Cross Device Flows

Pieter Kasselman Daniel Fett Filip Skokan

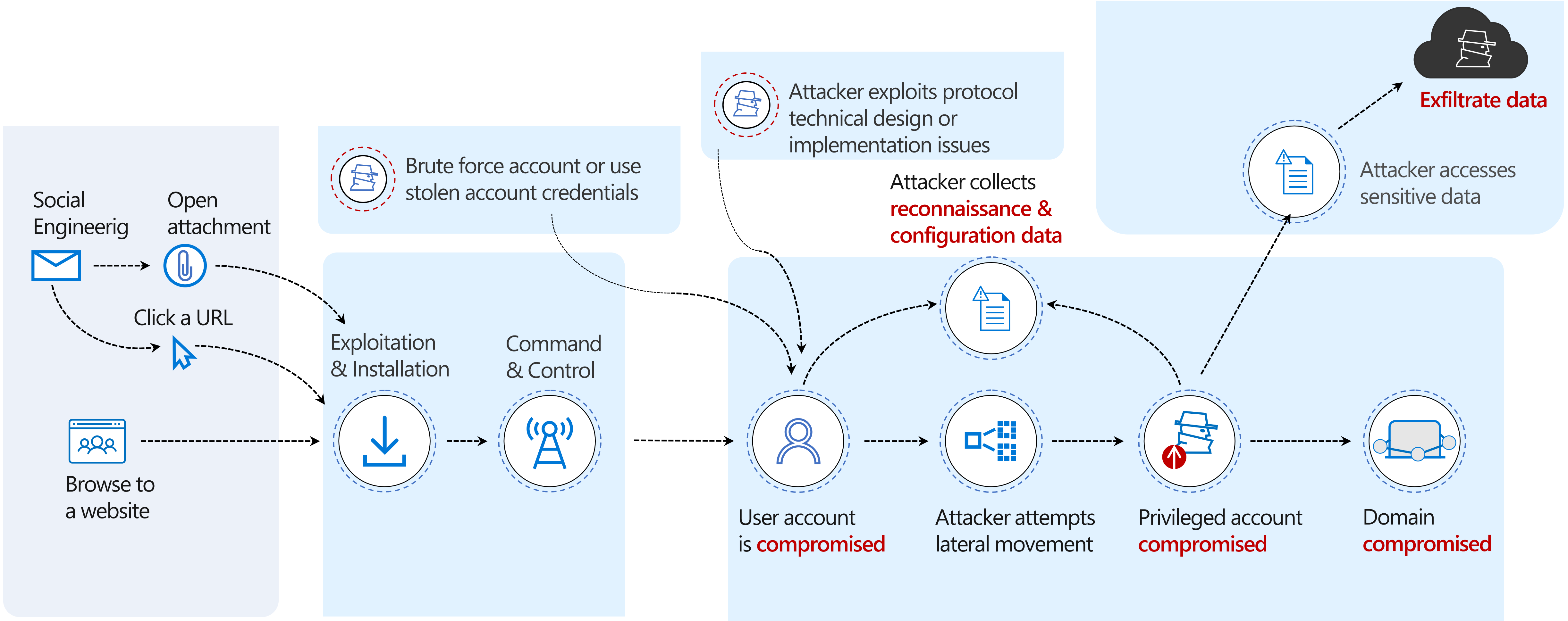
IETF 116 Yokohama (March 2023)
Date: 31 March 2023

Agenda

- Why are we here?
- Where are we?
- Where do we go next?

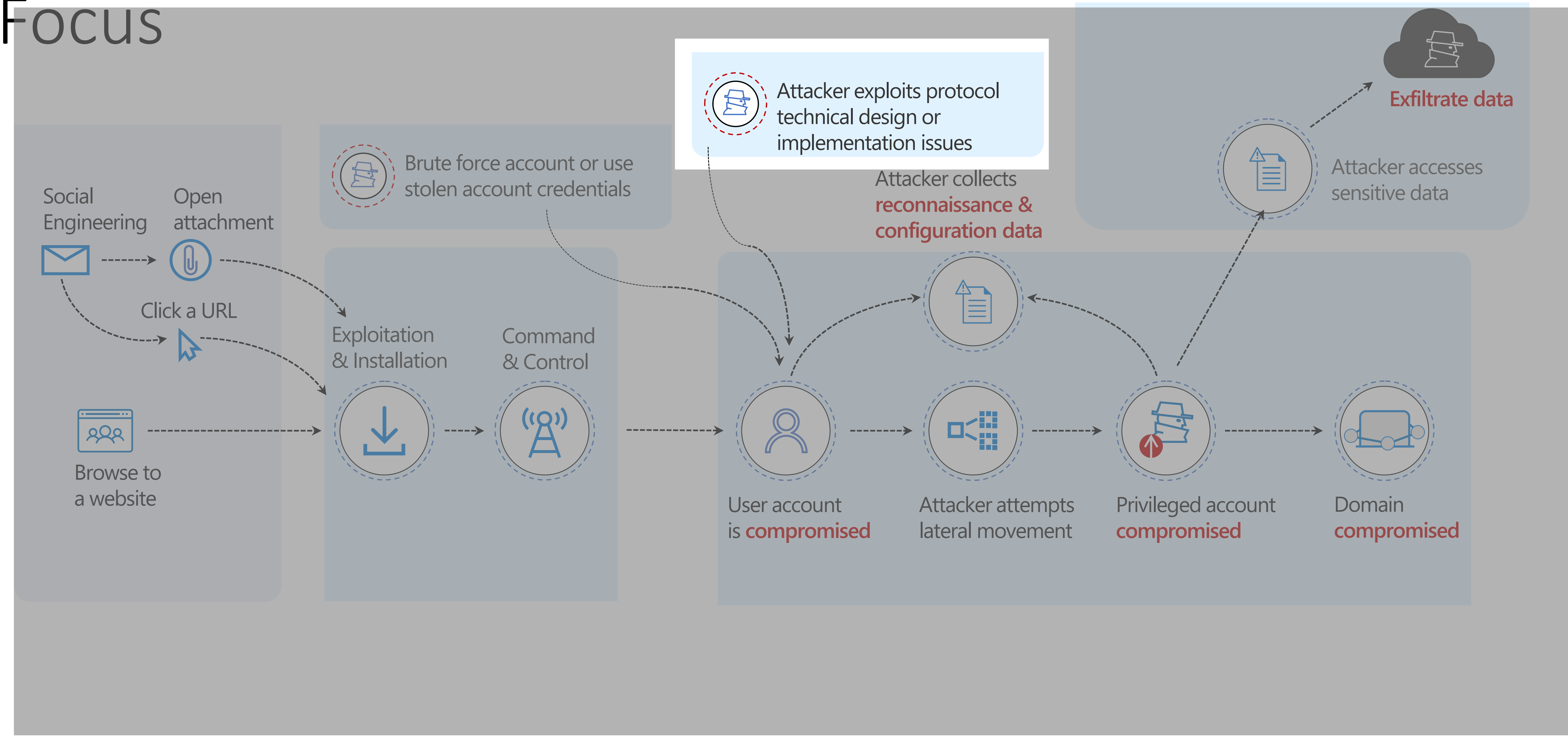
Why are we here?

Anatomy of an attack

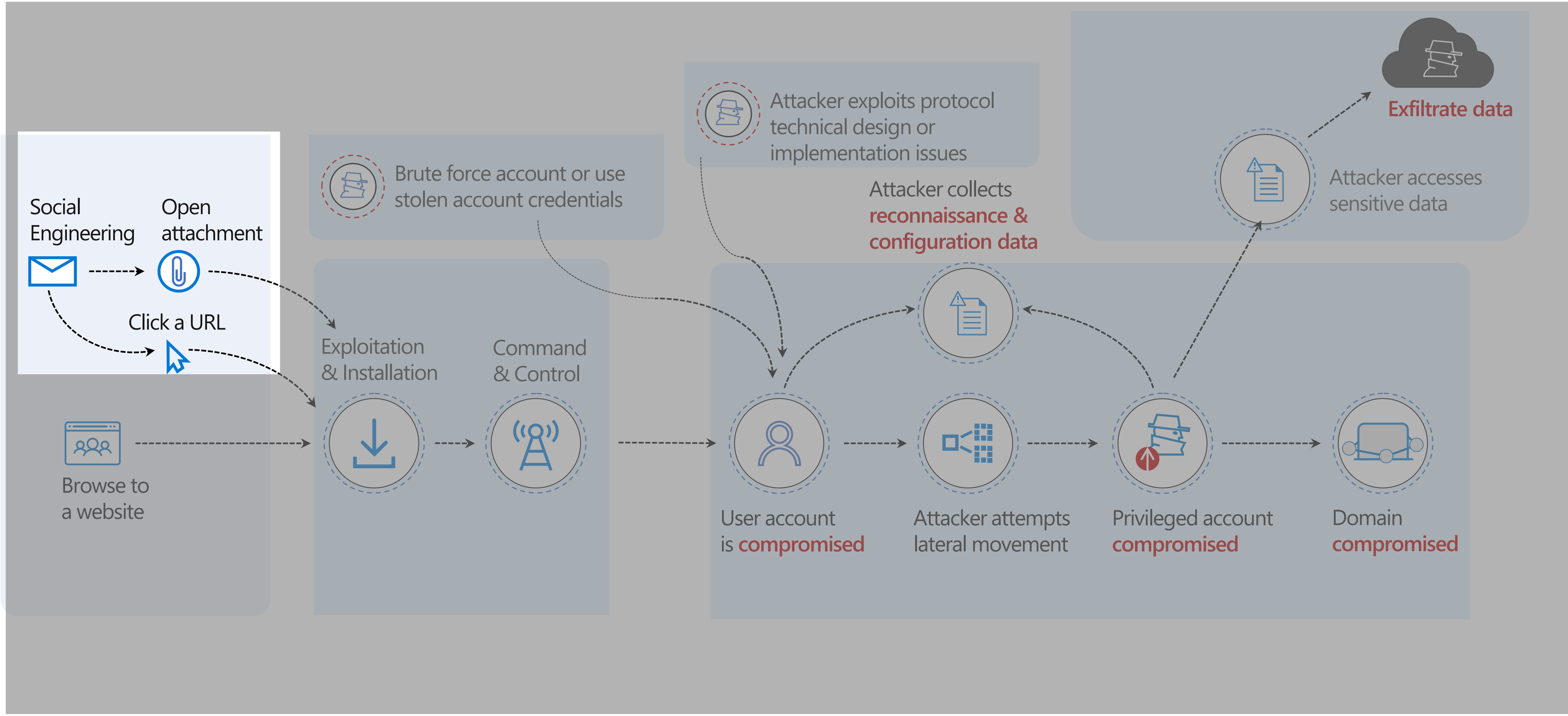


Social Engineerig
Open attachment
Click a URL
Browse to a website
Exploitation & Installation
Command & Control
Brute force account or use stolen account credentials
Attacker exploits protocol technical design or implementation issues
Attacker collects reconnaissance & configuration data
User account is compromised
Attacker attempts lateral movement
Privileged account compromised
Domain compromised
Attacker accesses sensitive data
Exfiltrate data

Where Protocol Analysts and Standards Experts Focus

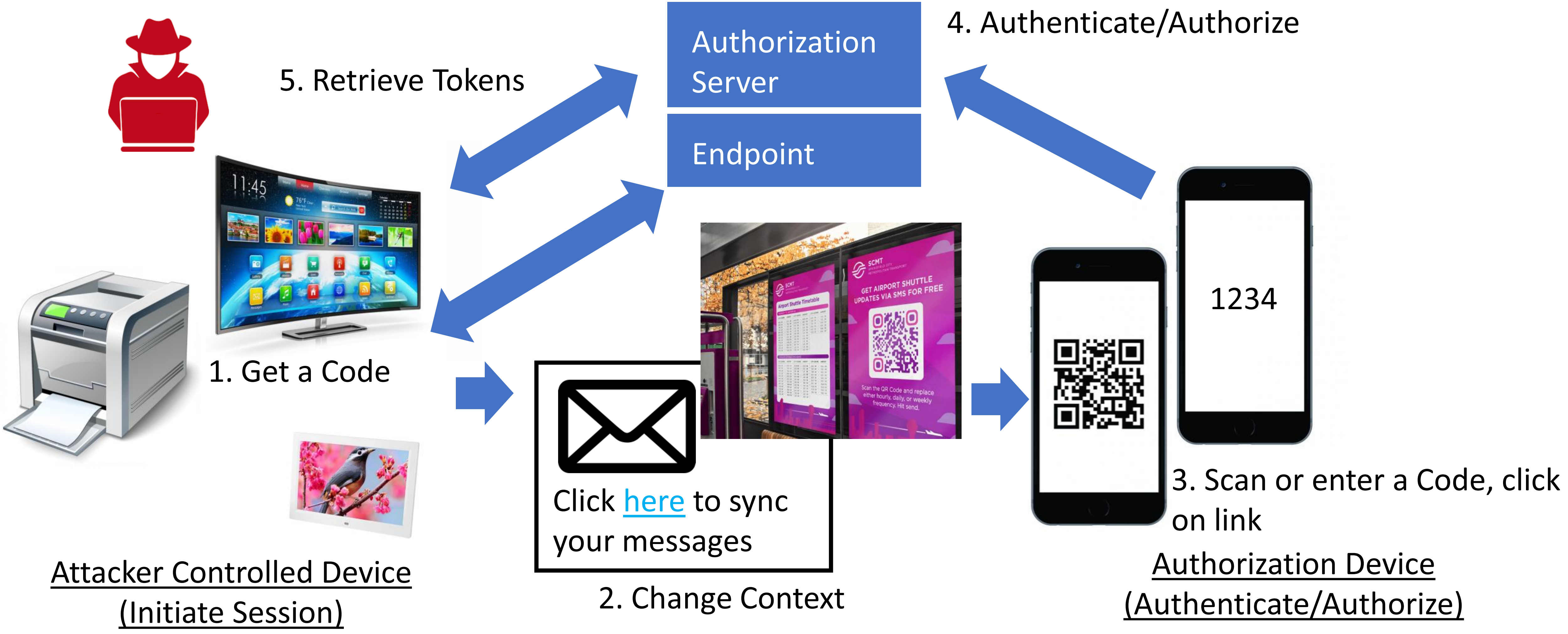

Attacker exploits protocol technical design or implementation issues
Brute force account or use stolen account credentials
Social Engineering
Open attachment
Click a URL
Browse to a website
Exploitation & Installation
Command & Control
Attacker collects reconnaissance & configuration data
Exfiltrate data
Attacker accesses sensitive data
User account is compromised
Attacker attempts lateral movement
Privileged account compromised
Domain compromised

Mind the Gap – Where Attackers (often) Enter



Social Engineering
Open attachment
Click a URL
Browse to a website
Brute force account or use stolen account credentials
Exploitation & Installation
Command & Control
Attacker exploits protocol technical design or implementation issues
Attacker collects reconnaissance & configuration data
User account is compromised
Attacker attempts lateral movement
Privileged account compromised
Domain compromised
Attacker accesses sensitive data
Exfiltrate data

Cross-Device Flow Social Engineering Exploit


11:45
1234
SCMT
GET AIRPORT SHUTTLE UPDATES VIA SMS FOR FREE
Airport Shuttle Timetable

Authorization Server

Endpoint

5. Retrieve Tokens

4. Authenticate/Authorize

1. Get a Code

Click here to sync your messages

2. Change Context

3. Scan or enter a Code, click on link

Attacker Controlled Device (Initiate Session)

Authorization Device (Authenticate/Authorize)

Attack Pattern Summary: Exploit the Unauthenticated Channel

1. Initiate the session, retrieve code (QR code, user code)
2. Use social engineering to change context and persuade user to authorize session (illicit consent grant)
3. Bypasses multi-factor authentication (don’t need to harvest credentials)

Designed for Homo Securitus, used by Homo Sapiens

<u>Homo Securitus</u>

1. A security expert
2. Knows how the protocol should work
3. Detects a social engineering attempt
4. Is laser focused on current context
5. Foolproof mitigation for cross device flows

<u>But is a rare species….</u>

<u>Homo Sapiens</u>

1. "Expertise elsewhere" - not a security expert
2. Busy and in a rush, needs to get things done
3. Worries about breaking things
4. Wants to help

Needs to make fewer decision,
Needs help to make better decisions
Needs protection even if a bad decision is made

Mitigation Framework

Pragmatic Mitigations

- Other.....
- User Experience
- Secure QR
- Trusted Devices
- Sender Constrained Toke
- User Code Meta Data
- Content Filtering
- Proximity

Explore Alternatives

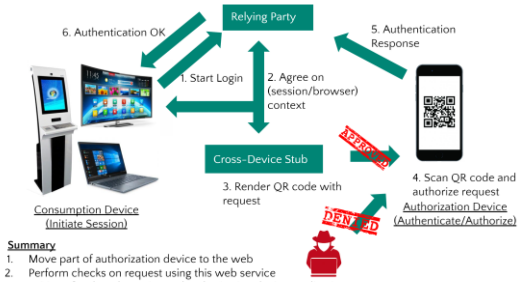
Authenticated Channel

- Authorization Code Grant (WebAuthn fido)

Unauthenticated Channel

- Client Initiated Back Channel Authentication (OpenID)
- Device Authorization Grant

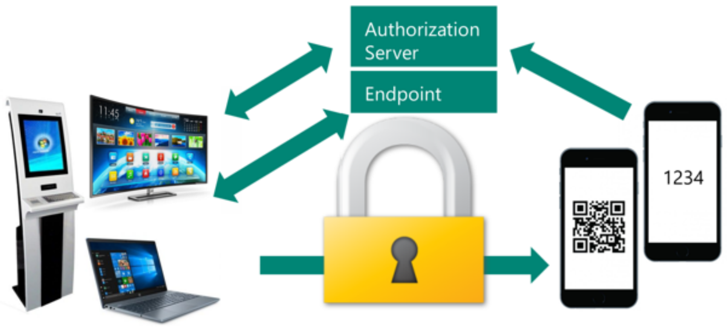
Foundational Underpinnings



Relying Party
6. Authentication OK
5. Authentication Response
1. Start Login
2. Agree on (session/browser) context
Cross-Device Stub
APPROVED
3. Render QR code with request
4. Scan QR code and authorize request
Authorization Device (Authenticate/Authorize)
DENIED
Consumption Device (Initiate Session)

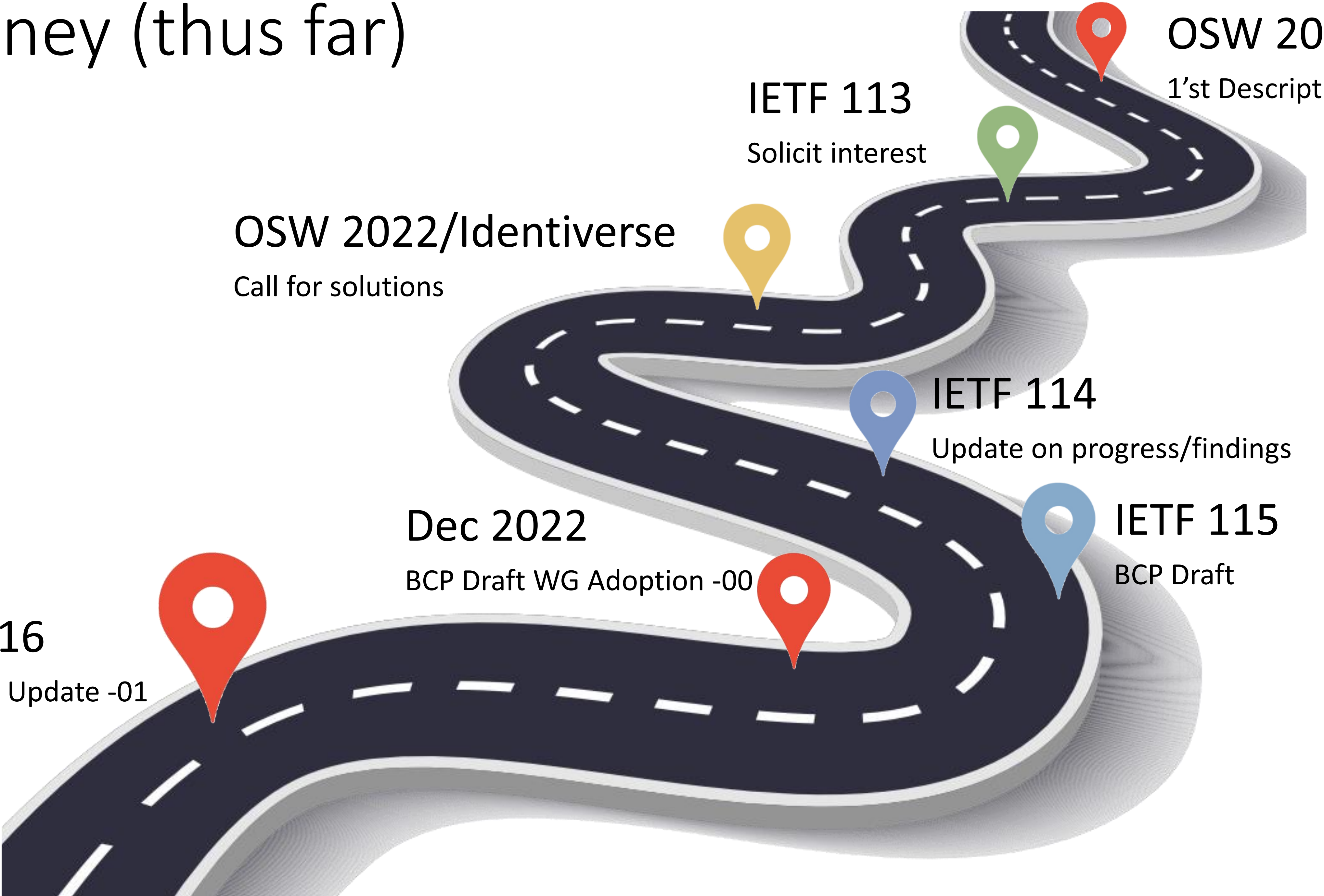
Summary

1. Move part of authorization device to the web
2. Perform checks on request using this web service
3. Pairing of stub web service and authorization device application



Where are we?

The Journey (thus far)



Attacks

OSW 2021

1’st Description

IETF 113

Solicit interest

OSW 2022/Identiverse

Call for solutions

IETF 114

Update on progress/findings

IETF 115

BCP Draft

Dec 2022

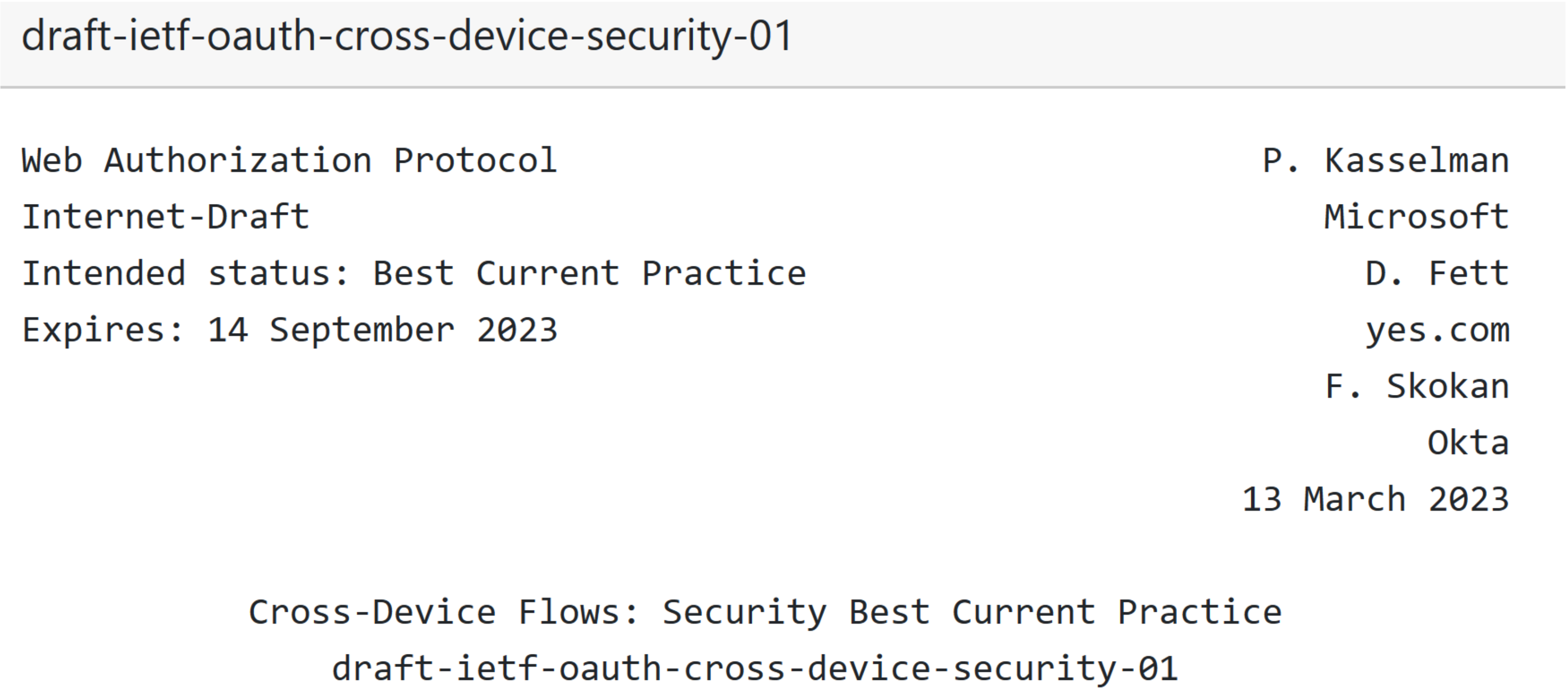
BCP Draft WG Adoption -00

IETF 116

BCP Draft Update -01

Cross-Device Flows: Security Best Current Practice

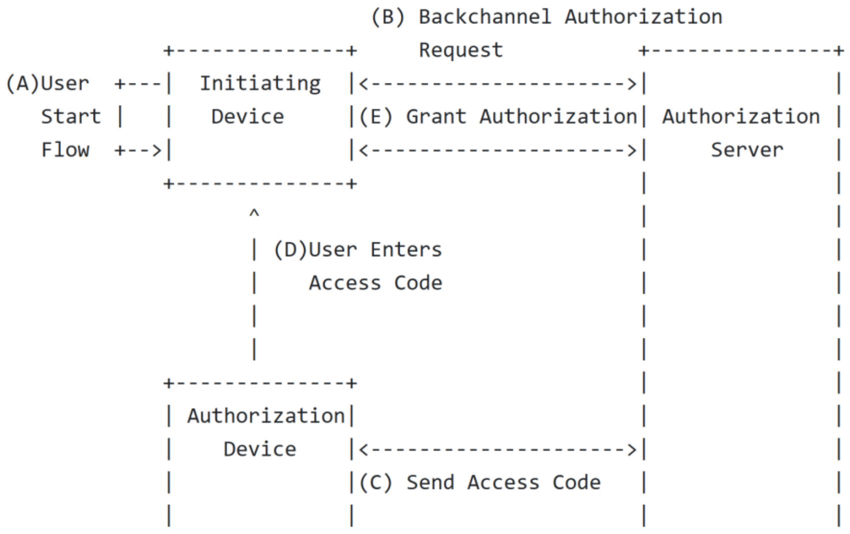
draft-ietf-oauth-cross-device-security-01 - Cross-Device Flows: Security Best Current Practice



draft-ietf-oauth-cross-device-security-01

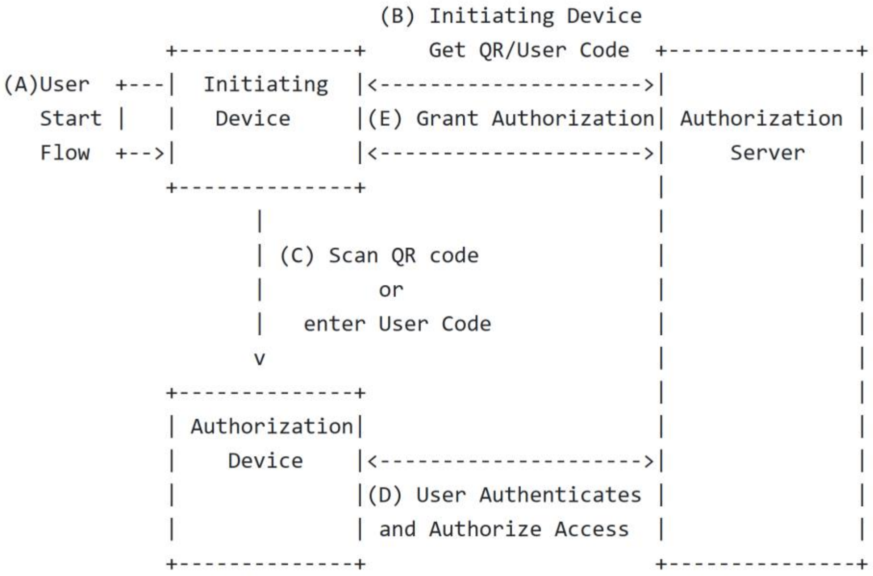
```
Web Authorization Protocol                                  P. Kasselman
Internet-Draft                                                 Microsoft
Intended status: Best Current Practice                           D. Fett
Expires: 14 September 2023                                       yes.com
                                                               F. Skokan
                                                                    Okta
                                                           13 March 2023


             Cross-Device Flows: Security Best Current Practice
                 draft-ietf-oauth-cross-device-security-01
```

What’s New: Distinguish protocol patterns



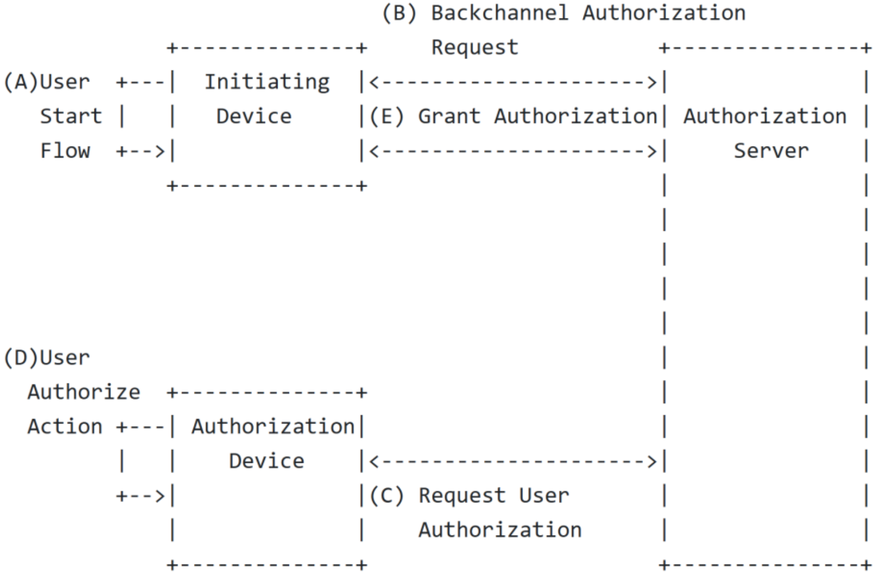
```
                              (B) Backchannel Authorization
             +--------------+     Request           +----------------+
(A)User  +---|  Initiating  |<--------------------->|                |
   Start |   |    Device    |(E) Grant Authorization| Authorization  |
   Flow  +-->|              |<--------------------->|     Server     |
             +--------------+                       |                |
                    ^                               |                |
                    | (D)User Enters                |                |
                    |    Access Code                |                |
                    |                               |                |
                    |                               |                |
             +--------------+                       |                |
             | Authorization|                       |                |
             |    Device    |<--------------------->|                |
             |              |(C) Send Access Code   |                |
             |              |                       |                |
             +--------------+                       +----------------+
```

Figure 3: Cross Device Flows (Hybrid)



```
                              (B) Initiating Device
             +--------------+     Get QR/User Code  +----------------+
(A)User  +---|  Initiating  |<--------------------->|                |
   Start |   |    Device    |(E) Grant Authorization| Authorization  |
   Flow  +-->|              |<--------------------->|     Server     |
             +--------------+                       |                |
                    |                               |                |
                    | (C) Scan QR code              |                |
                    |         or                    |                |
                    |   enter User Code             |                |
                    v                               |                |
             +--------------+                       |                |
             | Authorization|                       |                |
             |    Device    |<--------------------->|                |
             |              |(D) User Authenticates |                |
             |              | and Authorize Access  |                |
             +--------------+                       +----------------+
```

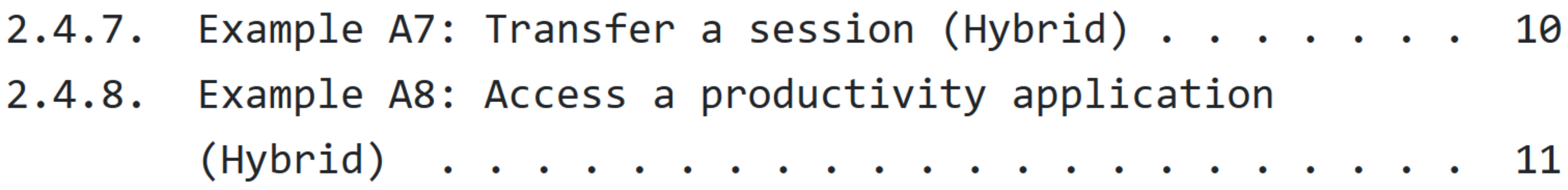
Figure 1: Cross Device Flows (User Transferred)



```
                              (B) Backchannel Authorization
             +--------------+     Request           +----------------+
(A)User  +---|  Initiating  |<--------------------->|                |
   Start |   |    Device    |(E) Grant Authorization| Authorization  |
   Flow  +-->|              |<--------------------->|     Server     |
             +--------------+                       |                |
                                                    |                |
                                                    |                |
                                                    |                |
                                                    |                |
(D)User                                             |                |
  Authorize  +--------------+                       |                |
  Action +---| Authorization|                       |                |
         |   |    Device    |<--------------------->|                |
         +-->|              |(C) Request User       |                |
             |              |    Authorization      |                |
             +--------------+                       +----------------+
```

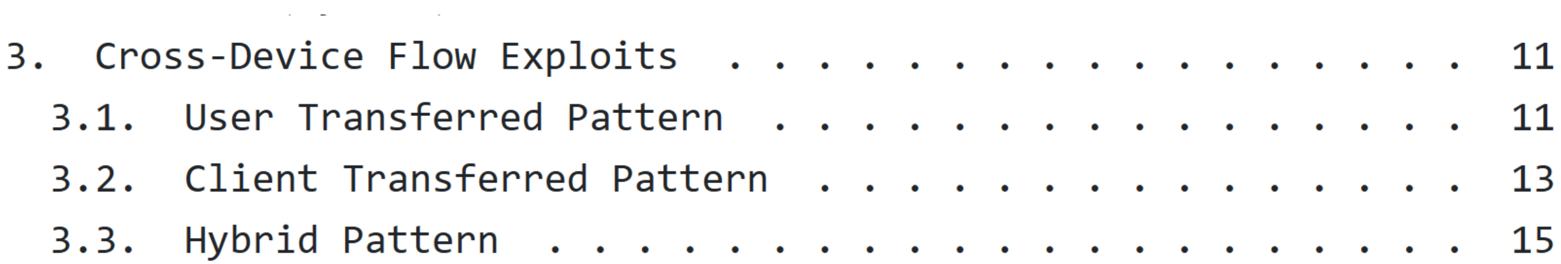
Figure 2: Cross Device Flows (Client Transferred)

What's New: Additional Scenarios



Classified according to protocol pattern

What’s New: Exploits for each pattern



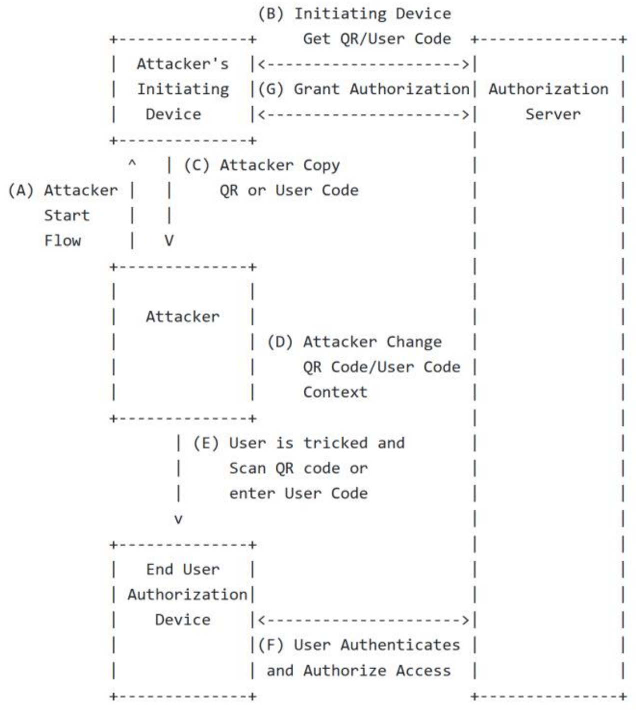

(B) Initiating Device
Get QR/User Code
Attacker's Initiating Device
(G) Grant Authorization
Authorization Server
(A) Attacker Start Flow
(C) Attacker Copy QR or User Code
Attacker
(D) Attacker Change QR Code/User Code Context
(E) User is tricked and Scan QR code or enter User Code
End User Authorization Device
(F) User Authenticates and Authorize Access

Figure 4: Attacker Initiated Cross Device Flow Exploit (User Transferred Pattern)

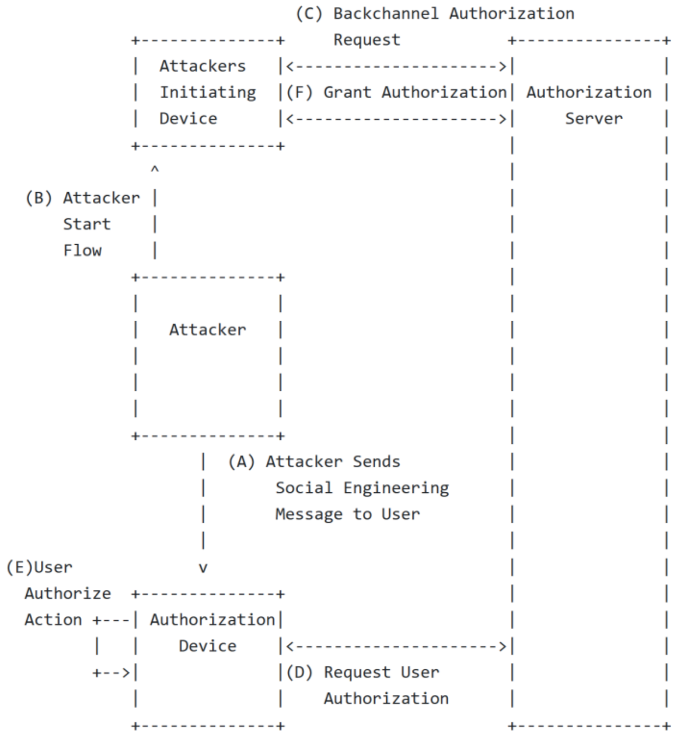

(C) Backchannel Authorization Request
Attackers Initiating Device
(F) Grant Authorization
Authorization Server
(B) Attacker Start Flow
Attacker
(A) Attacker Sends Social Engineering Message to User
(E)User Authorize Action
Authorization Device
(D) Request User Authorization

Figure 5: Attacker Initiated Cross Device Flow Exploit (Client Transferred Pattern)

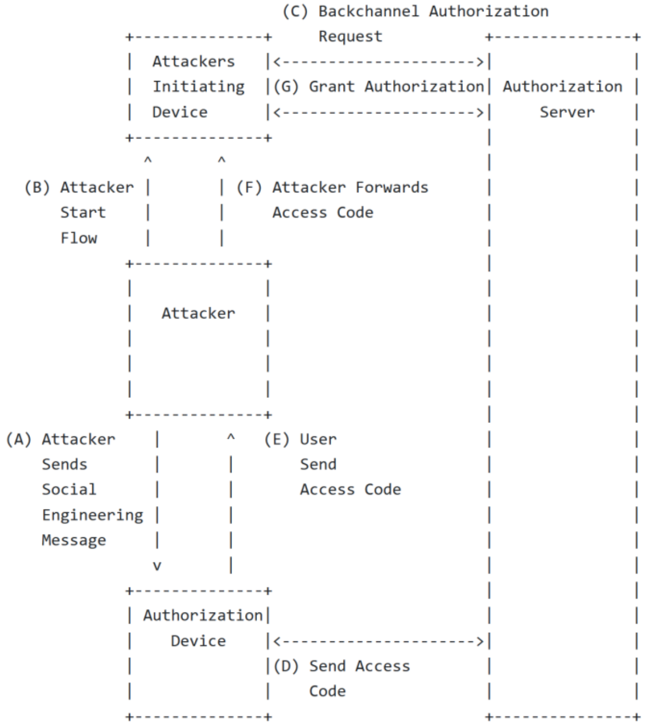
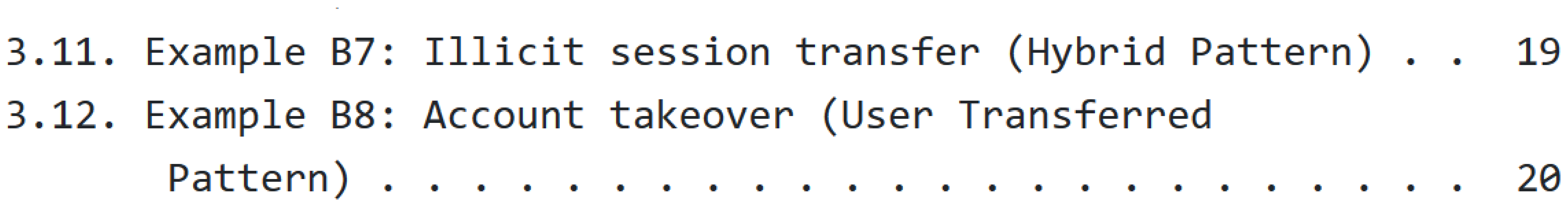

(C) Backchannel Authorization Request
Attackers Initiating Device
(G) Grant Authorization
Authorization Server
(B) Attacker Start Flow
(F) Attacker Forwards Access Code
Attacker
(A) Attacker Sends Social Engineering Message
(E) User Send Access Code
Authorization Device
(D) Send Access Code

Figure 6: Attacker Initiated Cross Device Flow Exploit (Hybrid Pattern)

What’s New: Additional Exploits

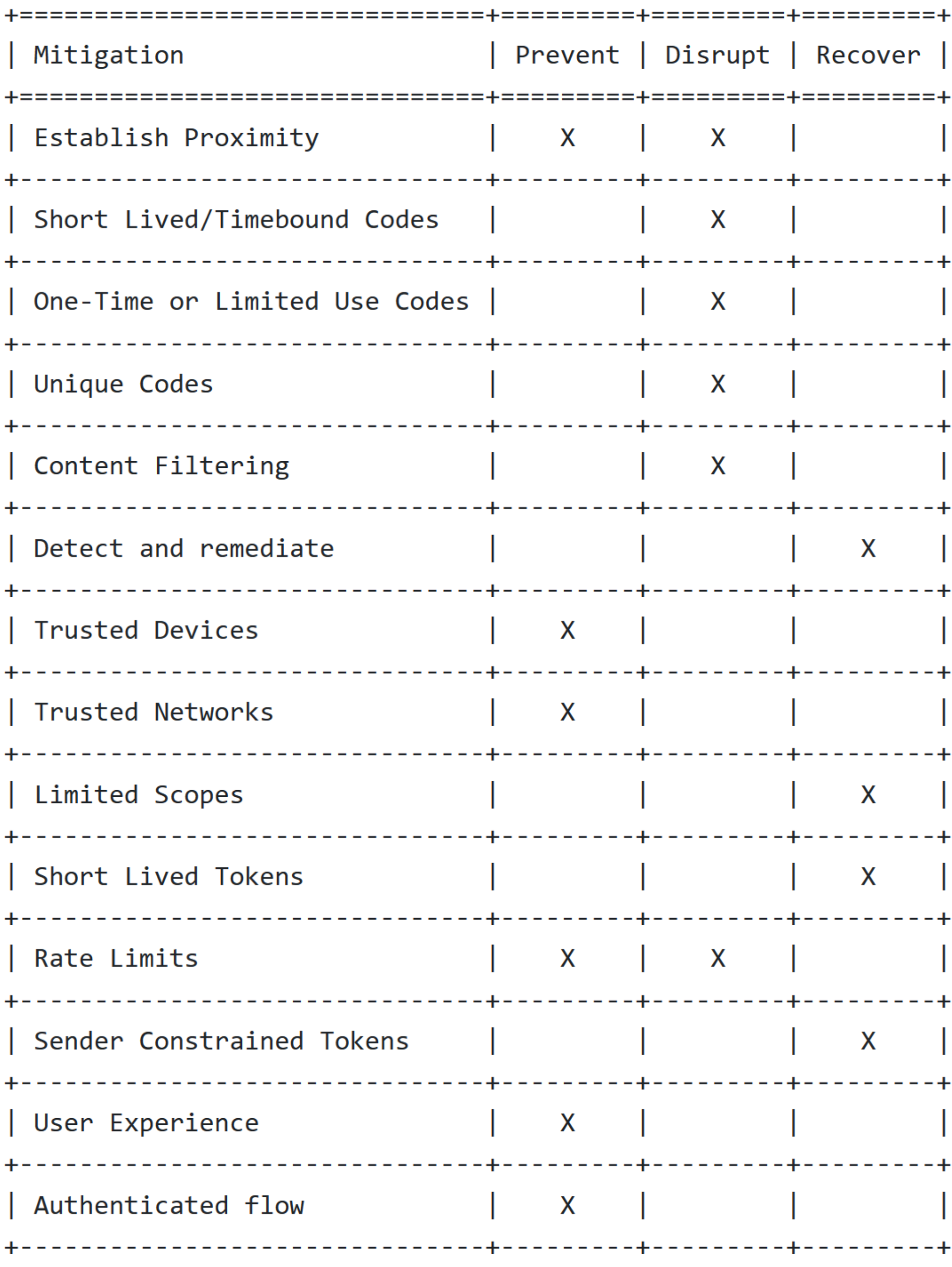


Classified according to protocol pattern

What’s New: Mitigation Limitations

Limitations: Proximity mechanisms raises the bar for an attack. However, depending on how the proximity check is performed, an attacker may be able to circumvent the protection: The attacker can use a VPN to simulate a shared network or spoof a GNSS position. For example, the attacker can try to request the location of the end-user's authorization device through browser APIs and then simulate the same location on his initiating device using standard debugging features available on many platforms.

Limitations: Starting with and authenticated does not prevent the attacks described in Example B5: Illicit Network Join and Example B7: Illicit Session Transfer and it is recommended that additional mitigations described in this document is used if the cross-device flows are used in scenarios such as Example A5: Add a device to a network and Example A7: Transfer a session.



Mitigation	Prevent	Disrupt	Recover
Establish Proximity	X	X	
Short Lived/Timebound Codes		X	
One-Time or Limited Use Codes		X	
Unique Codes		X	
Content Filtering		X	
Detect and remediate			X
Trusted Devices	X		
Trusted Networks	X		
Limited Scopes			X
Short Lived Tokens			X
Rate Limits	X	X	
Sender Constrained Tokens			X
User Experience	X		
Authenticated flow	X		

Table 1: Practical Mitigation Summary

Where do we go Next?

Seen in other places….

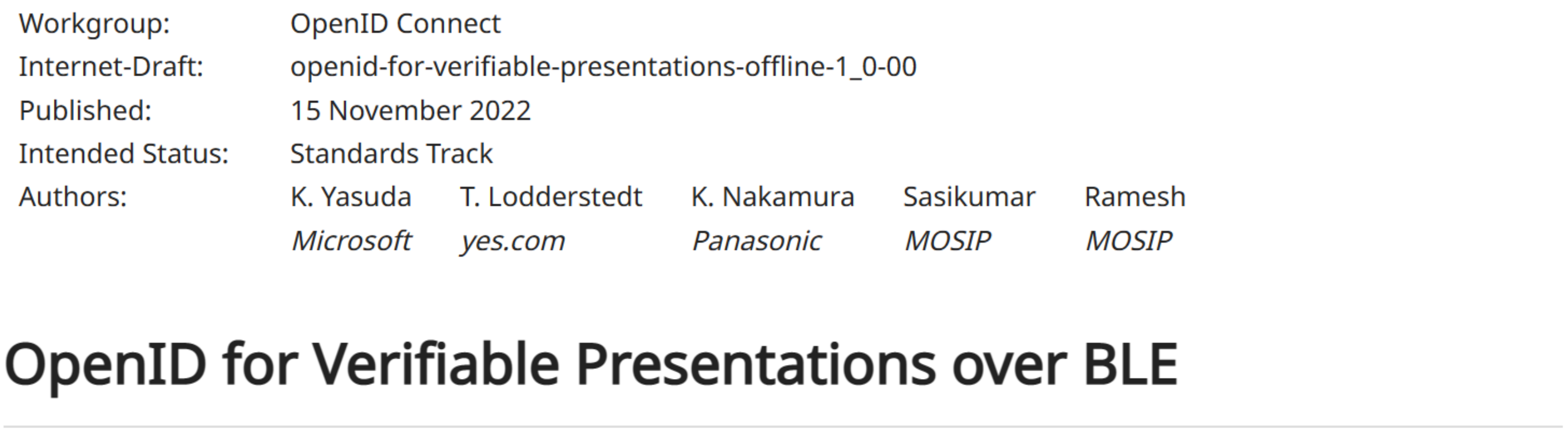
Secure Ranging and Proximity

- IEEE 802.15.4 Ultra Wide Band (UWB)
- Designed to be resistant to relay type attacks
- Developing new use cases in FiRa Consortium

fira The Power to Be Precise

OpenID for Verifiable Presentations over BLE

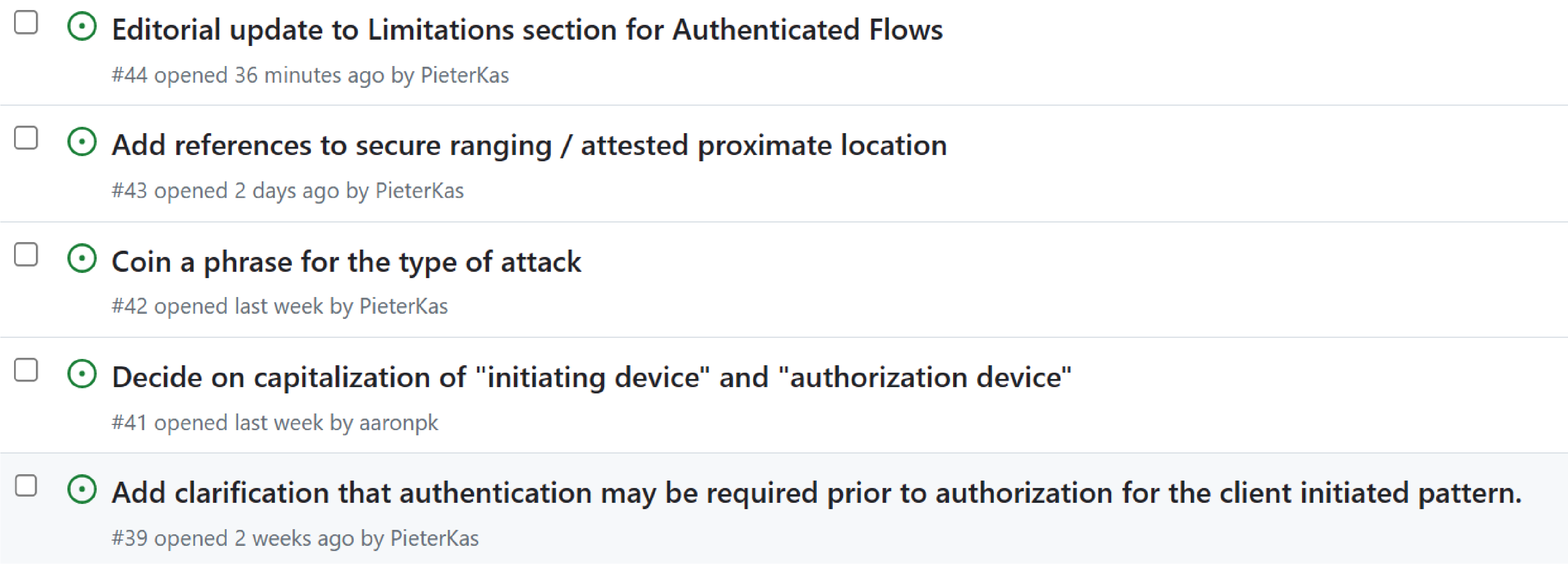
- Too early to reference or consider in the BCP?



Workgroup:	OpenID Connect				
Internet-Draft:	openid-for-verifiable-presentations-offline-1_0-00				
Published:	15 November 2022				
Intended Status:	Standards Track				
Authors:	K. Yasuda *Microsoft*	T. Lodderstedt *yes.com*	K. Nakamura *Panasonic*	Sasikumar *MOSIP*	Ramesh *MOSIP*

OpenID for Verifiable Presentations over BLE

Open Issues



□ ⊙ **Editorial update to Limitations section for Authenticated Flows**

#44 opened 36 minutes ago by PieterKas

□ ⊙ **Add references to secure ranging / attested proximate location**

#43 opened 2 days ago by PieterKas

□ ⊙ **Coin a phrase for the type of attack**

#42 opened last week by PieterKas

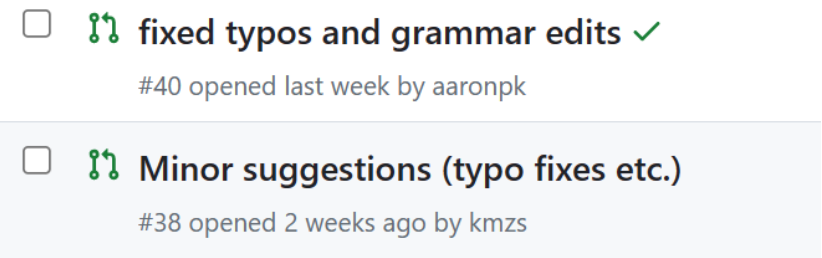
□ ⊙ **Decide on capitalization of "initiating device" and "authorization device"**

#41 opened last week by aaronpk

□ ⊙ **Add clarification that authentication may be required prior to authorization for the client initiated pattern.**

#39 opened 2 weeks ago by PieterKas

PRs



□ **fixed typos and grammar edits** ✓

#40 opened last week by aaronpk

□ **Minor suggestions (typo fixes etc.)**

#38 opened 2 weeks ago by kmzs

Coin a Phrase to Describe the Attack

- Illicit Consent Grant Attack?
  - Describes outcome, not the mechanism
- Attacker-in-the-Middle Attack?
  - Describe attacker capability, but both too broad and too narrow
- Authorization Context Manipulation Attack?
  - Describes the mechanism
- Authorization Context Manipulation Exploit?
  - Describe mechanism, hints that protocol functions as expected.
- Other?

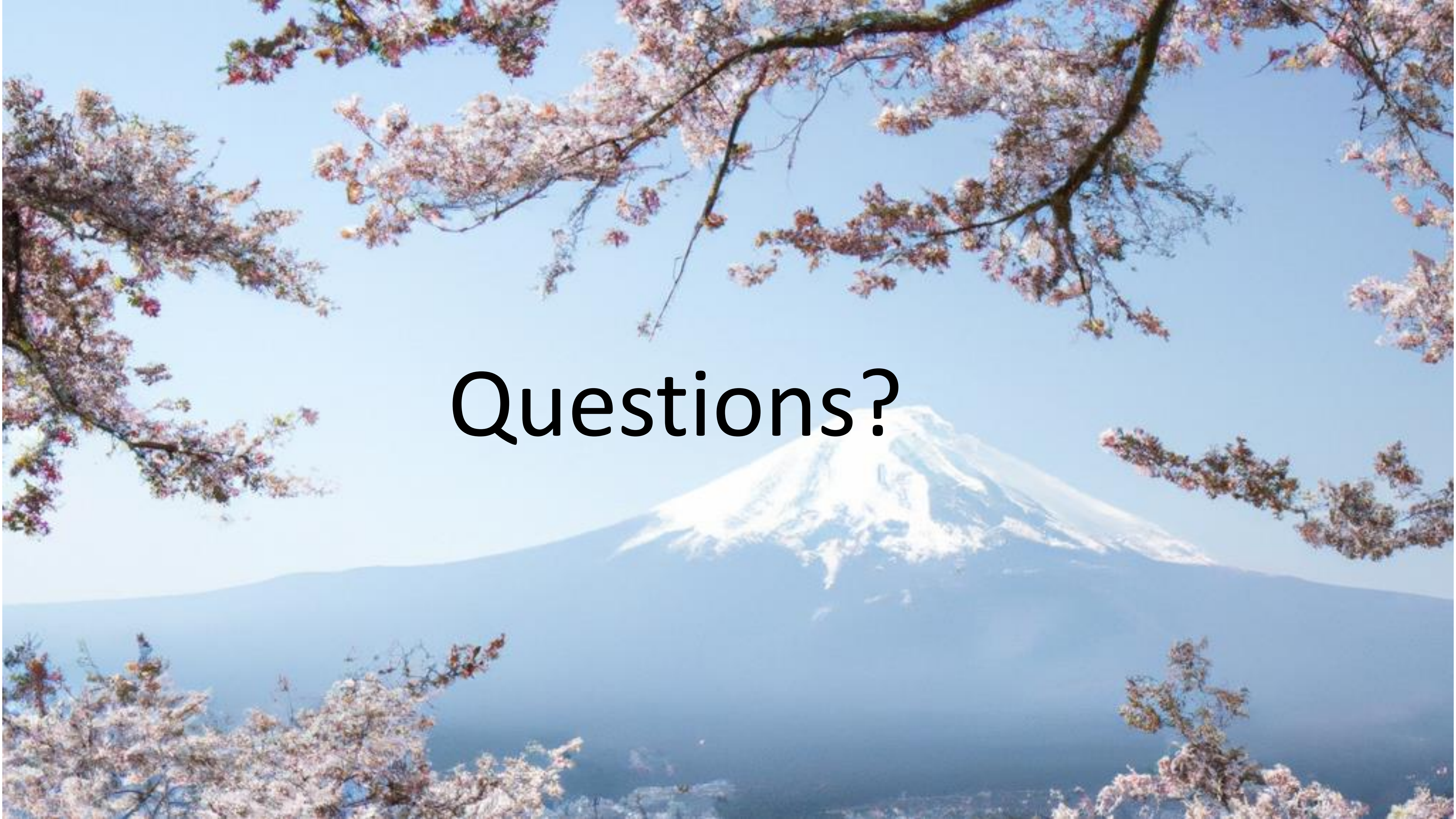
Formal Analysis by University of Stuttgart

Research Team:

Pedram Hosseyni **Tim Würtele** **Klaas Pruiksma** **Clara Waldmann**

Focused on Device Authorization Grant

Expecting results towards the end of summer



Questions?