COMP3334 Computer Systems Security

Semester 2, 2023/2024, Section 1

March 27, 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. Among the following, which cryptographic hash function is the most recommended to use as of today for password hashing? (1 pt)
   A. scrypt
   B. SHA3
   C. Diffie–Hellman
   D. HMAC

2. What is the purpose of password *salts*? (1 pt)
   A. Pad the password to a multiple of the length of a block
   B. Hide the password length from an attacker
   C. Make password cracking more difficult
   D. Accelerate the speed of password hashing

3. What is a password-strength meter? (1 pt)
   A. A password recovery tool
   B. A tool to evaluate the strength of user passwords
   C. A type of password-specific cryptographic hash function
   D. A hardware device that allows users to authenticate themselves

4. In the generation of Rainbow tables, the *reduce* operation aims to: (1 pt)
   A. Convert a hash value into a password
   B. Convert a password into a hash value
   C. Reduce the time it takes to crack a password
   D. Reduce the space of possible passwords

5. Which of the following is NOT an application of public-key cryptography? (1 pt)
   A. Digital signature
   B. Password hashing
   C. Decryption
   D. Key exchange

6. What is a FIDO2 security key used for? (1 pt)
   A. To encrypt data stored on a computer
   B. To authenticate a user during a login process
   C. To protect a computer from viruses and malware
   D. To secure a wireless network

(turn to next page)

Short Answer Questions [10 pts]

7. In public-key encryption, which key is used to *encrypt* the ciphertext? (1 pt)

Public key ← decrypt → private key

8. Express how a HOTP is calculated, and define the parameters involved. (1 pt)

$HOTP(K, C) = HMAC_K(C)$

K: Pre-shared key, C: Counter

9. In the context of compromising user accounts, what is an *offline* guessing attack? (1 pt)

The attacker breached/stole a database including password hashes, and tries to recover passwords from the hashes.
~~Optional: without interacting with the server anymore~~
Optional: typically by running password recovery tools such as hashcat.

10. Give one disadvantage of OTP (one-time passwords). (1 pt)

Does not prevent phishing, plaintext code is displayed to the user and needs to be typed manually, OTP is vulnerable to MITM attacks, the shared secret is stored on the server...

11. Express the entropy (in bits) of a random 7-digit password. (1 pt)

$\log_2(10^7)$ → 8-digit → $\log_2(10^8)$

12. Give one example of a rate-limiting mechanism to prevent online guessing attacks. (1 pt)

CAPTCHA, block IP address, lockout account

(turn to next page)

13. Based on your reading of the textbook *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin* (2nd ed.) by Van Oorschot, P. C. (2021), Chapter 2: "Cryptographic Building Blocks," what main advantage does elliptic curve cryptography (ECC) offer compared to integer factorization cryptography (IFC) and finite field cryptography (FFC)? (2 pts)

ECC is easier to compute (computational efficiency)

ECC has smaller keys

14. Explain the danger of not authenticating keys for communications that are encrypted using public-key cryptography. (2 pts)

Man-in-the-middle attacker can swap someone's public key for his own, then

get encrypted communications to himself so he can decrypt the communication.