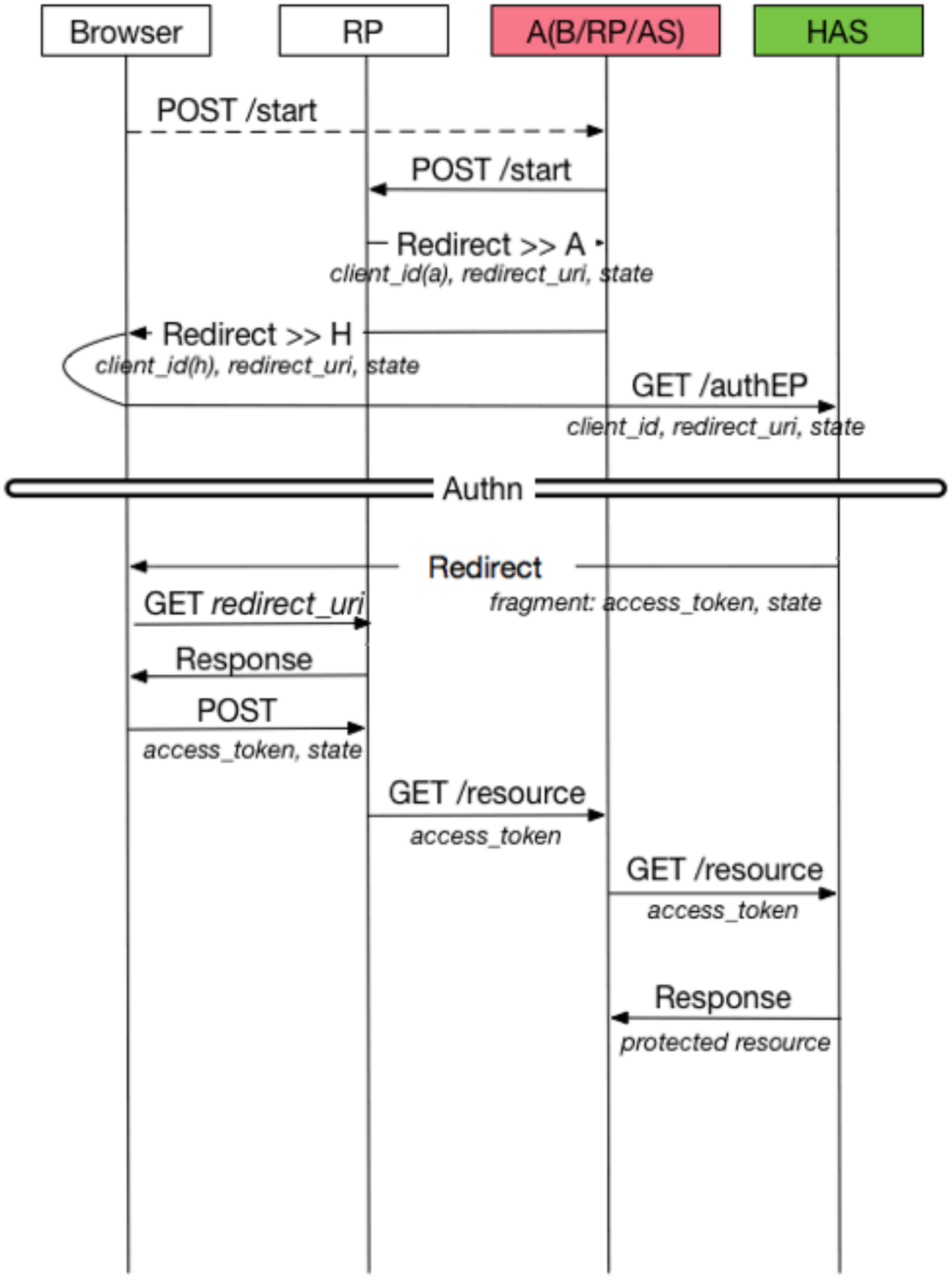
SECURITY THREATS

FETT, KÜSTERS AND SCHMITZ

- http://arxiv.org/abs/1601.01229
- 307 redirect
- IDP Mix-Up


Browser
RP
A(B/RP/AS)
HAS
POST /start
POST /start
Redirect >> A
client_id(a), redirect_uri, state
Redirect >> H
client_id(h), redirect_uri, state
GET /authEP
client_id, redirect_uri, state
Authn
Redirect
fragment: access_token, state
GET redirect_uri
Response
POST
access_token, state
GET /resource
access_token
GET /resource
access_token
Response
protected resource

SPECIFICATION FLAWS

- Malicious endpoints attacks
  - Broken end-user authentication
  - Server side Request Forgery (SSRF)
  - Code injection attacks
  - Denial-of-Sevice (DoS) attacks
- Session Overwriting

IMPLEMENTATION FLAWS

- Client flaws
  - Replay attacks
  - Signature Manipulation
  - Token Recipient Confusion
  - ID Spoofing
  - Key Confusion
  - Sub Claim spoofing within the access token
- Identity Provider flaws
  - Sub Claim spoofing
  - Redirect URI Manipulation

REPLAY ATTACK

Header: { "alg": "HS256" }

Body: {

"iss": "http://openidConnectProvider.com/",

"sub": ”user1",

"exp": 1444148908,

"iat": 1444148308,

"nonce": "40c6b33b9a2e",

"aud": "http://client.com/",

}

Signature: AF45JF93LKD76D...

SIGNATURE MANIPULATION

<header><body><signature>

TOKEN RECIPIENT CONFUSION

Header: { "alg": "HS256" }

Body: {

"iss": "http://openidConnectProvider.com/",

"sub": ”user1",

"exp": 1444148908,

"iat": 1444148308,

"nonce": "40c6b33b9a2e",

"aud": ”another client",

}

Signature: AF45JF93LKD76D...

ID SPOOFING

- ID = sub : iss
- The combination of sub and iss are the only claims that the Client can rely upon as a stable identifier !

KEY CONFUSION

- Wrong reference
- ’Session overwriting ’

SUB CLAIM SPOOFING

- The sub Claim in the UserInfo Response MUST be verified to exactly match the sub Claim in the ID Token

SUB CLAIM SPOOFING (CLAIMS PARAMETER)

```
{ "id_token":
  { ”sub”: {”value”: ”subOfTheVictim”}}
}
```

REDIRECT URI MANIPULATION

- This URI MUST ***exactly match*** one of the Redirection URI values for the Client pre-registered at the OpenID Provider