


Provable Security Analysis of FIDO2



SaTC: CORE: Small: Authentication on the Web: Provable Security for Emerging Protocols

PI: Alexandra (Sasha) Boldyreva 

FIDO2 overview

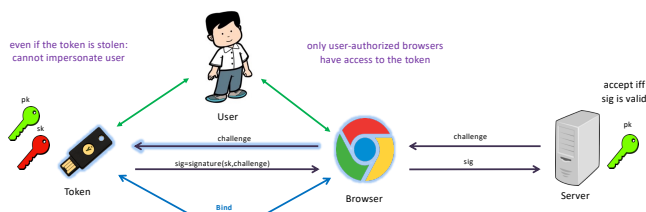


- Passwords are problematic
- Mission: **passwordless** authentication standards
- Global effort: 250+ members
- Adopted as ITU and W3C standards
- Good usability
- Smooth deployment



FIDO2 has 2 parts:

- **CTAP2**: user **authorizes access** to his token: **binds** user-selected browsers to the token
- **WebAuthn**: server **authenticates** user's token via **challenge-response**



Questions we asked:

- What does FIDO's security mean formally?
- Is FIDO2 secure?

Results overview:

- We performed modular provable-security analysis of FIDO2
- For each part, CTAP2 and WebAuthn, and for the whole FIDO2, we
 - Formalized the syntax and security model
 - Analyzed the protocol under the security model

For CTAP2:

- Defined PIN-based access control for authenticators (PACA) protocol and its security
- Proved **CTAP2** is a **weakly** secure PACA:
 - **trusted binding**: no active attacks allowed against browsers
 - **no authorized browsers can be compromised**
- Proposed an efficient fix to make it strongly secure

For WebAuthn:

- Defined passwordless authentication (PIA) protocol and its security
- Proved **WebAuthn** is PIA secure:
 - only **valid** tokens can be registered to the server
 - server accepts authentication (logins) only from the **registered** token

For FIDO2:

- Proved FIDO2 security from PIA-secure WebAuthn and strongly-secure sPACA
 - user impersonation requires authorized access to registered token
 - if some authorized browser is compromised: require user gesture to decline malicious access

Preliminary results have been published in the Proceedings of **CRYPTO 2021**.

Limitation of our initial work:

- assumes all tokens have unique keys

Current and future work:

- re-visit security implications for the case of shared keys
- study the anonymity property targeted by sharing keys

The work is with collaboration with

- **Shan Chen**, a former Georgia Tech PhD student. He just became an Assistant Professor at SUSTech in Shenzhen, China
- **Maunel Barbosa**, University of Porto
- **Bogdan Warinschi**, University of Bristol