Exercises
Authentication - Authorization

Computer Security

Question 1

We are designing the password policy for an online banking website. Which of the following rule sets is more adequate in your opinion, and why?

- Passwords must be at least 12 characters long, with at least one lowercase, one uppercase, one number and one special character. Passwords must be changed at least every 30 days and cannot match previous ones. Accounts are locked after 3 wrong attempts.
- Passwords must be at least 8 characters long, and not belong to a dictionary of common passwords. They must be changed at least every 30 days and cannot match previous ones. Accounts are locked after 5 wrong attempts.

Question 1

We are designing the password policy for an online banking website. Which of the following rule sets is more adequate in your opinion, and why?

- Passwords must be at least 12 characters long, with at least one lowercase, one uppercase, one number and one special character. Passwords must be changed at least every 30 days and cannot match previous ones. Accounts are locked after 3 wrong attempts.

Question 1

We are designing the password policy for an online banking website. Which of the following rule sets is more adequate in your opinion, and why?

- Passwords must be at least 12 characters long, with at least one lowercase, one uppercase, one number and one special character. Passwords must be changed at least every 30 days and cannot match previous ones. Accounts are locked after 3 wrong attempts.

This seems stronger, because it enforces long (against bruteforcing), non-reused (against stealing) passwords and mitigates bruteforcing. However, it will lead users to write down passwords.

Question 1

We are designing the password policy for an online banking website. Which of the following rule sets is more adequate in your opinion, and why?

- Passwords must be at least 8 characters long, and not belong to a dictionary of common passwords. They must be changed at least every 30 days and cannot match previous ones. Accounts are locked after 5 wrong attempts.

Question 1

We are designing the password policy for an online banking website. Which of the following rule sets is more adequate in your opinion, and why?

- Passwords must be at least 8 characters long, and not belong to a dictionary of common passwords. They must be changed at least every 30 days and cannot match previous ones. Accounts are locked after 5 wrong attempts.

This one has an additional measure (non dictionary words) that is missing in the previous scheme. Given that guessing is more likely than cracking, and that writing down passwords is a pitfall, this scheme is definitely better with respect to the previous one.

Question 2

Consider biometric authentication.

(2 points) Describe (a) how the authentication phase works and (b) explain the phases that are needed to deploy such an authentication system in a company.

Question 2

Consider biometric authentication.

(2 points) Describe (a) how the authentication phase works and (b) explain the phases that are needed to deploy such an authentication system in a company.

It is based on recording features extracted from a biometric characteristic of each user. At each authentication, the measured features are compared with the recorded ones. Each user is thus required to measure the characteristic when a system is deployed.

Question 2

Consider biometric authentication.

(3 points) The company is evaluating whether to use a fingerprint scanner or iris recognition as a characteristic for authentication purposes. What are the considerations that you would make?

Question 2

Consider biometric authentication.

(3 points) The company is evaluating whether to use a fingerprint scanner or iris recognition as a characteristic for authentication purposes. What are the considerations that you would make?

Fingerprint scanning and iris recognition are both very precise authentication methods. Fingerprint scanning is slightly easier to fool with counterfeits. Iris recognition is a more invasive procedure which may be less tolerable by users. Additionally, iris recognition is far more costly.

Question 3

Discuss the following statements related to authentication: are they true or false? And why?

A. Password authentication is widely used because it is weaker but cheaper

Question 3

Discuss the following statements related to authentication: are they true or false? And why?

A. Password authentication is widely used because it is weaker but cheaper

True, because it does not require special equipment, and it is even easier to deploy in many environments.

Question 3

A. Biometric systems are not deterministic, and this is an issue

Question 3

A. Biometric systems are not deterministic, and this is an issue

True, because the biometric features that they measure (e.g., fingerprints, hand geometry) may change over time, and measurement errors can occur. Thus, they need to be carefully evaluated for false acceptance and false rejection ratios.

Question 3

A. Biometric systems identify a person on the basis of their physical characteristics, making it impossible for an attacker to impersonate someone else

Question 3

A. Biometric systems identify a person on the basis of their physical characteristics, making it impossible for an attacker to impersonate someone else

False. Attacks have been developed against biometric systems. For example it is rather easy to duplicate someone's fingerprints.

Question 3

A. Introducing a biometric system to protect a high-value target will decrease risks for the target, often at the expense of increasing personal risk for the users

Question 3

A. Introducing a biometric system to protect a high-value target will decrease risks for the target, often at the expense of increasing personal risk for the users

True, if the system makes attacking a user the most viable way to access the high value target.

Question 4

What are the differences between MAC and DAC?

Make an example of real-world MAC system and at least one example of real-world DAC system.

Question 4

What are the differences between MAC and DAC?

Make an example of real-world MAC system and at least one example of real-world DAC system.

Key difference: in DAC owner assigns control over resource, in MAC security admin sets levels.

Example of MAC: classification of secret documents in the military.

Examples of DAC, you name it, any OS.

Question 5

What are the differences between access control lists and capability lists?

Question 5

What are the differences between access control lists and capability lists?

ACLs are efficient with per-object operations, but cannot be used to assign multiple owners to the same object (this can be partially addressed with groups). Capabilities are efficient with per-subject operations, which make them inefficient when objects change frequently.

The End