Poster: User Awareness of Phishing and WebAuthn

Mindy Tran
Leibniz University Hannover
mindy.tran@stud.uni-hannover.de

Sabrina Amft
CISPA
sabrina.amft@cispa.de

Dominik Wermke
CISPA
dominik.wermke@cispa.de

***Abstract*—Two-factor authentication (2FA) adds an additional layer of security to password-based authentication. SMS and software-based 2FA methods are the most commonly adopted 2FA methods, but are vulnerable to several security attacks such as SIM-jacking, cloning, and phishing. WebAuthn implements several security measures to protect users from these attacks. However, active user adoption of WebAuthn still remains low. Common causes for low user adoption are often users' doubts regarding benefits and utility.**

In this work, we investigate users' understanding and mental model of traditional 2FA methods and WebAuthn. We were particularly interested in finding out, whether users are aware of differences and benefits. For this, we designed and conducted a preliminary pilot study including a practical experiment. Our work utilizes expert reviews and answers from a pilot study to iteratively improve our survey and experiment.

Our results will be used to improve and guide the study design of a prospective large-scaled quantitative study.

I. Introduction

Web authentication has been an important topic for decades. Countless online services require users to verify their identity to get access to sensitive information or perform certain user actions. Despite having several security and usability issues, passwords are still the most commonly used authentication approach. Online services have introduced Two-factor authentication (2FA) in an attempt to add an additional layer of security. This method requires users to provide two or more distinct factors to prove their identity. This can be something you know (e.g. passwords), have (e.g. mobile device) or are (e.g. fingerprint). The most commonly used Two-factor authentication methods are SMS one-time passwords, email, and software one-time passwords [1]. These approaches are vulnerable to several cybersecurity attacks such as SIM-jacking, cloning, as well as social engineering attacks such as phishing and MFA fatigue [2]–[5]. Furthermore, these Two-factor authentication methods suffer from low user adoption and acceptance since users need to carry an additional device with them.

The WebAuthn protocol from the FIDO2 alliance poses a new promising alternative that holds multiple advantages over traditional Two-factor authentication methods. Firstly, WebAuthn is robust against phishing attacks. Throughout the whole authentication process the origin is consistently being recorded, verified, and sent over with a signed challenge. In case of a phishing attack, the relying party will immediately be able to recognize the mismatching origin and reject the authentication attempt. Secondly, Webauthn uses public-key cryptography. Sensitive information (private keys) are not stored on a server and thus making databases less attractive to attackers.

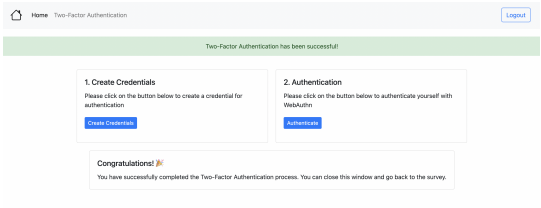

Fig. 1. Screenshot of the prototype website used in the experiment.

One problem WebAuthn faces is low user adoption and acceptance. Past research found that one general reason for low user adoption are users' doubts regarding the benefits and utility, often caused by incorrect mental models [6]. Moreover, previous work has shown that prompts can effectively promote good security behavior and increase adoption [7]. For this, we need to identify users' perception, mental model and awareness of the benefits and differences. Our findings can help in establishing effective approaches to correct users' mental model, familiarize end users with the differences, and motivate them to use WebAuthn.

II. Approach

We decided to iterate our planned study consisting of a survey and practical experiment part in a multi-stage approach (cf. Figure 2).

A. Expert and User Review

Before conducting a pilot study, we evaluated our setup during expert reviews with 4 PhD students. The experts evaluated the experiment website's design against usability guidelines and principles to find possible usability problems. They also reviewed the survey for improvements in phrasing and survey flow. In addition to the expert review, we also conducted an user review. Four users were asked to take part in the survey and to provide feedback.

B. Pre-screening Survey

Before being invited to the main survey and experiment, we filtered participants with certain screening questions. We required all participants to have experience with using 2FA and to possess either a smartphone, device with a built-in authenticator, or a (physical) security key. We additionally inquired users to name a 2FA app that they used in the past.

These screening questions ensured that all participants had the appropriate knowledge and required hardware to take part in this survey. We also decided to add an attention check question and exclude all participants that failed this check from our survey.

Overall, we invited 100 participants to take part in our pre-screening survey. All eligible participants were invited to take part in our follow-up survey. Five of our participants stated, that they never used 2FA before. 35 of our participants couldn't name a 2FA app or gave an invalid answers. Two of our participants didn't pass the attention check and were therefore filtered out as well. After filtering out all ineligible participants, we invited 58 participants to the main pilot study.

C. Pilot Study

Main goal of our pilot study was to conduct a small-scale preliminary study to identify adverse events and utilize any results to improve and guide the study design for a full-scale quantitative study.

Another specified aim of our pilot study was to gain a more in-depth and extensive view of the users' mental models. In contrast to the quantitative study, participants were asked to provide free text answers to questions about security and advantages/disadvantages of their respective 2FA method. This encouraged participants to elaborate their ideas and thoughts further and might reveal new and unexpected insights. Another question exclusive to the pilot study was the participants' description of the components and processes involved when using the 2FA method. This question will not be included in the large-scaled quantitative study since individual analysis takes up a lot of time and the broad variety of possible answers makes it even harder to summarize answers. Thus some unrepresented answers might not get captured.

D. Ethical Consideration

Our university did not require a formal IRB process for our approach. Nonetheless, we modeled our study after previous, IRB-approved crowd worker studies, adhered to the strict German and U.S. data and privacy protection laws and the General Data Protection Regulation in the E.U., and structured our study following the ethical principals of the Menlo report for research involving information and communications technologies.

E. Limitations

In general, self-report studies may suffer from several biases, including over- and under-reporting, sample bias, and social-desirability bias. However, while we utilize self-report data, our central claims are not about the accuracy of respondents' answers to a given question, but rather about the concepts and misconceptions conveyed by their answers. Conducting user studies on crowd working platforms like Amazon's Mechanical Turk is a commonly used and generally accepted procedure for human-computer interaction and usable security and privacy research [8]. While the quality of answers can suffer in a crowd worker context, we tried to ensure a high data quality by following best practices by limiting access to our surveys to high-reputation cloud workers and by manually filtering low quality answers. Due to our recruitment criteria, our study only included participants that are familiar with the term "Two-Factor Authentication". Tech illiterate users likely would not be able to pass the pre-screening questions and are therefore not included. We thus assume that our participants are likely more security and tech-savvy than average users.

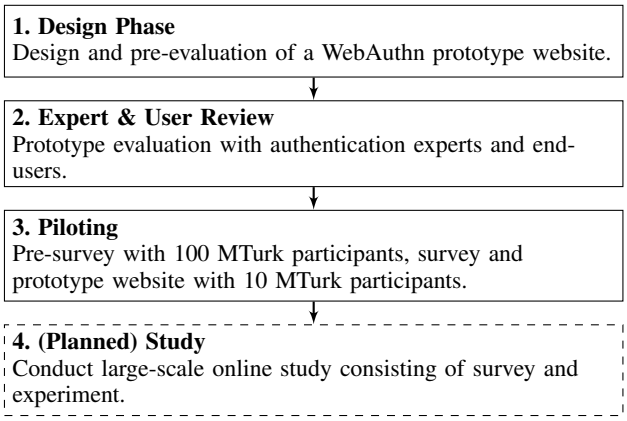

Fig. 2. Overview of the different stages in our approach, from prototype website design to a (planned) large-scale survey & experiment study.

III. Outlook

While still work in progress, our pre-screening and pilot study already provide some first insights. All participants from our pilot study thought that traditional 2FA methods protect them from phishing attacks. Moreover, they showed misconceptions regarding 2FA with QR Codes.

References

[1] Dave Childers. State of the Auth: Experiences and Perceptions of Multi-Factor Authentication. In *DuoLabs Report*. Duo Labs, 2021.

[2] kajeet.net. What is SIM Jacking and How to Avoid It. https://www.kajeet.net/iot-security-what-is-sim-jacking-and-how-to-avoid-it/. Online; accessed March 22, 2022.

[3] Philip Polleit and Michael Spreitzenbarth. Defeating the Secrets of OTP Apps. In *Proc. of the 11th International Conference on IT Security Incident Management & IT Forensics (IMF 2018)*. IMF, 2018.

[4] Unbound Security. Why SMS OTP Is Not Enough Security for Authentication. https://www.unboundsecurity.com/blog/sms-based-otp-is-just-not-good-enough/. Online; accessed March 22, 2022.

[5] Lisandro Ubiedo. Current MFA Fatigue Attack Campaign Targeting Microsoft Office 365 Users. https://www.gosecure.net/blog/2022/02/14/current-mfa-fatigue-attack-campaign-targeting-microsoft-office-365-users/. Online; accessed March 22, 2022.

[6] 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 *Meiklejohn S., Sako K. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10957*. Springer, 2018.

[7] Maximilian Golla, Grant Ho, Marika Lohmus, Monica Pulluri, and Elissa M. Redmiles. Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns. In *Proc. of the 30th USENIX Security Symposium*. USENIX, 2021.

[8] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How I Learned to Be Secure: A CensusRepresentative Survey of Security Advice Sources and Behavior. In *Proc. 23nd ACM Conference on Computer and Communication Security (CCS'16)*. ACM, 2016.