Single Sign-On Security:
OAuth & OpenID Connect Training

HACKMANIT

Dr. Christian Mainka | @CheariX

The Password Dilemma

Username / Password1

Username / Password2

Username / Password3

Username / Password4

Username / Password5

Slashdot
News for Nerds. Stuff that matters.

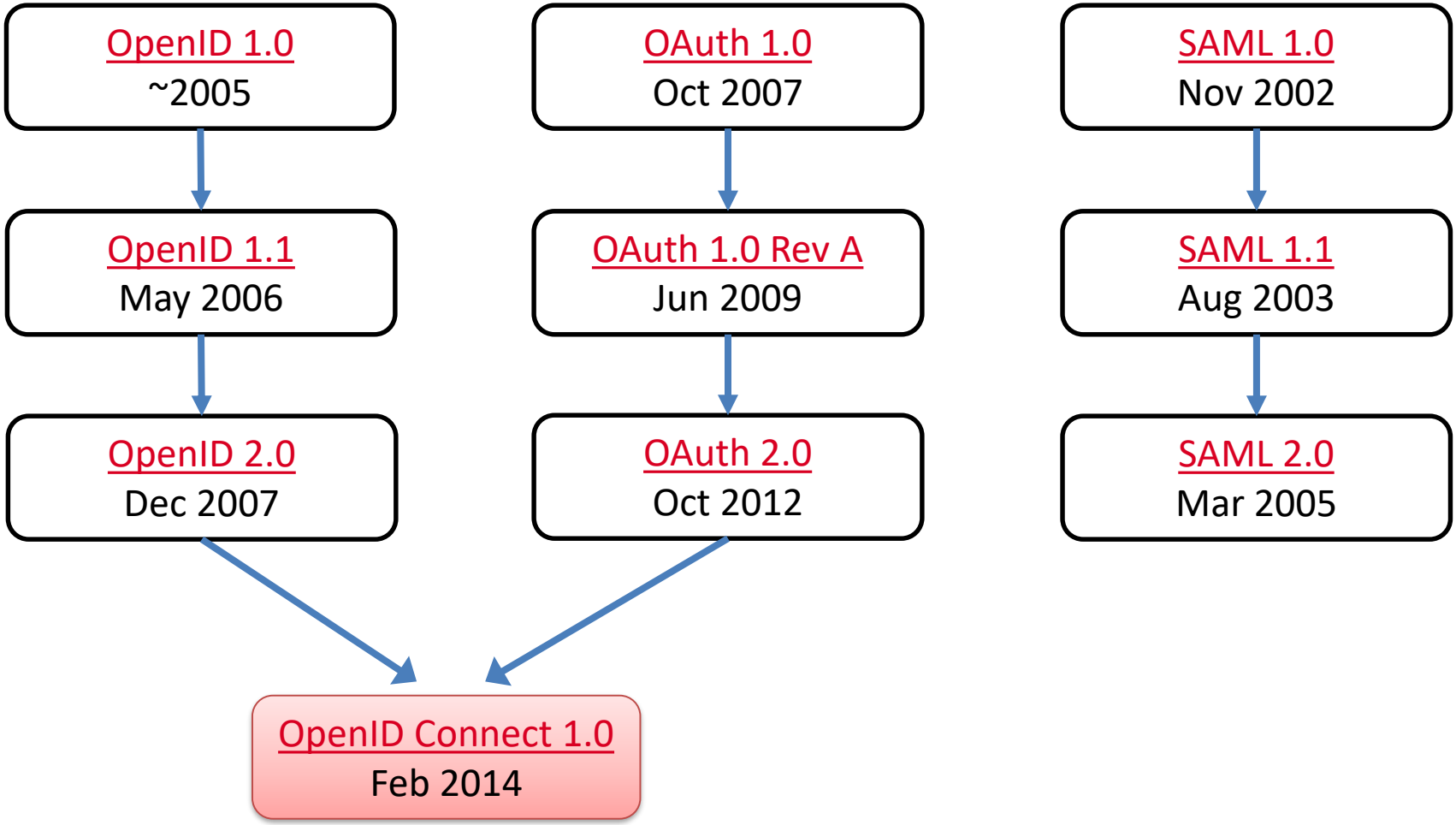
salesforce
SOFTWARE

stackoverflow

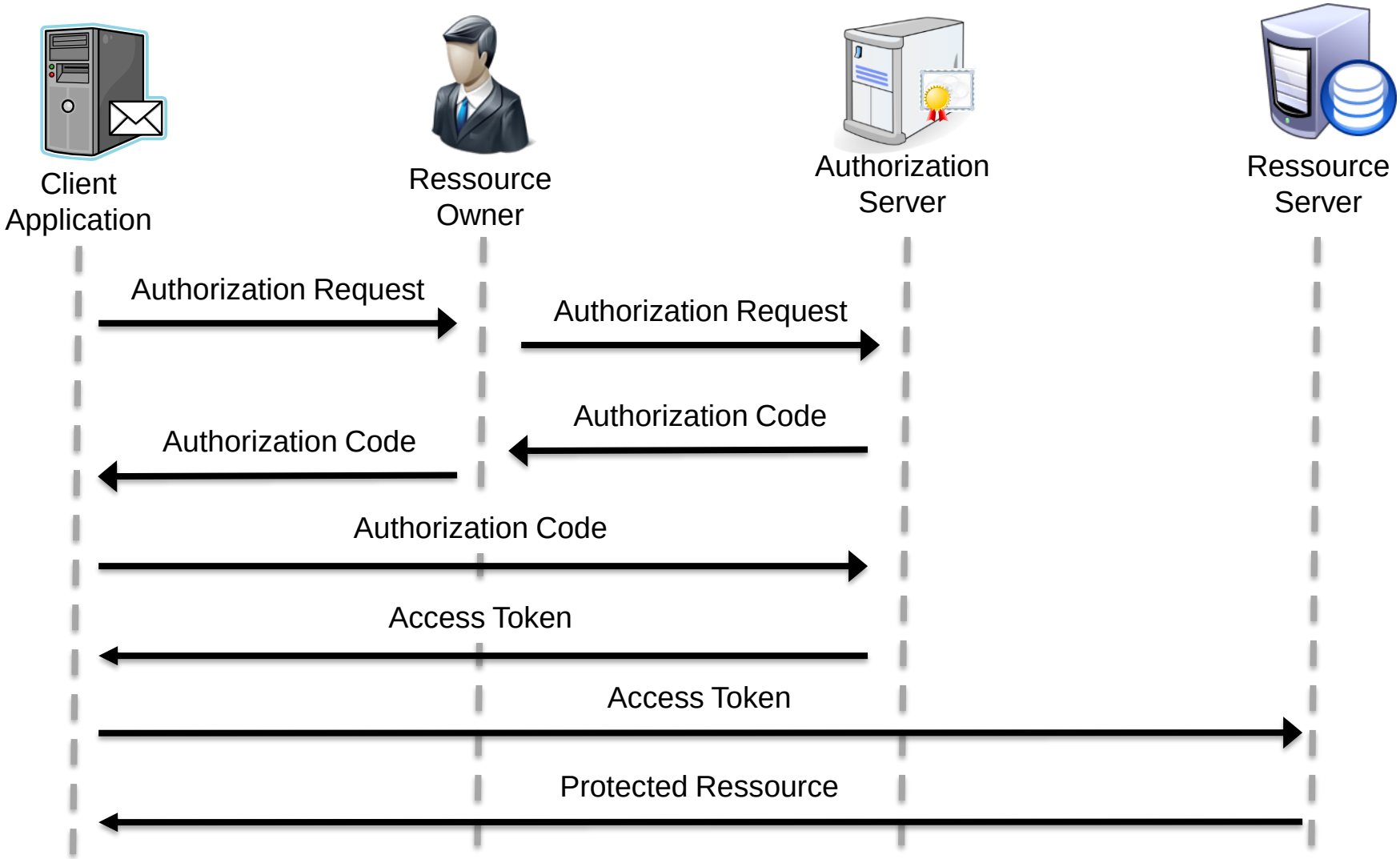
NETFLIX

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

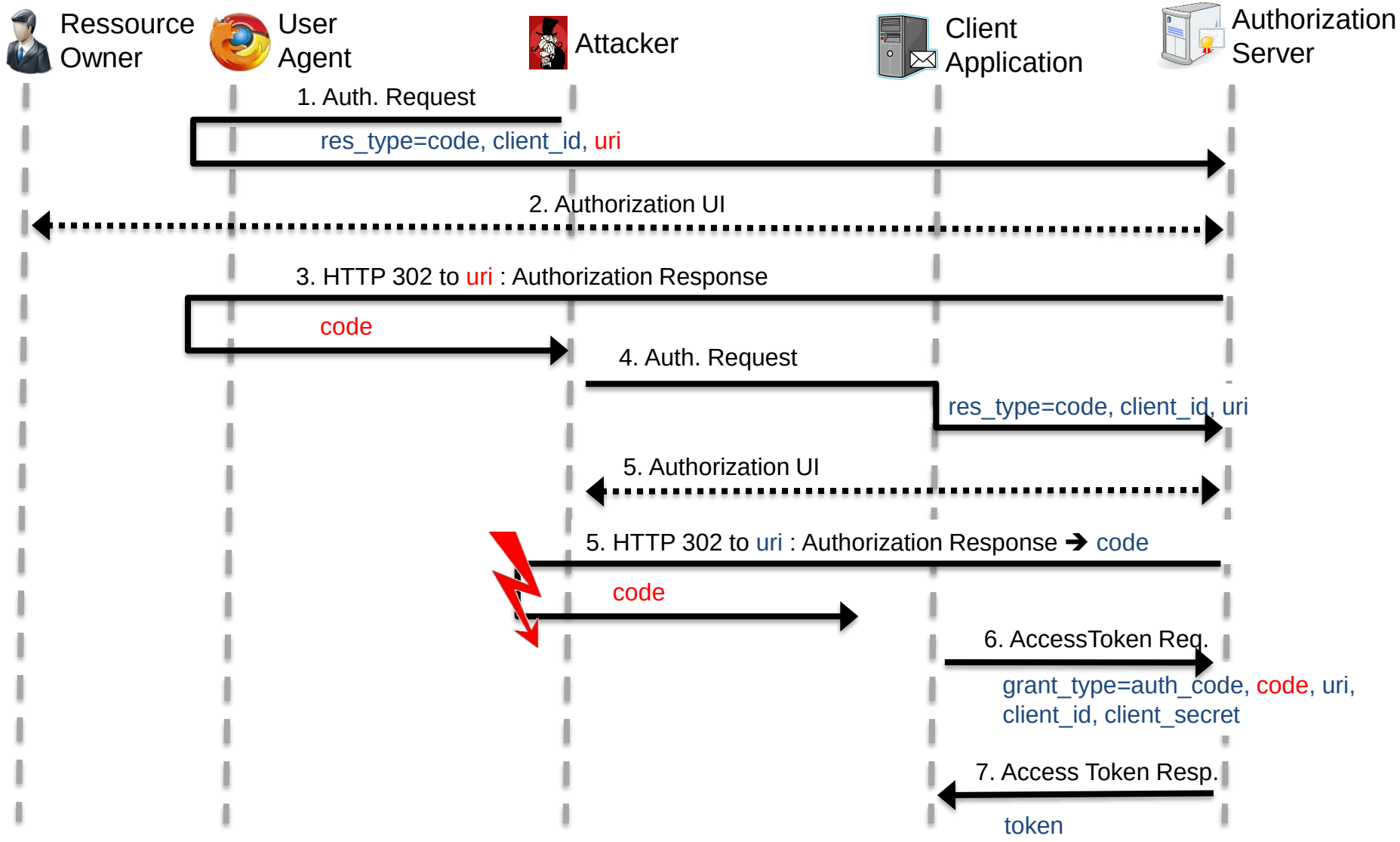
History of Single Sign-On



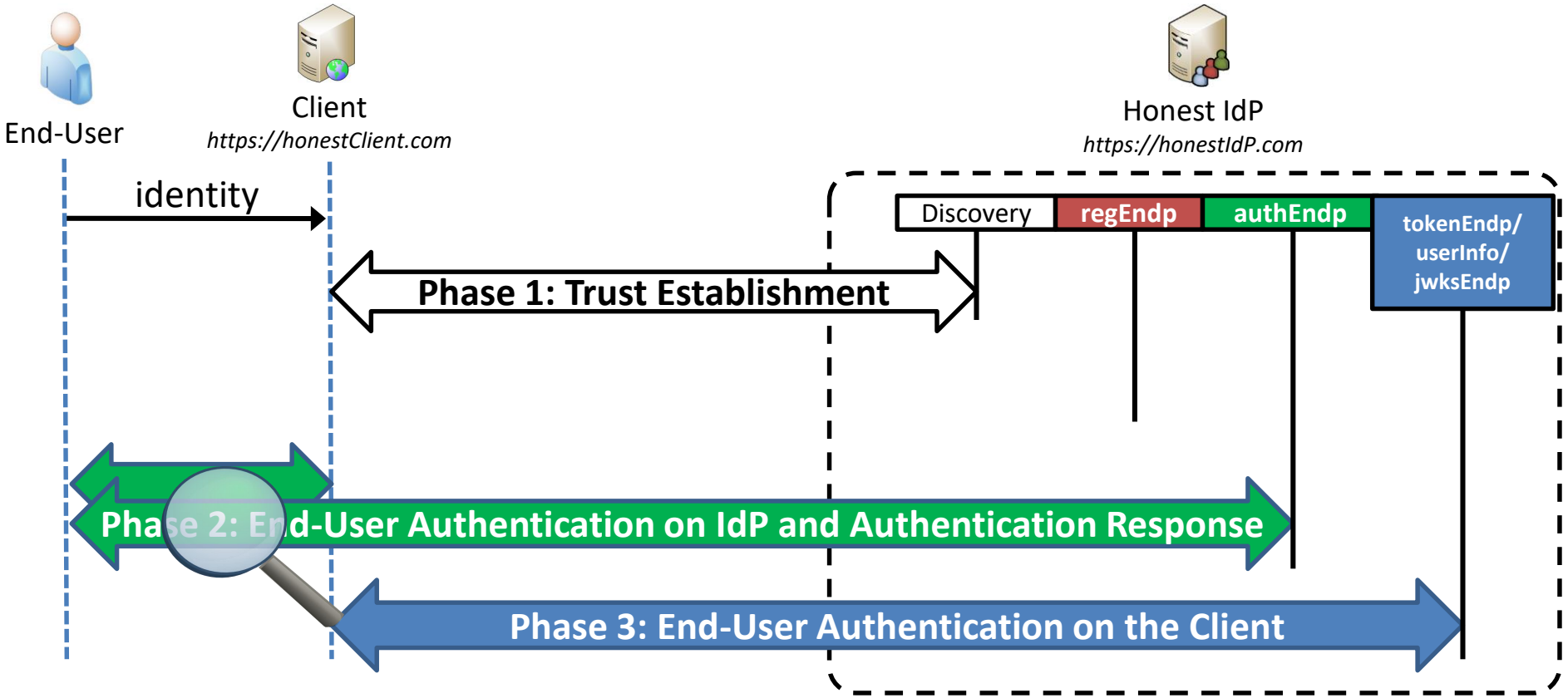
OAuth 2.0 Overview and Terminology



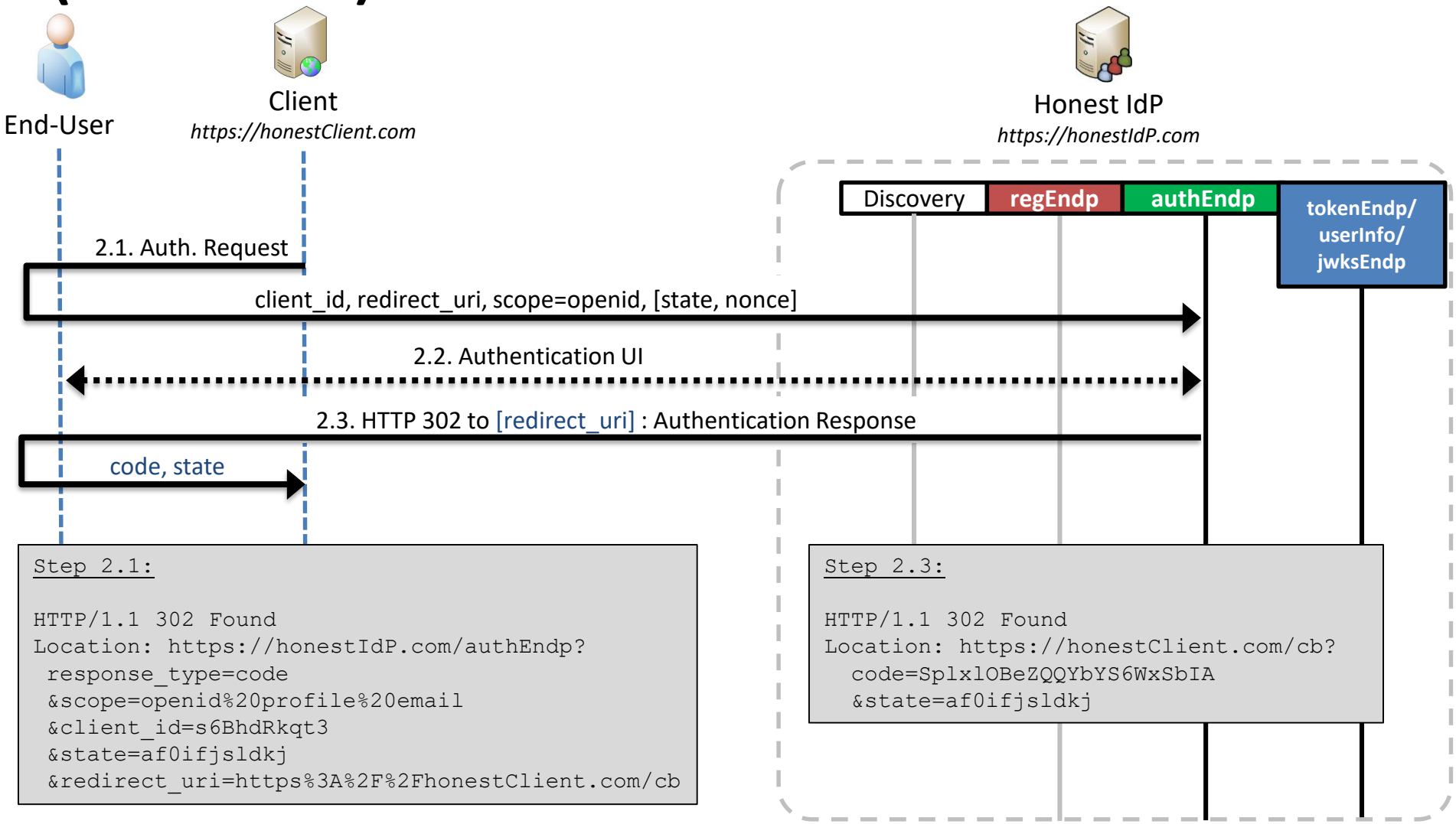
Attack: Authorization Code Grant



OpenID Connect in Three Phases



OpenID Connect: End-User Authentication on IdP (Code Flow)



Flow Recognition Cheat-Sheet

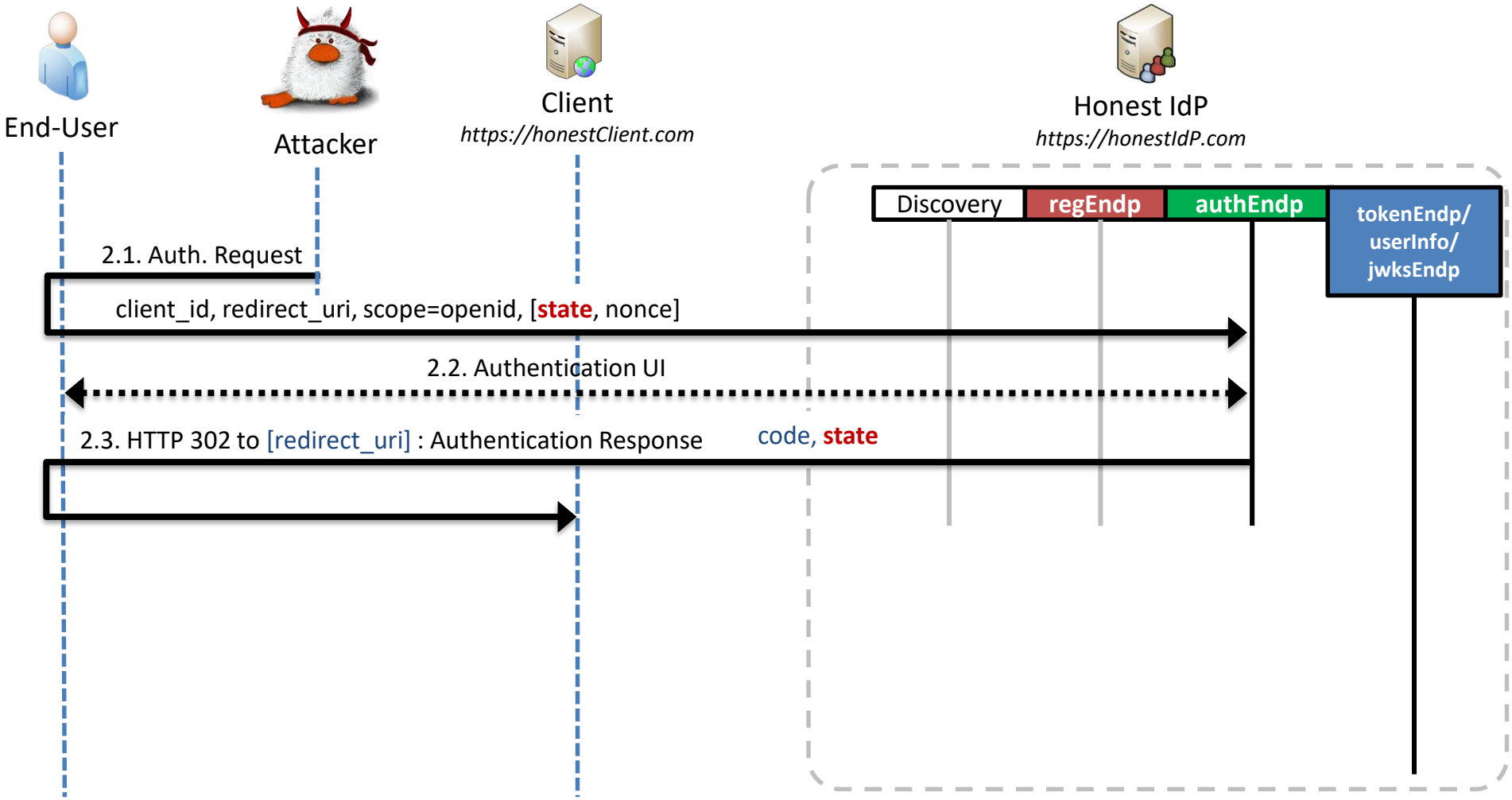
- OpenID Connect has `scope=openid`
  - OAuth does not define a scope value
- Flow distinguished by `response_type`

	OAuth	OpenID Connect
Code Flow	• `code`	• `code`
Implicit Flow	• `token`	• `id_token` • `id_token token` (token means access_token)
Hybrid Flow	(not existing)	• `code token` • `code id_token` • `code token id_token`

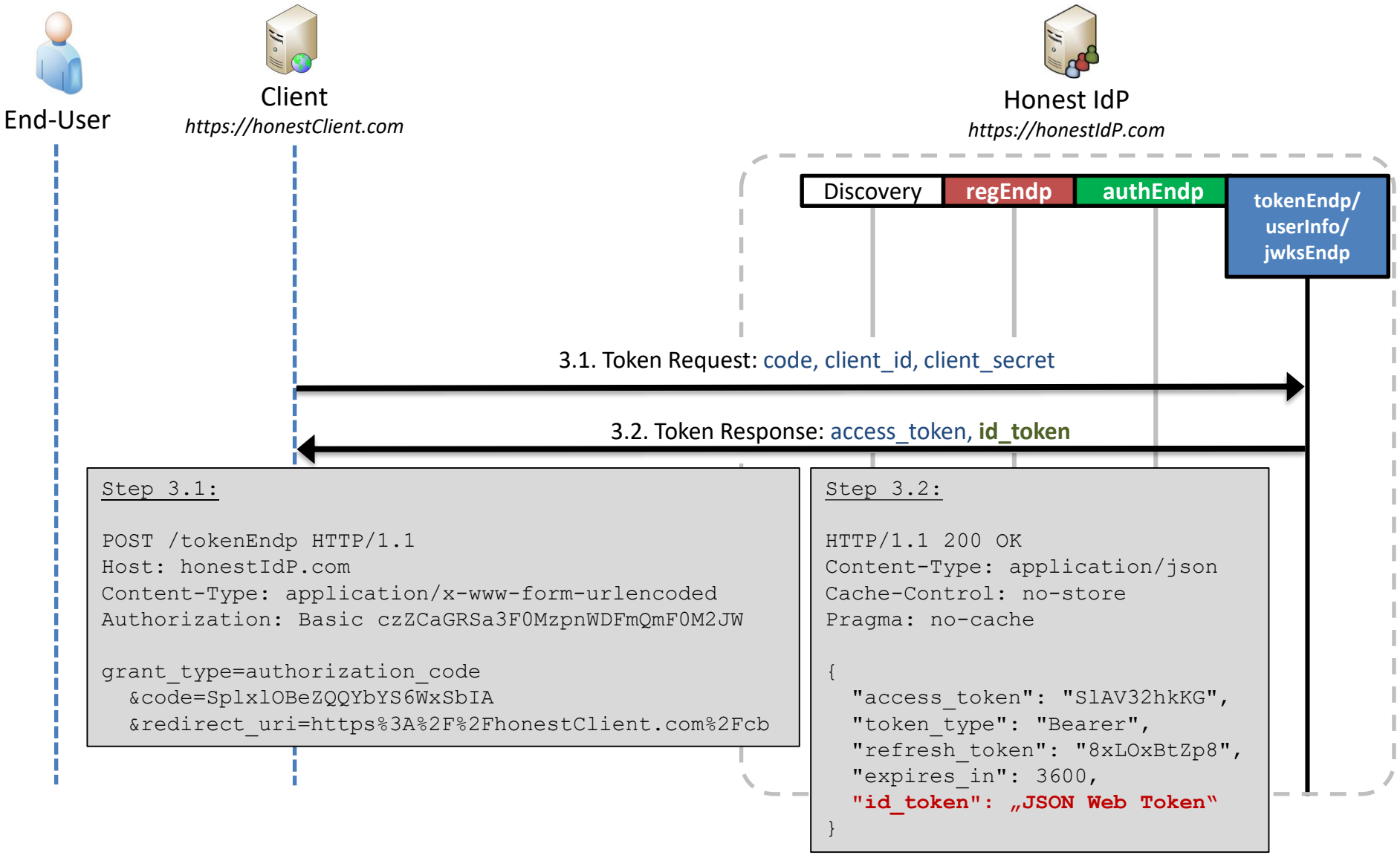
Agenda: First Attacks

- Classic Web Attacks
    - Cross-Site Scripting (XSS)
    - Clickjacking
    - Cross-Site Request Forgery
- Applying to OAuth/OpenID Connect
    - Attacks on state: CSRF
    - Attacks on state: XSS
    - Clickjacking
- Redirects in SSO: Cut-and-Paste Attack
- Authentication vs. Authorization

CSRF Attack


End-User
Attacker
Client
https://honestClient.com
Honest IdP
https://honestIdP.com
Discovery
regEndp
authEndp
tokenEndp/
userInfo/
jwksEndp
2.1. Auth. Request
client_id, redirect_uri, scope=openid, [state, nonce]
2.2. Authentication UI
2.3. HTTP 302 to [redirect_uri] : Authentication Response
code, state

OIDC: id_token in Code Flow



Attack: Signature Bypass

Identity

= iss sub

Freshness

= iat exp nonce

Recipient

= aud

Signature

= sig alg

JWT Header

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

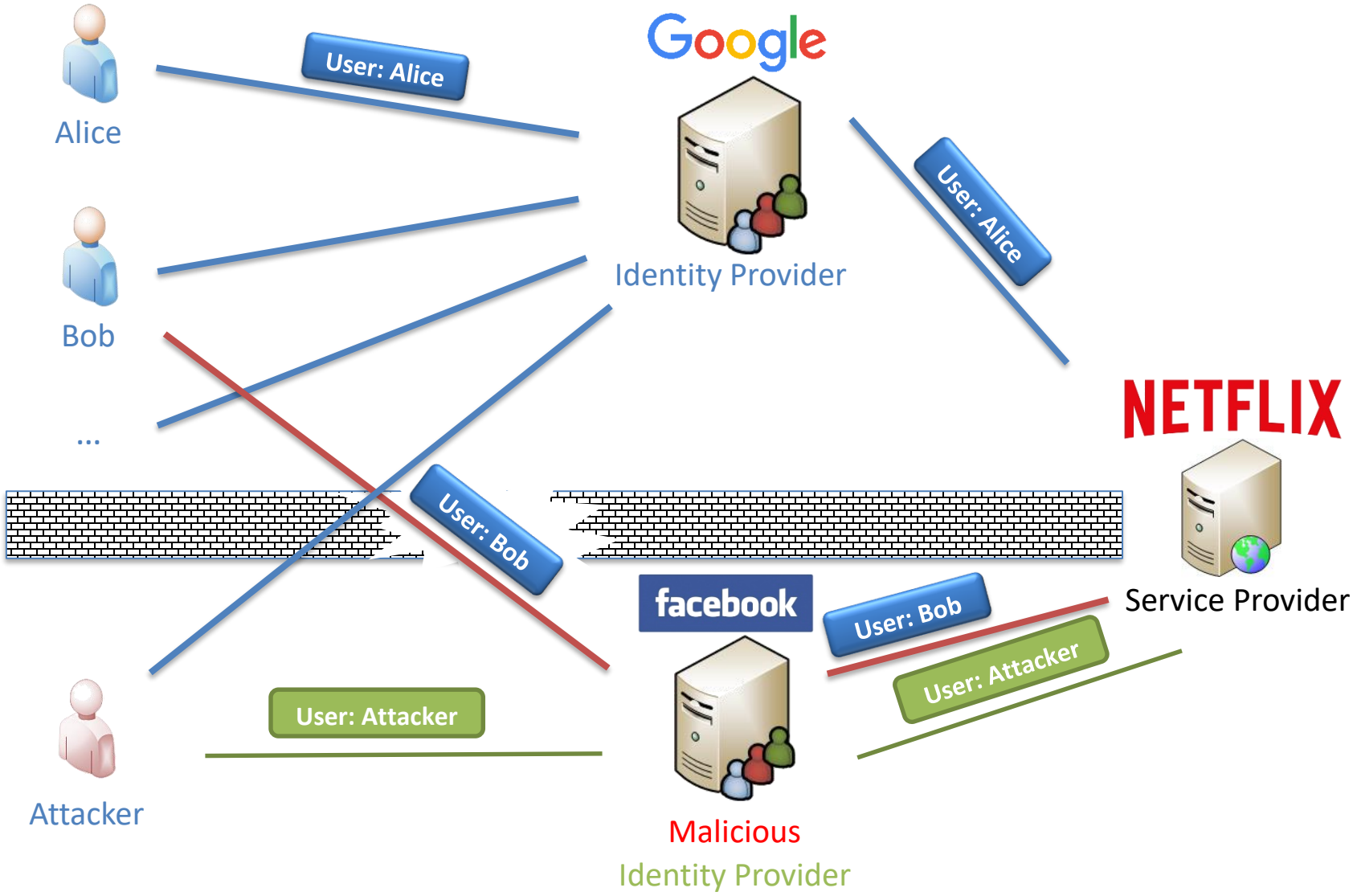
JWT Body

```
{
  "iss": "https://idp.com/",
  "sub": "user1",
  "iat": 1442673964,
  "exp": 1444148308,
  "nonce": "40c6b33b9a2e",
  "aud": "client_id"
}
```

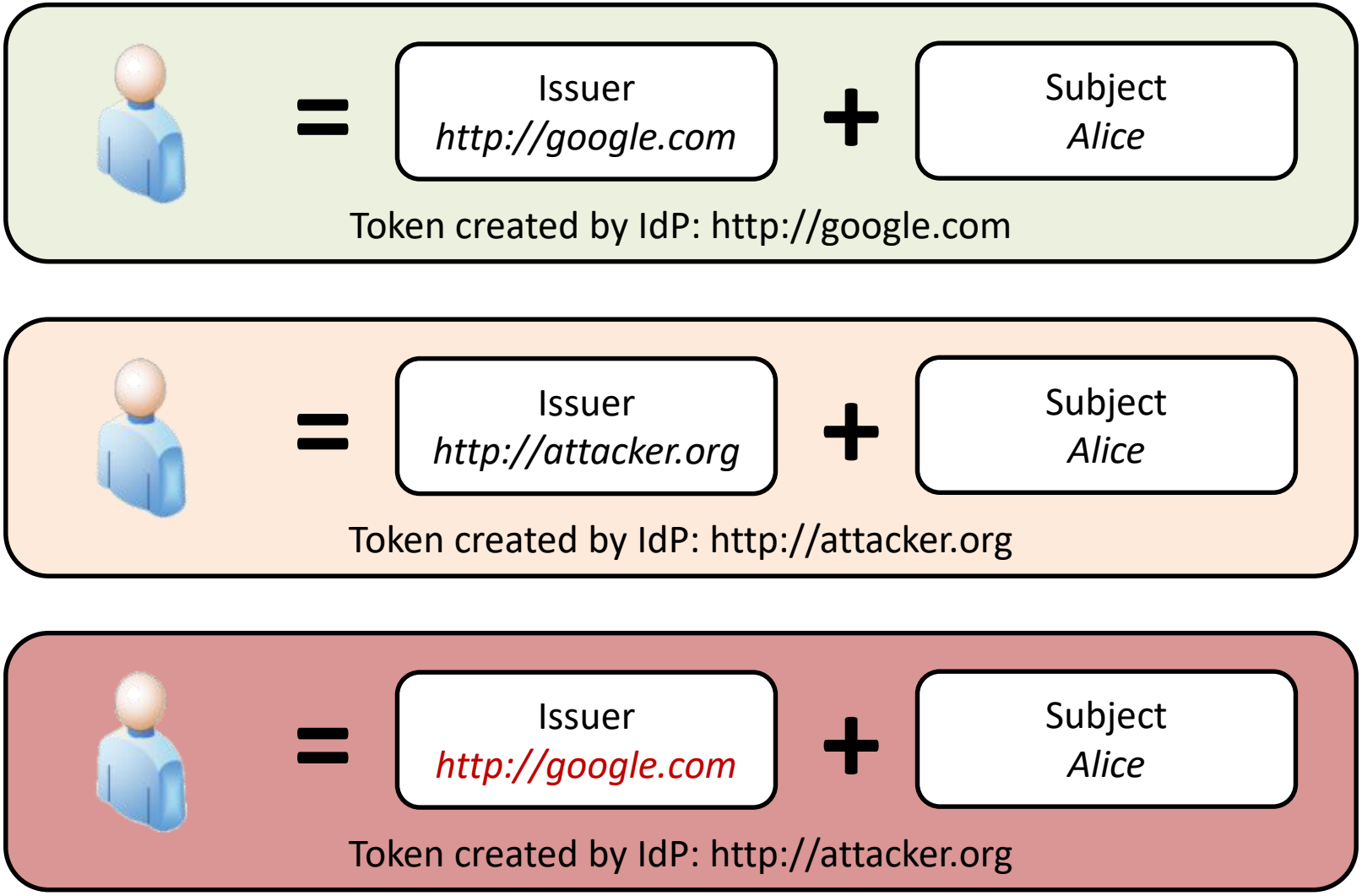
JWT Signature

```
[0x02, 0xF1, …, 0xDA]
```

Single Sign-On Attacker Paradigm

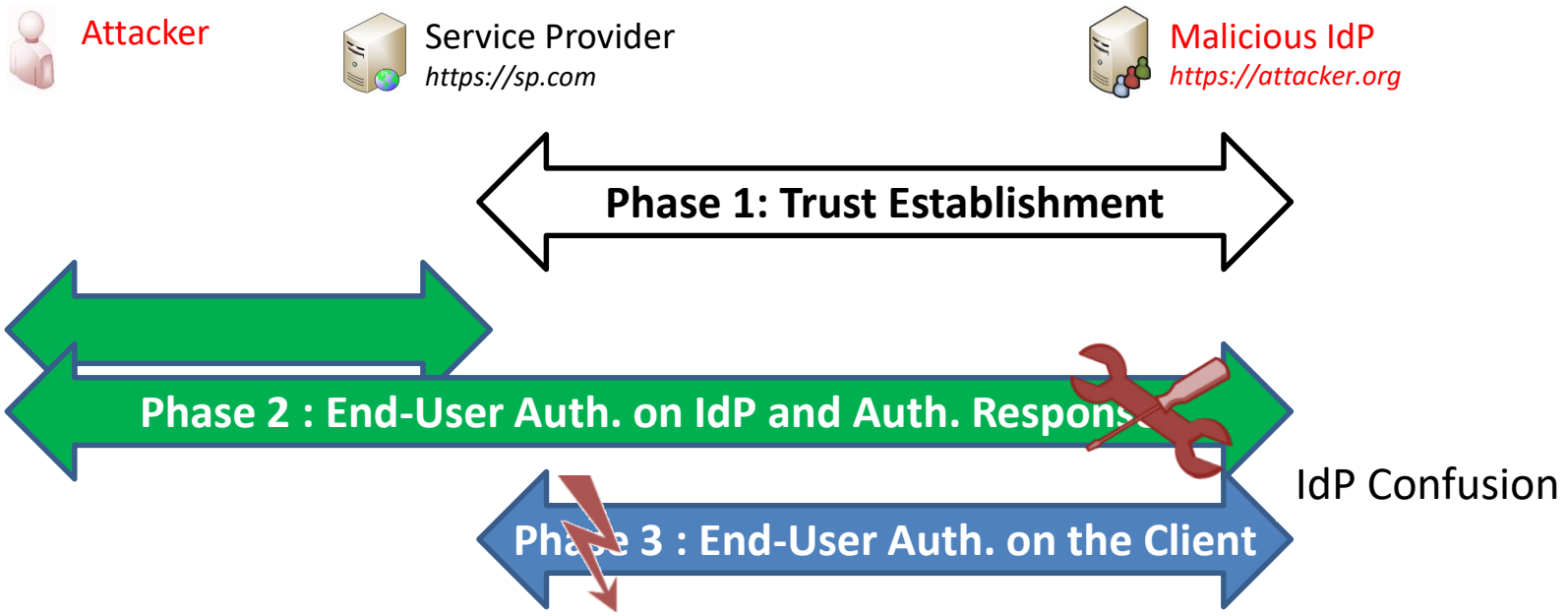


Attack: ID Spoofing



Cross-Phase Attacks on Single Sign-On

- Attacker manipulates step(s) in one protocol phase
- Issue appears in different phase



SoK: Single Sign-On Security

Christian Mainka, Vladislav Mladenov, Tobias Wich, Jörg Schwenk (EuroS&P 2017)

	Single-Phase Attacks				Cross-Phase Attacks		
OIDC Client Library	**ID Spoofing**	**Wrong Recipient**	**Replay**	**Signature Bypass**	**Issuer Confusion**	**IdP Confusion**	**Malicious Endpoints**
mod_auth_openidc	✓	✓	✓	Vuln.	✓	Vuln.	Vuln.
MITREid Connect	✓	✓	✓	✓	✓	Vuln.	Vuln.
oidc-client	Vuln.	Vuln.	Vuln.	✓	Vuln.	Vuln.	Vuln.
phpOIDC	Vuln.	Vuln.	Vuln.	Vuln.	Vuln.	Vuln.	Vuln.
DrupalOpenIDConnect	Vuln.	Vuln.	Vuln.	Vuln.	Vuln.	Vuln.	Vuln.
pyoidc	Vuln.	Vuln.	Vuln.	Vuln.	✓	Vuln.	Vuln.
Ruby OpenIDConnect	✓	✓	✓	✓	✓	Vuln.	Vuln.
Apache Oltu	✓	✓	Vuln.	Vuln.	✓	Vuln.	Vuln.
Total	**4/8**	**4/8**	**5/8**	**5/8**	**3/8**	**8/8**	**8/8**

Implementation Flaw: 6/8

Specification Flaw: 8/8

HACKMANIT

THREAT ANALYSIS | TRAINING | PENETRATION TESTS

Dr. Christian Mainka: christian.mainka@hackmanit.de

www.hackmanit.de | @hackmanit