

Tutorial 2

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

Confidentiality: encipherment, routing control

Traffic flow confidentiality: encipherment, traffic padding, routing control

Data Integrity: encipherment, data integrity, digital signature

Availability: Access control, authentication exchange

No repudiation: digital signature, notarisation

Q.2 Comments on following attacker profiles:

Hacker: A person skilled in information technology who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerised system by non-standard means.

Crackers: People who hack a system by breaking into it and violating it with some bad intentions.

Script kiddies: They are unskilled individuals who use scripts or programs developed by others, primarily for malicious purposes.

Spies: People who perform the act of obtaining secrets and confidential information without the permission and knowledge of the holder using proxy servers, trojan horses and spywares.

Employees: Disgruntled ~~and~~ employees often present an insider threat to data. They can easily breach the sensitive information and exploit it for malicious purposes.

Cyber terrorists: They are well funded group of politically inspired attackers who attempt to steal or corrupt corporate and government data in order to disrupt/harm the countries, businesses and individuals.

8.3 Explain the following security approaches.

Attack Deterrence: Access control

Attack Prevention: Encryption, data integrity

Attack Deflection: Bit stuffing, notarisation

Attack Avoidance: Authentication exchange, digital signatures