

Cross Device Flows

Pieter Kasselmann

Daniel Fett

Filip Skokan

IETF 117 San Francisco (July 2023)

Date: 27 July 2023

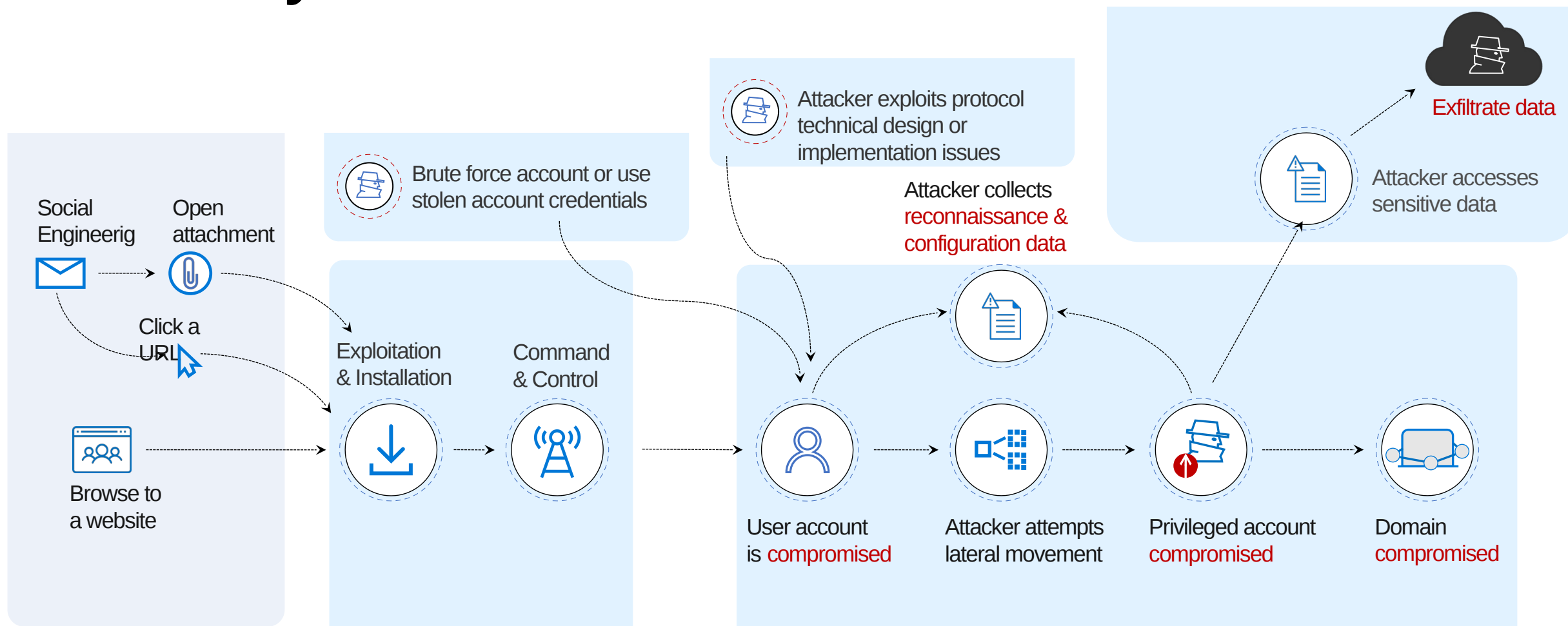


Agenda

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

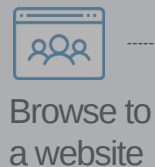
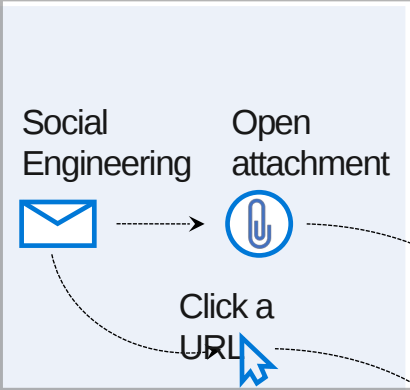
Why are we here?

Anatomy of an attack



Mind the Gap – Where Attackers (often)

Enter



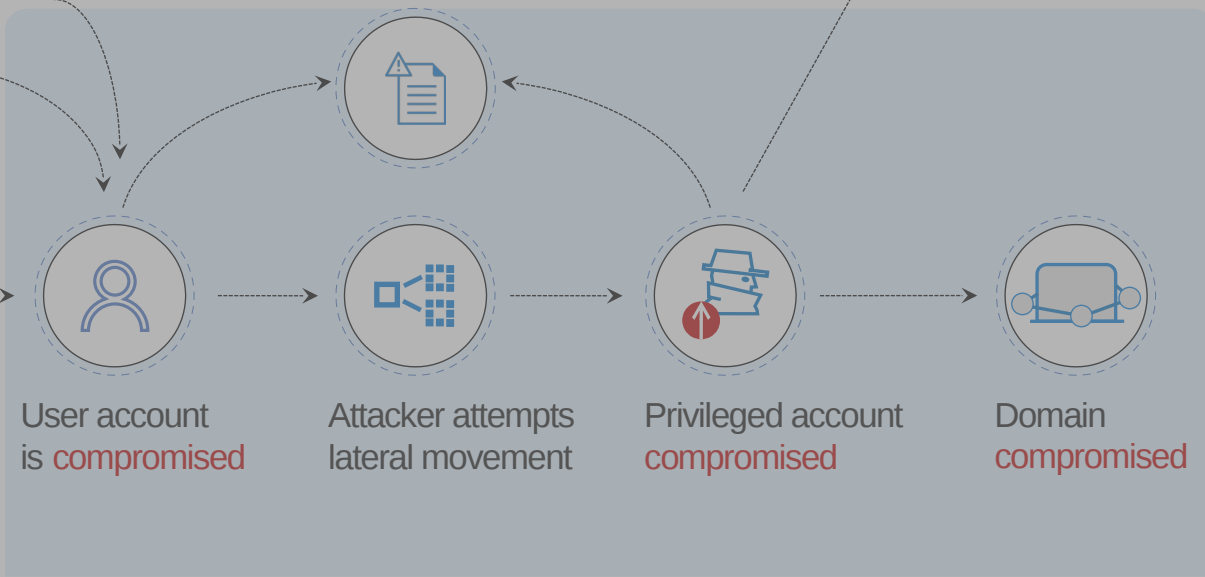
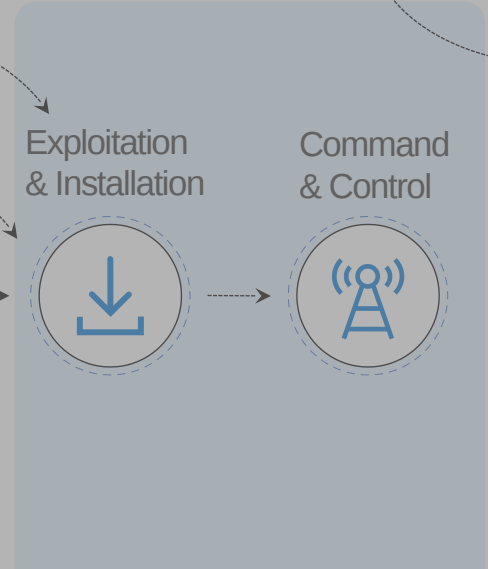
Brute force account or use stolen account credentials

Attacker exploits protocol technical design or implementation issues

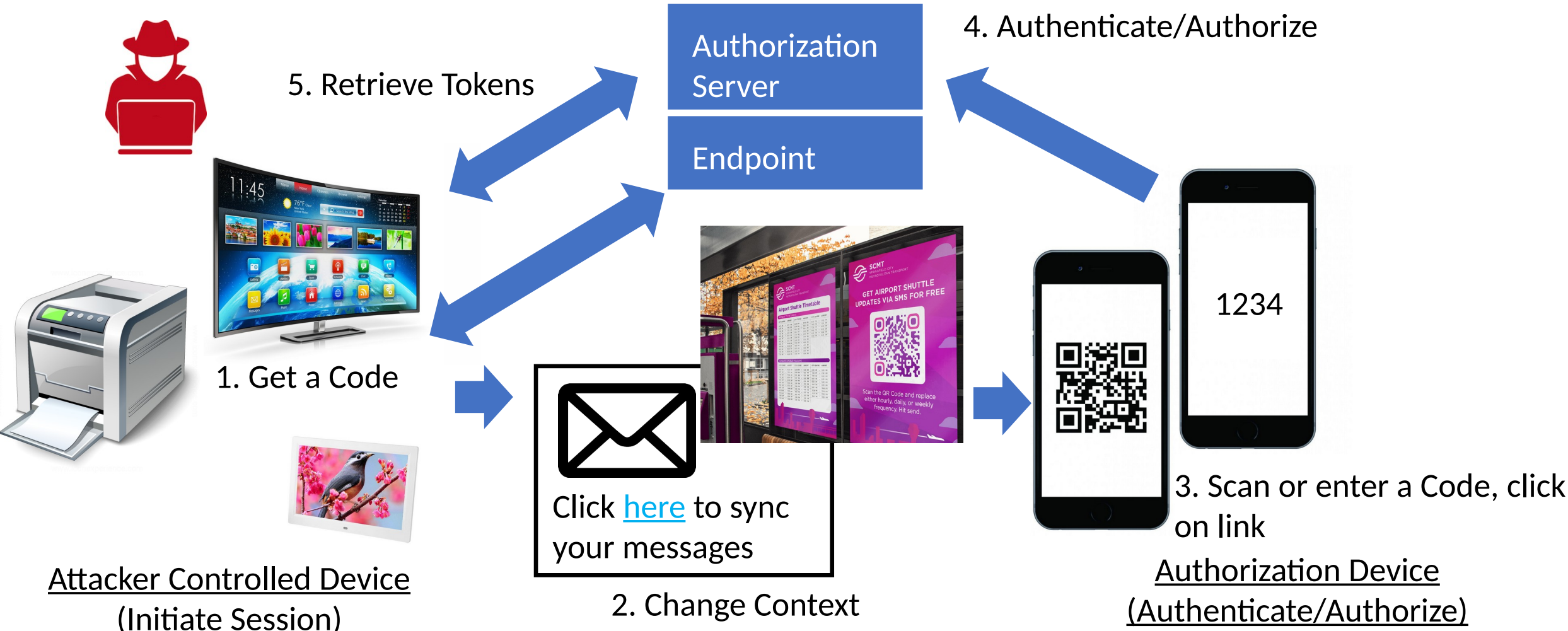
Attacker collects reconnaissance & configuration data

Attacker accesses sensitive data

Exfiltrate data



Cross-Device Flow Social Engineering Exploit



Attack Pattern Summary: Exploit the Unauthenticated Channel

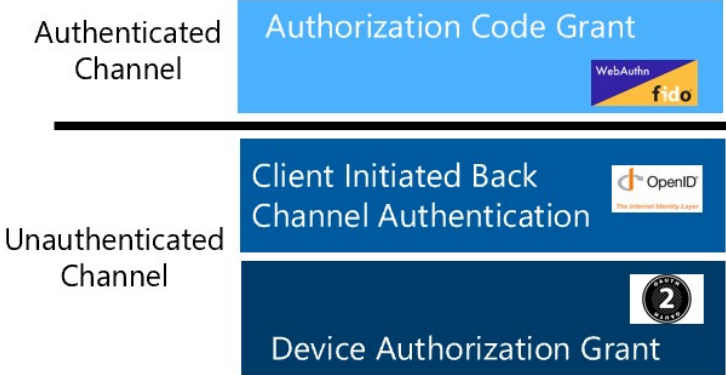
- 1. Initiate the session, retrieve code (QR code, user code)
- 2. Use social engineering to change context and persuade user to authorize session (illicit consent grant)
- 3. Bypasses multi-factor authentication (don't need to harvest credentials)

Mitigation Framework

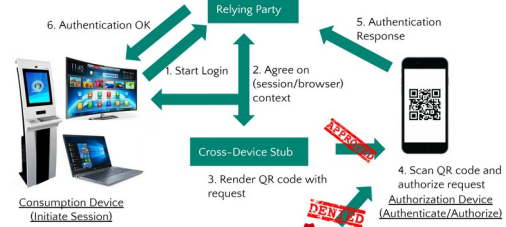
Pragmatic Mitigations

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

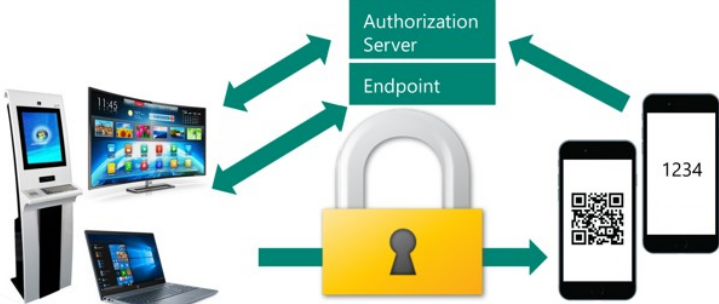
Explore Alternatives



Foundational Underpinnings

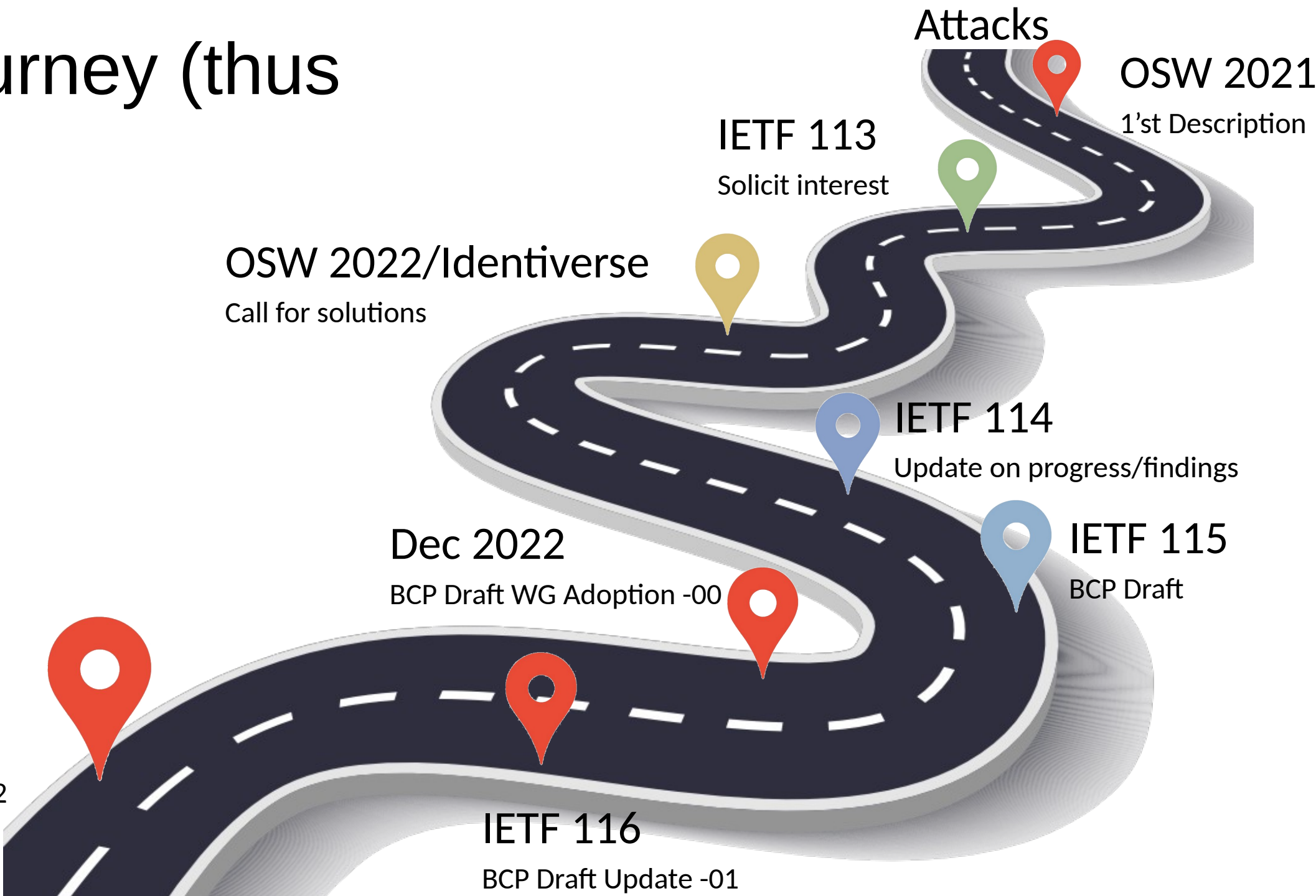


- Summary**
1. Move part of authorization device to the web
 2. Perform checks on request using this web service
 3. Pairing of stub web service and authorization device application



Where are we?

The Journey (thus far)



OSW 2022/Identiverse
Call for solutions

IETF 113
Solicit interest



OSW 2021
1'st Description



Attacks

IETF 114
Update on progress/findings



Dec 2022
BCP Draft WG Adoption -00

IETF 115
BCP Draft



IETF 117
BCP Draft Update -02



IETF 116
BCP Draft Update -01



Cross-Device Flows: Security Best Current Practice

Web Authorization Protocol
Internet-Draft
Intended status: Best Current Practice
Expires: 11 January 2024

P. Kasselmann
Microsoft
D. Fett
yes.com
F. Skokan
Okta
10 July 2023



Cross-Device Flows: Security Best Current Practice
draft-ietf-oauth-cross-device-security-02

Abstract

This document describes threats against cross-device flows along with near term mitigations, protocol selection guidance and the analytical tools needed to evaluate the effectiveness of these mitigations. It serves as a security guide to system designers, architects, product managers, security specialists, fraud analysts and engineers implementing cross-device flows.

<https://datatracker.ietf.org/doc/draft-ietf-oauth-cross-device-security/>

What's New: "Cross-Device Consent Phishing" Name

3. Cross-Device Flow Exploits

Attackers exploit cross-device flows by initiating an authorization flow on the Initiating Device and then use social engineering techniques to change the context in which the request is presented to the user in order to convince them to grant authorization on the Authorization Device. The attacker is able to change the context of the authorization request because the channel between the Initiating Device and the Authorizing Device is unauthenticated. These attacks are also known as Cross-Device Consent Phishing (CDCP) attacks.

What's New: Renamed cross-device flow patterns

- 2. Cross Device Flow Concepts . . .
- 2.1. User Transferred Pattern —————> 2.1. User-Transferred Session Data Pattern . . .
- 2.2. Client Transferred Pattern —————> 2.2. Backchannel-Transferred Session Pattern . .
- 2.3. Hybrid Pattern —————> 2.3. User-Transferred Authorization Data Pattern

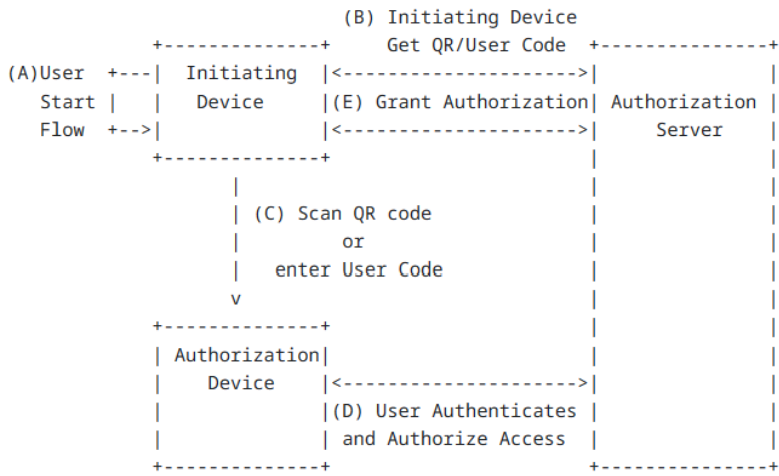


Figure 1: Cross-Device Flows: User-Transferred Session Data Pattern

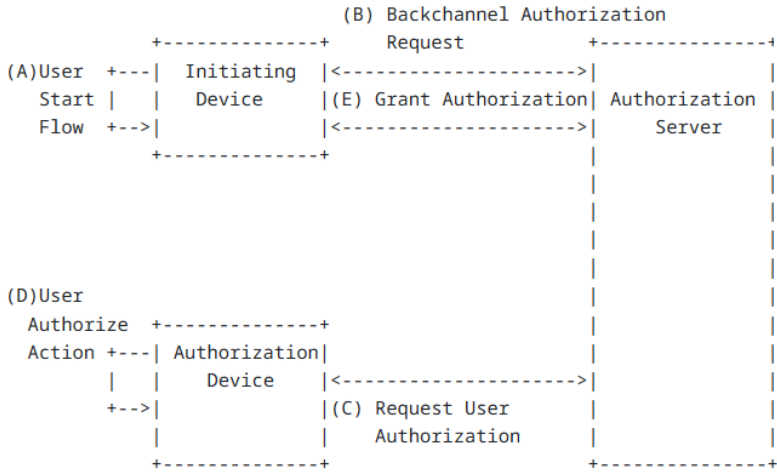


Figure 2: Cross-Device Flows: Backchannel-Transferred Session Pattern

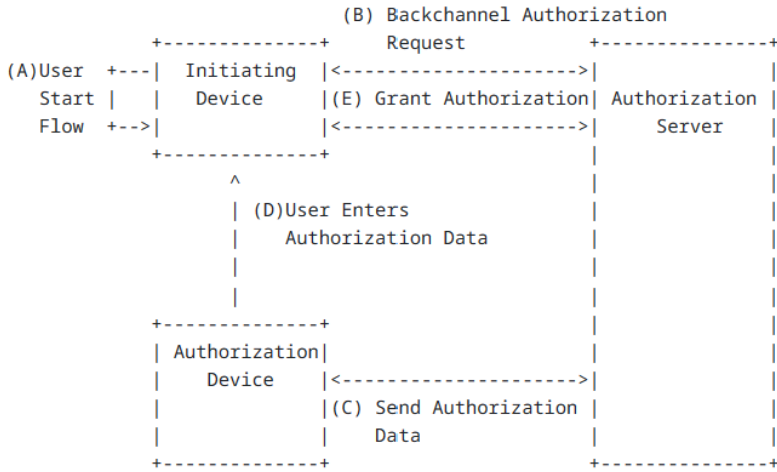


Figure 3: Cross-Device Flow: User-Transferred Authorization Data Pattern

Where do we go Next?

Normative Requirements?

- Several “should, may, recommended”, no “SHOULD, MAY or RECOMMENDED”
 - Security BCPs typically have normative requirements.
 - Raised on mailing list
- Why change
 - Provide clear guidance to implementors
 - Emphasise importance of mitigations
 - Make conformance\adoption meaningful
- Proposal:
 - Adopt normative “SHOULD, MAY and RECOMMENDED” for client and authorization servers.
 - No MUSTs
- PR: <https://github.com/oauth-wg/oauth-cross-device-security/pull/75>



Open Issues

- Add Section on User Education as a mitigation**

#80 opened yesterday by PieterKas

- Update rate limits section**

#78 opened 2 weeks ago by PieterKas

- Capitalize SHOULD, RECOMMENDED and MAY where appropriate**

#73 opened 3 weeks ago by PieterKas

- A better name for "Authenticated Flow"**

#72 opened 3 weeks ago by PieterKas

- Update section on formal analysis**

#53 opened on Jun 14 by PieterKas

Formal Analysis by University of Stuttgart

Research Team:

Pedram Hosseyni



Tim Würtele



Klaas Pruiksmā



Clara Waldmann

Focused on Device Authorization Grant

Update at OAuth Security Workshop 2023 (OSW 2023)

UX Research

Maryam Mehrnezhad, Royal Holloway University of London (RHUL)

- Initial literature study
 - 9 papers published in the last 3 years
 - Highlights training as an effective mitigation
- No published research on UX to prevent cross-device phishing
- Topic for discussion at OAuth Security Workshop 2023 (OSW 2023)



Next Steps

- Close on Normative Requirements
- Update Formal Analysis section after OSW 2023 (August)
- Address remaining open issues
- WG Last Call before IETF 118?

A photograph of the Golden Gate Bridge at night. The bridge's towers and suspension cables are illuminated with warm orange lights, contrasting with the deep blue twilight sky. The bridge spans across a body of water, with city lights visible in the distance. The word "Questions?" is overlaid in white text in the upper right corner.

Questions?