Poster: simFIDO – FIDO2 User Authentication with simTPM

Dhiman Chakraborty
dhiman.chakraborty@uni-saarland.de
CISPA Helmholtz Center for Information Security,
Saarland University

Sven Bugiel
bugiel@cispa.saarland
CISPA Helmholtz Center for Information Security

ABSTRACT

WebAuthn as part of FIDO2 is a new standard for two-factor and even password-less user authentication to web-services. Leading browsers, like Google Chrome, Microsoft Edge, and Mozilla Firefox, support the WebAuthn API. Unfortunately, the availability of hardware authenticators that support FIDO2 authentication is still focused heavily on desktop computers, while for mobile devices, only a limited choice of suitable authenticators is available to users (few roaming authenticators with wireless connectivity and even fewer built-in platform authenticators on mobile devices). This creates a void for users, in particular users of older device generations that lack platform authenticators and the right connectivity, to authenticate themselves with WebAuthn to web-services.

In this poster, we present the idea of *simFIDO*, a FIDO2 setup using a recently developed simTPM as (platform) authenticator for mobile devices and even as roaming authenticator offered by mobile devices to connected computers. The move-ability property of the key storage of simTPM makes the users' lives easier for credential portability between devices. In particular, a seamless integration of simTPM with non-mobile devices through phones will help to create a kind of universal authentication setup using FIDO2.

Although we present the concrete design and implementation of a SIM card-based FIDO2 authenticator, we hope this poster will contribute to the discussion about how and in which form hardware authenticators can be made available to users.

CCS CONCEPTS

• **Security and privacy** → *Multi-factor authentication*; *Hardware-based security protocols*; *Usability in security and privacy*.

ACM Reference Format:
Dhiman Chakraborty and Sven Bugiel. 2019. Poster: simFIDO – FIDO2 User Authentication with simTPM. In *2019 ACM SIGSAC Conference on Computer& Communications Security (CCS '19), November 11–15, 2019, London, United Kingdom.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3319535.3363258

1 INTRODUCTION

The prevalence of text-based passwords [3] has recently been challenged by the introduction of FIDO2 [9], the successor to Universal 2nd Factor (U2F). FIDO2 was jointly developed by the FIDO Alliance and the World Wide Web Consortium (W3C), and has since been adapted by all major browsers like Google Chrome, Microsoft Edge, and Mozilla Firefox, as well as major websites such as Google services, Windows Hello, Dropbox, GitHub, and others. With FIDO2, users authenticate themselves with hardware authenticators in a public-key cryptographic challenge-response protocol, either using the authenticator as a second factor or even as a single factor. A crucial question for the industry and research community is *how such hardware authenticators are made available to the end-users and in which form to best cater for the end-user needs (e.g., no extra device to carry and portability between client devices)?* For instance, existing authenticators are Security Keys, like YubiKey or Feitian; built-in secure cryptoprocessors, like TPM or Titan M; or software solutions based on trusted execution environments, like ARM TrustZone. However, the FIDO2 specifications [9] do not restrict the authenticator realization beyond the required capabilities, opening a chance to explore different form-factors and integrations. In fact, NIST recently called in a challenge [12] for a solution for a SIM card-based secure element with FIDO2 authentication capability.

In this poster, we would like to add to the landscape of possible FIDO2 authenticators and hope to engage into discussions about how an "ideal" authenticator could look like and what challenges exist on the way to such a solution. Based on a recently published SIM card-based TPM [4], we introduce *simFIDO*, a full stack implementation of FIDO2 for Android-based mobile devices using our *simTPM* as hardware authenticator. Using the SIM card as authenticator can offer intuitively many benefits, listed in the following, but also needs thorough evaluation and discussion. We see, in particular, the following benefits and capabilities of our solution:

- **Integration with Google Strongbox**: Providing a hardware-backed isolated environment for Android's Strongbox on devices where a Titan M chip is not available.
- **No extra device plus portability**: By using the SIM card, we piggy-back on the omnipresence of mobile devices and allow easy migration of the authenticator to a new mobile device.
- **User identification before password release**: Using the extended authorization policies of TPM, our simTPM can be linked with Android's user authentication (e.g., password, PIN, pattern, biometric) to implement user presence verification that only allows authorized use of our authenticator.
- **Platform and roaming authenticator**: Using simTPM, a universal authenticator can be implemented where simTPM works as both platform authenticator to device-local apps and as roaming authenticator to attached non-mobile devices through over-the-air (bluetooth, NFC, etc.) or wired connections.

2 TECHNICAL BACKGROUND

We briefly introduce technical background information on FIDO2 and our simTPM.

CCS '19, November 11–15, 2019, London, United Kingdom

ACM ISBN 978-1-4503-6747-9/19/11.
https://doi.org/10.1145/3319535.3363258

2.1 FIDO2

FIDO2 is an open authentication standard that was jointly developed by the FIDO Alliance and the W3C, extending the previous Universal 2nd Factor (U2F) standard. FIDO2 consists of two specifications [9], WebAuthn [14] and CTAP2 [8]. WebAuthn provides a standardized access for relying parties (e.g., a web-service) to authenticate users via a hardware authenticator through a WebAuthn conforming client application, like the browser or an app. The Client-To-Authenticator-Protocol (CTAP2) is used for communication between a WebAuthn client application and a suitable hardware authenticator. The authenticator can be either a roaming authenticator, i.e., an external device connected via USB, NFC, Bluetooth, etc., or a platform authenticator, i.e., built-in to the client platform. Examples for roaming authenticators are Security Keys, like YubiKey, or recently also Android phones in version 7+ [7]. Platform authenticators are, for instance, secure co-processors like the Trusted Platform Modules (TPM) or Google's Titan M chip.

While an explanation of the WebAuthn and CTAP protocols is beyond the scope of this poster—we refer to excellent related work [10]—it is noteworthy that FIDO2 provides significant security benefits over the incumbent text-based passwords. This includes removing shared secrets between client and relying party (like passwords) that could be leaked through phishing, keyloggers, or server-sided data leaks; reuse of the same authenticator is unlinkable; and authentication sessions cannot be replayed.

The FIDO2 specifications demand that authenticators should support different levels of user verification, i.e., use of the authenticator has to be authorized and physical presence of the user should be shown. This could be done through pressing a physical button on the authenticator or local authorization to the authenticator via PIN or biometrics (e.g., fingerprint).

Specifically on Android devices, the keystore system [1] that uses the Trusted Execution Environment (TEE) or, on newer devices with Android version 9+ and necessary hardware support, the secure element or Google's Titan M chip, can act as a platform or roaming authenticator and Android recently added corresponding APIs [2].

2.2 TPM and simTPM

The Trusted Platform Module (TPM) is secure co-processor available on almost all desktop and server platforms today. Among the different features it offers, the most relevant in this context are the secure storage of cryptographic credentials, attesting the trusted origin of TPM-generated credentials (key attestation), and enforcing authorization policies on usage of such credentials. Recently, Chakraborty et al. [4] presented the implementation of TPM as a secure applet on a SIM card, called *simTPM*, providing aforementioned capabilities of a TPM to an Android host device. Like a regular TPM, the simTPM can be used as a FIDO2 authenticator.

The largest difference to a default TPM implementation and the existing TEE-based or secure element based authenticators on Android is simTPM's movability between devices, allowing the user to migrate their authentication keys easily to a new phone in contrast to device-bound keys in built-in chips or TEE. By implementing the authenticator in the SIM card, not only this movability is given, but also other general user concerns with hardware authenticators are addressed (c.f. [13]), such as the need and costs for an extra device.

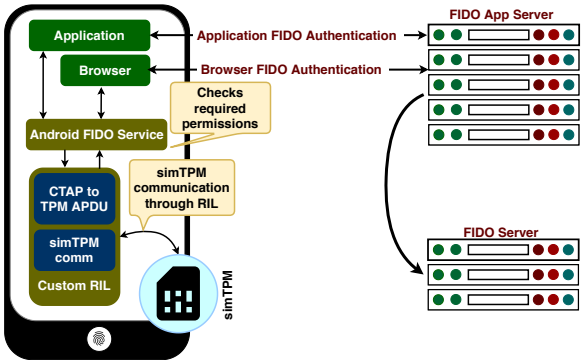

Figure 1: simTPM as platform authenticator for mobile devices

As such, simTPM can add to the landscape of available FIDO2 authenticators and the next section explain how we applied simTPM in this context when building the *simFIDO* software stack. We hope that by adding a new FIDO2 authenticator, we can encourage further research about the design, deployment, and form factor of hardware authenticators in order to cater for user needs and proliferate adoption of FIDO2 authentication.

3 APPLICATION OF SIMTPM

We briefly present the application of simTPM for FIDO2 user authentication and how we integrated simTPM to this end into Android's software stack.

3.1 FIDO2 based authentication

Our simTPM provides a hardware token for FIDO2 authentication (see Figure 1). Apps and browsers on the device that implement WebAuthn can each call the simTPM via a new Android service called *Android FIDO Service (AFS)* to use the TPM as a regular FIDO2 authenticator. To ensure that only approved apps can make use of the authenticator, we introduce a new Android permission and AFS acts as enforcement point for incoming requests regarding this permission. Only upon a successful permission check, it forwards the request to the *Android Radio Interface Layer (RIL) daemon*, which forwards messages between Android and the SIM card (see [4] for details). Since a SIM card only understands Application Protocol Data Unit (APDU ISO/IEC 7816-4) commands and since the TPM applet of the SIM card only understands TPM commands within those APDU that are according to the Trusted Computing Group specification, but the incoming commands from the application are in the form of CTAP commands, the custom RIL has to translate between the different specifications. It converts the CTAP commands into the corresponding TPM commands and then to APDU commands and forwards them to simTPM. The response follows the same path back to the application. This implementation will use TPM as an internal authenticator and make the FIDO2 stack available on the phone. Solving this technical challenge was the fundamental step in making the simTPM available as authenticator on the device.

3.2 User presence check and authorization

As mentioned before, FIDO2 requires authenticators to authorize their use and verify user presence. The simTPM, like a regular TPM chip, does not have a dedicated physical channel to the user (e.g., a button as on YubiKeys). However, in the particular case of simTPM on Android, we can overcome this limitation by linking TPM's extended authorization policies (EAP) with Android's user authentication within the on-board Trusted Execution Environment. EAP allows to restrict the usage of TPM-generated credentials by enforcing different forms of authorization. This includes challenge-response authentication with pre-determined TPM-external credentials. In our case, such an external credential is stored in the Android TEE (keystore), where Android can enforce user presence (e.g., fingerprint scan) for use of the TEE credentials. Thus, we achieve indirect user presence verification and authorization via the TEE: only if the user successfully authenticates to the TEE can they correctly sign the response to the simTPM in an EAP session to authorize the use of the simTPM-backed FIDO2 credential. EAP is flexible enough to not impede the movability of the simTPM between devices or to support simpler policies on devices without a TEE and direct user authorization to the simTPM (e.g., PIN). Since the policy for TPM-generated keys is included in the key attestation by the TPM, which is necessary to establish trust into FIDO2 authentication credentials by the relying party, the relying party could even verify if a TPM-backed authentication credential conforms with its security policy (e.g., mandatory user presence verification via TEE).

3.3 Universal authenticator

Another interesting feature of simFIDO is its applicability as both a platform and roaming authenticator. As explained in Section 3.1, simFIDO makes the simTPM available as platform authenticator. However, there are several ways to connect a mobile phone to another platform, e.g., via Bluetooth, NFC or USB. This allows a phone to expose the simTPM as a roaming authenticator to such connected devices (see Figure 2). We introduced a new Android system service *External FIDO request receiver service (XFRR)* that exposes the phone to connected devices via CTAP as a roaming authenticator and that is connected to the previously introduced *Android FIDO Service (AFS)* to forward received CTAP commands to the simTPM. This creates a setup where the simTPM serves as a platform authenticator to apps on the mobile device as well as a roaming authenticator to connected devices.

3.4 Google StrongBox integration

Lastly, Google recently introduced a new hardware security module (Titan M) in Google Pixel 3 devices. It is equipped with it's own CPU, storage, TRNG, and additional tamper-proofing mechanisms. It can provide a TPM-like secure storage and isolated co-processing. To make use of it, Android added a new StrongBox keymaster API that allows apps to store credentials in the new hardware security module. Unfortunately, this chip is currently only available on very limited Google products, making the rest of billions of devices (specifically older devices) miss out on this strong protection. A simTPM can retroactively bring this kind of service to any mobile or non-mobile device that houses a SIM card circuit.

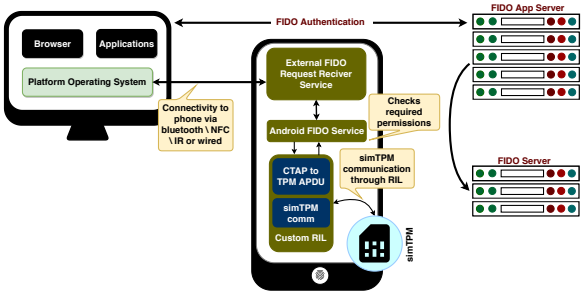

Figure 2: simTPM as roaming authenticator for connected non-mobile devices

4 CONCLUSION

simFIDO is a novel setup to provide FIDO2 user authentication with a SIM card-based Trusted Platform Module. In this poster, we present the design and realization of simFIDO on Android. By adding the SIM card to the landscape of FIDO2 authenticators and discussing it as a poster, we hope to encourage further research on the design, deployment, and form-factors of FIDO2 authenticators: while a simTPM offers appealing benefits, such as movability between devices, availability on mobile devices and as roaming authenticator on connected devices, and no need for extra devices, many other questions and user concerns remain open. For instance, accessibility of the authenticator [6, 11], recovery [5, 13], or availability [11].

REFERENCES

[1] Android Developer Documentation. [n.d.]. Android keystore system. https://developer.android.com/training/articles/keystore

[2] Android Developer Documentation. [n.d.]. FIDO2 API for Android. https://developers.google.com/identity/fido/android/native-apps

[3] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*. IEEE.

[4] Dhiman Chakraborty, Lucjan Hanzlik, and Sven Bugiel. 2019. simTPM: User-centric TPM for Mobile Devices. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association.

[5] James S. Conners and Daniel Zappala. 2019. Let's Authenticate: Automated Cryptographic Authentication for the Web with Simple Account Recovery. In *Who Are You?! Adventures in Authentication Workshop (WAY '19)*.

[6] Sanchari Das, Andrew Kim, Ben Jelen, Joshua Streiff, L. Jean Camp, and Lesa Huber. 2019. Towards Implementing Inclusive Authentication Technologies for Older Adults. In *Who Are You?! Adventures in Authentication Workshop (WAY '19)*.

[7] FIDO Alliance. 2019. Android Now FIDO2 Certified, Accelerating Global Migration Beyond Passwords. https://fidoalliance.org/android-now-fido2-certified-accelerating-global-migration-beyond-passwords/

[8] FIDO Alliance. 2019. Client to Authenticator Protocol (CTAP) — Proposed Standard, January 30, 2019. https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-client-to-authenticator-protocol-v2.0-id-20180227.html

[9] FIDO2 Alliance. [n.d.]. FIDO2: WebAuthn & CTAP. https://fidoalliance.org/fido2/

[10] Juan Lang, Alexei Czeskis, Dirk Balfanz, and Marius Schilder. 2016. Security Keys: Practical Cryptographic Second Factors for the Modern Web. In *Financial Cryptography*.

[11] Robbie MacGregor. 2019. Evaluating the Android Security Key Scheme: An Early Usability, Deployability, Security Evaluation with Comparative Analysis. In *Who Are You?! Adventures in Authentication Workshop (WAY '19)*.

[12] NIST. 2019. Expanding the SIM Card Use for Public Safety Challenge. https://www.challenge.gov/challenge/expanding-the-sim-card-use-for-public-safety-challenge/.

[13] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. 2018. A Tale of Two Studies: The Best and Worst of YubiKey Usability.

[14] World Wide Web Consortium. 2019. Web Authentication: An API for accessing Public Key Credentials Level 1 — W3C Recommendation, 4 March 2019. https://www.w3.org/TR/webauthn/