

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	12
4 Authentication Protocols and Key Establishment	22
5 Operating Systems Security and Access Control	22
6 Software Security – Privilege and Escalation	22
7 Malicious Software	22
8 Public Key Certificate Management and Use Cases	22
9 Web and Browser Security	27
10 Firewalls and Tunnels	27
11 Intrusion Detection and Network-Based Attacks	27
 II Notes	 28
1 Basic Concepts and Principles	28
2 Cryptographic Building Blocks	28
3 User Authentication	28
4 Authentication Protocols and Key Establishment	28
5 Operating Systems Security and Access Control	28
6 Software Security – Privilege and Escalation	28
7 Malicious Software	28

8	Public Key Certificate Management and Use Cases	28
9	Web and Browser Security	28
10	Firewalls and Tunnels	28
11	Intrusion Detection and Network-Based Attacks	28

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

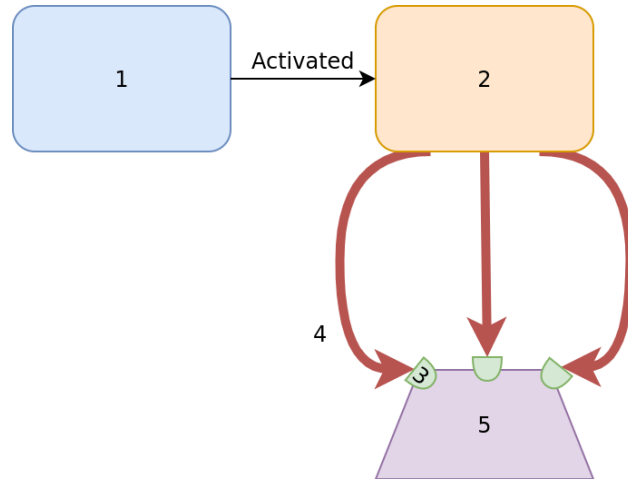


Figure 1.1

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. Describe each of the following properties of cryptographic hash functions.

a) Preimage resistance

b) Second preimage resistance

c) Collision resistance

37. How are hash functions used for password storage and verification? What property or properties of hash functions make this a desirable use case?

38. Is it generally better to MAC then encrypt, or encrypt then MAC?

3 User Authentication

39. Describe each of the following ways to defeat password authentication. For each technique you describe, provide one way to prevent it.

- a) Online guessing
- b) Offline guessing
- c) Defeating password recovery
- d) Bypassing authentication interface
- e) Password capture

40. Describe 3 advantages of passwords. Describe 3 disadvantages.

41. What is a password hash salt? A pepper?

42. What is iterated hashing? What is it used for? How does it compare with other techniques to solve the same problem?

43. Explain the following:

a) Dictionary attack

b) Mangling rules

44. Describe the trade-off that occurs when using system-assigned passwords. How do these passwords help to mitigate dictionary attacks

45. Suppose you had a password scheme that has an alphabet of size b and allows passwords as long as n characters. How long would it take to brute force passwords in this scheme in:

a) The worst case?

b) The average case?

46. Consider $q = GT/R$. What does this equation describe? What is each variable for?

47. Draw password distributions in Figure 3.1 according to the captions.

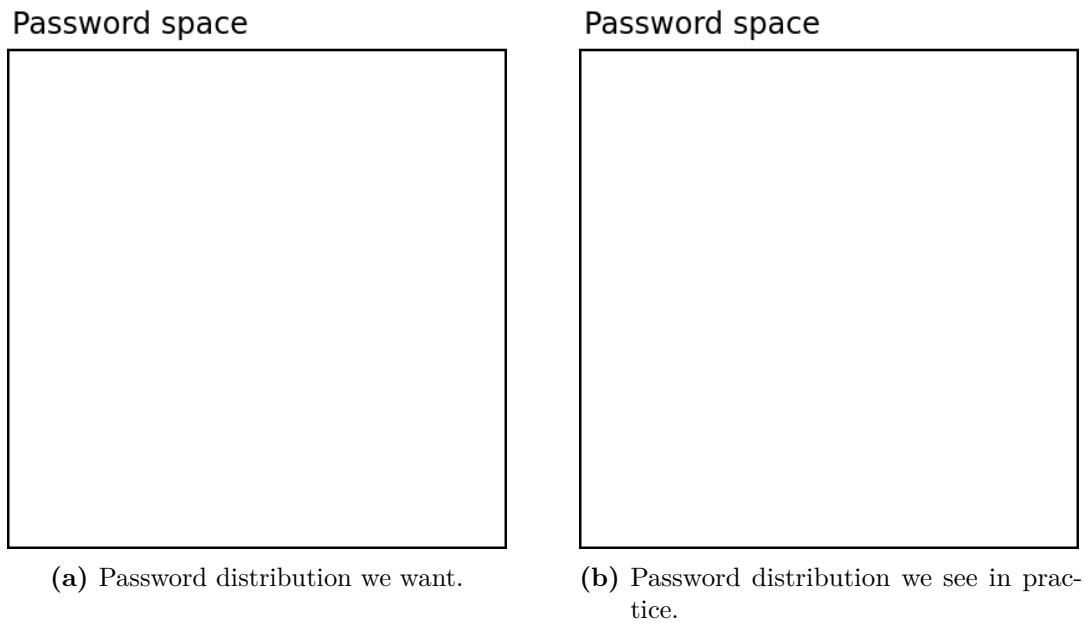


Figure 3.1

48. Discuss rate limiting and password change policies with respect to online guessing attacks. How does $q = GT/R$ factor into making decisions regarding these policies?

49. Discuss the drawbacks of complex site login password composition policies. Suggest at least three better alternatives.

50. What is a passkey? Why are complex passwords preferred for passkeys? How can passphrases help with usability issues associated with these complex passwords?

51. How can password blacklisting be used to reduce the effectiveness of dictionary attacks?

52. Why are secret questions generally a terrible method for password recovery? Why do you think they are so widely used despite their drawbacks?

53. What is a one-time password? How can a Lamport Hash Chain be used to extend a single key word to t one-time passwords?

54. Explain how Lamport Hash Chains are vulnerable to a man-in-the-middle attack using small $n = t - i$.

55. Describe the following categories of authentication and provide an example for each:

a) What you have

b) What you are

c) What you know

d) Where you are

56. What is multi-factor authentication?

57. Describe some advantages and disadvantages of hardware token authentication.

58. Give an example of each of the following modalities with respect to biometric authentication:

a) Physical

b) Behavioral

c) Mixed

59. Biometrics are secrets.

a) True

b) False

60. Biometric authentication to a remote site via a phone sends your biometric signature for authentication.

a) True

b) False

61. Is it better to have a higher false acceptance rate or false rejection rate? Make an argument using the definitions of each.

62. Draw a bimodal distribution with a higher false acceptance rate than false rejection rate. Clearly define where your t is located with a straight line.

- 21

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

67. What is a distinguished name? What does it do?

68. What is a public key certificate? What does it do? What trusted third party does it rely on?

69. Which of the following is generally preferred?

- a) An entity sends a public key in their certification request
- b) An entity sends a certification request and the CA generates their key pair
- c) These are equivalent

70. What does a PKI do? Give one example of a PKI and how it is used in practice.

71. What is X509 used for? What does it specify?

72. What is a certificate chain? Why are they necessary?
73. What part of a certificate chain requires implicit trust? What part(s) is expected to sign its own certificate?
74. What happens if part of a certificate chain is broken?
75. What is an out-of-band channel? What do we use them for when checking certificate integrity?
76. Why is allowing users to manually trust certificates not always the best idea? Why do browsers do it anyway?
77. Consider Trust-On-First-Use under the following circumstances. What is the result in each case?
- a) An attacker has replaced a self-signed certificate with their own
 - b) The self-signed certificate is legitimate

78. Suppose you tried to browse a site with an X509v3 certificate that had 4 extension fields, one marked critical, the other three non-critical. What would happen in the following scenarios (assuming the rest of the certificate is fine)?

- a) You have an older browser that cannot handle the critical extensions
- b) You have an older browser that cannot handle one of the non-critical extensions
- c) You have an older browser that cannot handle any of the non-critical extensions

79. Draw a picture of a cross certificate between two hierarchies. Describe one use case for cross certificates.

80. Consider the difference between *trust* and *trustworthiness*. What does a certificate trust model provide with respect to these terms?

81. Label (a), (b), and (c) in Figure 8.1 with the correct label from the following choices:

- a) Ring mesh
- b) Bridge CA model
- c) Separate domains

82. Circle the trust anchor(s) for the right-most leaves in each diagram in Figure 8.1.

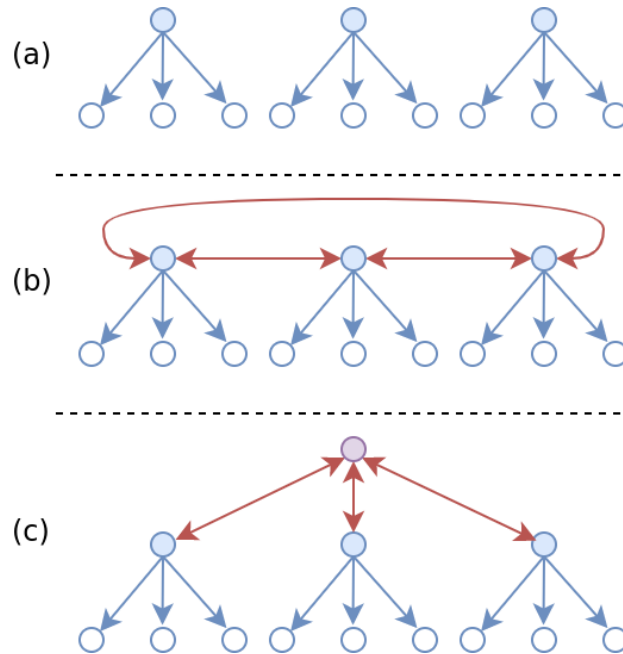


Figure 8.1

83. What are the leaf nodes in the browser trust model for CAs?

84. For each label in Figure 8.2, decide which of the following terms suits it best.

- a) Browser trust model
- b) Strict CA hierarchy model
- c) Enterprise PKI model

85. Circle the trust anchor(s) for the right-most leaves in each diagram in Figure 8.2.

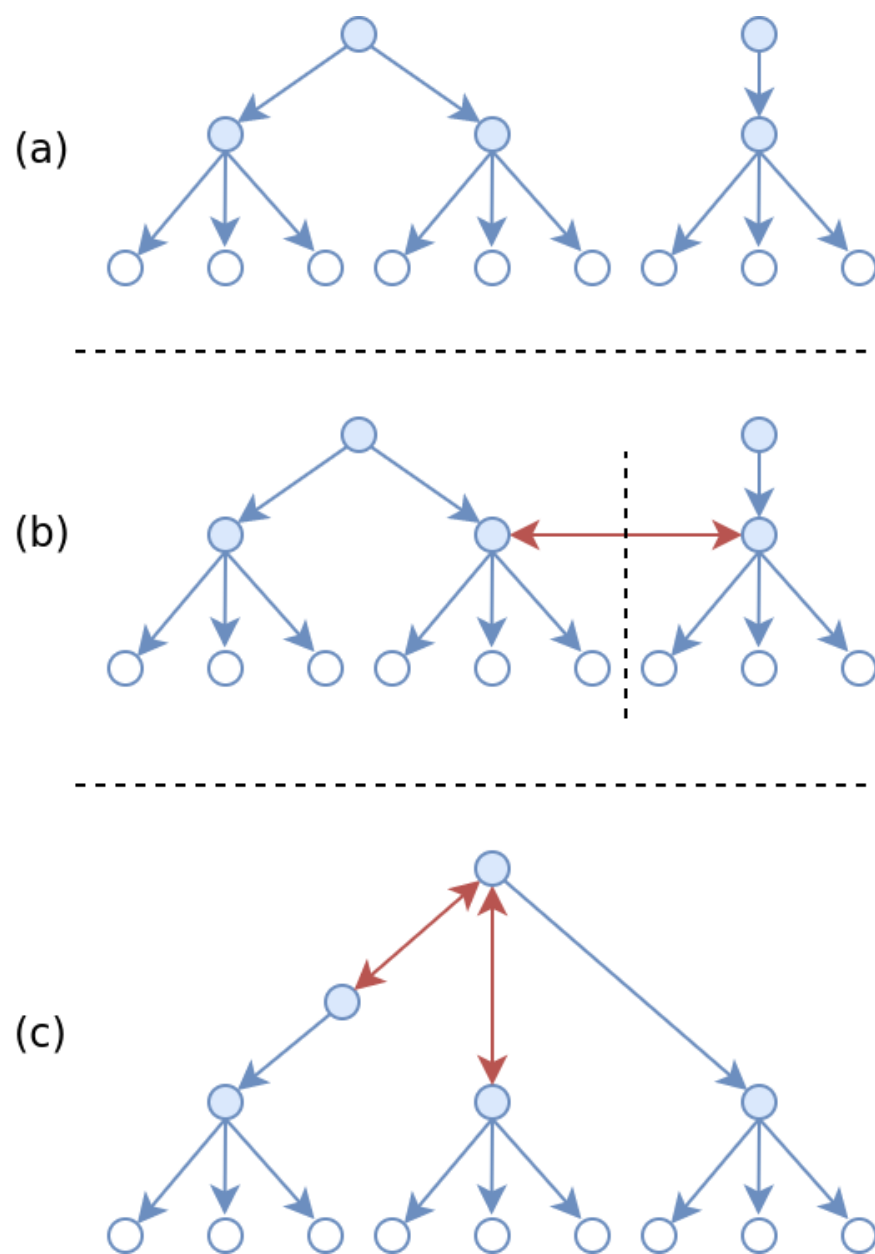


Figure 8.2

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