RUHR-UNIVERSITÄT BOCHUM

RUB

Wie sicher ist Single Sign-on? Angriffsszenarien für Identity Provider

Vladislav Mladenov, Andreas Mayer, Marcus Niemietz, Jörg Schwenk

Wie sicher ist Single Sign-on? Angriffsszenarien für Identity Provider

Motivation

User

Username/Password 1

Username/Password 2

Username/Password 3

Username/Password 4

http://www.salesforce.com

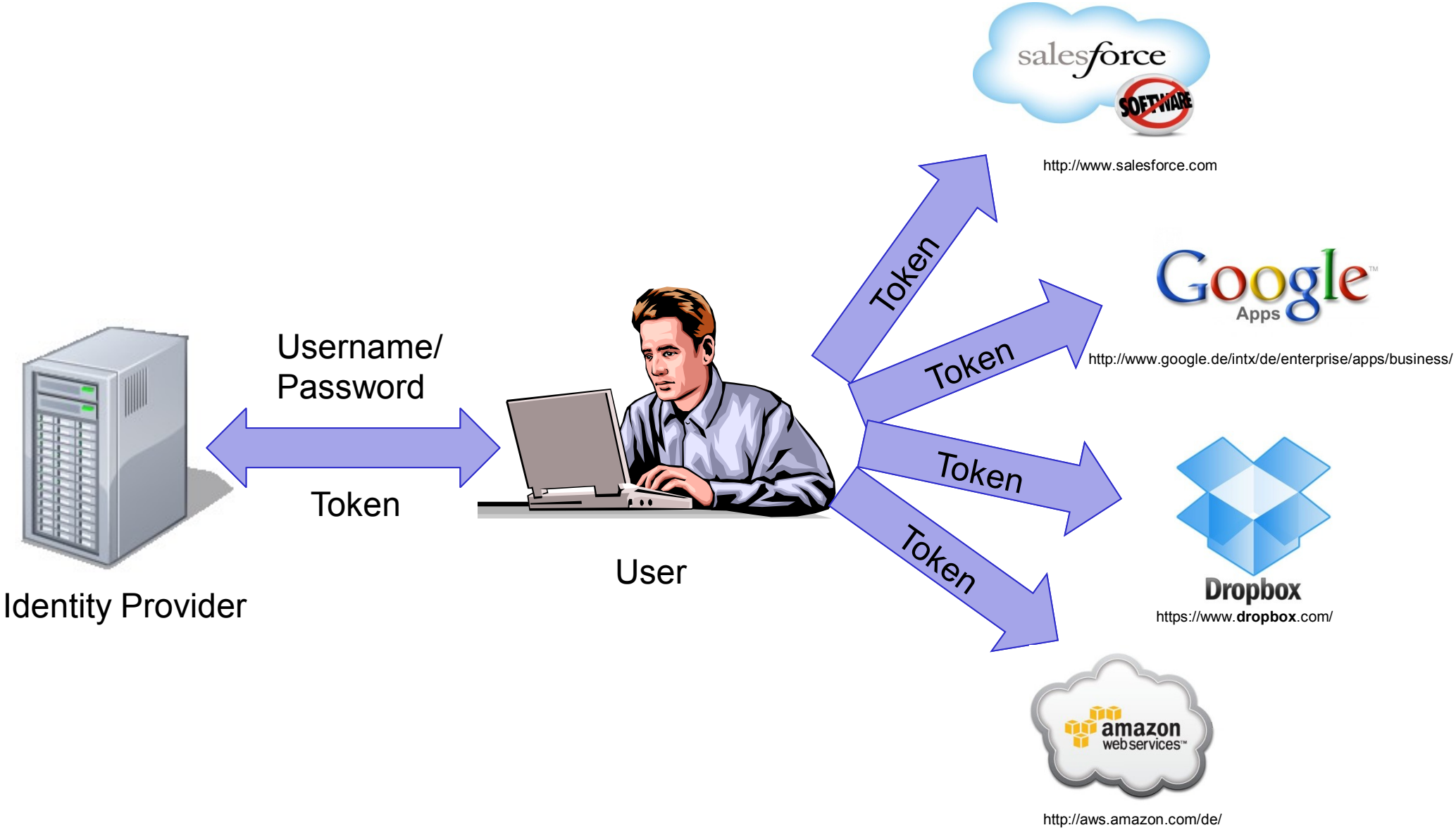
http://www.google.de/intx/de/enterprise/apps/business/

https://www.**dropbox**.com/

http://aws.amazon.com/de/

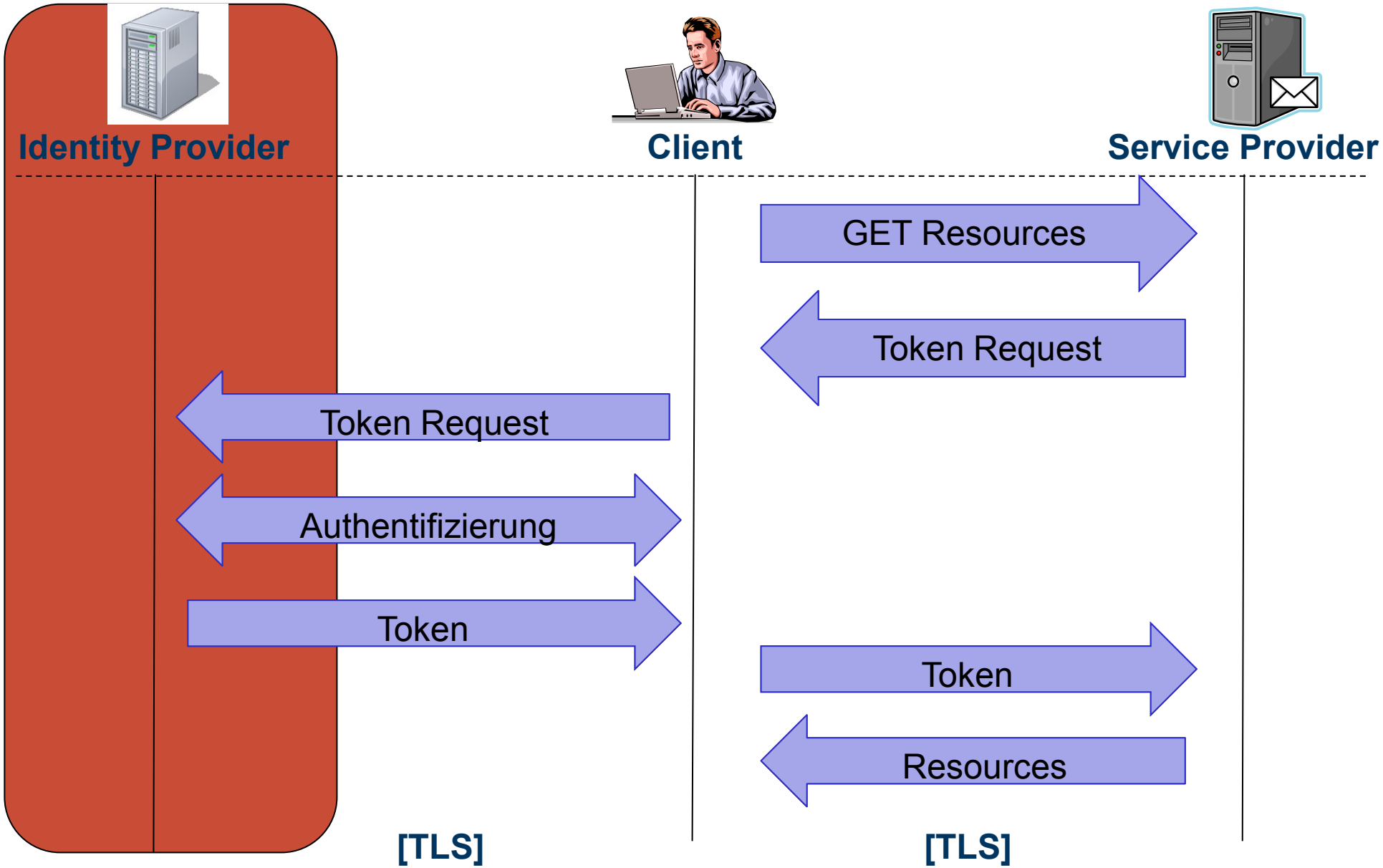
Wie sicher ist Single Sign-on? Angriffsszenarien für Identity Provider

Motivation



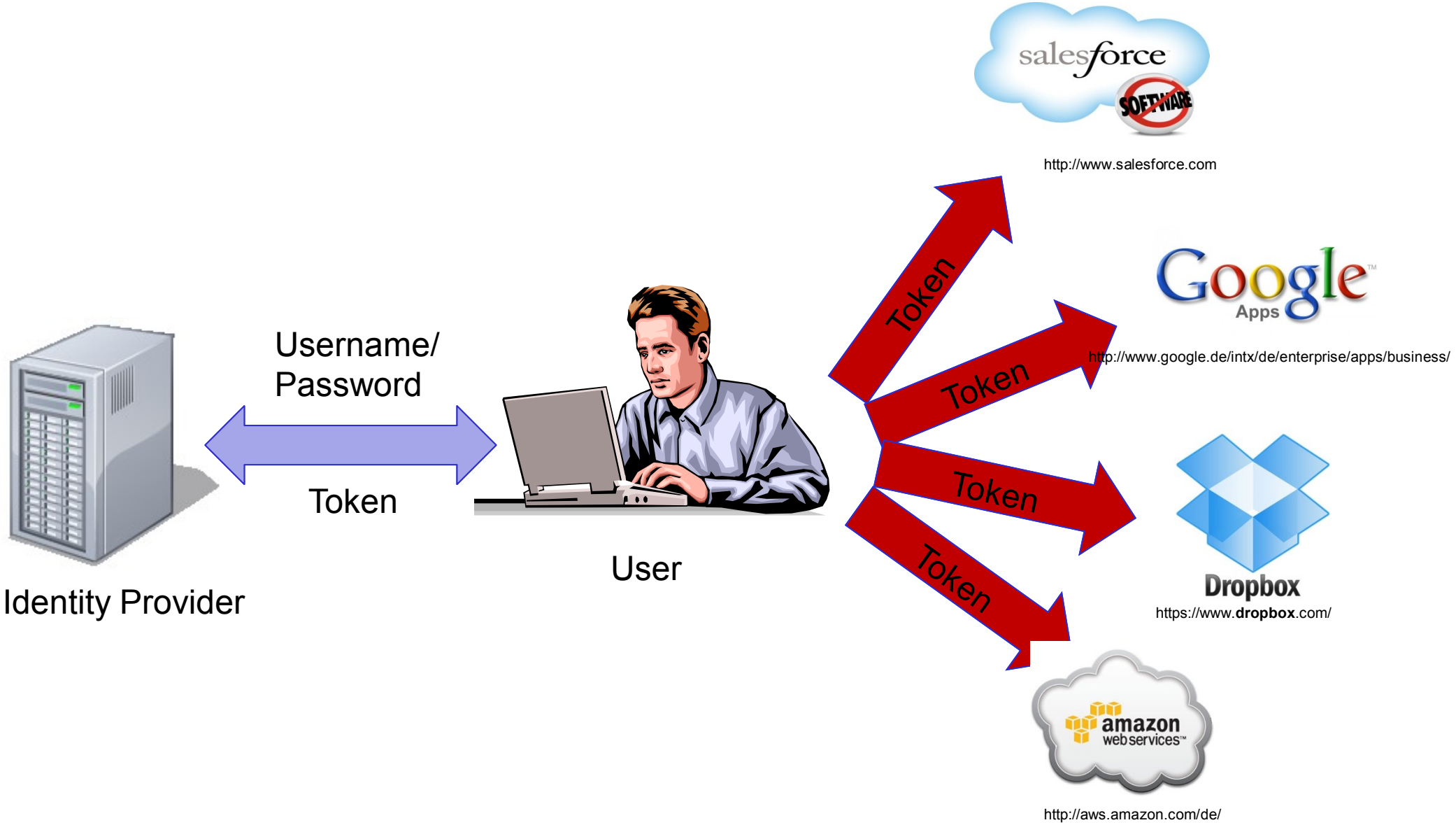
Wie sicher ist Single Sign-on? Angriffsszenarien für Identity Provider

Angriffe auf Identity Provider



Wie sicher ist Single Sign-on? Angriffsszenarien für Identity Provider

Angriffe auf Identity Provider



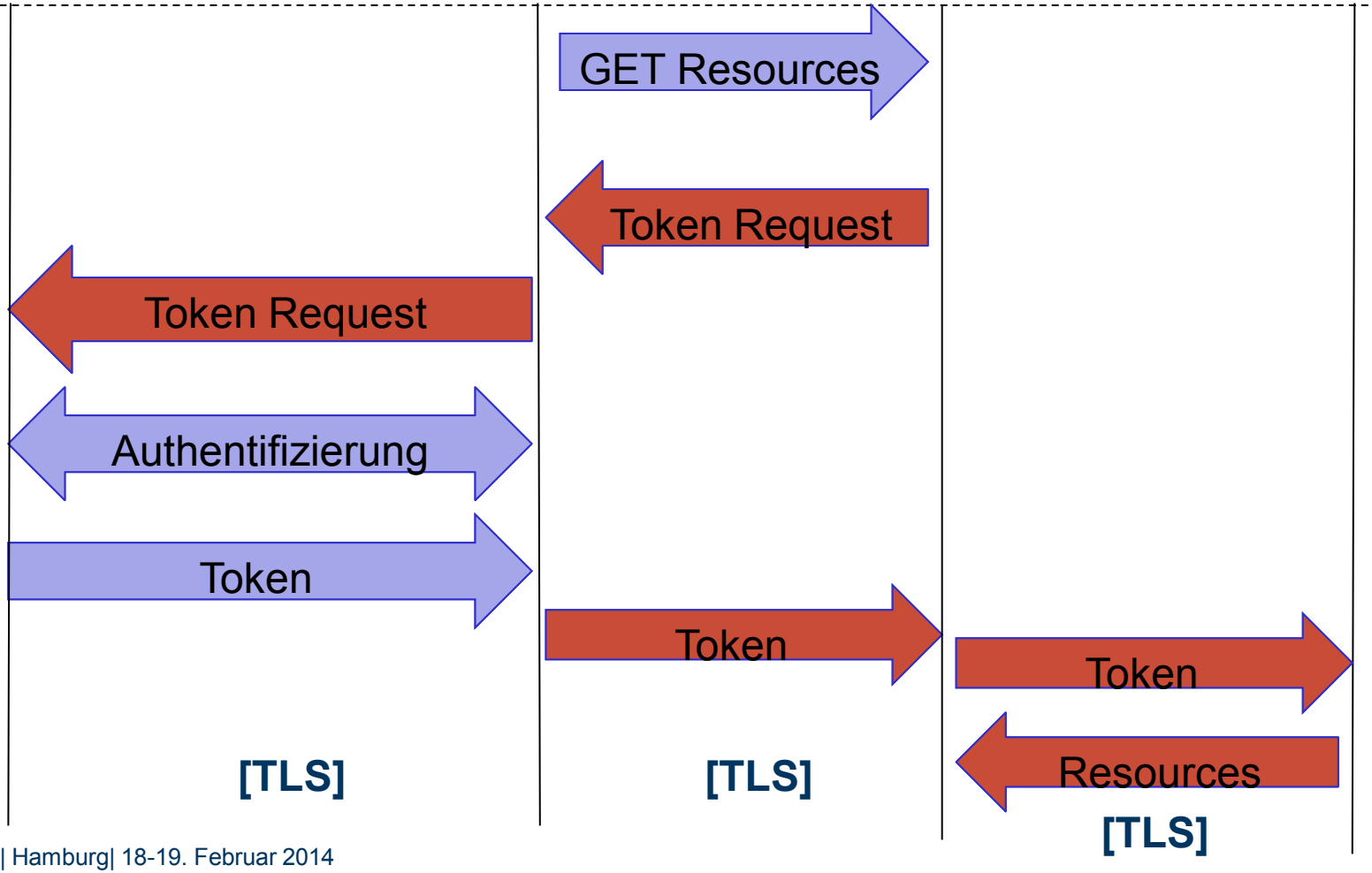
Wie sicher ist Single Sign-on? Angriffsszenarien für Identity Provider

Angriffe auf den Identity Provider

SAML-based ACS Spoofing




Identity Provider | **Client** | **Attacker** | **Service Provider**



Wie sicher ist Single Sign-on? Angriffsszenarien für Identity Provider

Ergebnisse der Untersuchung

SSO System	ACS Spoofing	Cookie theft
Okta	-	✓
OneLogin	✓	✓
SSOCircle	✓	✓
WSO2 IS	✓	-
Cloudseal	-	✓
Guanxi	✓	-

- Vier untersuchte Identity Provider
  - SAML-based ACS Spoofing
  - Cookie Diebstahl via XSS, CSRF, Clickjacking

- Sämtliche Service Provider sind von den Schwachstellen betroffen, unter anderem Google, Salesforce, RightScale usw.