D 27

SCHEME OF VALUATION

(Scoring Indicators)

Revision: 2015 **Course Code: TED (15) 5136**

Course Title :INFORMATION SECURITY

Qst. No.	Scoring Indicator	Split up score	Sub Total	Total
	PART A			
I. 1)	• **Data Confidentiality** : Assures that the private or confidential information is not made available to unauthorized individuals • **Privacy**: Assures that the individuals control information related to them. Individual can control the storage and disclosure of their information	1 1	1+1 = 2	2
I. 2)	• It should come from genuine source • The content of the message have not been altered • Timeliness of message (i.e. it has not been delayed or replayed) • Sequence or order of message have to maintained (Any two is enough 1 each)	1 each	1+1=2	2
I. 3)	• Static Biometric Characteristics : Facial characteristics, finger print, hand geometry, retina, Iris etc • Dynamic Biometrics : Voice Pattern, Signature pattern (Any four enough)	0.5 each	4 * 0.5 = 2	2
I. 4)	• Both masquerader and misfeasor are intruders • **Masquerader** : An unauthorized outsider who penetrates the system to exploit a legitimate user's account • **Misfeasor** : A legitimate user (insider) who access resources in an unauthorized manner by misusing his privileges	1 1	1+1 = 2	2
I. 5)	• An action that prevents authorized use of resources like networks, systems or applications by exhausting CPU, memory, bandwidth and disk space.	2	2	2
	PART B			
II. 1)				

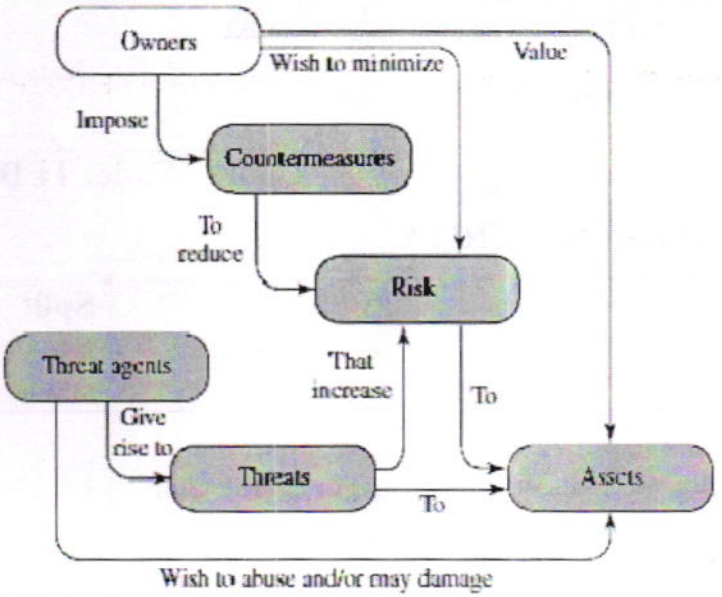


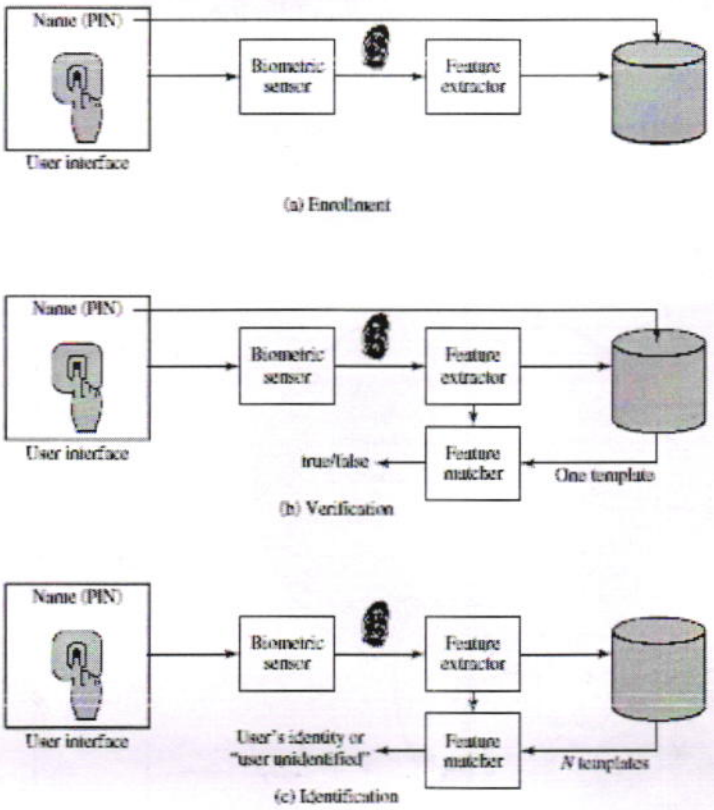
Figure 1.2 Security Concepts and Relationships

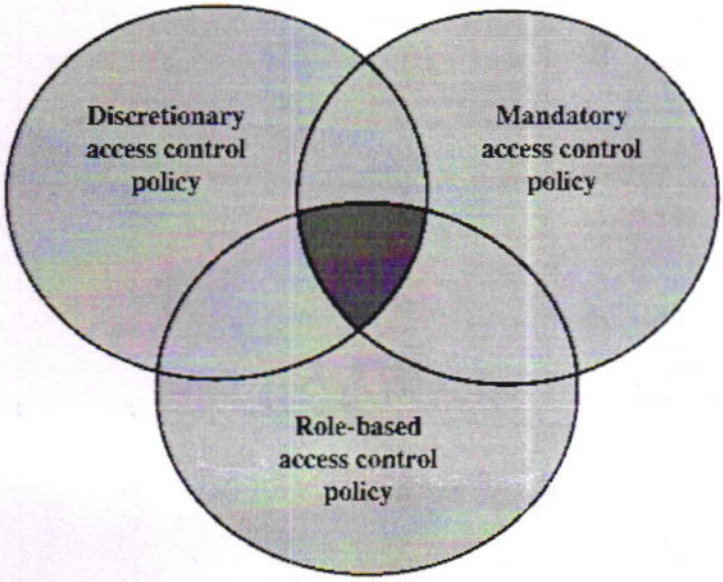
- **Assets** are generally 4 types : Valuable resources such as Hardware, software, Data and Network
- **Vulnerabilities** can be leaky (confidentiality issue), corrupted (integrity issue) or unavailable.
- Corresponding to the various types of vulnerabilities, there are **threats** that. A threat represents potential security harm to an asset.
- An **attack** is a threat action and, if successful, leads to threat consequence. The agent carrying out the attack is referred to as an attacker, or **threat agent**.
- Attacks can be active or passive. It may be an inside attack or outside attack
- Finally, a **countermeasure** is any means taken to deal with a security attack. A countermeasure can be devised to **prevent** a particular type of attack. When prevention is not possible, the goal is to **detect** the attack and then **recover** from the effects of the attack. A countermeasure may itself introduce new vulnerabilities that may be exploited by threat agents representing a residual level of **risk** to the assets.
- **Owners** will seek to minimize that risk given other constraints.

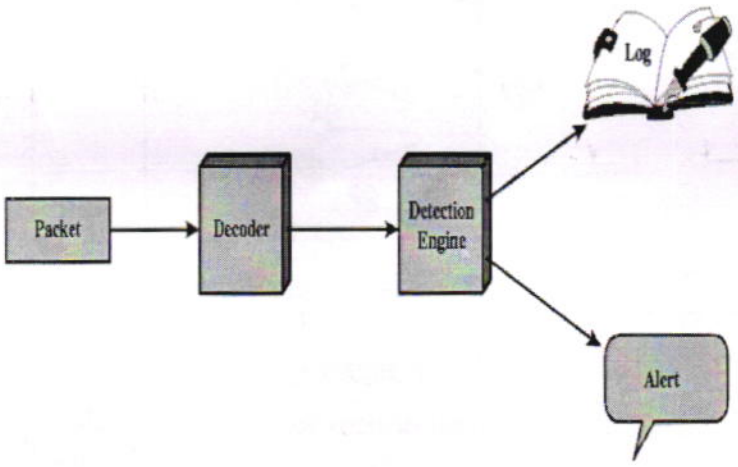
3 for Diagram | 3 + 3 = 6 | 6

3

II. 2)	A number of network security algorithms based on cryptography make use of random numbers. Random numbers exhibit the	1	1+5=6	6

	property of uniqueness and unpredictability. Examples : 1) Generation of keys for public-key encryption algorithms. 2) Generation of a stream key for symmetric stream cipher 3) Generation of a symmetric key for use as a temporary session key or in creating digital envelope 4) In key distribution technique like **Kerberos**, random numbers are used for handshaking to prevent replay attacks. 5) Session key generation by key distribution centre or by one of the principals.	5		
II. 3)	 Figure 3.6 **A Generic Biometric System** Enrollment creates an association between a user and the user's biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user. • First step is **enrollment** – User presents the name, some password or PIN to the system – System senses some biometric characteristics of the user – Digitizes the input and extract a set of features that can be stored as a set of numbers referred to as user's	2 for Diagram	6	6

	template – Enrollment creates an association between a user and the user's biometric characteristics • Second step is either **verification** or **identification** which depends on application – For **verification**, the user enters a PIN and also uses a biometric sensor. The system extracts the corresponding features and compares that to the template stored for the user. – For **identification**, the user uses the biometric sensor without providing any additional information like PIN. The systems extracts the features and compares it with the set of stored templates. If there is no match, the user is rejected.	2 2		
II. 4)	 • An access control policies are stored in an authorization database which decides what types of access are permitted to each user or process under each circumstance. • Access control policies are generally grouped into the following categories: • **Discretionary access control (DAC):** – **DAC** controls access based on the identity of the user and on	1.5 for diagram	4 x1.5=6	6

	access rules (authorizations) stating what requestors are (or are not) allowed to do. This policy is termed *discretionary* because an entity or user might have access rights that permit him to enable another entity to access some resource. • **Mandatory access control (MAC):** – MAC controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is termed *mandatory* because an entity that has clearance to access a resource may not enable another entity to access that resource. • **Role-based access control (RBAC):** – RBAC controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles. • These three policies are not mutually exclusive as indicated in the fig. An access control mechanism can use two or even three of these policies to cover different system resources.	1.5 1.5 1.5		
II. 5)	• Snort is an open source, highly configurable and portable host-based or network-based IDS. Snort is referred to as a lightweight IDS.  • A Snort installation consists of four logical components, shown here in Figure – **Packet Decoder:** efficiently processes each captured	2 for diagram 4	2+4=6	6