

COMP4108 Final Exam Practice

William Findlay

December 13, 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	4
3 User Authentication	4
4 Authentication Protocols and Key Establishment	4
5 Operating Systems Security and Access Control	4
6 Software Security – Privilege and Escalation	4
7 Malicious Software	4
8 Public Key Certificate Management and Use Cases	4
9 Web and Browser Security	4
10 Firewalls and Tunnels	4
11 Intrusion Detection and Network-Based Attacks	4
II Notes	5
1 Basic Concepts and Principles	5
2 Cryptographic Building Blocks	5
3 User Authentication	5
4 Authentication Protocols and Key Establishment	5
5 Operating Systems Security and Access Control	5
6 Software Security – Privilege and Escalation	5
7 Malicious Software	5

8	Public Key Certificate Management and Use Cases	5
9	Web and Browser Security	5
10	Firewalls and Tunnels	5
11	Intrusion Detection and Network-Based Attacks	5

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

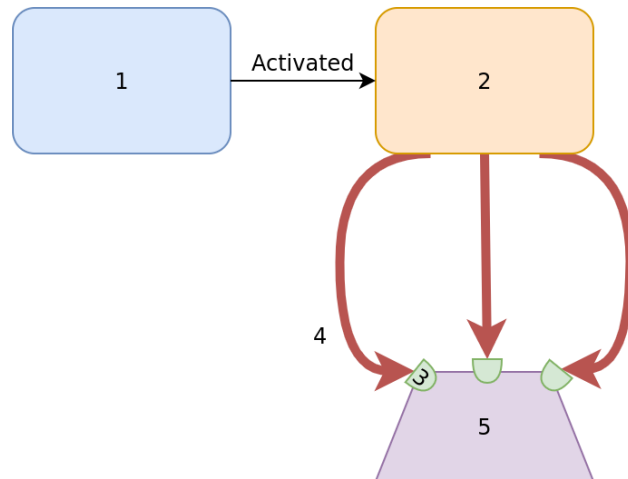
2. Briefly explain how repudiation violates accountability.

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

- 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