CS 433 Project Proposal

Zane Globus-O'Harra, Doug Ure

14 April 2023

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).

For our project, we hope to replicate the results of this paper using software. We will create programs for the server and device, make it so that they can talk to each other, and implement the 2D-2FA requirements. If we have time, we will also attempt to implement "Typing-Proof," an algorithm presented by Dr. Li et al. in his paper.[2] However, we think that this additional implementation will be a bit more challenging for us, as it involves cross-referencing audio intensity spikes with keystroke timings, and would involve more work of figuring out how to filter audio and detect keystrokes.

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

[2] Typing-Proof: Usable, Secure and Low-Cost Two-Factor Authentication Based on Keystroke Timings, by Ximing Liu, Yingjiu Li, Robert H. Deng