Poster submission – Published Work

“It’s Stored, Hopefully, on an Encrypted Server”: Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn

Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur

Citation

@inproceedings {274547,

author = {Leona Lassak and Annika Hildebrandt and Maximilian Golla and Blase Ur},

title = {"It{\textquoteright}s Stored, Hopefully, on an Encrypted Server{\textquoteright}{\textquoteright}: Mitigating Users{\textquoteright} Misconceptions About {FIDO2} Biometric {WebAuthn}},

booktitle = {30th USENIX Security Symposium (USENIX Security 21)},

year = {2021},

isbn = {978-1-939133-24-3},

pages = {91--108},

url = {https://www.usenix.org/conference/usenixsecurity21/presentation/lassak},

publisher = {USENIX Association},

month = aug,

}

Official Publication

https://www.usenix.org/system/files/sec21-lassak.pdf

Abstract

While prior attempts at passwordless authentication on the web have required specialized hardware, FIDO2's WebAuthn protocol lets users sign into websites with their smartphone. Users authenticate locally via the phone's unlock mechanism. Their phone then uses public-key cryptography to authenticate to the website. Using biometrics (e.g., fingerprint, face) for this local authentication can be convenient, yet may engender misconceptions that discourage adoption. Through three complementary studies, we characterized and sought to mitigate misconceptions about biometric WebAuthn. We also compared it to non-biometric WebAuthn and traditional passwords. First, 42 crowdworkers used biometric WebAuthn to sign into a website and then completed surveys. Critically, 67% of participants incorrectly thought their biometrics were sent to the website, creating security concerns. In remote focus groups, 27 crowdworkers then co-designed short notifications to mitigate biometric WebAuthn misconceptions. Through a 345-participant online study, we found

that some notifications improved perceptions of biometric WebAuthn and partially addressed misconceptions, yet key misconceptions about where the biometric is stored partially persisted. Nonetheless, participants were willing to adopt biometric WebAuthn over non-biometric WebAuthn or passwords. Our work identifies directions for increasing the adoption of biometric WebAuthn by highlighting its security and usability.