Total points: 80

Simon Fraser University
CMPT 403
Final exam

Date:	10th August, 2022
Time:	7 PM to 9 PM
Duration:	120 minutes
Final page number:	5

Name: ____

Student ID: ____

1. Write your name and student ID (number) in the space above.
2. Circle the correct answer.

Solution: THIS IS THE ANSWER KEY.

. (1) Which of the following is the best way to defeat a teardrop attack?

A. Ingress/egress filtering

B. Deep packet inspection

C. VPNs

D. Tor

(2) In the original Bell-LaPadula model (without water mark), suppose there are three security levels, High > Medium > Low, and three entities, Alice, Bob and Carol. The following four actions are taken, but some are blocked by the model:

1 Alice reads file X. (SUCCESS)

2 Bob reads file X. (BLOCKED)

3 Bob writes to file Y. (BLOCKED)

4 Carol writes to file Y. (BLOCKED)

Which of the following can we conclude?

A. Carol has security level Medium.

B. Alice, Bob and Carol all have different security levels.

C. Alice's security level is at least as high as Carol's.

D. Bob has security level Low.

(3) Continuing the above, in the Bell-LaPadula high water mark model, which of the above actions would NOT be blocked?

A. 2, 3, and 4.

B. 3 and 4.

C. 4.

D. 2 and 3.

(4) "Let's Encrypt" increased the adoption rate of TLS significantly. Which cost of using TLS did it decrease to achieve this?

A. Computational cost of generating TLS keys

B. Monetary cost of obtaining TLS certificates

C. Communication (data) cost of TLS public key infrastructure

D. Time cost of TLS encryption

(5) Which of the following threats does DNSSEC defend against?

A. A Man-in-the-Middle attacker changes DNS responses.

B. Queries are intercepted by a eavesdropping attacker to compromise privacy.

C. An attacker compromises an authoritative resolver and falsifies responses.

D. An authoritative resolver chooses to lie when responding to DNS queries.

(6) Which of the following is not a valid use of secure multi-party computation?

A. Alice wants to know if a book is available at the library; her book title is private information. Bob has the library records. Alice inputs the book title and Bob inputs the records.

B. Alice wants to know know the racial composition at Bob's company; racial composition is private information. Bob has the relevant demographic data. Alice inputs her query and Bob inputs the demographic data.

C. Alice wants to know if she has a higher IQ than Bob; their IQs are private information. They both take IQ tests and input the results of those tests.

D. Alice wants to know the calorie content of what she ate today; what she ate today is private information. Bob has a data set of the calorie content of food. Alice inputs her diet and Bob inputs his data set.

(7) In the low-water mark Biba integrity model, a low security subject could read a high security object. This is because:

A. This model does not care about the leakage of confidential information.

B. Such an action is allowed if the subject has acquired permission from a high security subject.

C. The subject's security level should then be increased to high.

D. The object's security level should then be decreased to low.

(8) A worm uses a zero-day attack to infiltrate critical enterprise servers. Of the following, the best defense against it is:

A. Host-based intrusion detection.

B. Ingress filtering.

C. Deep packet inspection.

D. Stateless packet filtering.

(9) Which of the following best describes the vulnerability that caused the ping of death attack?

A. No authentication of IP

B. Open services being leveraged for amplification attacks

C. The lack of ingress/egress filtering in networks

D. An unintentional programming error

(10) If you search for something on a search site (with TLS) through Tor,

A. The exit relay can see the search site but not the search query.

B. The exit relay can see the search query but not the search site.

C. No relay will see the search site or the search query.

D. The entry and exit relay can both see the search site and the search query.

(11) If you use Tor on an unencrypted wireless router,

A. It is not possible to use Tor on an unencrypted wireless router.

B. The router and any nearby eavesdropper can see what sites you are visiting.

C. The router and any nearby eavesdropper can see you are using Tor.

D. The router and any nearby eavesdropper can capture the keys you negotiate with Tor relays.

(12) Which of the following attacks does not benefit from IP spoofing?

A. Teardrop attack.

B. NTP Amplification attack.

C. Smurf attack.

D. Impersonating a website.

(13) The main advantage of Tor compared to VPNs is:

A. Tor offers more bandwidth as it has a bigger network.

B. VPNs use volunteer nodes who may be potential attackers.

C. VPNs are potential eavesdroppers.

D. Tor can defend against deep packet inspection from ISPs.

(14) The use of a Public Key Infrastructure solves the following problem:

A. How can Alice and Bob avoid man-in-the-middle integrity attacks on data transmission?

B. How can we establish a secure channel between Alice and Bob?

C. Given Bob's public key, how can Alice know it truly belongs to Bob?

D. How can we deliver public keys to Alice in a data efficient manner?

(15) Which of the following is a correct statement about differential privacy?

A. We can make a data set differentially private by adding noise to its elements.

B. To collect data with differential privacy, each participant adds noise to their own data before submitting it.

C. Generally, the more people there are in the data set, the more noise we have to add to the query response.

D. The amount of noise to be added depends on the data set.

Solution:
B, C, B, B, A,
B, A, A, D, A,
C, A, C, C, B