CTRAPS: CTAP Client Impersonation and API Confusion on FIDO2

DEF CON 33

M. Casagrande D. Antonioli

KTH VETENSKAP OCH KONST

DEFCON

ORSHIN

EURECOM Sophia Antipolis

Daniele Antonioli

- Asst. Prof at EURECOM (France)
  - Software and System Security (S3) group
- Research **security and privacy**
  - Bluetooth (BLUFFS, BLURtooth, BIAS, KNOB, …)
  - E-Scooters (E-Spoofer, E-Trojans, …)
  - FIDO2 (CTRAPS, …)
  - Web tracking (FP-tracer, …)
  - …
- More at https://francozappa.github.io

Marco Casagrande

- Postdoc at KTH (Sweden),
  - Networked Systems Security (NSS) group P. Papadimitratos
  - PhD at EURECOM (France), Dec 2024, D. Antonioli
- Research in Security and Privacy
  - Proprietary protocols (fitness trackers, e-scooters, …)
  - Standard protocols (BLE, Wi-Fi, NFC, FIDO2, …)
  - Mobile (Android, …)

CTRAPS Talk Outline

1. Introduction
2. Background and Threat Model
3. Client Impersonation (CI) Attacks and Demo
4. API Confusion (AC) Attacks and Demo
5. Vulnerabilities and Toolkit
6. Evaluation
7. Countermeasures and Disclosure

References

CTRAPS Research Paper (IEEE EuroS&P25)

CTRAPS: CTAP Client Impersonation and API Confusion on FIDO2

Marco Casagrande
Department of Digital Security
EURECOM
Sophia Antipolis, France
marco.casagrande@eurecom.fr

Daniele Antonioli
Department of Digital Security
EURECOM
Sophia Antipolis, France
daniele.antonioli@eurecom.fr

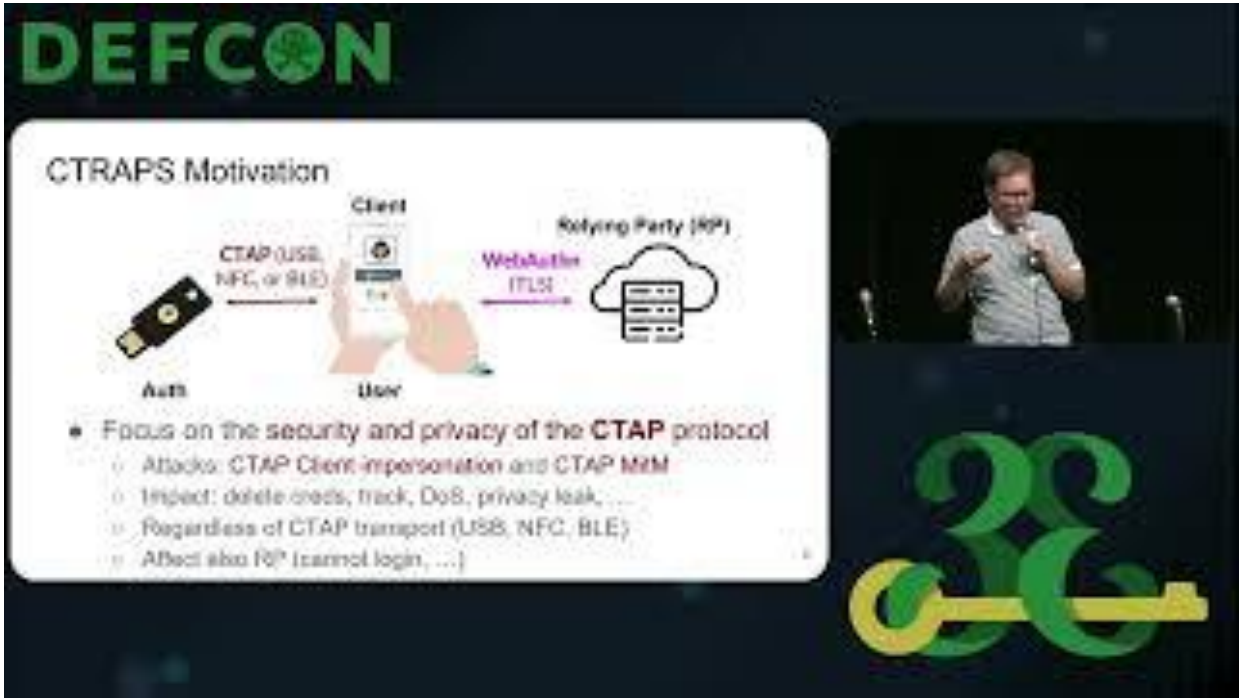
***Abstract*—FIDO2 is a popular technology for single-factor and second-factor authentication. It is specified in an open standard including the WebAuthn and CTAP application layer protocols. We focus on CTAP which allows the communication between FIDO2 clients and authenticators. No prior work explored the CTAP Authenticator API which is a critical protocol-level attack surface as it deals with credential creation, deletion, and management. We address this gap by presenting the first security and privacy evaluation of the CTAP Authenticator API. We uncover two classes of CTAP protocol-level attacks we call CTRAPS.**

FIDO market to rapidly grow from USD 230.6 million in 2022 to USD 598.6 million in 2031 [60]. Yubico, a FIDO authenticator market leader, sold more than 22 million YubiKey authenticators [67]. This growth will continue because of the recent industry-wide push towards single-factor passkey-based authentication [20], [29], [56].

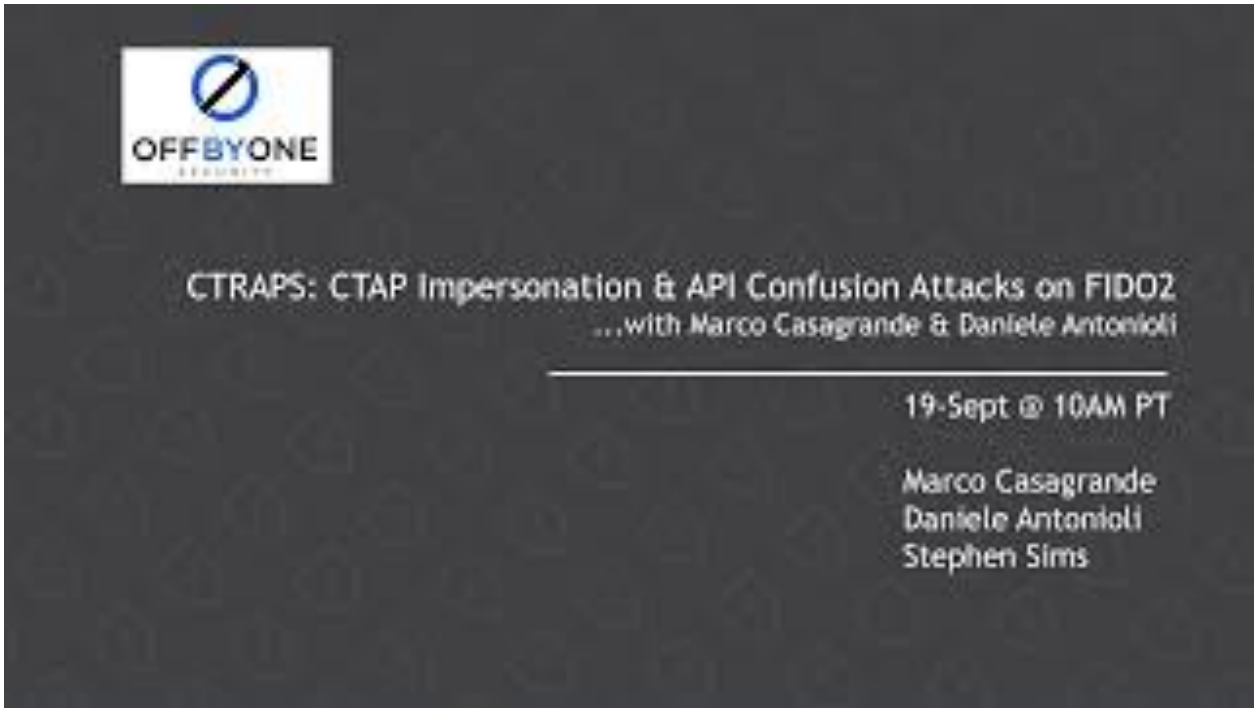
FIDO2 involves three entities: an *authenticator* that generates and asserts possession of authentication credentials (e.g., public-private key pairs), a *relying party* that authenticates the user (e.g., challenge-response protocol based on credentials), and a *client* who wants to authenti-

https://francozappa.github.io/publication/2025/ctraps/

CTRAPS DEF CON 33 Talk



CTRAPS OffByOne Security Podcast

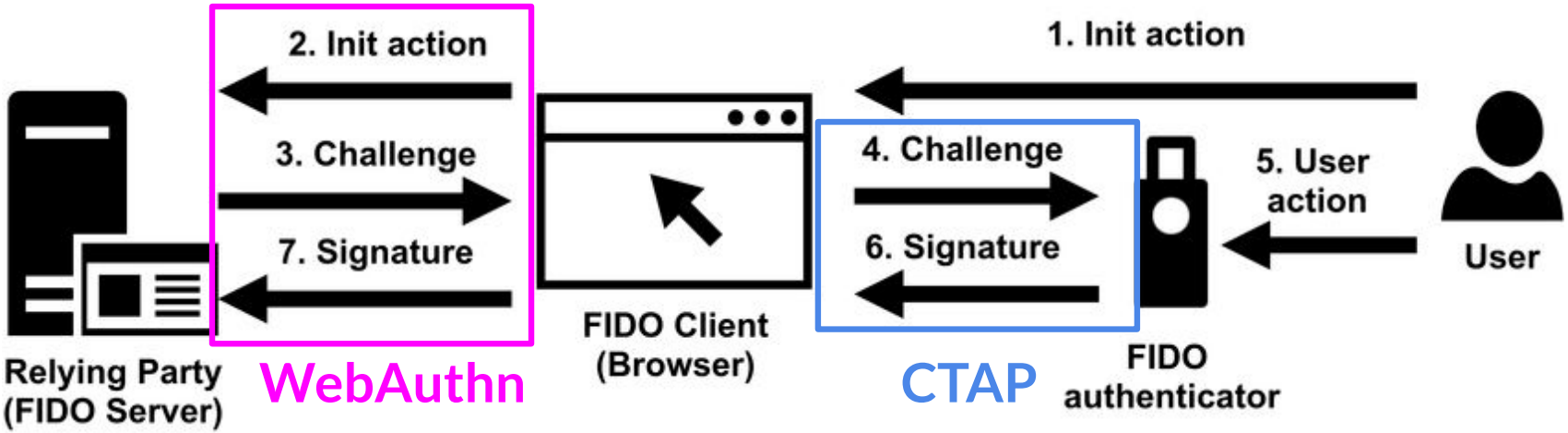


Introduction

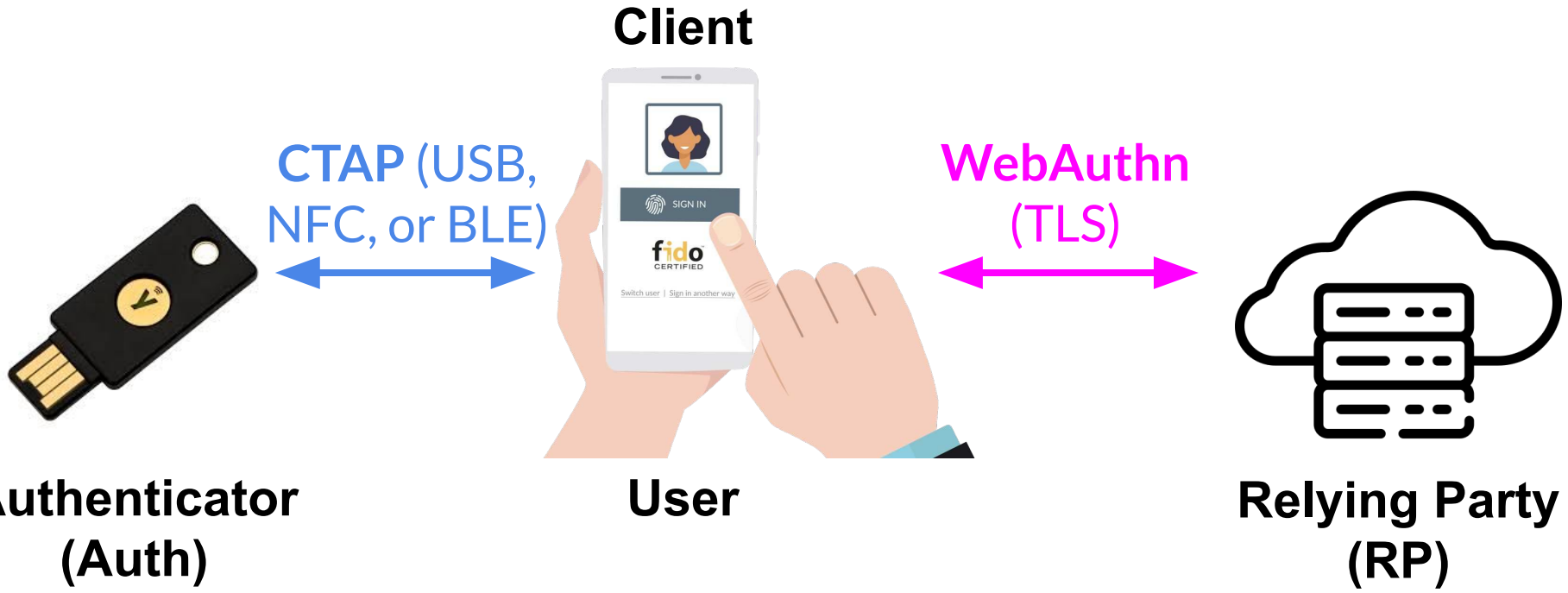
FIDO2 Introduction

- **Fast IDentity Online 2 (FIDO2)**
  - Open authentication standard
  - Resilient to *phishing (password compromise)*
  - *Authenticator*: USB dongle, smartphone, …
  - *Credentials*: key pairs used to authenticate
- **Second-factor** auth (2FA)
  - Login with username, password, and Authenticator
- **Passwordless** auth (passkey)
  - Login with Authenticator

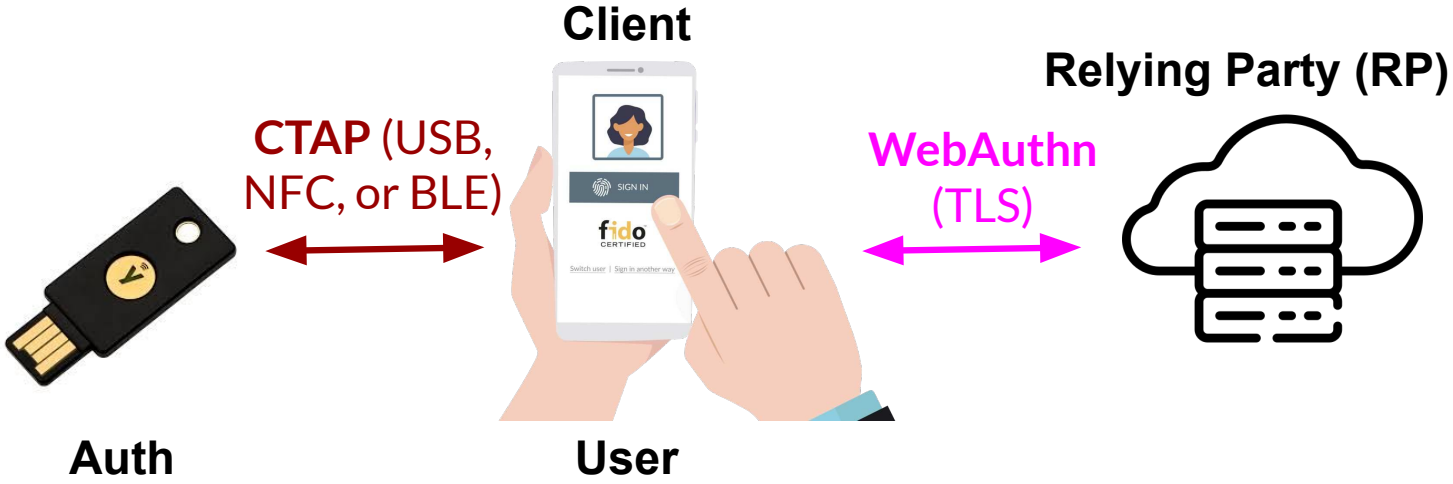
FIDO2 Auth Flow (simplified) [ref]



FIDO2 **Entities** and **CTAP** and **WebAuthn** Protocols



CTRAPS Motivation



- Focus on the security and privacy of the **CTAP** protocol
  - Attacks: CTAP Client impersonation and CTAP MitM
  - Impact: delete creds, track, DoS, privacy leak, …
  - Regardless of CTAP transport (USB, NFC, BLE)
  - Affect also RP (cannot login, …)

CTRAPS Contributions

- **8 CTAP design vulns** (V_1, …,V_8)
  - Affecting millions of FIDO2 devices (billions of credentials)
- **11 CTRAPS attacks**
  - 4 Client Impersonation (CI_1, …, CI_4)
  - 7 API Confusion MitM (AC_1, …, AC_7)
- Open source CTRAPS toolkit
  - Virtual CTAP testbed, 4 attack Clients, …
- Evaluation **exploiting 16 FIDO2 entities**
  - 6 Auth (Yubico, Feitian, …), 10 RP (Apple, Microsoft, Nvidia, …)
- Discuss **8 design fixes** compliant with FIDO2

Background and Threat Model

FIDO2 Credentials and Authentication

- FIDO2 credentials
  - ECDSA key pairs, *sign (prikey), verify (pubkey)*
  - *Non-discoverable*: enc prikey stored on RP (2FA)
  - *Discoverable*: enc prikey stored on Auth (passkey)
  - Cred prikey encrypted with Auth master key
- FIDO2 auth flow
  - Make a FIDO2 cred and store cred keys
  - Use Auth cred to authenticate User to RP
  - Challenge from RP, signed response from Auth

CTAP Introduction

- **CTAP (Client to Authenticator Protocol)**
  - Standard AL protocol over USB, NFC, or BLE
  - Client request and Auth respond
- *CTAP1* (known as U2F)
  - Standardized 2FA with non-disc creds
  - Authenticator API (create cred, auth cred, …)
- *CTAP2* (latest v2.2)
  - Standardized passwordless with disc creds
  - Extended Authenticator API (cred tracking protection, …)

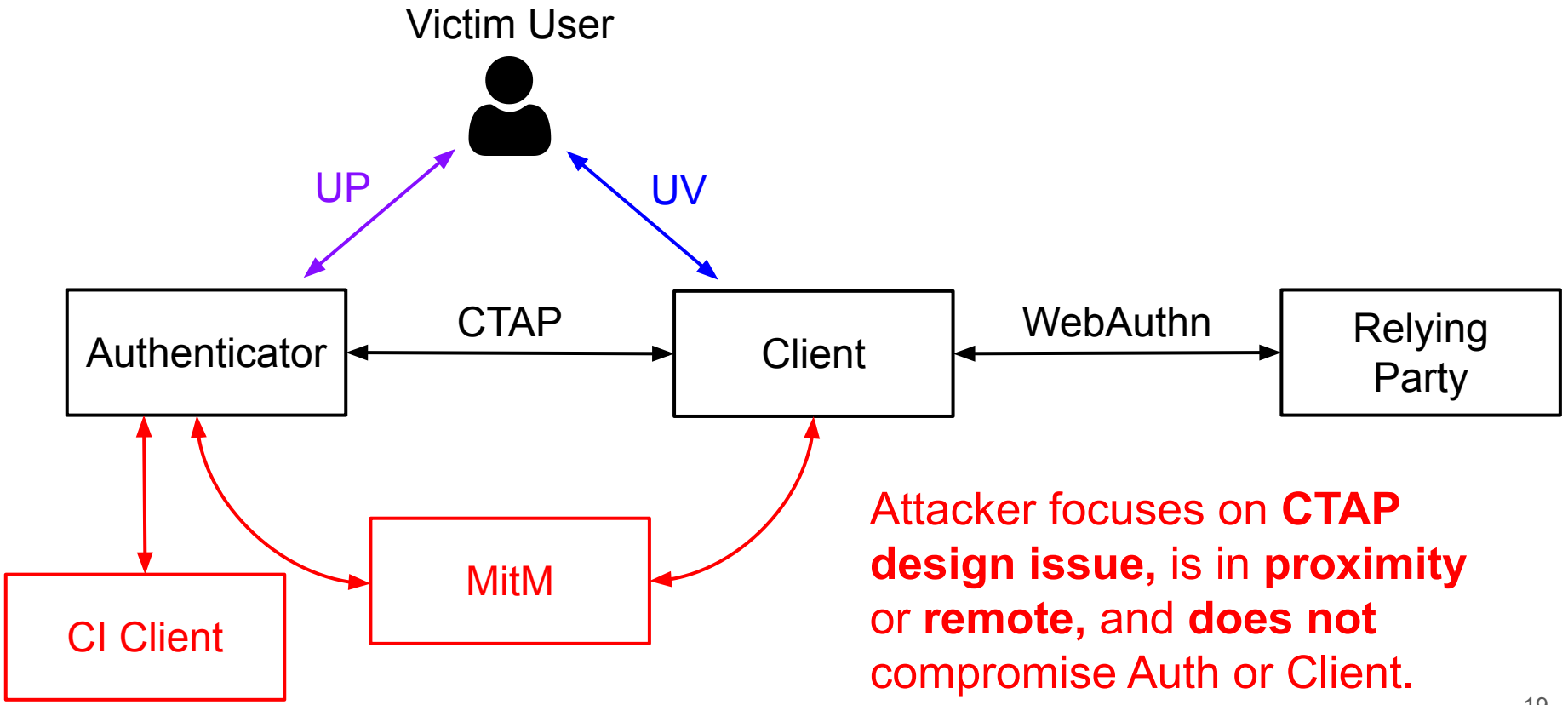
Focus 7 Core CTAP Authenticator APIs

CTAP API	UV	UP	Subcmd
MakeCred (MC)	Yes	Yes	No
GetAssertion (GA)	Opt	Opt	Yes
CredMgmt (CM)	Yes	No	Yes
ClientPin (CP)	Opt	No	Yes
Reset (Re)	No	Yes	No
Selection (Se)	No	Yes	No
GetInfo (GI)	No	No	No

EnumRpis,
EmumCreds, ...

User Verification (UV): eg: PIN on Client verified by Auth
User Presence (UP): eg: Auth and Client are in NFC range

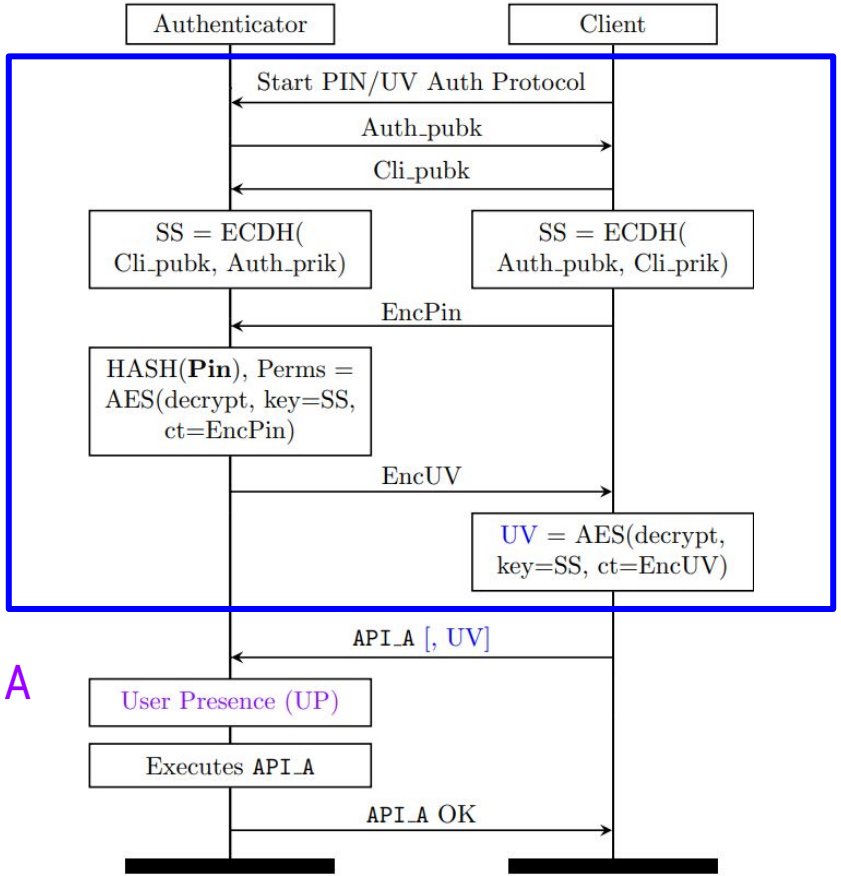
CTRAPS Threat Model



Attacker focuses on **CTAP design issue,** is in **proximity** or **remote,** and **does not** compromise Auth or Client.

Client Impersonation (CI) Attacks and Demos

CTAP Authenticator API Call (UV, UP)

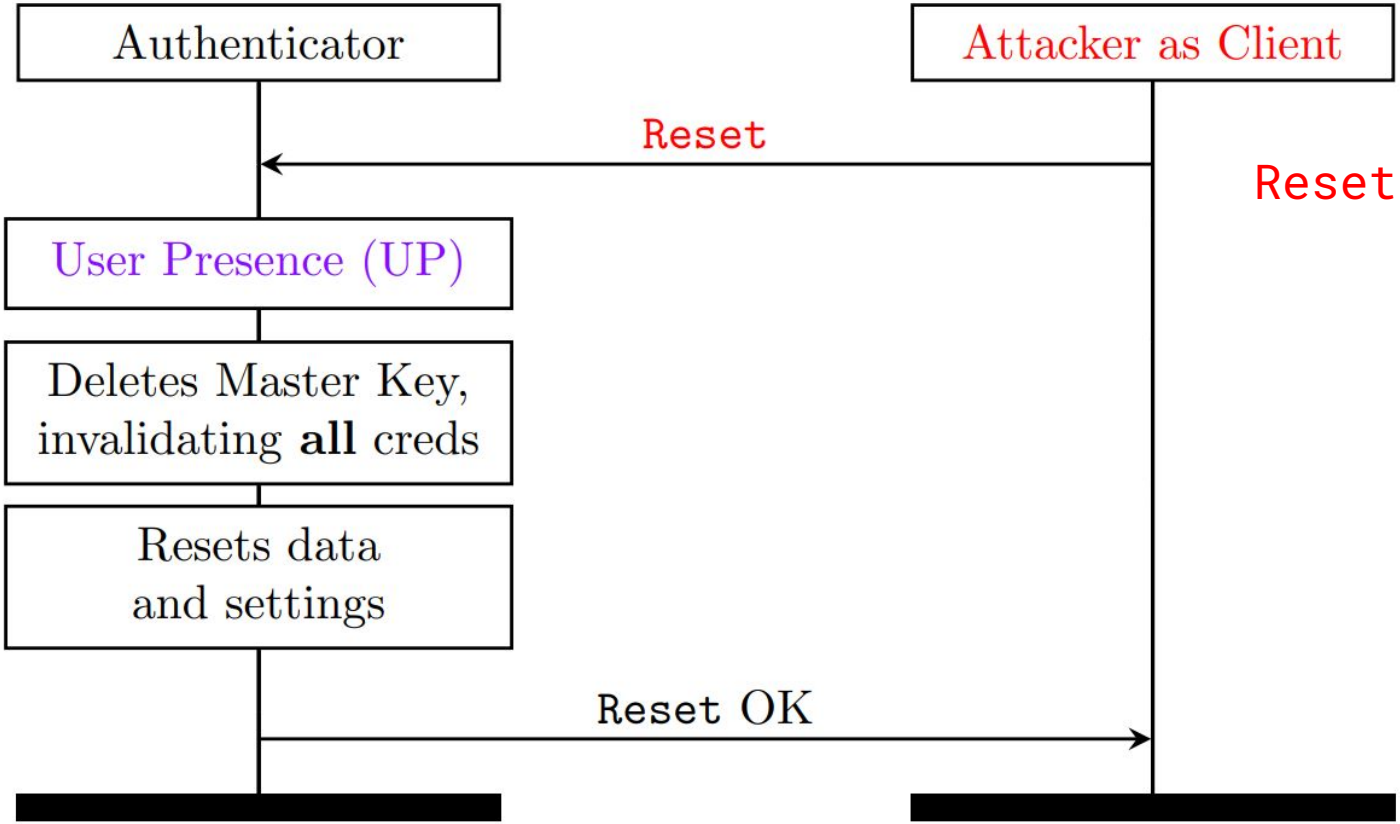


Auth and Client run PIN/UV Auth protocol **if** API_A requires UV

UV **reusable** within a session

UP test **if** API_A requires UP

CI_1: Factory Reset Auth

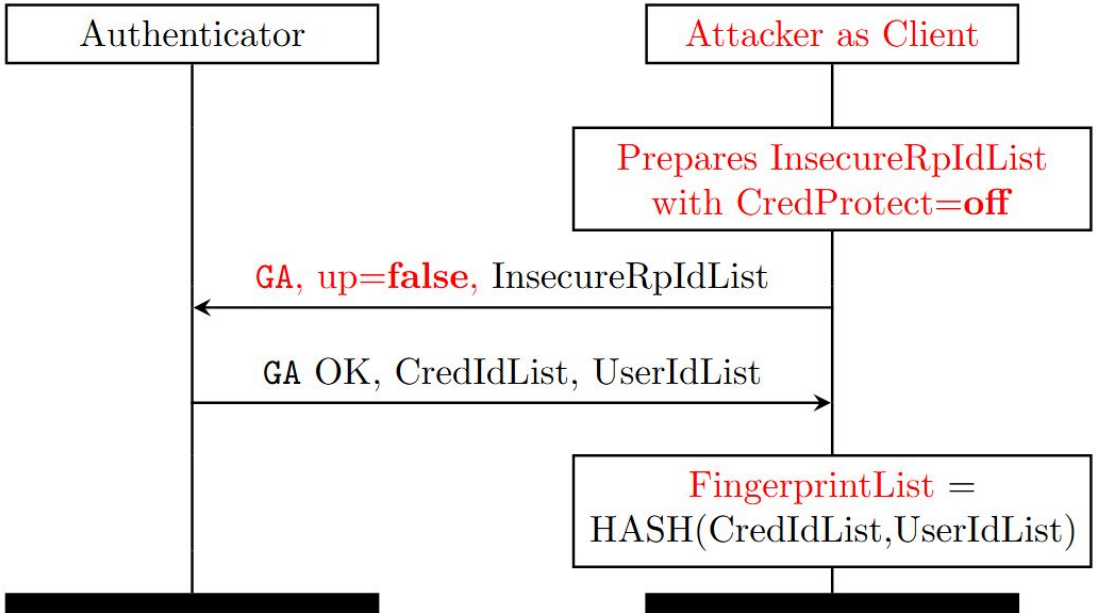


`Reset` requires UP

DEMO CI_1: Factory Reset Auth over NFC

CI_2: Track User from Discov Creds in Auth

GA=GetAssertion, no UV if CredProtect=off. Eg: Apple, Microsoft



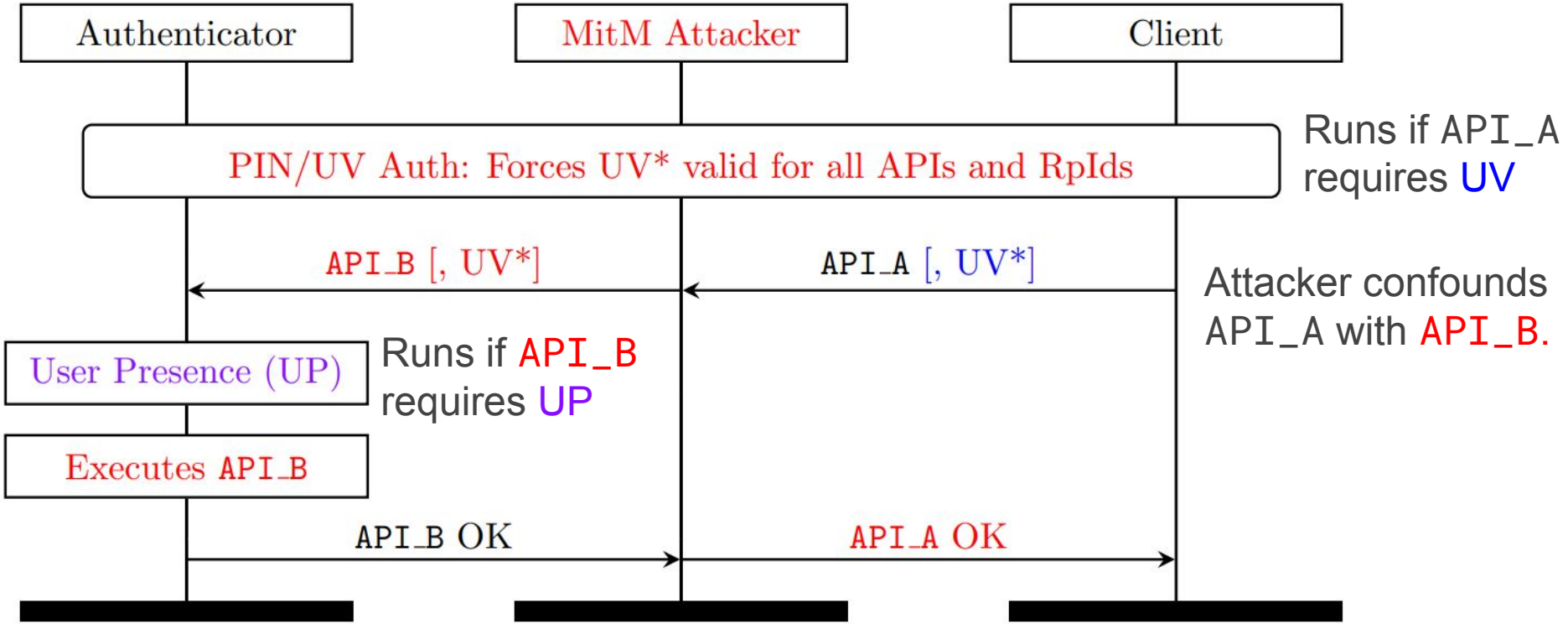
DEMO CI_2: User Tracking via Creds over NFC

Four Client Impersonation (CI) Attacks Summary

- **CI_1**: Factory Reset Authenticator (`Reset`)
- **CI_2**: Track User from Credentials (`GetAssertion`)
- **CI_3**: Force Authenticator Lockout (`ClientPin`)
- **CI_4**: Profile Authenticator (`GetInfo`)

API Confusion (AC) Attacks and Demos

API Confusion (AC) Attack Technique

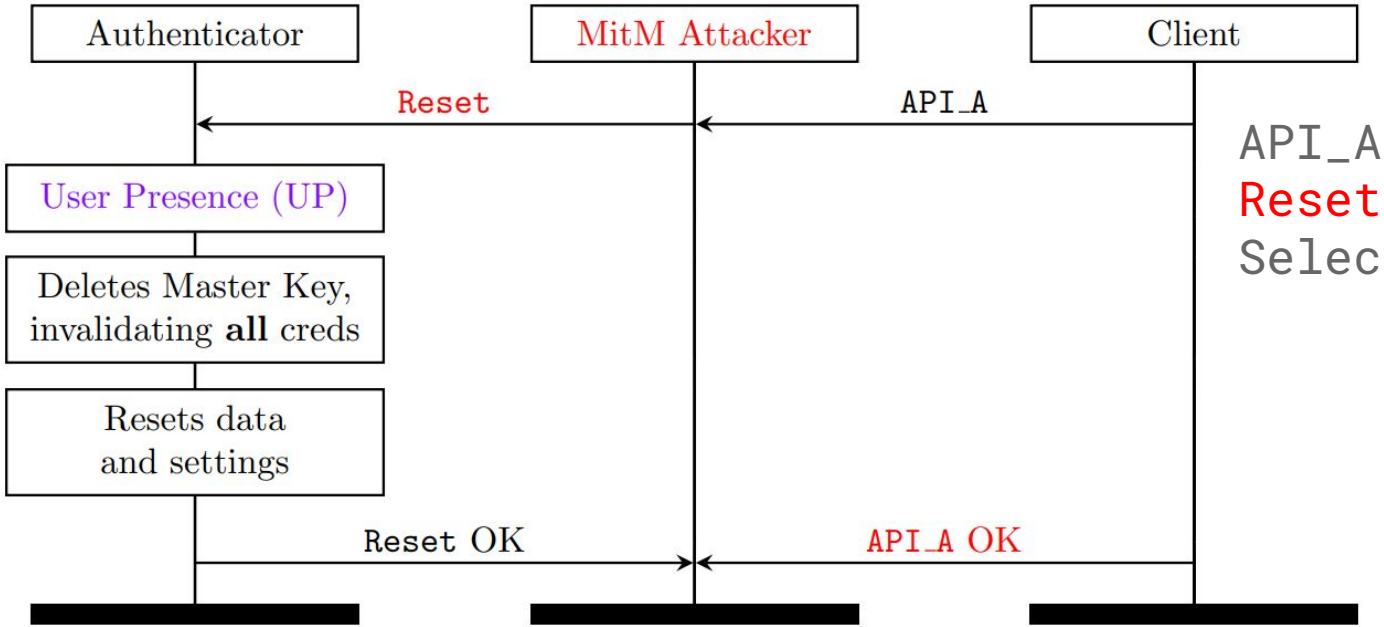


AC CTAP API Combinations

	CM	Re	GA	MC	CP	Se	GI
MC	✓	✓	✓	n/a	✓	✓	✓
GA	✓	✓	n/a	✓	✓	✓	✓
CM	n/a	✓[1]	✓	✓[1]	✓	✓	✓
CP	✓	✓[1]	✓	✓[1]	n/a	✓	✓
Re	n/a	n/a	✓[2]	n/a	✓	✓	✓
Se	n/a	✓	✓[2]	n/a	✓	n/a	✓
GI	n/a	✓[1]	✓[2]	✓	✓	✓	n/a
Total	3	6	6	4	6	6	6

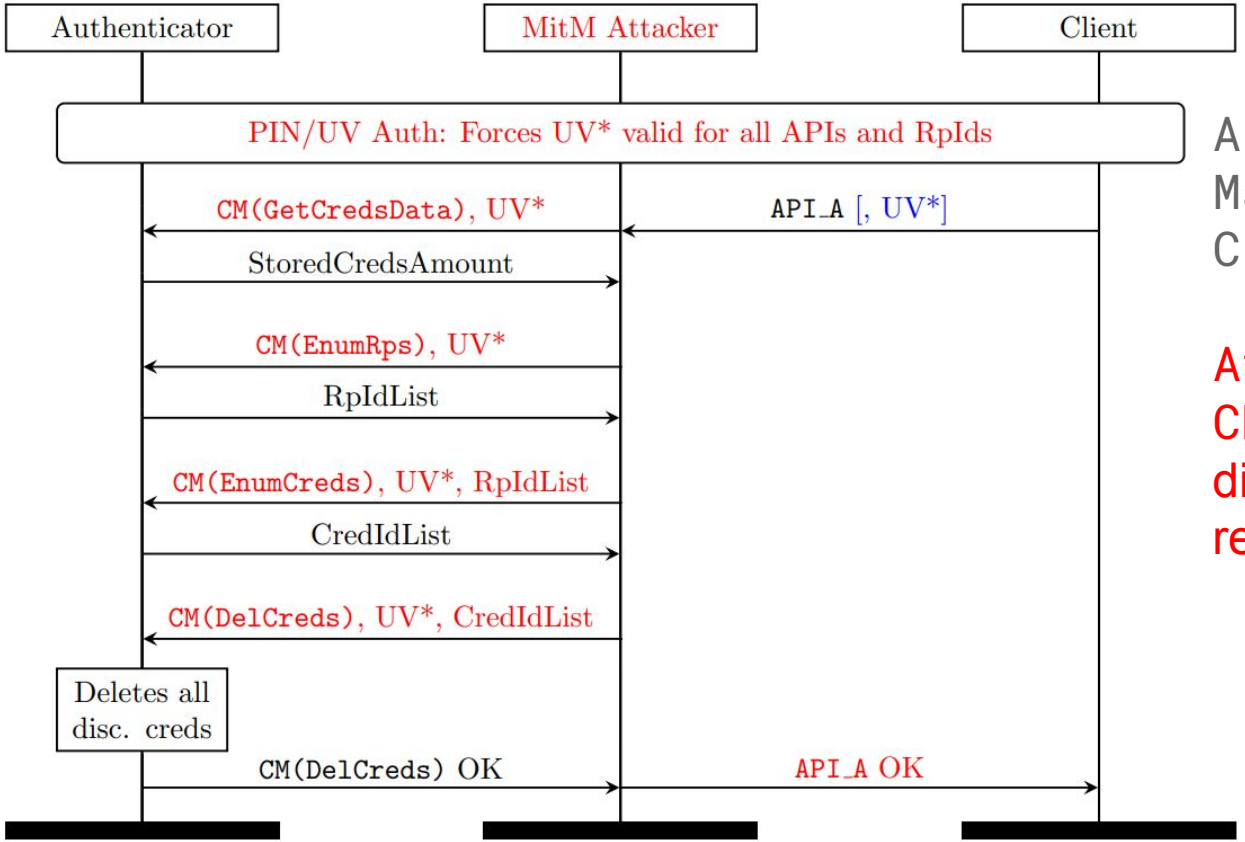
✓[1] : NFC ✓[2] : CredProtect=off (default)

AC_2: Factory Reset Auth



API_A requires UP like Reset, eg: Get Assertion, Selection, ...

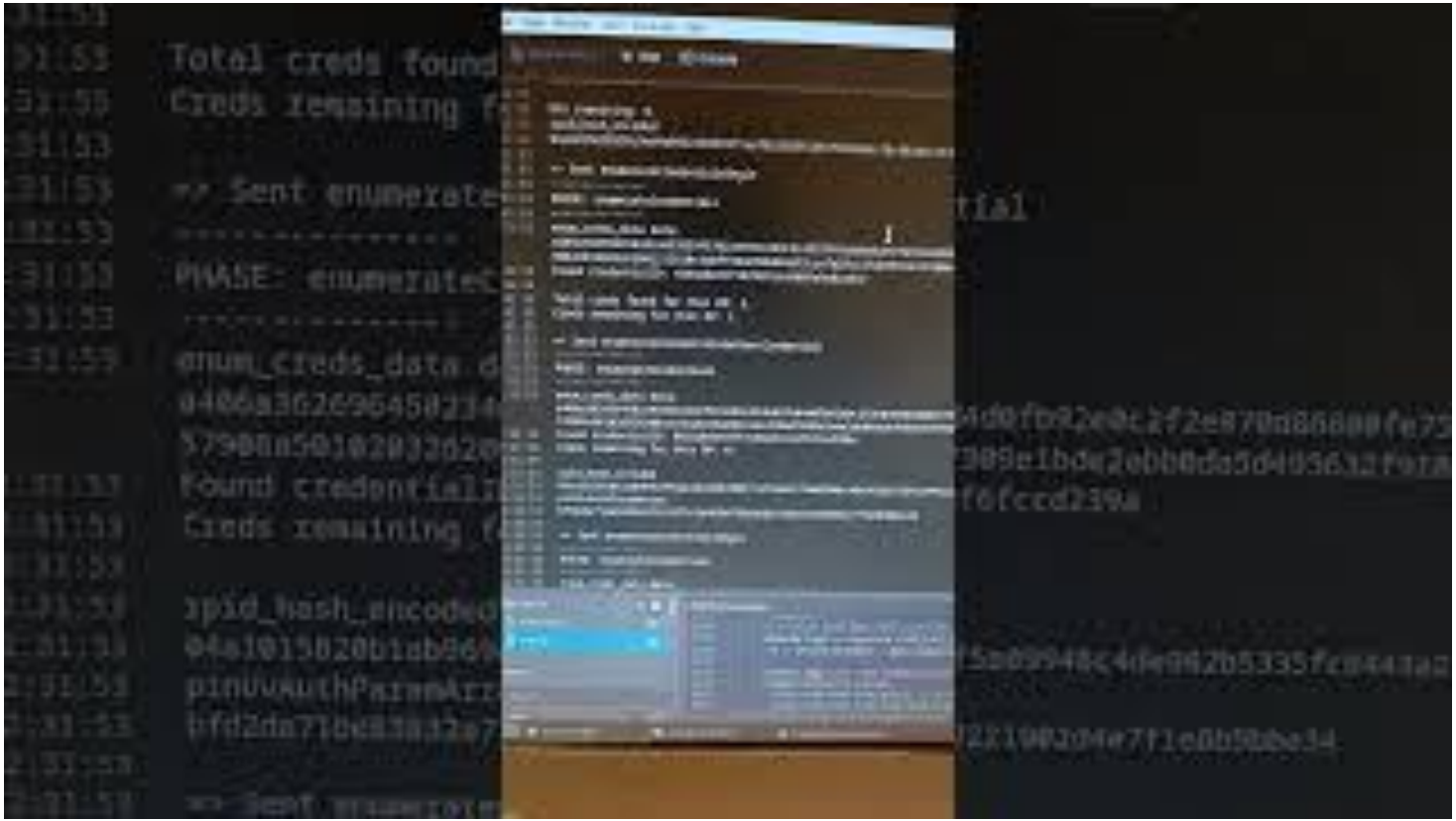
AC_1: Delete Discov Creds



API_A requires UV, eg: MakeCredential, ClientPin, ...

Attacker calls CM=CredMgmt N times with different subcommands reusing UV

DEMO AC_1: Delete Discov Creds over USB



Seven API Confusion (AC) Attacks

- **AC_1**: Delete Discoverable Creds (`CredMgmt`)
- **AC_2**: Factory Reset Authenticator (`Reset`)
- **AC_3**: Track User from Credentials (`GetAssertion`)
- **AC_4**: Fill Authenticator Credentials Storage (`MakeCred`)
- **AC_5**: Force Authenticator Lockout (`ClientPin`)
- **AC_6**: Authenticator DoS (`Selection`)
- **AC_7**: Profile Authenticator (`GetInfo`)

Vulnerabilities and Toolkit

CTRAPS Eight CTAP Design Vulns

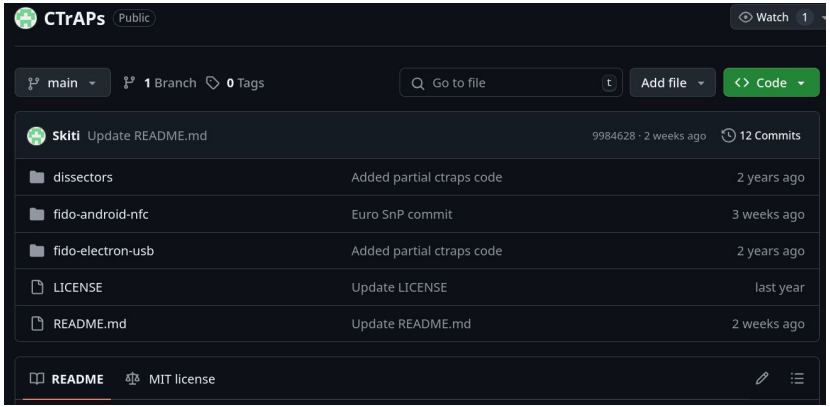
- V_1: Unauthenticated CTAP Client
- V_2: No Authenticator feedback about API call
- V_3: NFC range provides UP
- V_4: Weak destructive APIs authorization
- V_5: User trackable via CredId and UserId
- V_6: `Reset` does not require UV
- V_7: `CredMgmt` does not require UP
- V_8: `Selection` is usable for DoS

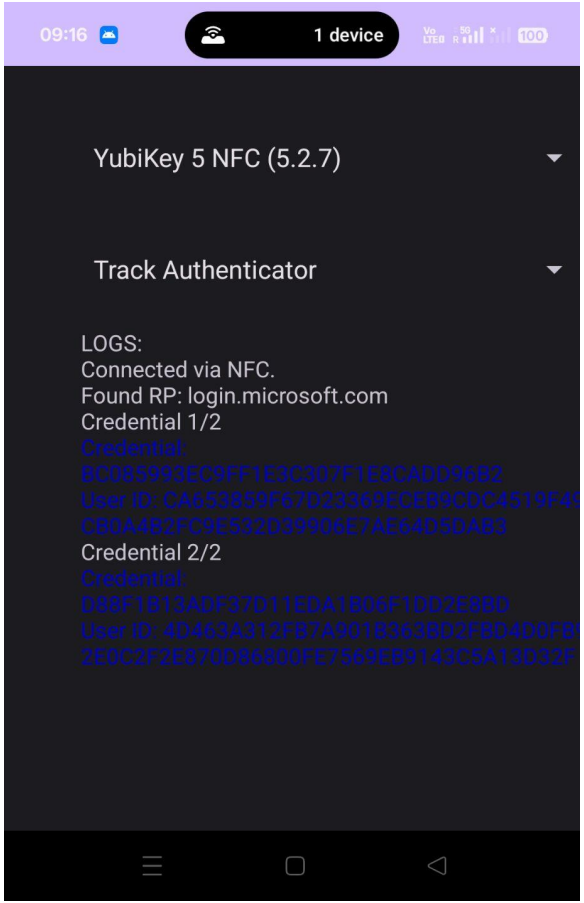
Map CI and AC Attacks to Vulns

		V1	V2	V3	V4	V5	V6	V7	V8
Re	CI_1	✓	✓	✓	✗	✗	✓	✗	✗
GA	CI_2	✓	✓	✓	✗	✓	✗	✗	✗
CP	CI_3	✓	✓	✗	✗	✗	✗	✗	✗
CI	CI_4	✓	✓	✗	✗	✗	✗	✗	✗
CM	AC_1	✓	✓	✗	✓	✗	✗	✓	✗
Re	AC_2	✓	✓	✓	✓	✗	✓	✗	✗
GA	AC_3	✓	✓	✓	✗	✓	✗	✗	✗
MC	AC_4	✓	✓	✓	✗	✗	✗	✗	✗
CP	AC_5	✓	✓	✗	✓	✗	✗	✗	✗
SE	AC_6	✓	✓	✗	✗	✗	✗	✗	✓
GI	AC_7	✓	✓	✗	✗	✗	✗	✗	✗

CTRAPS Toolkit

1. Virtual CTAP testbed
2. Four attack Clients
3. CTAP Wireshark dissector





CTRAPS Toolkit: Virtual CTAP Testbed

- Virtual RP and CTAP Client
  - Tests physical Auths without breaking real systems
- Extending Yubico `fido2-python`
  - Raw CTAP packets
  - Customizable Client config (UV, UP, ECDH, extensions, …)
  - Templates for existing Relying Party (RpId, CredProtect, …)

CTRAPS Toolkit: Four Attack Clients

- Android app for *CI over NFC*
  - Runs on attacker's phone, 2cm max range (Redmi 5 Plus)
- Proxmark3 Lua script for *CI over NFC*
  - Custom CTAP API over ISO14443A, 6.5cm max range
- Android app for CI *over NFC*
  - Runs on victim's phone
  - Custom CTAP API over Android NFC API
- Electron app to simulate *AC over USB*
  - MitM on USB HID traffic using `node-hid` lib

Evaluation

Setup: Test 6 Popular Authenticators

Authenticator	Manuf	Year	FVer	OSF	DCr
YubiKey 5	Yubico	2018	5.2.7	No	25
YubiKey 5 FIPS	Yubico	2021	5.4.3	No	25
Feitian K9	Feitian	2016	3.3.01	No	50
Solo V1	SoloKeys	2018	4.1.5	Yes	50
Solo V2 Hacker	SoloKeys	2021	2.964	Yes	50
OpenSK	Google	2023	2.1	Yes	150

Setup: Test 10 Popular Relying Parties

Rp	RpId	Cred
Adobe	adobe.com	Disc
Apple	apple.com	DiscWeak
DocuSign	account.docusign.com	NonDisc
Facebook	facebook.com	NonDisc
GitHub	github.com	Disc
Hancock	hancock.ink	Disc
Microsoft	login.microsoft.com	DiscWeak
NVidia	login.nvgs.nvidia.com	Disc
Synology	account.synology.com	Disc
Vault Vision	auth.vaultvision.com	Disc

Cred type, DiscWeak = discoverable and unprotected

Result: Exploit 6 Authenticators

Authenticator	CI_1	CI_2	CI_3	CI_4	AC_1	AC_2	AC_3	AC_4	AC_5	AC_6	AC_7
YubiKey 5	✓	✓	✓	✓	✓	✓	✓	✓	✓	n/a	✓
YubiKey 5 FIPS	✓	✓	✓	✓	✓	✓	✓	✓	✓	n/a	✓
Feitian K9	✓	✓	✓	✓	✓	✓	✓	✓	✓	n/a	✓
Solo V1	✓	✓	✓	✓	✓	✓	✓	✓	✓	n/a	✓
Solo V2 Hacker	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OpenSK	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Auths vulnerable to all CI attacks

Auths vulnerable to all AC attacks

n/a: not applicable as Auth does not implement `Selection`

Result: Exploit 10 Relying Parties

Rp	RpId	Cred	Delete Creds	Track User	DoS Authenticator
Adobe	adobe.com	Disc	CI_1, AC_1, AC_2	CI_2, AC_3	CI_3, AC_4, AC_5, AC_6
Apple	apple.com	DiscWeak	CI_1, AC_1, AC_2	CI_2, AC_3	CI_3, AC_4, AC_5, AC_6
DocuSign	account.docusign.com	NonDisc	CI_1, AC_2	n/a	CI_3, AC_5, AC_6
Facebook	facebook.com	NonDisc	CI_1, AC_2	n/a	CI_3, AC_5, AC_6
GitHub	github.com	Disc	CI_1, AC_1, AC_2	CI_2, AC_3	CI_3, AC_4, AC_5, AC_6
Hancock	hancock.ink	Disc	CI_1, AC_1, AC_2	CI_2, AC_3	CI_3, AC_4, AC_5, AC_6
Microsoft	login.microsoft.com	DiscWeak	CI_1, AC_1, AC_2	CI_2, AC_3	CI_3, AC_4, AC_5, AC_6
NVidia	login.nvgs.nvidia.com	Disc	CI_1, AC_1, AC_2	CI_2, AC_3	CI_3, AC_4, AC_5, AC_6
Synology	account.synology.com	Disc	CI_1, AC_1, AC_2	CI_2, AC_3	CI_3, AC_4, AC_5, AC_6
Vault Vision	auth.vaultvision.com	Disc	CI_1, AC_1, AC_2	CI_2, AC_3	CI_3, AC_4, AC_5, AC_6

Cannot login and lost creds, Account trackable, Cannot login

n/a: not applicable because RP does not support Disc Creds

Countermeasures and Disclosure

CTRAPS Countermeasures ($\mathbf{C_N}$ fixes $\mathbf{V_N}$)

- $\mathbf{C_1}$: Trusted CTAP Client
- $\mathbf{C_2}$: Authenticator visual feedback
- $\mathbf{C_3}$: User interaction for UP over NFC
- $\mathbf{C_4}$: Dedicated PIN for destructive APIs (`CM`, `Re`, …)
- $\mathbf{C_5}$: Dynamic and UV-protected CredId and UserId
- $\mathbf{C_6}$: `Reset` must require UV (on Client)
- $\mathbf{C_7}$: `CredMgmt` must require UP
- $\mathbf{C_8}$: Rate limiting `Selection` calls

CTRAPS Disclosure

- FIDO Alliance
  - Nov 2023: first contact
  - May 2024: feedback, request to disclose to vendors
- Authenticator Vendors
  - Dec 2023: Yubico, Solo, Feitian, Google (P2/S2)
  - Yubico CVE-2024-35311 [YSA-2024-02]
- Relying Parties
  - Dec 2023: Microsoft, Apple

Grazie! Q&A

https://francozappa.github.io/publication/2025/ctraps/

CTRAPS: CTAP Client Impersonation and API Confusion on FIDO2

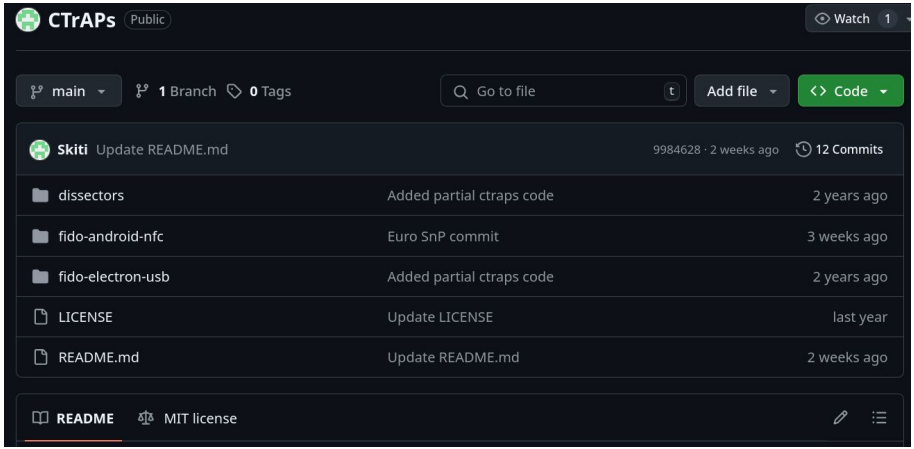
Marco Casagrande
Department of Digital Security
EURECOM
Sophia Antipolis, France
marco.casagrande@eurecom.fr

Daniele Antonioli
Department of Digital Security
EURECOM
Sophia Antipolis, France
daniele.antonioli@eurecom.fr

***Abstract*—FIDO2 is a popular technology for single-factor and second-factor authentication. It is specified in an open standard including the WebAuthn and CTAP application layer protocols. We focus on CTAP which allows the communication between FIDO2 clients and authenticators. No prior work explored the CTAP Authenticator API which is a critical protocol-level attack surface as it deals with credential creation, deletion, and management. We address this gap by presenting the first security and privacy evaluation of the CTAP Authenticator API. We uncover two classes of CTAP protocol-level attacks we call CTRAPS.**

FIDO market to rapidly grow from USD 230.6 million in 2022 to USD 598.6 million in 2031 [60]. Yubico, a FIDO authenticator market leader, sold more than 22 million YubiKey authenticators [67]. This growth will continue because of the recent industry-wide push towards single-factor passkey-based authentication [20], [29], [56].

FIDO2 involves three entities: an *authenticator* that generates and asserts possession of authentication credentials (e.g., public-private key pairs), a *relying party* that authenticates the user (e.g., challenge-response protocol based on credentials), and a *client* who wants to authenti-



KTH VETENSKAP OCH KONST

DEFCON

ORSHIN

EURECOM
Sophia Antipolis

Backup

FIDO2 Alliance Board Members [ref]

CTRAPS CVE-2024-35311 [YSA-2024-02]

- Yubico implementation-specific issue
  - Leaks Relying Parties stored in Auth
  - No UV required
- Affected YubiKeys
  - All YubiKey 5, Security Key, Bio, FIPS, and CSPN Series
  - Fixed in newer keys
  - Not patched in old keys (no firmware update)

DEMO Yubico Auth CVE-2024-35311