CORRECTED

EPFL

1

Teacher: Prof. Dr. ETH Mathias Payer
COM-402 Information Security and Privacy – Quiz 01
7th October 2024
Duration: 15 minutes

Anon Ymous

SCIPER : **999999**

Do not turn the page before the start of the quiz. This document is double-sided, has 4 pages, the last ones possibly blank. Do not unstaple.

- **No other paper materials** are allowed to be used during the quiz.
- Using a **calculator** or any electronic device is not permitted during the quiz.
- For each question, mark the box(es) corresponding to the correct answer(s). Each question has **one or more** correct answers.
- For each question, we give:
  3 points by default,
  0 points if you give no answer,
  −1 point per incorrectly checked or missed answer.
  Each question has a minimum of 0 points, we do not award negative points.
- Use a **black or dark blue ballpen** and clearly erase with **correction fluid** if necessary.
- If a question is wrong, we may decide to nullify it.

Respectez les consignes suivantes | Observe this guidelines | Beachten Sie bitte die unten stehenden Richtlinien		
choisir une réponse | select an answer Antwort auswählen	ne PAS choisir une réponse | NOT select an answer NICHT Antwort auswählen	Corriger une réponse | Correct an answer Antwort korrigieren
☒ ☑ ■	☐	☐ ▭
ce qu'il ne faut **PAS** faire | what should **NOT** be done | was man **NICHT** tun sollte		
▨ ☒ ▢ · ▨ ▢		

CORRECTED

Question 1
As discussed in the exercise sessions, which of the following are possible attacks for textbook RSA?

- [x] When given access to plaintexts of ciphertexts of its choice, the adversary can recover the plaintext of any ciphertext.
- [x] When given access to ciphertexts of plaintexts of its choice, the adversary is able to guess which plaintexts out of two was the one that was encrypted.
- [ ] When given two ciphertexts of the same plaintext encrypted via RSA with public keys (n_1, e) and (n_2, e) respectively, where n_1 and n_2 are coprime, the adversary can recover the plaintext.

Explanation:

- Correct: When given access to ciphertexts of plaintexts of its choice, the adversary is able to guess which plaintexts out of two was the one that was encrypted.
- Wrong: When given two ciphertexts of the same message, the adversary can recover the message
- Correct: When given access to plaintexts of ciphertexts of its choice, the adversary can recover the plaintext of any ciphertext.

The first, second and third are from demos in the first exercise session. For second point, to perform Håstad's broadcast attack, the number of ciphertexts needed has to be at least the RSA public exponent. For fourth and fifth point, padding with random string is not enough using generalization of Håstad's broadcast attack, however, randomized padding such as OAEP prevents these type of attacks.

Question 2
Which of the following statements regarding Kerberos is/are true?

- [ ] The TGS grants the user ticket granting ticket for authentication.
- [ ] The AS grants the user session ticket to specific services.
- [x] The key innovation of Kerberos is delegated authentication, users can authenticate once and access multiple services.
- [x] OAUTH2 extends Kerberos' idea of delegated authentication to Internet services.

Explanation: The roles of AS and TGS are reversed. AS grants the user the ticket granting ticket for authentication. And the TGS grants the service-specific tickets.

Question 3
Which of the following statements about symmetric crypto is / are correct?

- [ ] Encryption and decryption are done with separate keys.
- [x] TLS uses both symmetric and asymmetric crypto at the same time.
- [x] Symmetric crypto is faster than asymmetric crypto.
- [x] Encryption and decryption are done with the same key.
- [ ] The WPA3 protocol is based on symmetric crypto.

Explanation: In symmetric crypto encryption and decryption handled with the same key. Kerberos is a symmetric crypto protocol while WPA3 is an asymmetric one.

Corrected

Question 4
In a CBC mode of operation encryption scheme, what happens to decryption if a bit is flipped in one of the ciphertext blocks due to a transmission error?

- ☐ Only one bit will be corrupted.
- ☐ The relevant block and all the following ones are corrupted.
- ☐ Only one block is corrupted, and unless there is an integrity check, the decryptor will not realize.
- ■ Only two blocks are corrupted.
- ☐ Only one block is corrupted, and the decryptor can realize even without integrity checks.

Explanation: Since XORing is done on the ciphertext, only one block and it's direct follower are corrupted

Question 5
Which of the following are valid authentication factors in a 2FA system?

- ■ Google Authenticator TOTP
- ■ FaceID
- ■ Yubikey hardware token
- ■ Password
- ■ Single-use code via email

Explanation: All the factors are something you know, something you own, something you are.

Question 6
Which of the following statements about the liblzma backdoor are true?

- ☐ Some components of the backdoor were deliberately introduced inside the OpenSSH source code
- ☐ The backdoor did not have any negative performance impact, making it impossible to detect via performance testing
- ■ An attacker exploiting the backdoor can get root access to any machine running an OpenSSH server where a vulnerable version of liblzma is present and loaded by OpenSSH
- ☐ Andreas Freund accidentally found the backdoor via a fuzzing campaign on OpenSSH

Explanation: the backdoor was self-contained in liblzma, and was found through performance testing by Andreas Freund because it had a negative performance impact on OpenSSH.

CORRECTED

Question 7
In an assumed secure asymmetric cryptosystem, hashing the message using SHA-256 and then encrypting the concatenation of the message and the hash with the recipient's public key provides...

- [x] Confidentiality
- [ ] Authenticity
- [ ] Availability
- [ ] Non-repudiation
- [x] Integrity

Explanation:

- Confidentiality: message is encrypted
- Integrity: appended (and encrypted) hash ensures the message cannot be tampered with
- Availability: neither hashing nor encrypting ensures availability if an attacker can drop the message in transit
- Authenticity and non-repudiation: the message is not signed by the original author, the source of the message can therefore not be verified.

Question 8
Which of the following statements about exploits is correct?

- [x] An exploit is the weaponization of an underlying vulnerablity.
- [x] Isolating a system may be a viable alternative to patching the system if no patch is available yet.
- [ ] All malware requires a software-based exploit to be installed.
- [ ] 0-day exploits are exploits for which a patch exists but the patch has not been deployed everywhere.

Explanation:

- 0-day are exploits without patches.
- Malware does not necessarily need to rely on exploiting a vulnerability but
- could be installed through phishing.
- true
- If no patch is available and a service is essential then it must be isolated as a fallback until a patch is available.

Question 9
When connecting to a website for the first time, your connection...

- [x] cannot be MITMed if the website is on the HSTS-preload list
- [ ] cannot be MITMed if the website uses TLS
- [ ] cannot be MITMed if the website uses TLS and HSTS
- [ ] cannot be MITMed if the website uses IPv6

Explanation: Only HSTS-preload ensures an authenticated TLS connection from the start. Without HSTS-preload, an attacker can downgrade the connection to a pure HTTP connection on the first connection and intercept traffic.

CORRECTED

Question 10

Suppose a computer system is setup to use a new hypothetical filesystem, *MACfs*, which exclusively uses Mandatory Access Control (MAC) to determine which users have what access to which files. There are 3 users in *MACfs*. They (and their files) are split in 3 corresponding "security" levels (from least to most secret): Alice (unclassified), Bob (classified), and Charlie (secret). Which of the following statements are true?

- ☐ When configured to ensure **both** Confidentiality and Integrity, Charlie can modify the files of Alice.
- ■ When configured to ensure Confidentiality **only**, Alice can modify the files of Bob.
- ■ When configured to ensure Integrity **only**, Charlie can modify the files of Alice.
- ■ When configured to ensure **both** Confidentiality and Integrity, Bob can read the files of Alice.
- ☐ When configured to ensure Confidentiality **only**, Bob can read the files of Charlie.

Explanation: In Mandatory Access Control, confidentiality is ensured by having a "no write-down" policy – users from higher levels are not allowed to write to lower levels. Integrity is ensured by having a "no write-up" policy – lower levels are not allowed to write to higher levels. In both cases, higher levels can always read files of lower levels, whereas lower levels can never read files of upper levels.