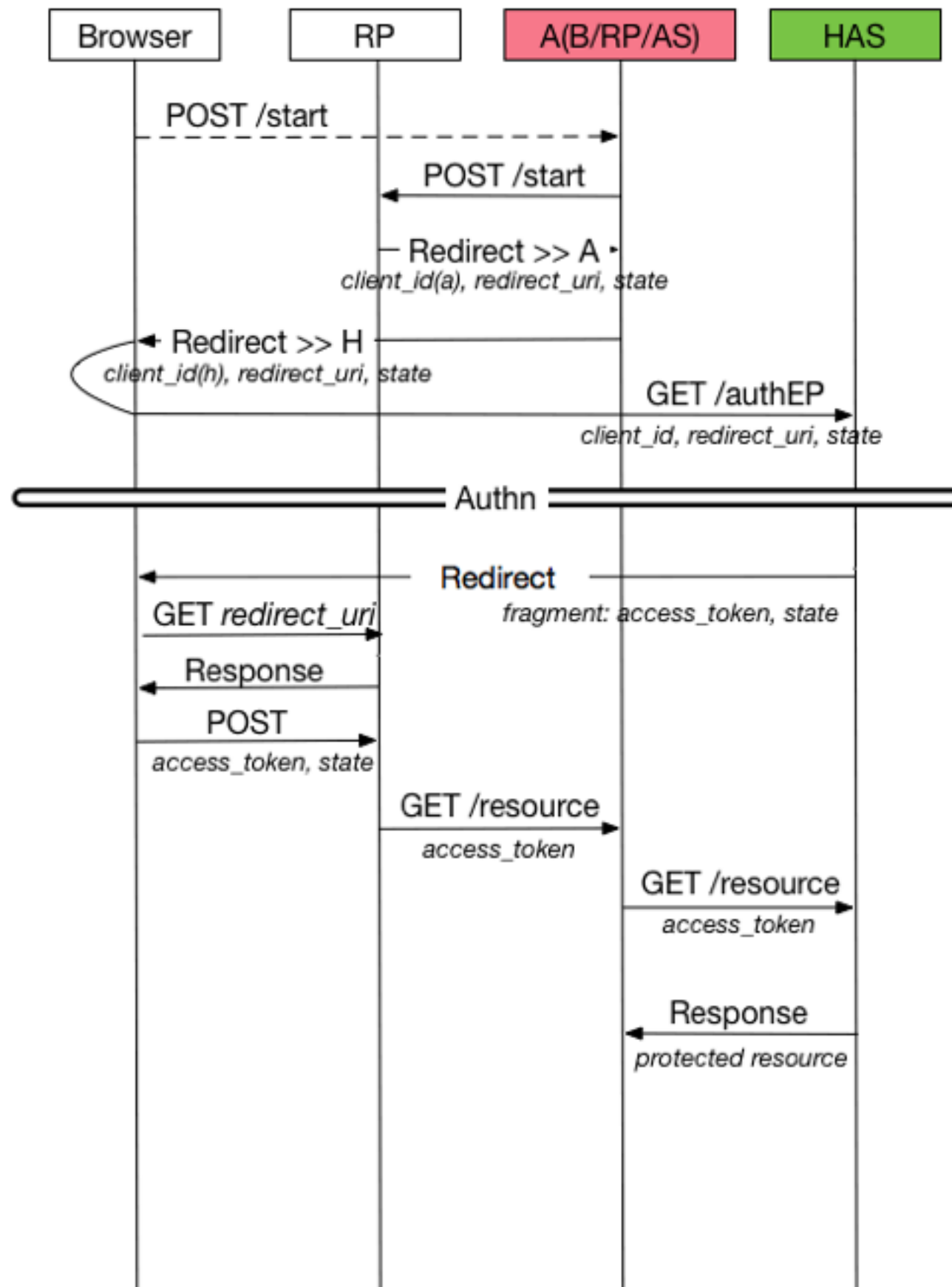


---

# SECURITY THREATS

# MIXUP

- ▶ <http://arxiv.org/abs/1601.01229>
- ▶ The client is confused into using endpoints from several ASes in a authorization flow.
- ▶ Bad implementations
  - ▶ metadata validation (issuer)
  - ▶ id token validation (iss, nonce, aud, iat, exp)
  - ▶ signature validation (exclusion, manipulation, none)
  - ▶ misc (sub, state)



## MALICIOUS ENDPOINTS

► <http://arxiv.org/abs/1508.04324v2/>

issuer:	http://malicious.com
regEndp:	https://honestOP.com/register
authEndp:	https://login.honestOP.com/
tokenEndp:	http://malicious.com
userInfoEndp:	http://malicious.com