CPSC 502.04: Research Project in Information Security (F21)
Supervisor: Rei Safavi-Naini <rei@ucalgary.ca>

UNIVERSITY OF CALGARY

Name: Kiley Carson UCID: 30009983

Critiqued Papers

Due 11-09-2021 @ 23:59

FIDO2 is the Fast IDentity Online (FIDO) Alliance's proposed standard for passwordless user authentication, the goal was to be both more secure than password (with MFA) authentication and easier to use. The standards defined formalize the W3C's Web Authentication (WebAuthn) and the FIDO Alliance's Client-to-Authenticator Protocol v2.0 (CTAP2). In 2019, WebAuthn became an official web standard and in 2018, the CTAP protocol was recognized as international standards by the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T). FIDO2 is a token-based system that the project intends to strengthen via a One-time Password. In FIDO2, the FIDO authenticator possess the the capability (within a smartphone, security key, laptop or tablet) to create key pairs, protect the private key, and share the public key. The authenticator does this on a per credential basis. FIDO2 specifications list many informal security goals, such as user authentication, unlinkability, DoS resistance, privacy, etc., but they are all informal. Thus, without a formal analysis, it is not clear what security goals can really be achieved. Understanding the FIDO2 authentication system, the cryptographic building blocks, the security model and the proof are all goals of the project. Additionally, the deliverables include a design of a security enhancement to the FIDO2 protocol, a proof of concept implementation of the design and an evaluation. The relevant papers that will be critiqued are "Provable Security Analysis of FIDO2", the specifications of both the Web Authentication and CTAP2 sub-protocols, the request for comments for "Time-Based One Time Passwords", and a paper on a system that has implemented Time-Based One Time Passwords.

Provable Security Analysis of FIDO2

Four main things are done in the paper by Barbosa, Boldyreva, Chen and Warinschi [1]; general information about the FIDO2 protocol is provided, a modular-style security analysis of the protocol is completed, flaws are identified, and lastly, improvements for a stronger protocol via modifications of the CTAP2 protocol are suggested. This paper is the first provable security analysis of the new FIDO2 protocols for a standard of passwordless user authentication using the Bellare-Rogaway Model [2], a communication model that uses oracles for distributed security. The analysis covers the core components of FIDO2 - W3C's Web Authentication (WebAuthn) specification and the new Client-to-Authenticator Protocol (CTAP2). One of the good qualities of the analysis completed is that it captures strong adversarial capabilities as it using a computational model in the provable security approach. Since the project is about understanding the FIDO2 authentication system, the cryptographic building blocks, and the security model and proof, this is a suitable paper to critique. A strong quality in the paper was the definition of between "Strong Unforgeability" and "Unforgeability with Trusted-Binding", and the trust implications of the client and the authenticator. These definitions allowed for the security goals to be considered in both the scenario where there are and where there are not assumptions of trust made. This revealed that an attack was possible in the CTAP2 protocol. The clear and thorough models of the cryptographic flows of both the Web Authentication Protocol and the Client to Authenticator v2 protocols were another strong quality of the paper. Each subprotocol was decomposed into an oracle query with inputs and outputs, allowing for comprehension of the step-by-step process. However, because the proof was done in a modular style, understanding the flow of the entire FIDO2 protocol was difficult. Additionally, there were also unexplained inconsistencies in the notation used in the figures, creating some ambiguity if parameters/outputs were still the same.

Name: Kiley Carson UCID: 30009983

Web Authentication Specifications

In *Web Authentication: An API for accessing Public Key Credentials - Level 2* [3], the specifications of the one of the cryptographic building blocks, Web Authentication (WebAuthn), of the FIDO2 system is provided. Since one of the goals of the project is to understand the cryptographic building blocks of FIDO2, these specifications are relevant to the project. An API that enables the creation and use of strong, scoped, and verified public-key credentials by web applications in order to authenticate users is defined in this specification. The web application requests authenticators to create and bind one or more public key credentials, each scoped to a given WebAuthn Relying Party. In order to upload user privacy, the user agent has control over access to authenticators and their public key credentials. Authenticators are responsible for ensuring that no operation is performed without user consent. Authenticators provide cryptographic proof of their properties to Relying Parties via attestation. The presence of a security considerations section in the WebAuthn specifications is a strong quality of this document. It contained a description about how to design a system where an authenticator does not need to be physically close to the client or where the authenticator and client do not communicate directly. The specifications state that physical proximity as a key strength for "something you have" and that designing a solution without this requirement would require consideration of the strength of the authenticator. The section also spoke to how the authenticator provides key management and cryptographic signatures and the fact that it could be a separate device or embedded in a WebAuthn client. However, the specifications do not have security models and proofs that would be needed in order to verify the security of the protocols.

Client to Authenticator Protocol (CTAP) V.2. Specifications

Another one of the cryptographic building blocks of the FIDO2 system is the FIDO Alliance's Client to Authenticator (CTAP) Protocol v2; these specifications are therefore relevant to the project. Two CTAP protocol versions (CTAP1/UAF and CTAP2) are referred to in the document, specifically an application layer protocol for communication between a client/platform and a roaming authenticator. Additionally, the bindings between this protocol and other transport protocols using different physical media forms are described and requirements are defined. Based on the requirements of the application layer protocol, each transport binding defines how a transport layer connection should be created. The project will be focusing on the CTAP2 version as authenticators implementing CTAP2 are referred to as FIDO2 authenticators. These specifications don't explicitly include the security considerations for the protocol, nor security models and a proof, rather a reference to the FIDO Security Reference Document [4] is attached at the bottom of the specification. In that document, the CTAP2 protocol is discussed with security threats such as a malicious device with direct communication access to FIDO Authenticator, a hostile or compromised ASM/FIDO Client or sniffing occuring between ASM/FIDO Client and the Authenticator. Consequences and possible mitigations are provided. Additionally, a note exists in the specification stating that "for other requirements than those specified in this specification[,] for example… security and privacy requirements … [one] can refer to the applicable certification documents (e.g. the FIDO Alliance, FIPS, Common Criteria, etc)". [5]

Name: Kiley Carson UCID: 30009983

RFC:6238, TOTP: Time-Based One-Time Password Algorithm

An extension of the HMAC-based One-Time Password (OTP) algorithm, as defined in RFC 4226, to support a time-based factor is described in this document. A time-based variant of the OTP algorithm provides short-lived OTP values, which are desirable for enhanced security. [6] There are a wide range of network applications that the proposed algorithm can be used for. Some examples include remote Virtual Private Network (VPN) access and Wi-Fi network logon to transaction-oriented Web applications. The authors believe that a common and shared algorithm will facilitate adoption of two-factor authentication on the Internet by enabling interoperability across commercial and open-source implementations. [6] This document also contains the security considerations that must be taken into account when including this protocol in the design. The relevancy of this document to the project is a design of a security enhancement of FIDO2 using OTPs, specifically Time-based OTPs. FIDO2 can be implemented in a single factor, two-factor and multi-factor form. Barbosa, *et al* [1] discuss the drawbacks of using a hardware security token due to the assumption trusted binding between the client and the authenticator. They state that in order to prevent an attack where a second malicious client connects to the authenticator during the binding phase, a user gesture is required to decline malicious access. Their proposal to strengthen CTAP2 includes a transition from using an unauthenticated Diffie-Hellman key exchange to a password authenticated key exchange protocol. This is where a Time-based OTP could be used.

Time-based OTP Authentication via Secure Tunnel(TOAST)

This research builds upon existing cryptographic standards and web protocols to design a cryptographically secure authentication system that is complementary to the one used today. Offline generation of one-time passwords through the Time-based One Time Pad (OTP) algorithm are used. Additionally, a seed exchange through a login-protected Transport Layer Security (TLS/SSL) tunnel to a software-based token and a password-protected keystore (BC UBER) with a strong key derivation function are used. All cryptographic algorithms in this authentication scheme are based on open standards. The system is also compared to existing schemes, and evaluated based on its security guarantees and its usability. [7] As the project involves a design of a security enhancement to the FIDO2 system using a OTP, this paper provides helpful information about design choices - specifically the comparison between a SMS based system and a Google Authenticator based system. For SMS OTP, the server generates the one-time code using the TOTP algorithm and sends this to the user's cellphone via SMS. The Google Authenticator however uses an offline variety of TOTP where a prior sharing of the secret seed between the client and the server is required. In this case, it is the user's device (vs. the server) that generates the one-time codes, then both parties are expected to generate the same one-time code during a given time window. The differences in usability are also discussed, noting that a problem with SMS-based OTP is the system is only as good as the network that the phone is subscribed to. Particularly, a slow network could result in delays in authentication. Since the Google Authenticator is an offline variety of TOTP-based authentication, issues with slow networks are avoided.

References

[1] M. Barbosa, A. Boldyreva, S. Chen, and B. Warinschi, "Provable security analysis of fido2," in *Annual International Cryptology Conference*, Springer, 2021, pp. 125–156.

[2] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Annual international cryptology conference*, Springer, 1993, pp. 232–249.

[3] (2021). "Web authentication: An api for accessing public key credentials - level 2," [Online]. Available: https://www.w3.org/TR/webauthn-2/.

[4] (2021). "Fido security reference," [Online]. Available: https://fidoalliance.org/specs/common-specs/fido-security-ref-v2.1-rd-20210525.html.

[5] (2021). "Client to authenticator protocol (ctap) proposed standard," [Online]. Available: https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html.

[6] (2011). "Rfc:6238, totp: Time-based one-time password algorithm," [Online]. Available: https://www.rfc-editor.org/rfc/rfc6238.

[7] M. L. T. Uymatiao and W. E. S. Yu, "Time-based otp authentication via secure tunnel (toast): A mobile totp scheme using tls seed exchange and encrypted offline keystore," in *2014 4th IEEE International Conference on Information Science and Technology*, IEEE, 2014, pp. 225–229.