CS 433: 2D-2FA Project Midterm Report

Zane Globus-O'Harra, Doug Ure

12 May 2023

1 Introduction

Two-factor authentication (2FA) is the contemporary approach to authorizing a user. The first authentication factor is the user's password, with the second factor being an additional piece of information that only the user could know, often a PIN or a push notification sent to the user over a secure channel to a trusted device. However, both PIN-2FA and push-based 2FA have some issues, which are addressed in the paper "2D-2FA: A New Dimension In Two-Factor Authentication" by Maliheh Shirvanian and Shashank Agrawal.[1]

Some attacks to these two common 2FA methods include shoulder surfing, short PINs, and neglectful user approvals. The authors present a new approach to 2FA, which they have coined "2D-2FA." In this new approach, when a user logs in with their username and password, a unique identifier is displayed to them. The user then inputs this same identifier on their device. A one-time PIN is generated on the device, and transferred automatically to the server, along with the identifier. The identifier is used in the PIN's computation, so that the PIN is bound to a specific session.

The user's device and the server agree on a secret key during a one-time registration process, which is also used in the PIN computation. Once the PIN is transferred to the server, the server authenticates the session associated with the identifier by verifying the PIN, thereby taking two dimensions into account (the PIN and the identifier).

1.1 Motivation

We are motivated to work on this project for several key reasons. Firstly, the subject of this project has real-world relevance. 2FA is becoming increasingly more common to authenticate users, and as it becomes more prevalent, attackers will focus more of their efforts on finding ways to break through its layers of security. Our project will help us learn about ways to further increase the security of 2FA by using additional information along with the user's credentials and the server-provided "identifier."

This is also a learning opportunity for us. Neither of us are very familiar with security, and it is something that we are very interested in learning about. By completing this project, we will develop valuable technical skills and increase our knowledge base, as well as preparing us for future projects and industry roles.

Lastly, this project could have a real impact on end-users. 2FA enhances users' trust and confidence in online systems by making their personal information and online interactions more secure. This project has the potential to contribute to a larger goal of make a more secure digital environment.

[1] `https://arxiv.org/abs/2110.15872`

1.2 Objectives

Our objectives have not changed much from when they were laid out in the project proposal: we still plan to replicate the results of the 2D-2FA paper using software. We will create programs for the server and the device described in the 2D-2FA paper, requiring the programs to communicate with each other, and implementing the 2D-2FA requirements. To see specifically what we plan to deliver, see section 1.3.

1.3 Deliverables

Along with the final report, presentation, and poster, we plan on completing the following software-related deliverables:

- A working implementation of 2D-2FA.
  - Programs for the server and the device, as described in the 2D-2FA paper.
  - This implementation will work across multiple devices.
  - This implementation will work for multiple users.
- Test cases for our code.
- Documentation.
  - Installation instructions.
  - Usage instructions.
  - A design diagram.
  - Well-commented code.

Our implementation will use a 6-digit code as the identifier, instead of a pattern or a QR code as suggested in the 2D-2FA paper. Additionally, while we are planning for our implementation to work across multiple devices, we plan on using devices that we know and trust, and do not plan on deploying this software to arbitrary devices.

2 Related Work

Some related work and existing knowledge that we have used has mostly been to understand the basics of the implementation of the 2D-2FA presented in the paper. For example, when implementing the device–server communications, Doug used online resources[2] to help figure out these communications.

Zane worked on the hashing functionality, and for this he needed to understand HMAC (hash-based message authentication code) to create a hash of the identifier and the timestamp using the user's secret key as the HMAC key. For this, he consulted the Wikipedia page[3] to get a basic understanding, as well as Python's standard libraries for hashing[4] and message authentication.[5]

[2] https://realpython.com/python-sockets/

[3] https://en.wikipedia.org/wiki/HMAC

[4] https://docs.python.org/3/library/hashlib.html

[5] https://docs.python.org/3/library/hmac.html

Other than these outside sources, we have not needed to consult any additional research cited by Shirvanian and Agrawal, nor have we needed to find any further papers ourselves. Should we need to do additional research as we continue our progress on this project, we will be sure to include references to that material in our final report.

3 Current Progress

So far, we have been meeting once a week to discuss our project, what we have completed for the project since we last met, and what we plan on completing before we meet again. We do not have a fixed timeline, but we have a shared document where we have laid out the requirements for our system, and each week we select a few items from this document to complete.

As of 2023-05-09, we have implemented a rough outline of the device and the server such that they can communicate, as well as the basic 2D-2FA functionality. Specifically, we have implemented the basic 2D-2FA functionality of the device and the server. These two pieces of code communicate, and a test identifier correctly grants authorization to a test user with a fake secret key.

4 Lessons

The important lessons that we have learned, include project planning, collaboration skills, and iterative development. For the project planning, we have thoroughly read through the description of the implementation of 2D-2FA written by Shirvanian and Agrawal. From this, we have broken down each element of the implementation into smaller chunks that are easier to tackle and carry out.

In terms of collaboration, we have weekly meetings where we discuss what we have accomplished in the past week, and what we plan on completing for the next week. During the week, we update each other with our progress, as well as asking questions or seeing if we have suggestions for each other.

With regard to iterative development, this goes hand in hand with our project planning. Because we have broken down the problem into bite-sized chunks, we can iteratively implement these small portions, easily adding features and functionality to them as we progress, and iteratively changing them or modifying them when we encounter the need to do so.

5 Timeline and Future Plans

Now that we have a base outline for our device and server programs that allow them to communicate, as well as the basic 2D-2FA functionality, our next objectives are to allow for some sort of system where users can register, and our software can authenticate previously-registered users. Next, we will implement functionality so that the device and the server to be able to function across different machines.

More specifically, our “To-Do” list contains the following items:

- 2D-2FA functionality for multiple users.
- 2D-2FA functionality across multiple device.

- Create test cases.
- More in-depth documentation.
- Final report, presentation, and poster.

The items that we will be completing next will be first two on the above list.