Exercises
03. Authentication

Question 1

User credentials (username and password) are stored in the developer's backend using a salted custom-implemented reversible encryption scheme (the password is salted and then encrypted). This allows the server to retrieve the user's original password if necessary.

Analyze the security of this password management scheme identifying potential weaknesses and countermeasures.

This approach has several critical issues:

- **Reversible Encryption**: Because the passwords can be decrypted, if an attacker obtains the encryption key (or exploits weaknesses in the custom encryption algorithm), they can recover all user passwords.
- **Custom Implementation**: Custom cryptographic implementations are notoriously error-prone compared to well-established, peer-reviewed algorithms. This increases the risk of implementation flaws.
- **Key Management**: The security of the entire scheme hinges on the secure management of the encryption key. A breach in key management undermines the confidentiality of all stored passwords.

Countermeasures:

- **Use One-Way Hashing**: Replace the reversible encryption with a one-way password hashing algorithm.
- **Avoid Custom Cryptography**: Leverage established cryptographic libraries and standards rather than developing a custom scheme.
- **Implement Secure Key Management Practices**: If any reversible encryption is ever deemed necessary (which is rarely the case for password storage), ensure that keys are stored securely, preferably using a hardware security module (HSM) or a similarly secure method.

Question 2

A friend of yours suggests using a custom challenge and response protocol to authenticate devices that works as follows: devices involved in the communication have to share the SHA3 of a pre-shared secret, securely stored in each device. If the hashes match on both endpoints, the authentication is successful.

Highlight the weaknesses of the proposed protocol and suggest a modification to make it working.

Weaknesses of the Proposed Protocol:

- **Lack of Freshness**: The use of a static hash for authentication means that if an attacker intercepts the hash value during transmission, they can replay it to gain unauthorized access. This is known as a replay attack.
- **Exposure to Man-in-the-Middle Attacks**: Without a mechanism to ensure the integrity and confidentiality of the transmitted hash, an attacker could intercept and modify the communication, potentially replacing the legitimate hash with their own.
- **Preshared Secret Management:** The protocol requires secure storage and management of the preshared secret on each device. If the secret is compromised on any device, the entire authentication scheme is vulnerable.
- **No Mutual Authentication**: The protocol as described only verifies the identity of the device sending the hash, not the receiver. This could allow an attacker to impersonate the control system to the device.

Suggested Modification to Improve the Protocol:

- **Introduce Nonces for Freshness**: Both the device and the control system generate random nonces for each authentication session to prevent replay attacks.
- **Mutual Authentication**: Both parties authenticate each other, ensuring that the communication is between legitimate devices and the control system.
- **Use HMAC with a Secure Hash Function**: Use HMAC (Hash-based Message Authentication Code) instead of a plain hash function to include the nonce in the authentication process.

Question 3

As a password recovery scheme, a company implemented the following mechanism: when a user asks to reset their password, an email is sent to the user with a new randomly generated password. This password is created by combining a randomly selected word (up to 9 lowercase characters) from a dictionary of animal names with a randomly generated 3-digit number (e.g., "dolphin451").

Analyze the security of this password recovery scheme. Identify its potential weaknesses and suggest improvements to enhance its security.

The password recovery scheme presents several security vulnerabilities. The limited password space, with a small dictionary of animal names and only 1,000 possible 3-digit number combinations, makes it easier for attackers to crack passwords. Additionally, the predictable structure and lack of special characters or mixed case reduce the overall complexity, further weakening security. A maximum length of 12 characters is also insufficient by modern standards.

Sending passwords via email introduces significant risks, as emails can be intercepted or stored insecurely. To enhance security, the process should use a larger word pool, include special characters, and vary the password format. Longer passwords should be generated, and instead of sending the password directly, a secure reset link should be provided, ideally with two-factor authentication. Users should also be required to change the generated password immediately upon login. These changes would greatly improve the security of the password recovery process.

Question

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

Question

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.

Question

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)?

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.

The End