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

1. **Social Engineering**
   - Click a URL
   - Browse to a website

2. **Open attachment**
   - Exploitation & Installation
   - Command & Control

3. **Brute force account or use stolen account credentials**

4. **Attacker exploits protocol technical design or implementation issues**

5. **Attacker collects reconnaissance & configuration data**

6. **User account is compromised**
   - Attacker attempts lateral movement
   - Privileged account compromised
   - Domain compromised

7. **Attacker accesses sensitive data**

8. **Exfiltrate data**
Where Protocol Analysts and Standards Experts Focus

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

Exploitation & Installation → Command & Control

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

Attacker collects reconnaissance & configuration data
Attacker exploits protocol technical design or implementation issues

Exfiltrate data
Attacker accesses sensitive data
Mind the Gap – Where Attackers (often) Enter

Social Engineering → Open attachment → Click a URL

- Brute force account or use stolen account credentials
- Attacker exploits protocol technical design or implementation issues
- Attacker collects reconnaissance & configuration data

Exploitation & Installation → Command & Control

- 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

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)
Designed for Homo Securitus, used by Homo Sapiens

**Homo Securitus**
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

**But is a rare species....**

**Homo Sapiens**
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**
Where are we?
What’s New: Distinguish protocol patterns

2. Cross Device Flow Concepts

2.1. User Transferred Pattern

2.2. Client Transferred Pattern

2.3. Hybrid Pattern
What’s New: Additional Scenarios

2.4.7. Example A7: Transfer a session (Hybrid) ........ 10
2.4.8. Example A8: Access a productivity application (Hybrid) ....................... 11

Classified according to protocol pattern
What’s New: Exploits for each pattern

3. Cross-Device Flow Exploits .................................. 11
3.1. User Transferred Pattern ................................. 11
3.2. Client Transferred Pattern ............................... 13
3.3. Hybrid Pattern .............................................. 15
What’s New: Additional Exploits

3.11. Example B7: Illicit session transfer (Hybrid Pattern) ..... 19
3.12. Example B8: Account takeover (User Transferred Pattern) ................................................ 20

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.
Where do we go Next?
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

OpenID for Verifiable Presentations over BLE

- Too early to reference or consider in the BCP?
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?