CIS 751 In-Class Assignment 1

Chuck Zumbaugh

September 3, 2025

1 Security Principles Respected

- Separation of privilege - Users must provide several pieces of information to reset password.
- Psychological acceptability - Challenge questions are common and simple to use.
- Least privilege - Unauthenticated users are not able to reset a password without completing some method of authentication.
- Economy of mechanism - This is a very simple implementation that would just require a lookup of the username and security question answers.
- Fail-safe defaults - The default is that unauthenticated users are not able to reset a password after only providing the username. This can only be done after some method of authentication.
- Complete mediation - Since we don't know anything else about the system, this is satisfied as the system asks for authentication each time a user attempts to reset their password.

2 Security Principles Violated

- Work factor - Assuming the attacker already knows the username (hence the attempt at resetting the password), they only need to know a few basic details about the person.
- Compromise recording - Without any additional security mechanisms in place, an attacker could change the password and access the account without anyone knowing there was a compromise.
- Open design - Presumably, the full security architecture and design of this email service (including password reset mechanism) is not publicly available.
- Least common mechanism - I would assume that there is a direct connection from the user to the email server.

3 Making The System More Secure

- Work Factor - The system could either require additional, more time consuming authentication when the request is made from a new device (ex. phone call), or require access to a two-factor authentication system.
- Compromise recording - All requests to reset a password should be logged with information such as the sender's IP address. This could be made known during the reset process to deter attackers.
- Open design - The email service company could publish documentation regarding their authentication mechanisms and allow third-party audits. This may find faults in the current system that can be corrected.
- Least common mechanism - The email service can hide the email server behind a reverse proxy, so only the proxy is exposed to the internet.