Tutorial - 2

U20CS005

1. Comment on the following security services as listed below and also complete the entries with their supporting security mechanisms.

Security services

(i) Confidentiality

(ii) Traffic flow confidentiality

(iii) Data integrity

(iv) Availability

(v) No repudiation.

→ (i) Confidentiality:

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

(ii) Traffic flow confidentiality (TFC):

TFC mechanisms are techniques devised to hide/ masquerade the traffic pattern to prevent statistical traffic analysis attacks.

(iii) Data integrity:

This ~~mechanism~~ service assures that data and programs are changed only in specified and authorised manner.

(iv) Availability:

Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

(v) No repudiation:

It prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove the alleged sender in fact the sent

the message, same on ~~sender side~~ sender's side.

Security service — Security Mechanism.

Confidentiality — Encryption (Encipherment)

Security Service	Supporting security Mechanism.
- Confidentiality	Cryptographic algorithm, Access control, Notarization
- Traffic flow confidentiality	Traffic padding, Routing control, access control
- Data integrity	Cryptographic algorithm, Digital signature, Authentication exchange
- Availability	Access control, Authentication exchange, Routing control
- No rupudiation.	Digital Signature, Authentication exchange, Access control

2. Comments on the following attacker profiles.
- Hackers
- Crackers
- Script kiddies
- Spies.
- Employees
- Cyber terrorists.

→ - Hackers:

Person who uses advanced computer skills to attack computers, but not with a malicious intent. They uses their skills to expose security flaws.

- Crackers:

Person who violates system security with malicious intent. They have advanced knowledge of computers and networks and the skills to exploit them. They destroys data, deny legitimate users of service, or otherwise cause serious problems on computers & networks

- Script kiddies:

They are not as skilled as Crackers. Script kiddies download automated hacking software from web sites

and use it to break into computers. Generally script kiddies tend to be young computer users with large amount of leisure time, which they can use to attack systems.

- Spies:
They are the person hired to break into a computer and steal information and are hired to attack specific computer that contains sensitive information. The possess excellent computer skills.

- Employees:
They are 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
  - Being overlooked, revenge
  - For money.

- Cyberterrorists:
~~The expert~~ Cyberterrorists are criminals who uses computer technology and the internet, especially to cause fear and disruption.

3. Explain the following security approaches.
Security approaches
(i) Attack Deterrence
(ii) Attack Prevention
(iii) Attack Deflection
(iv) Attack Avoidance.

→ - Attack Deterrence:
It refers to measures taken to discourage an attacker from attempting to ~~a~~ breach a system, such as through the use of security warning or by making target less attractive.

- For this we can use security warnings or pop-ups which notifies when system is in risk

2) Attack Detection:
It refers to identifying that an attack is occuring on a system ~~such as by~~ by using intrusion detection system or by monitoring network traffic for suspicious activities. For this we can use firewall which blocks unauthorized incoming network traffic

3) Attack deflection:
It refers to redirecting an attack away from its intended target, such as by using honeypot which is a decoy system that is set up to attract attacker away from real network or by implementing routing changes to redirect traffic

4) Attack Avoidance:
It refers to taking steps to prevent an attack from occurring in the first place such as through use of firewalls or by software patching to fix vulnerabilities that can be exploited by attackers.

Security Approaches	Security Mechanism
Attack Deterrence	Access control
Attack Prevention	Cryptographic algorithm, Data integrity
Attack Deflection	Notarization
Attack Avoidance	Authentication Exchange, Digital Signature