Cross Device Flows

Pieter Kasselman    Daniel Fett    Filip Skokan

IETF 114 Philadelphia (July 2022)
Date: 26 July 2022
Common Attack Pattern

1. Get a Code
2. Change Context
3. Scan or enter a Code, click on link
4. Authenticate/Authorize
5. Retrieve Tokens

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**
  - Authenticated Channel: Authorization Code Grant
  - Unauthenticated Channel: Client Initiated Back Channel Authentication, Device Authorization Grant

- **Explore Alternatives**
  - Authorization Server
  - Endpoint

- **Foundational Underpinnings**
  - Sequence:
    1. **Authentication Request**: Where part of authorization device is at the walls
    2. **Agreed on Checksum**: Agreed on checks before sending
    3. **Send QR code with request**: Send QR code with request
    4. **Scan QR Code and send request**: Send QR code and send request
    5. **Authorization Response**: Authorization response
    6. **Authorization Complete**: Authorization complete
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