REVA UNIVERSITY

Established as per the Section 2(f) of the UGC Act, 1956
Approved by AICTE, COA and BCI, New Delhi

Lecture 1.1

Introductory Class

School of Computing and Information Technology

Prof. Jeevaa M

OUTLINE

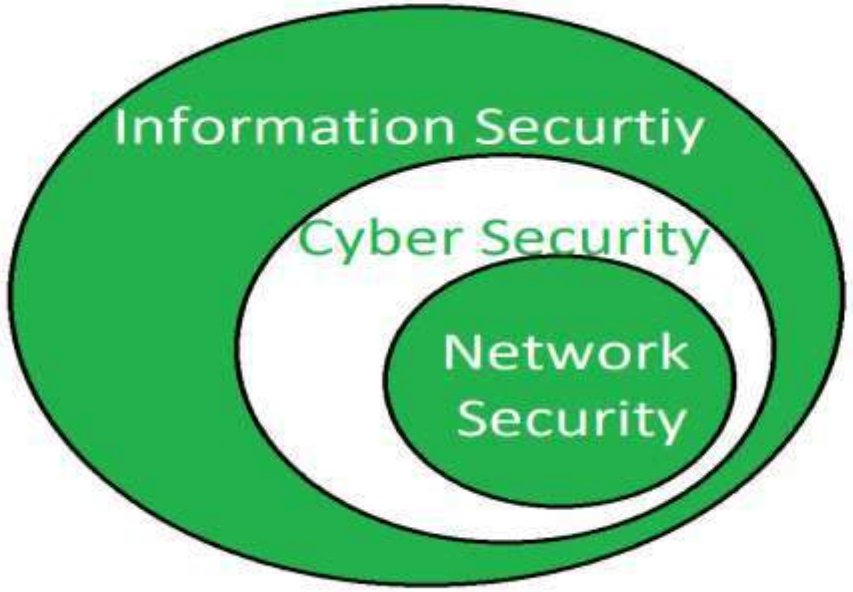
- Importance of Information and Network Security
- Course Description
- Course Objectives
- Course Contents
- Learning Resources
- Additional Resources
- Real World Applications
- Information and Network Security Related Companies in India
- Job Roles in Industry
- Type of Assignments
- Quizzes
- Pedagogy
- Marks Distribution
- Course Delivery

B22CIO602: Information and Network Security

6th Semester

INFORMATION AND NETWORK SECURITY

Security of the data and safe networks in the world which connects digitally is the most important step in today’s world for everyone.



To Study **Information And Network Security,**

1. Basic Computer Science Knowledge

Computer Architecture
Operating Systems (Windows, Linux)
Computer Networks

2. Networking Fundamentals

TCP/IP Model & OSI Model
IP Addressing & Subnetting
Routing & Switching
Network Protocols (HTTP, HTTPS, DNS, FTP, SSH)

3. Programming & Scripting

Python (Commonly Used For Security Tools)
C/C++ (For Understanding Vulnerabilities)
Bash Or Powershell (For Automation)

To Study **Information And Network Security**,

4. Cryptography Basics

Encryption & Decryption (AES, RSA, DES)

Hashing (MD5, SHA)

Digital Signatures & Certificates

5. Cybersecurity Concepts

Firewalls & Intrusion Detection Systems

Malware & Attack Types (DDos, Phishing, Ransomware)

Penetration Testing & Ethical Hacking Basics

Importance of Information and Network Security

Information Security is not just about stopping viruses, keeping hackers out. It is also about working with employees and management to make sure that everyone is aware of current threats and how they can protect their Information and Systems.

Information Security means protecting information and information systems from Unauthorized Access, Disclosure, Disruption, Modification, Perusal, Inspection, Recording or Destruction.

Computer Security is the generic name for the collection of tools designed to protect the processed and stored data and to thwart hackers.

Network Security is to protect data during their transmission.
In Connection with the Internet, the term **Internet Security** is often used.

INTRODUCTION TO INFORMATION AND NETWORK SECURITY

1. What is Information Security?

Information Security (InfoSec) refers to the protection of data from unauthorized access, modification, disclosure, or destruction. It ensures confidentiality, integrity, and availability (CIA Triad) of information.

2. What is Network Security?

Network Security focuses on protecting network infrastructure from cyber threats, ensuring secure communication and preventing unauthorized access to systems.

3. Key Objectives of Security

Confidentiality: Ensuring that sensitive data is accessible only to authorized individuals.

Integrity: Preventing unauthorized modification of data.

Availability: Ensuring data and services are accessible when needed.

Authentication & Authorization: Verifying users' identities and granting appropriate permissions.

INTRODUCTION TO INFORMATION AND NETWORK SECURITY

4. Common Threats in Information & Network Security

Malware (Viruses, Worms, Trojans, Ransomware)

Phishing & Social Engineering Attacks

Denial-of-Service (DoS) & Distributed DoS (DDoS) Attacks

Man-in-the-Middle (MitM) Attacks

SQL Injection & Cross-Site Scripting (XSS)

5. Security Measures & Tools

Firewalls: Control incoming and outgoing traffic.

Antivirus & Anti-malware: Detect and remove threats.

Encryption: Protects data using cryptographic techniques.

Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS): Monitor network traffic for threats.

Multi-Factor Authentication (MFA): Adds extra layers of security for user authentication.

INTRODUCTION TO INFORMATION AND NETWORK SECURITY

6. Importance of Cybersecurity

With the rise of cybercrime, organizations and individuals must adopt best security practices to protect their systems, data, and privacy.

Cybersecurity is essential for businesses, governments, and individuals to prevent financial loss, data breaches, and reputational damage.

Emerging Trends in Cybersecurity

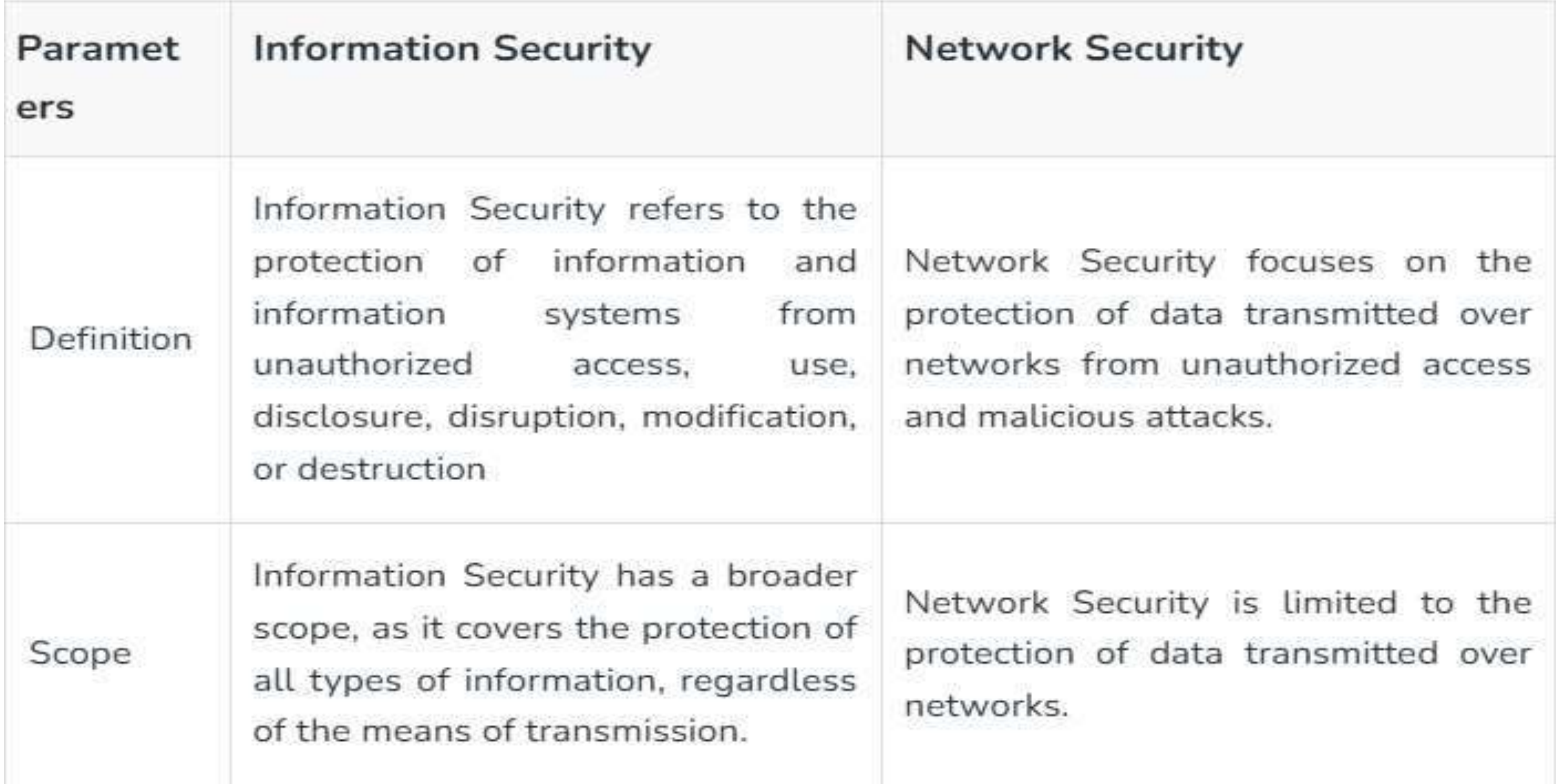
Artificial Intelligence (AI) in Security

Blockchain for Security Applications

Internet of Things (IoT) Security

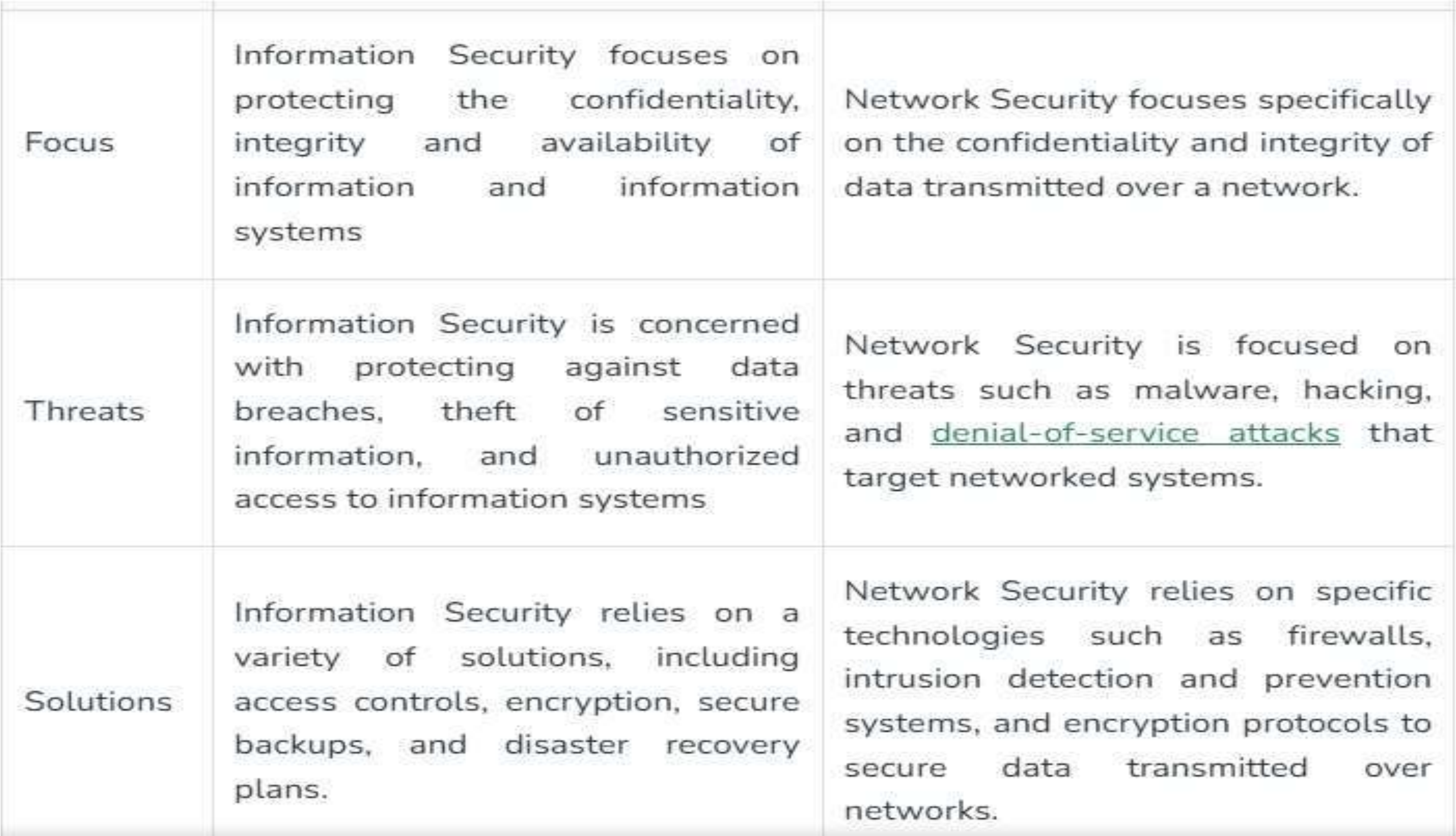
Zero Trust Architecture (ZTA)

Difference Between Information Security and Network Security



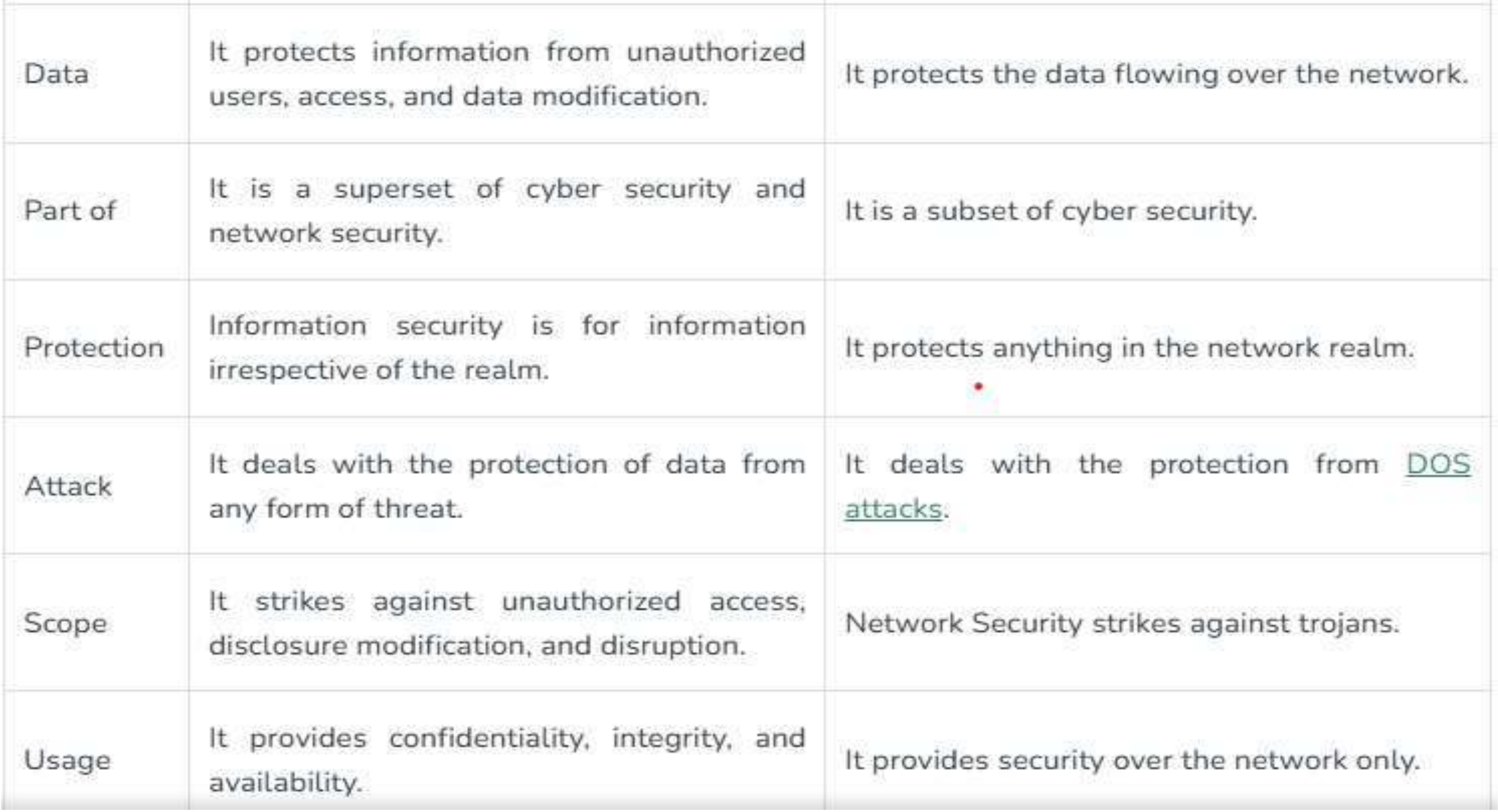
Parameters	Information Security	Network Security
Definition	Information Security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction	Network Security focuses on the protection of data transmitted over networks from unauthorized access and malicious attacks.
Scope	Information Security has a broader scope, as it covers the protection of all types of information, regardless of the means of transmission.	Network Security is limited to the protection of data transmitted over networks.

Difference Between Information Security and Network Security



Focus	Information Security focuses on protecting the confidentiality, integrity and availability of information and information systems	Network Security focuses specifically on the confidentiality and integrity of data transmitted over a network.
Threats	Information Security is concerned with protecting against data breaches, theft of sensitive information, and unauthorized access to information systems	Network Security is focused on threats such as malware, hacking, and denial-of-service attacks that target networked systems.
Solutions	Information Security relies on a variety of solutions, including access controls, encryption, secure backups, and disaster recovery plans.	Network Security relies on specific technologies such as firewalls, intrusion detection and prevention systems, and encryption protocols to secure data transmitted over networks.

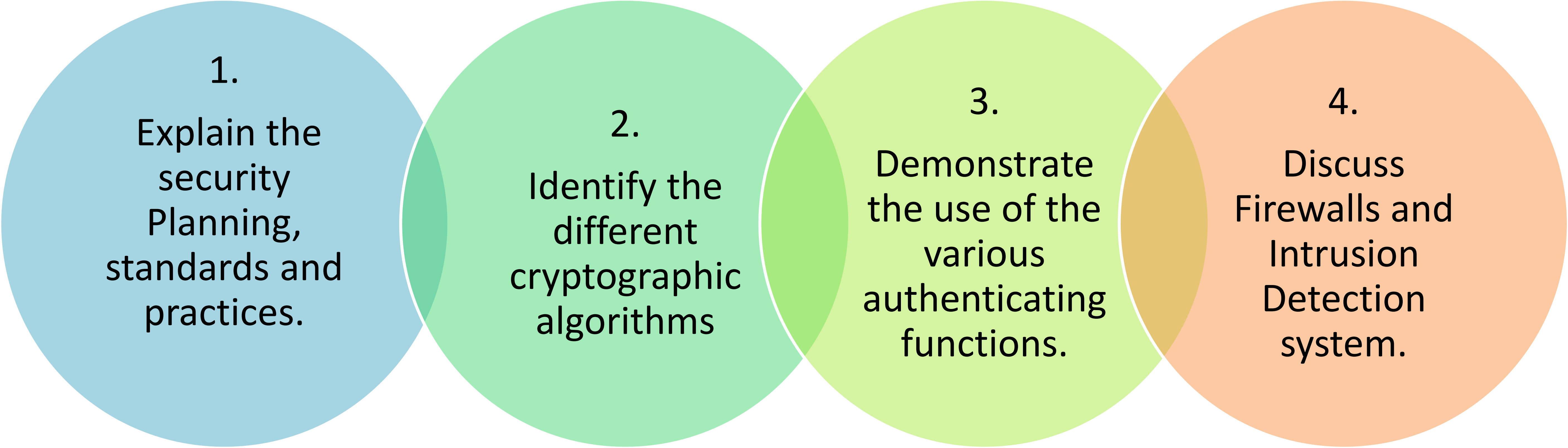
Difference Between Information Security and Network Security



Data	It protects information from unauthorized users, access, and data modification.	It protects the data flowing over the network.
Part of	It is a superset of cyber security and network security.	It is a subset of cyber security.
Protection	Information security is for information irrespective of the realm.	It protects anything in the network realm.
Attack	It deals with the protection of data from any form of threat.	It deals with the protection from DOS attacks.
Scope	It strikes against unauthorized access, disclosure modification, and disruption.	Network Security strikes against trojans.
Usage	It provides confidentiality, integrity, and availability.	It provides security over the network only.

COURSE OBJECTIVES

Objectives of this course are to :



1. Explain the security Planning, standards and practices.

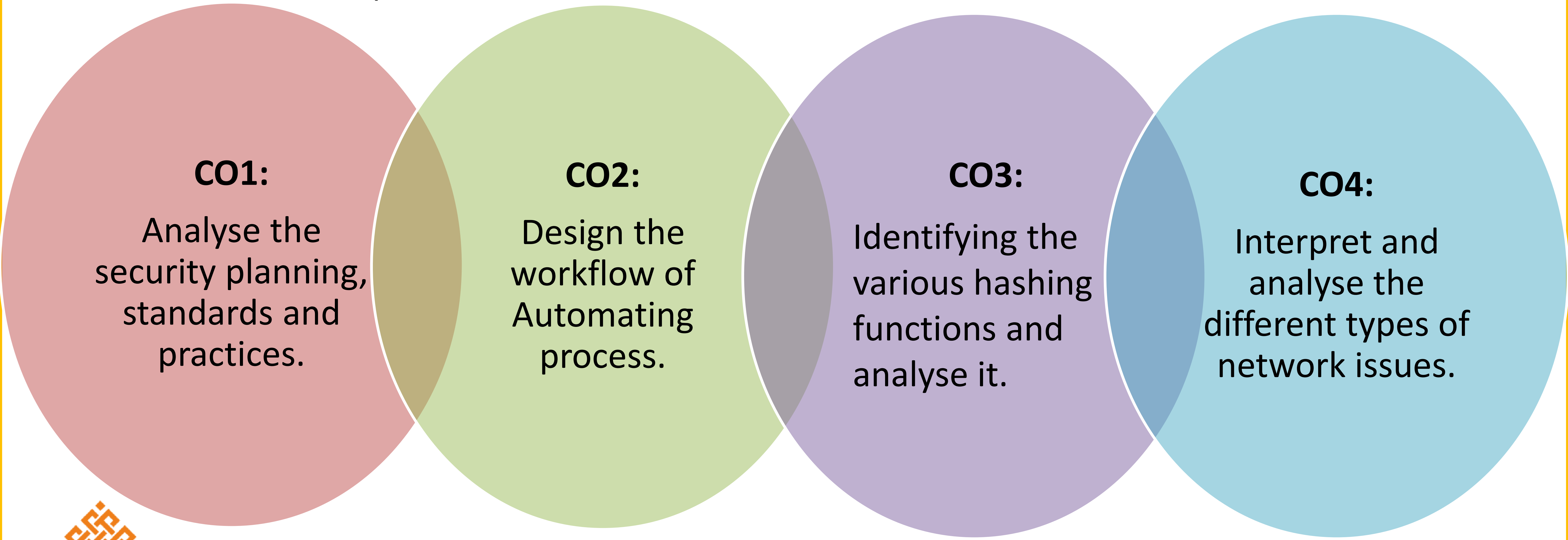
2. Identify the different cryptographic algorithms

3. Demonstrate the use of the various authenticating functions.

4. Discuss Firewalls and Intrusion Detection system.

COURSE OUTCOMES

On successful completion of this course; student shall be able to:



CO1:

Analyse the security planning, standards and practices.

CO2:

Design the workflow of Automating process.

CO3:

Identifying the various hashing functions and analyse it.

CO4:

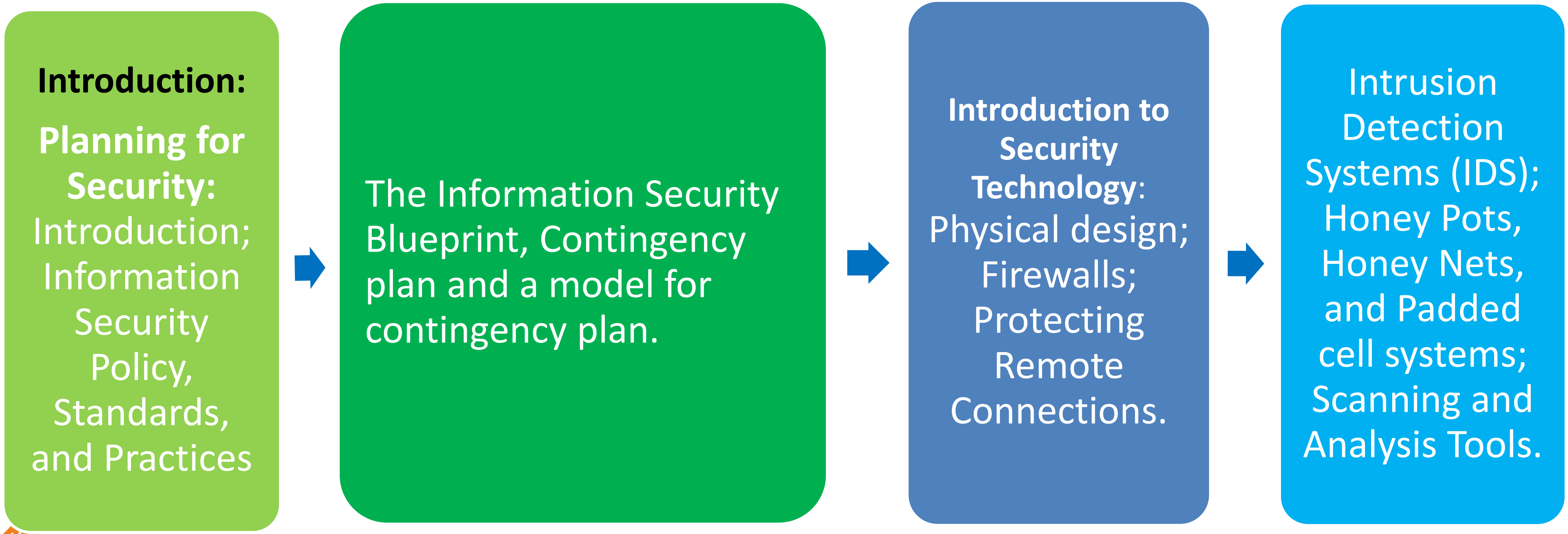
Interpret and analyse the different types of network issues.

Introduction Class

Course Contents

COURSE CONTENTS

UNIT – 1:



Introduction:

Planning for Security: Introduction; Information Security Policy, Standards, and Practices

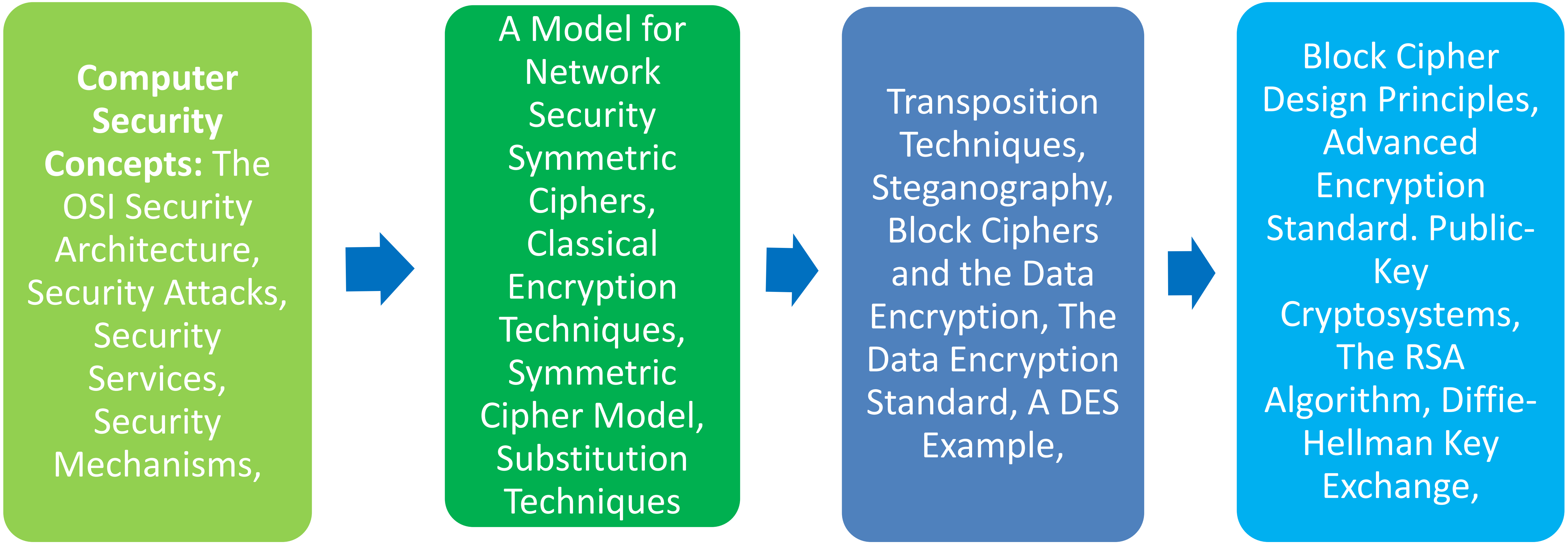
The Information Security Blueprint, Contingency plan and a model for contingency plan.

Introduction to Security Technology: Physical design; Firewalls; Protecting Remote Connections.

Intrusion Detection Systems (IDS); Honey Pots, Honey Nets, and Padded cell systems; Scanning and Analysis Tools.

COURSE CONTENTS

UNIT – 2:



Computer Security Concepts: The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms,

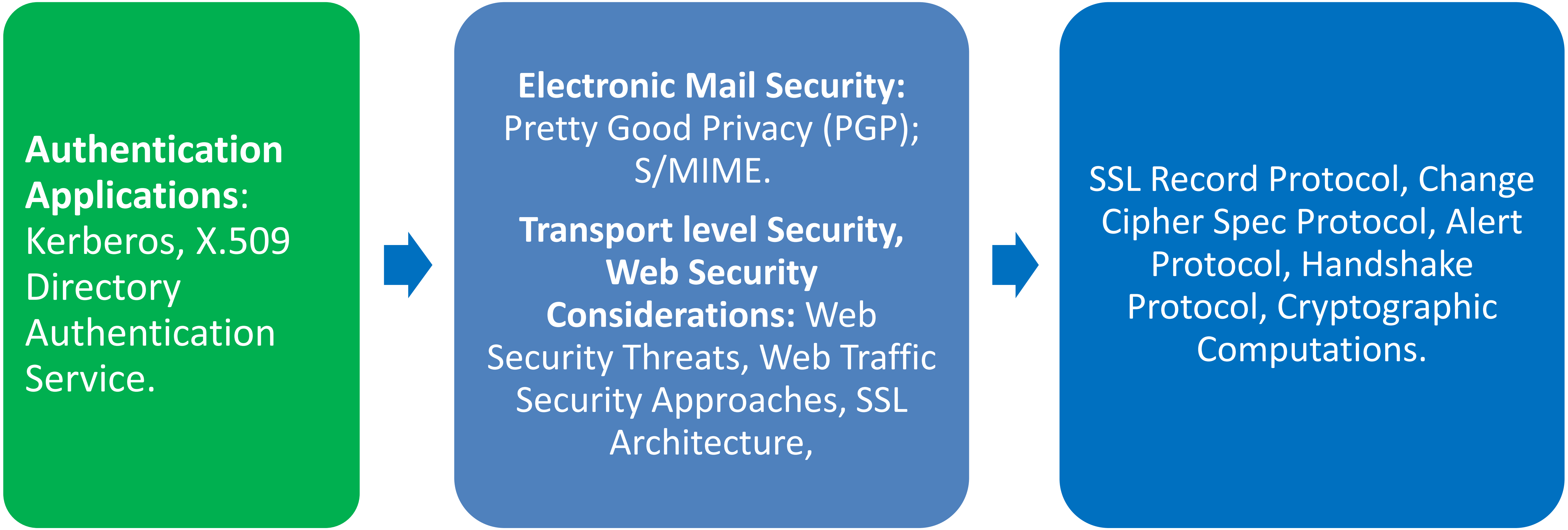
A Model for Network Security Symmetric Ciphers, Classical Encryption Techniques, Symmetric Cipher Model, Substitution Techniques

Transposition Techniques, Steganography, Block Ciphers and the Data Encryption, The Data Encryption Standard, A DES Example,

Block Cipher Design Principles, Advanced Encryption Standard. Public-Key Cryptosystems, The RSA Algorithm, Diffie-Hellman Key Exchange,

COURSE CONTENTS

UNIT – 3:



Authentication Applications: Kerberos, X.509 Directory Authentication Service.

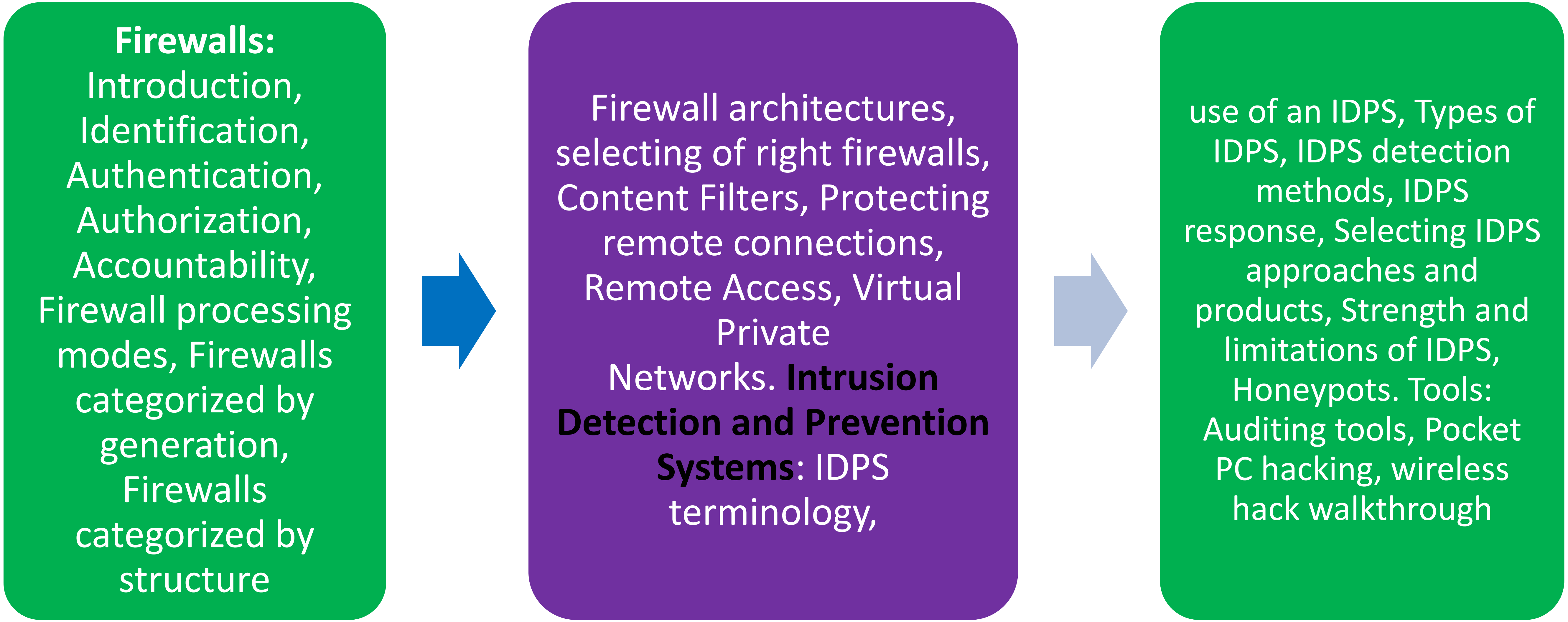
Electronic Mail Security: Pretty Good Privacy (PGP); S/MIME.

Transport level Security, Web Security Considerations: Web Security Threats, Web Traffic Security Approaches, SSL Architecture,

SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, Handshake Protocol, Cryptographic Computations.

COURSE CONTENTS

UNIT – 4:



Firewalls: Introduction, Identification, Authentication, Authorization, Accountability, Firewall processing modes, Firewalls categorized by generation, Firewalls categorized by structure

Firewall architectures, selecting of right firewalls, Content Filters, Protecting remote connections, Remote Access, Virtual Private Networks. **Intrusion Detection and Prevention Systems**: IDPS terminology,

use of an IDPS, Types of IDPS, IDPS detection methods, IDPS response, Selecting IDPS approaches and products, Strength and limitations of IDPS, Honeypots. Tools: Auditing tools, Pocket PC hacking, wireless hack walkthrough

Introduction Class

Learning Resources

LEARNING RESOURCES

Text books:

1. William Stallings, Cryptography and Network Security, Pearson Publications, 6th edition,20l4.

2. M. E. Whitman and Herbert J. Mattored, Principles of Information Security, Information Security Professional, 4thedition, 20l4.

TEXT BOOKS

Behrouz A. Forouzan, Cryptography and Network Security, Tata McGraw-Hill, 2007.

Joseph MiggaKizza, Guide to Computer Security, Springer Science & Media Inc., 3rd edition, 20l5

DISCUSSION

5 MINUTES