Introduction to Cyber Security

IMPORTANT NOTES: Study lecture materials at least 1 hour and prepare Question 1-4 prior to the tutorial session. Those questions will be discussed in the tutorial.

1. Distinguish or define the following terms within the context of security: Vulnerability, Threat and Control.

   Vulnerability is a weakness in a security system, that might be exploited to cause loss or harm. It is a means by which a threat agent can cause harm.

   A *threat* is a set of circumstances that has the potential to cause loss or harm.

   A *control* is a protective measure that prevents a threat agent from exercising vulnerability. That is, a control is an action, device, procedure, or technique that removes or reduces vulnerability.

2. Categorise the type of security threats (or attacks) to computers/distributed systems/computer networks by the type of security goal that is breached.

   (a) Interruption: attack on availability

   (b) Interception: attack on confidentiality

   (c) Modification: attack on integrity

   (d) Fabrication: attack on authenticity

3. Give an example scenario to each of the above category – can be your own personal computer, corporate computer systems such as Monash University, etc. Relate those threats to hardware/software/data as applied to corporate computer systems.

   The answers can vary. There are some answers outside the scope of this subject! This can be answered using examples as follows:

   (a) **Interruption:** send a huge numbers of icmp packets using ping command from thousands of machine to one specific computer to increase processing load so eventually the machine cannot provide any other services.

   (b) **Interception:** using packet sniffer software to detect data transmitted across the network even the data is transmitted in cipher text in attempt to retrieve plaintext. The main purpose of this kind of attack is to retrieve cryptographic keys. Example: ARP poisoning attack.

   (c) **Modification:** an attacker intercepts a message; changes its content, and sends to intended recipient. The recipient receives the message without being aware that the content of the message has been changed.

   (d) **Fabrication:** initially, an attacker needs to have a secret key shared between Alice and Bob. The attacker applies a cryptographic operation with the key to a message and sends it to the Bob. Bob receives the message without being aware that the message has not been sent from Alice.

   Note that, to succeed in modification and fabrication, the attacker needs to have the cryptographic key, which can be retrieved by interception.

4. What are the differences between passive attack and active attack?

   Passive attack has the nature of eavesdropping on, or monitoring of, transmission of information between the communicating parties, but does not modify or tamper the message. It captures the message and may read the content. It can be used for traffic analysis e.g., who is a particular person communicating with and the frequency of communication.

   Active attack modifies a message stream or creates a false message. It is used to launch more severe forms of attack.

5. Describe different types of passive attacks and active attacks.

   Passive attacks, 2 types:

   (a) **Release of message content:** captures and read the content.

   (b) **Traffic analysis:** does not read the message but observes the pattern. Observation usually involves determining the location and identity of communicating parties, frequency and length of communication.

   Active attacks, 4 types:

   (a) **Masquerade:** assumes a false identity.

   (b) **Replay:** passive capture of data and subsequent retransmission.

   (c) **Modification of Message:** message is altered, delayed or reordered to produce unauthorized effect.

   (d) **Denial of Service:** cripple the server with a flood of requests; eat up all the computing resources of the server, causes disruption of services of an entire network or suppression of all messages directed to a particular destination.

6. For each of the following example systems, state the security goal you think is most important and rank in order of imporance any other relevant goals, giving your reasoning: (1) online banking, (2) bureau of meterology weather forecast website, (3) military intelligence database.

   Goals from most important to least (there may be several plausible answers):

   (a) **online banking:** integrity (to make sure financial accounts are not being tempered with to prevent loss of money to bank customers), authenticity (to make sure only the authorised users can spend their bank account funds), availability (to make sure funds can be accessed when required), confidentiality (to protect the financial transaction privacy of customers).

   (b) **bureau of meterology (BOM) weather forecast website:** Goals from most important to least (there may be several plausible answers): availability (to make sure weather forecase can be accessed whenever required), integrity (to make sure hackers cannot post incorrect weather forecasts), authenticity (to make sure only the authorised BOM forecasters can post forecasts), confidentiality is not required (as the forecast is public knowledge).

   (c) **military intelligence database:** Goals from most important to least (there may be several plausible answers): confidentiality (to prevent military opponents from changing plans based on knowledge of the other side's intelligence), integrity (to prevent false intelligence from being injected by military opponents), authenticity (to prevent false intelligence from untrusted sources), availability (to make sure intelligence can be accessed on demand for military applications).