

Yubiduino: TOTP on an Arduino

Jessica Fleck, Brandon Mills, Paul Tela
Department of Computer Science and Engineering
The Ohio State University
Columbus, OH 43210
{fleck.48, mills.511, tela.3}@osu.edu

Abstract—This project consisted of creating a product similar to a YubiKey out of an Arduino Due called the Yubiduino. Using an Arduino Due, a SD card, a real time clock, an Ethernet shield, and a user is allowed to plug in this Arduino into a USB port and have a two-factor authentication for whatever program they choose that supports this type of functionality. This 2nd factor consists of a one-time password with a shared secret key that uses the current time. After determining the best connections for the Arduino, and the RTC, the code was written in C using the open source Arduino IDE software. A Time-base one time password algorithm was written using HMAC-SHA-1 to create a one time password for authentication. This one time password is based off of the current time using the real time clock and sent to the computer by making the Arduino act as a keyboard. To use, the user will plug in the Yubiduino, log onto the website of their choosing, and then for the second form of authentication, push the button on the Yubiduino and the key would be produced to finish the login process. The first time the user would like to use this, they would plug it into the computer to create the secret key shared between the program they are logging into and the Arduino.

I. INTRODUCTION

Two-factor authentication is becoming more and more popular in todays world because hacks are becoming more frequent. Two-factor authentication is an addition to your password that requires your password and then something you have, like a phone or a YubiKey. This keeps unwanted people out of your accounts because they would not have access to the 2nd factor of the authentication because you physically have it. The websites that support two-factor authentication usually hold valuable information about the user, which is a good reason to have extra security over your account. Because of this, we decided to create a YubiKey out of an Arduino and called it the Yubiduino. The Yubiduino creates the second layer of the two-factor authentication and makes your account more secure because no one else will have your Yubiduino. Using the Arduino IDE, we created cryptography code that generates a key each time the Arduino is pressed using the secret key and current time to add that extra layer of security to the account of your choosing. This Yubiduino will work with and base32-encoded key to allow users the option to use the Yubiduino for many different websites.

II. SYSTEM DESIGN

The process of creating the Yubiduino started with gathering all of the hardware needed. Everything needed was an Arduino Due, many wires, a real time clock, a button, a breadboard,

and an Ethernet Shield. After the materials were collected, the wiring was done as shown in the two figures below.

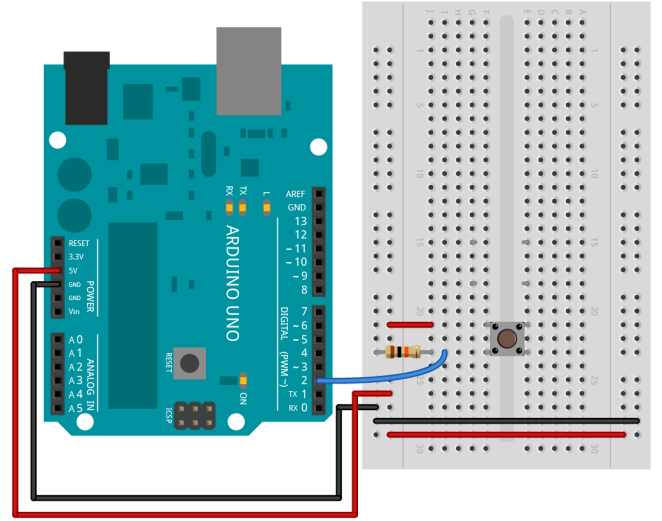


Fig. 1. Button Circuit

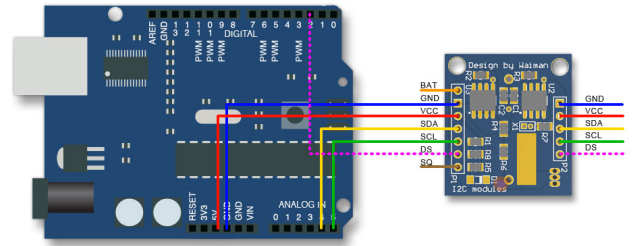


Fig. 2. RTC Circuit

The first step after the wiring was making the Arduino act as a keyboard when the button was pressed. The next step in the process was getting the real time clock to connect with the Arduino and being able to get the time each time the button is pressed to allow the new key to be created. Getting the clock

to work then lead into reading in the secret key from the SD card, which is the second half of the data needed to create the one time password. Then once both parts needed for the one time password were retrieved, we wrote the cryptography code to combine the two parts into a one time password needed to logging to the application.

III. IMPLEMENTATION AND EVALUATION

A. Implementation

B. Evaluation

IV. CONCLUSION

Security is very important when it comes to a users information. The Yubiduino helps make sure that everyone's information is secure and safe from intruders while being very easy to use and set up. Two Factor Authentication makes it harder to get into accounts because the second factor has to be physically there. The Arduino, ethernet shield, SD card, and real time clock made it possible to create this second factor to help shield intruders from getting into important accounts.

REFERENCES

- [1] H. Kopka and P. W. Daly, *A Guide to L^AT_EX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.