

# COMP4108 Final Exam Practice

*William Findlay*

*December 13, 2019*

# Contents

<b>1 Preamble</b>	<b>1</b>
1.1 Textbook . . . . .	1
1.2 General . . . . .	1
 <b>I Mock Exam</b>	 <b>1</b>
1 Basic Concepts and Principles	1
2 Cryptographic Building Blocks	2
3 User Authentication	2
4 Authentication Protocols and Key Establishment	2
5 Operating Systems Security and Access Control	2
6 Software Security – Privilege and Escalation	2
7 Malicious Software	2
8 Public Key Certificate Management and Use Cases	2
9 Web and Browser Security	2
10 Firewalls and Tunnels	2
11 Intrusion Detection and Network-Based Attacks	2
 <b>II Notes</b>	 <b>3</b>
1 Basic Concepts and Principles	3
2 Cryptographic Building Blocks	3
3 User Authentication	3
4 Authentication Protocols and Key Establishment	3
5 Operating Systems Security and Access Control	3
6 Software Security – Privilege and Escalation	3
7 Malicious Software	3

<b>8</b>	<b>Public Key Certificate Management and Use Cases</b>	<b>3</b>
<b>9</b>	<b>Web and Browser Security</b>	<b>3</b>
<b>10</b>	<b>Firewalls and Tunnels</b>	<b>3</b>
<b>11</b>	<b>Intrusion Detection and Network-Based Attacks</b>	<b>3</b>

## 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*.

## 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