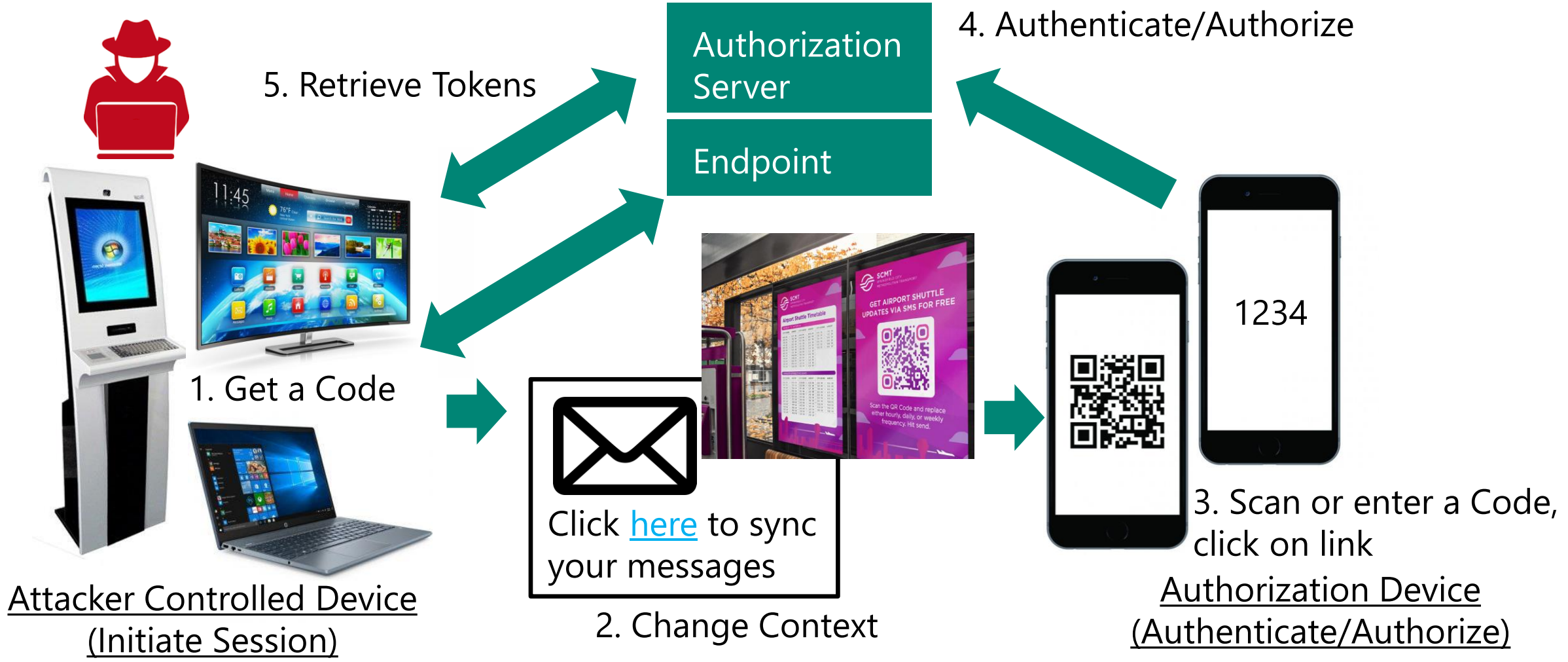
Cross Device Flows

Pieter Kasselman Daniel Fett Filip Skokan

IETF 114 Philadelphia (July 2022)
Date: 26 July 2022

Common Attack Pattern



Attack Pattern Summary

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)

Points to ponder…

Cross Device Flows spans multiple scenarios and protocols

- Authorization (Device Authorization Grant, Client Initiated Backchannel Authentication)
- Wallet invocation (OIDF SIOP, OIDC for VCs)
- Authentication (W3C WebAuthn/FIDO)
- Consumption and Authorization device reversals

Shared Achilles heel

- Unauthenticated channel between consuming and authorising device

Significant interest from customers and researchers

- Shared attack information, feedback, mitigations

Three-pronged approach:

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

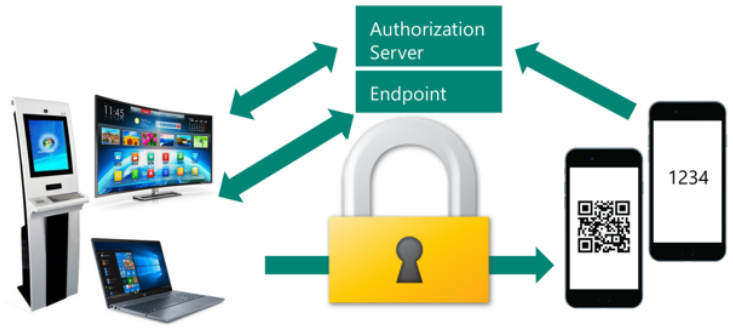
WebAuthn fido

Unauthenticated Channel

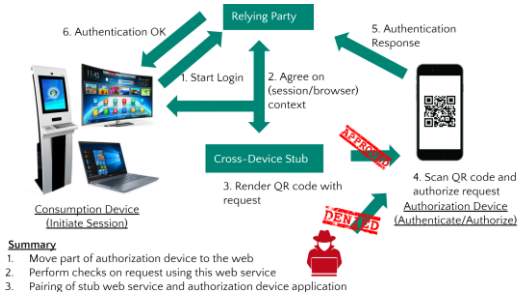
Client Initiated Back Channel Authentication

OpenID

Device Authorization Grant



Foundational Underpinnings



Next Steps

Publish white paper based on what we have learnt so far

- Describe known attacks and practical mitigations for Cross Device Flows
- Cross Device Protocol selection guidance
- Describe foundational underpinnings

Collaborate with researchers to develop verification models to test mitigations

Create protocol/scenario specific guidance (mini-BCPs?)

OAuth Security Workshop Slack Channel?

- Contact Daniel Fett or Pieter Kasselman