FIT5163 Information and Computer Security
Applied 1
Introduction to Information and Computer Security

1. What are the differences between computer/network/inter network security?

2. Categorise the type of security threats (or attacks) to computers /distributed systems /computer networks.

3. Relate those threats to hardware/software/data as applied to corporate computer systems.

4. Enumerate the desirable properties that security mechanisms should have?

5. What is the difference between passive and active security threats?

6. What do you mean by authentication in relation to security and what properties it satisfies?

7. It is stated that it is impossible to design security mechanism(s) to shield any kind of security attacks - Why is this statement true?

8. 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 last four? That is, is any of the four equivalents to one or more of the three? Is one of the three encompassed by one or more of the four?

9. For a user workstation in a typical business environment, list potential locations for confidentiality attacks.

10. List ways in which secret keys can be distributed to communicating parties.

11. 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.

12. Consider a desktop publishing system used to produce documents for various organisations.
    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.