FIT2093: Tutorial 1

Introduction to cyber security

Review Questions

1. What is cyber security?
2. Distinguish or define the terms within the context of security: Vulnerability, Threat and Control.
3. Categorise the type of security threats (or attacks) to computers/distributed systems/computer networks (also known as logical security risks).
4. Give an example 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.
5. Enumerate the desirable security properties for overall security?
6. What are the differences between passive attack and active attack?
7. Describe different types of passive attacks and active attacks.
8. List and briefly define categories of security services.
9. List and briefly define 6 categories of security mechanism.

Problems

1. Preserving confidentiality, integrity, and availability of data is a restatement of the concern over interruption, interception, modification, and fabrication. How do the first three concepts relate to the fourth one? That is, is any of the four equivalent to one or more of the three?
2. It is stated that it is impossible to design security mechanism(s) to shield any kind of security attacks - Why is this statement true?
3. One control against accidental software deletion is to save all old versions of a program. Of course, this control is prohibitively expensive in terms of cost of storage. Suggest a less costly control against accidental software deletion. Is your control effective against all possible causes of software deletion? If not, what threats does it not cover?

4. For a user workstation in a typical business environment, list potential locations for confidentiality attacks.
5. You discover that your computer has been infected by a piece of malicious (virus) code. You have no idea when the infection has occurred. You do have backups performed every week since the system was bought, but, offcourse, there have been numerous changes to the system over time. How could you use the backups to construct a “clean” version of your computer system?
6. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement.
7. Consider a desktop publishing system used to produce documents for various organizations.
    a. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.
    b. Give an example of a type of publication for which data integrity is the most important requirement.
    c. Give an example in which system availability is the most important requirement.