Cross Device Flows

Pieter Kasselman        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

Social Engineering
- Open attachment
- Click a URL
- Browse to a website

Exploitation & Installation
- Brute force account or use stolen account credentials

Command & Control
- Attacker exploits protocol technical design or implementation issues

User account is compromised
- Attacker attempts lateral movement

Privileged account compromised
- Domain compromised

Attacker accesses sensitive data
- Exfiltrate data

Attacker collects reconnaissance & configuration data
Mind the Gap – Where Attackers (often) Enter

- Social Engineering
  - Open attachment
  - Click a URL

- Exploitation & Installation

- Command & Control

- User account is compromised
- Attacker attempts lateral movement
- Privileged account compromised
- Domain compromised

- 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

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

Explore Alternatives

Foundational Underpinnings

Legend:
- Authorization Server
- Endpoint
- Authentication
- Device
- QR Code
Where are we?
The Journey (thus far)

- **OSW 2021**
  - 1st Description
- **OSW 2022/Identiverse**
  - Call for solutions
- **IETF 113**
  - Solicit interest
- **Dec 2022**
  - BCP Draft WG Adoption -00
- **IETF 114**
  - Update on progress/findings
- **IETF 115**
  - BCP Draft
- **IETF 116**
  - BCP Draft Update -01
- **IETF 117**
  - BCP Draft Update -02
- **Attacks**
  - IETF 117 BCP Draft Update -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.
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

2.1. User Transferred Pattern
2.2. Client Transferred Pattern
2.3. Hybrid 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 Pruiksma  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?
Questions?