CTRAPS: CTAP Client Impersonation and API Confusion on FIDO2

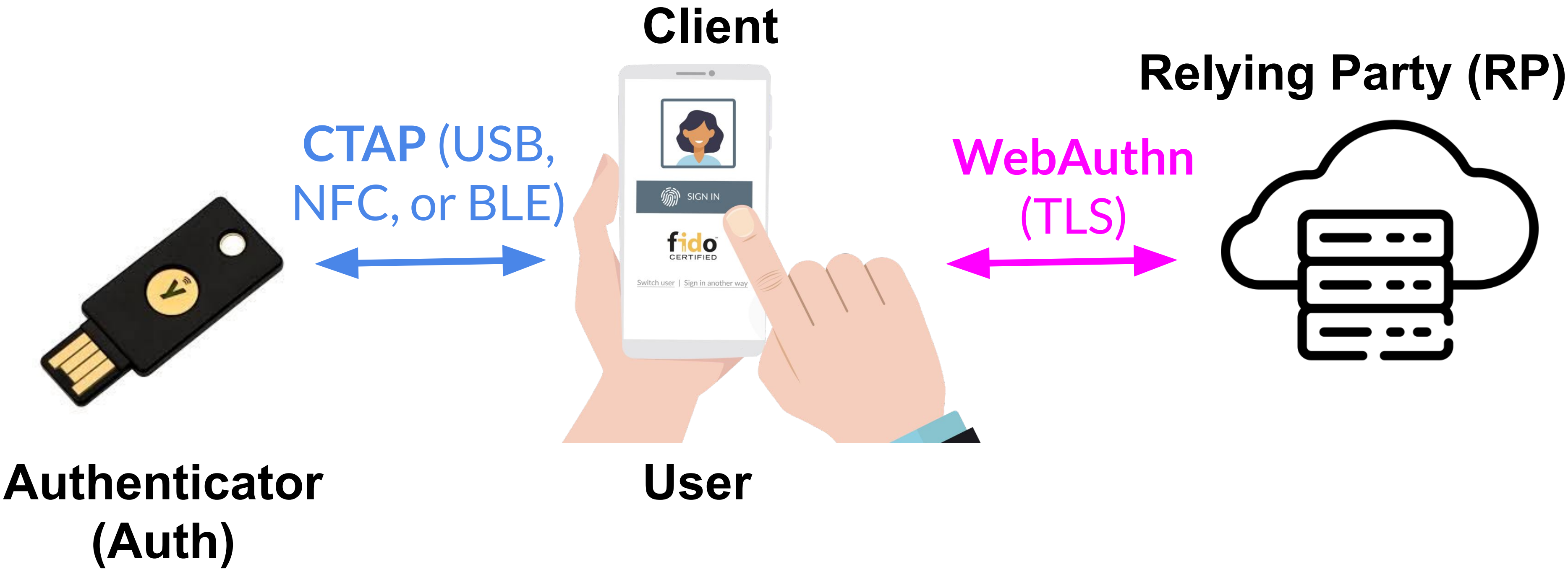
IEEE EuroS&P’25

M. Casagrande (KTH) D. Antonioli (EURECOM).

KTH
VETENSKAP
OCH KONST

EURECOM
Sophia Antipolis

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



Client

Relying Party (RP)

CTAP (USB, NFC, or BLE)

WebAuthn (TLS)

Authenticator (Auth)

User

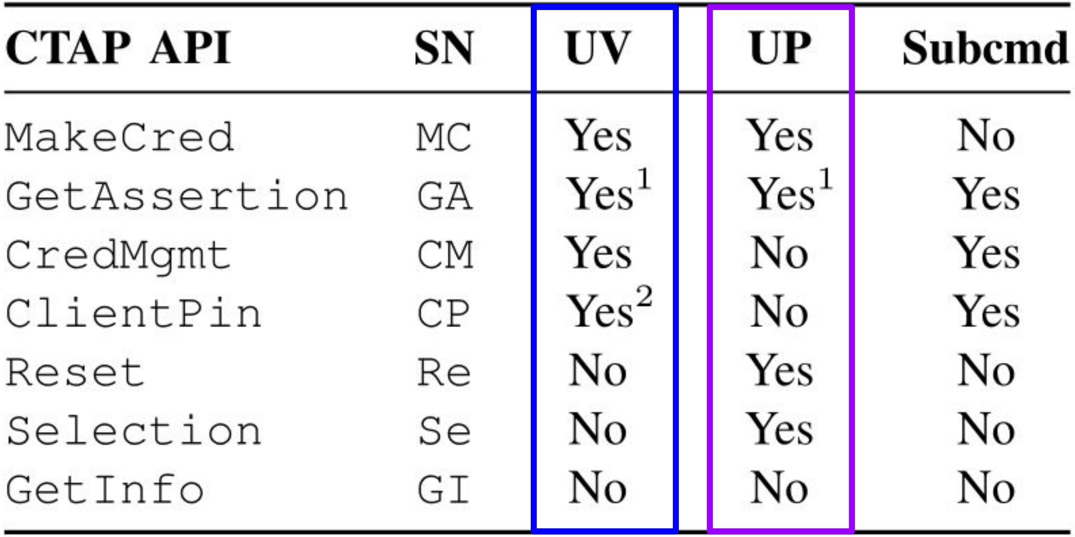
CTRAPS Motivation

- FIDO2 trusted by billions of accounts daily
    - CTAP attacks have critical S&P impact (delete creds, track, …)
    - Regardless of transport (USB, NFC, BLE) and target (Cli, Auth)
- Limited prior work on CTAP
    - Formal verif and theoretical eve, spoof, MitM attacks on CTAPv2.0 *[Barbosa21,Guan22]*
    - Practical MitM on CTAPv2.1 DH *[Barbosa23]*

CTRAPS Contributions

- First S&P evaluation of the **CTAP Authenticator API**
  - Uncover **7 design issues** (unauth Client, …)
  - Affecting CTAP v2.0, v2.1, and v2.2
- Two new attack classes resulting in **11 CTRAPS attacks**
  - **Client Impersonation** attacks (CI_1, …,CI_4)
  - Client-Auth **API Confusion** attacks (AC_1, …, AC_7)
  - Eg: Reset Authenticator via NFC with 0-click
- Open source CTRAPS toolkit (virt testbed, 4 Clients, …)
- Evaluation **exploiting 16 FIDO2 devices (Auth, Cli, RP)**
- Discuss **8 backward-compliant fixes**

CTRAPS Authenticator API Attack Surface



CTAP API	SN	UV	UP	Subcmd
`MakeCred`	`MC`	Yes	Yes	No
`GetAssertion`	`GA`	Yes[1]	Yes[1]	Yes
`CredMgmt`	`CM`	Yes	No	Yes
`ClientPin`	`CP`	Yes[2]	No	Yes
`Reset`	`Re`	No	Yes	No
`Selection`	`Se`	No	Yes	No
`GetInfo`	`GI`	No	No	No

UV: User enters on Client PIN or password

UP: User presses a button on Auth or Auth and Client in NFC range

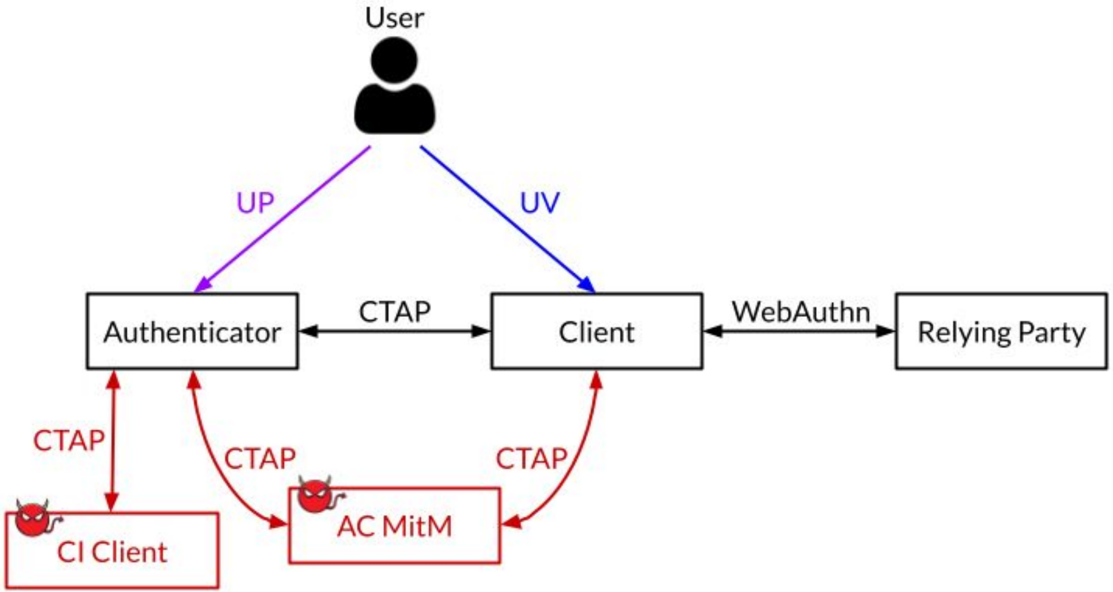
Yes[1] : depends on Client and RP configuration

Yes[2] : depends on the API subcommand.

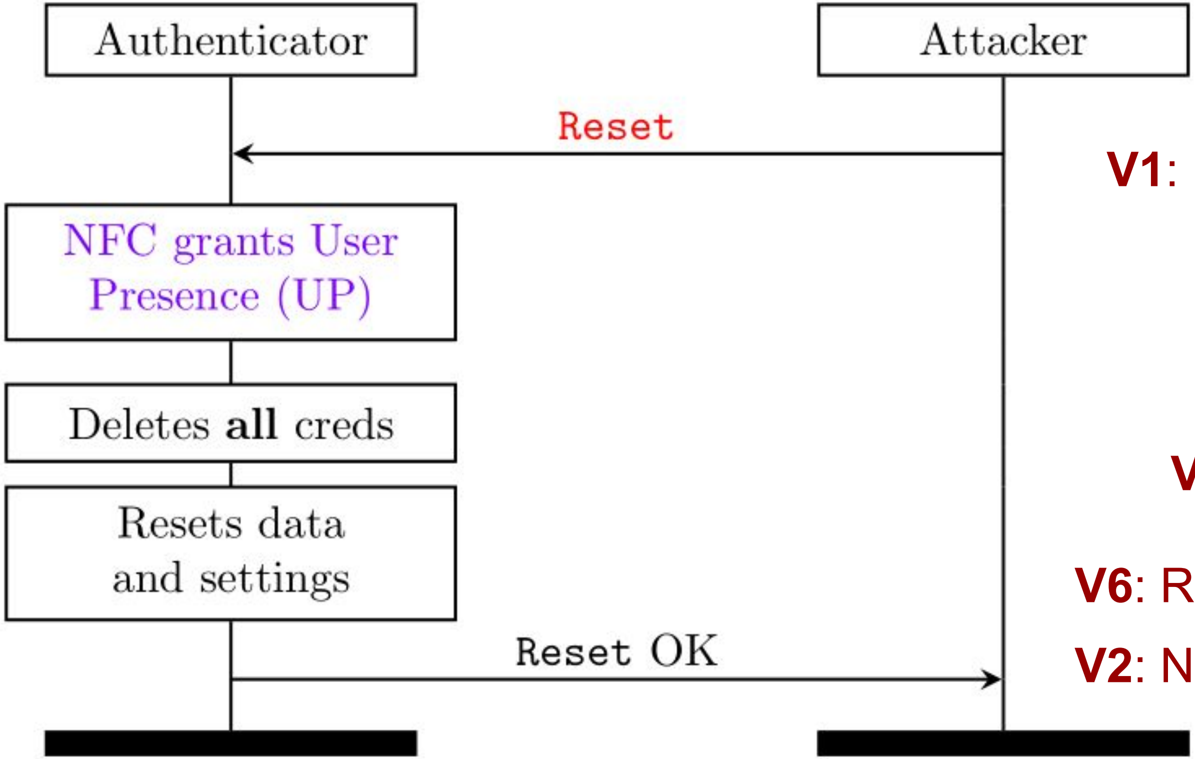
CTRAPS Threat Model

Attacker focuses on **design issues on CTAP Auth API**.

CI and AC attackers are **in proximity** (eg: NFC range with Auth) or **remote** (eg: malicious app spoofing Client on User's phone)



CI_1 Attack: Factory Reset Auth over NFC (Reset)



V1: no Client authentication

V3: NFC range is UP

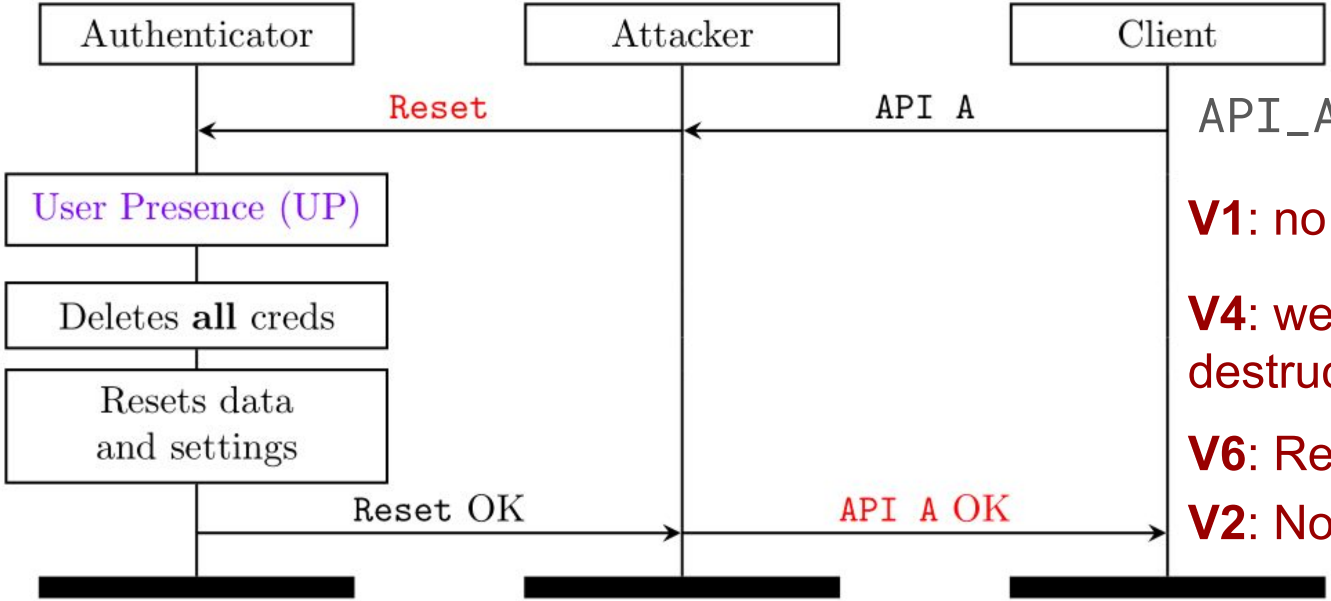
V6: Reset has no UV

V2: No visual feed on Auth

Four CI Attacks

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

AC_2 Attack: Factory Reset Auth (`Reset`)



API_A can be MC, GA, …

V1: no Client authentication

V4: weak access ctrl for destructive API such as Reset

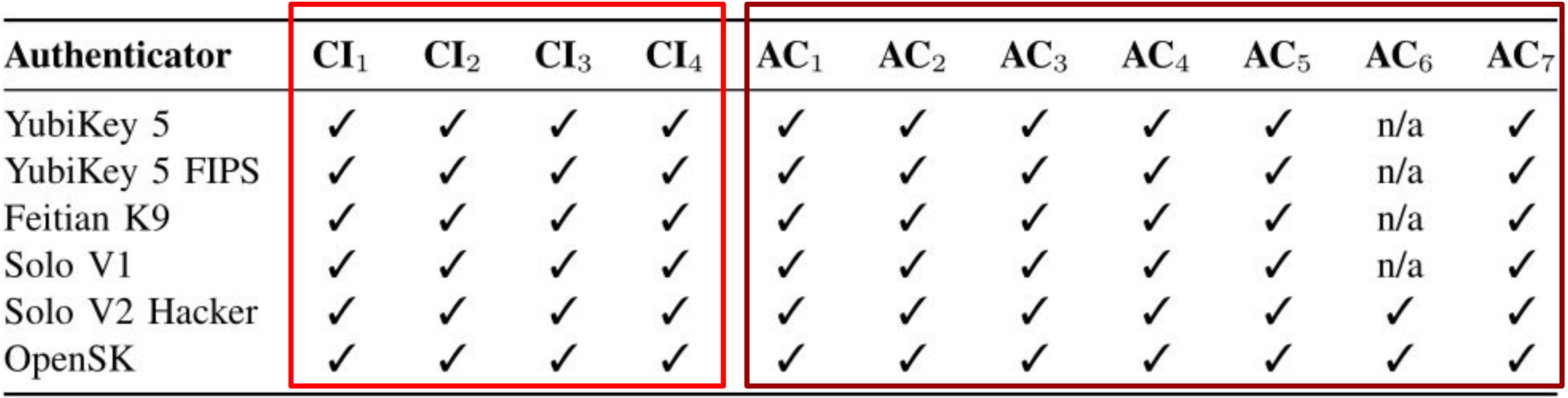
V6: Reset has no UV

V2: No visual feed on Auth

CTRAPS Seven 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`)

CTRAPS Exploit 6 Authenticators



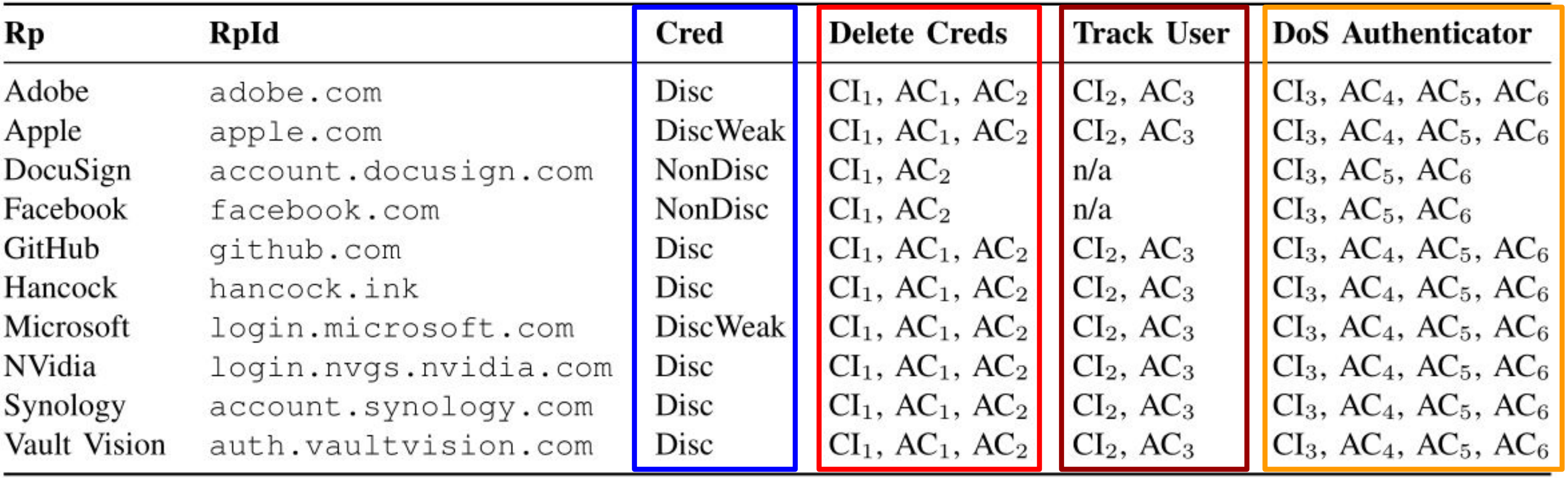
Authenticator	CI_1	CI_2	CI_3	CI_4	AC_1	AC_2	AC_3	AC_4	AC_5	AC_6	AC_7
YubiKey 5	✓	✓	✓	✓	✓	✓	✓	✓	✓	n/a	✓
YubiKey 5 FIPS	✓	✓	✓	✓	✓	✓	✓	✓	✓	n/a	✓
Feitian K9	✓	✓	✓	✓	✓	✓	✓	✓	✓	n/a	✓
Solo V1	✓	✓	✓	✓	✓	✓	✓	✓	✓	n/a	✓
Solo V2 Hacker	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OpenSK	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Auths vulnerable to all CI attacks

Auths vulnerable to all AC attacks

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

CTRAPS Exploit 10 Relying Parties (RPs)



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

DiscWeak: discoverable and unprotected

Cannot login and lost creds, Account trackable, Cannot login

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