# Exercises
## Authentication

Computer Security

# Question

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.

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.

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.*

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.

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.*

Consider biometric authentication.

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?

Consider biometric authentication.

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.*

In a company, each employee has a private office, where only authorized people can enter. The workstation is positioned such that the computer screen faces the wall. Also assume that passwords are only used to access cloud-based services over TLS. We need to design proper policies to minimize the risk that passwords get compromised. Such policies will be enforced whenever a user chooses a new password.

What are the main characteristics of a password on which we can act when writing a policy?

In a company, each employee has a private office, where only authorized people can enter. The workstation is positioned such that the computer screen faces the wall. Also assume that passwords are only used to access cloud-based services over TLS. We need to design proper policies to minimize the risk that passwords get compromised. Such policies will be enforced whenever a user chooses a new password.

What are the main characteristics of a password on which we can act when writing a policy?

*Complexity = length, rich character set*
*Non guessability = not belonging to dictionaries, not user related*
*Frequency of change*

In a company, each employee has a private office, where only authorized people can enter. The workstation is positioned such that the computer screen faces the wall. Also assume that passwords are only used to access cloud-based services over TLS. We need to design proper policies to minimize the risk that passwords get compromised. Such policies will be enforced whenever a user chooses a new password.

What is the most likely attack scenario against passwords considering the above description of the conditions of each employee? Why?

In a company, each employee has a private office, where only authorized people can enter. The workstation is positioned such that the computer screen faces the wall. Also assume that passwords are only used to access cloud-based services over TLS. We need to design proper policies to minimize the risk that passwords get compromised. Such policies will be enforced whenever a user chooses a new password.

What is the most likely attack scenario against passwords considering the above description of the conditions of each employee? Why?

*Guessing, because the office space is confined and accessible only to authorized personnel. Cracking is the second most-likely attack. Snooping is certainly not an option here.*

In a company, each employee has a private office, where only authorized people can enter. The workstation is positioned such that the computer screen faces the wall. Also assume that passwords are only used to access cloud-based services over TLS. We need to design proper policies to minimize the risk that passwords get compromised. Such policies will be enforced whenever a user chooses a new password.

Given the previous answer, what is the most important characteristic that you need to enforce in the password policy (in order to avoid the attack scenario)?

In a company, each employee has a private office, where only authorized people can enter. The workstation is positioned such that the computer screen faces the wall. Also assume that passwords are only used to access cloud-based services over TLS. We need to design proper policies to minimize the risk that passwords get compromised. Such policies will be enforced whenever a user chooses a new password.

Given the answer provided in point B., what is the most important characteristic that you need to enforce in the password policy (in order to avoid the attack scenario)?

*Against guessing, we must enforce that passwords are not related to the user and, in general, not belonging to dictionaries or common passwords.*

# Question

In a company, each employee works in an open space. We need to design proper policies to minimize the risk that passwords get compromised. Such policies will be enforced whenever a user chooses a new password. Also, assume that passwords are only used to access a cloud-based email client over TLS.

What is the most likely attack scenario against passwords considering the above description of the conditions of each employee? Why?

Given the previous answer, what is the most important characteristic that you need to enforce in the password policy (in order to avoid the attack scenario)?

The End