Passwordless Authentication

FIDO2 Implementation Project

Rajeev KARUVATH

CSEC.604.02 - (ONLINE) Crypto & Authentication
Term Project Proposal

Table of Contents

Introduction

Passwords are some of the most common cases of security breaches & authentication usability complaints. They were originally developed for an older technological landscape, and haven't really scaled well with the meteoric rise of technologies like the Internet & advances in cryptography like Public Key Infrastructure. Furthermore, passwords are the root cause of 80% of security breaches & common user practices like weak passwords & password reuse result in severe degradation of any security provided by a password [1].

Passwordless Authentication aims to provide secure authentication without the need for a password. It takes advantage of advanced technologies like biometric authentication, cryptographic hardware modules & public key cryptography to deliver a seamless authentication service. This relieves users from remembering any complex passwords and in turns protects the user from attacks like password cracking [2].

Implementation Project Focus

The primary objective of this project is to understand the FIDO2 spec for passwordless authentication, and how the WebAuthn & CTAP protocol used for this can establish a completely seamless authentication flow without the use of any passwords.

This implementation project focuses on the following :

1. Understanding the FIDO2 specifications

The FIDO2 specification was initially developed by the FIDO Alliance (Fast Identity Online), a group of more than 260 industry veterans like Google, RSA, Infineon, Samsung and more. Their sole aim is to develop secure & open authentication standards to eliminate the reliance on passwords. This specification was later augmented in conjunction with the de facto web industry standards organization W3C. FIDO2 enhances the previously developed U2F (Universal Two Factor) authentication to completely eliminate the use of passwords. It builds upon strong cryptographically secure devices like TPM (Trusted Platform Modules) found on modern devices & dedicated security keys, by extending the “Two Factor” component i.e “something you have” to a single authentication flow.

2. Analyzing the WebAuthn and CTAP protocols & the underlying public key cryptography techniques used to establish passwordless authentication

WebAuthn and CTAP are two core protocols of the FIDO2 specification. WebAuthn is the open web standard that handles the authentication flow for passwordless login [4]. CTAP (Client to Authenticator Protocol) is an open protocol to securely interact with a cryptographic device (authenticator) to perform cryptographic operations in a trusted secure environment [3].

This will be achieved by implementing a WebAuthn flow for passwordless authentication by a CTAP compliant roaming authenticator device.

Implementation Plan
The project will be implemented in following phases :

Implementation of CTAP compliant roaming authenticator

The roaming authenticator selected for this project will be a hardware security key. Such devices provide a secure trusted environment for performing cryptographic operations, and can be built to be tamper resistant (including compliance to FIPS 140-2/3 standards).
The specific hardware platform selected for this project will be the Nordic nRF52840 Dongle.

Figure 1 Nordic nRF52840

The CTAP2 firmware will be derived from Google's OpenSK framework, and will be compiled to generate a Intel Hex firmware file. This firmware will be then flashed onto the device via Nordic's SDK (Software Development Kit) utilities.

Implementation of WebAuthn authentication flow

For this project, a web portal written in Python Django framework will serve as the backend to store user registration details (like PKI public keys). The frontend will be Angular based which will implement the WebAuthn protocol to interact with the browser's APIs to access Nordic dongle to register and login the user.

The web portal will consist of two screens :

1. Registration Screen
   User will insert the Nordic dongle, click on the register button to capture the user's username and public key on the portal.

2. Login Screen
   User will insert the Nordic Dongle, click on the logic button with the same username.If a valid authentication token is generated, the user is logged in [5].

Deliverables

The successful implementation of this project will yield :

1. A thorough report detailing out the FIDO2 spec, WebAuthn and CTAP protocols, build steps for compiling the nRF52840 OpenSK firmware & WebAuthn web server development instructions.
2. A video presentation demonstrating the working of passwordless authentication flow
3. A Github repository containing all the code developed as part of this project.

References

[1] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012, May). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy* (pp. 553-567). IEEE.

[2] Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020, May). Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 268-285). IEEE.

[3] Client to Authenticator Protocol (CTAP). fidoalliance.org. (2019) Retrieved 11 October 2020, from https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html

[4] Web Authentication: An API for accessing Public Key Credentials Level 1. W3.org. (2020). Retrieved 11 October 2020, from https://www.w3.org/TR/webauthn/.

[5] Chakraborty, D., & Bugiel, S. (2019, November). simFIDO: FIDO2 User Authentication with simTPM. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 2569-2571).