CSIT988/CSIT488 – "Security, Ethics and Professionalism"

Autumn 2025

Workshop 6

I. Multiple-Choice Questions

1. Which of the following statements are true?

   Select one or more:

A. In an asymmetric encryption scheme, a ciphertext is the result of running the decryption algorithm on a plaintext.
B. Stateful inspection firewalls and dual-homed host firewalls are among the common firewall architectures.
C. Signature-based method is one of the common detection methods for IDPSs.
D. WPA has improved security compared to WEP.
E. HTTPS is a prominent protocol for email security.

2. Which of the following statements are true?

   Select one or more:

   A. It is extremely uncommon for a CISO to have a CISSP.
   B. InfoSec consideration should be part of the hiring process.
   C. A background check should be conducted before the organization extends an offer to any security technician.
   D. Job rotation is based on the principle of least privilege.
   E. Ethics are rules adopted and enforced by governments.

3. Which of the following statements declare the business of the organisation and its intended areas of operations?

   Select one or more:

   A. Mission Statement
   B. Business Statement
   C. Values Statement
   D. Policy Statement
   E. Vision Statement

4. Which of the following statements are true?

   Select one or more:

   A. The BiBa integrity model is based on the principle of "no read up, no write down".
   B. Asymmetric encryption systems are usually less efficient than symmetric encryption systems.
   C. Every ISSP document should contain a section about Intrusion Detection Systems.
   D. Risk analysis is a major component of risk management.
   E. An example of non-technical attack to InfoSec is shoulder surfing.

5. Which of the following security properties can be achieved with a digital signature such as RSA?

   Select one or more:

   A. Confidentiality
   B. Availability
   C. Authentication
   D. Non-Repudiation
   E. Privacy

II. Short-Answer Questions and Case Studies

1. What is the difference between authentication and authorization? Can a system permit authorization without authentication? Why or why not?

2. In InfoSec, what is a firewall? How is an application layer firewall different from a packet filtering firewall? Why is an application layer firewall sometimes called a proxy server?

3. How does a network-based IDPS differ from a host-based IDPS?

4. What are the main components of cryptology?

5. Explain the relationship between plaintext and ciphertext.

6. Explain the key differences between symmetric and asymmetric encryption. Which can the computer process faster? Which lowers the costs associated with key management?

7. Caesar cipher: The following ciphertext was obtained via a Caesar cipher (i.e., shift cipher) with a shift of 13. Could you decrypt it?

   GUR SVANY RKNZ JVYY GNXR CYNPR VA GUR ARKG ZBAGU.

8. If one encrypts the plaintext obtained from Question 7 via a Caesar cipher with a left shift of 6, then what would be the resulting ciphertext?

9. Examine the chain of public-key certificates associated with the website:
   https://moodle.uowplatform.edu.au/login/index.php

10. List and describe the criteria for selecting InfoSec personnel.

11. What are the critical actions that management must consider taking when dismissing an employee? Do these issues change based on whether the departure is friendly or hostile?

12. How do the security considerations for temporary or contract workers differ from those for regular employees?

13. What is separation of duties? How can this method be used to improve an organization's InfoSec practices?

14. What are the domains of InfoSec knowledge covered by the CISSP?

15. What is the key difference between laws and ethics?

16. Find examples in the context of InfoSec management in Australia, where a person or an organization may:
    i. Be lawful but not ethical.
    ii. Be ethical but not lawful.