Thomas Jun Wei Lim (username: tjwlim)

Attempt 4

Written: Feb 7, 2017 1:34 PM - Feb 7, 2017 1:35 PM

Submission View

Your quiz has been submitted successfully.

🛑 **Information**

Choose the best answer.

Questions

Question 1   **1 / 1 point**

Think of a capability as a (digital) ticket that is handed out to a user (i.e., a process running on behalf of the user) and that the user has to present when accessing a resource. Assuming there are ways to detect ticket tampering, which of the following scenarios are still difficult to implement with capabilities?

1. Time-limited access to the resource
2. One-time access to the resource
3. Immediate withdrawal of access to the resource

○ 1, 2, and 3

○ 1 and 2

◉ 2 and 3

○ 3

〉 View Feedback

Question 2   **1 / 1 point**

When invoking an application to change their password, users are typically asked to enter their old password first, even when they have already logged in. Without this step, which of the following principles would be violated?

1. Check every access
2. Enforce least privilege
3. Verify acceptable use

○ 1, 2, and 3

○ 1 and 2

○ 2 and 3

◉ 1

〉 View Feedback

Question 3   **1 / 1 point**

Instead of running a separate application to change passwords, a user could become superuser and directly modify the file or database that stores password information. Which of the following design principles does this approach violate?

1. Check every access
2. Enforce least privilege

3. Verify acceptable use

⊙ 1, 2, and 3

◯ 1 and 2

◯ 2 and 3

◯ 1

> View Feedback

Question 4   1 / 1 point

Defending against password-guessing attacks by limiting the number of attempts that a user is given to enter the correct password can result in

◯ Leakage of the password

⊙ Denial-of-service attacks

◯ Unauthorized modifications to the password

> View Feedback

Question 5   1 / 1 point

If not carefully implemented, defending against loose-lipped systems by giving no information about the reason for being denied access can still result in

⊙ Leakage of sensitive information

◯ Denial-of-service attacks

◯ Unauthorized modifications to sensitive information

> View Feedback

Question 6   1 / 1 point

Which of the following physical authentication tokens are (typically) useful defenses against impersonation attacks?

◯ Police Badge

⊙ Driver's License

◯ Credit Card

> View Feedback

Question 7   1 / 1 point

Which of the following statements is correct?

○ Effective biometrics-based access control requires the presence of a guard (e.g., to prevent people from putting a finger made out of gelatin on a fingerprint scanner). Therefore, getting rid of biometrics-based access control and letting the guard control access directly is as effective.

○ By salting passwords, a leaked password file becomes useless to an attacker.

◉ Access control based on storing a cryptographic hash of a password is more secure than access control based on storing an encrypted version of the password.

> View Feedback

Question 8   1 / 1 point

Which of the following statements is correct?

○ Paul, cleared for (Top Secret, {A, C}), can read a document classified (Secret, {B, C}).

○ It is useful to have compartments at the Unclassified level.

◉ Without integrity, no system can provide confidentiality.

○ Without confidentiality, no system can provide integrity.

> View Feedback

Question 9   1 / 1 point

Which of the following statements is correct?

○ The file access-control mechanism of the UNIX operating system is an example of mandatory access control.

◉ A military facility in which only generals can enter a particular room is an example of mandatory access control.

○ The Bell-LaPadula Model can emulate the Chinese Wall Model.

○ When Biba and Bell-LaPadula are combined and each object/subject is assigned only a single label, instead of one for confidentiality and one for integrity, a user cannot access any information.

> View Feedback

Question 10   1 / 1 point

Given n sensitivity/clearance levels and m compartments, how many labels does the complete lattice consist of?

○ n * m

◉ n * 2^m

○ n * m!

○ n! * m

> View Feedback

Question 11   1 / 1 point

Which of the following need to be part of the trusted computing base?

1. Reference Monitor
2. Logging Mechanism
3. I/O Device Driver

○ 1, 2 and 3

○ 2 and 3

◉ 1 and 2

○ 1 and 3

> View Feedback

Attempt Score: 11 / 1

Overall Grade (last attempt)**:**   11 / 1