COMP4108 Final Exam Practice

William Findlay

December 14, 2019

Contents

1 Preamble 1
1.1 Textbook 1
1.2 General 1

I Mock Exam 1

1 Basic Concepts and Principles 1

2 Cryptographic Building Blocks 7

3 User Authentication 7

4 Authentication Protocols and Key Establishment 7

5 Operating Systems Security and Access Control 7

6 Software Security – Privilege and Escalation 7

7 Malicious Software 7

8 Public Key Certificate Management and Use Cases 7

9 Web and Browser Security 7

10 Firewalls and Tunnels 7

11 Intrusion Detection and Network-Based Attacks 7

II Notes 8

1 Basic Concepts and Principles 8

2 Cryptographic Building Blocks 8

3 User Authentication 8

4 Authentication Protocols and Key Establishment 8

5 Operating Systems Security and Access Control 8

6 Software Security – Privilege and Escalation 8

7 Malicious Software 8

8 Public Key Certificate Management and Use Cases 8

9 Web and Browser Security 8

10 Firewalls and Tunnels 8

11 Intrusion Detection and Network-Based Attacks 8

List of Figures

1.1 3

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

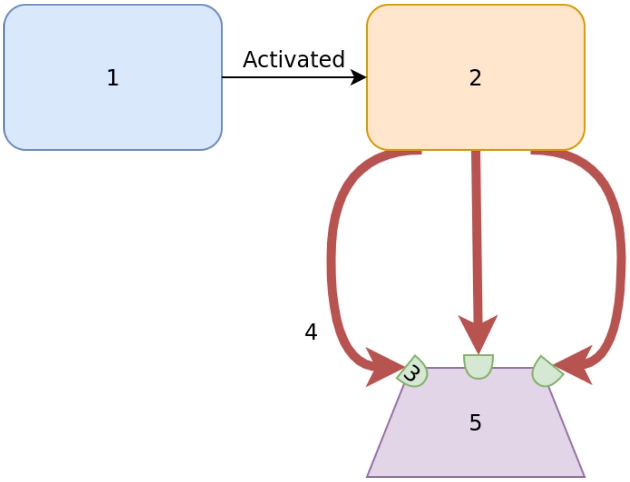

Figure 1.1

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

3 User Authentication

4 Authentication Protocols and Key Establishment

5 Operating Systems Security and Access Control

6 Software Security – Privilege and Escalation

7 Malicious Software

8 Public Key Certificate Management and Use Cases

9 Web and Browser Security

10 Firewalls and Tunnels

11 Intrusion Detection and Network-Based Attacks

Part II

Notes

1 Basic Concepts and Principles

2 Cryptographic Building Blocks

3 User Authentication

4 Authentication Protocols and Key Establishment

5 Operating Systems Security and Access Control

6 Software Security – Privilege and Escalation

7 Malicious Software

8 Public Key Certificate Management and Use Cases

9 Web and Browser Security

10 Firewalls and Tunnels

11 Intrusion Detection and Network-Based Attacks