Application Layer Security

Unit: 2

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

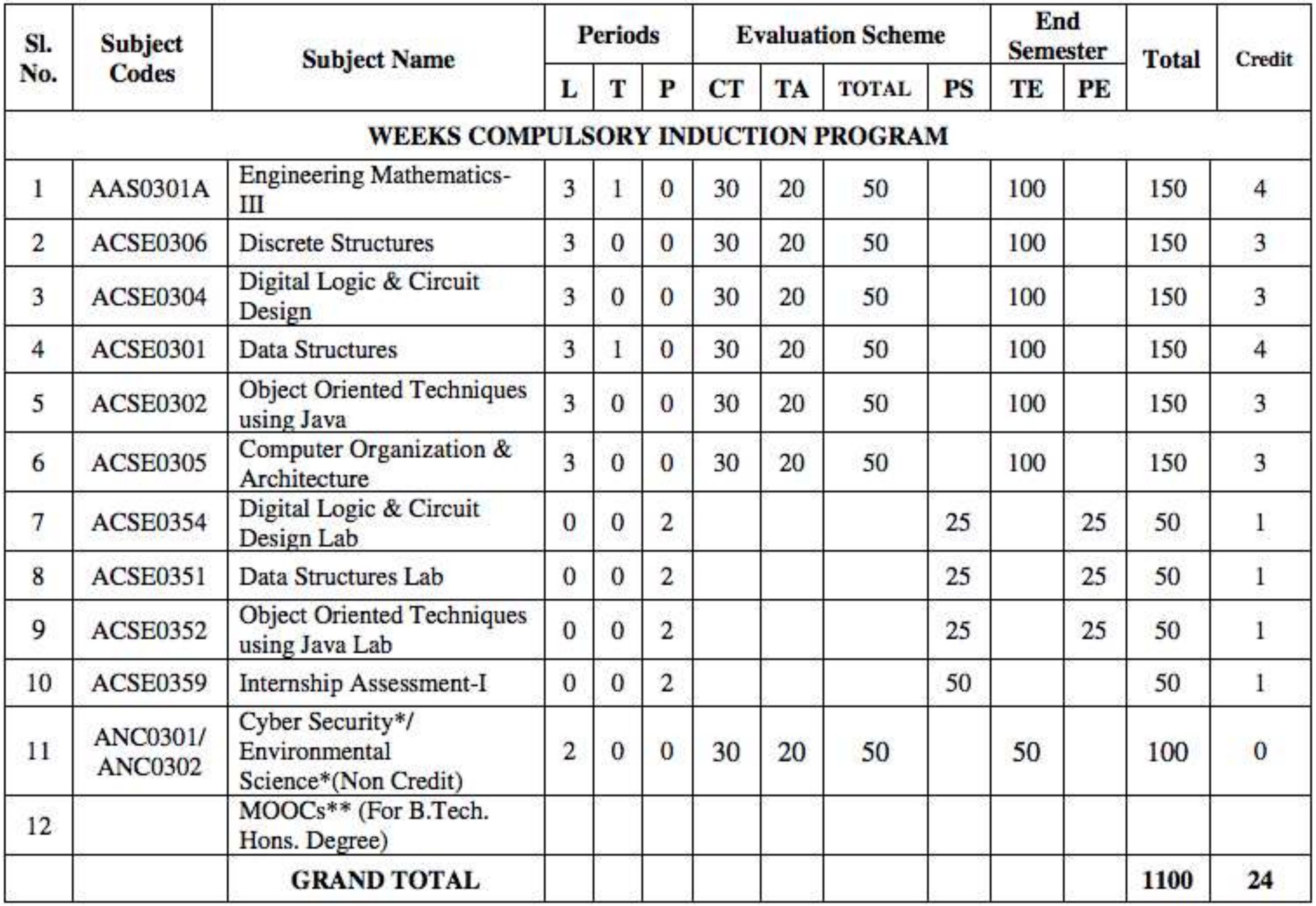
Qualification: Ph.D (Pre-Submission) M.Tech

Experience: 10 Years of teaching experience

Area of Interest: Computer Network

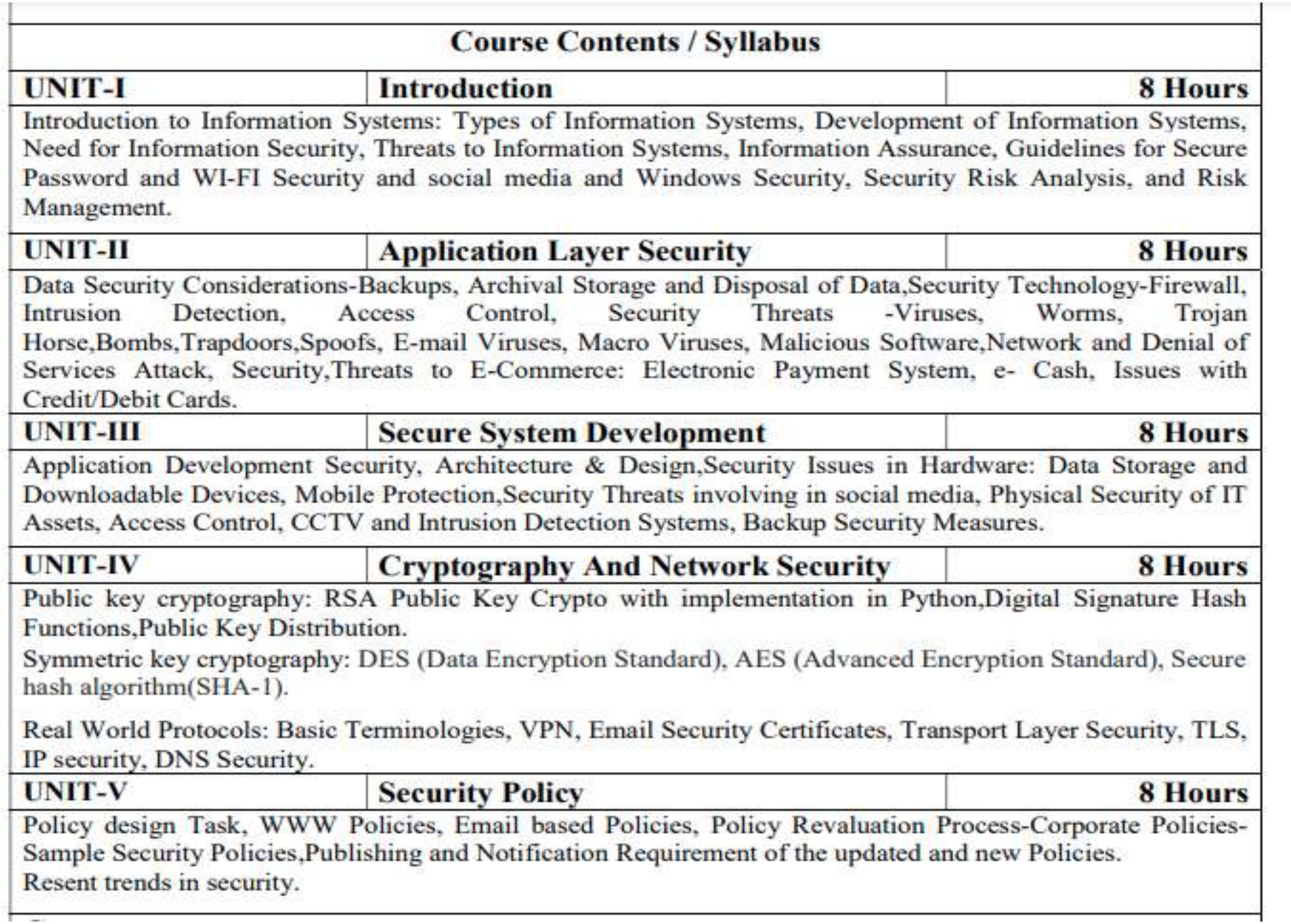
Reviewer: IET Communications ISSN 1751-8644 (SCI & SCOPUS INDEX)
Research Publications:
International Journal 09
Paper Presentation 06
International Patent 01 (Granted)
National Patent 04

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



Course Contents / Syllabus		
UNIT-I	**Introduction**	**8 Hours**
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.		
UNIT-II	**Application Layer Security**	**8 Hours**
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.		
UNIT-III	**Secure System Development**	**8 Hours**
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.		
UNIT-IV	**Cryptography And Network Security**	**8 Hours**
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.		
UNIT-V	**Security Policy**	**8 Hours**
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. Resent 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 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.

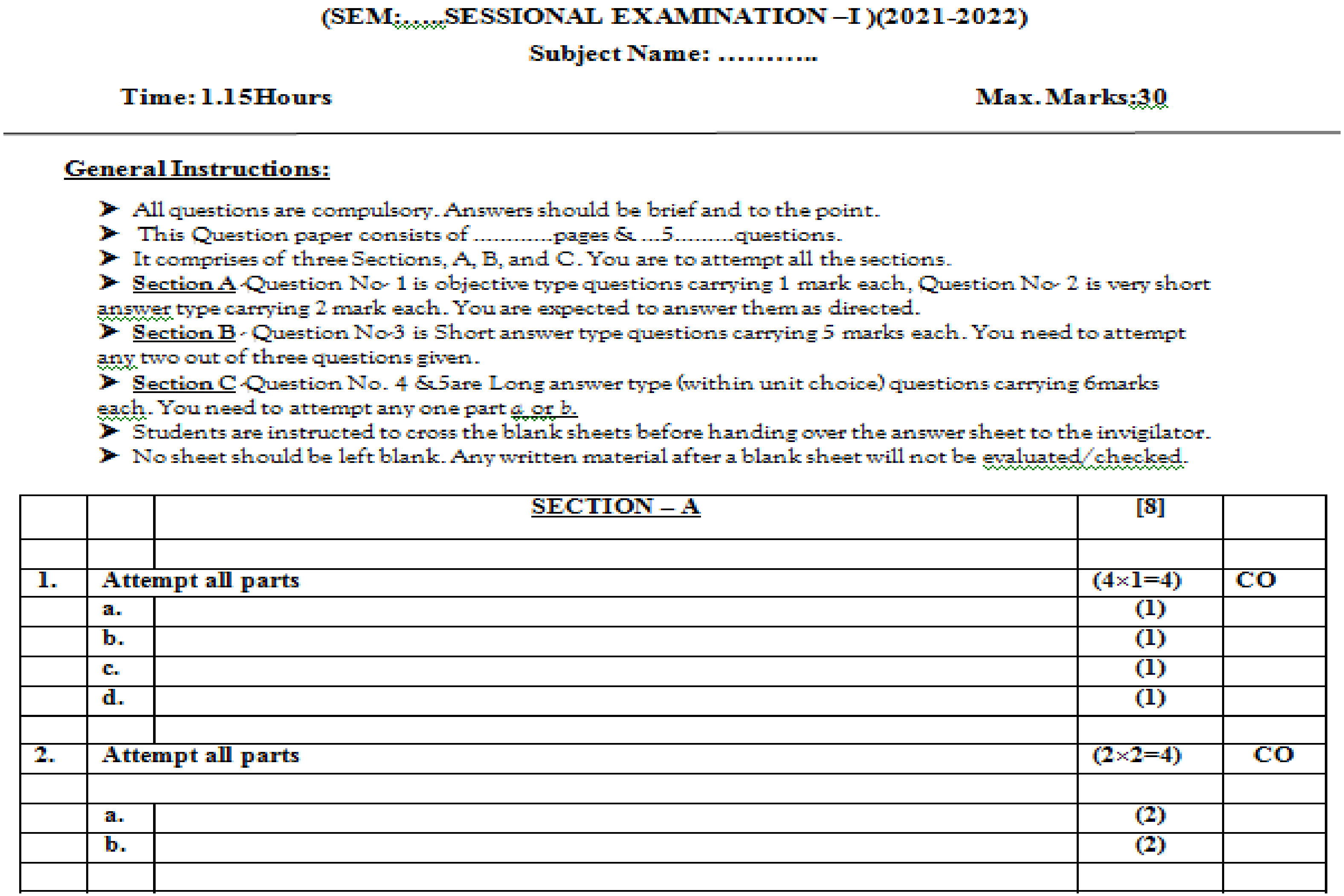
PEO2: To lead a successful career in industries or to pursue higher studies or to understand entrepreneurial endeavors.

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: ………..

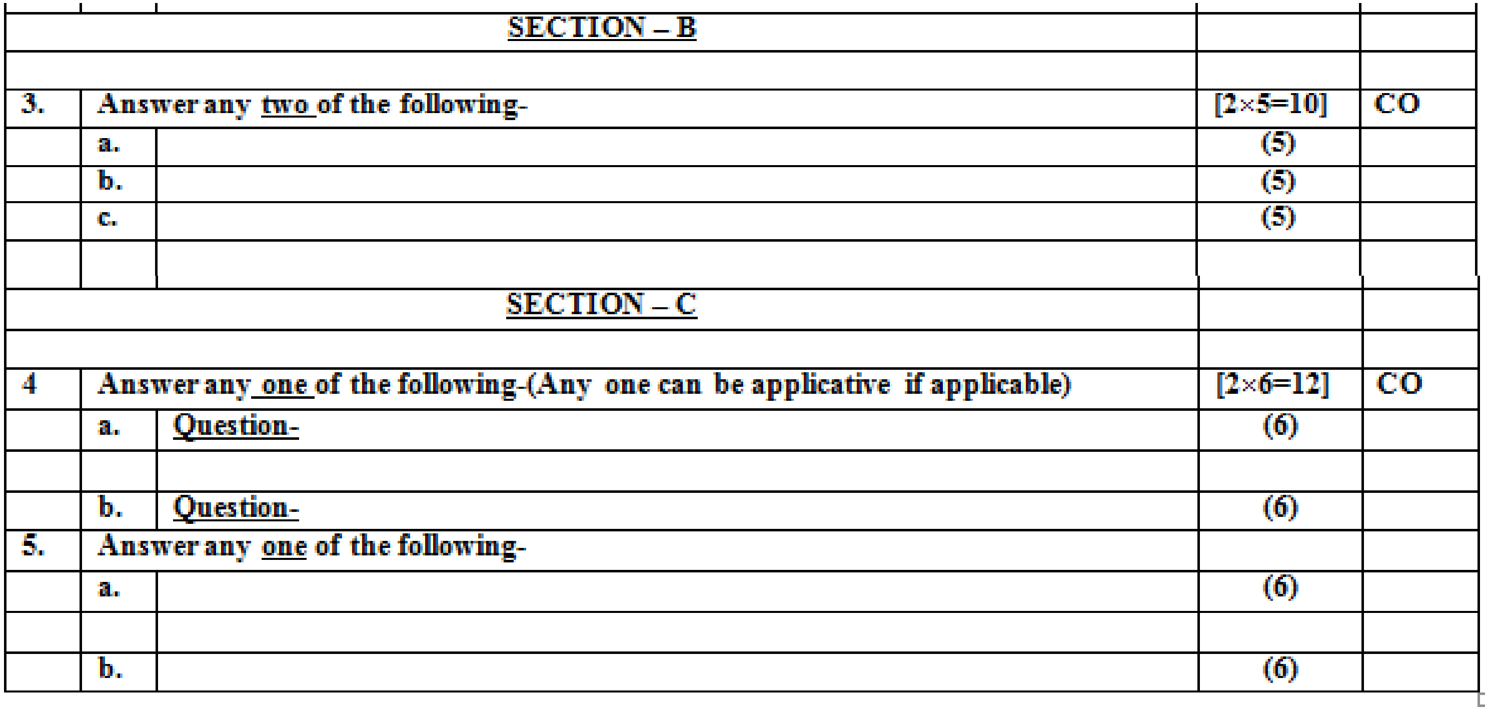
Time: 1.15Hours **Max. Marks:30**

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

- Application Security
- Data Security Considerations- Backups, Archival Storage and Disposal of Data
- Security Technology(Firewall and VPNs, Intrusion Detection Access Control)
- Security Threats
- Security Threats to E-Commerce(Electronic Payment System, e- Cash, Credit/Debit Cards)

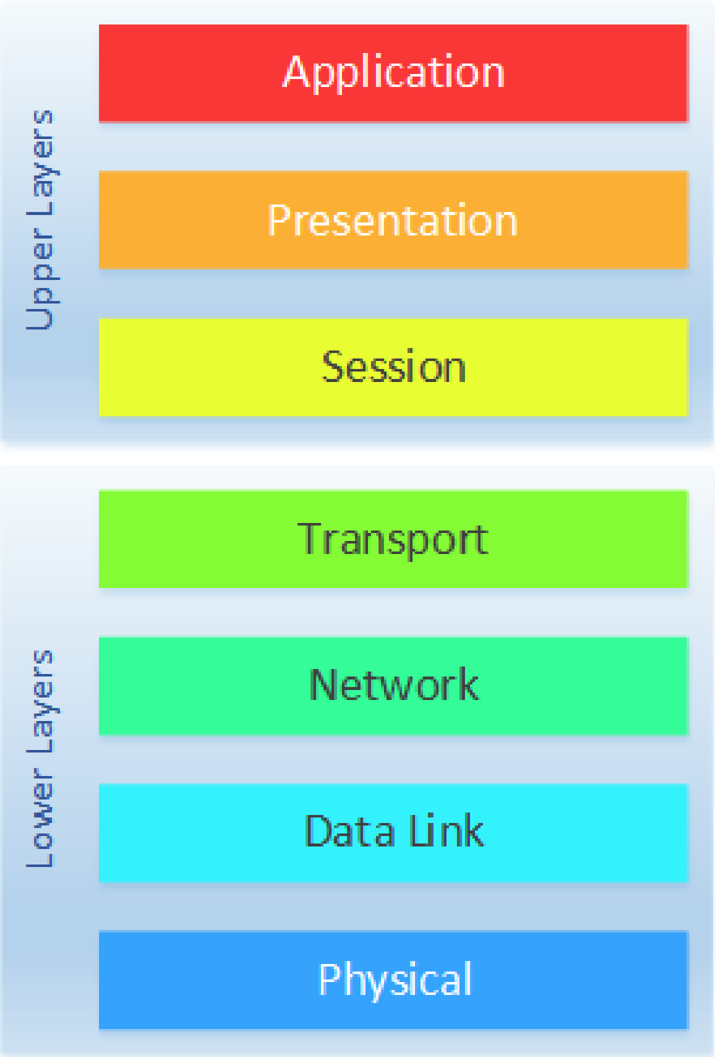
Unit Objective

Topic	Objective
Data Security Considerations	Develop an understanding of Data Security Considerations-Backups, Archival Storage and Disposal of Data
Security Technology	Examine Security Technology- Firewall and VPNs, Intrusion Detection, Access Control mechanism.
Security Threats	Study the various security threats characteristics Viruses, Worms, Trojan Horse, Bombs, Trapdoors, Spoofs, E-mail Viruses, Macro Viruses, Malicious Software
Security Threats to E-Commerce	Develop an understanding of threats to Electronic Payment System, e- Cash, Credit/Debit Cards.
Public Key Cryptography	Study of basic concept of asymmetric key Cryptography and digital signature

Topic Objective/Topic Outcome

Topic	Objective	CO Mapping
Data Security Considerations	Develop an understanding of Data Security Considerations- Backups, Archival Storage and Disposal of Data	CO2

Application Layer



Data Security Considerations(CO2)

- Data security consideration involves the protection of data against unauthorized access, modification, destruction, loss, disclosure or transfer whether accidental or intentional.
- Some of the important data security consideration are described below:
  - Backups
  - Archival storage
  - Disposal of Data

Data Security Considerations(CO2)

- Data backup refers to create additional copies of our data in separate physical or cloud locations from data files in storage.
- It is essential for us to keep secure, store, and backup our data on a regular basis. So that if there is loss or changes in data we can recover it using the backup copies.

Data Security Considerations(CO2)

To use the Golden 3-2-1 rule of Backup is very popular.

This rule includes:

Three copies of our data (1 primary and 2 backup copies)

Two different types of storage media.

Onsite (Local storage Hard drives DVDs and CDs) and Offsite (On remote server i.e Cloud)

One off-site backup, i.e., have two physical backups and one in the cloud.

Data Archival Security Considerations

- Data archiving is the process of retaining or keeping of data at a secure place for long-term storage. The data might be stored in safe locations so that it can be used whenever it is required.
- The archive data is still essential to the organization and may be needed for future reference.
- Also, data archives are indexed and have search capabilities so that the files and parts of files can be easily located and retrieved.
- The Data archival serve as a way of reducing primary storage consumption of data and its related costs.

Data Archival Security Considerations

The following list of considerations will help us to improve the long-term usefulness of our archives:

- Storage medium

The first thing is to what storage medium we use for archives. The archived data will be stored for long periods of time, so we must need to choose the type of media that will be lost as long as our retention policy dictates.

- Storage device

This consideration takes into account about the storage device we are using for our archives which will be accessible in a few years. There is no way to predict which types of storage devices will stand the best. So, it is essential to try to pick those devices that have the best chance of being supported over the long term.

Benefits of Data Archival

- Reduce cost
- Save storage space in the online system
- Reduce access complexity
- Improve system performance
- Efficient identification of preserved data
- Use archived data for historical researches

Data Disposal Security Considerations (CO2)

- Data destruction or disposal of data is the method of destroying data which is stored on tapes, hard disks and other electronic media so that it is completely unreadable, unusable and inaccessible for unauthorized purposes.
- It also ensures that the organization retains records of data for as long as they are needed.
- When it is no longer required, appropriately destroys them or disposes of that data.

Data Disposal Security Considerations (CO2)

The managed process of data disposal has some essential benefits-

•It avoids the unnecessary storage costs incurred by using office or server space in maintaining records which is no longer needed by the organization.

•Finding and retrieving information is easier and quicker because there is less to search.

The disposal of data usually takes place as part of the normal records management process. There are two essential circumstances in which the destruction of data need to be handled as an addition to this process-

•The quantity of a legacy record requires attention.

•The functions are being transferred to another authority and disposal of data records becomes part of the change process.

Data Disposal Security Considerations (CO2)

Eliminate access

In this consideration, we have to ensure that eliminating access account does not have any rights to re access the disposed of data again.

Destroy the Data

In this consideration, there is not necessary to remove data from storage media will be safe. Even these days reformatting or repartitioning a drive to "erase" the data that it stores is not good enough. Today's many tools available which can help us to delete files more securely. To encrypt the data on the drive before performing any deletion can help us to make data more difficult to recover later.

Destroy the device

In the most cases, storage media need to be physically destroyed to ensure that our sensitive data is not leaked to whoever gets the drives next. In such cases, we should not destroy them itself. To do this, there should be experts who can make probably a lot better at safely and effectively rendering any data on our drives unrecoverable. If we can't trust this to an outsider agency that specializes in the secure destruction of storage devices, we should have a specialized team within our organization who has the same equipment and skills as outside contractors.

Application Security (CO2)

Introduction to Application Security

- Security of information and information systems is, undoubtedly, the leading challenge for organizations.
- However, they cannot ignore the importance of third-party vendor applications such as Web browsers, and therefore, security measures must be applied to maintain the data and application security.
- In order to secure applications, we have various technologies such as firewall, Intrusion detection and Access control systems.
- Online purchase of products and services is considered to be one of the most vulnerable uses of the Internet as it involves exchange of finances and identity.

Introduction to Application Security

- Attackers, in the last decade, not only targeted the servers and Operating Systems (OSs) but also attacked the Client Applications.
- Organizations and individuals use various types of client-side applications that include Browsers, Multimedia Programs, and Document Readers.
- The most common attacks on the client-side applications include Phishing and Social Engineering.
- Attacker may send malware through e-mail.
- Attacker may ask to download a plug-in or a cookie to help you improve your search, but that may turn you into a victim of social engineering attack.

Introduction to Application Security …

- Any application interacting with the Web is always under threat.

- Most of the OS vendors use patched systems to keep vulnerabilities to the minimum, but even the patched systems are not devoid of attacks.

Zero-day attacks : 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.

Top vendors including *Microsoft*, *Apple computers*, *Adobe*, and *Mozilla* are the targets of these kinds of attacks.

Introduction to Application Security …

HTTP : Hyper Text Transfer Protocol

HTTPS : Hyper Text Transfer Protocol Secure

HTTPS is HTTP with encryption. The difference between the two protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses.

As a result, HTTPS is far more secure than HTTP. A website that uses HTTP has HTTP:// in its URL, while a website that uses HTTPS has HTTPS://

Daily Quiz

1. What is Zero day vulnerabilities?
2. Differentiate Data Backup and Data Archival.
3. What is application security?
4. What is data disposal?
5. Write Golden rule of data backup.

Topic Link

- https://youtu.be/2YGUvopGkQc
- https://youtu.be/Ofoshc9CblU

Topic Objective/Topic Outcome

Topic	Objective	CO Mapping
Security Technology	Firewall , Intrusion Detection, Access Control mechanism.	CO2

Security Technologies(CO2)

- **Firewall**

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.

- **Intrusion Detection**

Intrusion detection can be defined as the ability to monitor and react to computer misuse.

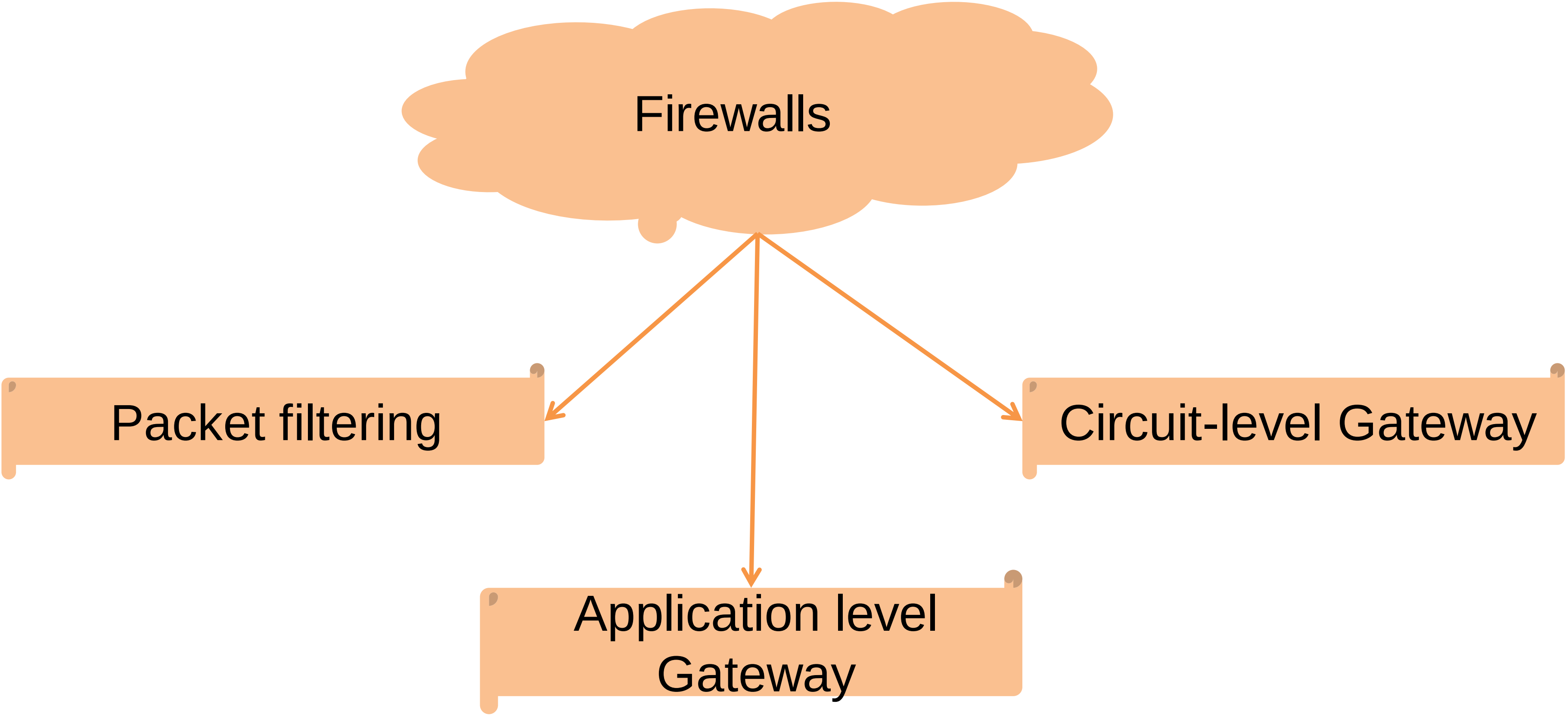
- **Access Control System**

Access control is a mechanism that defines and controls access rights for individuals who can use specific resources in the OS. Access control systems are the electronic systems that are designed to control through a network and they should have an access to a network.

Firewalls(CO2)

- It is a combination of software and hardware.
- It maintains private network security by applying security policies at two or more network boundaries.
- The Design goals includes -
  - All network traffic must pass through the firewall.
  - Only authorized traffic will be allowed to pass from a firewall.

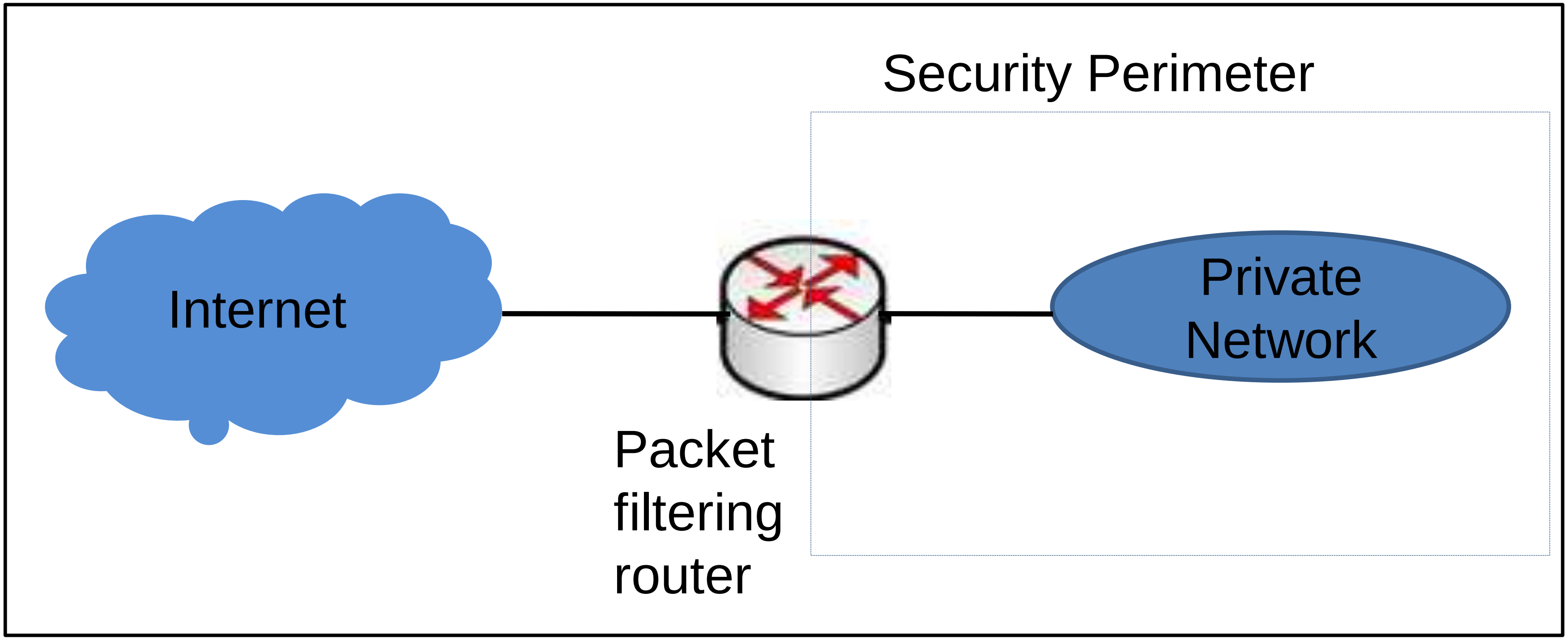
Types of Firewalls



Source: cyber security, G Padmavathi, swayam

Packet Filtering

It controls network access by analyzing incoming and outgoing packets.



Source: cyber security, G Padmavathi, swayam

Packet Filtering

Inspects the packets of data that are passed through the network and accepts or rejects the packets on the basis of the default or user-defined rules.

Packet filter is also known as network layer firewall.

Network layer firewalls are of two types-

1. Stateful-

Stateful firewalls maintain the state information of active session.

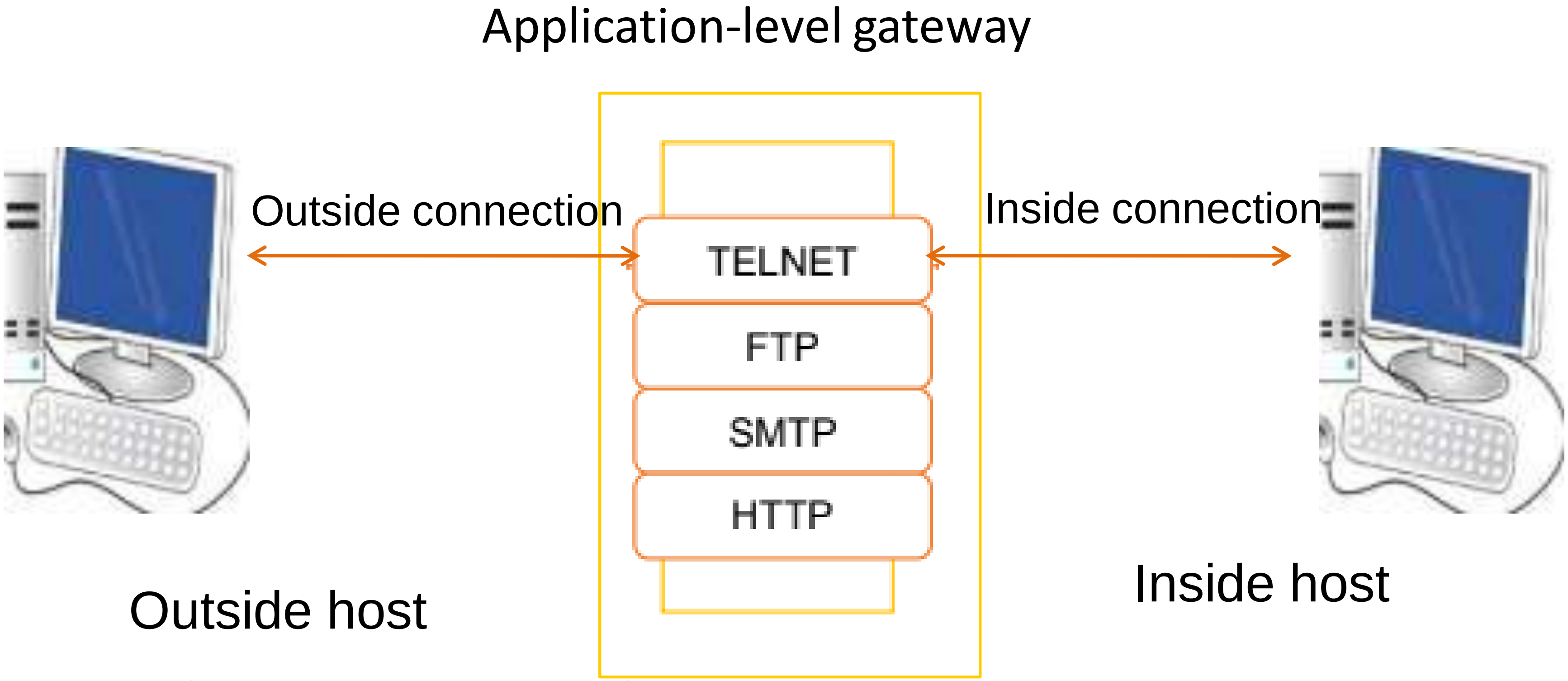
State contains properties, such as source and destination IP addresses, UDP or TCP ports, and the current stage of the connection’s lifetime.

2. Stateless-

They require less time to filter the packets as they do not maintain the state information of sessions.

Application level Gateway

- It is also known as proxy firewall.
- It filters the inbound traffic to certain specific applications



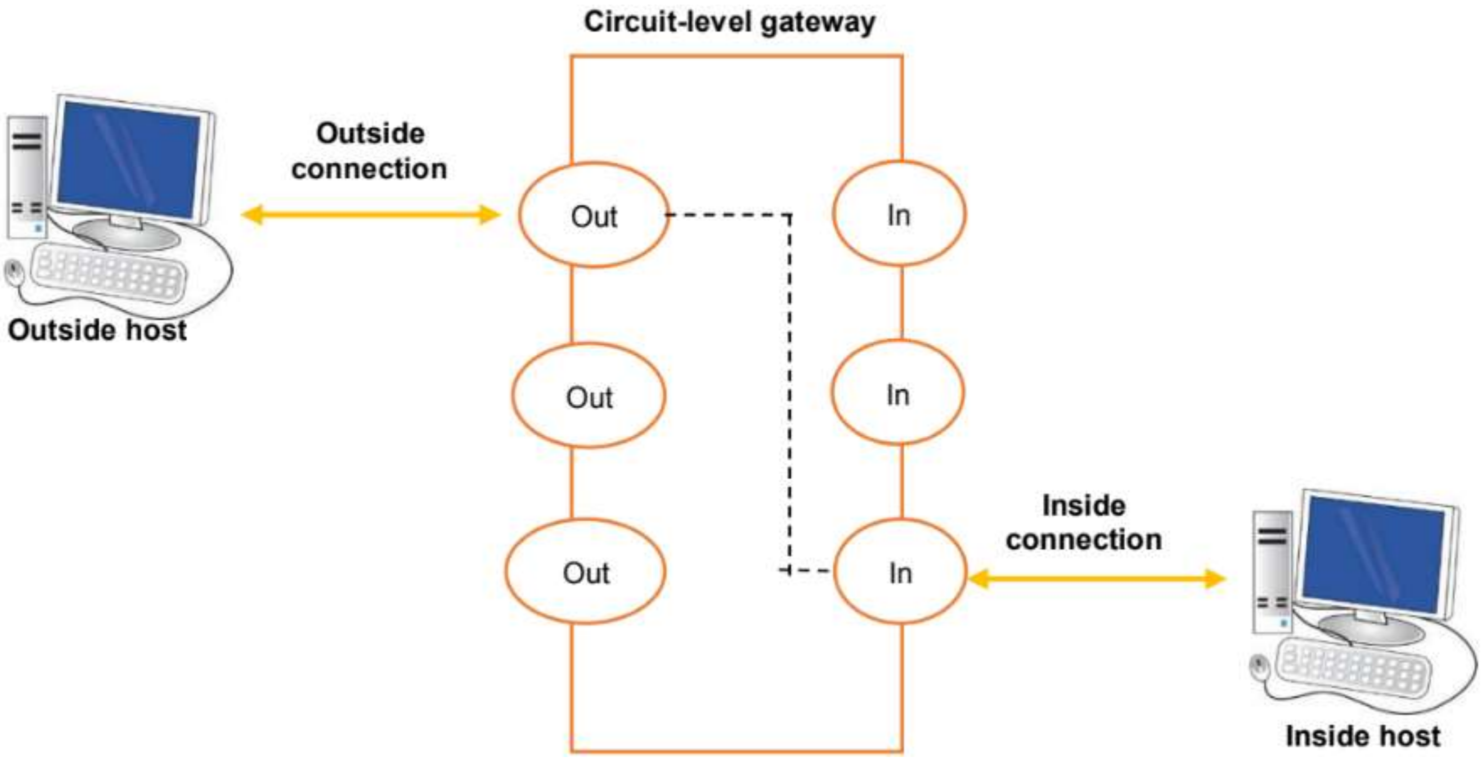
Source: cyber security, G Padmavathi, swayam

Application level Gateway

- Applies security mechanisms to specific applications such as File Transfer Protocol (FTP) and Telnet servers.
- Application layer firewalls are based on the application level of the TCP/IP stack. These firewalls intercept all packets that are sent or received from an application.
- Application layer firewalls help you in preventing unwanted outside traffic from reaching to protected machines.
- These firewalls can restrict or prevent spreading of computer worms and Trojans over a network.

Circuit-Level Gateway

It monitors the TCP data packets handshaking to ensure legitimate session



Source: Swayam

Circuit-Level Gateway

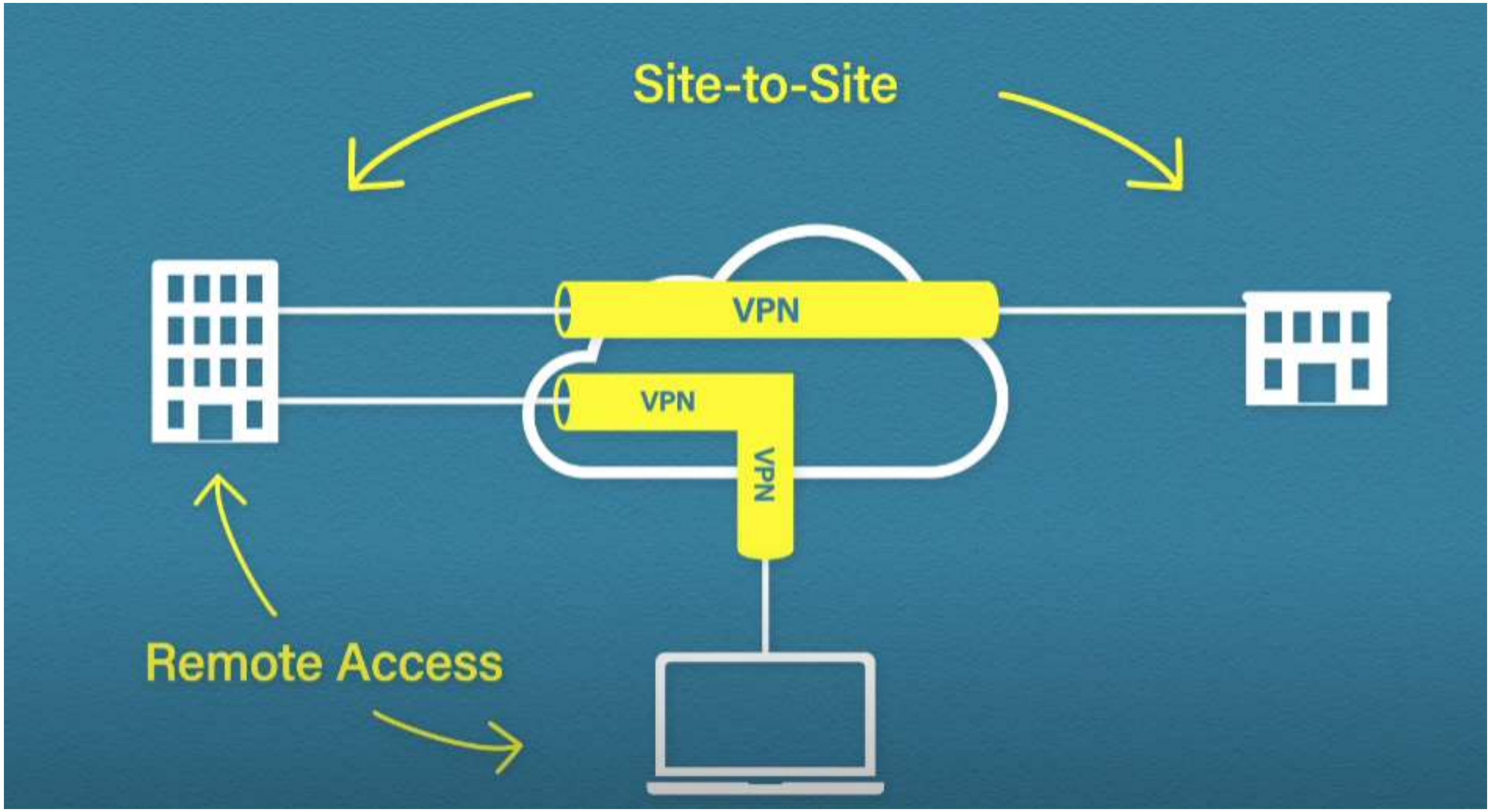
Applies security mechanisms after establishing a TCP or an UDP connection.

- The circuit-level gateway firewalls work at the session layer of the OSI model.
- They monitor TCP handshaking between the packets to determine whether or not the requested session is legitimate

Virtual Private Network (VPN)(CO2)

- VPN is a private communication network, which is the most secure, remote method of connecting a computer to a private network with the help of a public network, such as the Internet.
- It creates the virtual tunnel through which the data travels from one computer to the other over the network.
- Due to this, an attacker gets the way to use the remote client to relay attacks through the VPN tunnel.

Site to Site and Remote-Access VPNs



Source: CISCO

Intrusion Detection Systems(IDS)(CO2)

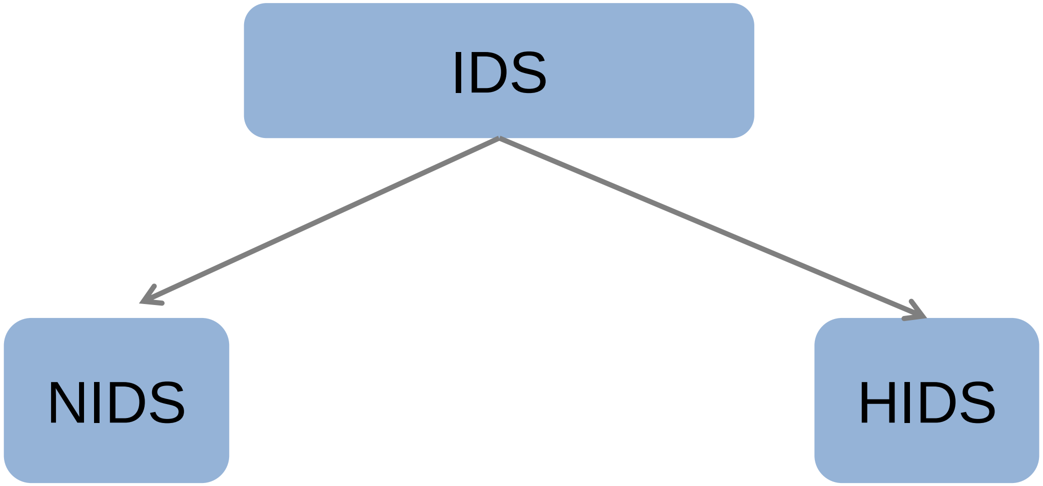
- IDS monitors network traffic for suspicious activity
- Issues alerts in case of illicit activity
- Anomaly detection and reporting are two main functions
- Administers two jobs namely, forensic analysis and alert generation
- Prone to false alarms or false positives

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

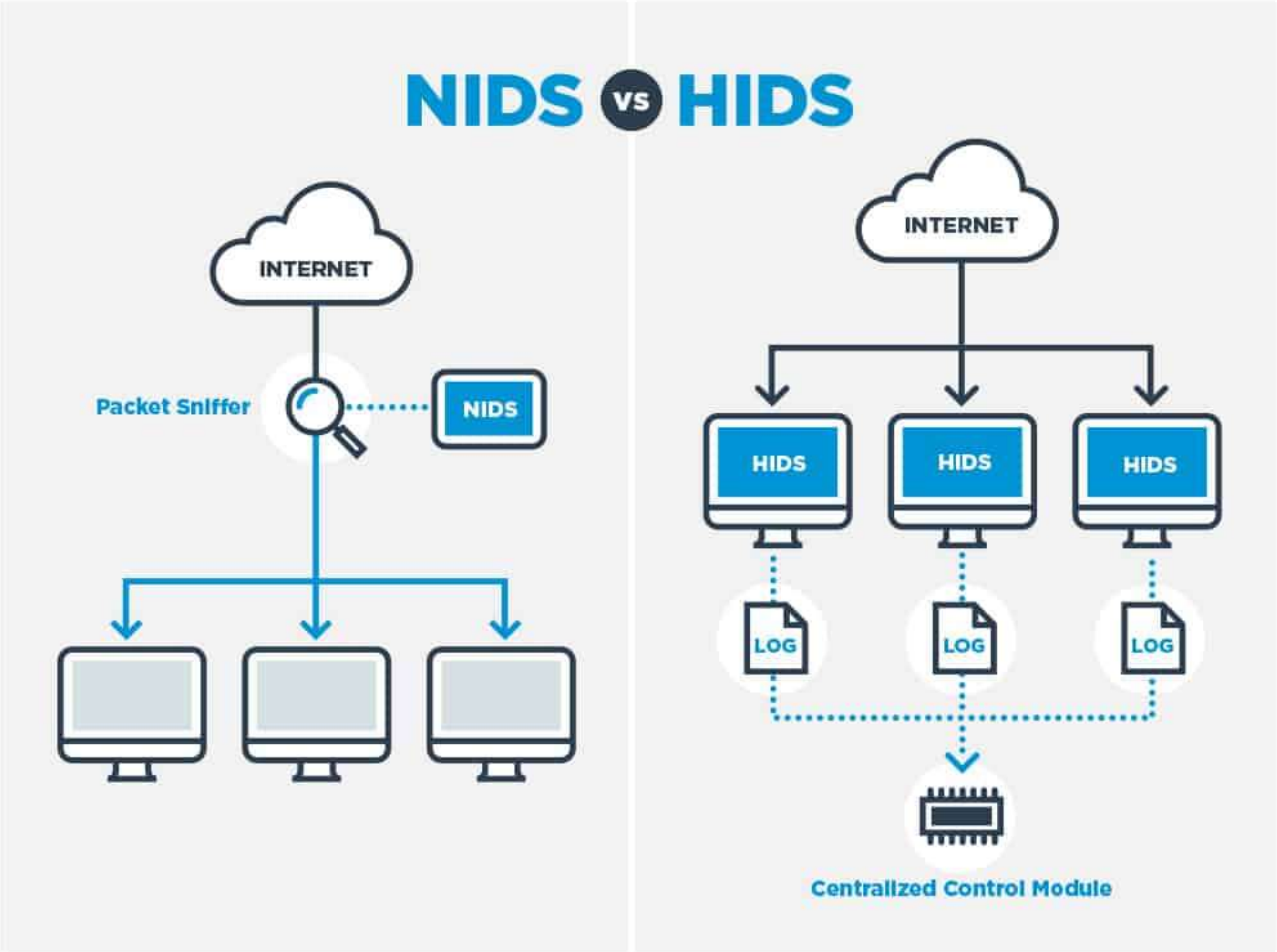
Types of Intrusion Detection Systems

- 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

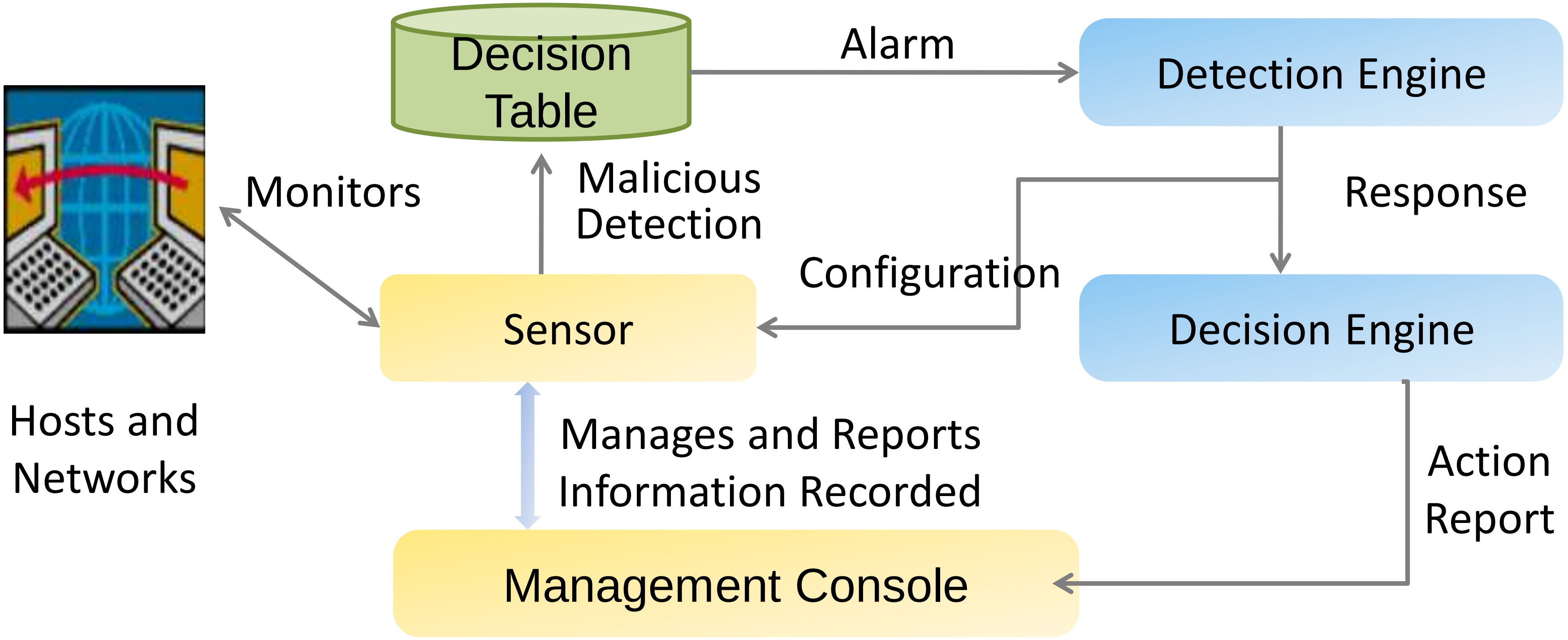
(NIDS) : A network intrusion detection system is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.

(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


Decision Table

Alarm

Detection Engine

Monitors

Malicious Detection

Response

Configuration

Sensor

Decision Engine

Hosts and Networks

Manages and Reports Information Recorded

Action Report

Management Console

Source: cyber security, G Padmavathi, swayam

Recap

- Firewalls

  -Packet filtering firewalls

  -Application level Gateway

  -Circuit-level Gateway

- Virtual Private Network (VPN)
- Intrusion Detection Systems(IDS)

  -NIDS

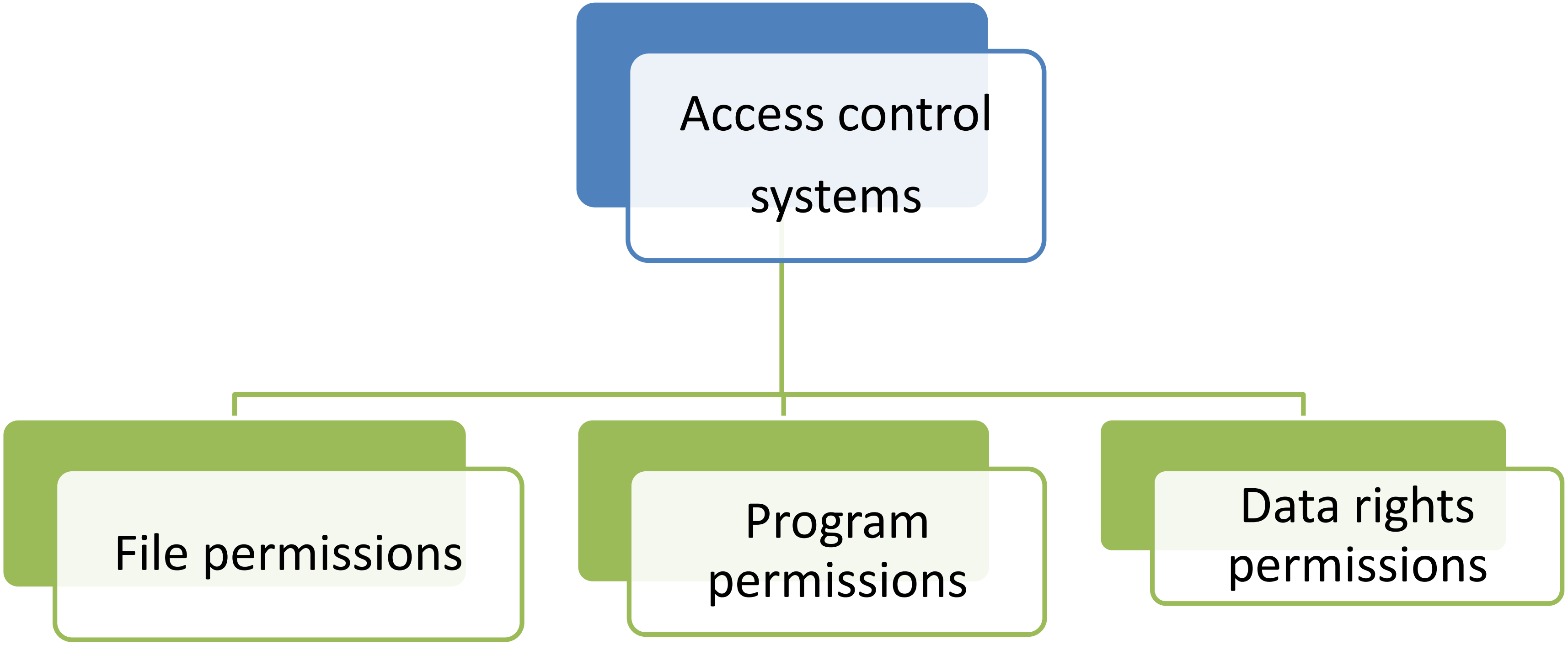
  -HIDS

Source: Swayam

Access Control(CO2)

- The term ‘access control’ refers to “the control of access to system resources after a user’s account credentials and identity have been authenticated and access to the system has been granted.”
- The permission to access a resource is called Authorization.

Access Control



Access control systems

File permissions

Program permissions

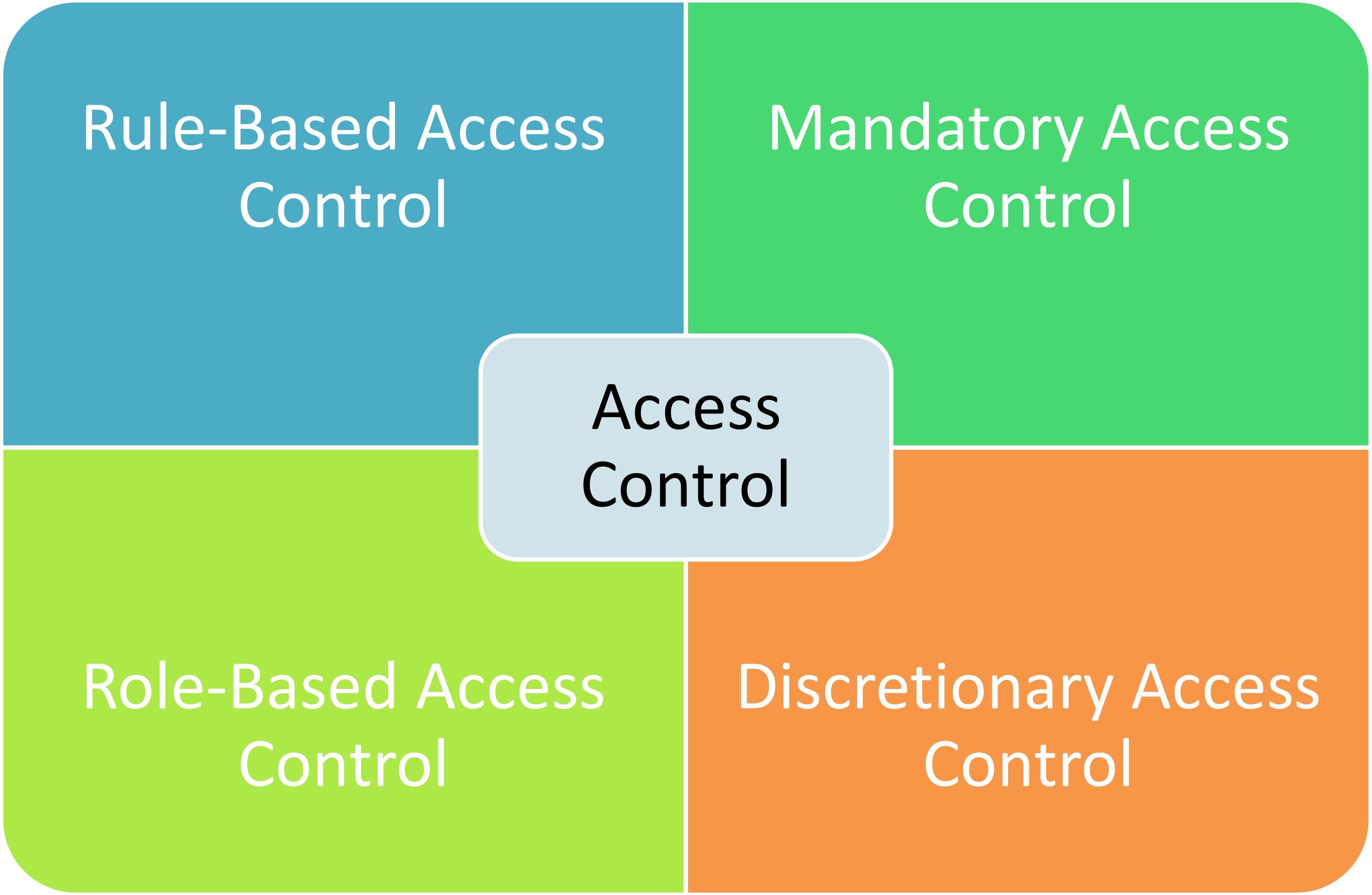
Data rights permissions

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

Mandatory Access Control

- Mandatory access control is widely considered the most restrictive access control model in existence.
- This type of access control allows only the system's owner to control and manage access based on the settings laid out by the system's programmed parameters.
- Such parameters can't be altered or bypassed. The end user doesn't have control over any of the permissions or privileges.
- They can only access points that the system owners allow them to access. Because of its high level of restriction, MAC is usually used for facilities or organizations that require maximum security, such as government facilities.

Discretionary Access Control

- Discretionary access control is the least restrictive type of access control.
- Under this system, individuals are granted complete control over any objects they own and any programs associated with such objects.
- The individuals can then determine who has access to their objects by programming security level settings for other users.

Role-Based Access Control

- Also known as nondiscretionary access control, role-based access control provides access based on an individual's position in an organization.
- In these systems, predefined roles are associated with specific permissions. They allow the administrator to assign an individual only the amount of access required for them to do their job.
- Because of its simplicity, this type of access control is one of the most popular forms used in businesses.

Rule-Based Access Control

- The last of the four main types of access control for businesses is rule-based access control.
- This system assigns or denies access to users based on a set of dynamic rules and limitations defined by the owner or system administrator.
- Such rules may limit access based on a number of unique situations, such as the individual's location, the time of day, or the device being used.
- The ability to customize rules and permissions makes RBAC an ideal form of access control for businesses that require a dynamic security solution.

Daily Quiz

1. What is access control?
2. Differentiate MAC and DAC.
3. What are the types of Firewall?
4. What are the types of IDS?
5. Write types of access control.

Weekly Assignment

1. Explain Application Security? Explain the steps involved in securing Database?
2. Explain the working of Virtual Private network?
3. Explain types of Firewall?
4. What is the data security consideration? Explain in this reference Data backup security, Data archival security and Data disposal considerations?
5. w can be Intrusion Detection system is the backbone of Information system? Justify along with its categories?

Topic Link

- https://www.youtube.com/watch?v=Zl_BQoJqClM
- https://www.youtube.com/watch?v=mY_LtZhd6xU

Topic Objective/Topic Outcome

Topic	Objective	CO Mapping
Security Threats	Study the various security threats characteristics Viruses, Worms, Trojan Horse, Bombs, Trapdoors, Spoofs, E-mail Viruses, Macro Viruses, Malicious Software	CO2

Security Threats(CO2)

- Viruses
- Worms
- Trojan Horse
- Bombs
- Trapdoors
- Spoofs
- E-mail viruses
- Macro viruses
- Malicious Software
- Network and Denial of Service Attack
- Security

Viruses(CO2)

- A virus refers to piece of software that is designed and developed with the purpose of infecting a computer system and performs illicit operations.
- A virus infected system can hamper data stored on a hard drive, crash the OS, or get spread on a network.
- Some of the ways by which a virus gets transmitted to a system are:

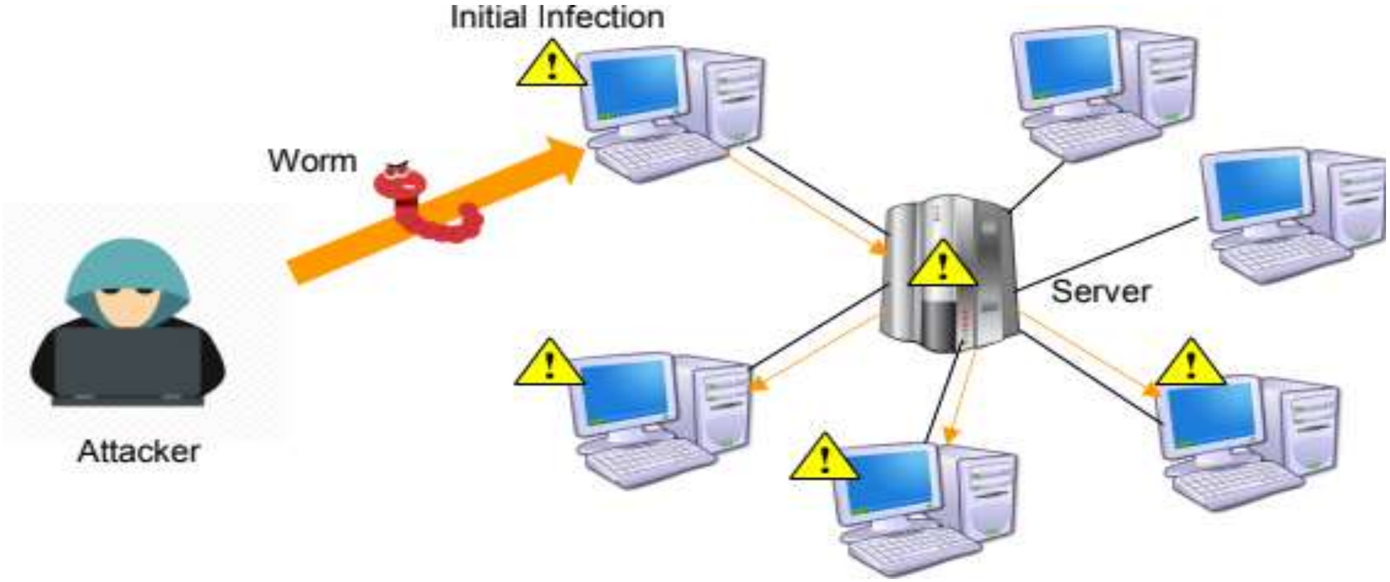
  -On using infected media, such as CDs or USB drives

  -Through e-mails and accessing social websites as a part of another program.

Full form of **VIRUS** : Vital Information Resource Under Seize.

Worms(CO2)

A worm is a type of malware or malicious software that can replicate rapidly and spread across devices within a network.



Source: swayam

Worms

- Worms can be defined as threats that are self-sufficient to replicate themselves and do not need any host application to get transmitted.
- They are also capable of delivering a virus to a system.
- Earlier, the worms used to reside in the RAM of a target computer; however, now a days, they can make use of TCP/IP, e-mail, or Internet services.

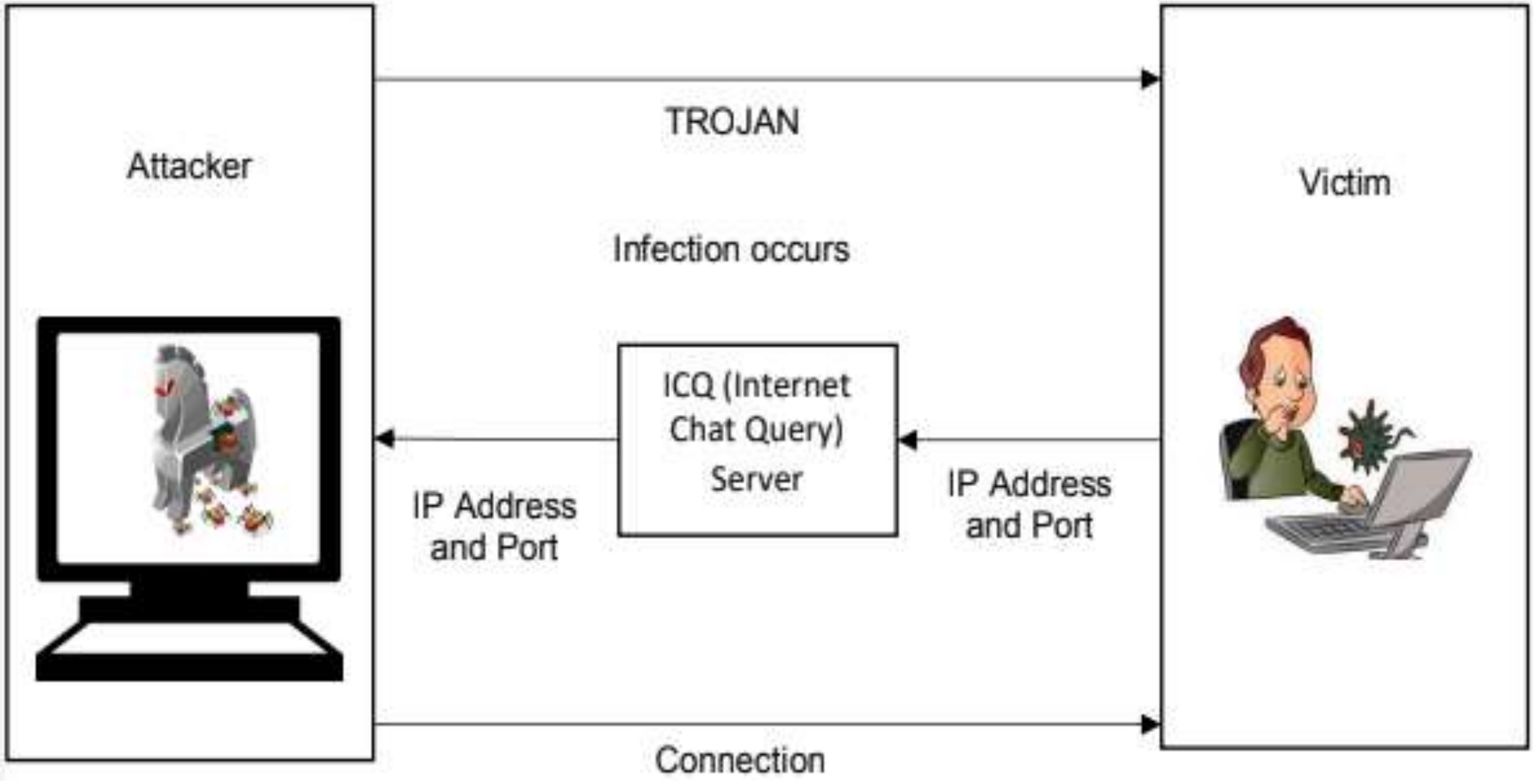
Trojan Horses(CO2)

- Trojan horses can be defined as programs that are transmitted to a system under disguise of any legitimate application or program, such as an attachment to a program or as part of an installation process.

- During installation, either a backdoor is created or the original program gets replaced by a Trojan horse.

- Due to difficulty in detection of a Trojan horse, best preventive measure is to backup data after installing new software.

Trojan Horses



Source: Swayam

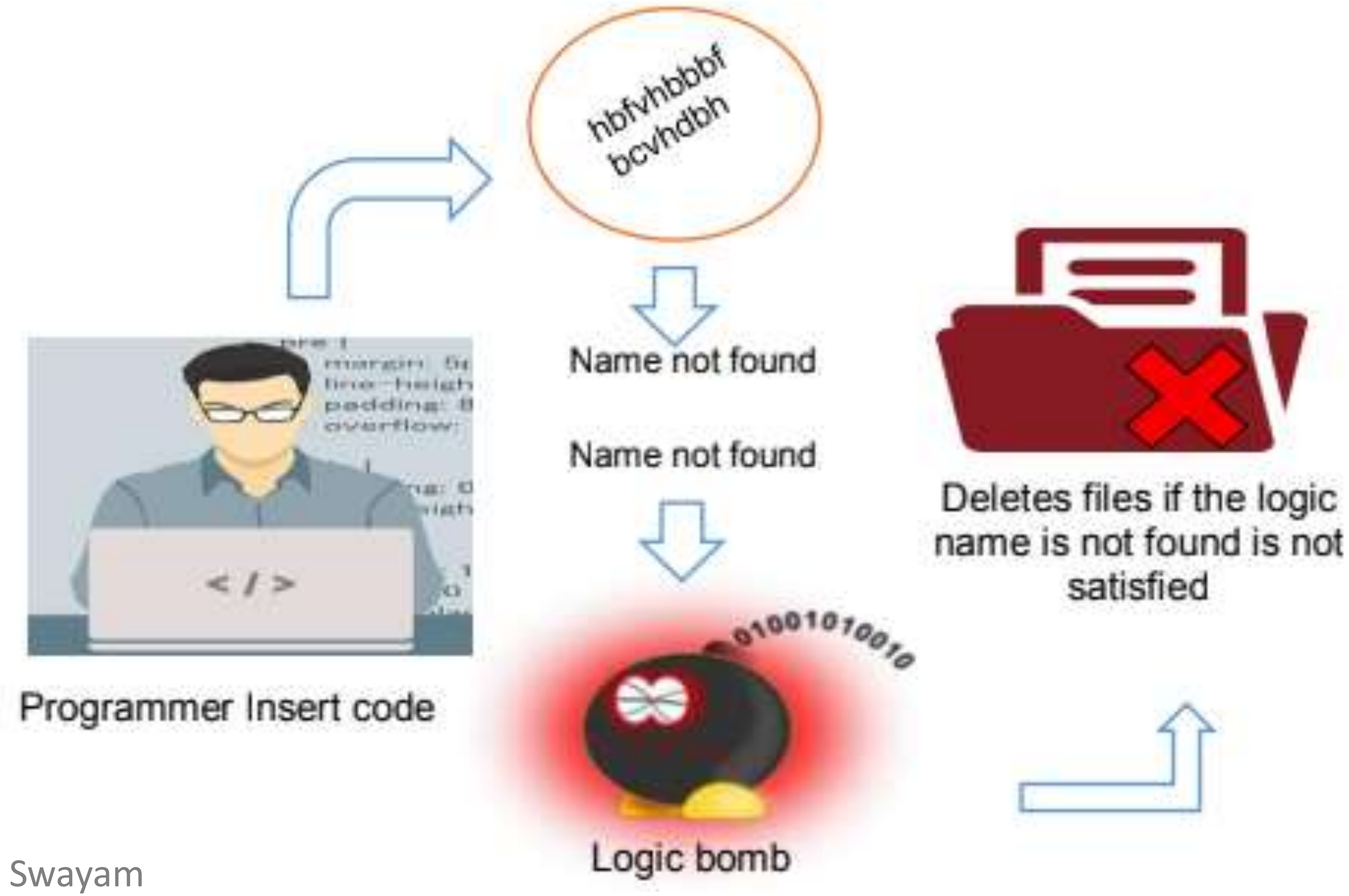
Logic bombs(CO2)

- Logic bombs refer to programs or code snippets that are executed when a predefined event occurs.

- These logic bombs display a message to user and occur at time when either the user is accessing the Internet or making use of a word processor application.

- The logic bombs do not directly attack; however, they are responsible for informing victim if the criteria for an attack to start have been met.

Logic bombs



Source: Swayam

Trapdoors(CO2)

- The back door term is referred to as gaining access to a network.

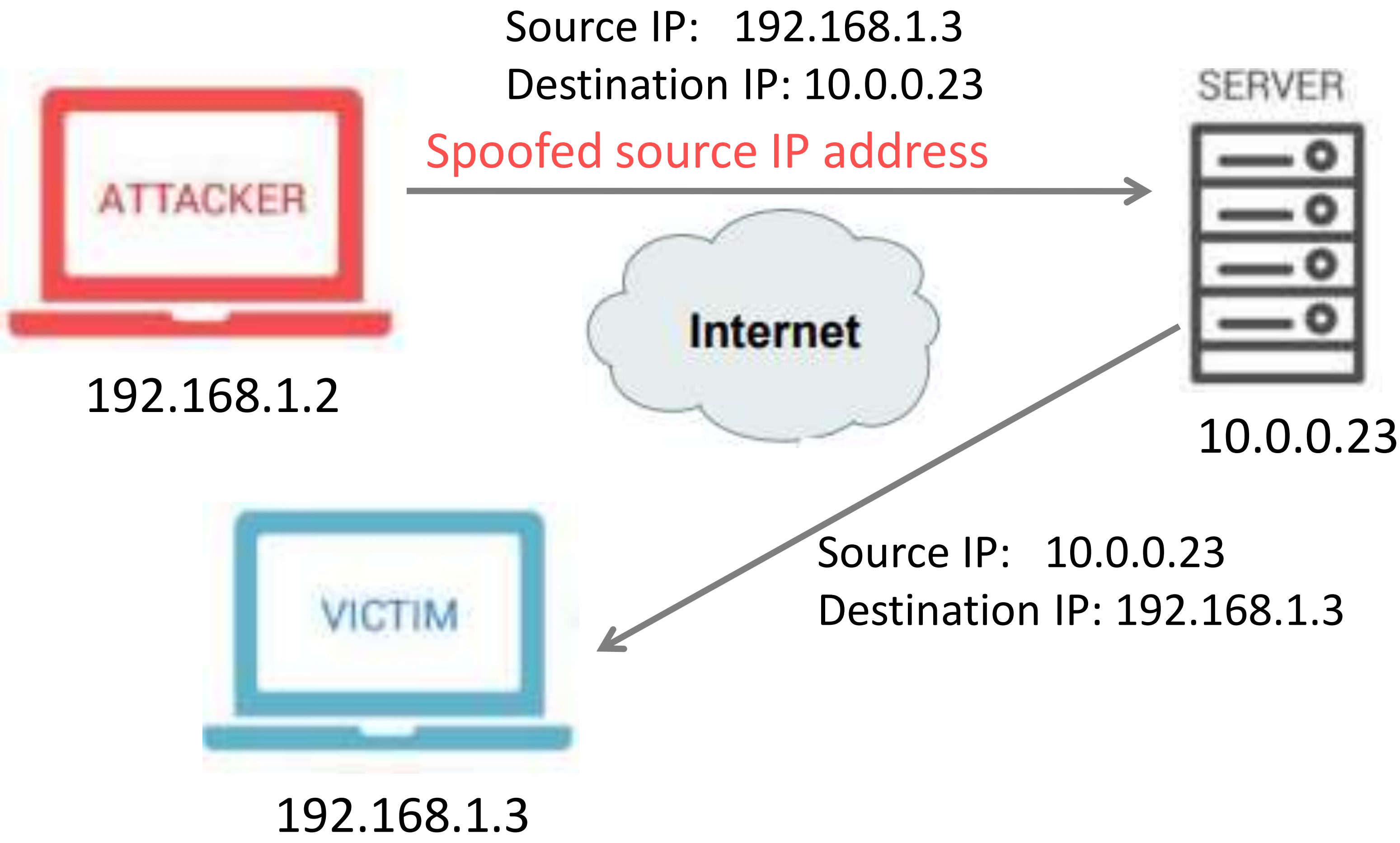
- The backdoor attack lets malicious user to enter illicit code at the time of its execution. Moreover, a backdoor attack is primarily an access or a modification attack. However, it requires user ID and password to gain administrative privileges.

- Some of the tools that are used to create backdoor attacks are Back Orifice and NetBus.

Spoofing (CO2)

- Spoofing means to provide false information about your identity to gain unauthorized access to other’s computer systems.
- IP spoofing and DNS spoofing are the most popular spoofing attacks.
- The objective of IP spoofing is to make the data look as if it has come from a trusted host, when it did not.
- In DNS spoofing, the DNS server is given information about a name server and the server assumes this information as legitimate, when it is not.

IP Spoofing



Source: swayam

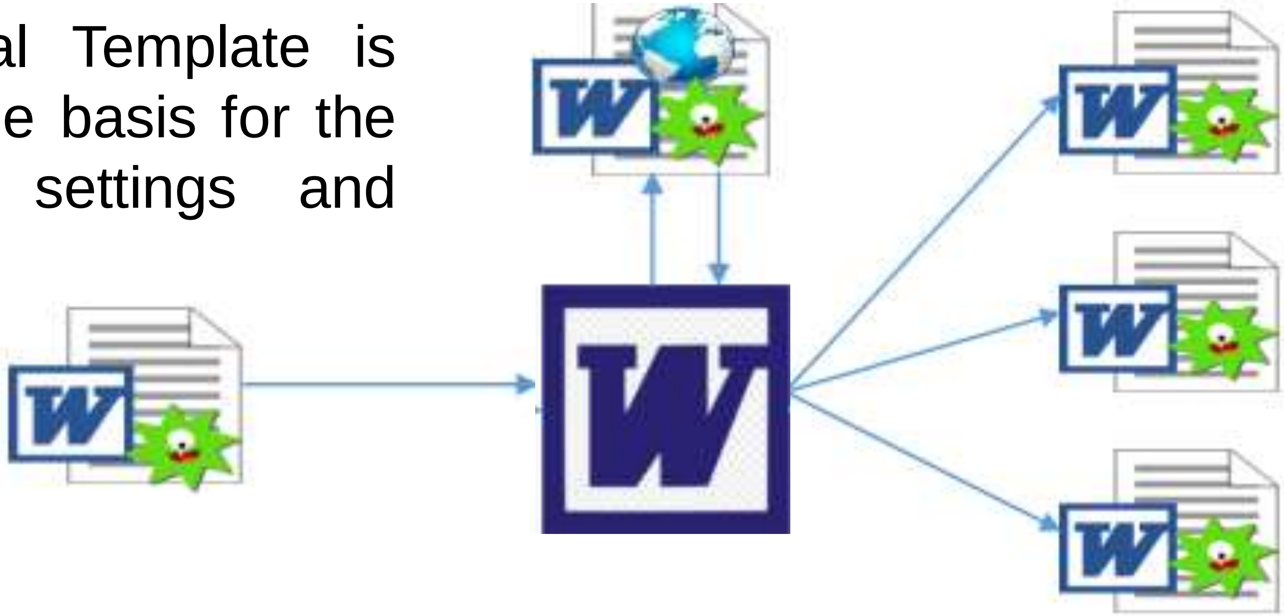
E-mail Viruses

An email virus is **malicious software or a program that attaches itself to an email to infect your computer**. Email viruses almost always are linked to malware or phishing attacks.

Source: Swayam

Macro Viruses

The Global Template is used as the basis for the document settings and macros



When an infected document is opened with Word, it will usually copy its macro codes in the Global Template

With the macro virus already resident in the Global Template, it can already produce additional copies of itself to other documents accesses by Word

Source: Swayam

Malicious Software

- Malicious code is a new kind of threat in the form of an auto-executable application.

Malicious code can be categorized into the following types:

- Code that causes access violations: Refers to the category of malicious code that tries to delete, steal, alter, or execute unauthorized files. It can steal passwords, files, and other confidential data.
- Code that enables DoS attacks: Refers to the category of malicious code that prevents the user from using the system. It may destroy the files that are open at the time of the attack.

Network and Denial of Service Attacks(CO2)

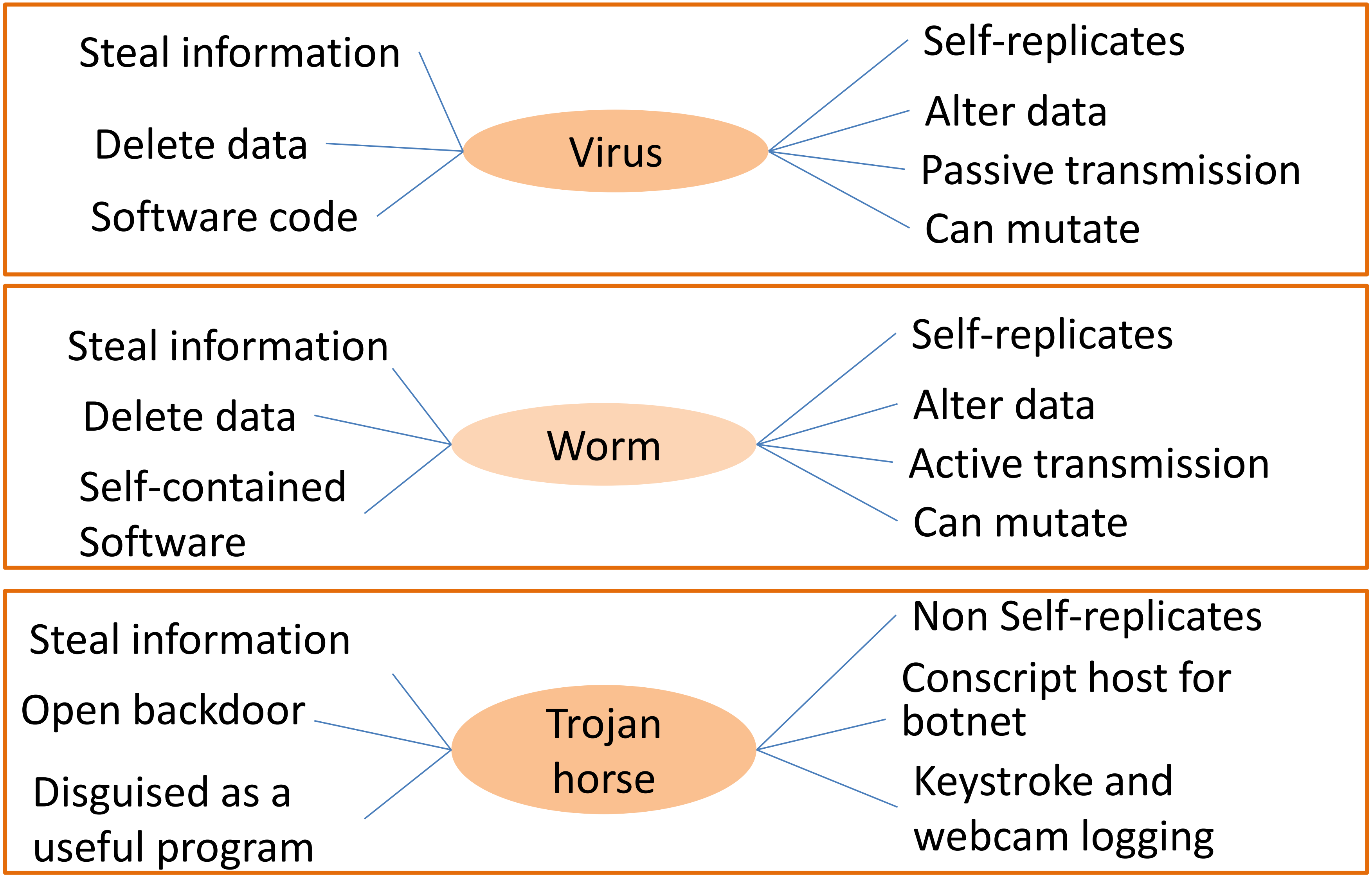
A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

Denial of Services Attack

- DoS Attack (Denial of Service Attack)
- DDoS Attack (Distributed Denial of Service Attack)
- DoS makes the system unresponsive to the actual service requests
- It does so by overpowering the system resources
- DDoS attack is similar to the DoS attack
- Difference is that the attack is launched from a series of host machines

Similarities and differences between Virus, Worms and Trojan horse



Steal information

Delete data

Software code

Virus

Self-replicates

Alter data

Passive transmission

Can mutate

Steal information

Delete data

Self-contained Software

Worm

Self-replicates

Alter data

Active transmission

Can mutate

Steal information

Open backdoor

Disguised as a useful program

Trojan horse

Non Self-replicates

Conscript host for botnet

Keystroke and webcam logging

Recap

- Access control systems
  - File permissions
  - Program permissions
  - Data rights permissions

- Security Threats
  - Viruses
  - Trojan Horses
  - Worm
  - IP Spoofing
  - Malicious Software

Daily Quiz

1. What is worm in Network security?
2. Differentiate trapdoor and Trojan horse.
3. What is DoS attack?
4. Write 5 viruses name.
5. Differentiate between virus and Worm.
6. What is IP Spoofing?
7. What is Trapdoor?
8. what is Ransomware?

Weekly Assignment

1. Explain Application Security? Explain the steps involved in securing Database?
2. Explain types of Firewall?
3. Explain the difference between Virus, Worms, Logic bomb and Trojan Horse?

Weekly Assignment

4. What is the data security consideration? Explain in this reference Data backup security, Data archival security and Data disposal considerations?

5. How can be Intrusion Detection system is the backbone of Information system? Justify along with its categories?

6. Write a short note on

   A. Denial of service attack.

   B. IP spoofing

   C. Electronic data interchange

Topic Links

- https://youtu.be/2YGUvopGkQc
- https://youtu.be/Ofoshc9CblU
- https://www.youtube.com/watch?v=Zl_BQoJqClM
- https://www.youtube.com/watch?v=mY_LtZhd6xU
- https://www.youtube.com/watch?v=qEbZN9GPQ6A
- https://youtu.be/dYQMzyfFrTE
- https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

Topic Objective/Topic Outcome

Topic	Objective	CO Mapping
Security Threats to E-Commerce	Develop an understanding of threats to Electronic Payment System, e- Cash, Credit/Debit Cards.	CO2

Threats to E-Commerce (CO2)

- E-Commerce refers to the activity of buying and selling things over the internet.
- E-commerce can be drawn on many technologies such as mobile commerce, Internet marketing, online transaction processing, electronic funds transfer, supply chain management, electronic data interchange (EDI), inventory management systems, and automated data collection systems.
- E-commerce threat is occurring by using the internet for unfair means with the intention of stealing, fraud and security breach

Source: swayam

Threats to E-Commerce

- Unauthorized internal users who may access confidential information by using passwords for committing fraud or theft.
- Former employees of an organization who have maintained access to the information sources directly by creating alternative password. “back doors” into the computer systems or indirectly through former co- workers.
- Weak access point in information infrastructure and security that can expose company information and trade secrets.

Source: swayam

Electronic Payment Systems

- E-Commerce or Electronics Commerce sites use electronic payment where electronic payment refers to paperless monetary transactions.
- Electronic payment has revolutionized the business processing by reducing paper work, transaction costs, labour cost.
- Being user friendly and less time consuming than manual processing, helps business organization to expand its market reach / expansion.
  - Credit Card
  - Debit Card
  - Smart Card
  - E-Money
  - Electronic Fund Transfer (EFT)
  - E- Wallet

Types of EPS

E Cash / E Money:

- A system that allows a person to pay for goods or services by transmitting a number from one computer to another.
- Like the serial numbers on real currency notes, the E-cash numbers are unique.
- This is issued by a bank and represents a specified sum of real money.
- It is anonymous and reusable.

E-Wallet:

- The E-wallet is another payment scheme that operates like a carrier of e-cash and other information.
- The aim is to give shoppers a single, simple, and secure way of carrying currency electronically.
- Trust is the basis of the e-wallet as a form of electronic payment.

Types of EPS

Smart Card:

- A smart card, is any pocket-sized card with embedded integrated circuits which can process data.
- This implies that it can receive input which is processed and delivered as an output.

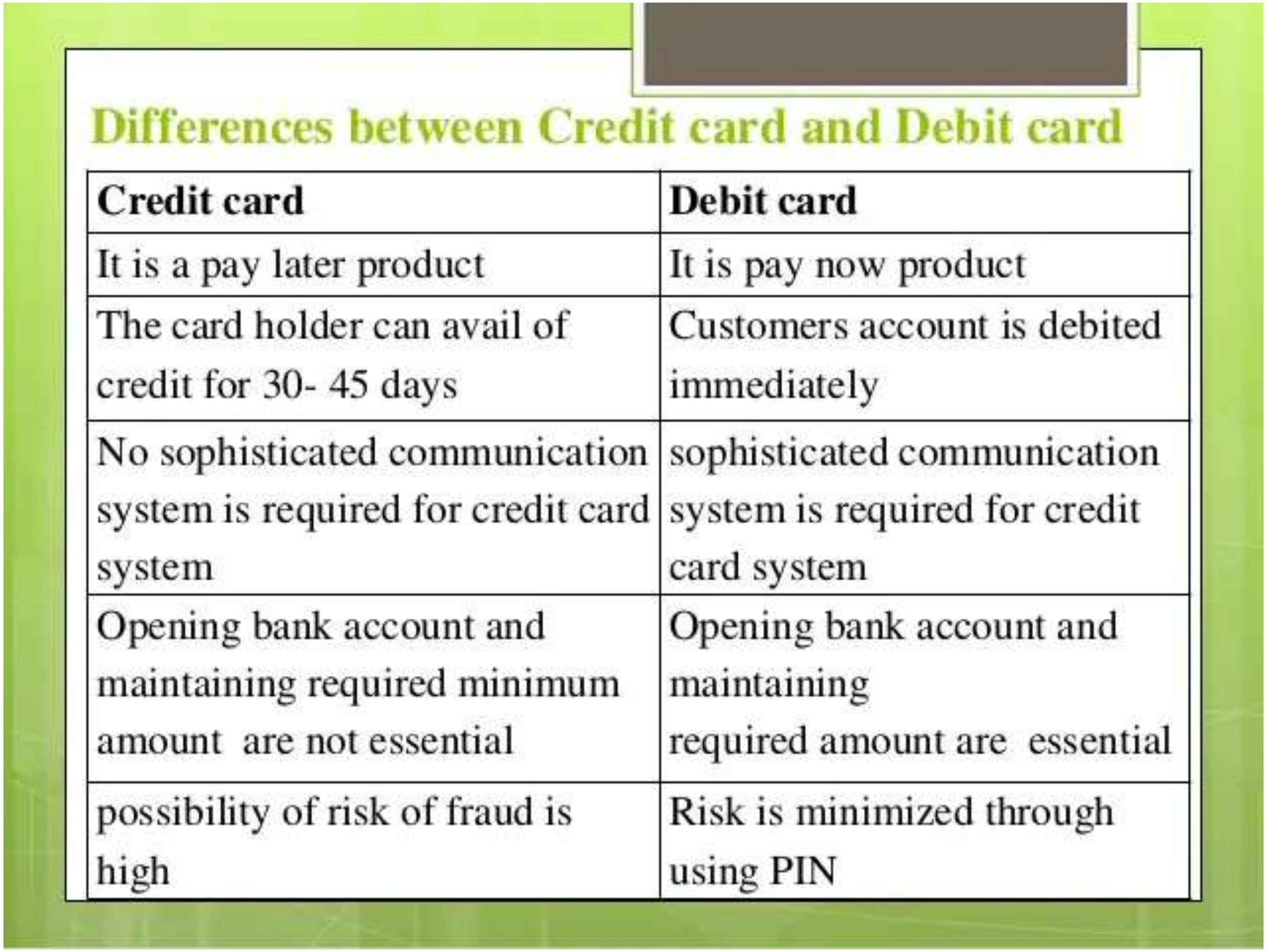
Credit Card :

- It is a Plastic Card having a Magnetic Number and code on it.
- It has Some fixed amount to spend.
- Customer has to repay the spend amount after sometime.

Debit Card :

- Similar to Credit card on coding and encryption.
- Purchase limit depends on the available balance in the account.

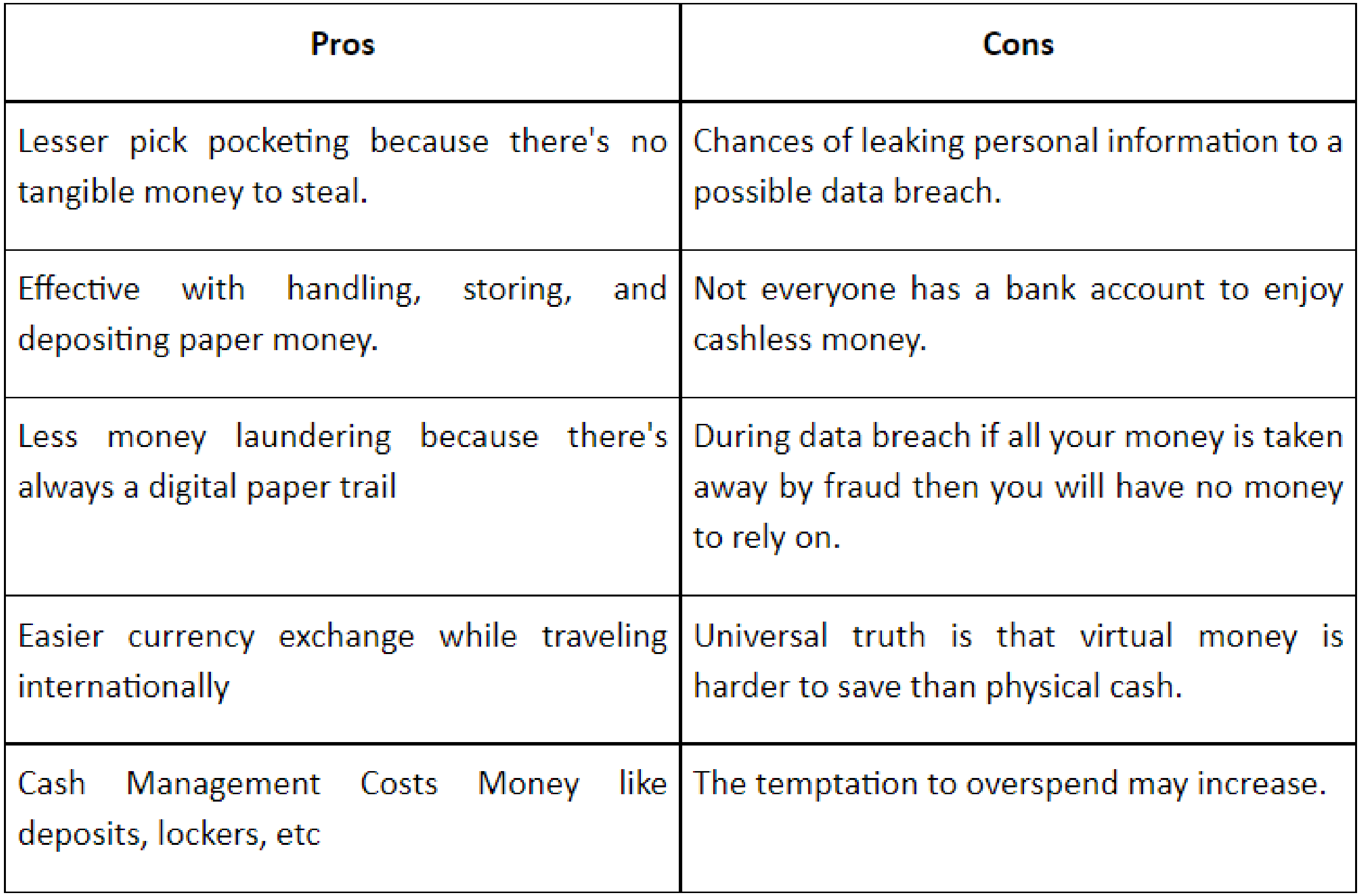
Credit and Debit Card Differences



Differences between Credit card and Debit card

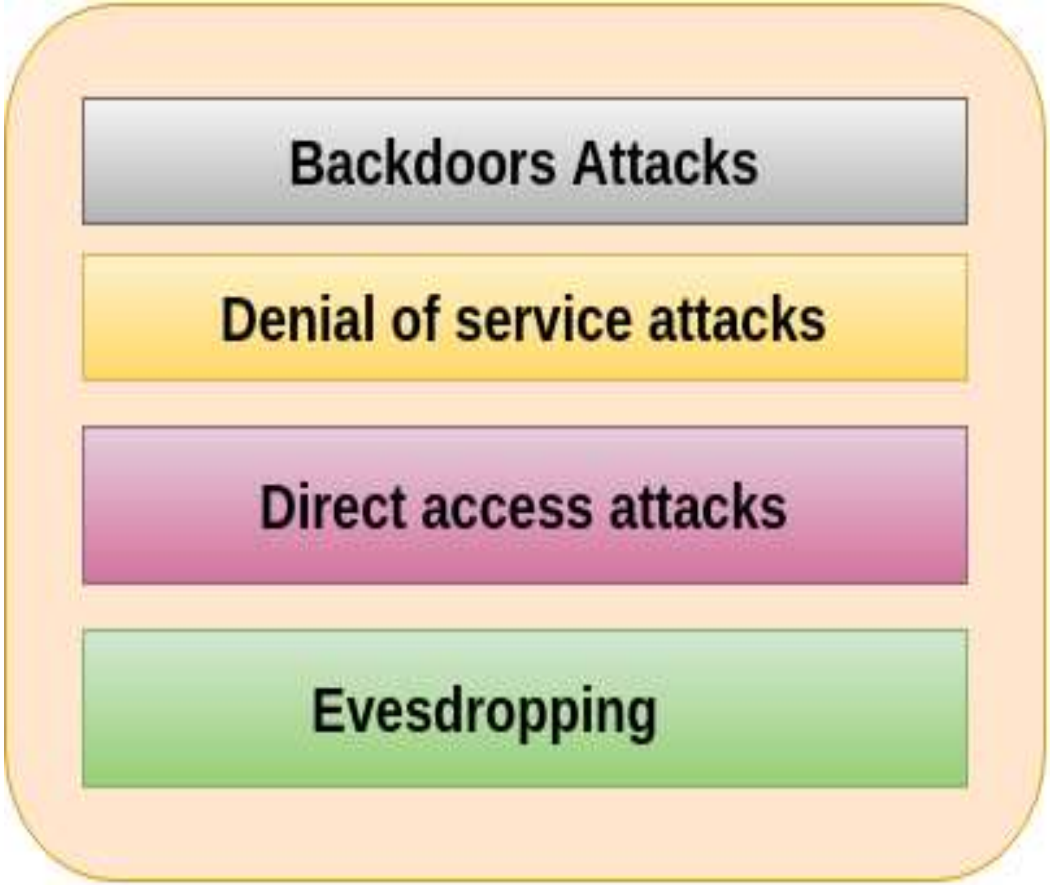
Credit card	Debit card
It is a pay later product	It is pay now product
The card holder can avail of credit for 30- 45 days	Customers account is debited immediately
No sophisticated communication system is required for credit card system	sophisticated communication system is required for credit card system
Opening bank account and maintaining required minimum amount are not essential	Opening bank account and maintaining required amount are essential
possibility of risk of fraud is high	Risk is minimized through using PIN

E-cash Pros and Cons



Pros	Cons
Lesser pick pocketing because there's no tangible money to steal.	Chances of leaking personal information to a possible data breach.
Effective with handling, storing, and depositing paper money.	Not everyone has a bank account to enjoy cashless money.
Less money laundering because there's always a digital paper trail	During data breach if all your money is taken away by fraud then you will have no money to rely on.
Easier currency exchange while traveling internationally	Universal truth is that virtual money is harder to save than physical cash.
Cash Management Costs Money like deposits, lockers, etc	The temptation to overspend may increase.

E-cash Threats



Backdoors Attacks

Denial of service attacks

Direct access attacks

Evesdropping

Source: javatpoint

Daily Quiz

1. What is Zero day vulnerabilities?
2. Differentiate Data Backup and Data Archival.
3. What are the types of Firewall?
4. What are the types of IDS?
5. Write 5 viruses name.
6. Differentiate virus and Worm.
7. What is IP Spoofing?
8. What is Trapdoor?
9. what is Ransomware?

Weekly Assignment

1. Explain Application Security? Explain the steps involved in securing Database?
2. What is digital signature? What are the requirements of digital signature system? List the security services provided by the digital signature.
3. Explain the working of Virtual Private network?
4. Explain types of Firewall?
5. Explain the difference between Virus, Worms, Logic bomb and Trojan Horse?

Weekly Assignment

8. What is the data security consideration? Explain in this reference Data backup security, Data archival security and Data disposal considerations?
9. How can be Intrusion Detection system is the backbone of Information system? Justify along with its categories?
10. Write a short note on

    A. Denial of service attack.

    B. IP spoofing

    C. Electronic data interchange

Topic Links

- https://youtu.be/2YGUvopGkQc
- https://youtu.be/Ofoshc9CblU
- https://www.youtube.com/watch?v=Zl_BQoJqClM
- https://www.youtube.com/watch?v=mY_LtZhd6xU
- https://www.youtube.com/watch?v=qEbZN9GPQ6A
- https://youtu.be/dYQMzyfFrTE
- https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

MCQ s

- Label the process of setting up of fake access points in high traffic public locations.

  a)Unsecured Wi-Fi b)Phishing Attacks

  b)Network Spoofing c)Spyware

- Recognize the cheapest form of Authentication.

  a)Password based Authentication b)Encryption

  c)Biometric based Authentication d)Smart cards

- Identify the activity that occurs due to malware in Cloud Services.

  a)Trojans b)Worms

  c)Macro viruses d)**Data Exfiltration**

MCQ s

- Which is the most common risk in social media?

  a)Third-party apps b) Spams

  c)Privacy settings d)**Human error**

- Point out the security methods applied against man-in-the-middle attack.

  a)Biometrics b)Cryptography

  c)Digital signature d)Access control list

- Data can be disposed by:

  a)Handing over the storage devices to anyone

  b)Shutting down the system that uses the storage device

  c)T**hrashing the storage devices into metal scrap**

  d) None of the above

MCQ s

- Firewalls are used to:

  a) Provide data backup facilities

  b) Prevent hackers from accessing your computer through the Internet by blocking back doors or open ports that connect your computer with the Internet

  c) Provide network integration facilities

  d) All of the above

- Quote the cryptographic type used by Digital Signatures for validating the authenticity and integrity of a message

  a) Private key

  b) Public key

  c) Digital key

  d) Digital Certificates

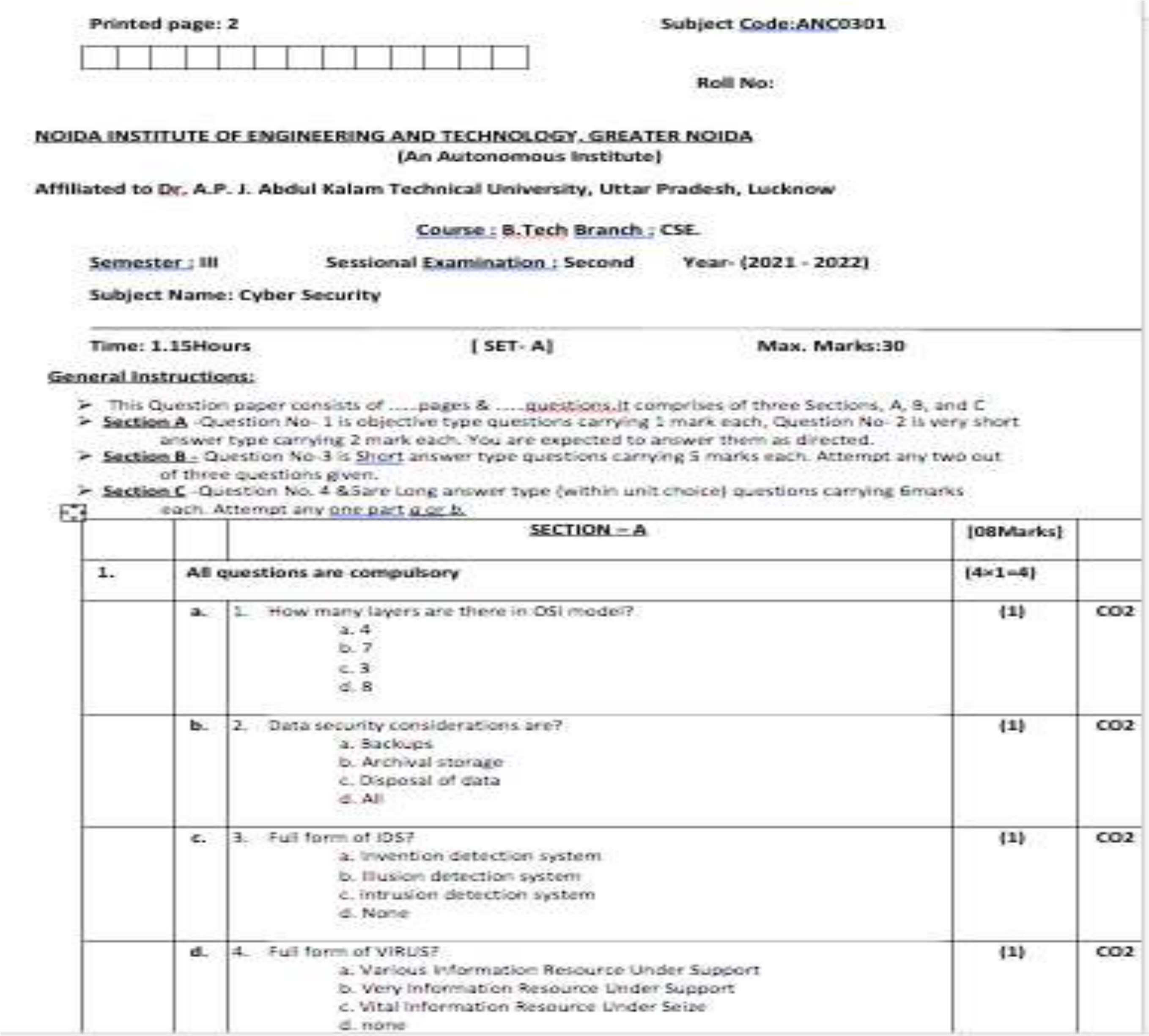
Glossary Questions

Fill the right options:

Management console, attack signatures, Sensors, malicious packet, match

1. An IDS comprises ___________and sensors
2. It has a database of ________
3. _________detect any malicious activity
4. It also matches the ___________against the database
5. If found a _____, the sensor reports the malicious activity to the management console

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

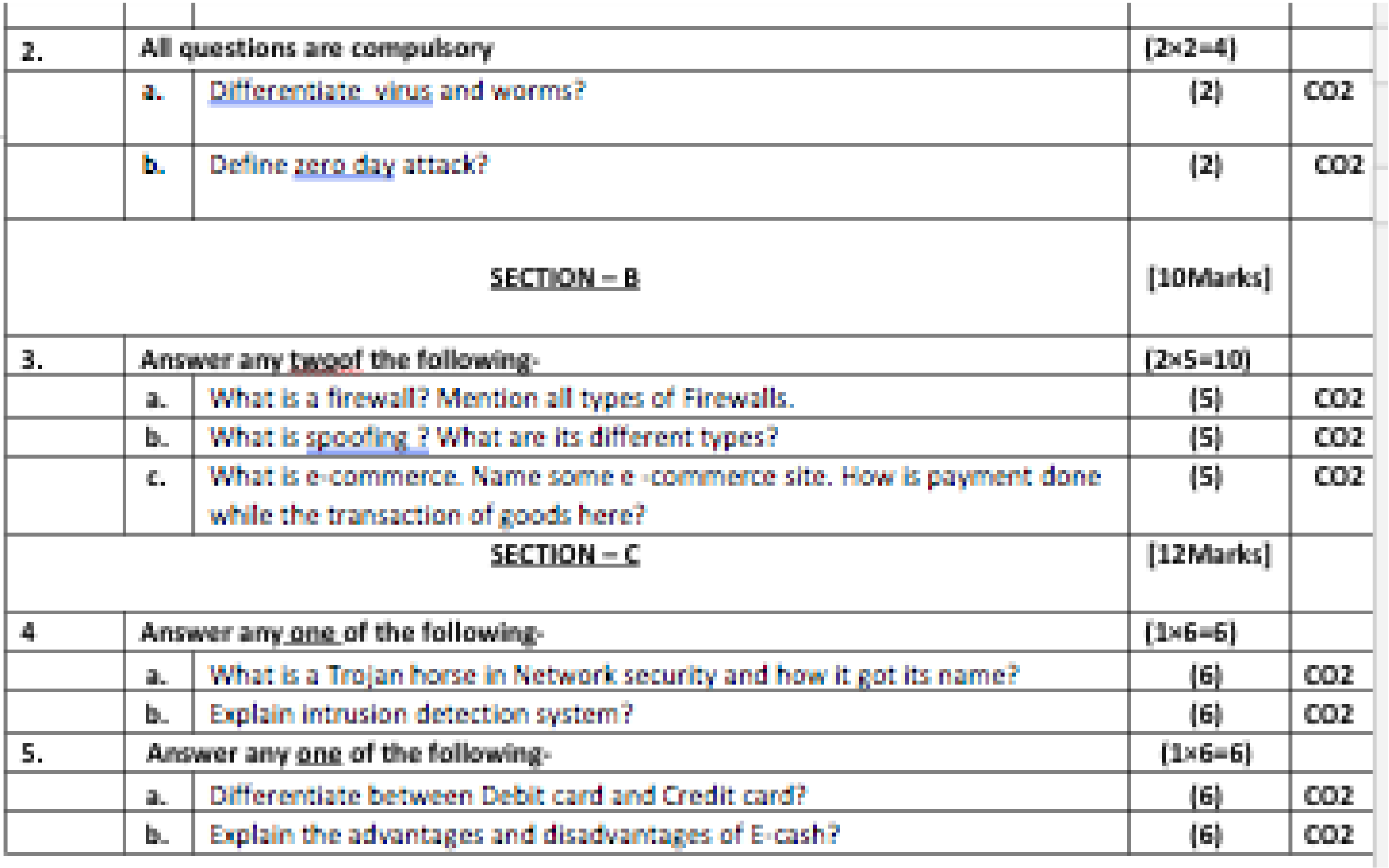
Time: 1.15Hours | [SET- A] | Max. Marks:30

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.

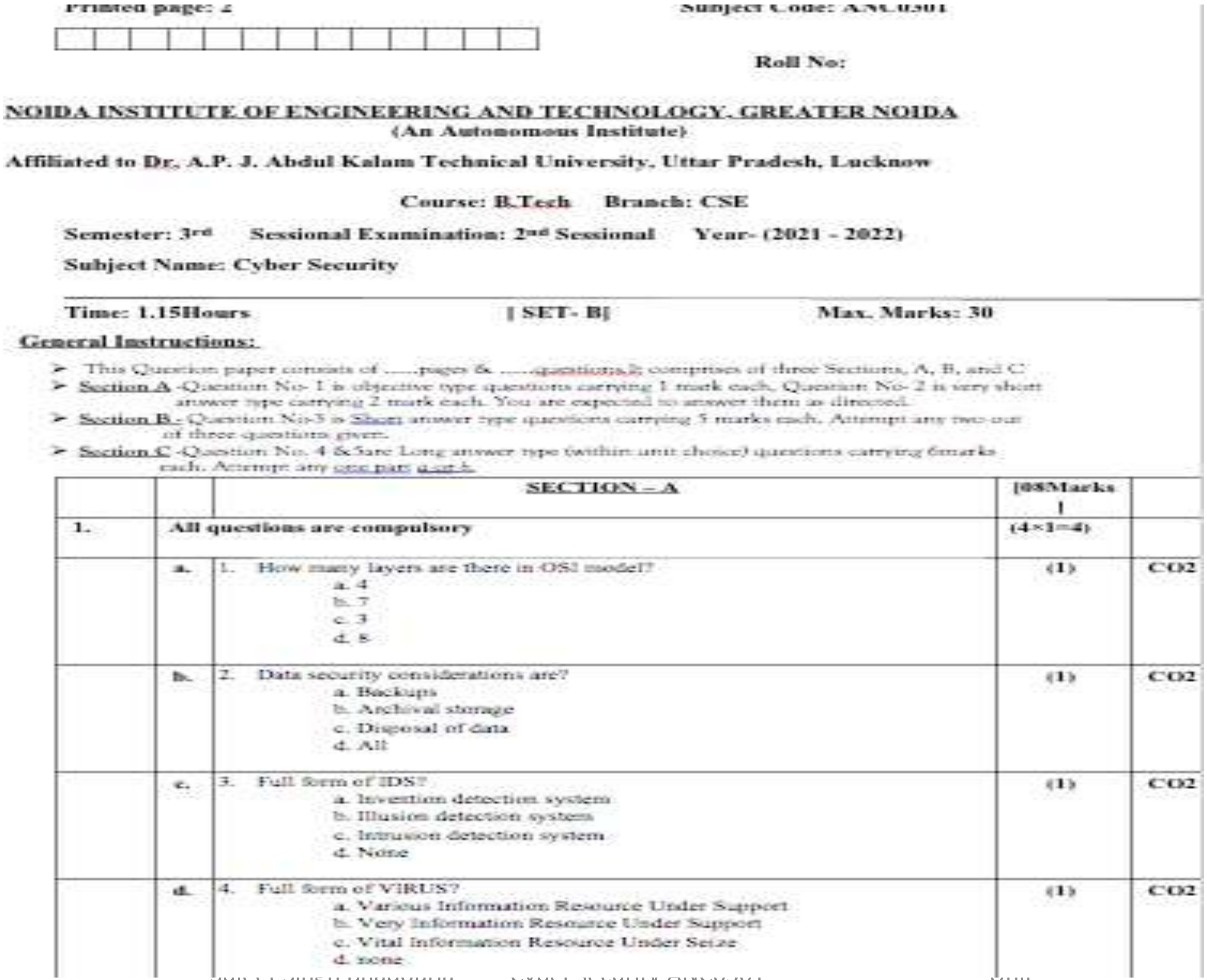
		SECTION – A	[08Marks]	
1.	All questions are compulsory		(4×1=4)	
	a.	1. How many layers are there in OSI model? a. 4 b. 7 c. 3 d. 8	(1)	CO2
	b.	2. Data security considerations are? a. Backups b. Archival storage c. Disposal of data d. All	(1)	CO2
	c.	3. Full form of IDS? a. Invention detection system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

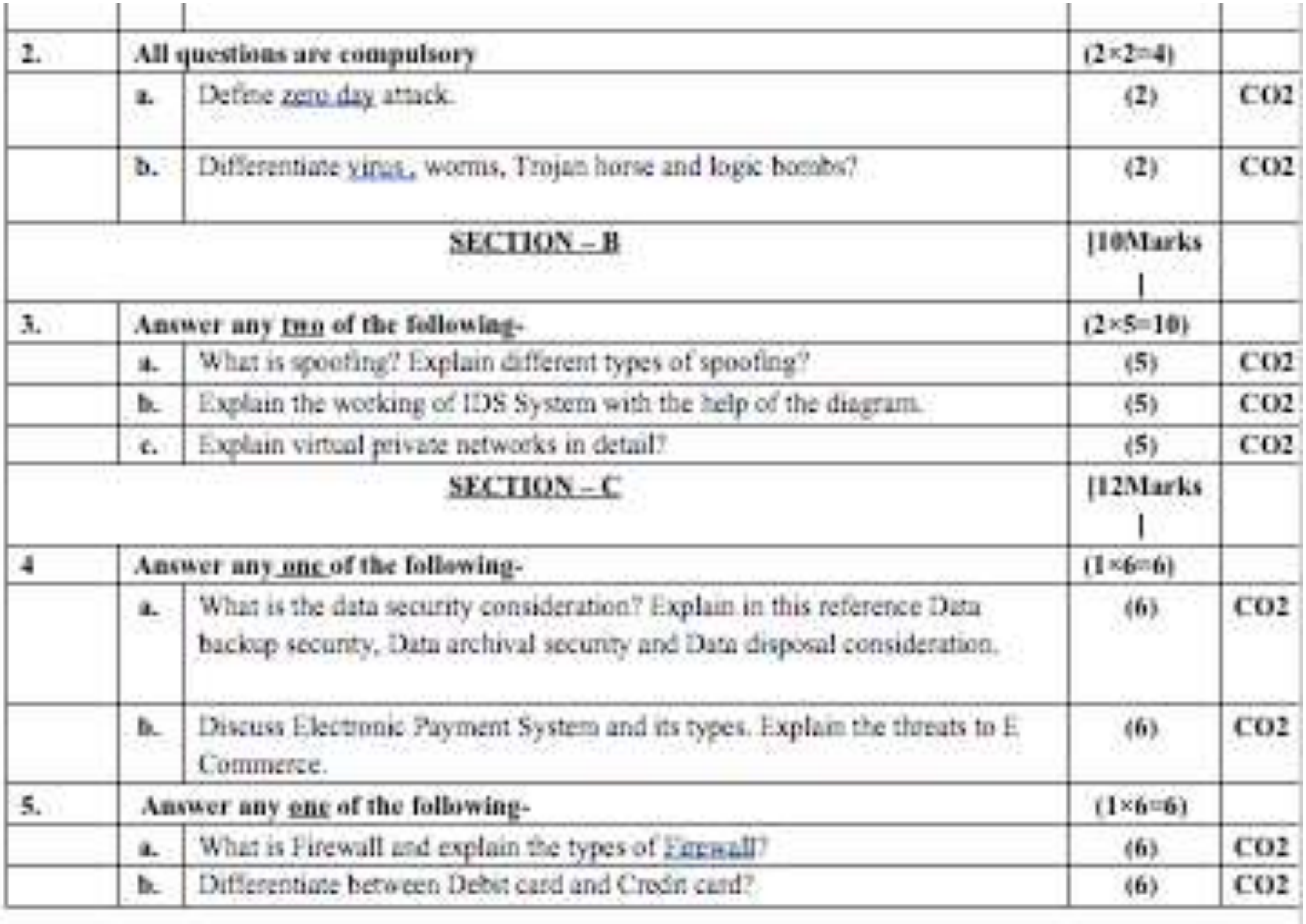
Time: 1.15Hours [SET- B] Max. Marks: 30

General Instructions:

- This Question paper consists of ......pages & ......questions,& 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.

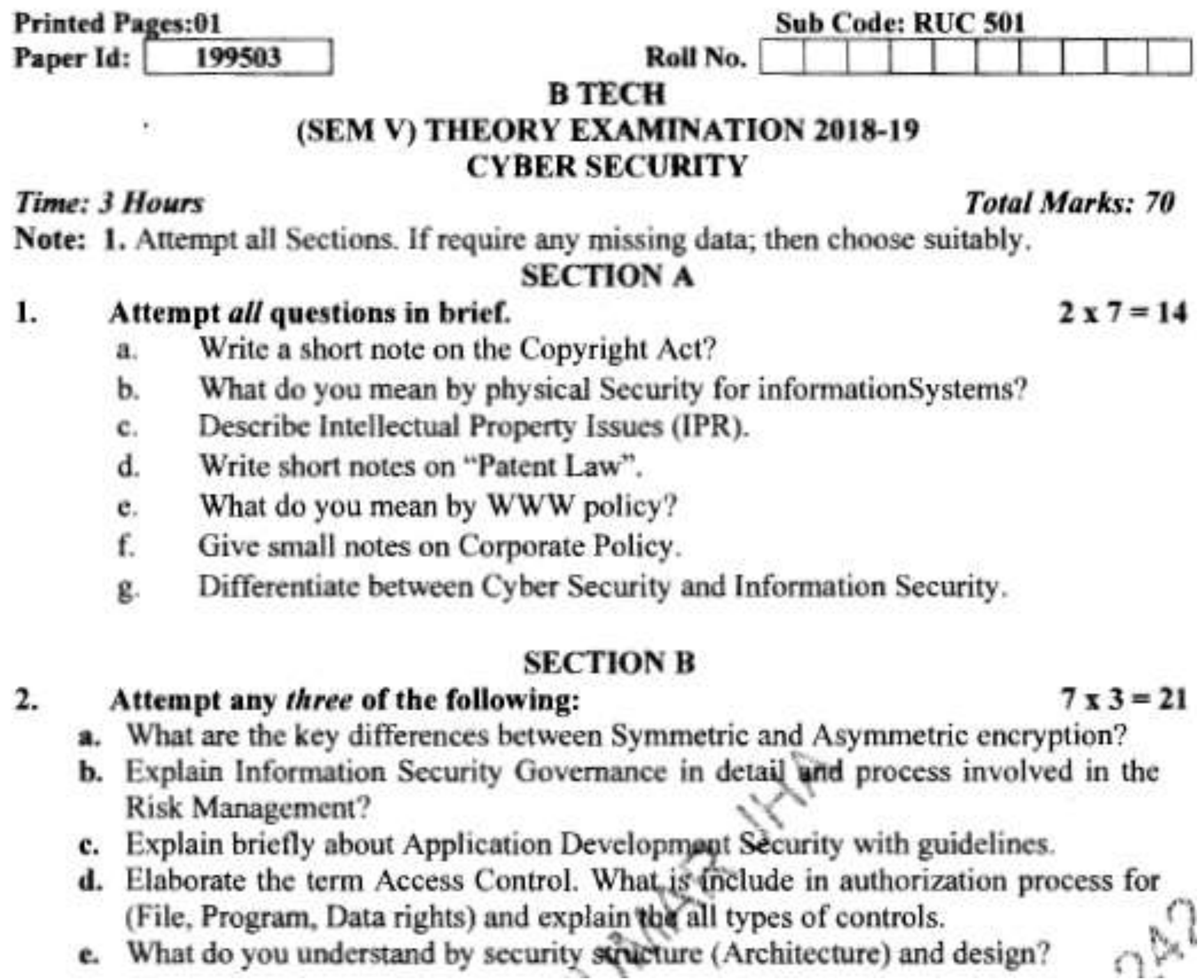
		SECTION – A	**[08Marks]**	
1.	**All questions are compulsory**		**(4×1=4)**	
	a.	1. How many layers are there in OSI model? a. 4 b. 7 c. 3 d. 8	**(1)**	**CO2**
	b.	2. Data security considerations are? a. Backups b. Archival storage c. Disposal of data d. All	**(1)**	**CO2**
	c.	3. Full form of IDS? a.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

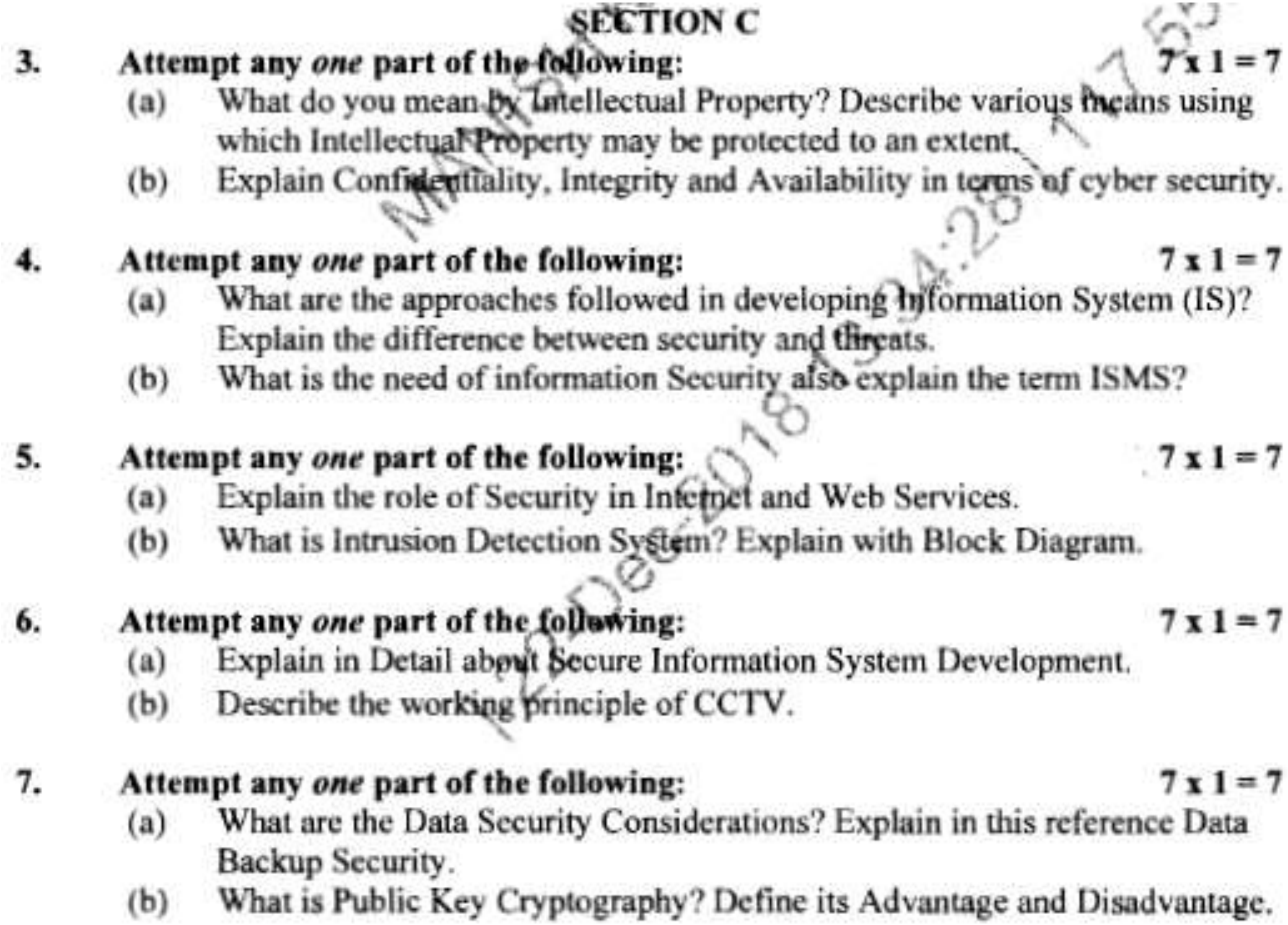
a. Write a short note on the Copyright Act?
b. What do you mean by physical Security for informationSystems?
c. Describe Intellectual Property Issues (IPR).
d. Write short notes on "Patent Law".
e. What do you mean by WWW policy?
f. Give small notes on Corporate Policy.
g. Differentiate between Cyber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

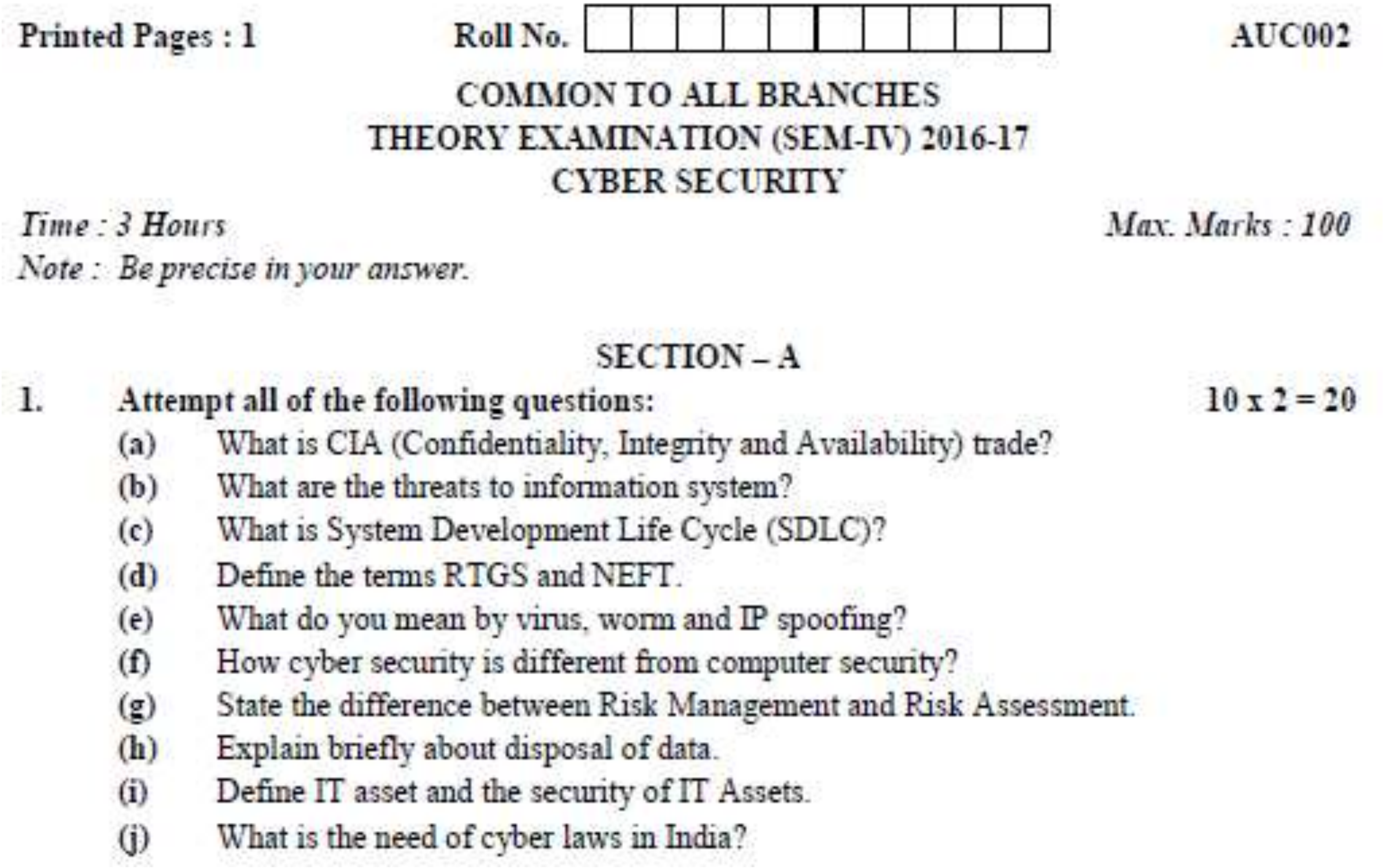
   (b) Describe the working principle of CCTV.

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?

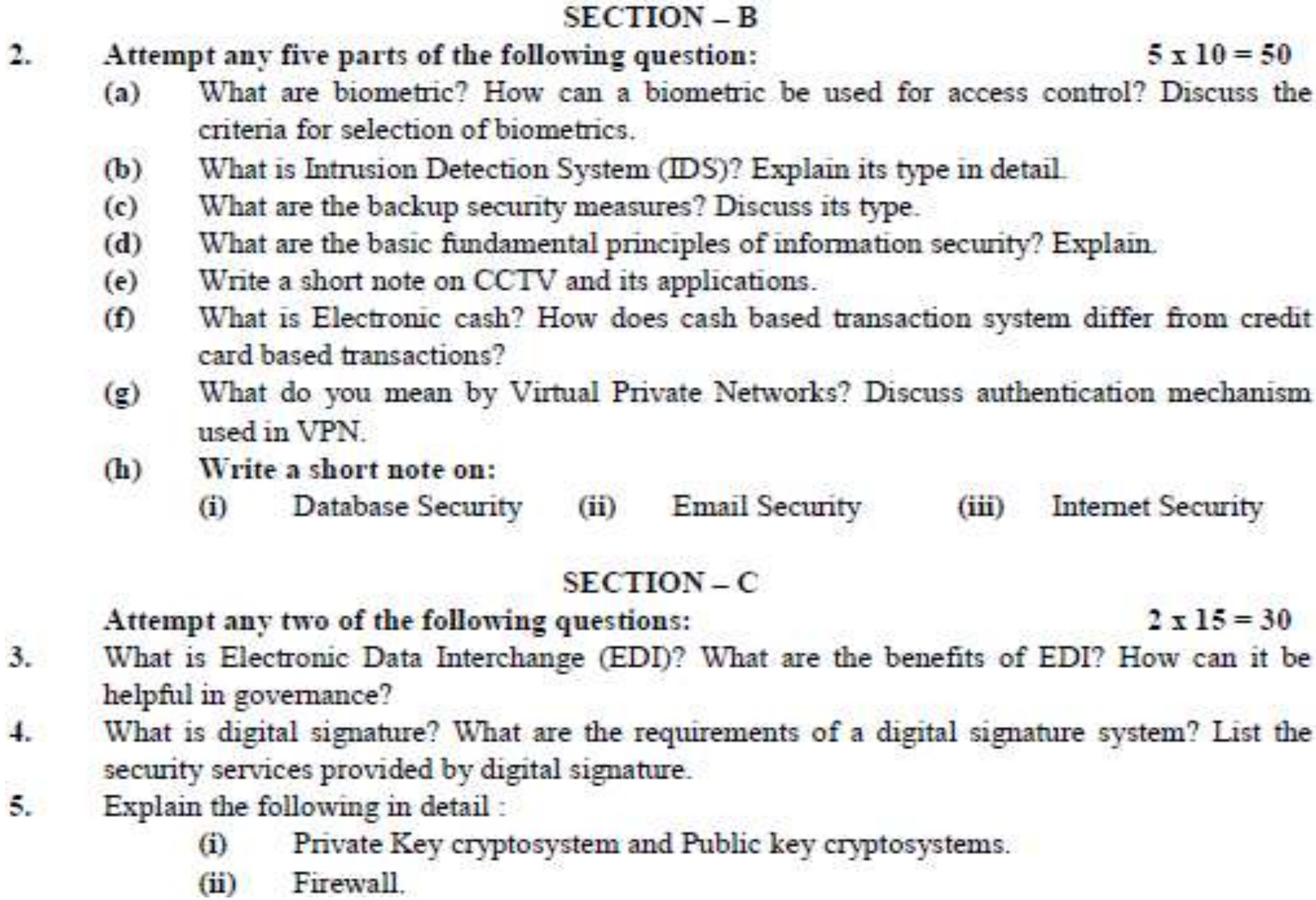
(g) State the difference between Risk Management and Risk Assessment.

(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. Explain the concept of access control mechanism
2. Explain the components of VPN.
3. Write characteristics of Stealth Viruses and polymorphic viruses
4. Explain host based IDS.
5. Differentiate symmetric and asymmetric key cryptography
6. What is digital signature?

Recap of Unit

- The major topics covered are Firewall and VPNs, Intrusion Detection Access Control, Security Threats, Security Threats to Digital Signature and Public Key Cryptography .
- Organizations today have to encounter lot of threats and risks due to the dependency on technology and Internet. Identifying and assessing the vulnerability or risk is an important exercise every organization must undergo at regular periodic intervals due to ever evolving nature of threats and attacks.
- This section discussed all the related concepts in detail along with their capabilities and the type of attacks they can mitigate. In future much more intelligent and smart approaches are also possible as the attack strategy is also changing.

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://www.cisco.com/c/dam/en_us/training-events/le21/le34/downloads/689/academy/2008/sessions/BRK-134T_VPNs_Simplified.pdf
5. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
6. https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-
7. https://www.comparitech.com/net-admin/network-intrusion-detection-tools/
8. https://onlinecourses.swayam2.ac.in/cec20_cs09

Thank You