LAST NAME: _____

FIRST NAME: _____

UCID: _____

CPSC 526
Practice Midterm Examination

Instructor: Prof. Reardon

True or False

Each of these questions is worth two points. A wrong answer or an empty answer is worth zero points. A correct answer is worth one point and a correct explanation is worth one point.

1. (2 points) The main reason we use CRL deltas because CRL will only ever grow in size.

2. (2 points) TLS requires the server to present a certificate to the client.

3. (2 points) Suppose that x is a binary string generated from a truly random source, and y is the bitwise negation of x (e.g., if $x = 1001$ then $y = 0110$.) Then $x \oplus y$ is a cryptographically suitable source of randomness.

Multiple Choice

Each correct answer is worth two points. Each unanswered question or incorrectly answered question is worth zero points. You may include an explanation in your response. This explanation will not be marked, but if compelling may be used to give points to an otherwise wrong answer.

4. (2 points) Consider the output of AES in ECB mode as a PRNG. Suppose it uses both a truly random key. This provides:

   (a) neither rollback resistance nor prediction resistance

   (b) only rollback resistance (not prediction resistance)

   (c) only prediction resistance (not rollback resistance)

   (d) both rollback resistance and prediction resistance

   (e) insufficient information in description to determine or the PRNG cannot be practically implemented

5. (2 points) Consider the following PRNG. The initial state is a 256 bit truly random number. Each time it emits randomness, it outputs the SHA256 hash of the current number and then updates the state by incrementing the number.

   (a) neither rollback resistance nor prediction resistance

   (b) only rollback resistance (not prediction resistance)

   (c) only prediction resistance (not rollback resistance)

   (d) both rollback resistance and prediction resistance

   (e) insufficient information in description to determine or the PRNG cannot be practically implemented

6. (2 points) Let m be a 1024-byte message encrypted with AES-CTR with a 256-bit key K using a random nonce (IV) to produce a cipher-text C. If someone with K, C, and the nonce tries to decrypt it, but a single bit is flipped in the the nonce. What is the result:

   (a) the full message m is decrypted

   (b) none of the message m is decrypted

   (c) a single bit in m is flipped, but the rest is fine

   (d) a single block of the message m is garbled, but the rest is fine

   (e) multiple blocks of the message m are garbled, but the rest is fine

7. (2 points) Suppose a 4-byte message is encrypted using 128-bit AES in CTR mode. How many bytes will be the ciphertext and—if used by this ciphermode—the IV or nonce?

   (a) 4 bytes

   (b) 8 bytes

(c) 16 bytes

(d) 20 bytes

(e) none of the above

8. (2 points) Which of the following best describes reflection attack?

(a) Alice sends Bob a message Alice sent Bob before.

(b) Bob sends Alice a message Alice sent Bob before.

(c) Eve sends Bob a message Bob sent Alice before.

(d) Eve sends Alice a message Bob sent Alice before.

(e) Alice sends Alice a message Bob sent Alice before.

9. (2 points) A cryptographically secure pseudo-random number generator uses the SHA256 hash of the current time in nanoseconds as a seed. What type of randomness is the output?

(a) non-cryptographically suitable pseudorandomness

(b) cryptographically suitable pseudorandomness

(c) non-cryptographically suitable true randomness

(d) cryptographically suitable true randomness

(e) none of the above

10. (2 points) What is a security feature of short-lived certs relative to its alternatives?

(a) they don't expire

(b) they are easier to get

(c) they don't require active communication to revoke

(d) they can be checked with an OCSP if they are valid

(e) none of the above

11. (2 points) Many people lock valuables in a safe in their house in addition to locking the doors of the house. *Mark one* security principle that is *most* relevant for this approach.

(a) evidence production

(b) defense in depth

(c) don't rely on security through obscurity

(d) privilege separation

(e) least surprise

12. (2 points) Which of the following can an active man-in-the-middle attacker not do?

(a) read data

(b) modify data

(c) inject data

(d) delete data

(e) none of the above

13. (2 points) What is meant by neutralization of HTTPS

(a) making HTTPS normal and HTTP abnormal

(b) making HTTPS more clear to users

(c) removing the lock icon for HTTPS

(d) adding more security indicators for HTTPS

(e) removing browser warnings for self-signed certs

14. (2 points) Eve and Alice both work at the same company, and Eve convinces Alice to let her do something quick on her computer. What security principle is relevant here?

    (a) separation of privilege

    (b) open design

    (c) complete mediation

    (d) reluctant allocation

    (e) none of the above

15. (2 points) In the context of Kerberos to access services, what purpose is served by the user's password?

    (a) to prove that the user has authenticated

    (b) to derive a key to decrypt messages from the ticket granting service

    (c) to derive a key to decrypt a message containing the ticket granting ticket

    (d) to login to the authentication server

    (e) none of the above

Written Answers

Be sure to explain your answers in detail for this section and write in complete sentences.

16. (15 points) Consider a stock trading account that does not allow users to remove cash from the account or transfer cash among accounts to prevent an attacker who logs in as the user from stealing money. The only way to withdraw money is to show government-issued identification in person.

    (a) (3 points) What is the security policy?

    (b) (3 points) What is the security mechanism?

    (c) (3 points) What is the threat as it relates to the policy?

    Now consider the following attack: an attacker manages to get a user's password, e.g., it was easy to guess, and signs in to their account. The attacker then buys many shares of a thinly traded stock, thus driving up the price. The attacker already owns shares of that stock, and so sells it at the higher price making a profit on the attacker's account. The victim is left holding shares they bought at an artificially higher price and will have to sell at a loss.

    (d) (3 points) What is the vulnerability as it relates to the policy?

    (e) (3 points) What assumptions is made by the security mechanism that causes that vulnerability?

17. (14 points) Assume that Alice (A) and Bob (B) both use symmetric key cryptography. They both know a random password p fixed ahead of time and use that to derive a key k.

    Alice and Bob established a shared symmetric session key using the following protocol:

    1. $A \to B : \{A, N\}_k$
    2. $B \to A : \{N - 1\}_k$
    3. $A \to B : \{p\}_{N \oplus k}$

    In the above, $\{M\}_x$ means the message M is sent encrypted with the key x, and $\oplus$ denotes the bitwise binary XOR operation. Suppose that all passwords, keys, and nonces are large enough to be un-brute-forceable.

    In step 1, Alice generates a random nonce N and sends it to Bob along with Alice's identity, encrypted with the password-derived key. In step 2, Bob subtracts one from the nonce and sends the result encrypted to Alice with the same password-derived key. They then both compute $N \oplus k$ and use it as a key for the final message, which is Alice proving to Bob she knows the key by sending their shared password.

(a) (2 points) What is/are long-term key/keys in this protocol?

(b) (2 points) What is/are short-term key/keys in this protocol?

(c) (5 points) Suppose that an adversary learns N and $\{A, N\}_k$. Can they use that to successfully authenticate to Bob? Explain why or why not?

(d) (5 points) Suppose a network attacker can eavesdrop on communication and at one point learns a session key for a particular session. Describe an attack they can do on other sessions.

18. (5 points) How does SSL/TLS protect against a network eavesdropper who records all of the server's messages in an SSL handshake and later impersonates the server to the client by replaying the recorded messages from the previous session back to a client.