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

DUO LABS

Duo Security is
now part of Cisco.

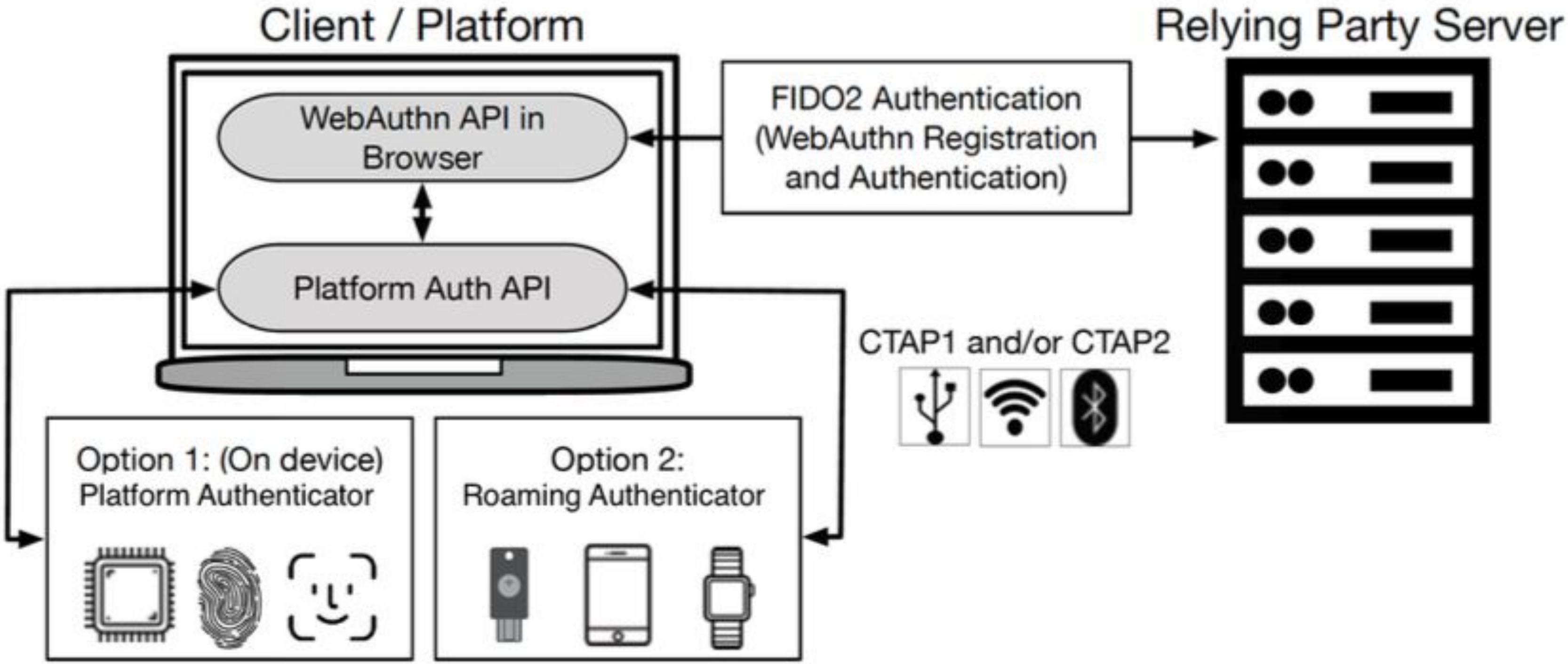
CISCO

Outline

- What is FIDO2
- Methods to facilitate the use of mobile phones as roaming authenticators
- Discussion of the framework we developed
- Future work

A FIDO2 Primer

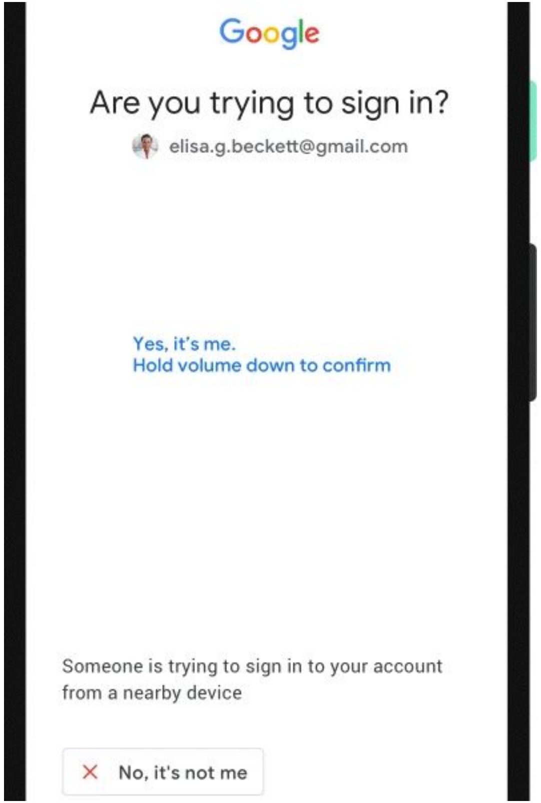
- FIDO2 is a set of specifications that detail how to perform strong web authentication using public-key crypto instead of passwords
- FIDO2 = WebAuthn + CTAP2
- The hope is that these sets of standards will provide a more secure and usable alternative to passwords
    - Work by Lystani et al. (2020) and Farke et al. (2020) shows there are still some hurdles to overcome


Client / Platform
Relying Party Server
WebAuthn API in Browser
FIDO2 Authentication (WebAuthn Registration and Authentication)
Platform Auth API
CTAP1 and/or CTAP2
Option 1: (On device) Platform Authenticator
Option 2: Roaming Authenticator

Source: Lystani et al., Is FIDO2 the kingslayer of user authentication? IEEE S&P 2020

caBLE (cloud assisted Bluetooth Low Energy)

- Google has been working on a proposal to extend CTAP2 that would allow mobile phones to function as roaming authenticators
- The big improvement is that you wouldn't have to go through the normal system BLE pairing process
- This approach is being used to allow Android devices to function as security keys on Google properties



Google

Are you trying to sign in?

elisa.g.beckett@gmail.com

Yes, it's me.
Hold volume down to confirm

Someone is trying to sign in to your account from a nearby device

✕ No, it's not me

Network Transport

- Recently, Duo Labs has proposed an extension to CTAP2 to support a network-based transport
- This would allow mobile phones to be used as roaming authenticators through an HTTPS-based transport
- The inclusion of this transport would overcome some of the flaws associated with relying on Bluetooth/BLE

How should We Evaluate Their Usability?

- We adopt and build upon metrics from Bonneau et al.’s (2012) to framework to evaluate smartphones as roaming authenticators
    - Scalability
    - Phone Availability/Account Recovery
    - Perceptions of the Security of Phones
    - Accessibility and Technology Access
- Addressing these points could spur adoption of FIDO2 passwordless authentication

Scalability (Perception and Reality)

- Smartphones must currently be paired with every browser one wishes to use for authentication
  - May cause challenges with public or shared computers
  - This focus on browser/phone pairings instead of more traditional web application/phone pairings could be confusing for users
- Smartphones have some advantages over security keys
  - 81% of people in the US already own one [Pew 2017]
  - Users can authenticate on nearly any phone/computer
  - Compatibility isn't based on a USB port
- Do users understand and appreciate these benefits?

Phone Availability/Account Recovery

- Phones can be lost/stolen
  - They are high value targets for theft
- Phones can be out of battery
  - Do users need additional nudges to charge their phones?
- Account recovery/revocation is an open challenge
  - Current FIDO2 recovery recommendation is to register multiple authenticators
- Researchers should collect data on incidents of unavailability
  - What are their perceptions and do they match up with reality?

Perceptions of the Security of Phones

- The most important barrier to widespread adoption may be people’s perceptions of smartphones’ overall security
- Pilot study data indicates that people are wary of storing credentials on smartphones and may not trust secure hardware for cryptographic keys
- Prior work has shown that people lack mental models for how security keys work
    - This affected how much they trusted security keys
- Researchers must study people’s mental models of WebAuthn & smartphones

Accessibility and Technology Access

- Authentication schemes may require biometrics to be used for user verification
    - This could present challenges for people who cannot use a finger scanner or for individuals for whom facial recognition is not reliable.
- Smartphones & clients must support the relevant technologies
    - Not all smartphones support biometrics
    - Not all computers have Bluetooth
- Evaluating the accessibility of different mobile authentication schemes is necessary

Future work

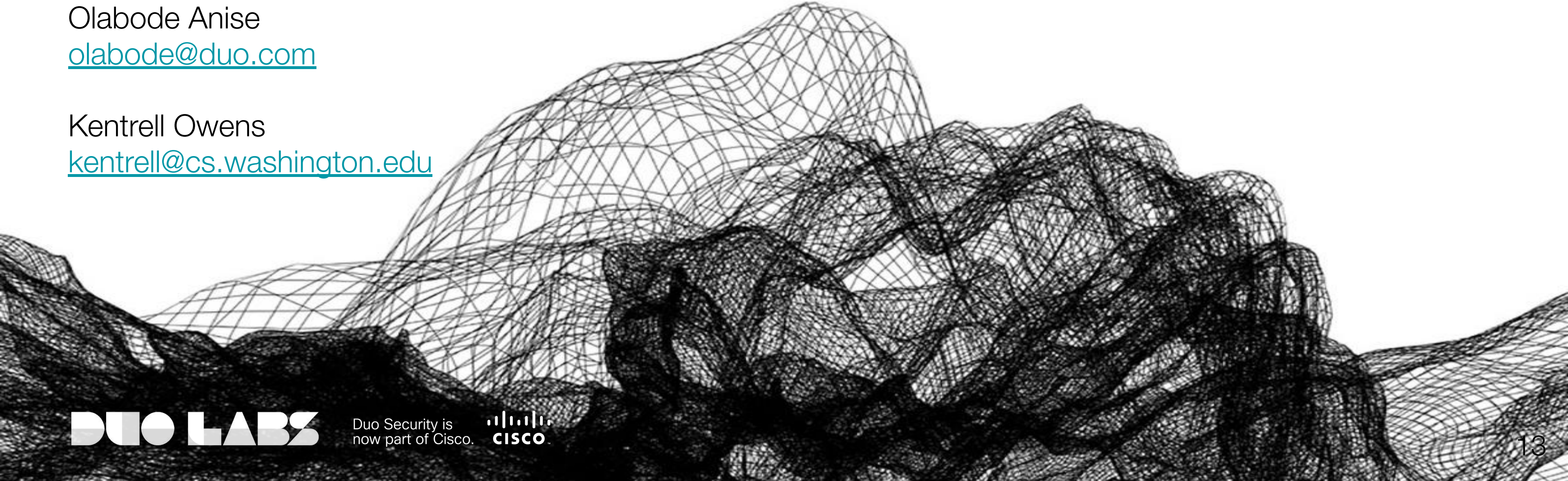
- We're running a study!
  - Between-subjects, longitudinal study evaluating the usability of smartphones as roaming authenticators using NEO
  - Daily logins to our web application over the course of two weeks
  - Collecting timing data, authentication error rates, and diary-style Likert data after each authentication
- Open questions
  - Do users understand & appreciate the benefits of smartphones as roaming authenticators?
  - What are people's mental models of WebAuthn & smartphones?
  - What privacy concerns may people have with using smartphones as roaming authenticators?

Thank you!

Speakers:

Olabode Anise
olabode@duo.com

Kentrell Owens
kentrell@cs.washington.edu



References

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.

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