A Framework for Evaluating the Usability and Security of Smartphones as FIDO2 Roaming Authenticators

Kentrell Owens
University of Washington

Blase Ur
University of Chicago

Olabode Anise
Duo Security

Abstract

Several online authentication schemes in development would enable smartphones to be used as *roaming* (or portable) *authenticators* to register and log into websites in place of passwords. The schemes are supported by a new standard for passwordless web authentication, FIDO2, that uses public-key cryptography and a challenge-response protocol to provide security and usability benefits for users. Prior work on the use of security keys as roaming authenticators has identified several challenges to widespread adoption of FIDO2 passwordless authentication, one of which is the fact that people have to purchase and carry around security keys for some variants of the approach. Conversely, most people in the US already have a smartphone, so using smartphones as roaming authenticators might overcome this usability barrier. We present an overview of authentication schemes that could support smartphones as roaming authenticators. We also identify several key metrics to consider when evaluating the usability and security of smartphones as roaming authenticators.

1 Introduction

For decades, the computing community has aimed to develop an online authentication scheme that is better than passwords [5]. Passwords have remained the standard for authentication on computers since the 1960s [15]; they are especially dominant on the web. Currently, Internet users intending to follow security best practices must generate and remember (or store) a unique password for every website on which they have an account [11]. Given that the majority of online data breaches result from weak or exposed passwords [28], there has been a push for an alternative authentication method for web applications that provides more security benefits and is easier for users than passwords. One such push involves federated identity systems like single sign-on, which have unfortunately seen low adoption in part due to users' concerns about privacy and trust [4,23,25]. Another such push involves automating the creation and recall of unique passwords using password managers [19]. Unfortunately, adoption of password managers remains low. A 2017 Pew survey found that only 12% of respondents reported ever using a password manager, with only 3% saying that it is their primary way of storing passwords [24].

The FIDO2 standard [3] is a new approach to web authentication that replaces passwords with public-key cryptography. In place of a user generating and transmitting a password to a website upon account registration, the user's device instead creates a public-private keypair and, at a high level, registers the public key on the website. As such, FIDO2 does not require users to remember anything, is resilient to remote attacks like phishing, and does not require a trusted third party [10].

Major browsers Chrome, Firefox, Edge, and Safari all already support FIDO2 [21]. To use FIDO2, a user must have an authenticator, of which there are two key types. *Platform authenticators* are those that are integrated with a broader-purpose client device and enable authentication on that device. For example, one can use Apple's Touch ID as a FIDO2 platform authenticator to log into websites from an iPhone or Mac laptop, or Windows Hello as a FIDO2 platform authenticator from a Windows laptop. In contrast, *roaming authenticators* like USB security keys are portable, and a single roaming authenticator can be used across all of a user's devices [26]. While roaming authenticators offer important usability benefits like allowing users to authenticate on different devices, prior work has shown users are reluctant to carry around USB security keys for authentication [8]. Additionally, users may not be willing to pay for a security key. Since at least 81% of Americans own a smartphone [20], the use of smartphones as roaming authenticators is likely to overcome these barriers.

Who Are You?! Adventures in Authentication (WAY) 2020.
August 7, 2020, Virtual Conference.

This scenario has driven recent technical efforts to enable smartphones to be used as roaming authenticators. To this end, several proposed modifications to the FIDO2 specification are in progress, including caBLE (cloud-assisted Bluetooth Low Energy) and the closely related Network Transport [18]. Similarly, Duo Security is experimenting with a software-based mobile authenticator that we refer to as NEO^{TM}. Because of the novelty of technologies like NEO, there has yet to be a usable security evaluation of the use of smartphones as roaming authenticators for passwordless authentication.

There are many open questions around the usability of smartphones as roaming authenticators relative to other authentication methods. Many potential barriers might exist for widespread adoption once technologies like caBLE and NEO become widely available. **In this work we translate key metrics from Bonneau et al.'s authentication framework [5] to encapsulate these open questions for the use of smartphones as roaming authenticators. These metrics are crucial for comprehensively evaluating such technologies from a usable security perspective and for mitigating potential barriers.** Answering these questions can help spur widespread adoption of passwordless authentication.

2 Background and Related Work

We provide relevant background on the FIDO2 standard's core protocols (Section 2.1) and current efforts toward technical implementations of the use of mobile devices as roaming authenticators (Section 2.2). We also summarize prior user studies on other aspects of the FIDO2 standard and the use of smartphones in two-factor authentication (Section 2.3).

2.1 FIDO2: WebAuthn and CTAP2

At a high level, the FIDO2 standard includes two key protocols: WebAuthn and CTAP2. The Web Authentication API (*WebAuthn*) is a standard jointly developed by the FIDO Alliance and the W3C [21]. The WebAuthn API enables web applications, termed *relying parties* in the specification, to leverage public-key cryptography to authenticate users. Instead of a password, a unique public/private key pair is generated for each website registration using an authenticator. The private key is stored on the user's authenticator, and the public key, along with a randomly generated credential ID, is stored on the web application's server. These credentials are scoped to the web application through the use of a relying party identifier that identifies the server. The user can then authenticate to that web application by interacting with their authenticator. Figure 1 maps out how WebAuthn is used within FIDO2 authentication.

The other half of FIDO2 is CTAP2, a protocol being developed by the FIDO alliance. It is used when a relying party is interacting with a roaming authenticator [2], such as mobile devices like smartphones. The two salient parts of the protocol

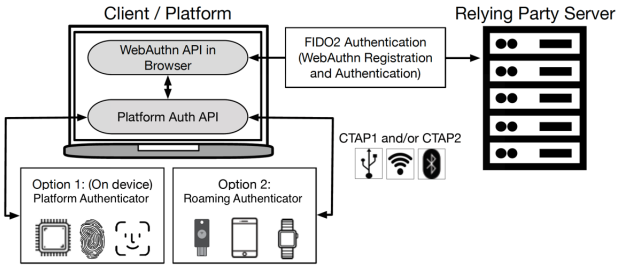

Figure 1: FIDO2 authentication with WebAuthn and CTAP2. This diagram is taken from Lystani et al. [17].

are the Authenticator API and the transport-specific bindings, referred to as *transports*, that can be used. The Authenticator API details how an authenticator should interact with a relying party when making a credential (i.e., public/private key pair) and creating assertions that provide proof of an authentication and a user's consent. The protocol defines how each of these operations should take place given the capabilities of the authenticator. The transports are how messages are conveyed from the host to a roaming authenticator. Currently, the modes that are supported are USB, NFC, and Bluetooth. The next section details implementations using these transports.

2.2 Mobile Roaming Authenticator Efforts

Next, we summarize three recent designs and implementations that aim to enable mobile devices to be used as FIDO2 roaming authenticators: simFIDO, caBLE, and NEO.

simFIDO is an implementation of FIDO2 by Chakraborty et al. [6] that uses a SIM-card based trusted platform module (TPM) called simTPM [7] to allow Android devices to serve as hardware authenticators. They introduced a new Android system service called *External FIDO Request Receiver Service* (XFRR) that forwards CTAP commands to the simTPM. Unlike typical implementations where credentials are bound to a particular device and cannot be removed, a SIM card (the authenticator) can be moved across devices.

caBLE (Cloud-Asssisted BLE) is a current proposal by Google that would extend CTAP2. It attempts to overcome some of the disadvantages of system BLE pairings, such as client-implemented preference syncing. caBLE allows mobile devices to serve as a roaming mobile authenticator by establishing a secure channel to pass CTAP2 messages between the authenticator and the client (e.g., Chrome) [18]. The latest version of this proposal, caBLEv2, allows two types of pairings between devices: temporary and permanent. These different types of pairings allow users to determine whether the pairing will be one-time (temporary) or permanent, where the latter is appropriate for a personal device.

Duo Labs has also been experimenting with different approaches that would allow mobile devices to serve as roaming authenticators. The prototype we discuss in this section will be referred to as **NEO**. To use NEO, the user first pairs their

mobile device with a Chrome browser with the aid of a mobile application and Chrome extension. The pairing process between the mobile device and the client takes place through a QR code generated by the extension. The QR code contains a shared secret. After the successful pairing, the client communicates with the mobile device through the proxying of the WebAuthn API actions via the Chrome Extension to an intermediary server. There is ongoing work to add an HTTPS-based transport (Network Transport) to the list of CTAP2 transports [18]. With the addition of the Network Transport to the CTAP2 specification, the Chrome extension would no longer be necessary during assertion or pairing for NEO or similar efforts because CTAP2 authenticators would be able to communicate with the client directly.

2.3 Related Usability Studies

While this paper focuses on the evaluation of roaming mobile authenticators, prior usable security research has focused on FIDO2 passwordless authentication with *USB security keys* as roaming authenticators, as well as the use of phones as a second factor in multi-factor authentication.

Most closely related, Lystani et al. [17] conducted a between-subjects lab study evaluating the usability of USB security keys as part of FIDO2 passwordless authentication. They sought to determine: (i) how users perceive FIDO2 passwordless authentication; (ii) user acceptance of FIDO2 using USB security keys; and (iii) what thoughts and concerns arise when using FIDO2 passwordless authentication. To answer these research questions, they recruited 94 participants and split them into two groups: a (control) passwords group and a security key group. The group using security keys watched additional informational videos about FIDO2 and setting up security keys to help equalize knowledge of the process across groups. Participants registered and authenticated on two mock web applications using passwordless authentication. Afterwards, they completed a survey involving several scales (System Usability Scale and Affinity for Technology Interaction scale), as well as free response questions. They found that FIDO2 passwordless authentication with security keys was seen as more usable and acceptable than passwords. However, their participants raised several concerns, which we revisit in our own context in Section 3. While useful in understanding users' perceptions of FIDO2 passwordless authentication, Lystani et al.'s work focuses on security keys as roaming authenticators. We build on this work, instead evaluating smartphones as roaming authenticators.

While our context uses a smartphone as a primary (and single) factor for authentication, a number of studies have evaluated the usability of phones as a *second* factor for authentication, including via SMS codes, TOTP codes, and push notifications [9, 13, 16, 22, 27]. For example, Weidman and Grossklags studied a transition from token-based 2FA to a smartphone, push notification 2FA system for employees at Penn State University [27]. They used an online survey to conduct a comparative usability evaluation between the previous token-based system and Duo Mobile. They found that employees preferred the token-based system to the Duo app for multiple reasons. These reasons included: (i) not wanting to have to use their personal device for work; (ii) wanting to be provided a work phone if they're required to use a phone for authentication; and (iii) having job restrictions that limited phone usage. Similarly, Reese et al. [22] conducted a longitudinal study assessing the usability of different forms of 2FA. Three of the five methods they evaluated (SMS, TOTP, and push) involved a mobile device. They had 72 participants log into a mock banking application, provide their second factor, and complete a task. They found that push was the fastest method and that TOTP was considered the most usable.

3 Framework of Key Usable Security Metrics

When evaluating smartphones as roaming authenticators in passwordless authentication with the goal of spurring adoption, there are several key usable security metrics we believe should be a particular focus for user studies. We initially developed this framework by adopting several broad metrics for the usability of authentication schemes from Bonneau et al. [5]. Based on the findings of Lyastani et al.'s investigation of FIDO2 security keys [17] and pilot sessions of our own user study (Section 4), we identified four sets of key challenges and specific potential concerns for our use case.

3.1 Scalability (Perception and Reality)

One of the challenges with passwords is that people must create and store a password for each website on which they have an account. FIDO2 passwordless authentication offers an opportunity to significantly reduce the cognitive load people experience for each successive account creation.

Compared to FIDO2 implementations with platform authenticators, a key advantage of using a smartphone as a roaming authenticator is that a single registration can allow a user to sign into a website from nearly any phone or computer. While using USB security keys as a roaming authenticator conceptually has this same property, it requires the user to carry an additional item, and it also suffers from interface issues, most notably the lack of a compatible USB port on some devices [17]. However, key questions remain about whether users will understand and appreciate these benefits, as well as whether they will know how to take advantage of them. Such perceptions will heavily influence adoption decisions.

Although registering a new account with USB security keys has its challenges [12], using a smartphone as a roaming authenticator could potentially increase friction in its user experience. Existing implementations currently require an out-of-band pairing of the authenticator with the browser client (e.g. via Bluetooth or QR code). While this method offers some

security benefits, people will have pair their phone once with every browser client they wish to authenticate on. This could cause challenges for public or shared computers, particularly those with browser clients that may not save state. Usability investigations of authentication schemes that support smartphones as roaming authenticators will need to quantitatively measure the user experience of pairing their smartphone with the user's other devices, a process that is needed to take full advantage of the roaming nature of the authenticator. They will also need to evaluate the cognitive load of registration with a diverse set of users who authenticate in a variety of settings, in addition to identifying the key usability barriers.

3.2 Phone Availability / Account Recovery

For people to feel comfortable adopting smartphones as roaming authenticators, researchers must grapple with availability issues that arise from using a smartphone to authenticate. That is, if the user's smartphone is their only authenticator and their smartphone is inaccessible for any of the reasons detailed below, the user will not be able to log into any websites.

Lystani et al. and others have identified analogous problems for USB security keys, particularly the difficulty of account recovery and revocation if the key is lost or stolen [1, 8, 17]. Smartphones, just like security keys, can be stolen or lost, temporarily or permanently. Identifying appropriate methods for recovering from authenticator loss is still an open problem, although FIDO2 recommends registering multiple authenticators to avoid being completely locked out [14].

Smartphones raise additional availability issues, though. Unlike security keys, phones can run out of battery, making it impossible for the owner to authenticate without charging the phone. Phones are also higher-value targets for general theft.

Usable security researchers should collect data on how frequently people's phones are unavailable to determine what solutions are necessary. For example, notifications from a mobile application when battery is low might be able to prevent a phone's battery from being completely drained. A process for nudging users toward registering multiple authenticators could alleviate some of the problems of account recovery and authenticator revocation. Again, beyond simply measuring the actual incidence of usability failures in this domain, it is critical to measure users' expectations and perceptions of such situations as those expectations will influence adoption.

3.3 Perceptions of the Security of Phones

We expect the most important barrier to widespread adoption may be people's perceptions of smartphones' overall security. Anecdotal data from our pilot studies suggests that people are wary of storing credentials on smartphones even after when told cryptographic keys are stored in secure hardware. Prior work has shown that people broadly lack mental models for understanding how security keys work, and this affects their perceptions of security keys' trustworthiness [17]. We must study people's mental models of how WebAuthn works on smartphones and assess their willingness to use smartphones as roaming authenticators for different types of accounts.

3.4 Accessibility and Technology Access

Depending on the implementation of the authentication scheme, using a smartphone as a roaming authenticator could present accessibility challenges. For example, schemes that require biometrics to verify user presence (e.g., as might be required after confirming a push notification) could cause problems for people who cannot use a fingerprint scanner or for individuals for whom facial recognition is not reliable.

Additionally, some people's smartphones or computers may not support all of the technologies required, and this lack of access to compatible technology is likely to be correlated with demographic factors. If a mobile authentication scheme requires Bluetooth or biometrics, not all people may be able to use these schemes. An evaluation of the accessibility of different mobile authentication schemes is necessary to ensure that new forms of web authentication are made broadly available without excluding the needs of some groups.

4 Future Work

Using the key metrics outlined in Section 3, we are currently conducting a between-subjects, longitudinal study on the usability of smartphones as passwordless roaming authenticators. In that study, we are randomly assigning participants to either register and authenticate using a password or NEO. In addition to using mostly open-ended questions to elicit participants' perceptions of their assigned authentication method, we are collecting timing data, authentication error rates, and diary-style Likert data after each authentication. These quantitative metrics help provide a more objective baseline for the user experience, complementing our measurement of participants' perceptions. The results of this experiment will help highlight necessary changes to improve the user experience and foster widespread adoption of smartphones as roaming authenticators for passwordless authentication.

References

[1] Seb Aebischer, Claudio Dettoni, Graeme Jenkinson, Kat Krol, David Llewellyn-Jones, Toshiyuki Masui, and Frank Stajano. Pico in the wild: Replacing passwords, one site at a time. In *Proc. EuroUSEC*, 2017.

[2] FIDO Alliance. Client to authenticator protocol (CTAP), Jan 2019.

[3] FIDO Alliance. FIDO2: WebAuthn & CTAP, May 2020. `https://fidoalliance.org/fido2/`.

[4] Lujo Bauer, Cristian Bravo-Lillo, Elli Fragkaki, and William Melicher. A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality. In *Proc. DIM*, 2013.

[5] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proc. IEEE S&P*, 2012.

[6] Dhiman Chakraborty and Sven Bugiel. simFIDO: FIDO2 user authentication with simTPM. In *Proc. CCS*, 2019.

[7] Dhiman Chakraborty, Lucjan Hanzlik, and Sven Bugiel. simTPM: User-centric TPM for mobile devices. In *Proc. USENIX Security*, 2019.

[8] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. Of two minds about two-factor: Understanding everyday FIDO U2F usability through device comparison and experience sampling. In *Proc. SOUPS*, 2019.

[9] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "It's not actually that horrible": Exploring adoption of two-factor authentication at a university. In *Proc. CHI*, 2018.

[10] James S. Conners and Daniel Zappala. Let's authenticate: Automated cryptographic authentication for the web with simple account recovery. In *Proc. WAY*, 2019.

[11] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The tangled web of password reuse. In *Proc. NDSS*, 2014.

[12] Sanchari Das, Andrew Dingman, and L. Jean Camp. Why Johnny doesn't use two factor: A two-phase usability study of the FIDO U2F security key. In *Proc. FC*, 2018.

[13] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. A comparative usability study of two-factor authentication. In *Proc. USEC*, 2014.

[14] Hidehito Gomi, Bill Leddy, and Dean H. Saxe. Recommended account recovery practices for FIDO relying parties. 2019.

[15] Troy Hunt. Authentication guidance for the modern era, May 2020. https://www.troyhunt.com/passwords-evolved-authentication-guidance-for-the-modern-era/.

[16] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M. Angela Sasse. "They brought in the horrible key ring thing!" Analysing the usability of two-factor authentication in UK online banking. In *Proc. USEC*, 2015.

[17] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication. In *Proc. IEEE S&P*, 2020.

[18] Nick Mooney. Addition of a network transport. https://github.com/w3c/webauthn/issues/1381.

[19] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Proc. SOUPS*, 2019.

[20] Pew Research Center. Demographics of mobile device ownership and adoption in the United States, 2019. https://www.pewresearch.org/internet/fact-sheet/mobile/.

[21] Suby Raman. Guide to web authentication. https://webauthn.guide.

[22] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A usability study of five two-factor authentication methods. In *Proc. SOUPS*, 2019.

[23] Scott Ruoti, Brent Roberts, and Kent Seamons. Authentication melee: A usability analysis of seven web authentication systems. In *Proc. WWW*, 2015.

[24] Aaron Smith. Americans and cybersecurity, January 2017. http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security.

[25] San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. What makes users refuse web single sign-on? An empirical investigation of OpenID. In *Proc. SOUPS*, 2011.

[26] W3C. Web authentication, Mar 2019. https://www.w3.org/TR/webauthn/.

[27] Jake Weidman and Jens Grossklags. I like it, but I hate it: Employee perceptions towards an institutional transition to BYOD second-factor authentication. In *Proc. ACSAC*, 2017.

[28] Tin Zaw and Richard Yew. 2017 Verizon data breach investigations report (DBIR) from the perspective of exterior security perimeter, 2017. https://www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/.