CTRAPS: CTAP Client Impersonation and API Confusion on FIDO2

Marco Casagrande (EURECOM, KTH) and Daniele Antonioli (EURECOM)

EURECOM
Sophia Antipolis

Abstract: FIDO2 is the de-facto standard for passwordless and two-factor authentication. In FIDO, User authenticates to a Relying Partiy, e.g., online service, using Client, e.g., web browser, and Authenticator, e.g., USB dongle. The Client-to-Authenticator Protocol (CTAP) secures Client-Authenticator communications. We assess the security of CTAP and its Authenticator API, finding eight novel design flaws. We exploit them by introducing two novel attack classes. In Client Impersonation (CI), Attacker impersonates a trusted CTAP Client to Authenticator. In API Confusion (AC), Attacker tricks Client, Authenticator, and User into calling an unwanted API. We show how to use CI and AC in eleven attacks that, for example, wipe credentials, perform factory resets, and track users. We successfully evaluate them on six popular authenticators and ten relying parties. We discuss countermeasures and release the CTRAPS open-source toolkit.

1. MOTIVATION

- CTAP Authenticator API is a critical attack surface handling credentials and authenticator settings
- No prior research on CTAP2.2
- Impacts billions of FIDO2 devices
- Destructive operations on sensitive online services

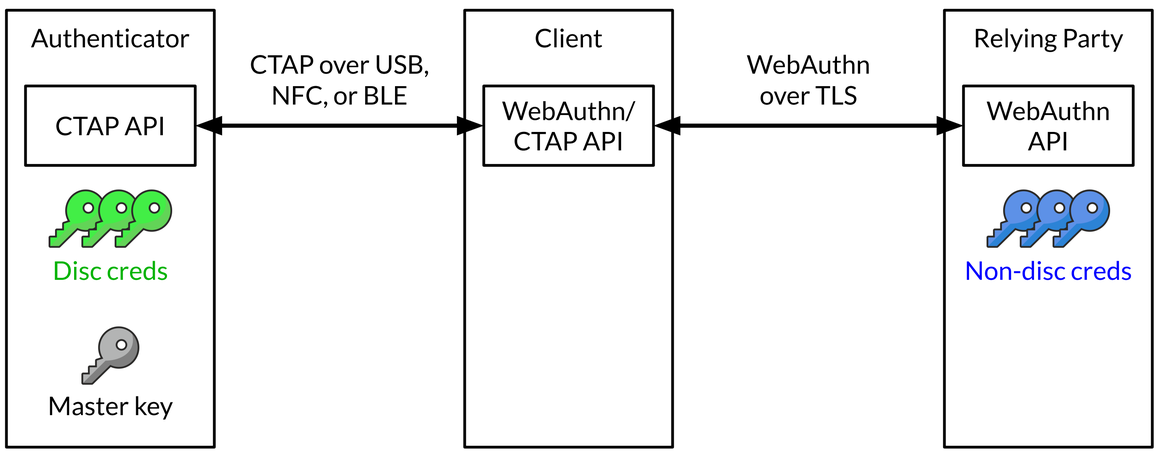
2. CTAP AUTHENTICATOR API

	MakeCred	GetAss	CredMgmt	ClientPin	Reset	Select	GetInfo
UV	Yes	Yes[1]	Yes	Yes[2]	No	No	No
UP	Yes	Yes[1]	No	No	Yes	Yes	No

Yes[1]: depends on Client and Relying Party. Yes[2]: depends on API subcommand

- User Verification (UV), e.g., enter a 6-digit PIN on Client
- User Presence (UP), e.g., press a button on Authenticator

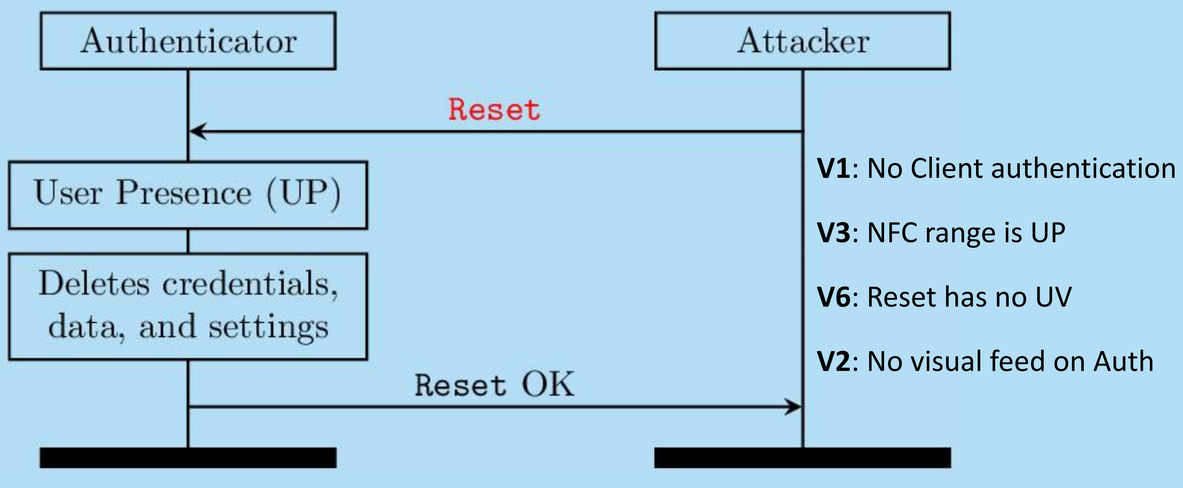
3. THREAT MODEL



- Credentials are public-private key pairs
  - Discoverable creds are stored on Authenticator
  - Non-discoverable creds are stored by Relying Party
  - Master key decrypts credentials before usage
- Two attacker models
  - CI Attacker impersonates CTAP Client to Authenticator
  - AC Attacker MitMs Client and Authenticator
- Deployed from proximity, e.g., using a NFC skimmer, and remote, e.g., using a remotely controllable USB hub

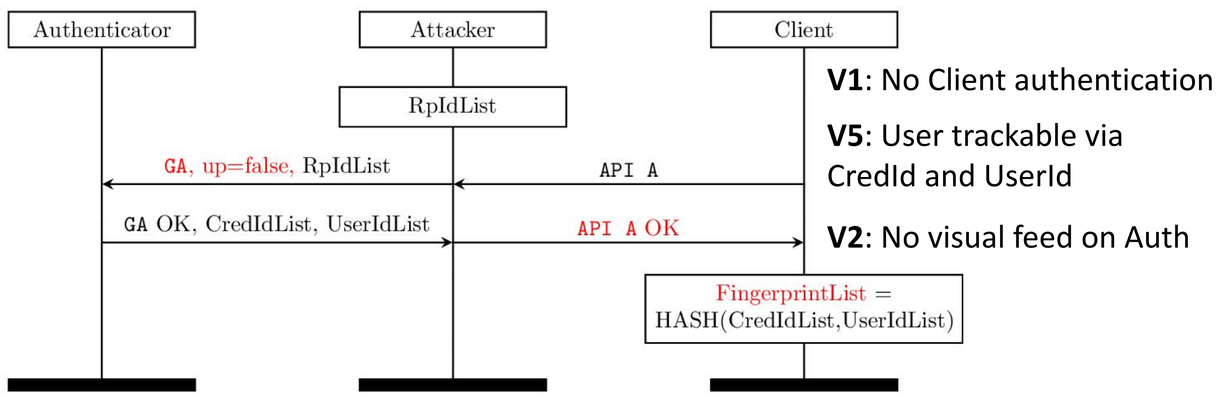
4. CLIENT IMPERSONATION (CI)

- Four CI attacks
- Limited/no user interaction (can bypass UV and/or UP)
- Diagram below shows CI Factory Reset



5. API CONFUSION (AC)

- MitM Attacker between Client and Authenticator
- User calls API A, instead Attacker calls API B with compatible authorizations (UV/UP)
- Seven AC attacks
- Confounds all possible (49) CTAP Auth API combinations
- Diagram below shows AC Tracking User via Creds



6. TOOLKIT AND DEMOS

*Visit **https://github.com/Skiti/ctraps** or scan the QR code for CTRAPS source code and video demos.*

7. EVALUATION

	Client Impersonation				API Confusion						
	Res	Auth	Pin	Info	CrMg	Res	Auth	Reg	Pin	Sel	Info
YubiKey 5 & 5 FIPS, Feitian K9, Solo V1	✓	✓	✓	✓	✓	✓	✓	✓	✓	n/a	✓
Solo V2H, OpenSK	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

- Six popular Authenticators
  - Open and closed source
  - NFC and USB transports
- CI targets four CTAP Auth API, AC targets seven
  - Selection API not supported by four Authenticators

RP	Cred	Delete Creds	Track Users	DoS Auth
DocuSign, Facebook	NonDisc	CI1, AC2	n/a	CI3, AC5, AC6
Apple, Microsoft	DiscWeak	AC1, CI1, AC2	CI2, AC3	AC4, CI3, AC5, AC6
Adobe, GitHub, Hancock, Synology, NVidia, VaultVision	Disc	AC1, CI1, AC2	CI2, AC3	AC4, CI3, AC5, AC6

- Ten widely used Relying Parties
  - Apple and Microsoft use discoverable creds without protecting them by requiring UV
- Affected by nine (out of eleven) CTRAPS attacks
  - Despite Attacker using CTAP and not WebAuthn
- Implementation flaw on YubiKeys (CVE-2024-35311)
  - Leak of Relying Parties registered using a YubiKey

10th IEEE European Symposium on Security and Privacy, June 30–July 4, 2025.