserve Information security

Summary

In this digital era when everything is accessed and operated through cyber space, security is the very important feature. To understand the need for cyber security, different incidents and statistical reports are presented. Lack of security may lead to setbacks in financial matters, personal and professional operations. Important terms related to Cyber Security are also discussed in this module. Different types of Cyber threats, the methods of Cyber Attacks are also explained. The four important fundamentals of security and the other essentials in securing the computers are also explored to understand the basic operations in cyberspace.

Cyber security is a broader term which protects all the hardware (devices, routers, and switches), software, information, and data that are part of the cyber space. Cyber Security cannot be misguided with data security.

References

1. Charles P. Pfleeger, Shari Lawerance Pfleeger, “Analysing Computer Security ”, Pearson Education India.
2. V.K. Pachghare, “Cryptography and information Security”, PHI Learning Private Limited, Delhi India.
3. Dr. Surya Prakash Tripathi, Ritendra Goyal, Praveen kumar Shukla ,”Introduction to Information Security and Cyber Law” Willey Dreamtech Press.(prefer)

Thank You