ALLTHENTICATE VISION STATEMENT

PROJECT TITLE: FIDO App (Title TBD) Dogthenticate (No)
TEAM NAME: Fat Stacks
MENTOR NAME: Bernie Conrad
MEMBER NAMES: Adam Yu, Arjun Singh, Hunter Massey, Olivia Gillam, Simon Yu
MEMBER EMAILS: adamgyu@ucsb.edu, arjunsingh@ucsb.edu, huntermassey@ucsb.edu, oliviagillam@ucsb.edu, simonyu@ucsb.edu
LEAD (FIRST SPRINT): Adam Yu
SCRIBE: Hunter Massey

WHAT IS THE PROBLEM? WHY IS THE PROBLEM IMPORTANT?

Traditional security products (keys, smart cards, passwords, fobs, etc.) are inconvenient for users and are associated with a number of security risks. Without proper security infrastructure, people deal with memorizing passwords and carrying around keys and smart cards wherever they go, increasing the risk of getting locked out of their computers, accounts, servers, doors, and even automobiles.

Malicious actors can use these vulnerabilities to execute phishing attacks, stealing users' credentials and gaining access to their information and accounts. The risk posed by these attacks necessitates the use of additional security measures, including two-factor and biometric authentication.

HOW IS THE PROBLEM SOLVED TODAY?

For online usage, tools such as password managers (KeePass, Bitwarden, LastPass) are adopted to organize a user's passwords. It solves the issue of memorizing passwords, and the passwords can be shared across devices. Each of these apps have their drawbacks; Keepass does not connect to the internet, which can be good for security, but inconvenient if one wants to share a key file amongst many devices. LastPass and Bitwarden have this sharing functionality, but then the issue of storing passwords on a third-party's server arises (see LastPass data breaches). All of these apps still rely on having a master password that still needs to be remembered, and forgetting the master password can be disastrous.

Two-factor authentication is widely used online, as another security measure in case one's password becomes compromised. Many companies have their own versions of 2FA in conjunction with either mobile phones (SMS or app) or with a separate email address. For e.g.: Google Accounts (Mobile) and Github (Email). UCSB adopted Duo Push as a way to tie 2FA to a mobile app, rather than SMS. In some cases, the use of mobile or email is used in place of a password (e.g. Paypal's one-time codes); this makes it easier for the user as authentication is dependent on a singular mobile device or email rather than a multitude of passwords, and eliminates the need for remembering/storing passwords.

HOW WILL WE SOLVE THE PROBLEM?

Our goal for the capstone project is to create a mobile authentication application that implements the FIDO protocol to communicate with WebAuthn Browser APIs. Using this mobile app, users will be able to quickly register new accounts and authorize login attempts with supported websites and Web3 applications. By eliminating the need for passwords, the risk of phishing attacks is eliminated.

INITIAL PROJECT MILESTONES: SPECIFICATION, DESIGN, PROTOTYPING

- Create a mobile FIDO authenticator in Flutter that talks to a desktop service that authenticates users in the browser
- Establish breakdown of individual responsibilities (e.g. authentication experts, app specialists)
- Create wireframe for FIDO app on Figma
- Implement basic app design on Flutter based on wireframe
- Implement working WebAuthn API calls using FIDO
- Come up with a FIDO based test harness for the app
- Integrate mobile app with existing Allthenticate product

IMPLEMENTATION CHOICES

- The mobile app will utilize the FIDO protocol for authentication.
- We will use the Flutter SDK for mobile app development, as it is used as the framework for our mentor's existing product.