Grade 11 Computer Science ISP

# What problem will your application solve?

My application will provide two-factor authentication codes that a user can use to verify their identity on websites that offer the feature. Two-factor authentication can also be used to securely access SSH terminals. The advantage of a dedicated application for two-factor authentication over SMS based two-factor authentication is that it is more secure. An attacker cannot use devices like a femtocell to intercept insecure SMS and gain access to a user’s accounts. The application’s source code will also be published online, adding to the security and providing an advantage over services like Google Authenticator.

The user will be able to input the base-64 shared secret provided by the service into the program and an account name. The user will then be able to see the 6 digit two-factor authentication code for their account and a small countdown timer will be visible to relay how much longer the code will work for. Ideally, the user will be able view the two-factor codes for multiple accounts at the same time. Future functionality may include support for different hashing algorithms, more than 6 digit codes and codes with letters. Multiple algorithm support would be the most important, as reliable collision attacks on SHA-1 have recently been discovered.

# What is your inspiration for this project?

I draw inspiration from this project through my interests in cybersecurity and algorithms. As I was using Google Authenticator one day, I realised that I had no idea how this seemingly simple, yet very important, application functioned. The tool is entirely my interest, no one has asked me to create it. I hope that it helps encourage people to secure their online accounts and think about their online security.

# What is your prior experience in this area?

Last year I wrote a Caesar cipher/ROT-N program in Processing. This is similar to a hash algorithm, but much less complicated. Theoretically, a hash should not be reversible, unlike the Caesar cipher. I have never coded an app for iOS before. I may use libraries to run the specific hashing algorithms, as this would provide me more time to work on the interface appearance and different features. I have never imported libraries to swift before.

# What are skills do you hope to acquire by completing this project?

I hope to acquire an enhanced knowledge of hashing algorithms, two-factor authentication and security protocols. I also want to learn how to code GUI for iOS and import swift/C libraries. Finally, I want to learn how to code specific algorithms to develop a deeper understanding of how they work.

# Rate the personal difficulty level of this project.

This may be a difficult project for me. There are many parts of the project that I have never undertaken before and other parts that are quite complicated. While the iOS GUI development appears relatively straight-forward, I have never attempted to do it before and am bound to run into issues. The same applies to library importing. Coding an entire algorithm from scratch, however, could prove to be quite difficult and frustrating, especially for edge cases.

# Identify what you think your biggest challenge for successfully completing this ISP will be.

Time management will likely be my biggest challenge. I will need to design my interface and write the algorithms effectively and efficiently. Free time over march break, despite it not being required to complete the project, will be limited.

# Make storyboards to indicate the user interface and/or functionality of your application.



