OAuth Redirect Security

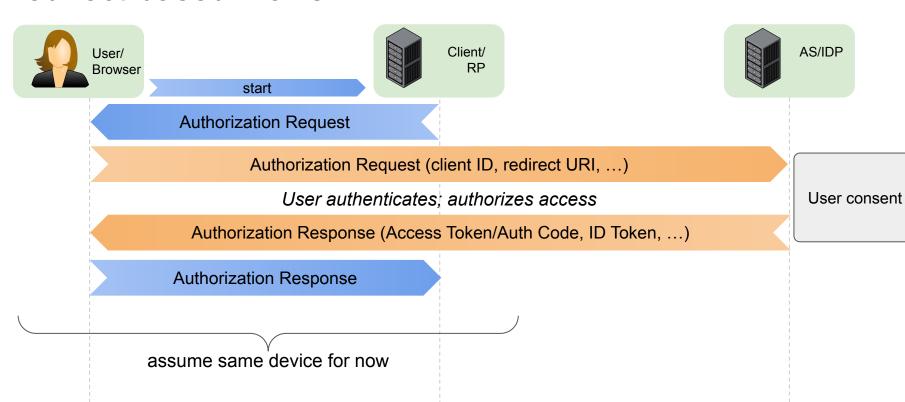
Dr. Daniel Fett

Dr. Daniel Fett

- Security specialist at yes.com
- Working groups:
 - IETF: OAuth
 - OpenID Foundation: OpenID Connect
 - OpenID Foundation: Financial-grade API Security Profile
 - OpenID Foundation: eKYC and Identity Assurance
- Formal analysis of web security



Redirect-based Flows



(Selected) Attacks

Auth Request MITM

Attacker forwards an auth request to a user who then completes the flow on the attacker's behalf.

CSRF

Attacker uses a <u>credential issued for themselves</u> and tries to inject it into a flow on a user's device between the user and a verifier.

Exfiltration of Personal Data (ID Token, VP Token)

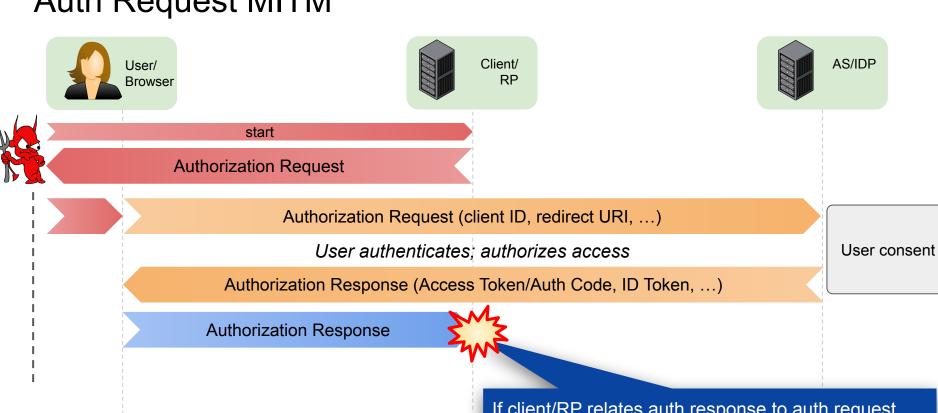
The exfiltration of personal data without the user's (proper) consent.

Injection

Attacker uses an exfiltrated <u>credential issued for a user</u> and tries to inject it into a flow on the attacker's own device to mislead a verifier.

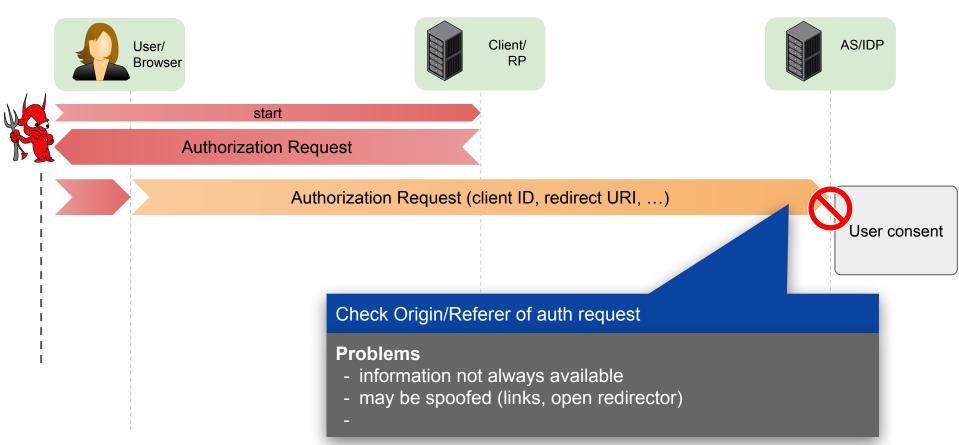
Auth Request MITM

Auth Request MITM



If client/RP relates auth response to auth request, attacker is now authorized/authenticated.

Auth Request MITM - Countermeasures - Option 1



Auth Request MITM - Countermeasures - Option 2









Authorization Request

Authorization Request (client ID, redirect URI, ...)

User authenticates; authorizes access

Authorization Response (Access Token/Auth Code, ID Token, ...)

Authorization Response



Check that auth request and auth response are in the same browser session

User consent

What about Cross-Device Flows?

In cross-device flows, both Option 1 and Option 2 break.

Independent of concrete protocol.

We are working on solutions...

Workgroup: Web Authorization Protocol

Internet-Draft: draft-kasselman-cross-device-security-00

Published: 19 October 2022

Intended Status: Best Current Practice

Expires: 22 April 2023

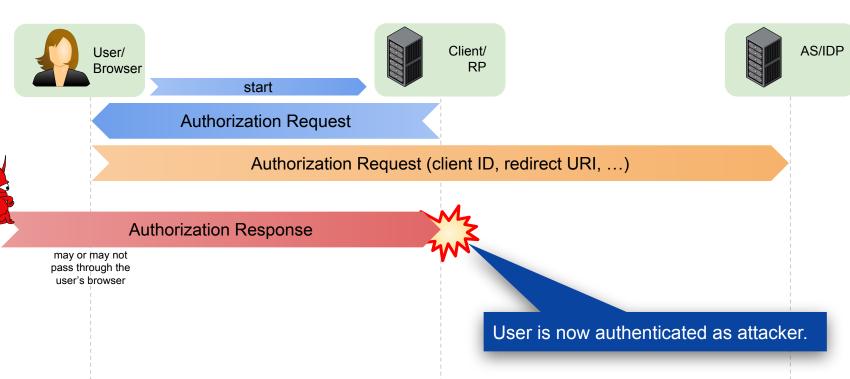
Authors: P. Kasselman D. Fett F. Skokan

Microsoft yes.com Okta

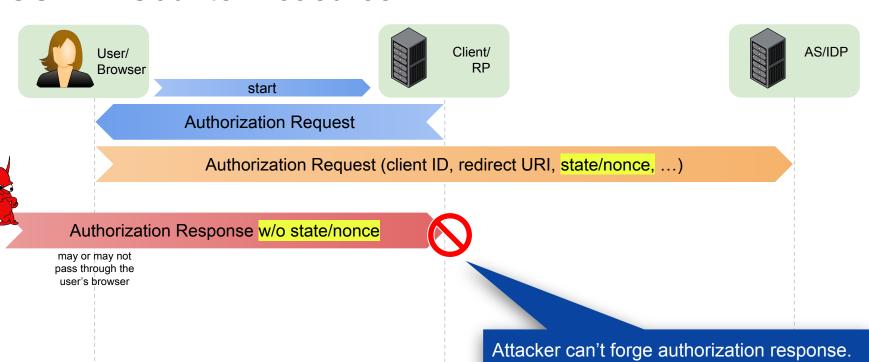
Cross Device Flows: Security Best Current Practice

CSRF

CSRF

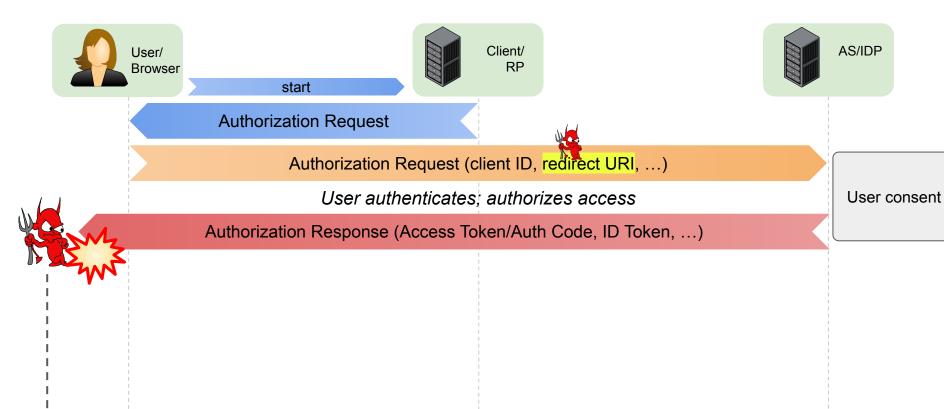


CSRF - Countermeasures

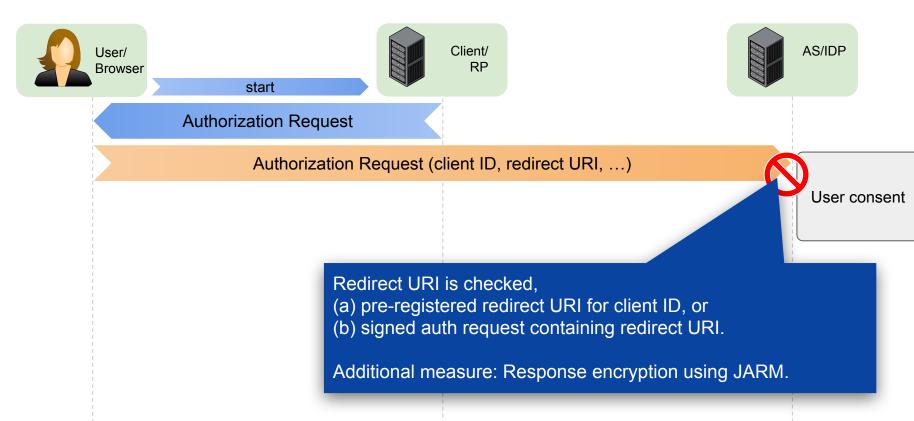


Exfiltration of PII

Exfiltration of PII

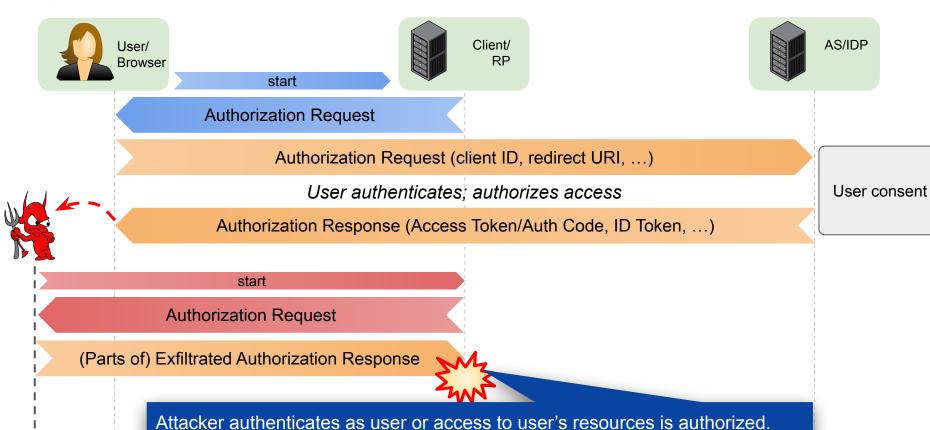


Exfiltration of PII - Countermeasures



Injection

Injection Attack



Injection Attack - Countermeasures

- For access token: Don't use frontchannel flow
- For ID Token & VP Token:
 - Ensure that token must be obtained for the correct client (Audience Restriction/"aud")
 - Ensure that token is bound to transaction (Nonce)



Dr. Daniel Fett yes.com danielf@yes.com @dfett42