CS 413
Information Security

Course Instructor

Naushad Siddiqui

Head of IT Audit, Sui Southern Gas Company

Visiting Faculty, NED University
Director & Faculty Member, ISACA Karachi

CS413 Information Security

Fall 2020

Week 01

Agenda

- Introduction
- Course Information
- Information Security Basics
- Aspects of Security
- Security Attacks
- Security Services
- Security Mechanism
- Security Techniques

Course Information

Course Information

Course Code & Title

- Code: CS 413
- Title: Information Security

Course Objectives

The objectives of this course are as follows:

- To understand the fundamentals of information security
- To understand the purpose and implementation of CIA triad
- To be able to solve different cryptographic techniques
- To understand the purpose of public key cryptosystems

Course Information

Indicative Learning Strategy

The course will be based on the following teaching and learning activities:

- Lectures covering the theoretical concepts using Power Point presentations
- Review questions and class exercises, during the lectures
- Case Studies
- Class Discussions & Presentations

Indicative References / Learning Materials:

Cryptography and Network Security by Behrouz A Frouzon

Reference Material:
Cryptography and Network Security by William Stallings
Cryptography and Network Security by S. Boss

References of Relevant Standards / Organizations:

- Information System Audit and Control Association www.isaca.org
- National Institute of Standards and Technology www.nist.gov

Course Information

Assessment Criteria & Schedule

Exams:

Material for exams will be taken from a variety of sources, including assigned readings and research, homework assignments, and class lectures.

Assessment Strategy:

Quizzes & Class Exercises:	10%	announced / surprised, during class
Assignments & Presentations:	10%	throughout the semester
Midterm Exam:	20%	9th week
Final Exam (theory):	60%	as per schedule announced by UIT

Course Information

Topics Coverage

Week 01	Security Terminologies, Security goals, CIA Triade, Security Attacks, Active and Passive attacks, Security Services, Security Mechanism, Relation between security goals, services and mechanism
Week 02	Security Mechanism Techniques: Cryptography & Steganography, Encryption, Decryption, Symmetric Key Encipherment, Asymmetric Key Encipherment, Examples of encryption and decryption, Cryptanalysis, Caesar Cipher
Week 03	Finding Coprime, concept of GCD, Multiplicative Inverse, Modulus and its significance in cryptography, Affine Cipher, Affine Cipher Encryption, Affine Cipher Decryption
Week 04	Playfair Cipher, Rules for Encryption, Rules for Decryption, How to encrypt and decrypt, Research and different variants of Playfair Cipher
Week 05	Vigenere Cipher, Vigenere Tableau, Process of encryption and decryption, Row transposition technique, Hill Cipher, Inverse of matrix, Utilizing additive and multiplicative inverse, Finding inverse key
Week 06	Hill cipher, Process of encryption and decryption, Encryption of plain text and converting it back using inverse key, Performing different examples of Hill Cipher, Enigma Machine
Week 07	Modern Block Ciphers, Components of modern block ciphers, Introduction of Data Encryption Standard (DES), Tables and Key generation process, Process of Encryption and decryption
Week 08	DES in detail, scheme of DES, Key structure of DES, Structure of DES's Round, Role of left circular shift, Permuted choice and generation of Key, Role of expansion permutation and logic behind its construction, Permutation tables

Course Information

Topics Coverage (cont…)

Week 09	Structure of S-boxes of DES and how data is traversed through it, Role of XOR, Confusion and Diffusion, Solving one single round of DES using subkey and input data, How to calculate Avalanche effect of any encryption technique
Week 10	Public Key Crypto system, Difference between symmetric key and asymmetric cryptography, Rivest, Shamir, Adleman (RSA) technique, Examples related to RSA
Week 11	Key exchange mechanism, Diffie Hellman technique, Examples of key exchange for symmetric techniques, El Gamal algorithm and how it is similar to Diffie Hellman
Week 12	Hash algorithm, Digital Signatures
Week 13	Advance Topics in Security: Security at network layer, IPSEC, Security at transport layer, SSL, TLS, Database security & SQL injections, Software security, Risk assessment, Policy formation
Week 14	Significance of compression, LZW Technique, Performing compression using LZW, Introduction to Kerberos, its purpose and working
Week 15	Information Security Ethics, Responsibilities of security professionals, CARE framework Different case studies of professional violation and responsibilities
Week 16	Course Revision Presentations, Makeup classes

Information Security Basics

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—*The Art of War,* Sun Tzu

Knowledge Check

Information Security is

A. Protecting information from inappropriate access
B. Protecting information from inappropriate use
C. The responsibility of everyone
D. All of the above

D. All of the above

Introduction to Information Security

What is Information

Information is **processed data** or **knowledge, proprietary** to a person or an organization, which assigns **value** to it

Information can be:

- Created & Owned (it is an **asset**)
- Processed & Stored
- Transmitted / Communicated
- Modified or corrupted
- Destroyed or lost
- Used (for proper or improper purposes)
- Shared or disclosed
- Stolen

Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected.

Introduction to Information Security (2)

Information Exists in Many Forms:

- Printed or written on paper
- Stored electronically
- Transmitted by post or electronic means
- Visual *e.g.* videos, diagrams
- Published on the Web
- Verbal/aural *e.g.* conversations, phone calls
- Intangible *e.g.* knowledge, experience, expertise, ideas

‘Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected’

Introduction to Information Security (3)

What is Information Security

- Information security is what keeps information assets ‘free of danger’ (protected, safe from harm)

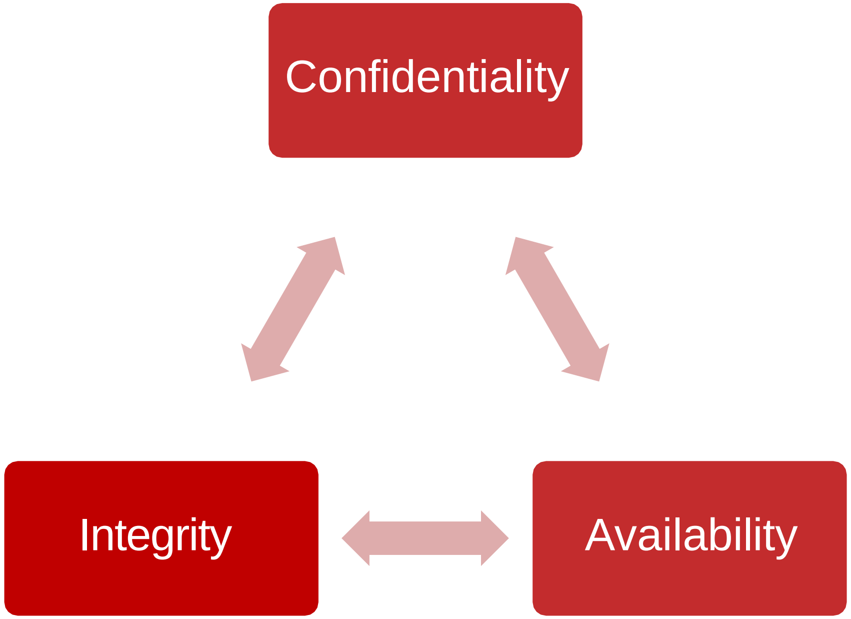
- It is not something you buy, it is something you do
  - It’s a *process* not a *product*

- It is achieved using a combination of suitable strategies and approaches:
  - Determining the risks to information assets and treating them accordingly
  - Protecting **CIA** (**C**onfidentiality, **I**ntegrity and **A**vailability)
  - Avoiding, preventing, detecting and recovering from incidents
  - Securing people, processes *and* technology … not just IT!

Introduction to Information Security (4)

Security Goals - The CIA Triad

- Confidentiality
- Integrity
- Availability

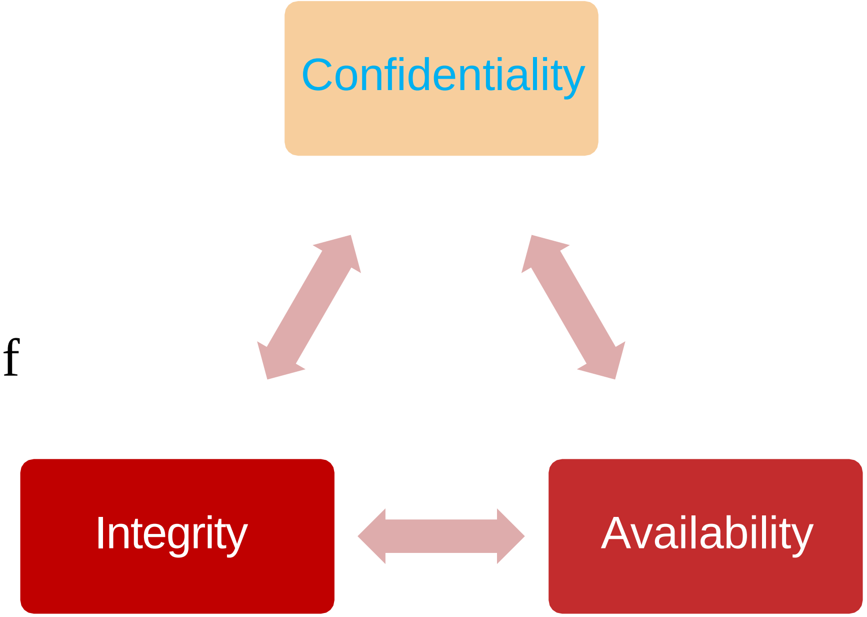


Introduction to Information Security (5)

The CIA Triad

- **C**onfidentiality
  - Confidentiality of information ensures that only those with sufficient privileges may access certain information
  - Prevent unauthorized disclosure of information
  - Applies to storage, transmission and processing of information
  - Control Examples:

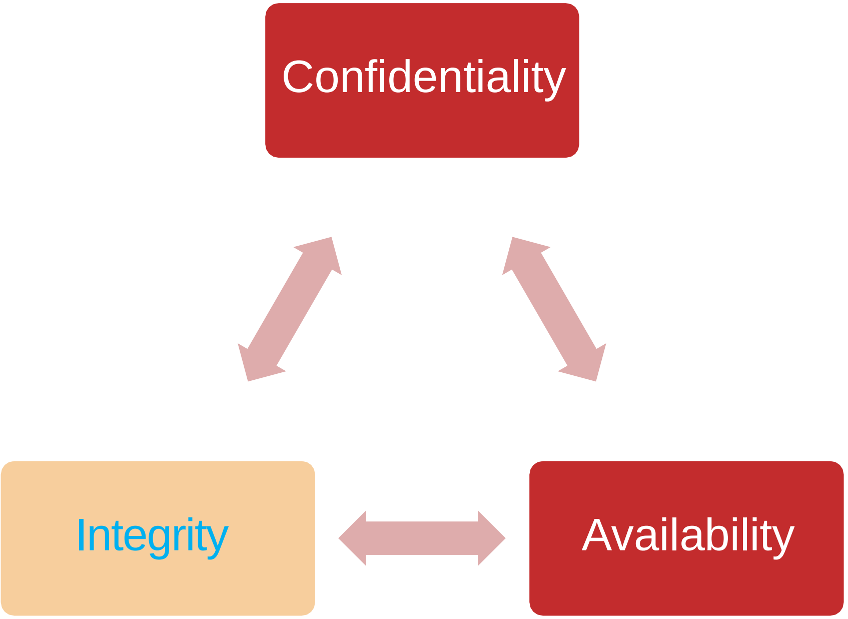
Authentication, access controls, and cryptography



Introduction to Information Security (6)

The CIA Triad

- Integrity
  - Integrity is the quality or state of being whole, complete, and uncorrupted
  - Used to verify that data has not been modified, tampered with, or corrupted
  - The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state
  - Control Examples: Hashing

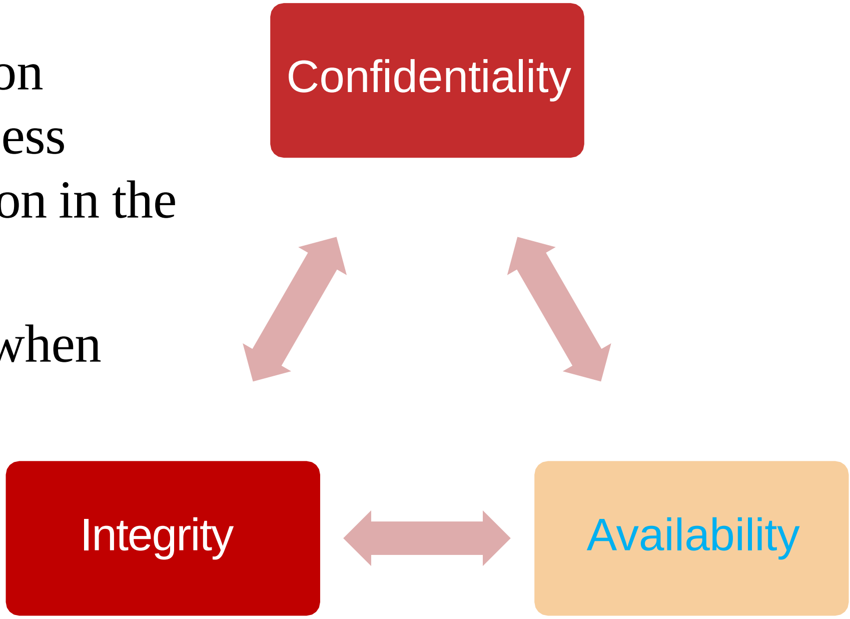


Introduction to Information Security (7)

The CIA Triad

- Availability
  - Availability is making information accessible to authorized user access without interference or obstruction in the required format
  - Ensure information is available when needed.
  - Control Examples:

Redundancy and backups

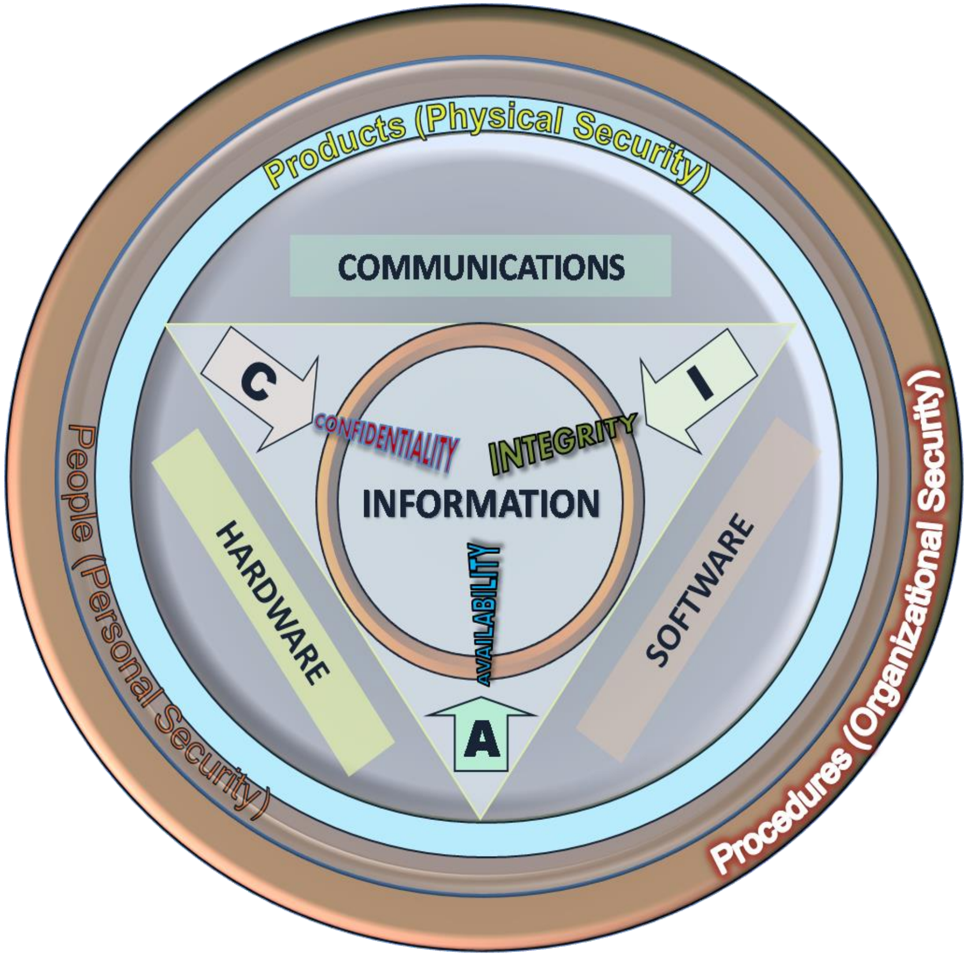


- relationship among these three

- all 3 Equally Important & Intertwined

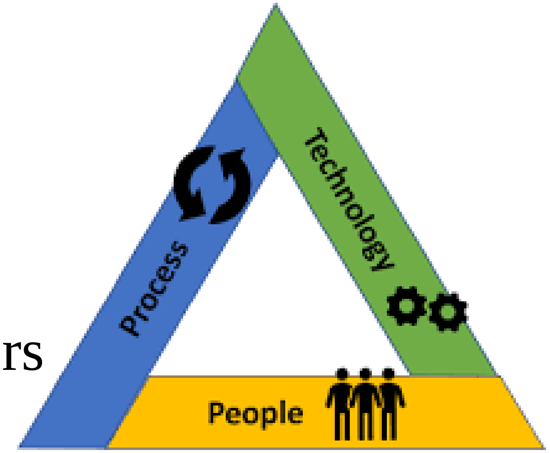
Introduction to Information Security (8)

The CIA Triad


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
A
HARDWARE
SOFTWARE
People (Personal Security)
Procedures (Organizational Security)

Introduction to Information Security (9)

Information Security Elements



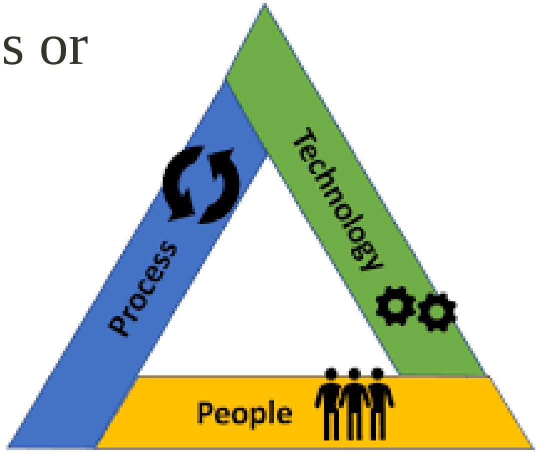
People who use or have an interest in *information security* include:

- Shareholders / owners
- Management & staff
- Customers / clients, suppliers & business partners
- Service providers, contractors, consultants & advisors
- Authorities, regulators and agencies

Our biggest **THREAT** arise from people (social engineers, unethical competitors, hackers, fraudsters, careless workers, bugs, flaws …), yet our biggest **ASSET** is our people (*e.g.* security-aware employees who spot trouble early)

Introduction to Information Security (10)

Information Security Elements



Processes are work practices or workflows, the steps or activities needed to accomplish business objectives.

- Processes are described in procedures.
- Virtually all business processes involve and/or depend on information, making it a critical business asset.

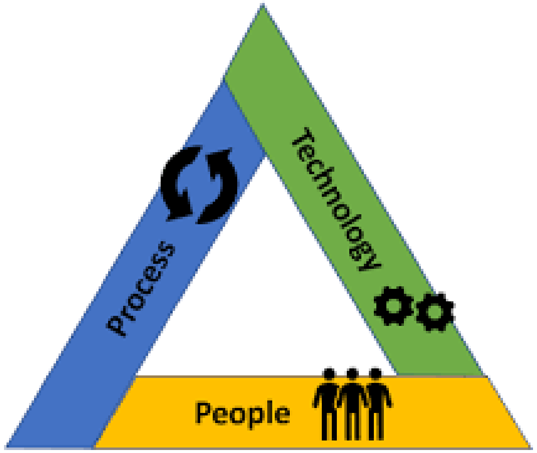
Information security policies and procedures define how we secure information appropriately and repeatedly.

Introduction to Information Security (11)

Information Security Elements

Technology

- Cabling, data/voice networks and equipment
- Telecommunications services (PABX, VoIP, ISDN, Videocon)
- Phones, cellphones, PDAs
- Computer servers, desktops and associated data storage devices (disks, tapes)
- Operating system and application software



Security Technologies

- Locks, barriers, card-access systems, CCTV

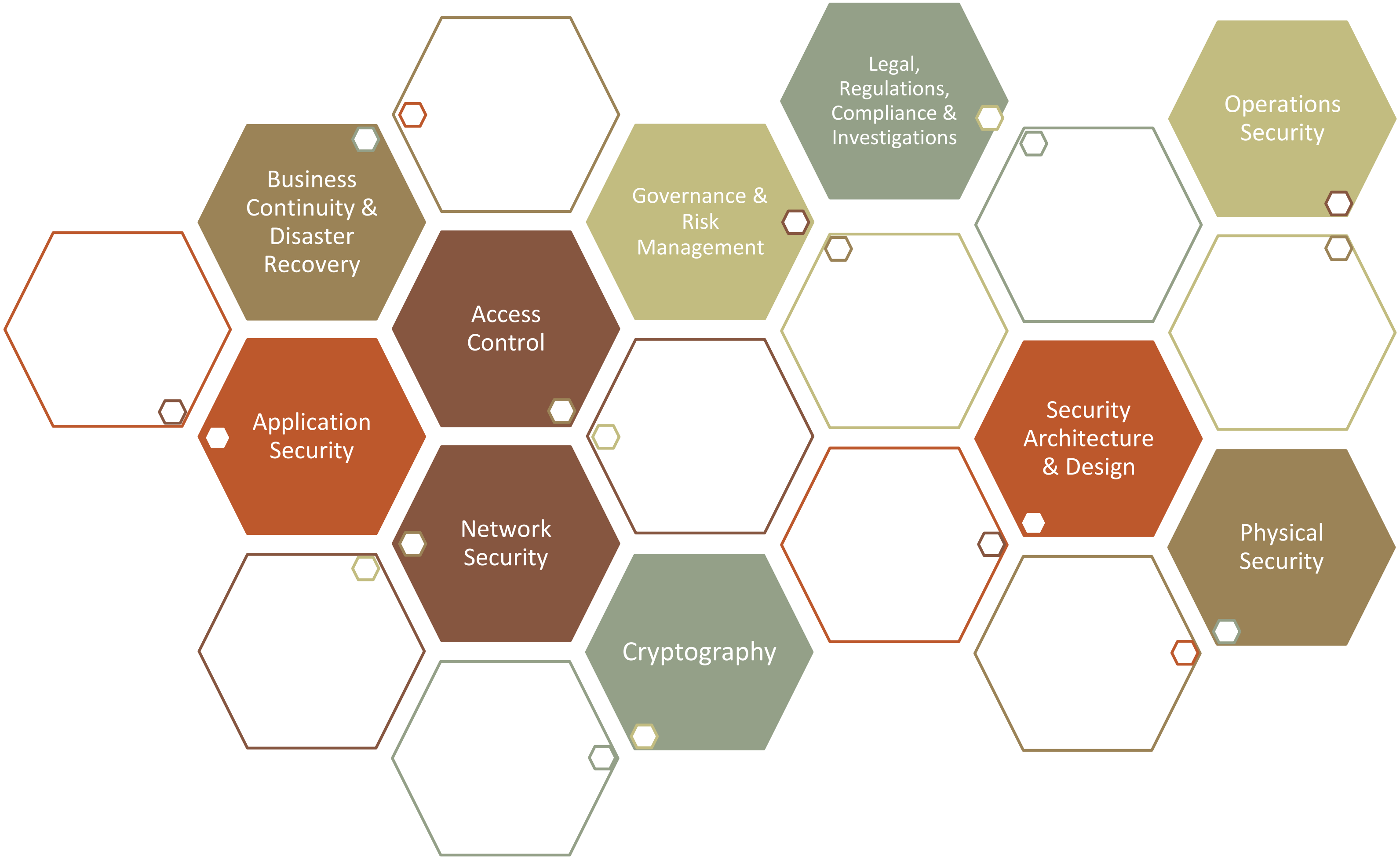
Introduction to Information Security (12)

Information Security & Cybersecurity

- The terms ‘Cybersecurity’ and ‘Information Security’ are often used interchangeably, but in reality, cybersecurity is a part of information security.
- **Information security** deals with information, regardless of its format—it encompasses paper documents, digital and intellectual property in people’s minds, and verbal or visual communications.
- **Cybersecurity**, on the other hand, is concerned with *protecting digital assets*—everything encompassed within network hardware, software and information that is processed, stored within isolated systems or transported by internetworked information environments.
- Cybersecurity usually relates to an entity initiating threats due to the existence of a global cyberspace (i.e., Internet).
- Cybersecurity **does not include** natural hazards, personal mistakes or physical security.

Introduction to Information Security (13)

Many Areas of Information Security


Legal, Regulations, Compliance & Investigations
Operations Security
Business Continuity & Disaster Recovery
Governance & Risk Management
Access Control
Application Security
Security Architecture & Design
Network Security
Physical Security
Cryptography

Knowledge Check

In Information Security, what does CIA stand for?

A. Cybersecurity, Internet, Accessibility
B. Central Intelligence Agency
C. Cybersecurity Investigation Agency
D. Confidentiality, Integrity, Availability

D. Confidentiality, Integrity, Availability

Knowledge Check

Risk, as it applies to information technology, is not associated with which one or more of the following items:

A. People

B. Practices

C. Processes

B. Practices

Knowledge Check

Which one of these represents the property of keeping an organization information accurate, without error, and without unauthorized modification?

A. Availability
B. Integrity
C. Confidentiality
D. Accountability

B. Integrity

Knowledge Check

Maria is buying books from an online retail site, and she finds that she is able to change the price of a book from Rs 109.99 to Rs 10.99.

Which part of the CIA triad has been broken?

A. Availability

B. Integrity

C. Confidentiality

D. None of the above

B. Integrity

Knowledge Check

You are working on college application online, when the admissions website crashes. You are unable to turn in your assignment on time.

Which part of the CIA triad has been broken?

A. Availability
B. Integrity
C. Confidentiality
D. None of the above

A. Availability

Knowledge Check

Ali gets his phone bill in the mail. The bill was supposed to be for Rs. 1000, but the mail person spilled water on the bill, smearing the ink. The bill now asks for Rs. 100.

Which part of the CIA triad has been broken?

A. Availability

B. Integrity

C. Confidentiality

D. None of the above

B. Integrity

Knowledge Check

Kim takes her college admissions test and is waiting to get her results by email. By accident, Kim's results are sent to Karen.

Which part of the CIA triad has been broken?

A. Availability
B. Integrity
C. Confidentiality
D. None of the above

C. Confidentiality

Aspects of Security

Aspects of Security

Consider 3 aspects of information security:

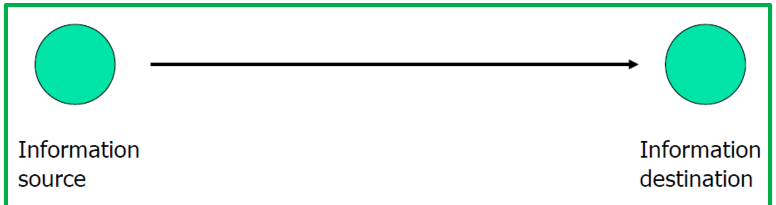
- **Security Attack**
- **Security Service**
- **Security Mechanism**

  - ***Security Attack:*** Any action that compromises the security of information owned by an organization.
  - ***Security Service:*** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The service is intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.
  - ***Security Mechanism:*** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

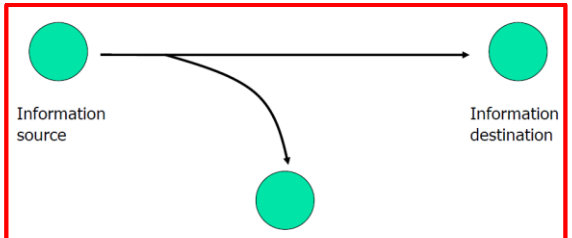
Security Attacks

- Any action that compromises the security of information owned by an organization
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- Often threat & attack used to mean same thing
- There is a wide range of security attacks
- They threaten the Confidentiality, Integrity and Availability of information
- Generic types of attacks may be
  - passive
  - active

Security Attacks (2)

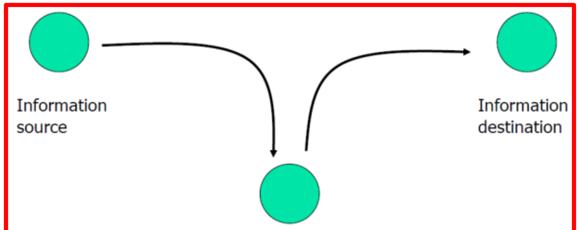


Normal Flow



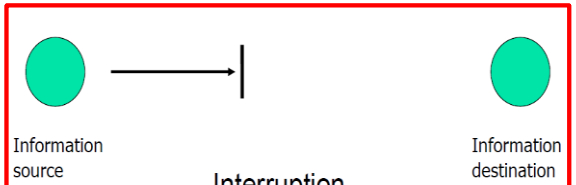
Interception

- Attack on **confidentiality**



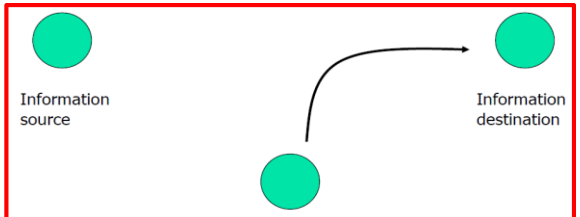
Modification

- Attack on **integrity**



Interruption

- Attack on **availability**

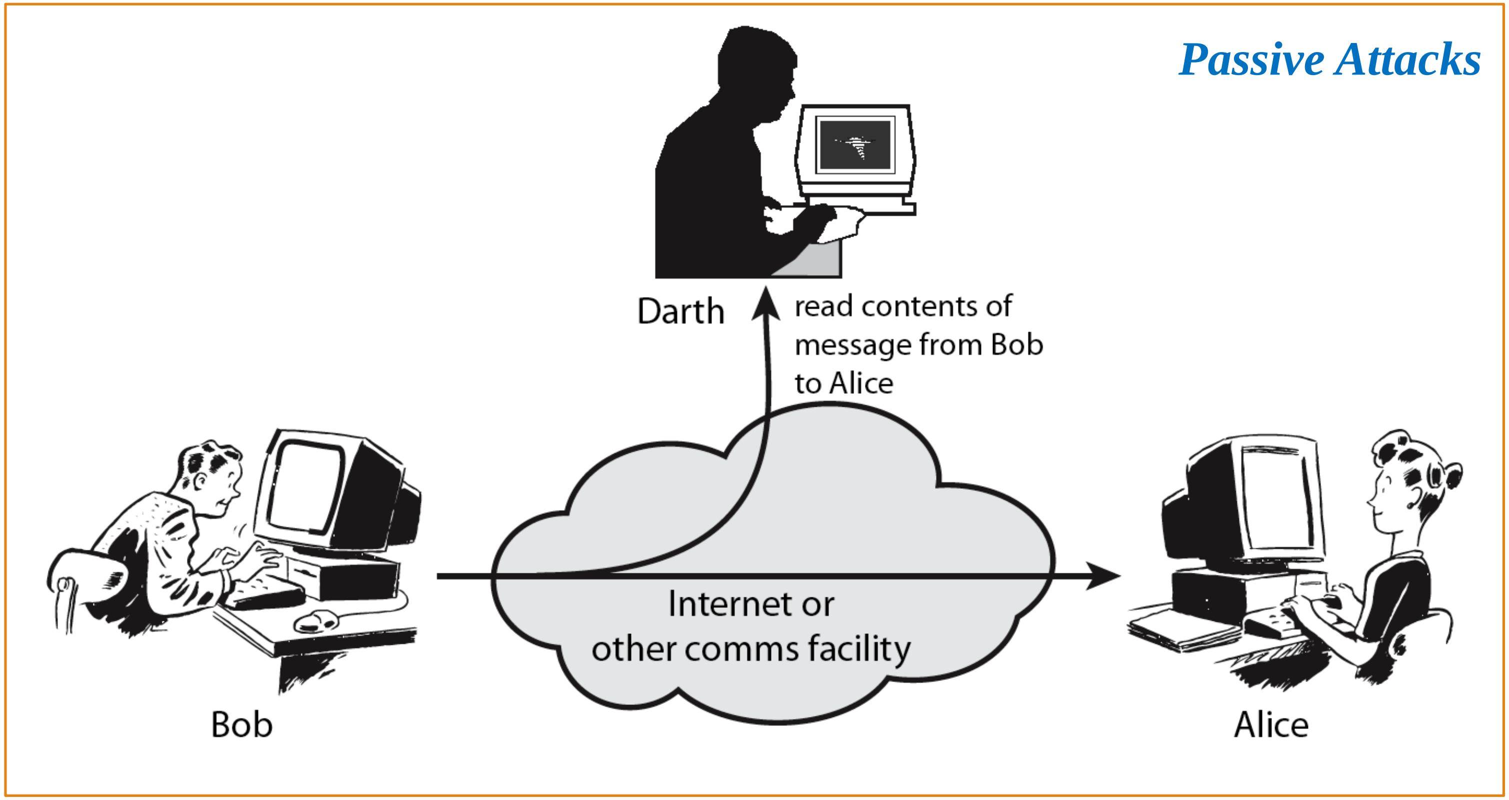


Fabrication

- Attack on **authenticity**

Security Attacks (3)

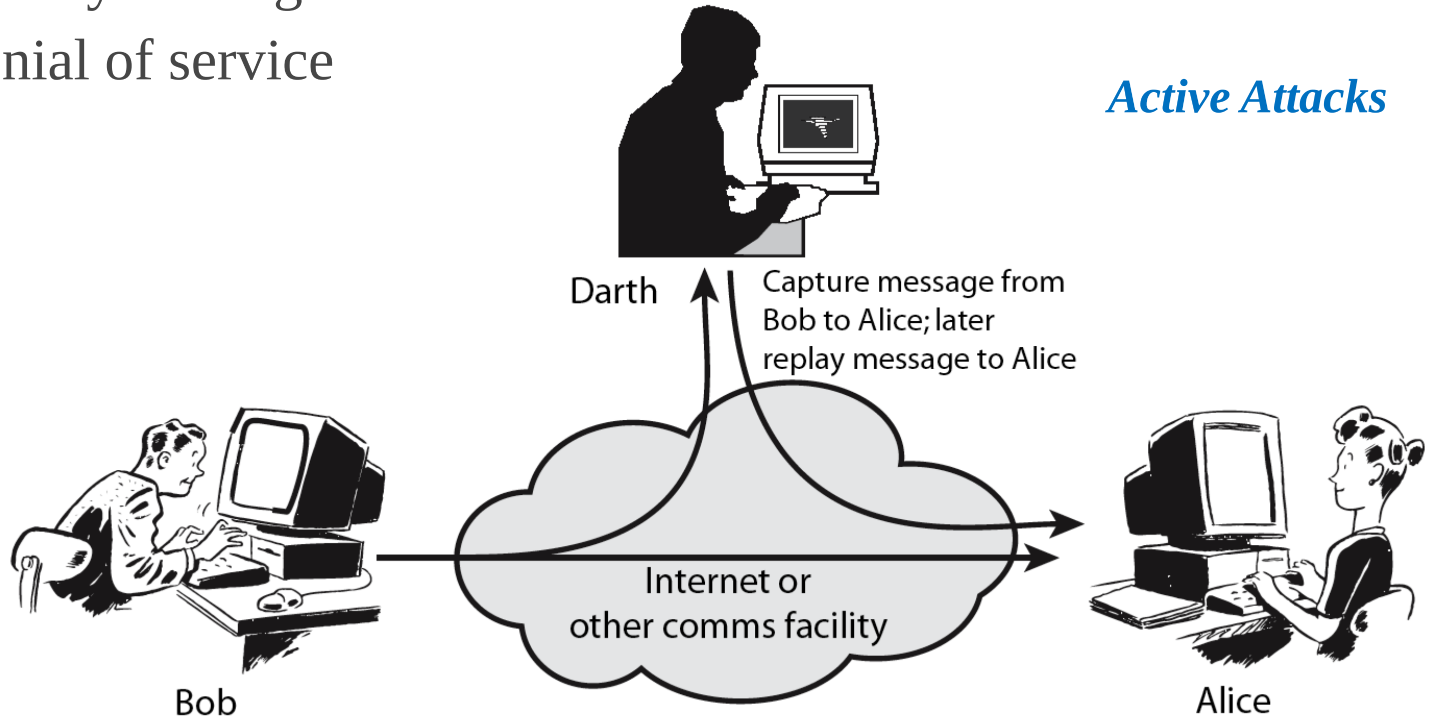
- ***Passive Attacks*** - eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows


Passive Attacks
Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Security Attacks (4)

- ***Active Attacks** - modification of data stream to:*
  - masquerade (concealment) of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

Active Attacks


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Security Attacks (5)

Threatening Confidentiality

- Snooping
- Traffic Analysis

Threatening Integrity

- Modification
- Masquerading
- Replaying
- Repudiation

Threatening Availability

- Denial of Service

Security Service

- Enhance security of data processing systems and information transfers of an organization
- Intended to counter security attacks
- Using one or more security mechanisms
- Often replicates functions normally associated with physical documents which
  - have signatures, dates
  - need protection from disclosure, tampering, or destruction
  - be notarized or witnessed
  - be recorded or licensed

Security Service (2)

- **Authentication**
  - assurance that the communicating entity is the one claimed
  - verifies a user’s identification via the process of logging into a system.
  - provides proof that a user possesses the identity that he or she claims
- **Access Control**
  - prevention of the unauthorized use of a resource
  - provides assurance that the user (a person or a computer) has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset
- **Non-Repudiation**
  - prevents either sender or receiver from denying a transmitted message
  - when a message is sent, the receiver can prove that the alleged sender in fact sent the message
  - used to prevent an entity from denying an action took place
  - examples: Digitally signed emails, System Event Logs

Security Service (3)

- **Data Confidentiality**
  - protection of data from unauthorized disclosure
- **Data Integrity**
  - assurance that data received is as sent by an authorized entity

Security Mechanism

- Security control measures
- Feature designed to detect, prevent, or recover from a security attack
- No single mechanism that will support all services required
- However one particular element underlies many of the security mechanisms in use ***cryptographic techniques***

Security Mechanism (2)

Specific Security Mechanisms

- encipherment
- digital signatures
- access controls
- data integrity
- authentication exchange
- traffic padding
- routing control

Pervasive Security Mechanisms

- trusted functionality
- security labels
- event detection
- security audit trails
- security recovery

Security Mechanism (3)

Encipherment

- The use of mathematical algorithms to transform data into a form that is not readily intelligible.

Digital Signature

- Data appended to, or a cryptographic transformation of, a data unit, allowing a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

Access Control

- A variety of mechanisms that enforce access rights to resources.

Data Integrity

- A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange

- A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding

- The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Relationship between Services & Mechanism

Security Service	Security Mechanism
Data Confidentiality	Encipherment, Routing Control
Data Integrity	Encipherment, Digital Signature, Data Integrity
Authentication	Encipherment, Digital Signature, Authentication Exchange
Nonrepudiation	Digital Signature, Data Integrity, Notarization
Access Control	Access Control Mechanism

Security Techniques

- Actual implementation of Security Goals require some techniques
- Two important techniques are as follows:
  - Cryptography
  - Steganography

- ***Cryptography:***
  - Greek Word: "Krypto" = Hidden / Secret
  - Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries.
  - Encryption and Decryption are two basic functions of Cryptography
  - It involves three distinct mechanism namely <u>Symmetric Key Encipherment</u>, <u>Asymmetric Key Encipherment</u> and <u>Hashing</u>

Security Techniques (2)

- ***Steganography:***
  - Strictly speaking, Steganography is not encryption
  - Steganography means ‘Covered Writing’ i.e. concealing the message itself by covering it with something else.
  - A plaintext message may be hidden in one of two ways.
  - The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text

Knowledge Check

Which of the following BEST indicates the probability that a successful attack will occur?

A. Value of the target and level of protection is high
B. Motivation and ability of the attacker is high
C. Value of the target is high and protection is low
D. Motivation of the attacker and value of the target is high

Correct Answer 'C'

Knowledge Check

___________ is used to prevent an entity from denying an action took place.

A. Confidentiality

B. Defense in Depth

C. Implicit Deny

D. Non-Repudiation

Correct Answer ‘D’

Knowledge Check

Anything deemed valuable to a company is considered an asset, even ideas.

A. True

B. False

Correct Answer ‘A’

Knowledge Check

Discuss

Active vs Passive Attacks

Knowledge Check

Discuss

Authentication vs Authorization.

End of Week 01