

Multi-Factor Authentication

CIS 434: Group 2

Rick Daniel, Cedric Crawford, Tin Dang,

 Caleb Cordray

02/19/2020

Individual Contribution

Rick Daniel

Cedric Crawford

Tin Dang

Caleb Cordray

Abstract

This project is pertaining to multi-factor authentication.  Multi-factor authentication is a security measure to verify one’s identity.  This project uses two different factors to authenticate a user who has forgotten their password.  The first factor used will be a security question the user already knows the answer to. The second factor will be a code obtained from a text message.  Once the user correctly answers the security question, and correctly enters the code received from a text message, they will be able to login and change their password.

Object

* Firstly, Propose a highly available, scalable, user friendly, integrated two factor authentication solution.  We would like our project to be available for use after it is completed for other projects. We will make the UI and code easy to understand, in the aim that it can be utilized in the future in an integration and configuration capacity.
* Secondly, enhance our security and privacy posture. Adding a second or third factor to a login environment will help us reach a more secure system, safeguarding users privacy. These goals will be obtained by first creating a user Interface that is intuitive and functional.
* Finally, we will create a secure login system. To achieve this a user will have to register their email address, a password, a security question and answer, and their cellphone number. This will allow for a secure multi-factor authentication in the event of a forgotten password.

Project Description

Need UML

Difficulties and solutions

Difficulties:

* Create a database to store security questions
* Create a database to store the user’s answers
* Verify the user’s email or account
* Verify the answers for security questions
* Connect with the third party to send out a one-time code to a given phone number
* Verify the one-time code
* Generate temporary password
* Verify the temporary password
* Save the new password into database.

Solutions:

Software development process

A screenshot of a cell phone

Description automatically generated

Designing a log in window with a Forgot My Password button

A screenshot of a social media post

Description automatically generated

Designing a window to type the Email or account

Designing a window to answer security questions

A screenshot of a cell phone

Description automatically generated

Designing a window to type the user’s phone number

A screenshot of a cell phone

Description automatically generated

Sending out an one-time code to a given phone number

A screenshot of a cell phone

Description automatically generated

Designing a window to type the one-time code

Designing a window to reset password

How would we improve the project with we have more time?

\_ If we had more time to work on the project, we would

* Spend more time work on the windows’s design to make it look more attractive
* Learn how to create a database to store the user’s information.
* Do more research to find a third party to send one-time code out that we can trust
* Put more security levels to protect user’s information
* Enhance our code to avoid mistakes that might lead a hacker break in

Professional Awareness

In any project or system where a user's data is utilized software engineers must have an understanding of professional, ethical, and legal responsibilities.  Maintaining the confidentiality of user’s data must always be one of the most major concerns when developing such software or systems. Data breaches are known to cause serious, life-changing hardships for user’s that fall victim to identity theft.  A software engineer's professional, and in some cases legal responsibility, would be to ensure that all necessary steps are taken to test and secure all access to user’s data. A software engineer’s ethical responsibility would be to make sure users know exactly what is being done with their data.  If a user thinks their data is only being used for authentication purposes it should not be sold to for advertising purposes.

Project Timeline

A screenshot of a cell phone

Description automatically generated

**Periods = Weeks 1 - 16**

Conclusion

Security is a critical component for numerous programs, especially when stored user data is involved. As such, we see an increasing number of websites and programs further securing their users’ data through strict login procedures and multi-factor authentication measures. Factors can be as plain as a captcha checkbox, to verify the authenticity of a human user, or as complex as DNA match verification like retina and fingerprint scans. In our case, we will verify a user’s identity through security questions and an sms code verification. Security questions were essentially a universal second measure of authentication for early internet websites. The familiarity of this type of authentication among users was a strong reason we chose this as our first factor of authentication. The user will answer a predetermined security question in which the wrong answer redirects them back to the security question prompting them to “try again”. Once the correct response is input into our system, the second factor of authentication begins

Nowadays, many modern programs and websites use more advanced authentication measures. Common factors include: code verification sent via SMS, IP address and location alerts, and fingerprint scanners (most commonly used when unlocking smartphones). We decided on a modern approach for the second factor of authentication, that being a code sent via SMS. The user will be asked to input their personal mobile phone number, after which Twilio’s API will send a text message to the number provided. The SMS will contain the verification code required for the user to verify their identity for the final time. Once the code is successfully input into our system, the user will be redirected and prompted to provide a new password for their account.

Additional user authentication factors are essentially the only way to secure account information and data in our technology driven era. Account breaches are becoming increasingly common when multi-factor authentication is not used. As personal passwords are compromised, the sense of relief is nice knowing important account data will be shielded from unwanted invaders through multi-factor authentication.

Reference

Stewart, James. “The Three Types of Multi-Factor Authentication(MFA).” *The Three Types of         Multi-Factor Authentication | Global Knowledge*, 26 June 2018,

Azad, Tariq, and Derrick Rountree. “Authentication Factor.” *Authentication Factor - an Overview | ScienceDirect Topics*,

Techno\_FreakCheck out this Author's contributed articles., et al. “Software Engineering:

Incremental Process Model.” *GeeksforGeeks*, 5 Dec. 2019,

www.geeksforgeeks.org/software-engineering-incremental-process-model/.