Privacy and Security of FIDO2 Revisited

Manuel Barbosa[12] Alexandra Boldyreva[3] Shan Chen[4]
Kaishuo Cheng[3] Luís Esquível[1]

1 U.PORTO

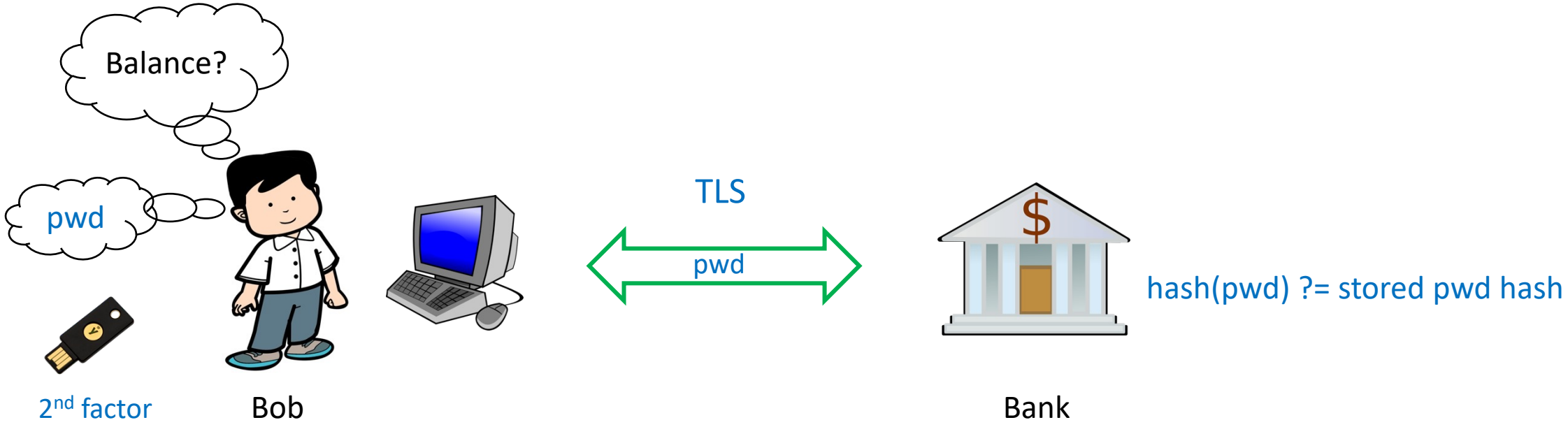
2 MAX-PLANCK-GESELLSCHAFT

3 Georgia Tech

4 SUSTech Southern University of Science and Technology

Typical Client Authentication

password (and possibly 2nd factor device)



The Use of Passwords is Problematic

☹ • Hard to memorize

☹ • Low entropy and subject to brute-force

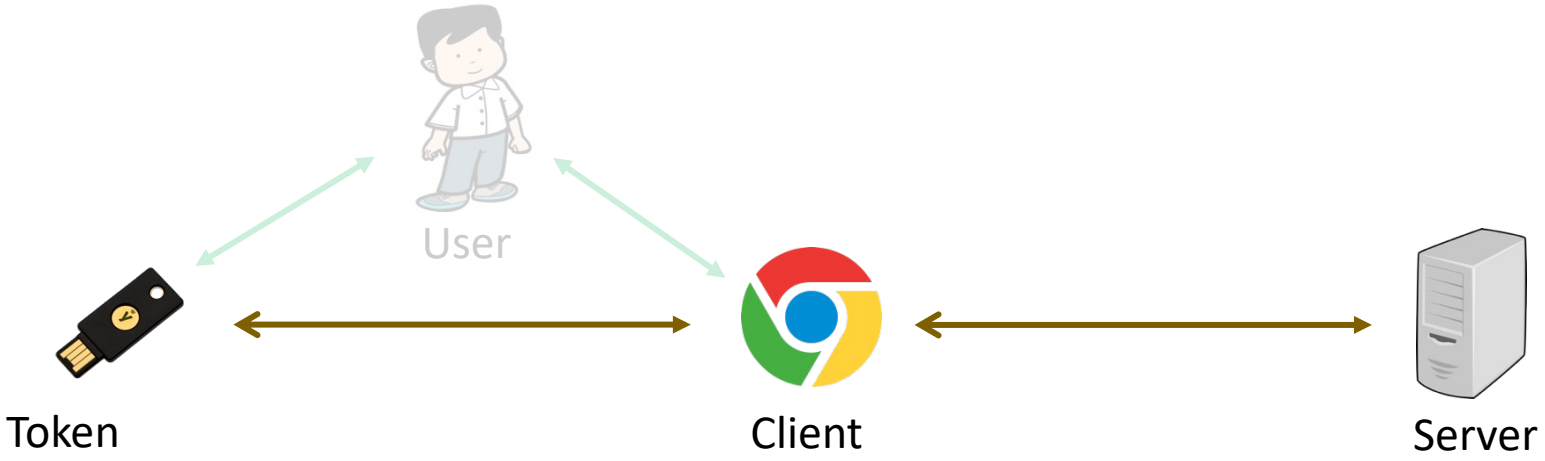
☹ • Vulnerable to phishing attacks even with multi-factor authentication (users can be tricked into sending their MFA codes)

FIDO2

- Standard for passwordless authentication driven by the Fast Identity Online (FIDO) Alliance
- Widely adopted by browsers, platforms, industry (Amazon, Apple, Google, Intel, Microsoft, RSA, VISA ...)

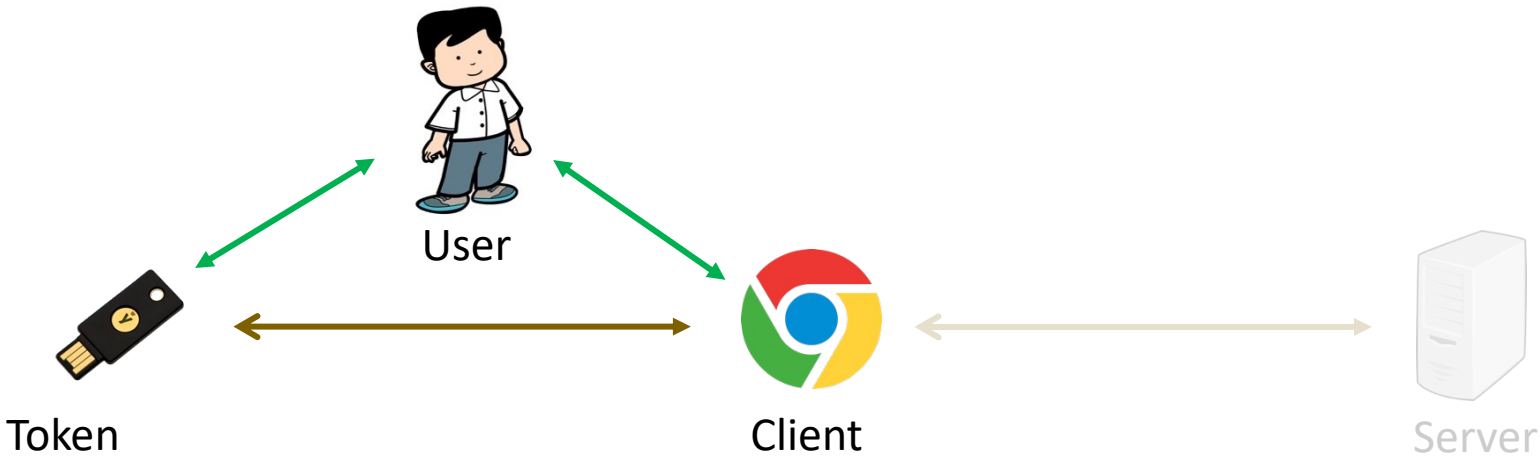
FIDO2 Overview

- Parties: user, authenticator (token), client (browser), server
- Two subprotocols:
  - WebAuthn: authorizes the token/user to the server
  - CTAP: ensures only an authorized client talks with the authenticator



FIDO2 Overview

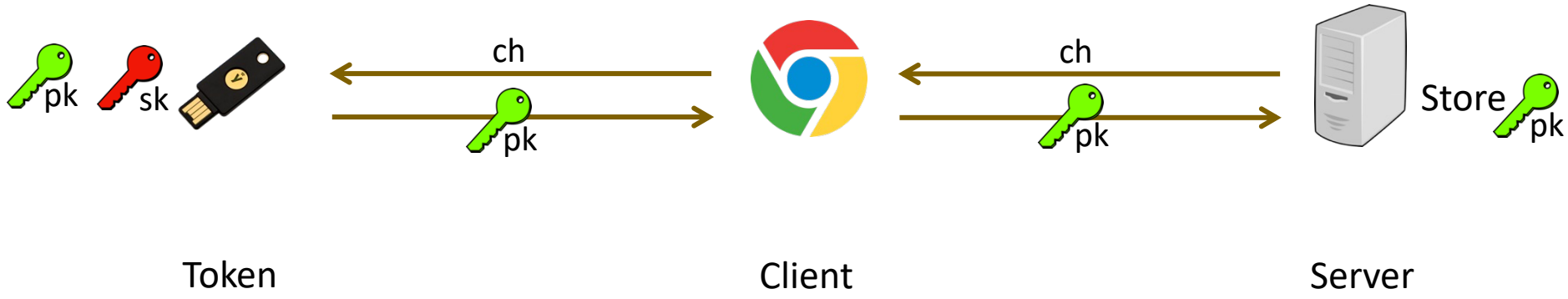
- Parties: user, token, client (browser), server
- Two subprotocols:
  - WebAuthn: authorizes the token/user to the server
  - CTAP: ensures only an authorized client talks with the authenticator



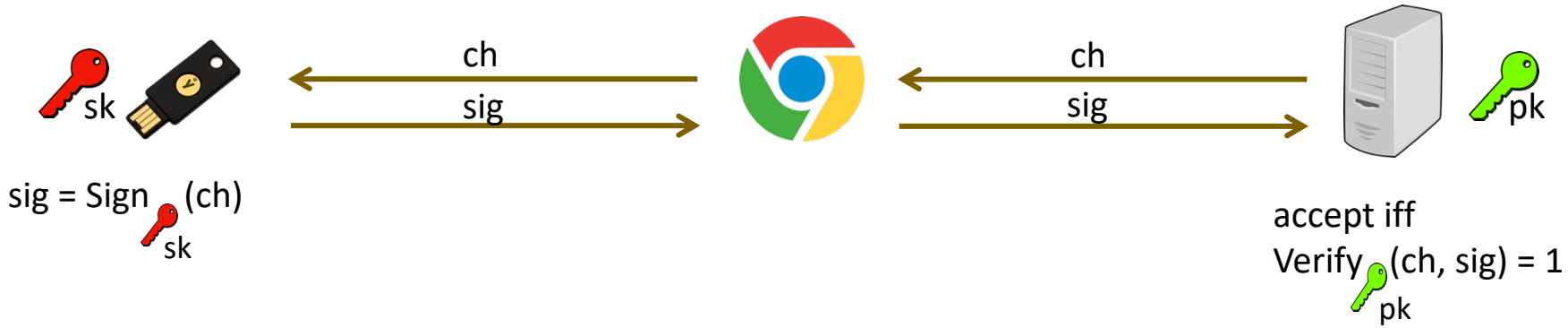
FIDO2 Overview

WebAuthn: challenge-response protocol

- Registration

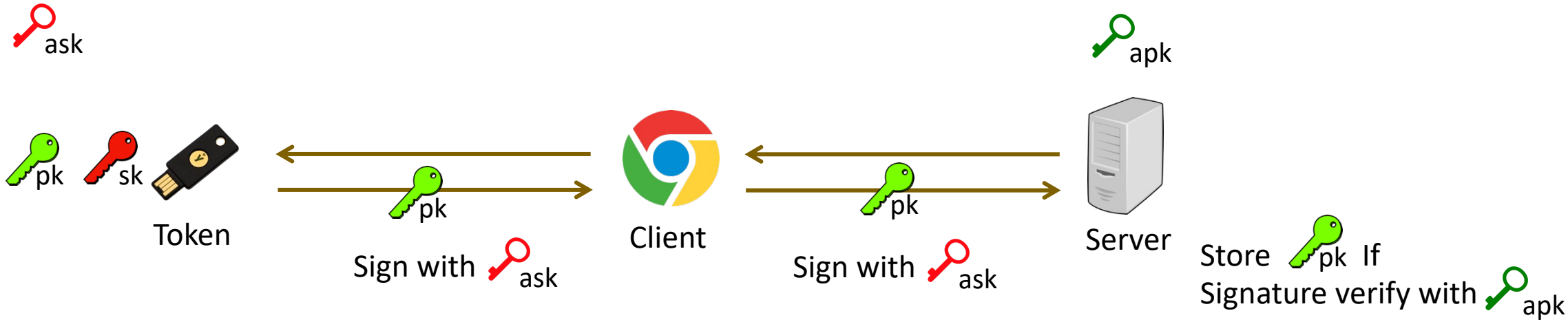


- Authentication



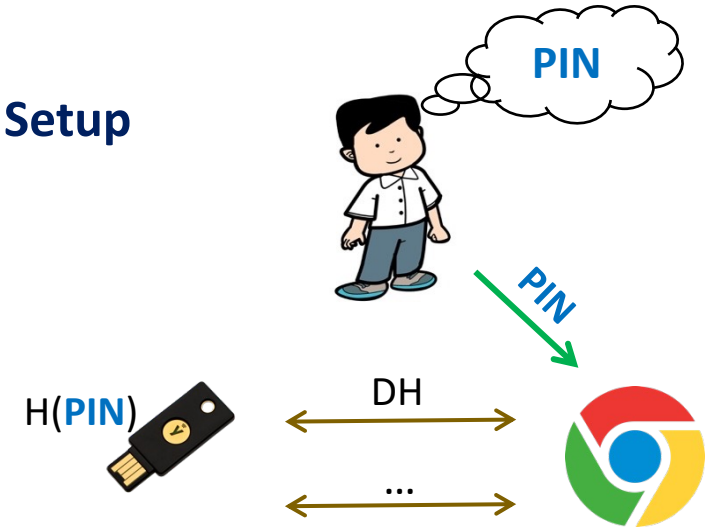
FIDO2 Overview

Optional Attestation in Registration

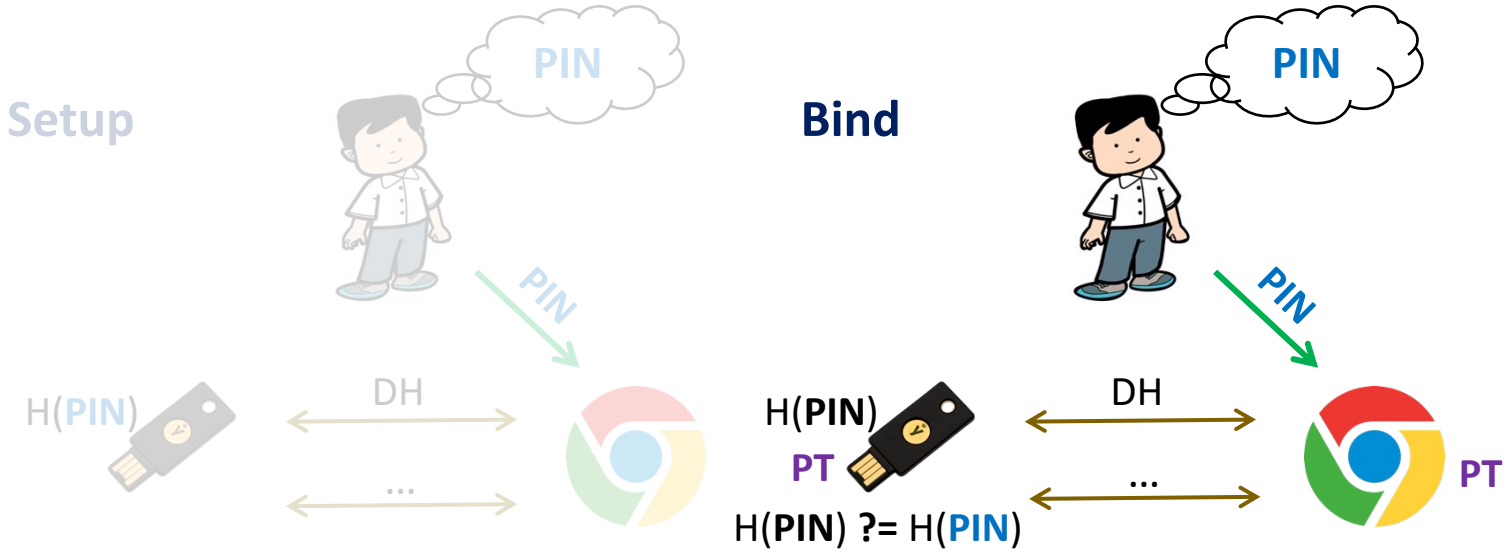


FIDO2 – CTAP2.1

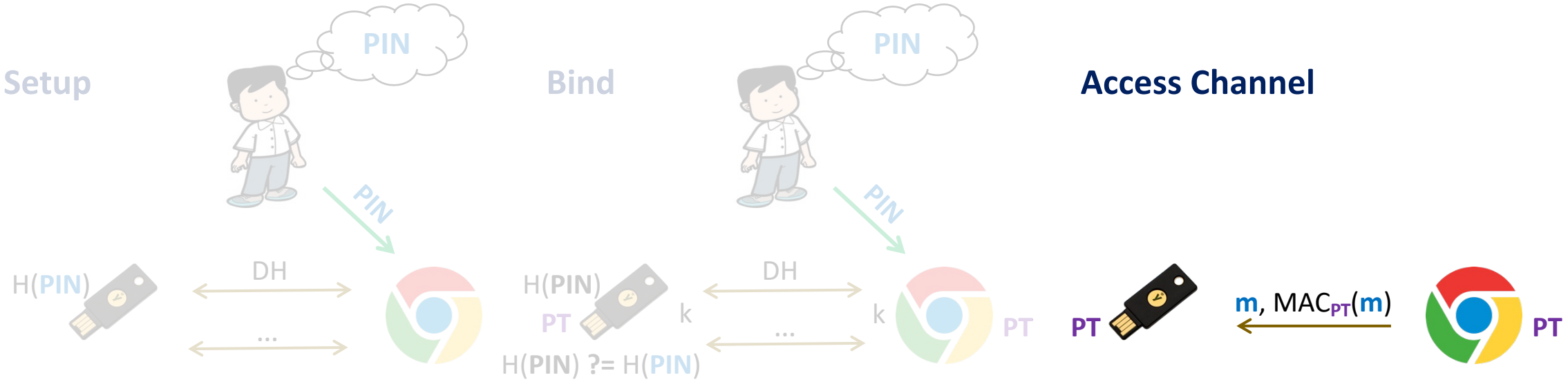
Setup



FIDO2 – CTAP2.1



FIDO2 – CTAP2.1



Security of FIDO2 (Informally)

- Privacy: No adversary should be able to link different registrations coming from the same token.

- Authentication security: No adversary should be able to authenticate on behalf of a token that it does not control.

Prior Work

	BBCW21	HLW23	BCZ23	BGGR23	This Work
Privacy					
WebAuthn	✗	✓	✗	✓	✓
CTAP	✗	✗	✗	✗	✓
Authentication Security					
WebAuthn	✓	✓	✓	✓	✓
CTAP	✓	✗	✓	✗	✓
Active adversary during registration	✓	✓	✗	✓	✓
Tokens sharing attestation key	✗	✓	✓	✓	✓

Our Contributions

Privacy:

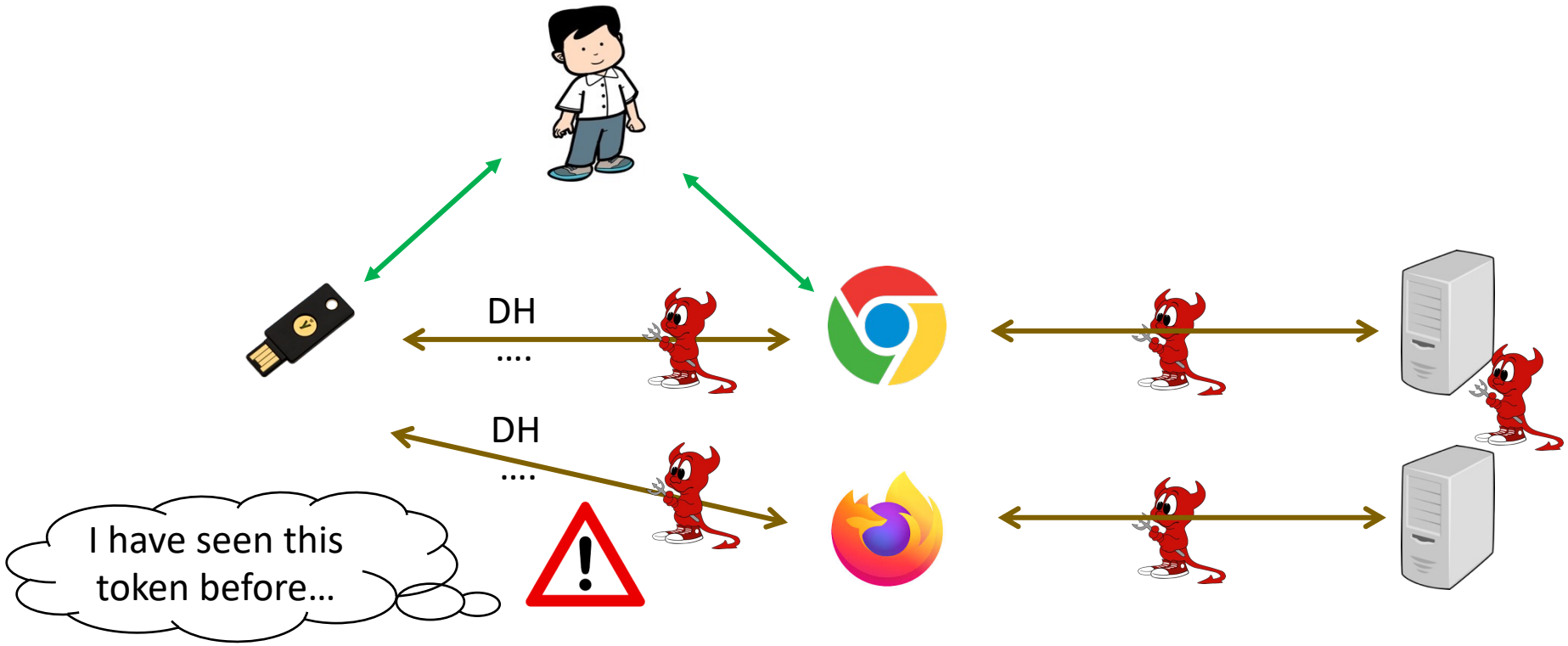
- We formally designed a new privacy model for the entire FIDO2 that allows attackers to observe CTAP communication.
- We analyzed FIDO2 in our privacy model, identified potential risks, and proposed fixes that require minor changes.

Authentication Security:

- We identified gaps in prior CTAP2.1 security analyses and gave our new formal authentication security model.
- We analyzed FIDO2 in our authentication model and proposed fixes that require minor changes.

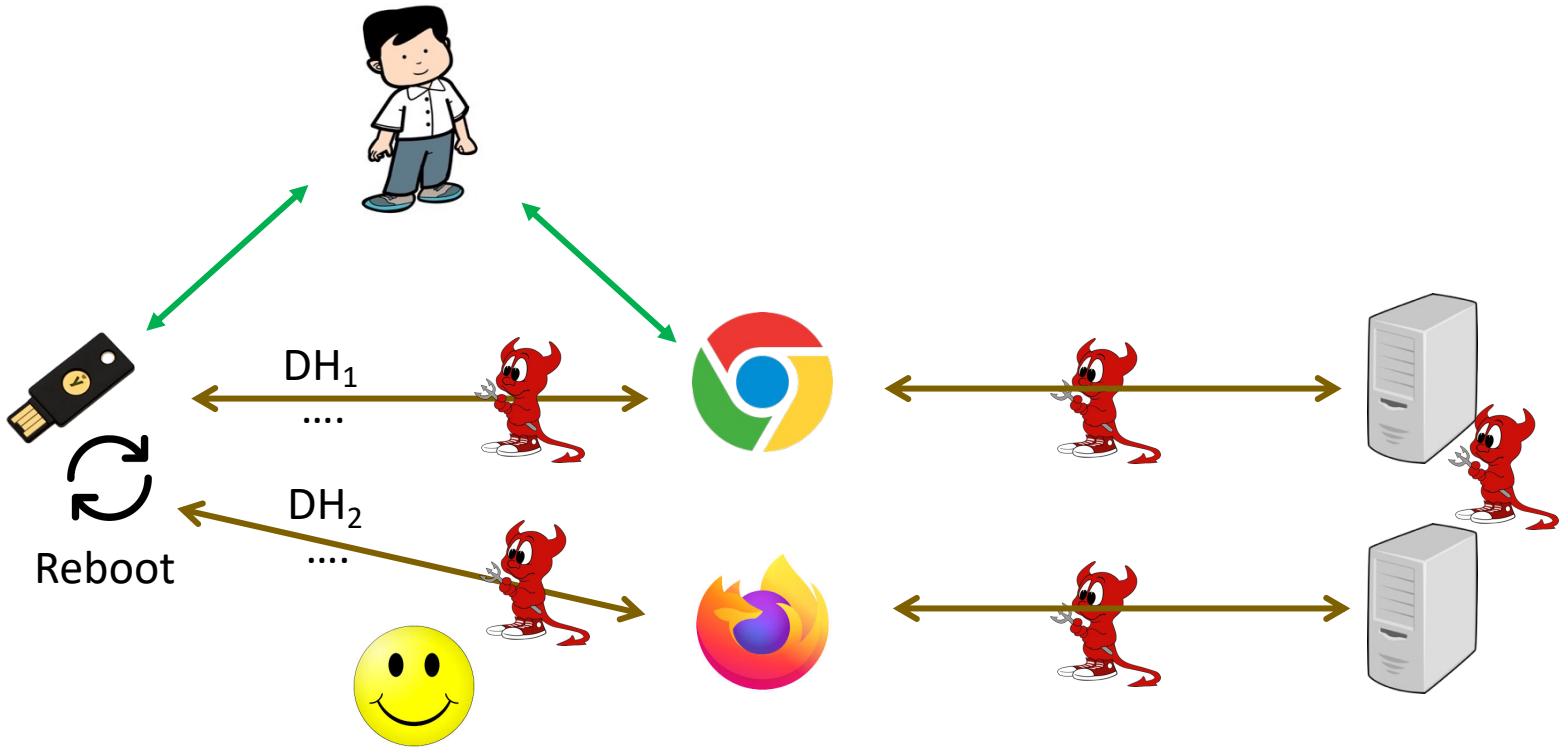
FIDO2 does not Achieve Privacy

CTAP2.1 reuses token DH shares until token is plugged out.



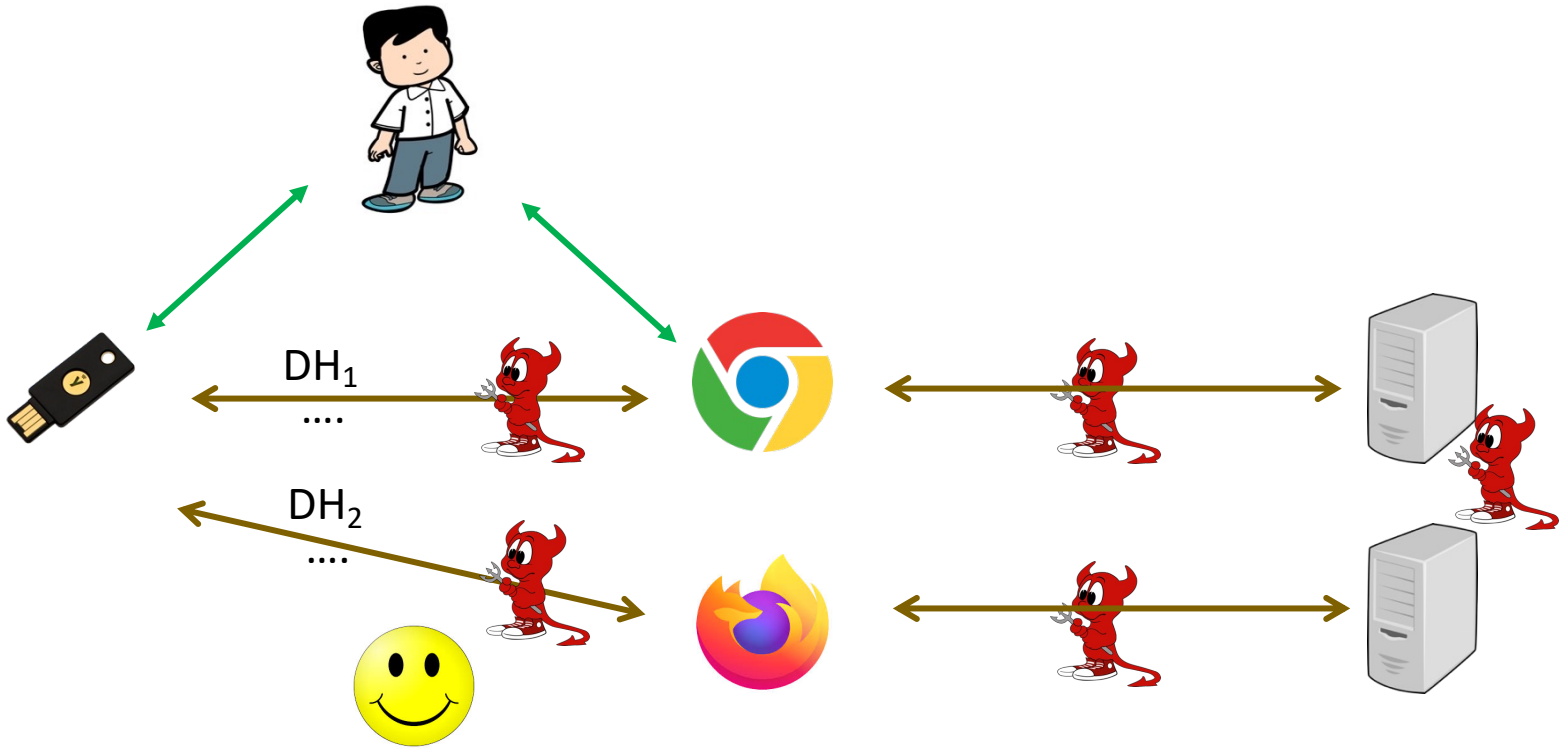
FIDO2 Achieves Privacy when users keep rebooting

Assuming user reboots the token after each usage, we prove that FIDO2 achieves privacy.



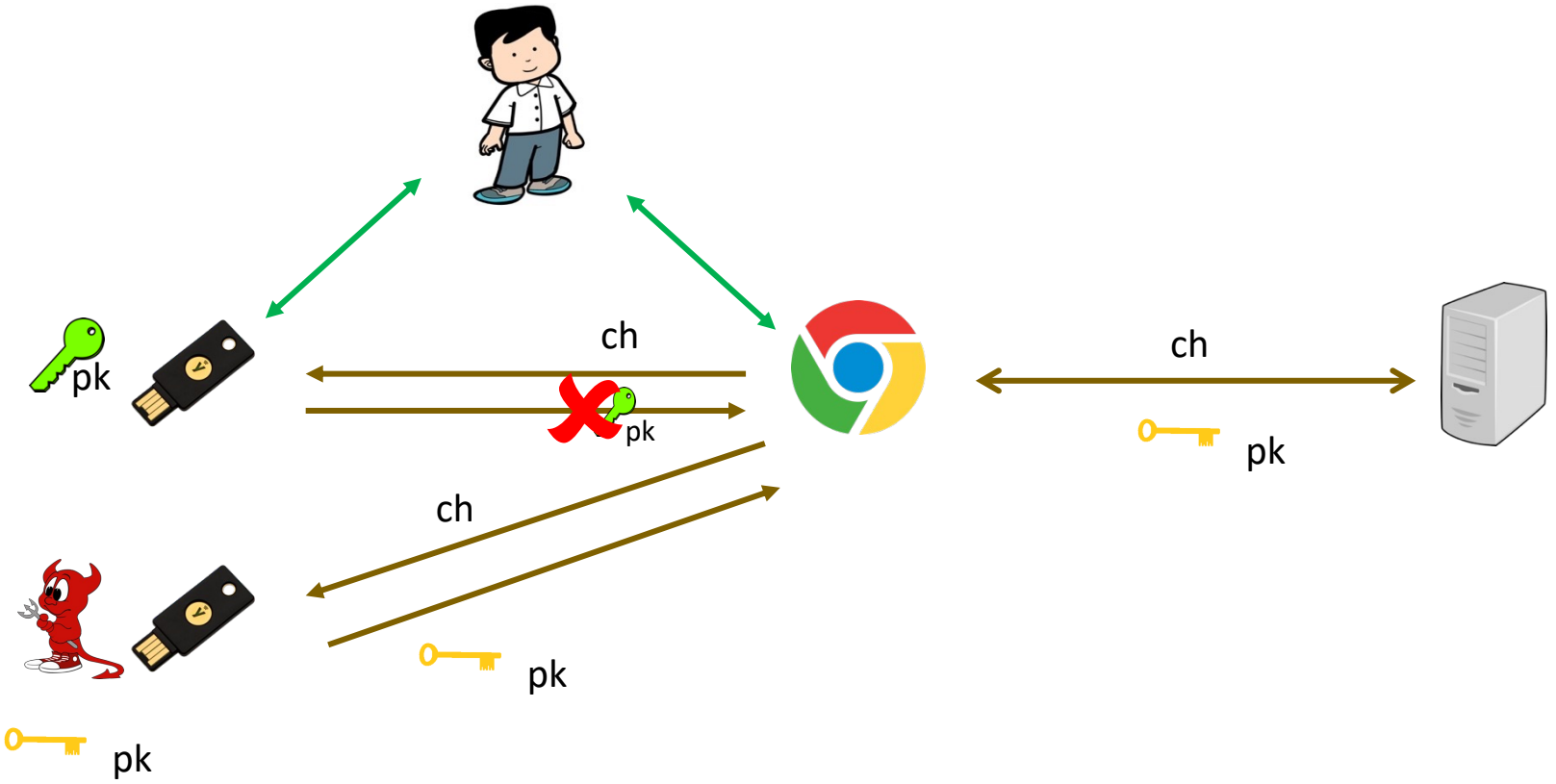
Our Improvement

We prove that FIDO2 achieves privacy without requiring user rebooting, if CTAP2.1 protocol refreshes DH shares after each binding operation.



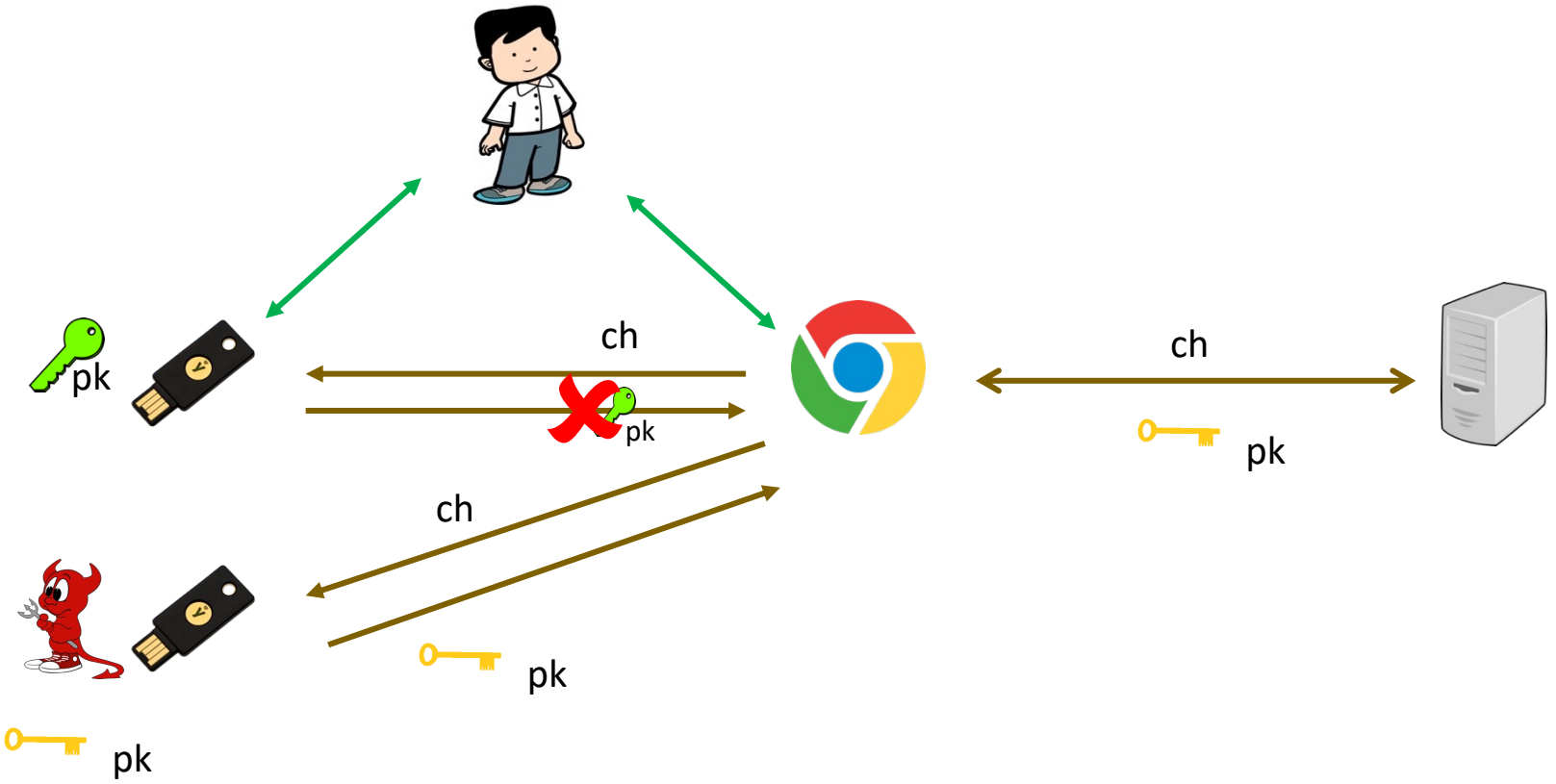
FIDO2 does not achieve authentication security

Rogue Key Attack [BCE23]



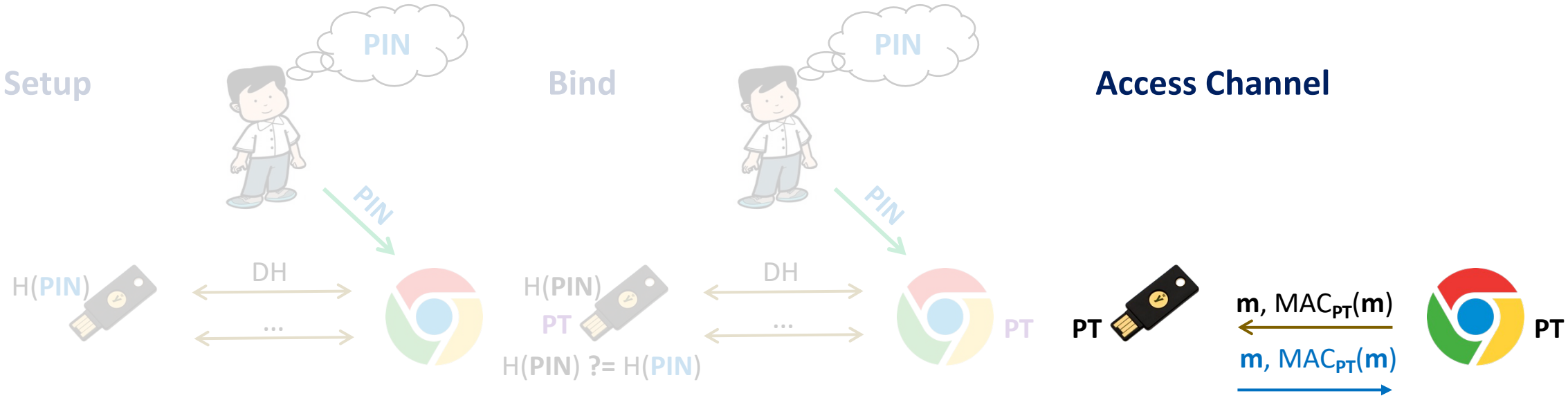
Prior works proved authentication security in weaker security models that did not allow for rogue-key attacks

- Server learns a prior token's unique attestation public key. [BBCW21]
- Attacker is passive during registration phase. [BCZ23]



Our Improvement

We prove that FIDO2 achieves authentication security if messages from token to client are authenticated as well. (adding backward authentication)



Summary:

- We designed a new privacy model for the entire FIDO2, analyzed FIDO2 in our privacy model, identified potential risks, and proposed fixes that require minor changes.

- We identified gaps in prior works, designed a new authentication security model, analyzed FIDO2 in our authentication model and proposed fixes that require minor changes.

The full paper is available at https://eprint.iacr.org/2025/459