COMP4108 Final Exam Practice

William Findlay

December 14, 2019

Contents

List of Figures

List of Tables

List of Listings

1 Preamble

1.1 Textbook

- here is a link to "Tools and Jewels"

1.2 General

1. Please follow the provided format
2. We should prioritize the mock exam over notes

Part I

Mock Exam

1 Basic Concepts and Principles

1. Provide definitions for the following:

   a) Confidentiality

   b) Data integrity

   c) Authentication

   d) Authorization

   e) Availability

f) Accountability

2. Briefly explain how repudiation violates accountability.

3. Describe the difference between a *trusted* and *trustworthy* actor.

4. Compare and contrast *privacy*, *protection*, and *anonymity*.

5. Come up with a simple example of a security policy for a house and describe a way it might be violated.

6. Label each number in Figure 1.1 using the following terms:

a) target asset

b) vulnerability

c) attacker

d) attack vector

e) threat agent

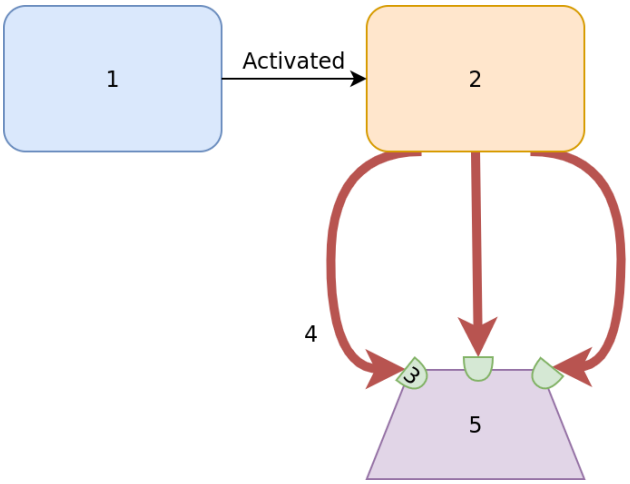

Figure 1.1

7. Draw a state machine diagram of a system's transition from a secure state to either a secure state or an insecure state.

8. Compare and contrast quantitative and qualitative risk assessment. Consider the advantages and disadvantages of each, as well as how each might work in theory/practice.

Qualitative	Quantitative

9. Consider $R = T \times V \times C$.

   a) What is this equation for?

   b) Describe each variable in this equation. How does each variable relate to the equation's purpose?

   c) Which two variables may be combined into P? What does the simplified equation look like? What does P represent?

10. Describe two risk assessment challenges.

11. Which of the following is not an adversary attribute?

    a) objectives

    b) outsider/insider

    c) methods

    d) funding level

    e) capabilities

    f) attack vector

12. What is a categorical schema? How is it different from a capability-level schema?

13. Compare and contrast a formal security evaluation with penetration testing.

Formal Security Evaluation	**Penetration Testing**

14. What is white-box pen testing? Black-box?

15. Consider STRIDE. What does each letter stand for?
    a) S:
    b) T:
    c) R:
    d) I:
    e) D:
    f) E:

16. Draw a tree model for compromising the password to a bank account. Include at least three leaf nodes.

17. Is it possible to completely test a comprehensive (and practical) set of security mechanisms for a system? Why or why not?

18. Explain the observability (or lack thereof) of security in the context of *negative goals*.

19. Assurance in security is best described as which of the following?

a) Simple, effective

b) Difficult, partial

c) Simple, practical

d) Difficult, complete

e) None of the above

2 Cryptographic Building Blocks

20. Suppose Alice encrypts a message to Bob using $E_k(m) = c$. How does Bob decrypt the message?

21. What is an exhaustive key search? What does the attacker try to do? Is this the worst case for attacking a cryptosystem?

22. Label each of the following attacks as either an action by an *active* or a *passive* adversary. Once you have labeled the attack, describe it.

a) Known plaintext attack

b) Ciphertext only attack

c) Chosen plaintext attack

d) Chosen ciphertext attack

23. What is the main advantage of a one-time pad? Describe three disadvantages. Why are one-time pads not used?

24. What is the current standard for block ciphers?

25. Describe a situation in which we would need to use a stream cipher. Why can't you use another type of cipher?

26. What is a mode of operation used for?

27. What is one major flaw with the ECB mode of operation?

28. Draw a picture of the CBC mode of operation.

29. Draw a picture of the CTR mode of operation.

30. If Alice wants to send a message to Bob using public-key encryption, _____ is used to encrypt and _____ is used to decrypt.

a) Bob's private key, Alice's public key

b) Bob's public key, Alice's private key

c) Bob's public key, Bob's private key

d) Alice's private key, Alice's public key

e) None of the above

31. If Alice wants to send a message to Bob using a public-key signature scheme, _____ is used to sign and _____ is used to verify

a) Bob's private key, Alice's public key

b) Bob's public key, Alice's private key

c) Bob's public key, Bob's private key

d) Alice's private key, Alice's public key

e) None of the above

32. How does hybrid encryption work? What role does symmetric key encryption play? Public-key encryption?

33. What three security properties do digital signature schemes provide? To whom to they provide them?

34. What two security properties do MACs provide? To whom do they provide them?

35. What security property does a cryptographic hash provide? To whom does it provide the property?

36.

Part II

Notes