CO403 : CRYPTOGRAPHY AND NETWORK SECURITY (CS-II)

Dr. Udai Pratap Rao, CoED, SVNIT Surat

B.Tech. IV (CO) Semester - 7

L	T	P	C
3	1	2	5

CO403 : CRYPTOGRAPHY AND NETWORK SECURITY (CS-II)

INTRODUCTION AND OVERVIEW (02 Hours)

ELEMENTARY NUMBER THEORY (04 Hours)

Finite fields, Arithmetic and algebraic algorithms

PSEUDO RANDOM BIT GENERATORS (02 Hours)

FORMAL DEFINITION OF SECURE ENCRYPTION (04 Hours)

Perfect secrecy, Semantic security, IND-CPA, IND-CCA

STREAM CIPHERS (04 Hours)

One time pad, Security proof of one time pad

BLOCK CIPHERS (04 Hours)

Need for block ciphers, Luby-rackoff construction and its security proof, Modes of operation

HASH AND MAC FUNCTIONS (04 Hours)

Definitions, Notions of security and unaffordability (EUF-CMA), Merkle-Damgard family of hash functions

HARD PROBLEMS (04 Hours)

Discrete logarithm, Factorization

PUBLIC KEY CRYPTO SYSTEMS (06 Hours)

Diffie Hellman, RSA encryption; Proofs of security under hardness assumptions, Digital Signature

NETWORK SECURITY (03 Hours)

IDENTITY MANAGEMENT (03 Hours)

ADVANCED TOPICS (02 Hours)

(Total Contact Time: 42 Hours + 14 Hours = 56 Hours)

PRACTICALS

1) Implementation of Client side scripting

2) Implementation of Server side scripting

3) Implementation of mini project using above technology including the database connectivity

BOOKS RECOMMENDED

1). Dhiren Patel, Information Security: Theory and Practice, PHI, 2008/2010

2). William Stallings, "Cryptography and Network Security - Principles and Practice", 6/E, Pearson Education, 2013.

3). Douglas Stinson: "Cryptography: Theory and Practice, Third Edition", 3/E, Chapman and Hall/CRC, 2005

4). Menezes Bernard, Network Security and Cryptography, Cengage Learning India, 2010

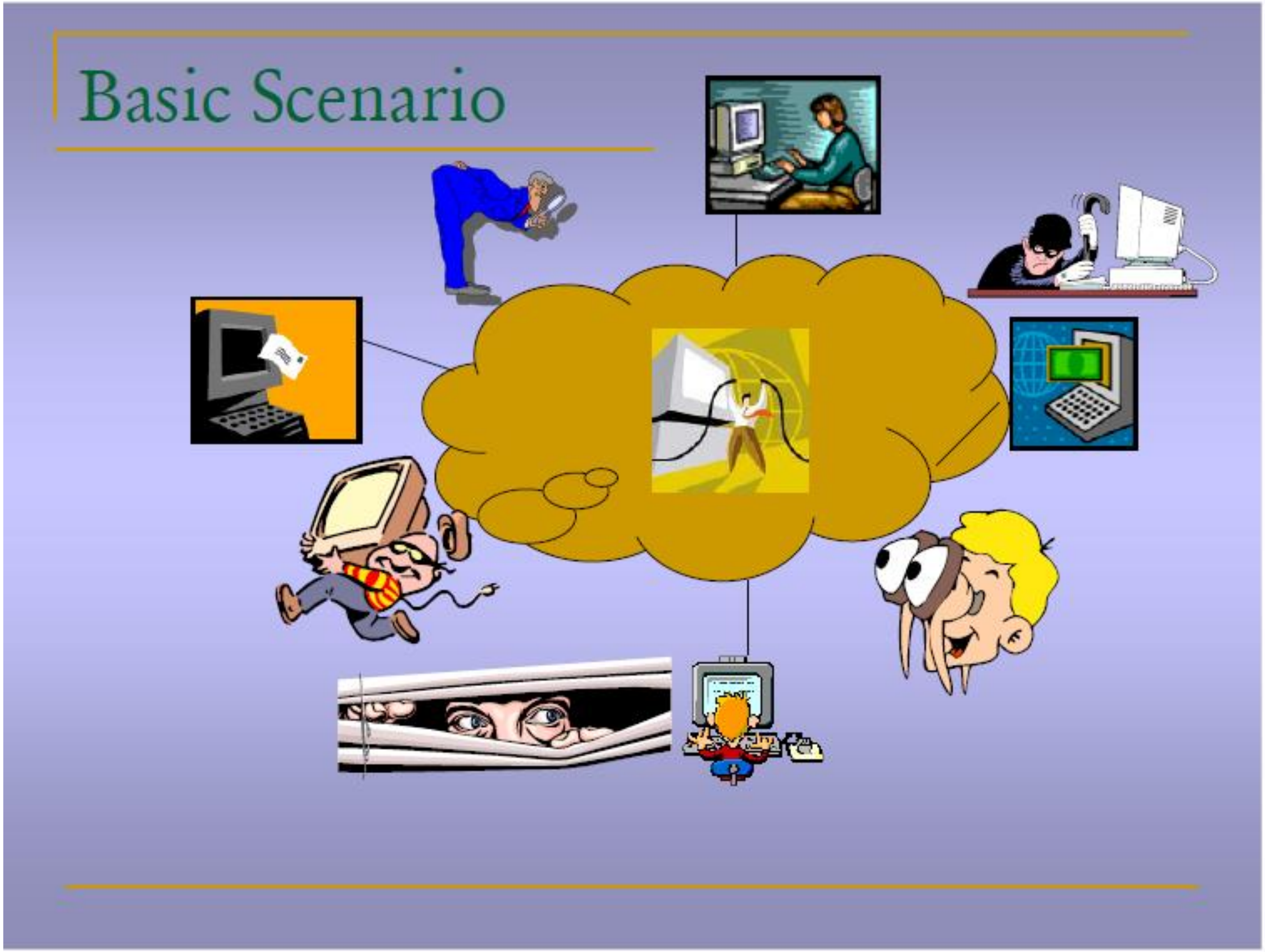
5). Alfred. J. Menezes, Paul C. van Oorschot, Scott A. Vanstone: "Handbook of Applied Cryptography", 1/E, CRC, 1996

COURSE OUTCOMES

- After successful completion of this course,
  - Student will be able to Understand the concepts related to the basics of cryptography and computer security.
  - Deduce the mechanisms to be employed while trying to satisfy any of the security services
  - Apply the concept of security services and mechanisms from the application developers and network administrator’s perspective.

Basic definitions

- Cryptography
  - study of encryption principles/methods
- Computer Security
  - generic name for the collection of tools designed to protect data
- Network Security
  - measures to protect data during their transmission
- Internet Security
  - measures to protect data during their transmission over a collection of interconnected networks



Basic Scenario

Basic Tasks to Secure the Information

- When an organization secures its information, it completes a few basic tasks:
  - It must analyze its assets and the threats these assets face from threat agents
  - It identifies its vulnerabilities and how they might be exploited
  - It regularly reviews the security policy to ensure it is adequately protecting its information

Basic Tasks to Secure the Information

- **Bottom-up approach:** major tasks of securing information are achieved from the lower levels(grassroots workers) of the organization upwards
  - This approach has one key advantage: the bottom-level employees have the technical expertise to understand how to secure information
  - It has a weakness: without approval from top levels of management, security schemas created by grassroots workers has small chance of success

Basic Tasks to Secure the Information

- **Top-down approach:** starts at the highest levels of the organization and works its way down
  - Advantage: the security plan initiated by top-level managers has the backing to make the plan work (funding and timing has the high level of support)

Defining Information Security

- Information security:
  - Tasks of guarding digital information, which is typically processed by a computer (such as a personal computer), stored on a magnetic or optical storage device (such as a hard drive or DVD), and transmitted over a network spacing.

Defining Information Security (continued)

- Ensures that protective measures are properly implemented
- is intended to protect information

Defining Information Security (continued)

- Analogy-
  - Alice places an object in a metal box, and then locks it with a combinational lock left there by Bob. Bob is the only person who can open the box since only he knows the combination.
  - number of digits in a combinational lock, longer the key; stronger the encryption, as extending the length of the key exponentially increases the number of possible key combinations.

Defining Information Security (continued)

- Information security is intended to protect information that has value to people and organizations
  - This value comes from the characteristics of the information:
    - **Confidentiality**
    - **Integrity**
    - **Availability**
- Information security is achieved through a combination of three entities

Defining Information Security (continued)

- **Confidentiality:** Prevention of unauthorized disclosure of information.
- **Integrity:** Prevention of unauthorized modification of information.
- **Availability:** Prevention of unauthorized withholding/custody of information or resources. Or keeping system available…

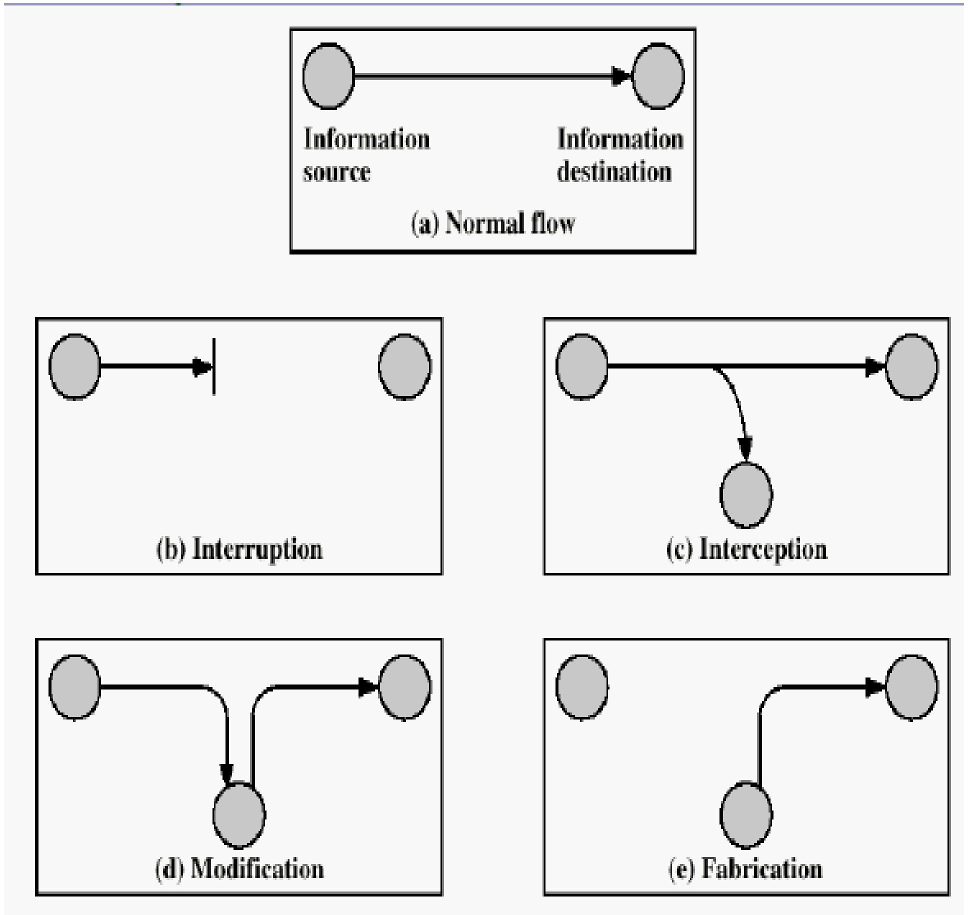
Defining Information Security (continued)

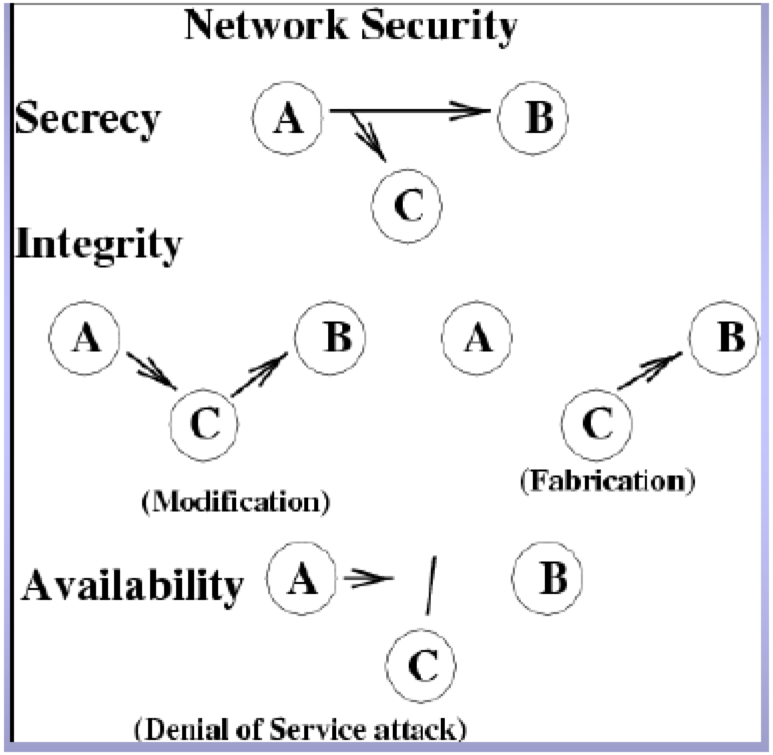
- **Nonrepudiation**: provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. In particular,
  - *Nonrepudiation of origin* proofs that the message was sent by the specified party.
  - *Nonrepudiation of destination* proofs that the message was received by the received party.

Defining Information Security (continued)

- ***Attacks against confidentiality***
  - Eavesdropping
  - traffic flow analysis
- ***Attacks against integrity***
  - Man-in-the-middle attack
- ***Attacks against availability***
  - Denial of Service attack

Security attacks



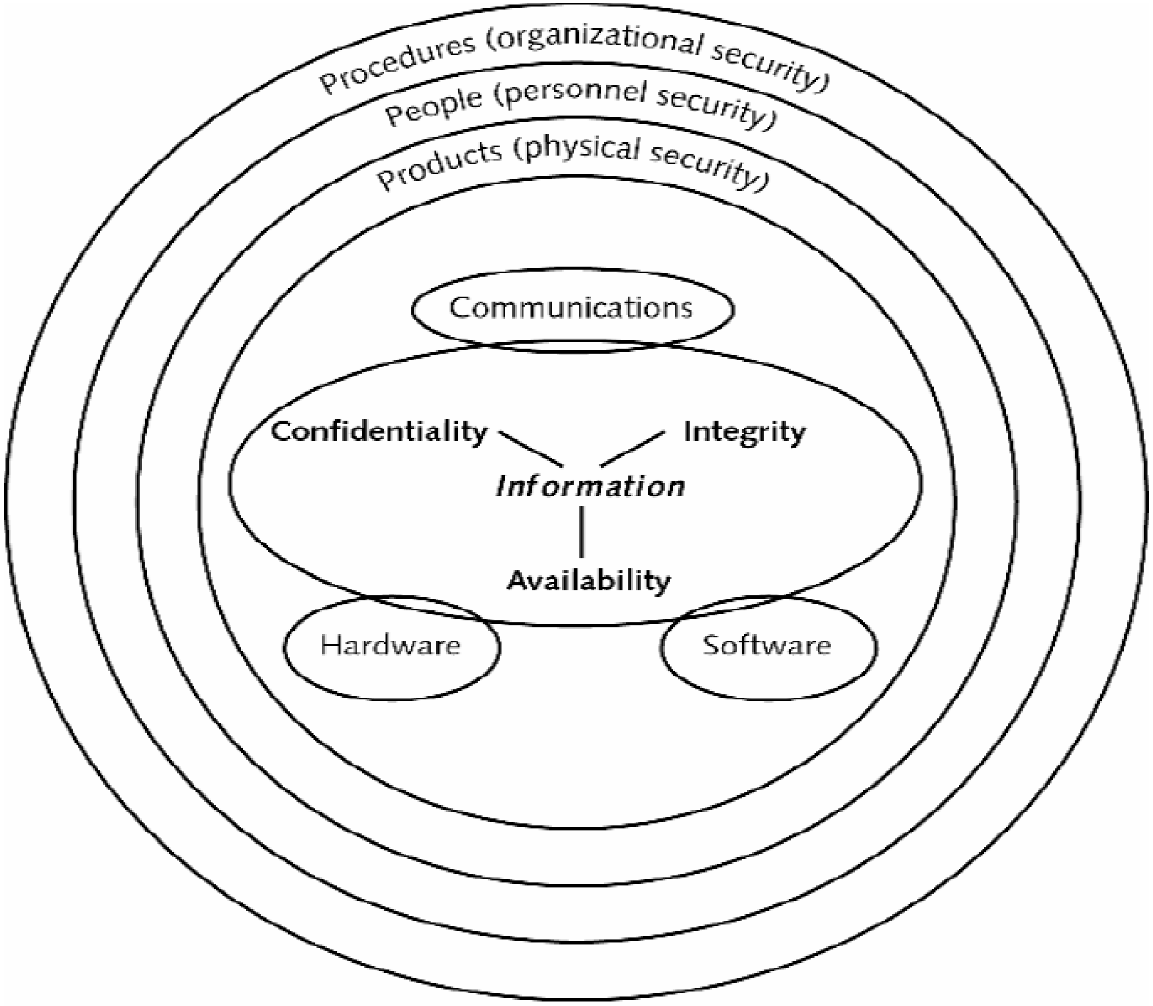


Defining Information Security (continued)

Security Service	Supporting Security Mechanisms
Confidentiality	encipherment
Traffic flow confidentiality	encipherment, traffic padding
Data integrity	encipherment, digital signature
Availability	authentication exchange
Nonrepudiation	digital signature

Relationship between security services and mechanisms

Defining Information Security (continued)


Procedures (organizational security)
People (personnel security)
Products (physical security)
Communications
Confidentiality
Integrity
Information
Availability
Hardware
Software

Information Security Components

Defining Information Security (continued)

Layer	Description
Products	The physical security around the data. May be as basic as door locks or as complicated as intrusion-detection systems and firewalls.
People	Those who implement and properly use security products to protect the data.
Procedures	Plans and policies established by an organization to ensure that people correctly use the products.

Information Security Layers

Defining Information Security (continued)

- A more comprehensive definition of information security is:
  - *That which protects the integrity, confidentiality, and availability of information on the devices that store, and transmit the information through products, people, and procedures.*

Information Security Terminology

- **Asset**
  - Something that has a value
- **Threat**
  - An event or object that may defeat the security measures in place and result in a loss
- **Threat agent**
  - A person or thing that has the power to carry out a threat

Information Security Terminology (continued)

- **Vulnerability**
  - Weakness that allows a threat agent to bypass security
- **Risk**
  - The likelihood that a threat agent will exploit a vulnerability
  - Realistically, risk cannot ever be entirely eliminated

Information Security Terminology (continued)

- **Security Mechanism**
  - a mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service**
  - It makes use of security mechanisms to counter security attacks.

Information Security Terminology (continued)

Term	Example in Information Security
Asset	Employee database
Threat	Steal data
Threat Agent	Attacker
Vulnerability	Software defect
Exploit	Send virus to unprotected e-mail server
Risk	Educate users
Security Mechanism	IPS, IDS etc…..

Some More Terminologies

- plaintext - original message
- ciphertext - coded message
- cipher - algorithm for transforming plaintext to ciphertext
- key - info used in cipher and known only to sender/receiver
- encipher (encrypt)
  - converting plaintext to ciphertext
- decipher (decrypt)
  - recovering plaintext from ciphertext
- cryptography
  - study of encryption principles/methods
- cryptanalysis (codebreaking)
  - study of principles/ methods of deciphering ciphertext without knowing key
- cryptology
  - field of both cryptography and cryptanalysis

Attacker Profiles

- Six categories:
  - Hackers
  - Crackers
  - Script kiddies
  - Spies
  - Employees
  - Cyberterrorists

Hackers

- Person who uses advanced computer skills to attack computers, but not with a malicious intent
- Use their skills to expose security flaws.
- **Hacker Code of ethics**: Breaking into another person's computer is ethically acceptable as long as they don't commit theft, damage, or break of confidentiality.

Crackers

- Person who violates system security with malicious intent
- Have advanced knowledge of computers and networks and the skills to exploit them
- Destroy data, deny legitimate users of service, or otherwise cause serious problems on computers and networks
- "crackers are often mistakenly called hackers”

Script Kiddies

- Break into computers to create damage
- Are unskilled users
- Download automated hacking software from Web sites and use it to break into computers
- Tend to be young computer users with almost unlimited amounts of free time , which they can use to attack systems

Spies

- Person hired to break into a computer and steal information
- Do not randomly search for unsecured computers to attack
- Hired to attack a specific computer that contains sensitive information
- Motivation is almost always financial.

Employees

- One of the largest information security threats to business
- Employees break into their company’s computer for these reasons:
  - To show the company a weakness in their security
  - To say, “I’m smarter than all of you”
  - For money.
  - A dissatisfied employee wanting to get back at the company

Cyberterrorists

- Experts fear that terrorists will attack the network and computer infrastructure to cause panic
- Cyberterrorists’ motivation may be defined as ideology, or attacking for the sake of their principles
- One of the targets highest on the list of cyberterrorists is the Internet itself

Approaches to provide the security

- The different approaches for providing security can be categorized into the following six areas:
  - ***Attack Deterrence*** –
    - Attack deterrence refers to persuading an attacker not to launch an attack by increasing the perceived risk of negative consequences for the attacker.
    - Having a strong legal system may be helpful in attack deterrence.
    - However, it requires strong evidence against the attacker in case an attack was launched.

Approaches to provide the security

- ***Attack Prevention*** –
  - Attack prevention aims to prevent an attack by blocking it before an attack can reach the target.
  - However, it is very difficult to prevent all attacks. This is because, to prevent an attack, the system requires complete knowledge of all possible attacks as well as the complete knowledge of all the allowed normal activities.
  - An example of attack prevention system is a firewall .

Approaches to provide the security

- ***Attack Deflection*** –
    - Attack deflection refers to tricking an attacker by making the attacker believe that the attack was successful,
    - though in reality, the attacker was trapped by the system and deliberately made to reveal the attack.
    - Research in this area focuses on attack deflection systems such as the honey pots .
- ***Attack Avoidance*** –
    - Attack avoidance aims to make the resource unusable by an attacker even though the attacker is able to access that resource.
    - An example of security mechanism for attack avoidance is the use of cryptography . Encrypting data renders the data useless to the attacker, thus, avoiding possible threat.

Approaches to provide the security

- ***Attack Detection*** –
  - Attack detection refers to detecting an attack while the attack is still in progress or to detect an attack which has already occurred in the past.
  - Detecting an attack is significant for two reasons; first the system must recover from the damage caused by the attack and second, it allows the system to take measures to prevent similar attacks in future.
  - Research in this area focuses on building intrusion detection systems and it is equally important for database protection.
- ***Attack Reaction and Recovery*** –
  - Once an attack is detected, the system must react to an attack and perform the recovery mechanisms as defined in the security policy.

Components of Intrusion Detection Systems

- An intrusion detection system typically consists of three sub systems or components:

1. Data Preprocessor :

   – Data preprocessor is responsible for collecting and providing the audit data (in a specified form) that will be used by the next component (analyzer) to make a decision.

   --Data preprocessor is, thus, concerned with collecting the data from the desired source and converting it into a format that is comprehensible by the analyzer.

Data used for detecting intrusions range from user access patterns (for example, the sequence of commands issued at the terminal and the resources requested) to network packet level features (such as the source and destination IP addresses, type of packets and rate of occurrence of packets) to application and system level behaviour (such as the sequence of system calls generated by a process.) We refer to this data as the audit patterns.

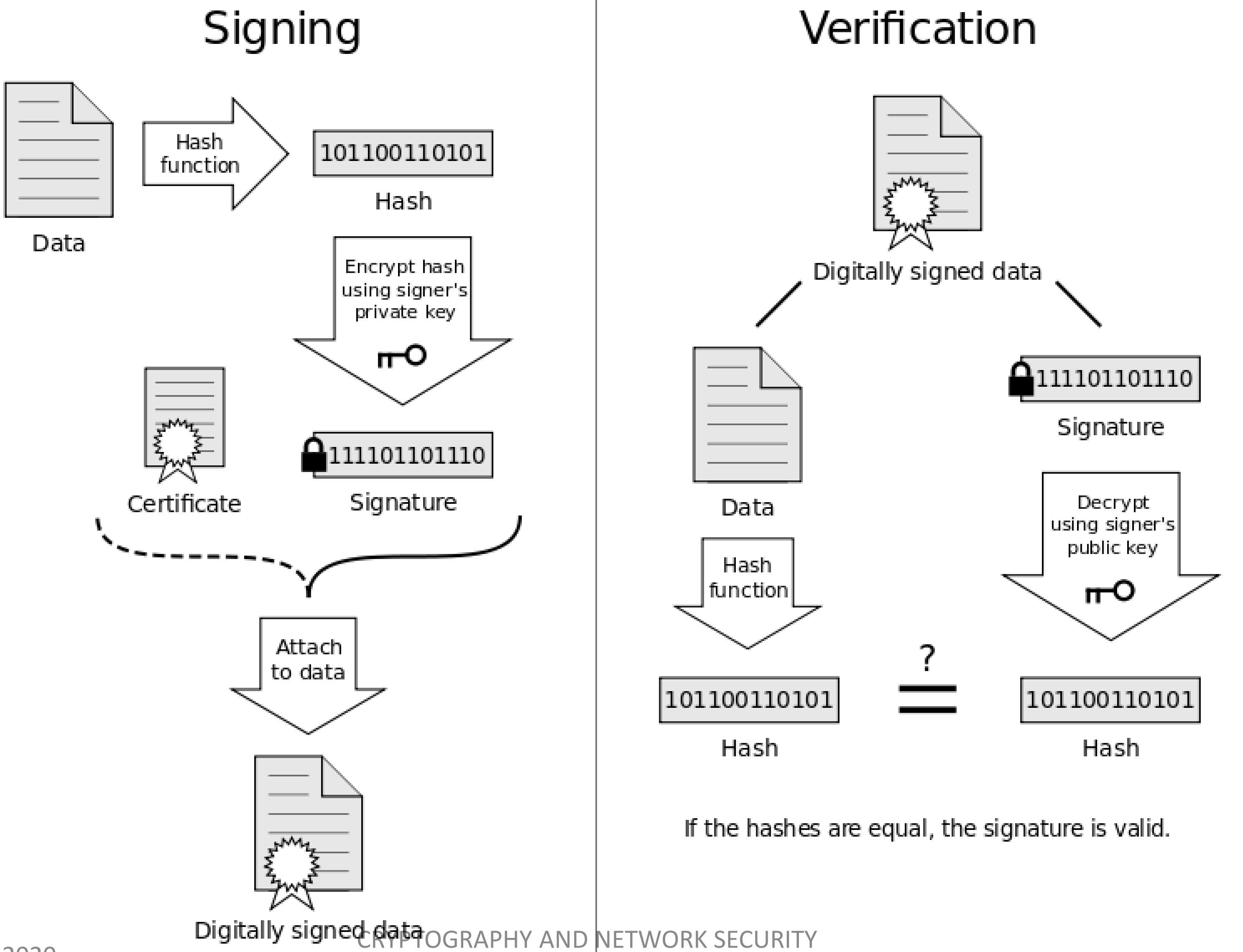
Components of Intrusion Detection Systems

2. Analyzer (Intrusion Detector) – The analyzer or the intrusion detector is the core component which analyzes the audit patterns to detect attacks. This is a critical component and one of the most researched. Various ***pattern matching, machine learning, data mining and statistical techniques*** can be used as intrusion detectors. The capability of the analyzer to detect an attack often determines the strength of the overall system.

3. Response Engine – The response engine controls the reaction mechanism and determines how to respond when the analyzer detects an attack. The system may decide either to raise an alert without taking any action against the source or may decide to block the source for a predefined period of time. Such an action depends upon the predefined security policy of the network.

digital signature

an additional data unit that is added to the principal data unit to enable recipient to verify the source



Metrics for Performance Evaluation of Classifier

	PREDICTED CLASS		
ACTUAL CLASS		Class=Yes (Positive)	Class=No (Negative)
	Class=Yes (Positive)	a	b
	Class=No (Negative)	c	d

- The entries in the confusion matrix have the following meaning :
  - a is the number of **correct** predictions that an instance is **positive,**
  - *b* is the number of **incorrect** of predictions that an instance **negative**,
  - *c* is the number of **incorrect** predictions that an instance is **positive**, and
  - d is the number of **correct** predictions that an instance is **negative.**

Metrics for Performance Evaluation of Classifier

- The *accuracy* (*AC*)- is the proportion of the total number of predictions that were correct. It is determined using the equation:

$$\text{Accuracy} = \frac{a+d}{a+b+c+d} = \frac{TP+TN}{TP+TN+FP+FN}$$

- Consider a 2-class problem
  - Number of Class 0 examples = 9990
  - Number of Class 1 examples = 10
- If model predicts everything to be class 0, accuracy is 9990/10000 = 99.9 %
  - ➢ Accuracy is misleading because model does not detect any class 1 example

Contd…

- The *recall or true positive rate* (*TP*) is the proportion of positive cases that were correctly identified, as calculated using the equation:

$$\text{TP} = \frac{a}{a+b} = \frac{TP}{TP+FN}$$

- The *false positive rate* (*FP*) is the proportion of negatives cases that were incorrectly classified as positive, as calculated using the equation:

$$\text{FP} = \frac{c}{c+d} = \frac{FP}{FP+TN}$$

Contd…

- The *true negative rate* (*TN*) is defined as the proportion of negatives cases that were classified correctly, as calculated using the equation:

$$\mathrm{TN} = \frac{d}{d+c} = \frac{TN}{TN+FP}$$

- The *false negative rate* (*FN*) is the proportion of positives cases that were incorrectly classified as negative, as calculated using the equation:

$$\mathrm{FN} = \frac{b}{b+a} = \frac{FN}{FN+TP}$$

Contd…..

- *The precision* (*P*) is the proportion of the predicted positive cases that were correct, as calculated using the equation:

$$\mathrm{P} = \frac{a}{c+a} = \frac{TP}{FP+TP}$$

IDS Example

- Suppose we train a IDS model to predict whether an action is **Malicious** or **Not malicious**. After training the IDS model, we apply it to a test set of 500 new actions (also labeled) and the IDS model produces the contingency matrix below.

		True Class	
		Malicious	Not malicious
Predicted Class	Malicious	70	10
	Not Malicious	40	380

(a) Compute the precision of this IDS model with respect to the malicious **class.**

(b) Compute the recall of this IDS model with respect to the malicious **class.**

Cond…

- **High-precision and low recall with respect to Malicious:** whatever the model classifies as malicious is probably malicious. However, many actions that are truly malicious are misclassified as NOT malicious i.e <False Negative (False Acceptance)>

- **High recall and low precision with respect to malicious:** the model filters all the malicious actions, but also incorrectly classifies some genuine actions as malicious i.e. <False Positive (False Rejectance)>.