Secure System Development

Unit: 3

Cyber Security

ANC0301

(B Tech IIIrd Sem)

Mr. Sujeet Singh Bhadouria

Assistant Professor (CSE)

NIET, Gr. Noida

Faculty Profile

FACULTY PROFILE
Name of Faculty: Sujeet Singh Bhadouria

Designation & Department: Assistant Professor, CSE

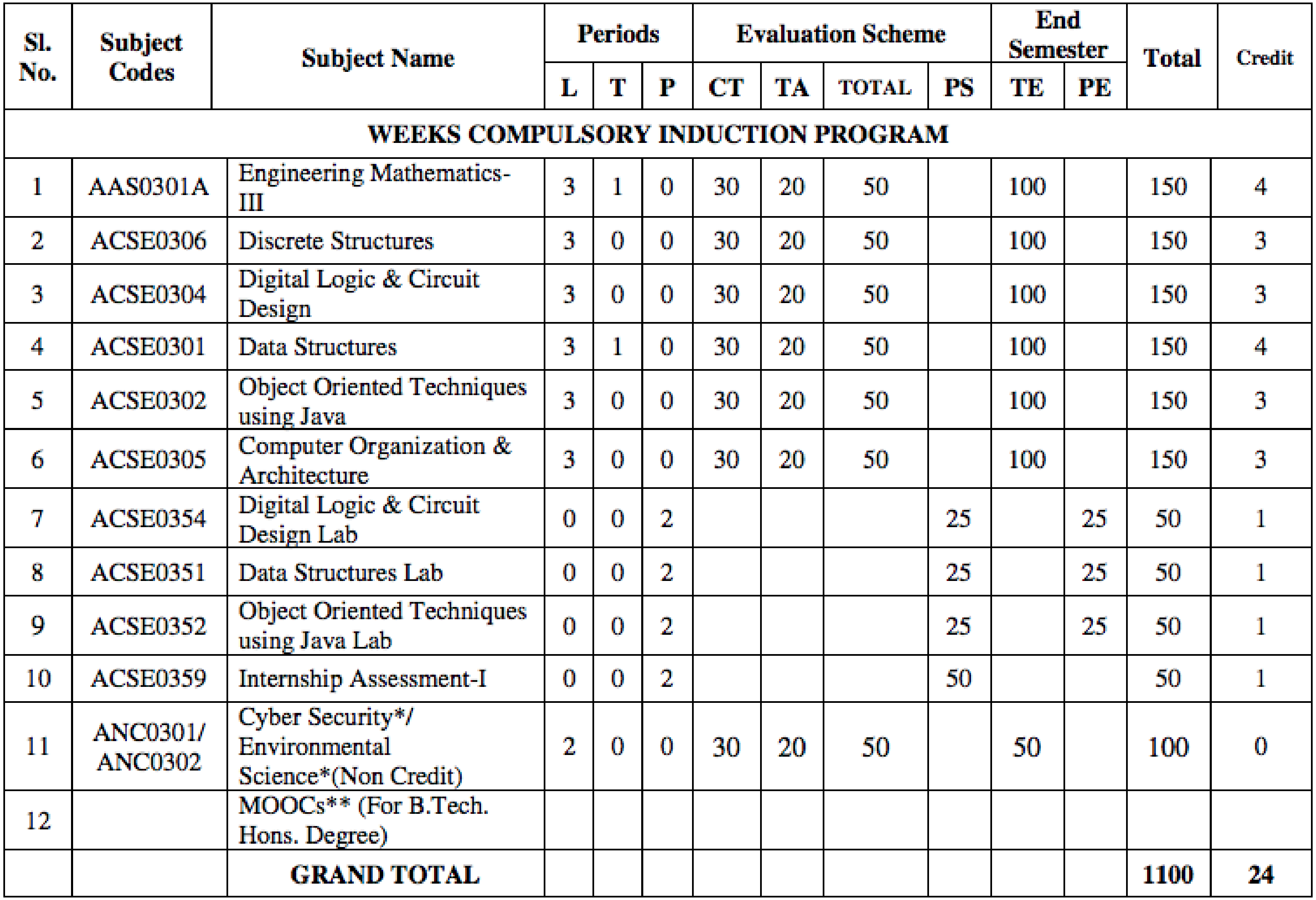
Qualification: Ph.D (Pre-Submission) M.Tech

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.

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 Information and Technology 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.

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.

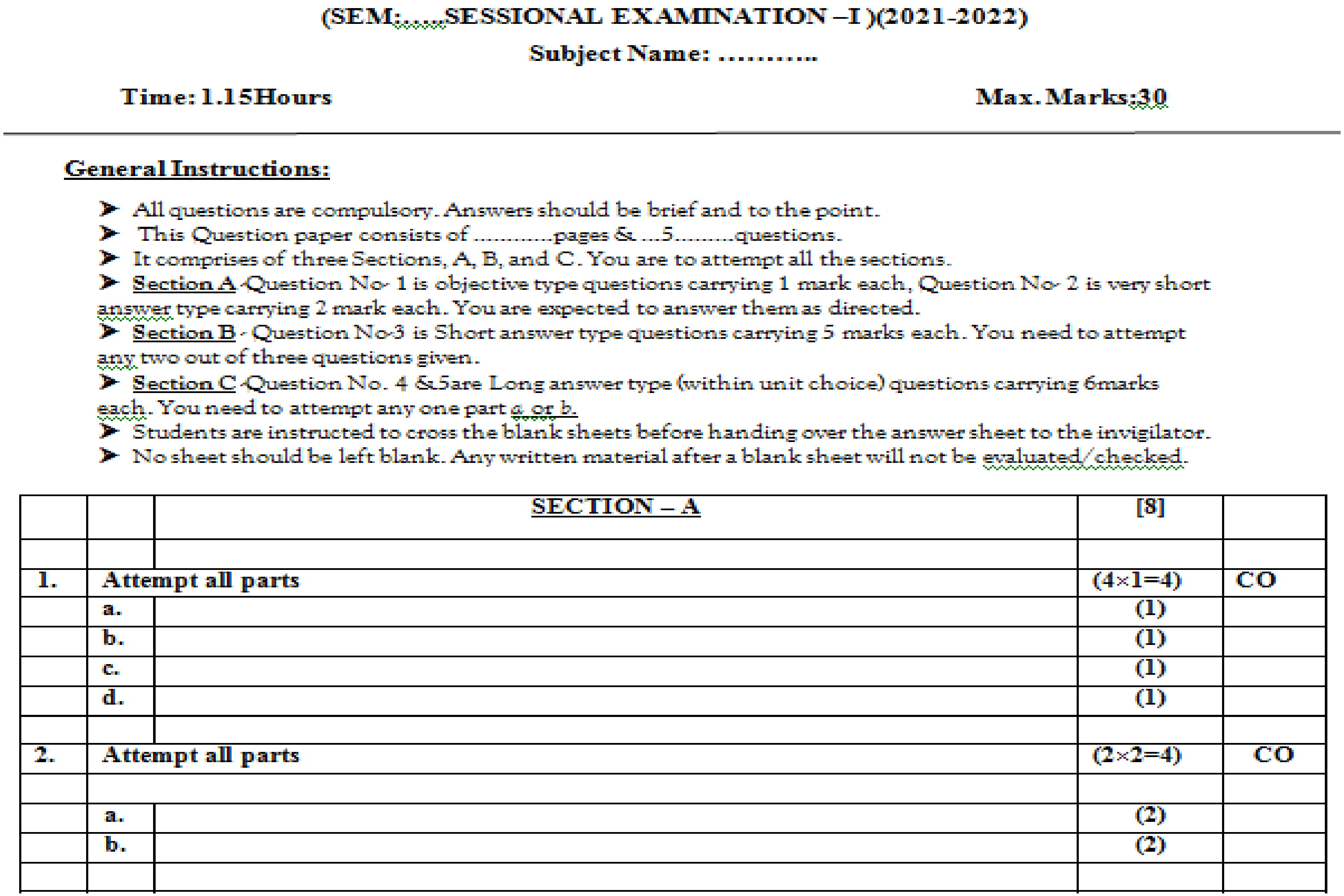
PEO2: To lead a successful career in industries or to pursue higher studies or to understand entrepreneurial endeavors.

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: ....

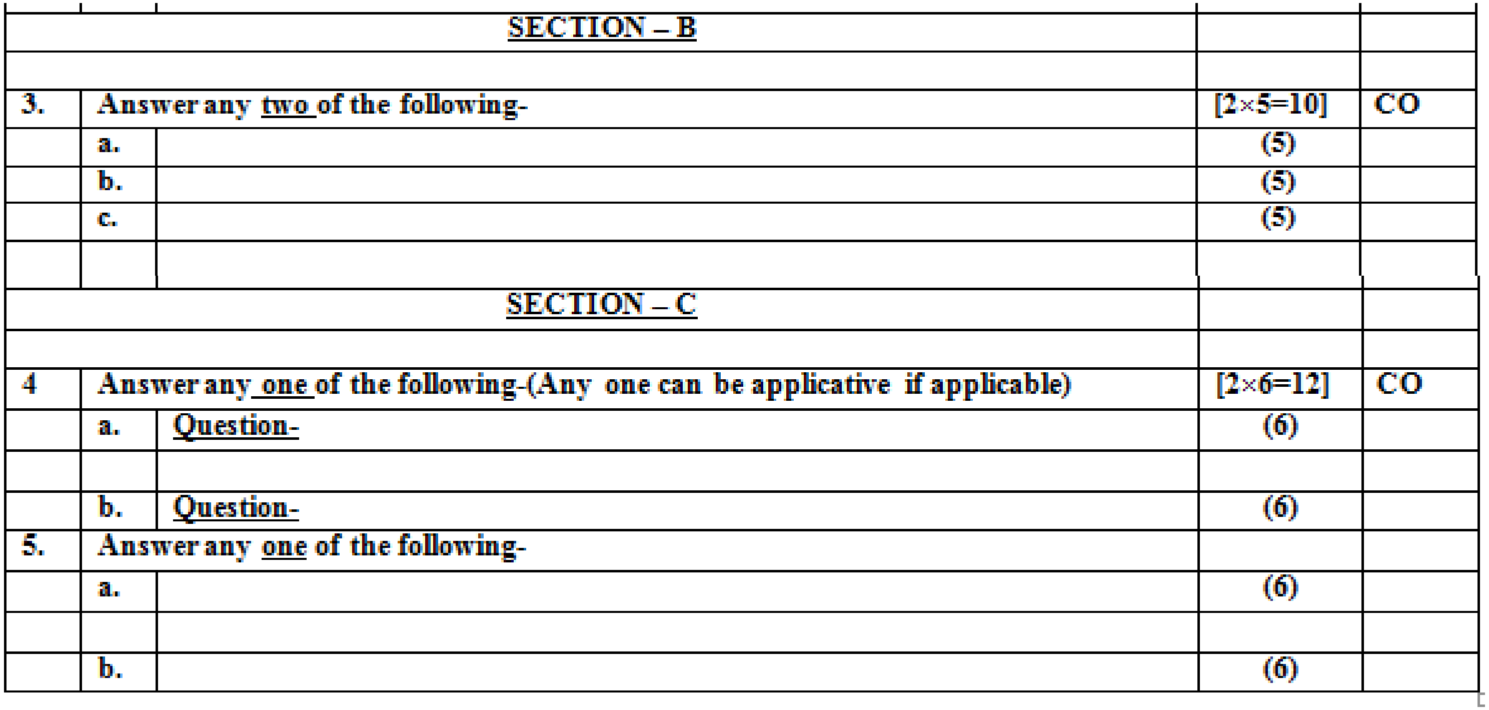
Time: 1.15Hours **Max. Marks:30**

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.

Brief Introduction about the Subject

- 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/

Unit Content

- Developing Secure Information Systems
- Application Development Security,
- Information Security Governance & Risk Management,
- Security Architecture & Design
- Security Issues in Hardware, Data Storage & Downloadable Devices,
- Physical Security of IT Assets, Access Control, CCTV and Intrusion Detection Systems
- Backup Security Measures.

Unit Objective

Topic	Objective
Application Development Security	Develop an understanding of Secure Information System Development and integration of security in development phases
IS Governance & Risk Management	Study of Information Security Governance & Risk Management
Security Architecture & Design Security Issues in Hardware	Examine the Security Architecture and Design Security Issues in Hardware
Data Storage	Understand the security issues in data storage and Downloadable Devices
Physical Security of IT Assets	Develop an understanding of Access Control, CCTV and IDS
Backup Security Measures	Study of concept of Backup Security Measures

Objective of Topics

Topic	Objective	CO Mapping
Application Development Security	Develop an understanding of Secure Information System Development and integration of security in development phases	CO3

Prerequisite

- Denial of Services Attack
- Threats to E-Commerce
- Mobile, cloud security

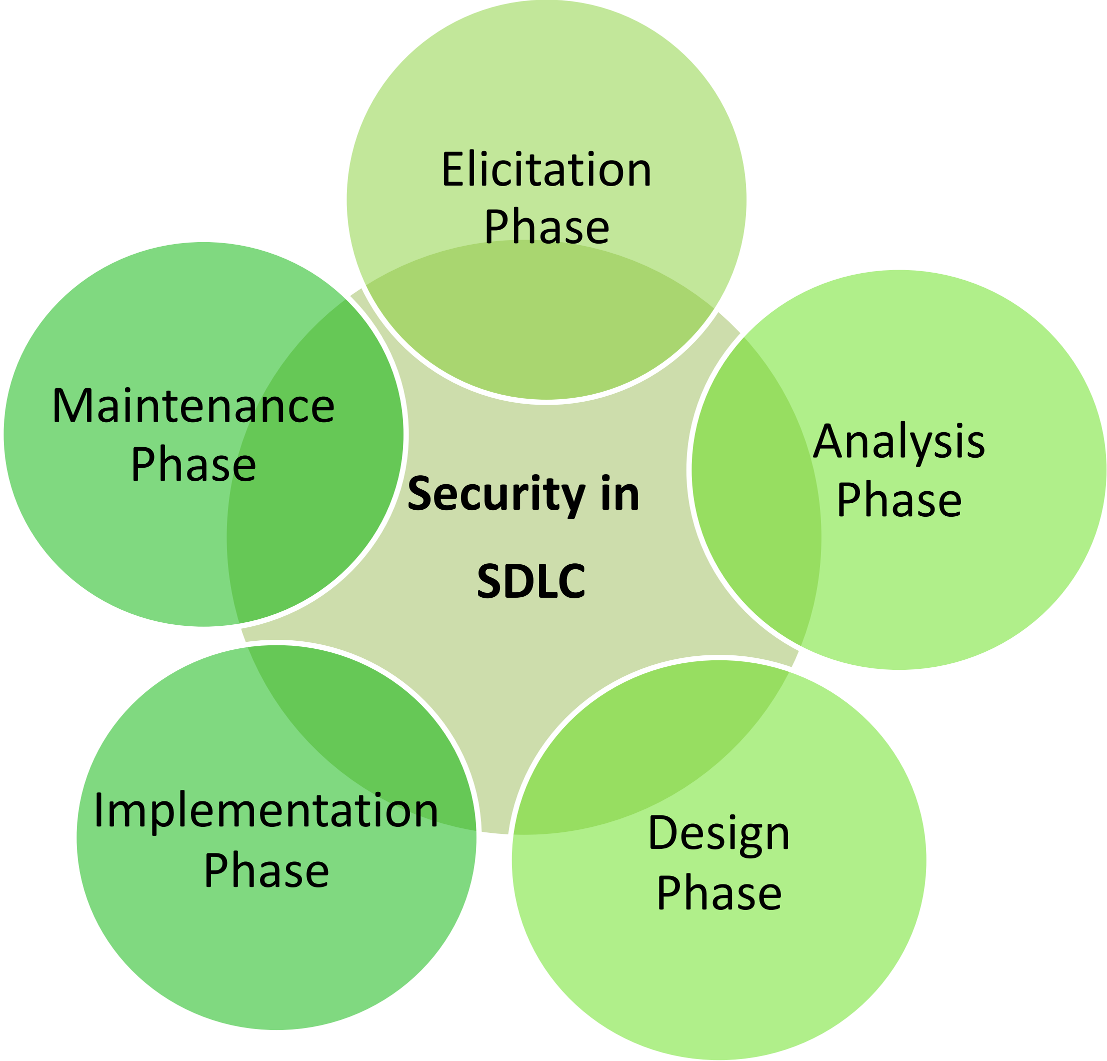
Secure Information System Development(CO3)

- During secure system development, stakeholders have to decide and select the development activities.
- Traditional system and software engineering lifecycles, such as Waterfall, V-model, Spiral, Prototype development, Agile, Incremental development, could be a good starting option. However, traditional development lifecycles do not take into account security concerns in particular.

Therefore, there exist approaches which focus on security development techniques, methods, and tools. The three secure system development lifecycles:

1. Microsoft Secure System Development Lifecycle
2. Open Web Application Security Project (OWASP) and Comprehensive Lightweight Application Security Process (CLASP)
3. Seven Touchpoints for Software Security

Integration of Security in SDLC Phases



Source: Springer link

Integration of Security in SDLC Phases

The Elicitation Phase:

- Determines the security requirements of the software application by executing a simple risk analysis exercise
- Information asset identification and valuation
- Threat identification and assessment
- Risk (asset/threat) identification
- Determine the level of vulnerability
- Risk assessment
- Risk prioritisation.

Integration of Security in SDLC Phases

The Analysis Phase:

- Determines the security services to be used to satisfy the security requirements;
- During the analysis phase, security services are selected according to their ability to mitigate the security risks identified.
- The output of this phase is a refined set of security requirements.
- Identify the relevant security services and level of protection required to mitigate each risk

Integration of Security in SDLC Phases

The Design Phase:

- determines how the security services will be implemented
- Map security services to security mechanisms;
- Consolidate security services and mechanisms.

The Implementation Phase:

- Identifies and implements appropriate software security tools and components
- Map security mechanisms to software security components.

Integration of Security in SDLC Phases

The Maintenance phase :

- During this phase, it is important to find ways to evaluate the security of the system to ensure that the system is as secure as intended
- Improve the auditability of the software application .
- Users and operations staff need to be educated in using the software application in a secure manner.

Application Development Security (CO3)

- Information is available for organizations in the form of assets, which need to be used (collected, stored, shared, and deleted) in an intelligent manner.

- An intelligent use of information assets helps organizations in maintaining themselves ahead of their competitor organizations.

- Therefore, these assets need to be protected from any kind of threats that may result into breach of confidentiality, integrity, or availability of resources.

Issues related to the secure development of applications

- Less trained/ skilled developers

- Less educational focus on secure development

- Difficulty of finding the right information related to specific security measures for particular applications or application development strategies.

- Lifecycle systems considering security mostly in the last phases only.

Common Framework for Application Security

Secure applications can be developed by following certain specifications that contains foundation, principles, and design guidelines.

- Foundation: Foundation is the basic knowledge of the development procedure and security issues to consider before starting to develop the application.
- Principles: Principles are the basic rules to be followed during the application development process.
- Design Guidelines: Design guidelines include the best code implementation methods that are tested and have been proven successful over time.

Daily Quiz

1. What is application security?

2. Mention some Information Security consideration?

3. What is SDLC?

Topic Links

- https://youtu.be/snJGzyXzVec
- https://youtu.be/8caqok3ah8o

Recap

Integration of Security in SDLC Phases(Sec SDLC)

1. Elicitation Phase
2. Analysis Phase
3. Design Phase
4. Implementation Phase
5. Maintenance Phase

Objective of Topics

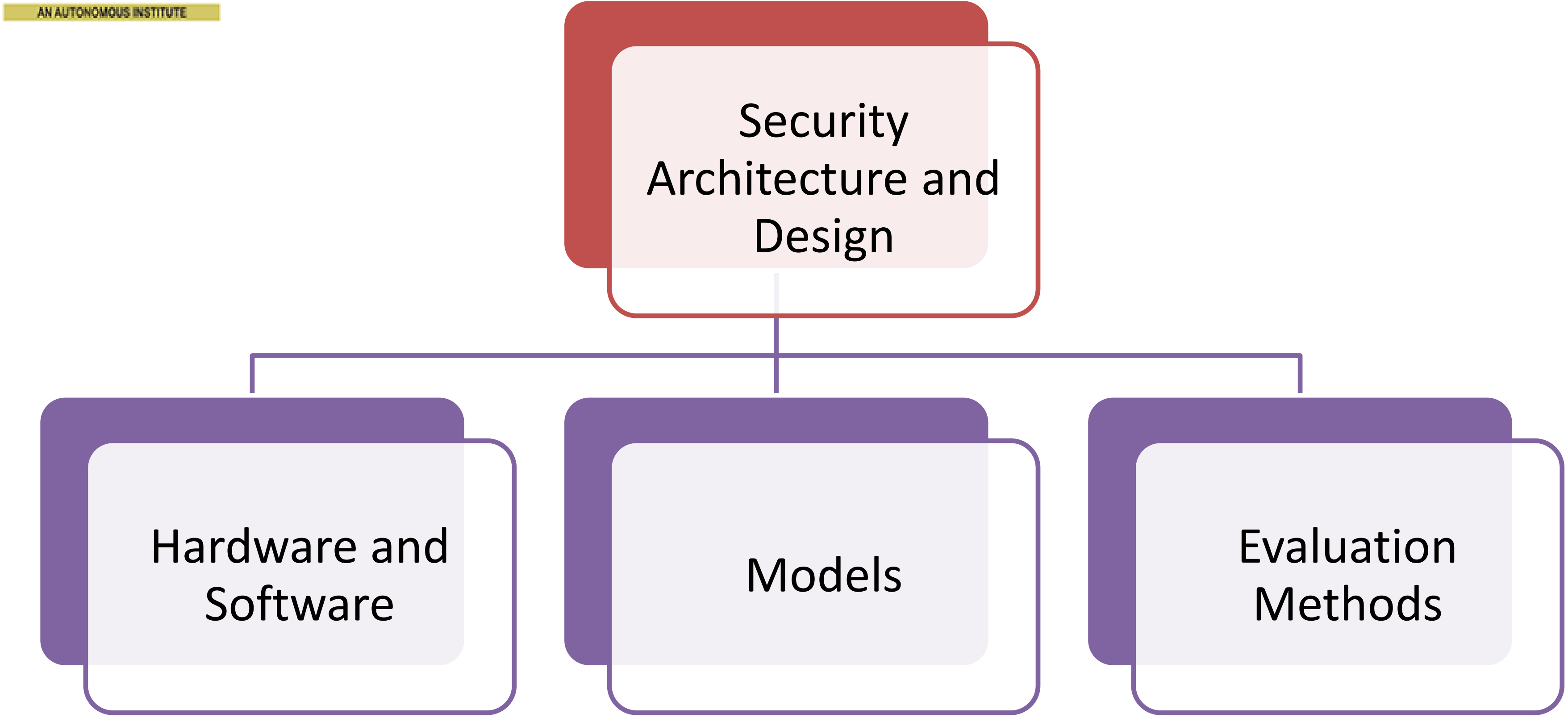
Topic	Objective	CO Mapping
Security Architecture & Design Security Issues in Hardware	Examine the Security Architecture and Design Security Issues in Hardware	CO3

Architecture and Design (CO3)

- Security Architecture Components-

  - Hardware
  - Operating System
  - Software

Architecture and Design (CO3)



Provides the way to design secure system

Explains the way to maintain the security of this system

Describes the level of security of a system.

Concepts for Secure System Design

1- Layering:

- Layering is a concept that arranges hardware, drivers for kernel and devices, operating system, and applications in a sequential order.
- The layering approach is used to differentiate the hardware from the software into different tiers.
- A generic list of security architecture layers is as follows

1. Hardware (bottom layer)

2. Kernel (a part of OS) and device drivers

3. Operating System

4. Application software (Top Layer)

Concepts for Secure System Design

2-Abstraction :

- The purpose of abstraction is to hide unnecessary details from users.
- We will only increase the risk of threats if we increase the complexity of the system.
- 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.

Concepts for Secure System Design

3-Security Domain :

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.

Concepts for Secure System Design

4-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

Concepts for Secure System Design

5- 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)

Daily Quiz

1. What does secure architecture design means?

2. What are Security Issues with Hardware?

3. What is security analysis?

4. What are the principles for secure system design?

Weekly Assignment

1. What do you mean by Application Security? Name the two protocol use for Email Security and Explain?
2. Elaborate the term access control? What is include in authorization process for (File, Program, Data rights) and explain the all types of control?
3. Define Vendor challenges and user challenges for application security?
4. Write a short note on data disposal.
5. What do you mean by physical security of IT assets?
6. Explain Information security governance.
7. Write design Security Issues in Hardware, Data Storage & Downloadable Devices?
8. What are the different Measures of Backup Security
9. What are the different types of Biometric?
10. Explain the Principles for Secure System Design

Topic Link

- https://youtu.be/cUvMIOdaSBs

Security Issues with Hardware (CO3)

- Hardware mainly faces security issues related to:

  -Stealing

  -Destruction,

  -Gaining unauthorized access

  -Breaching the security code of conduct.

- Example- if an organization has given laptops to some of its employees, it can be possible that they are using their laptop for illegitimate activities, which result into threats for the organizations' data integrity and confidentiality.

Ways to Secure Hardware

- Locks and access control mechanisms-
  - Biometric access control,
  - Authentication codes/tokens,
  - Radio Frequency Identification (RFID), etc.
- You also need to apply Local intranet and Virtual Private Networks (VPNs) to provide complete security for your system.
- However, network routers are also subjected to eavesdropping and other kinds of attack that may harm your organization’s internal security.

Daily Quiz

1. What is hardware security?

2. Differentiate breaching and stealing.

Topic Link

- https://youtu.be/Ye2H1n2MtIc
- https://youtu.be/xwgeclX3E4I

Objective of Topics

Topic	Objective	CO Mapping
Data Storage and Downloadable Devices	Understand the security issues in data storage and Downloadable Devices	CO3

Security Issues with Downloadable (Peripheral)Devices (CO3)

- **Peripheral devices :** The term peripheral device refers to all hardware components that are attached to a computer and are controlled by the computer system, but they are not the core components of the computer.
- Peripherals can also be defined as devices that can be easily removed and plugged into a computer system. Types are:

1. Input device sends data or instructions to the computer, such as Mouse, Keyboard, Scanner.
2. Output device provides output data from the computer, such as a Monitor, printer, projector.
3. Storage Device which performs both input and output functions, such as CDs, DVDs, Pen drive, Memory card.

Security Issues with Downloadable (Peripheral)Devices (CO3)

.The threats to the security of data storage devices can be External or Internal.

1. **Internal :** If you have stored some data on a CD and some unauthenticated user gets access to that CD, he/she may use it unlawfully. If the device has inbuilt security mechanisms, then it can be destroyed, thereby resulting in loss of some crucial data. This can create problems for data integrity and availability.
2. **External :** In external threat, unseen entity can create a change which cannot be easily detected. Such change of information if is allowed in the data storage device, then a person may alter the data in such a way that it is no longer available for authenticated users.

Security Issues with Downloadable (Peripheral)Devices (CO3)

Their loss and theft, disposal, stealing of data, denial of data, malware introduction, etc.

Specific security measures should be applied to protect information from being damaged, stolen, or corrupted by internal or external threats.

Introduction to Mobile Device Security(CO3)

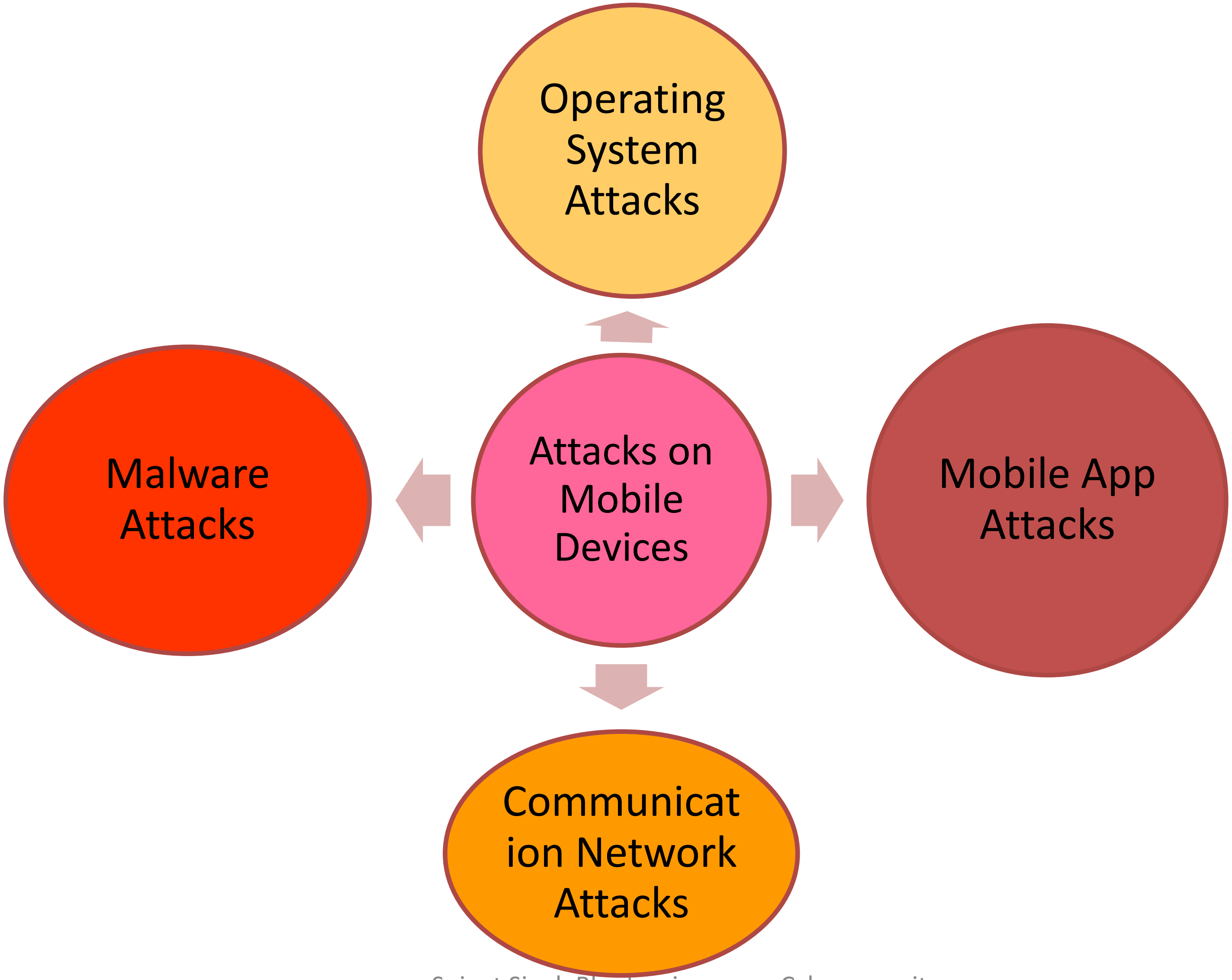
- At present around the world, up to five billion people are using mobile phones

- This has led to the rapid increase of cyber criminals

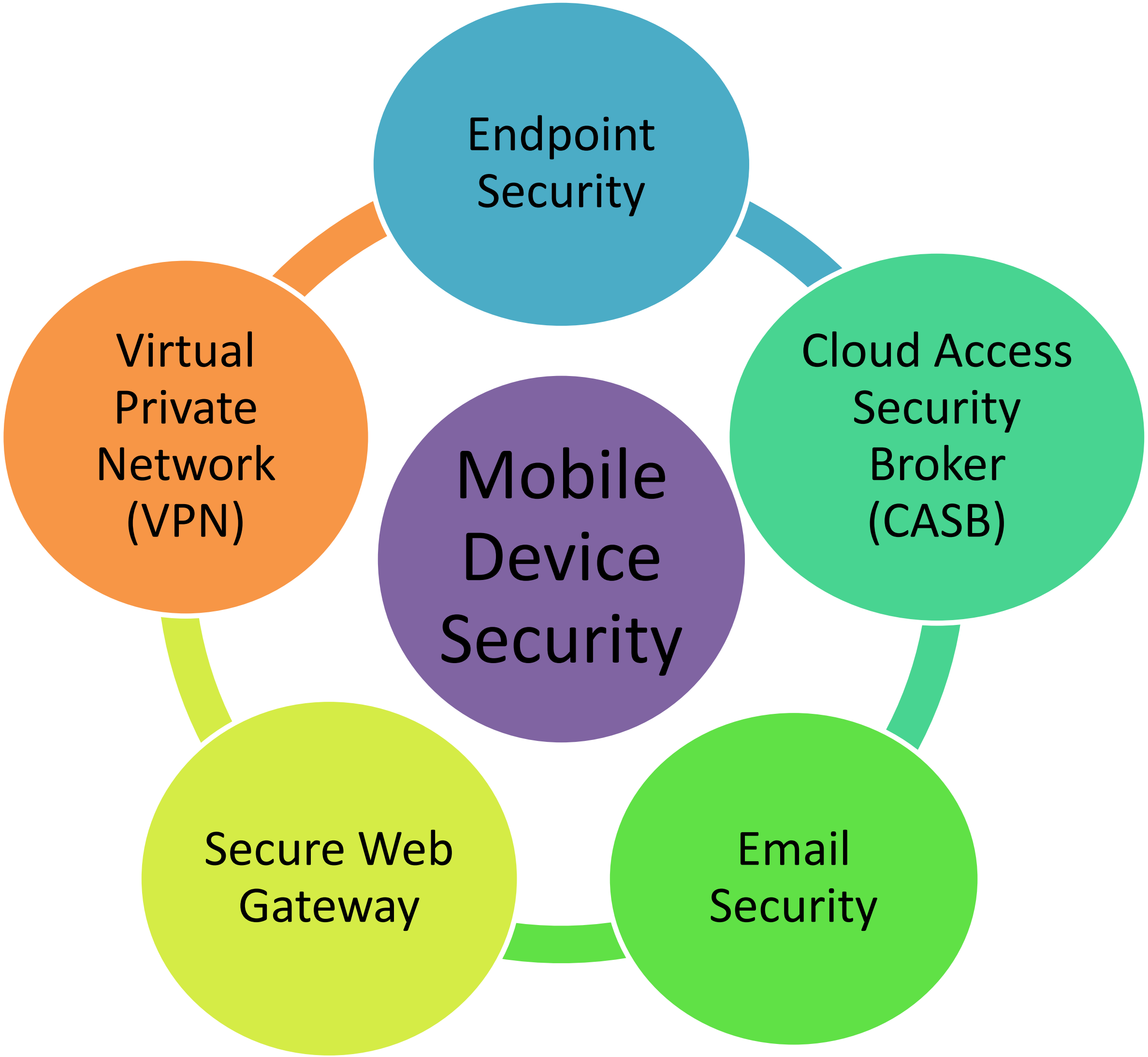
- They make use of the information obtained through mobile phones to earn profit and pushing users to become victims of cybercrimes

- Hence, mobile users must be aware of the potential threats caused by the cybercriminals as they are usually casted in wide nets

Various Attacks on Mobile Devices

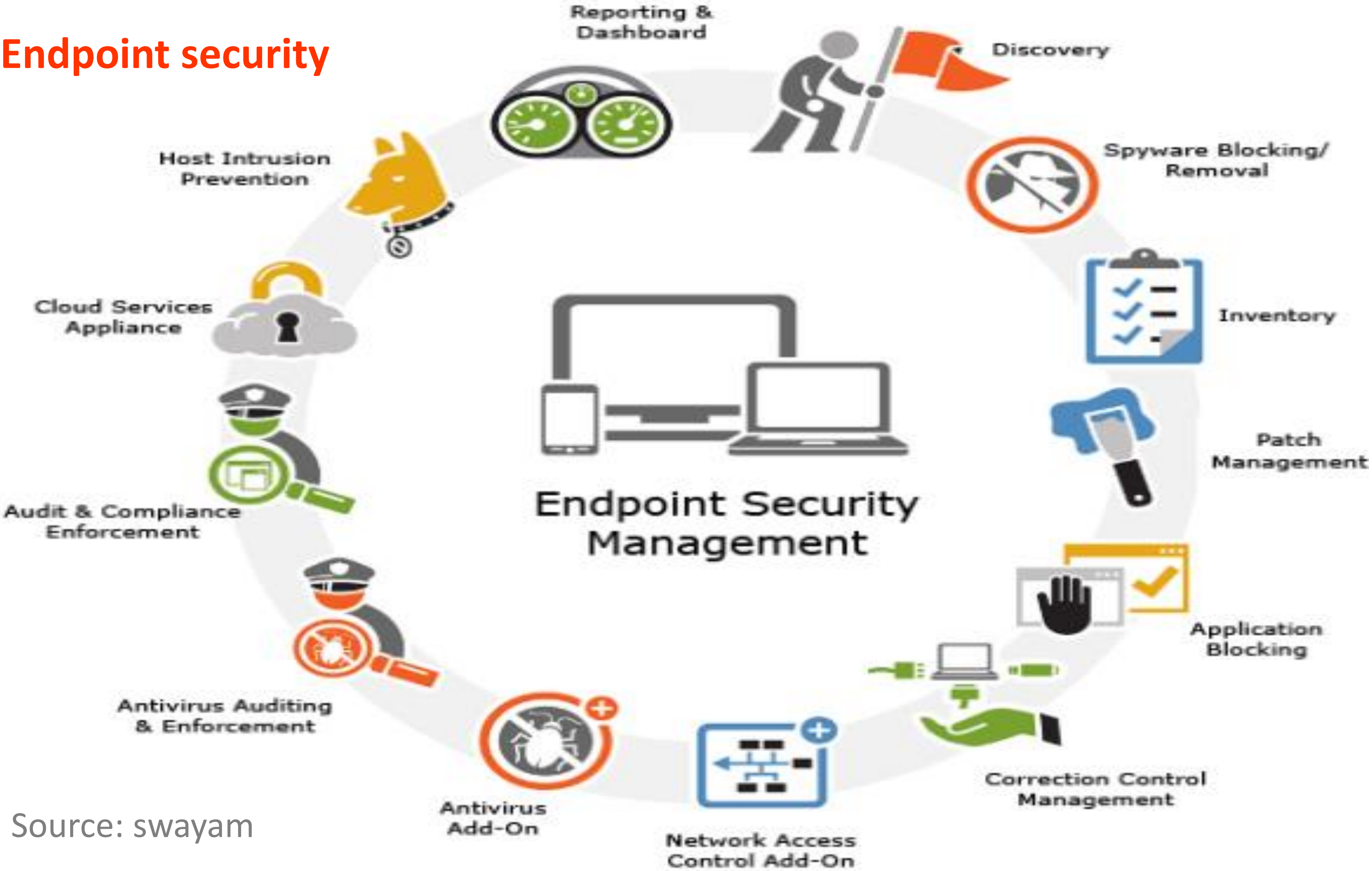


Components of Mobile Device Security



Components of Mobile Device Security

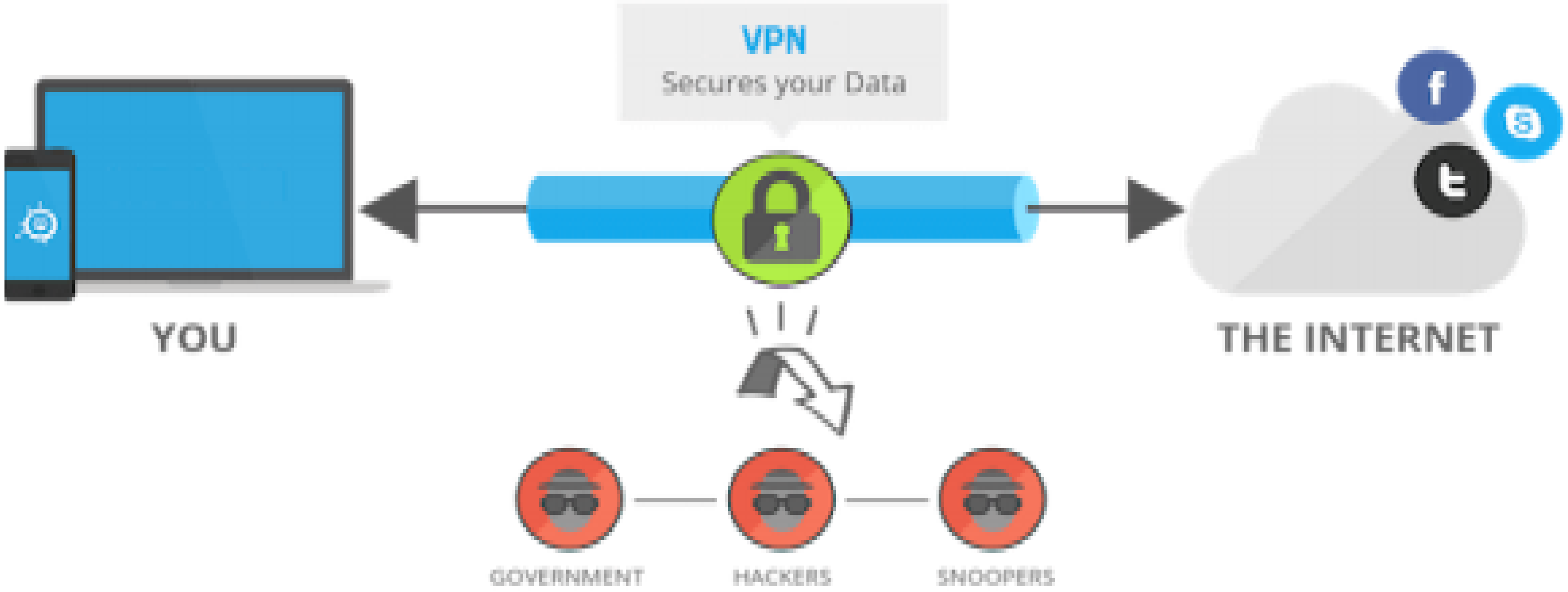
Endpoint security


Reporting & Dashboard
Discovery
Spyware Blocking/ Removal
Inventory
Patch Management
Application Blocking
Correction Control Management
Network Access Control Add-On
Antivirus Add-On
Antivirus Auditing & Enforcement
Audit & Compliance Enforcement
Cloud Services Appliance
Host Intrusion Prevention
Endpoint Security Management

Source: swayam

Components of Mobile Device Security

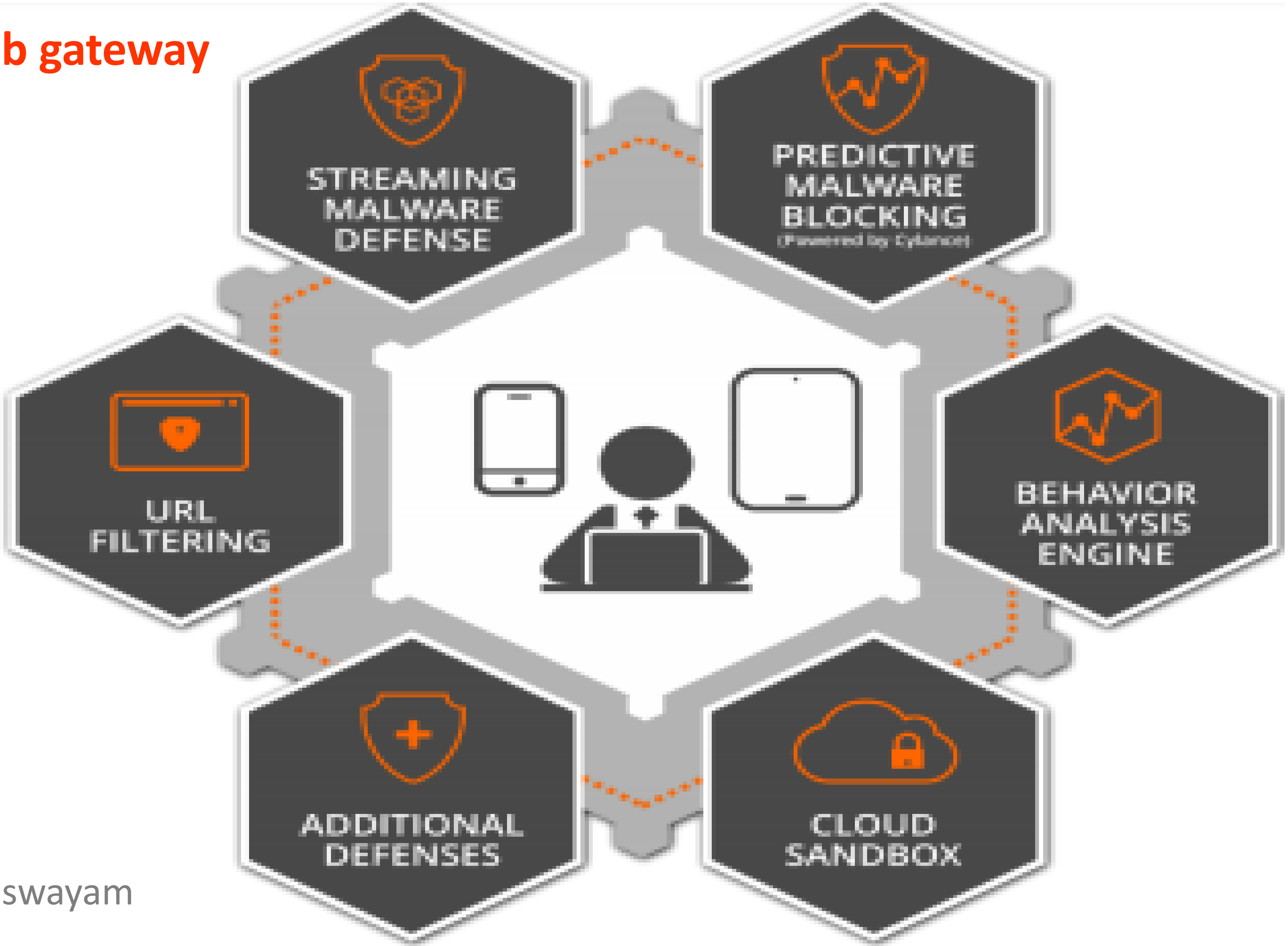
VPN



Source: swayam

Components of Mobile Device Security

Secure web gateway



Source: swayam

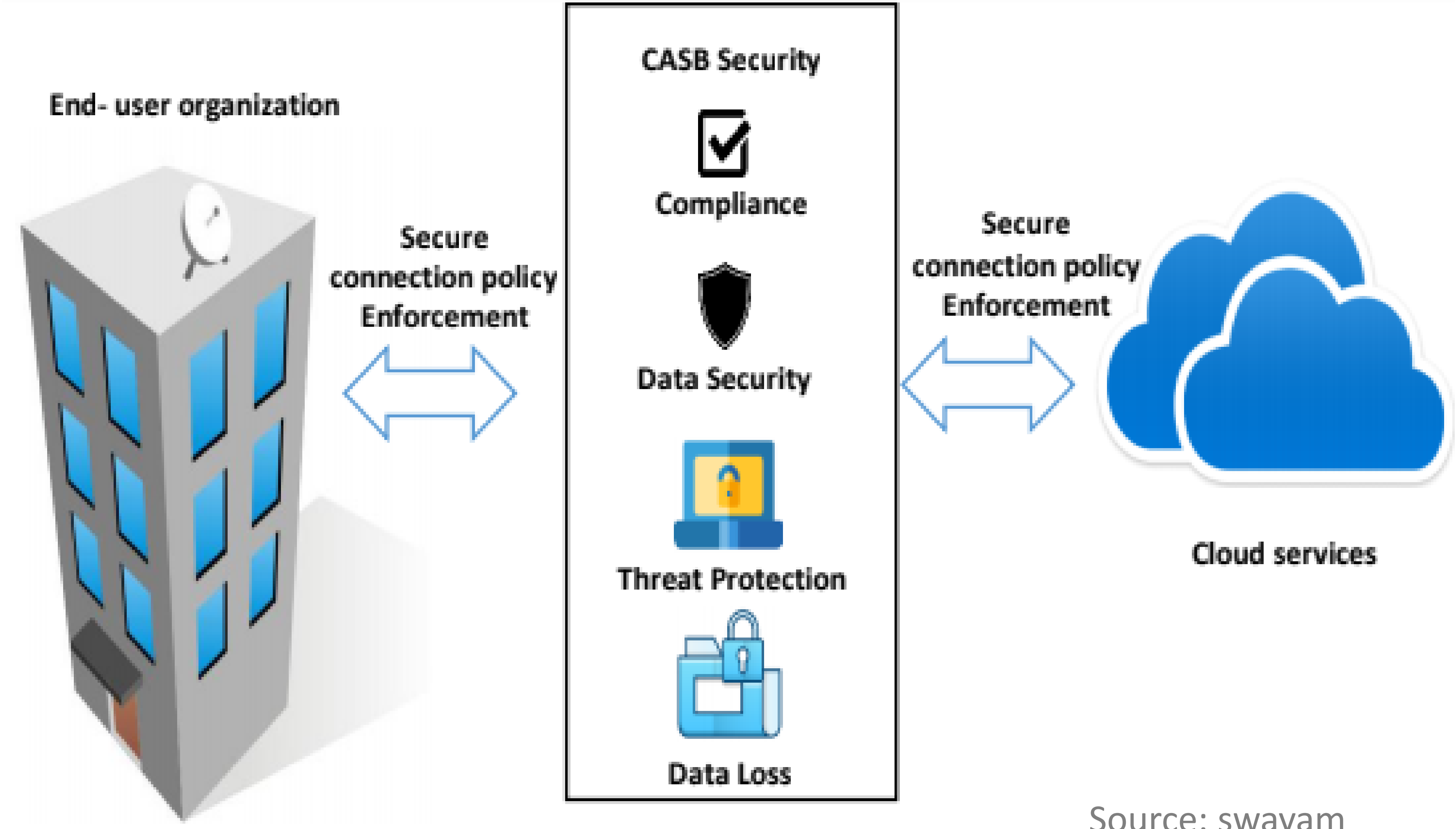
Components of Mobile Device Security

Email security

Source: swayam

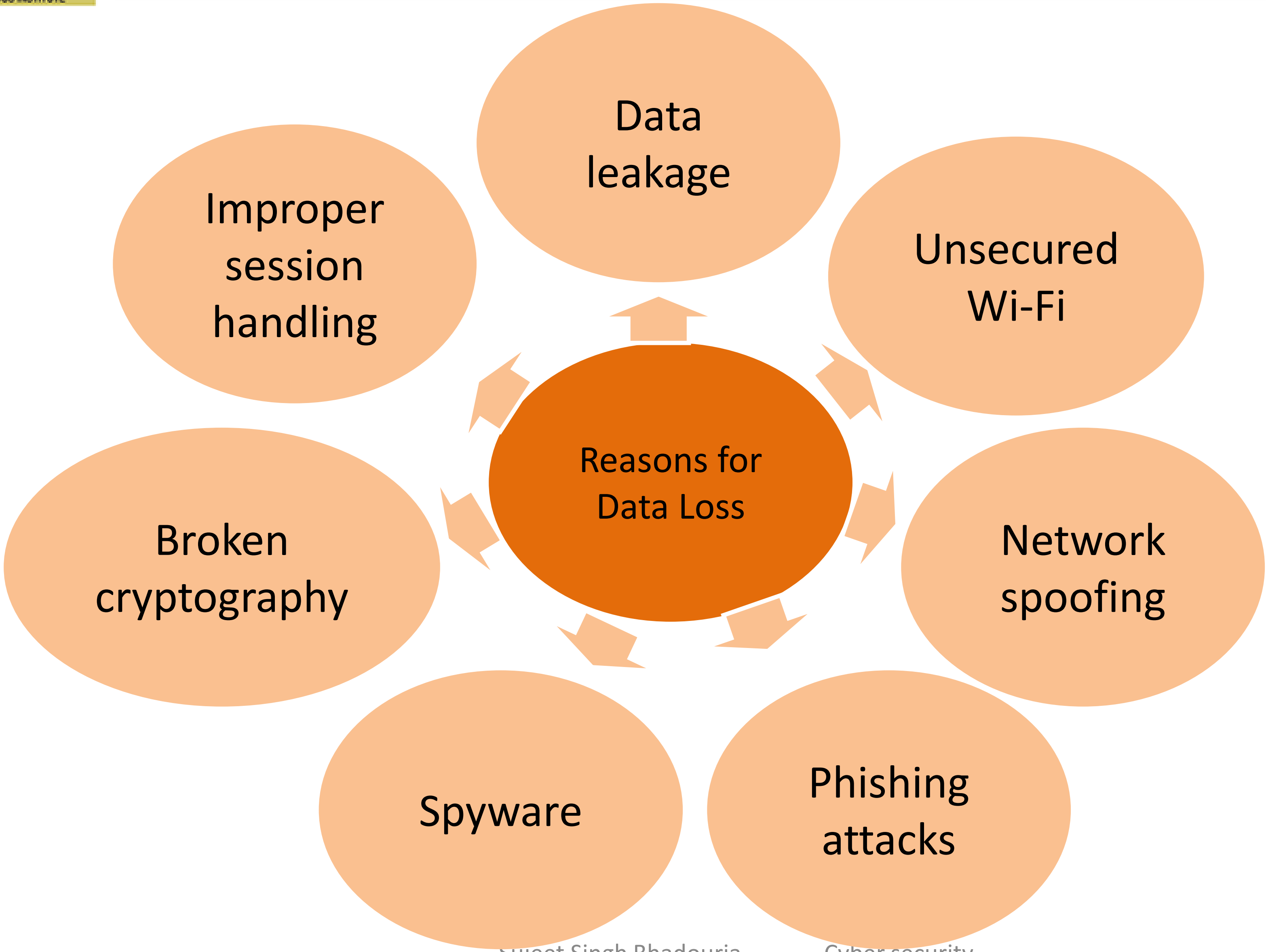
Components of Mobile Device Security

Cloud Access Security Broker (CASB)



Source: swayam

Common Mobile Device Security Threats


Reasons for Data Loss

Data leakage

Unsecured Wi-Fi

Network spoofing

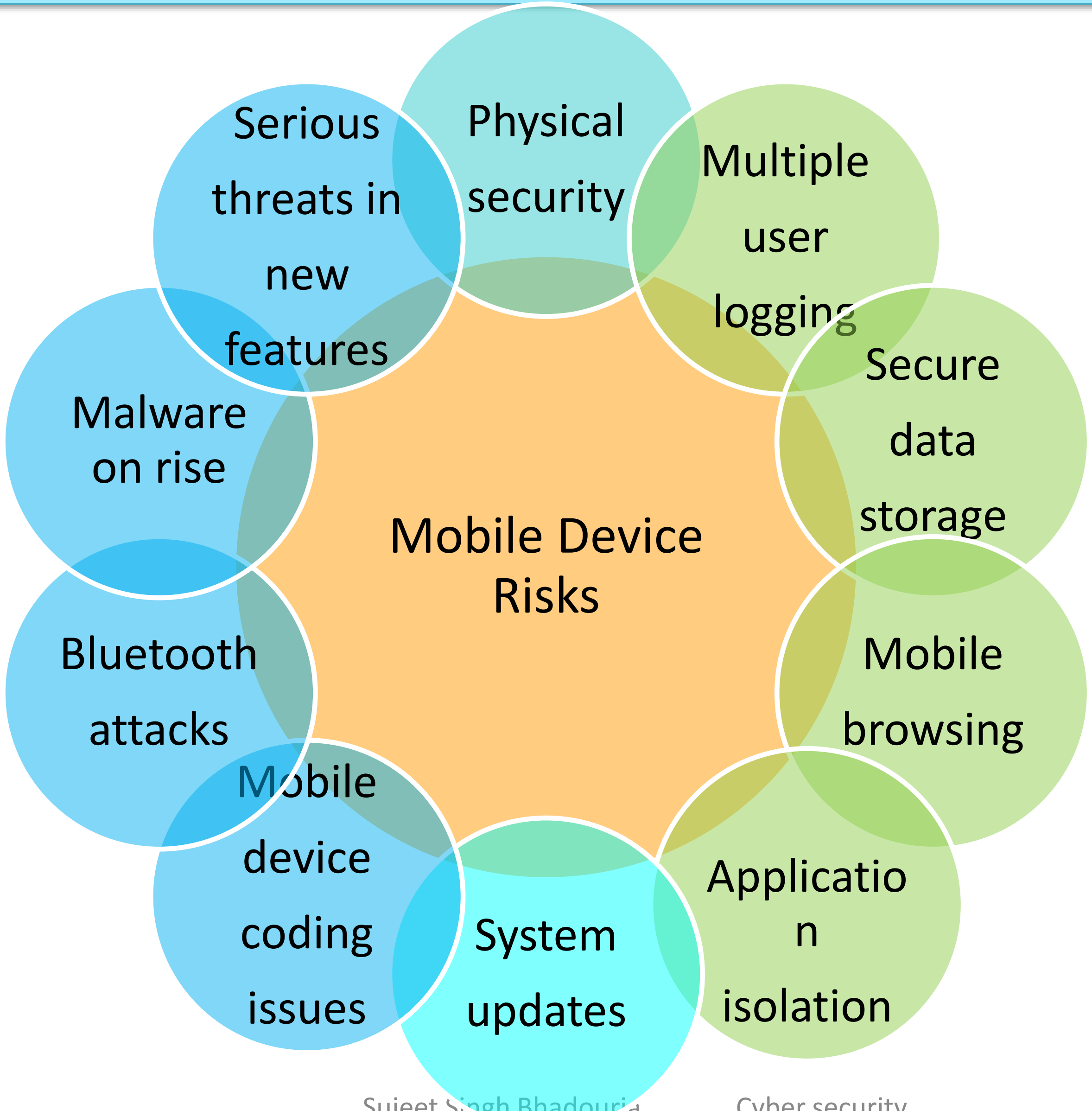
Phishing attacks

Spyware

Broken cryptography

Improper session handling

Common risks in Mobile Devices



Mobile Device Risks

Physical security

Multiple user logging

Secure data storage

Mobile browsing

Application isolation

System updates

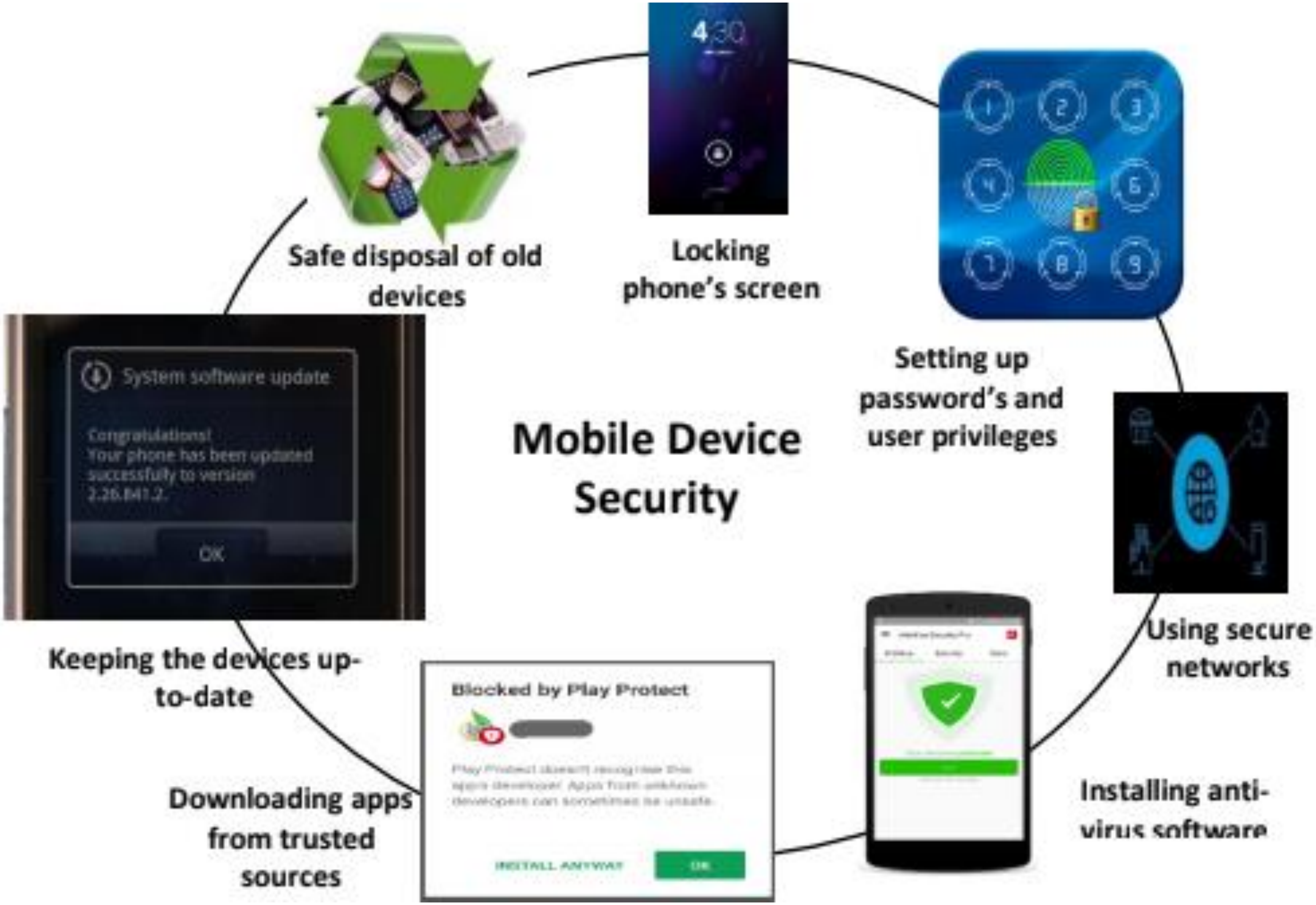
Mobile device coding issues

Bluetooth attacks

Malware on rise

Serious threats in new features

Steps to maintain Mobile Device Security


4:30
1
2
3
4
6
7
8
9
System software update
Congratulations!
Your phone has been updated successfully to version 2.26.841.2.
OK
Blocked by Play Protect
Play Protect doesn't recognise this app's developer. Apps from unknown developers can sometimes be unsafe.
INSTALL ANYWAY
OK

Mobile Device Security

Locking phone's screen

Setting up password's and user privileges

Using secure networks

Installing anti-virus software

Downloading apps from trusted sources

Keeping the devices up-to-date

Safe disposal of old devices

Source: swayam

Recap

- Security Architecture Components
- Security Architecture and Design
- Concepts for Secure System Design
- Secure Issues with Downloadable devices

Daily Quiz

1. What are security issues with storage devices?

2. What are security issues with peripheral devices?

Weekly Assignment

1. What do you mean by Application Security? Name the two protocol use for Email Security and Explain?
2. Elaborate the term access control? What is include in authorization process for (File, Program, Data rights) and explain the all types of control?
3. Define Vendor challenges and user challenges for application security?
4. Write a short note on data disposal.
5. What do you mean by physical security of IT assets?
6. Explain Information security governance.
7. Write design Security Issues in Hardware, Data Storage & Downloadable Devices?
8. What are the different Measures of Backup Security
9. What are the different types of Biometric?
10. Explain the Principles for Secure System Design

Topic Link

- https://youtu.be/Ye2H1n2MtIc
- https://youtu.be/xwgecIX3E4I

Objective of Topics

Topic	Objective	CO Mapping
Physical Security of IT Assets	Study of concept of Physical Security of IT Assets	CO3

Physical Security of IT Assets(CO3)

- When it comes to providing security to your IT assets, you should keep it as simple, coherent, and standardized as possible. The primary threats for the physical security are as follows:
  - Physical access exposure to human beings:
    - Organizations’ own employees => theft, fraud, accidents, and sabotage.
    - Data Tampering by unauthorized users
  - Physical access exposure to natural disasters:
    - Natural disasters may destroy your computer systems or all data storage systems.
    - They might even interrupt your network. (fire, lightening, or electric interruption)

Mechanisms to Solve Physical Security

Physical access controls :

- The physical access control measures can be applied in various forms, such as locks, biometric authentication systems, photo IDs, Entry logs, magnetic locks using electronic key card, and computer terminal locks.

Electronic and visual surveillance systems: Through closed circuit television(CCTV), RFID sensors

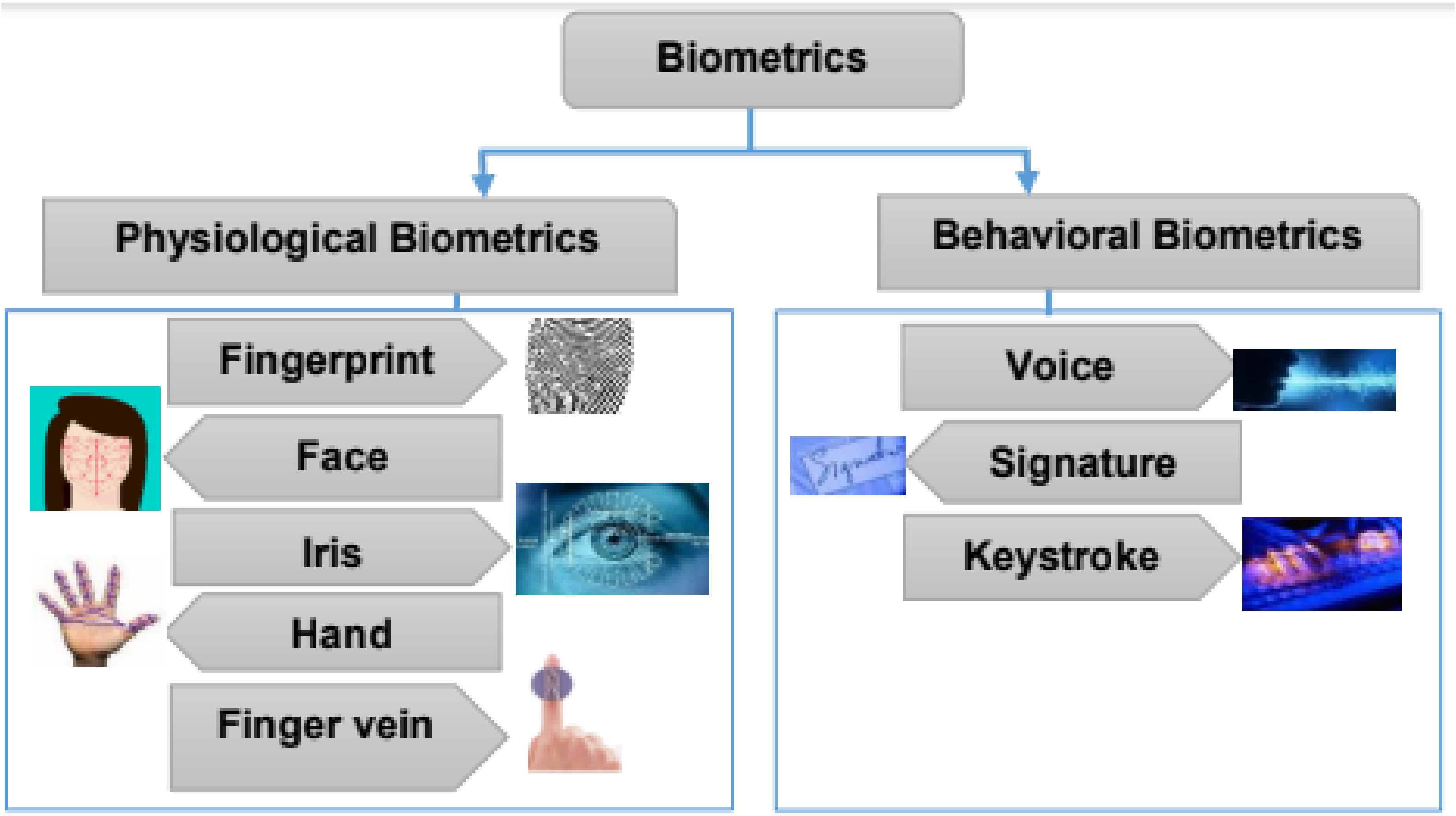
- CCTV cameras are also called the third eye because if human being missed noticing some people entering a restricted zone, these cameras could capture the event or photos.

Intrusion Detection Systems (IDS): IDS is a way of dealing with unauthorized access to information system assets.

Biometrics and its types

- Biometrics involves something a person is, or a person does
- It recognizes people based on two types
- Physiological characteristics - fingerprints, face, retina, iris
- Behavioural characteristics - gait, signature
- Another class of biometrics is esoteric biometrics - vein pattern, lip print, brain wave pattern

Biometrics and its types

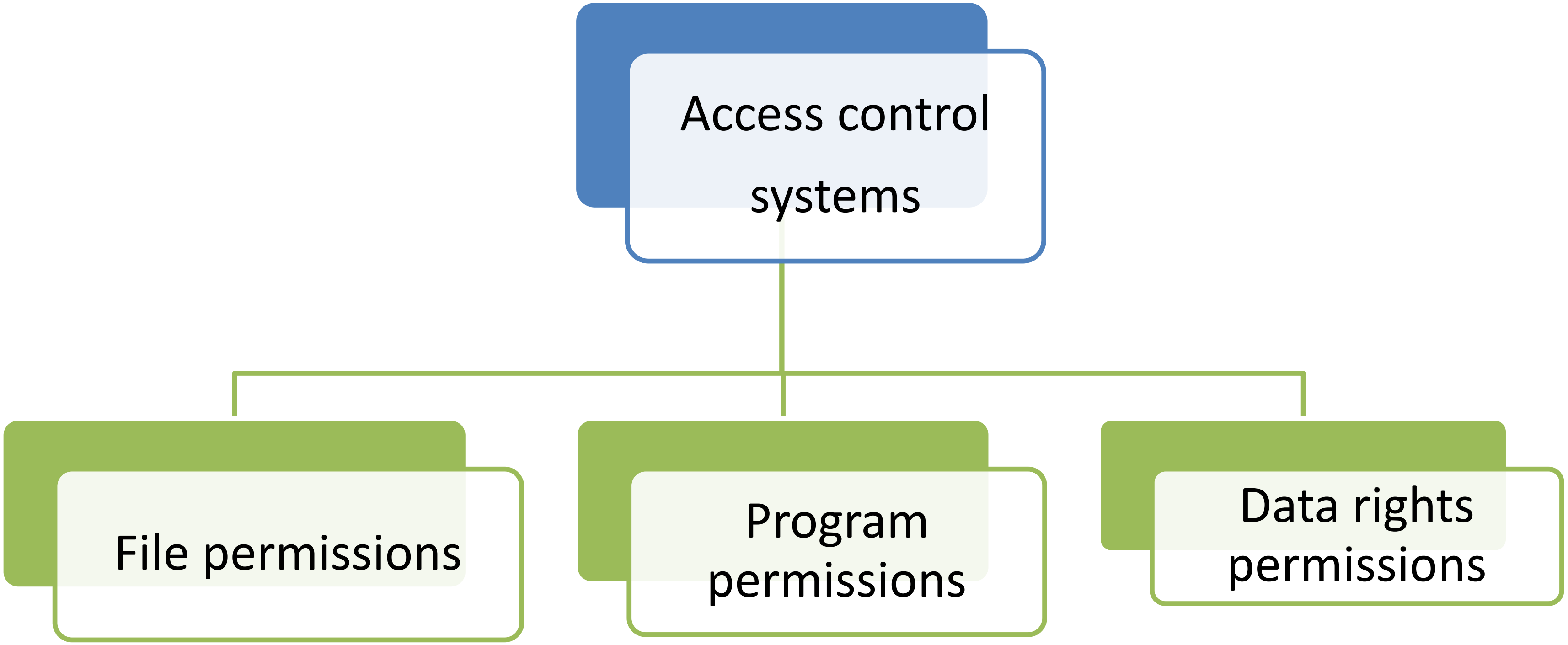


Source: swayam

Access Control(CO3)

- Access control is a mechanism that defines and controls access rights for individuals who can use specific resources in the OS.
- The access control is a security feature through which the system permits or revokes the right to access any data and resource in a system.
- The permission to access a resource is called authorization.

Access Control

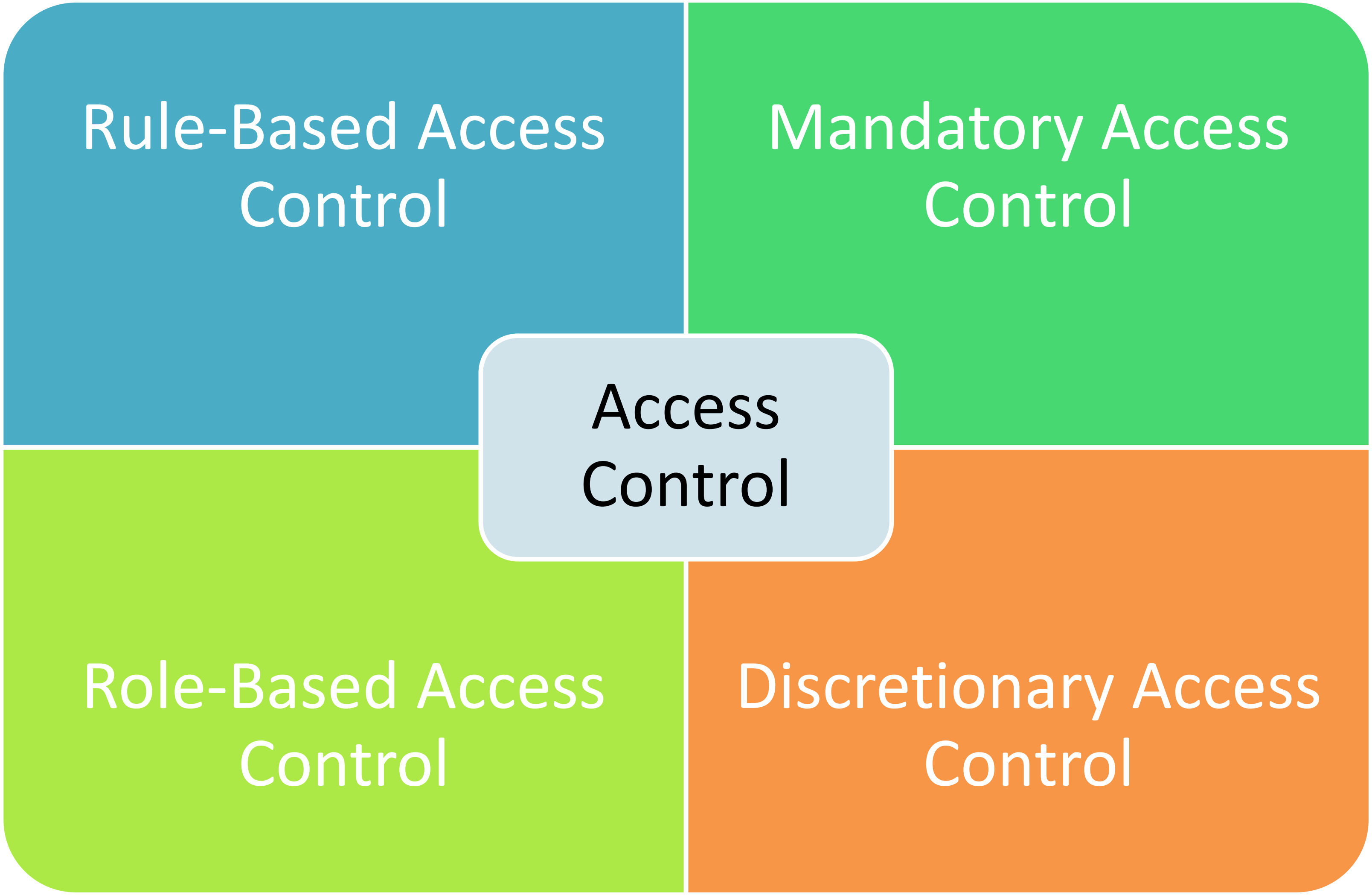


User can create, read, edit, or delete file on the server

User can execute a program on an application server

User can retrieve or update information in a database

Access Control



Rule-Based Access Control

Mandatory Access Control

Access Control

Role-Based Access Control

Discretionary Access Control

CCTV (CO3)

- **CCTV, or closed-circuit television,** is a system that allows you to keep an eye on what's going on in and around your business/area.
- It helps in crime prevention and as a security measure.
- Cameras collect images and transfer them to a monitoring-recording device where they are available to be watched, reviewed and/or stored. It links a camera to a video monitor using a direct transmission system. This differs from broadcast television where the signal is transmitted over the air and viewed with a television.
- If a business owner, security guard or employee is suspicious of a potential crime, the surveillance tapes can be used to observe and check for any suspicious activity.

Intrusion Detection Systems(IDS)

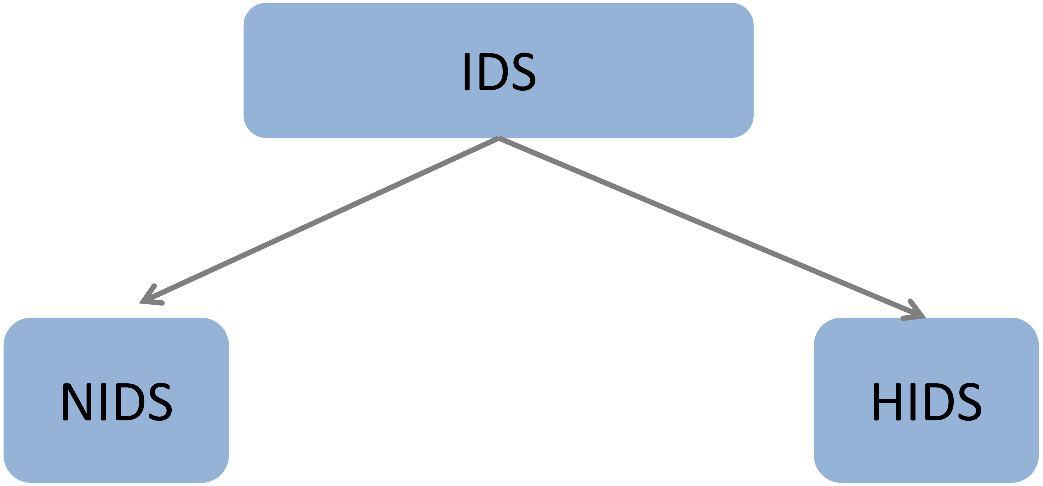
- IDS monitors network traffic for suspicious activity
- Issues alerts in case of illicit activity
- Anomaly detection and reporting are two main functions
- Administers two jobs namely, forensic analysis and alert generation
- Prone to false alarms or false positives

Components of Intrusion Detection System

- An IDS comprises Management console and sensors
- It has a database of attack signatures
- Sensors detect any malicious activity
- It also matches the malicious packet against the database
- If found a match, the sensor reports the
- malicious activity to the management console

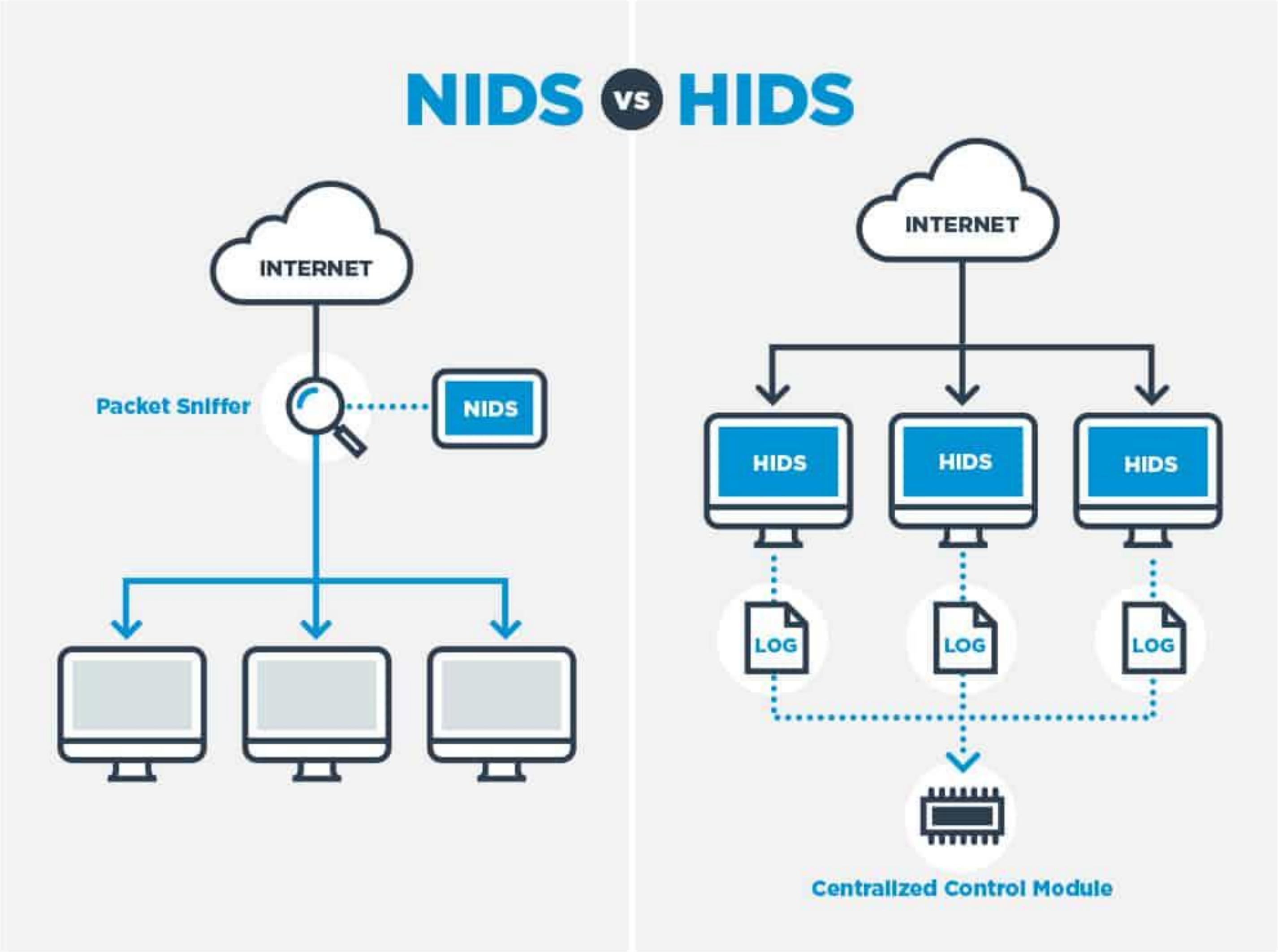
Types of Intrusion Detection Systems

- IDS is classified based on its level of operations



Source: cyber security, G Padmavathi, swayam

Types of Intrusion Detection Systems



Sourc

Types of Intrusion Detection System

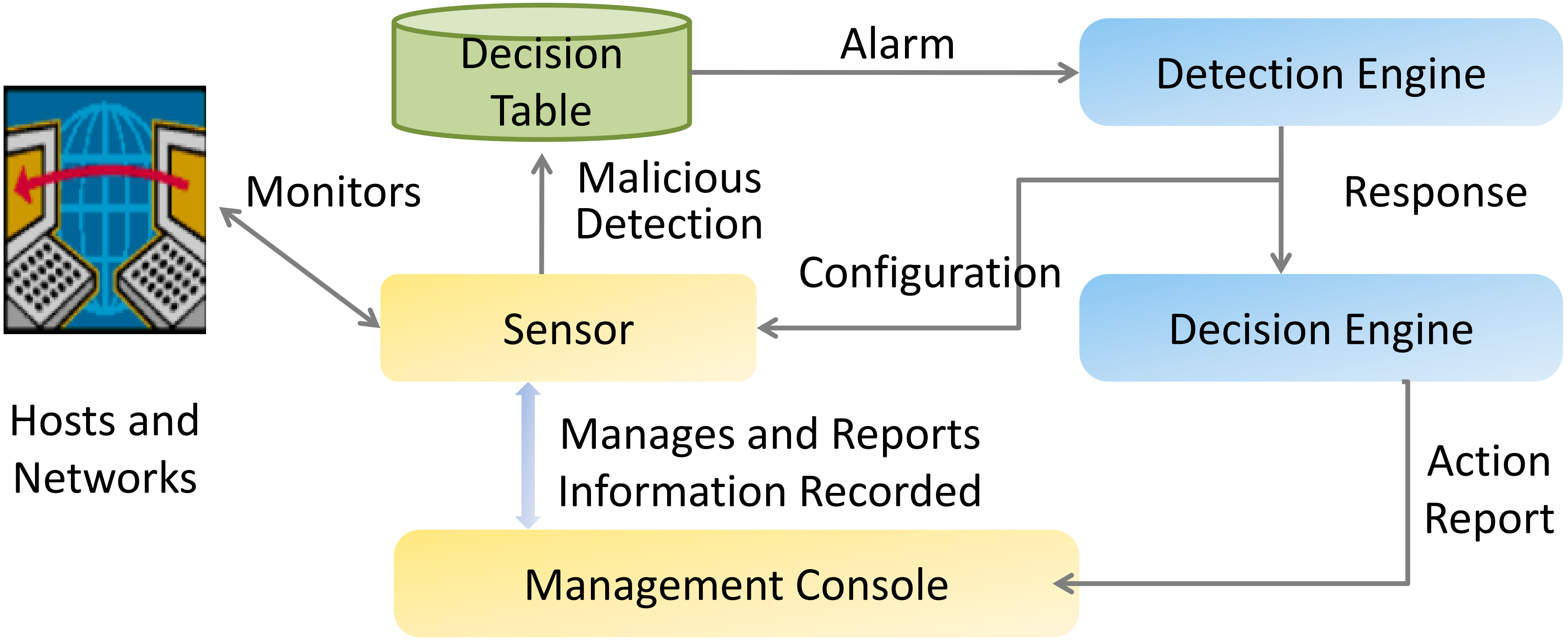
(NIDS) : A network intrusion detection system is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.

(HIDS) : A host intrusion detection system runs on all computers or devices in the network with direct access to both the internet and the enterprise's internal network.

A HIDS has an advantage over an NIDS in that it may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that an NIDS has failed to detect.

A HIDS may also be able to identify malicious traffic that originates from the host itself, such as when the host has been infected with malware and is attempting to spread to other systems.

Components of Intrusion Detection System



Source: cyber security, G Padmavathi, swayam

Objective of Topics

Topic	Objective	CO Mapping
Backup Security Measures	Study of concept of Backup Security Measures	CO3

Backup Security Measures (CO3)

- Data backups are taken to secure important data files and systems from being lost due to natural disasters or human errors and recover in case any kind of disaster has led to the loss of information. Therefore, it is very important to secure data backups.

- 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.

Backup Security Measures

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.

Backup Security Measures

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.

Daily Quiz

1. What is Biometric security?

2. Differentiate authentication and authorization.

3. What are Security Issues with Hardware?

4. What is memory protection?

5. What are the Open and Closed Systems?

Weekly Assignment

1. What do you mean by Application Security? Name the two protocol use for Email Security and Explain?
2. Elaborate the term access control? What is include in authorization process for (File, Program, Data rights) and explain the all types of control?
3. Define Vendor challenges and user challenges for application security?
4. Write a short note on data disposal.
5. What do you mean by physical security of IT assets?
6. Explain Information security governance.
7. Write design Security Issues in Hardware, Data Storage & Downloadable Devices?
8. What are the different Measures of Backup Security
9. What are the different types of Biometric?
10. Explain the Principles for Secure System Design.

Topic Links

- https://youtu.be/snJGzyXzVec
- https://youtu.be/8caqok3ah8o
- https://youtu.be/WPU2eisvqXE
- https://youtu.be/cUvMIOdaSBs
- https://youtu.be/0a264Edp5l0
- https://youtu.be/Ye2H1n2MtIc
- https://youtu.be/xwgecIX3E4I

MCQ s

- Secure information systems are developed by:

  a)Integrating security with the system after it has been developed

  b) Never integrating security with the information system

  c) Keeping security as a separate action until the last step of the system development

  d) Integrating risk analysis and management activities at the start of the system development lifecycle and continuing throughout the cycle

- Which of the following is a control gate in the development phase?

  a) Authorizing the decision

  b) Reviewing the architecture and design

  c) Reviewing the confidentiality and availability

  d) Reviewing the operational readiness

MCQ s

- The risk management process involves:

  a) Framing, deciding, executing, and deleting

  b) Framing, assessing, monitoring, and responding

  c) Monitoring, assessing, executing, and deleting

  d)All of the above

- Which of the following is used to provide physical security of IT assets?

  a) Physical access control technique

  b) CCTV surveillance technique

  c) IDS technique

  d) None

- Which of the following is a part of the secure system design?

  a) Layering **b)Abstraction**

  c) Security domains d) None

MCQ s

- Which of the following is an issue faced by data storage devices?

  a) Excessive data mounting

  b) Theft, destruction, and damage

  c) Too small size

  d) All of the above

- Express the correct relationship between vulnerabilities, threats and risks.

  a) Risk=threat *x* vulnerability b) Threat=risk *x* vulnerability

  c) Vulnerability=risk +threat d) Risk=threat – vulnerability

- Characterize the type of hackers who use their knowledge for good purposes.

  a) Black hat b)**White hat**

  c) Gray hat d)Blue hat

Glossary Questions

Fill the right options:

Intrusion Detection System, NIDS and HIDS, Software Development Life Cycle, Responding to the risks, CCTV

1. IDS stands for _____________

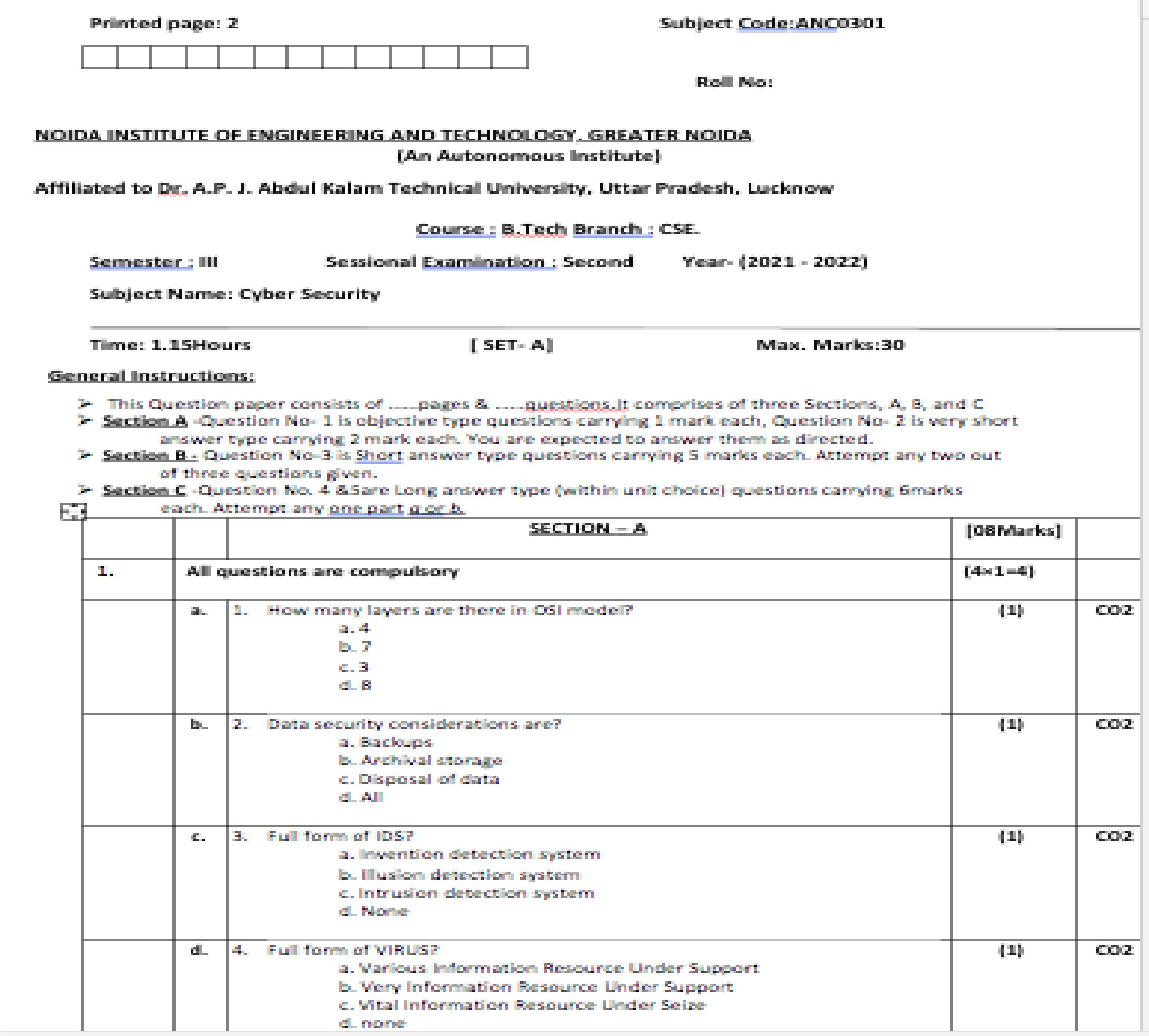
2. IDS can be broadly classified as ______ and ______.

3. SDLC stands for _________.

4. To take preventive or corrective measures so that systems can be kept protected from any kind of threats, whether internal or external is ________

5. __________ is used for physical security of an organization.

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

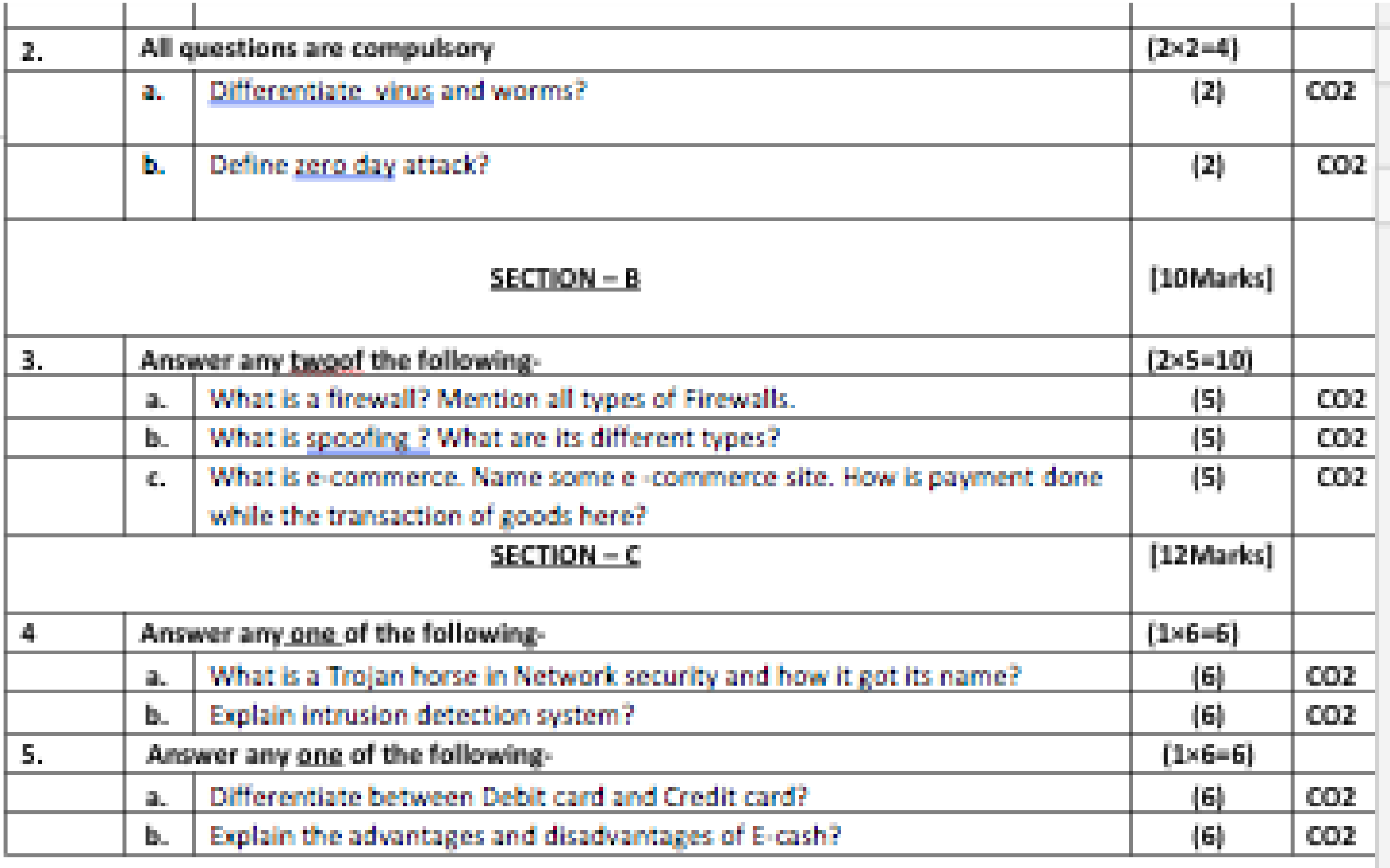
Time: 1.15Hours [SET- A] Max. Marks:30

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.

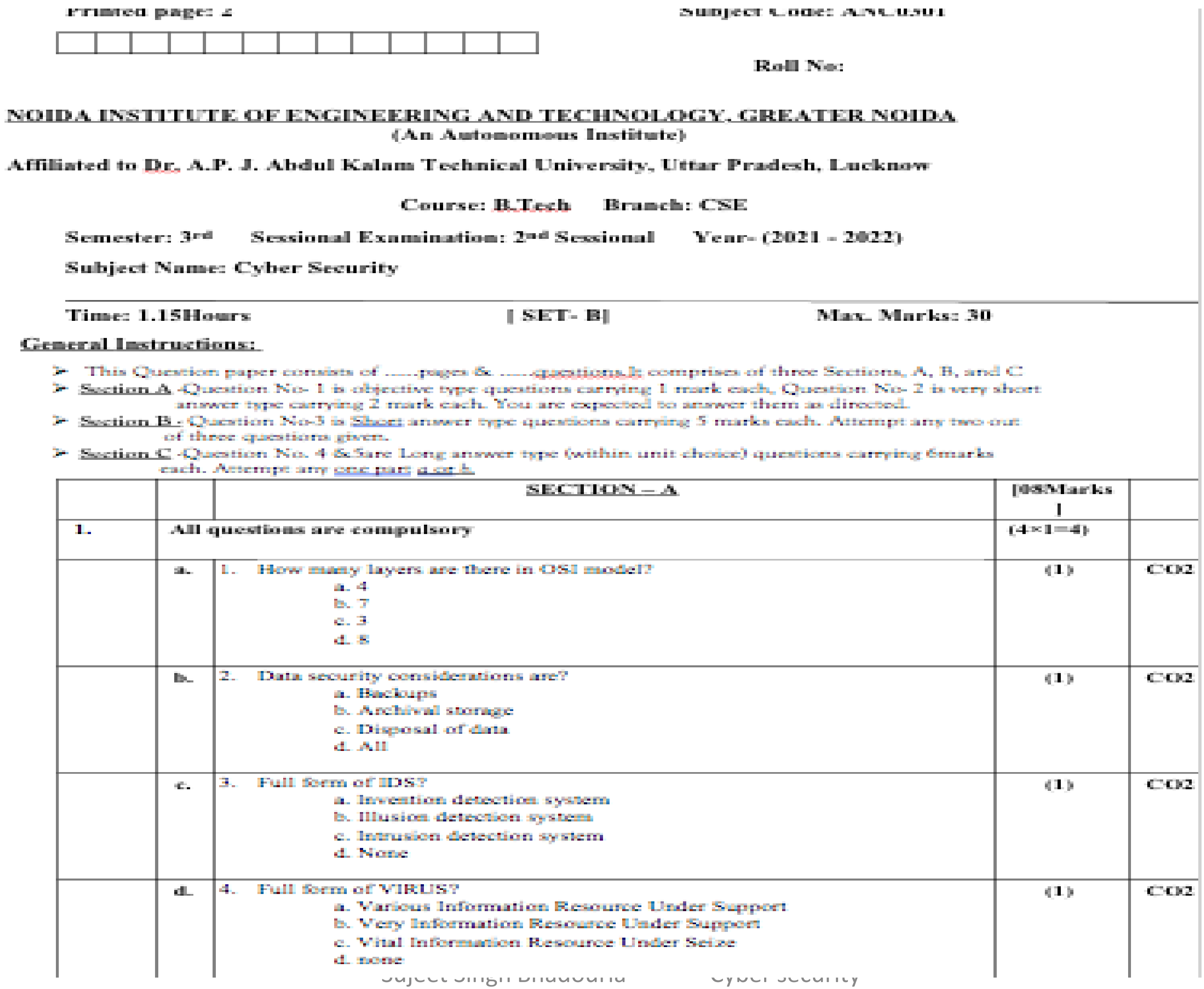
		SECTION – A	[08Marks]	
1.	All questions are compulsory		(4×1=4)	
	a.	1. How many layers are there in OSI model? a. 4 b. 7 c. 3 d. 8	(1)	CO2
	b.	2. Data security considerations are? a. Backups b. Archival storage c. Disposal of data d. All	(1)	CO2
	c.	3. Full form of IDS? a. Invention detection system 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 twoof 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

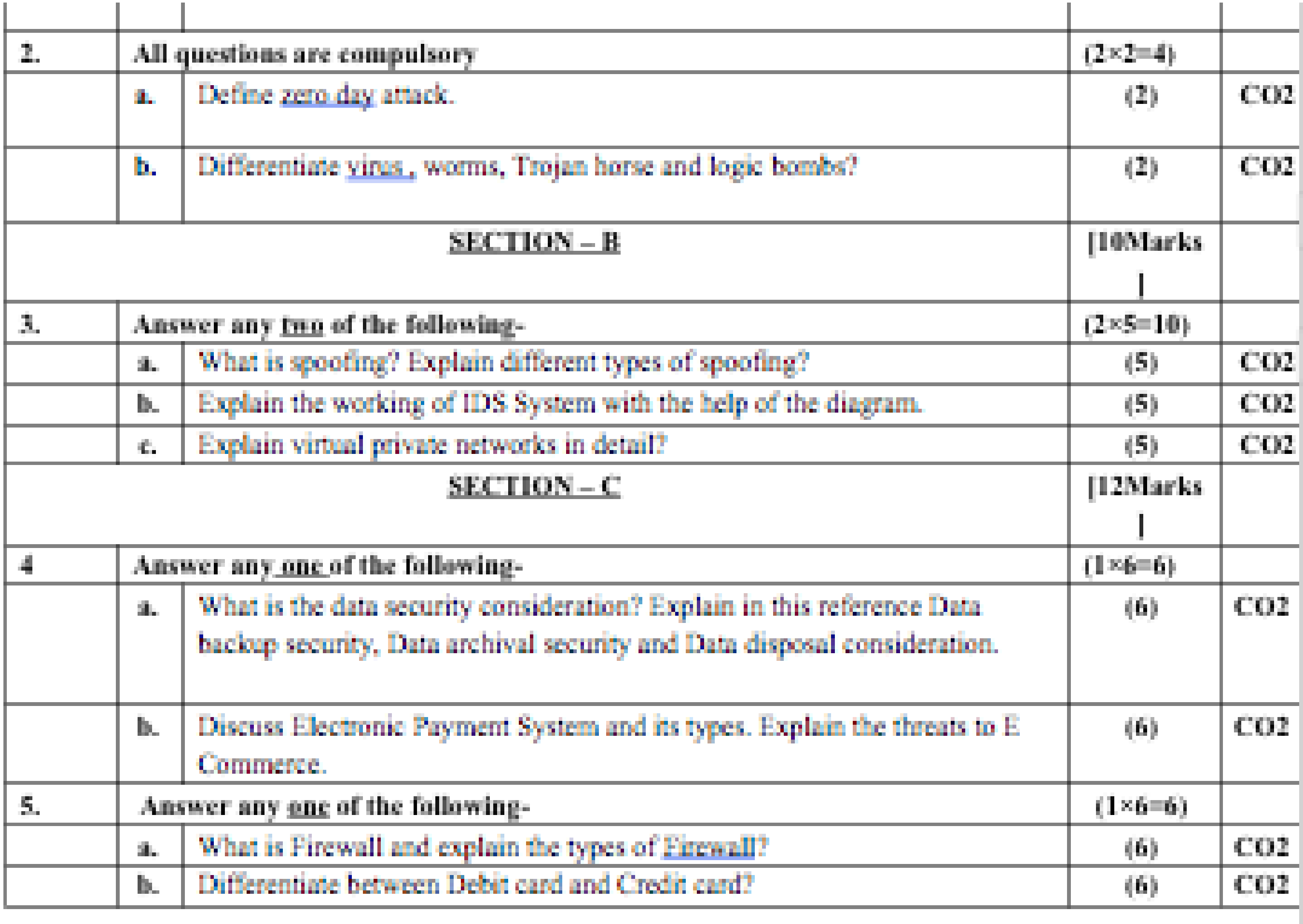
Time: 1.15Hours | SET- B| Max. Marks: 30

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.

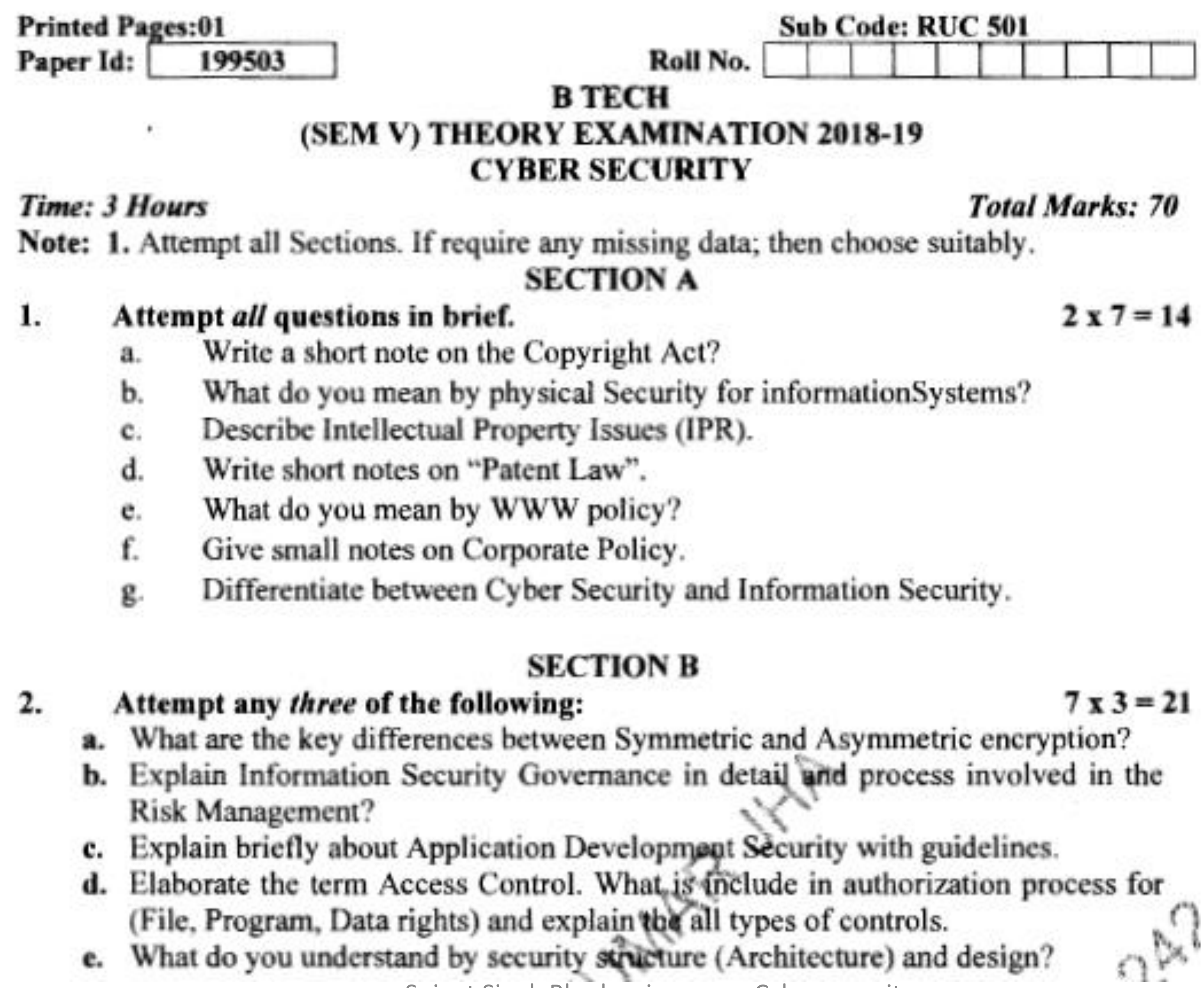
		SECTION – A	[08Marks]	
1.	All questions are compulsory		(4×1=4)	
	a.	1. How many layers are there in OSI model? a. 4 b. 7 c. 3 d. 8	(1)	CO2
	b.	2. Data security considerations are? a. Backups b. Archival storage c. Disposal of data d. All	(1)	CO2
	c.	3. Full form of IDS? a. Invention detection system 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?

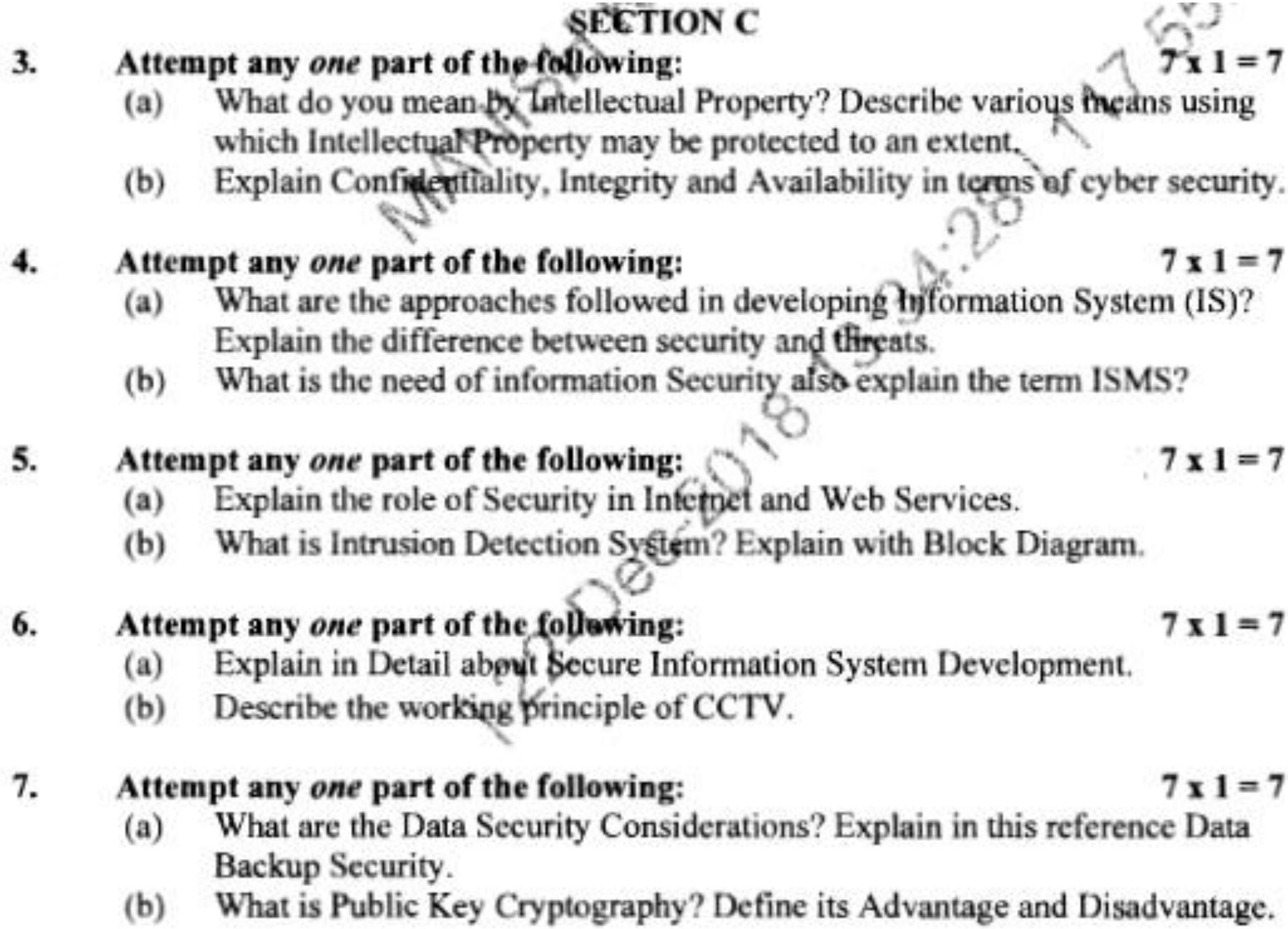
b. Explain Information Security Governance in detail and process involved in the Risk Management?

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.

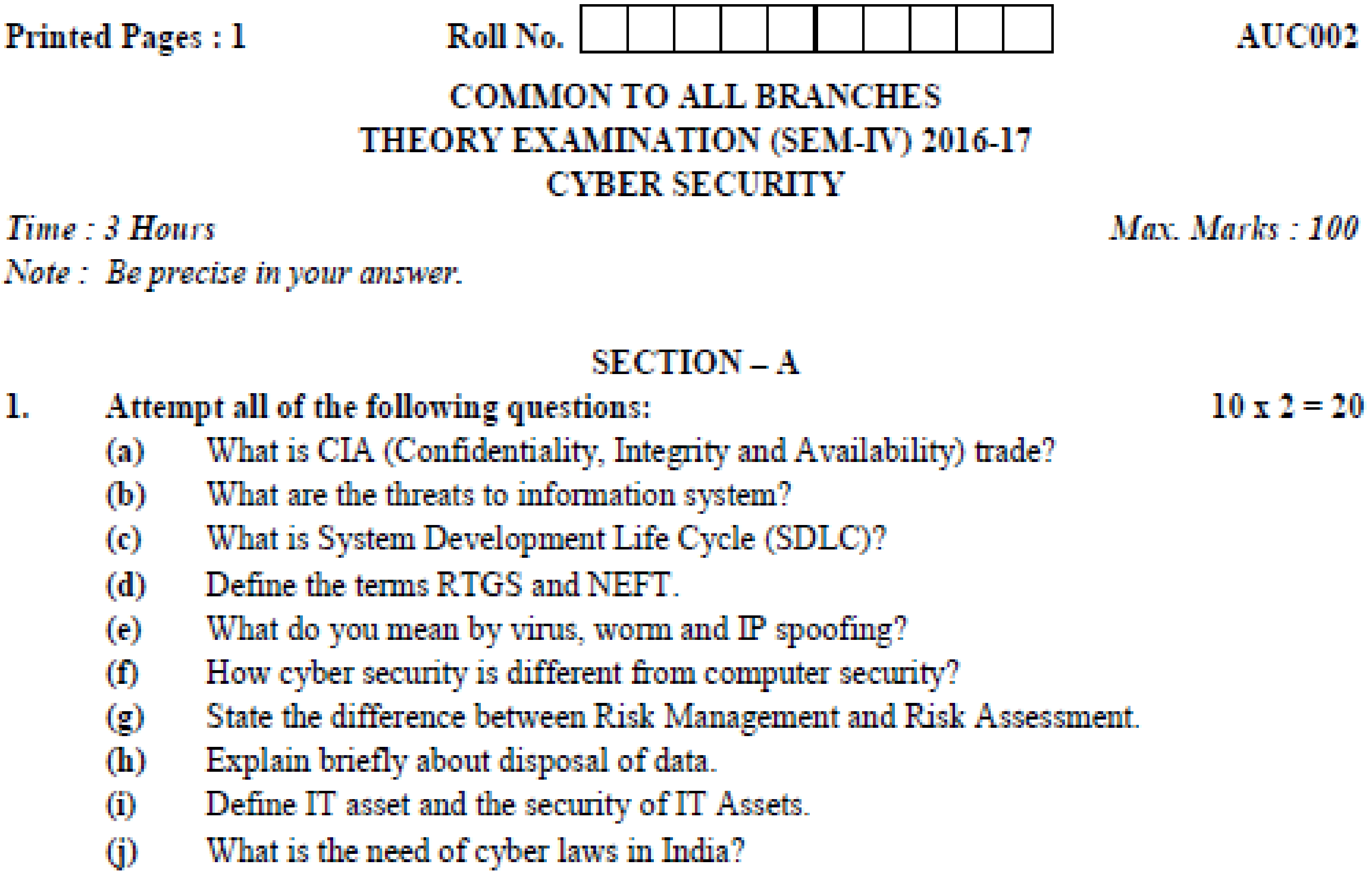
   (b) Describe the working principle of CCTV.

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*

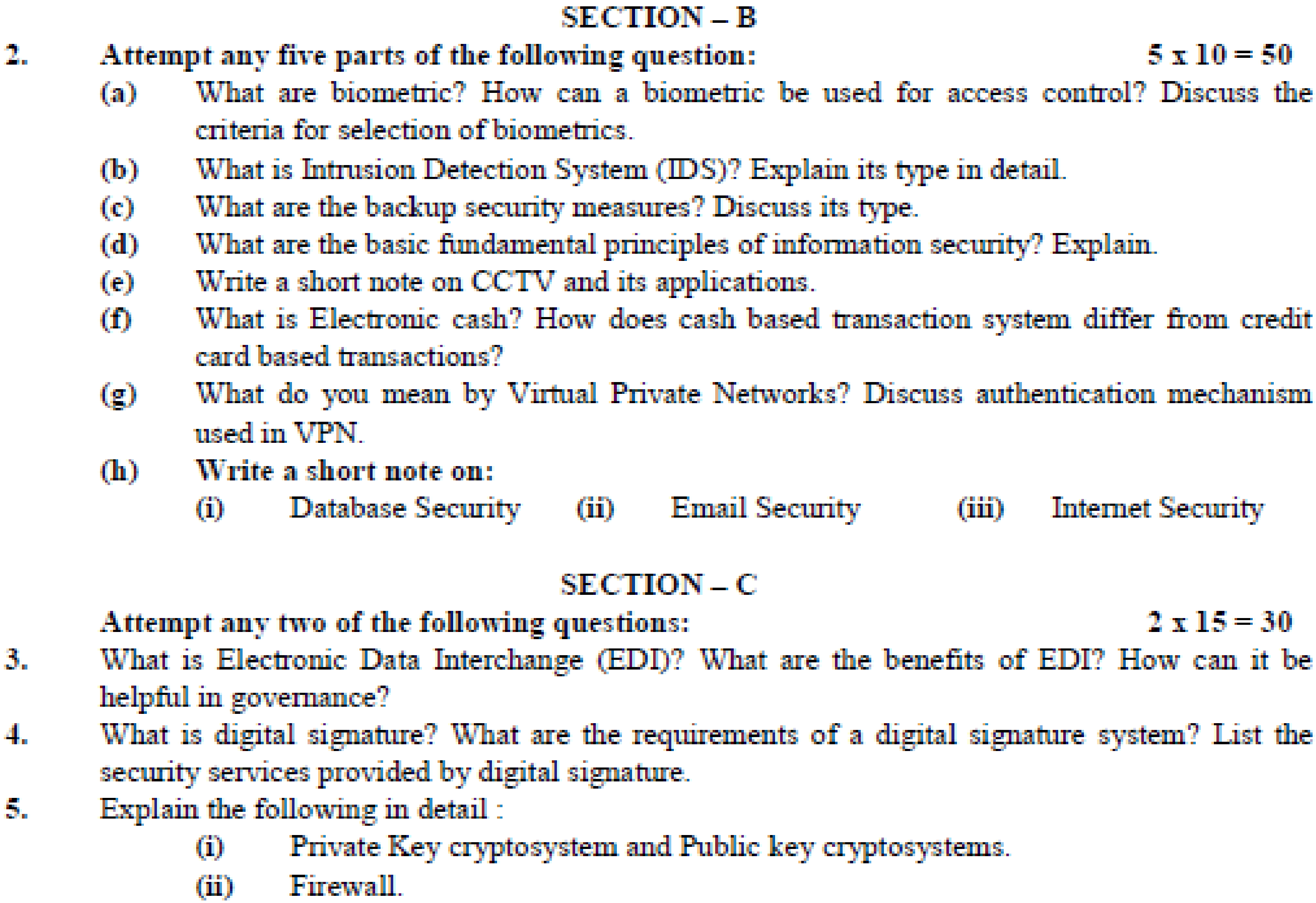
Note : Be precise in your answer.

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. Do vulnerabilities play a vital role in cyber security? Justify
2. Elaborate the term access control? What is include in authorization process for (File, Program, Data rights)?
3. Describe in brief the application development security.
4. Describe Risk Management Process.
5. Discuss backup security measures Types
6. What do you mean by Security Architecture & Design

Recap of Unit

The major topics covered are Application Development Security, Information Security Governance & Risk Management, Security Architecture & Design Security Issues in Hardware, Data Storage & Downloadable Devices, Physical Security of IT Assets, Backup Security Measures.

Biometric technology has proved itself as a powerful alternative to traditional password-based and token-based authentication technology.

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)
4. https://link.springer.com/content/pdf/10.1007/978-0-387-73269-5_6.pdf
5. http://www.m2sys.com/blog/biometric-resources/what-are-the-biometrics-
6. https://onlinecourses.swayam2.ac.in/cec20_cs09/unit?unit=59&lesson=66

Thank You