Provable Security Analysis of FIDO2 Protocol for Passwordless Authentication on the Web

Georgia Tech

Challenge:

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

FIDO2 helps the world to move away from password use

250+ MEMBER ORGANIZATIONS GLOBALLY

FIDO board members include leading global brands and technology providers

fido alliance
aetna
Alibaba Group
AMERICAN EXPRESS
ARM
Bank of America
BCcard
Crucial Tec
Daon
egis
FEITIAN
FINGERPRINTS
intel
gemalto
Google
infineon
ING
Lenovo
mastercard
Microsoft
Nok Nok
docomo
NXP
oberthur
PayPal
QUALCOMM
RAON SECURE
RSA
SAMSUNG
Synaptics
USAA
VASCO
VISA
yubico

+ SPONSOR MEMBERS + ASSOCIATE MEMBERS + LIAISON MEMBERS

20 All Rights Reserved | FIDO Alliance | Copyright 2017

Scientific Impact:

- The initial results are published in the Proceedings of CRYPTO 2021
- There are already follow-up works

Solution:

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

Broader Impact and Broader Participation:

- Our work provides useful feedback to FIDO2 Alliance and the standard bodies
- The initial work was an integral part of the PhD thesis of Shan Chen, who is now an Assistant Professor

Award # 1946919 SaTC: CORE: Small: Authentication on the Web: Provable Security for Emerging Protocols
PI: Alexandra Boldyreva, Georgia Tech