EsPReSSO
oder eine Erfrischung auf der Suche nach Single Sign-On

Vladislav Mladenov,
Tim Guenther,
Christian Mainka,

Horst-Görtz Institut für IT-Sicherheit, Ruhr-Universität Bochum

Single Sign-On

Service Provider 1

Service Provider 2

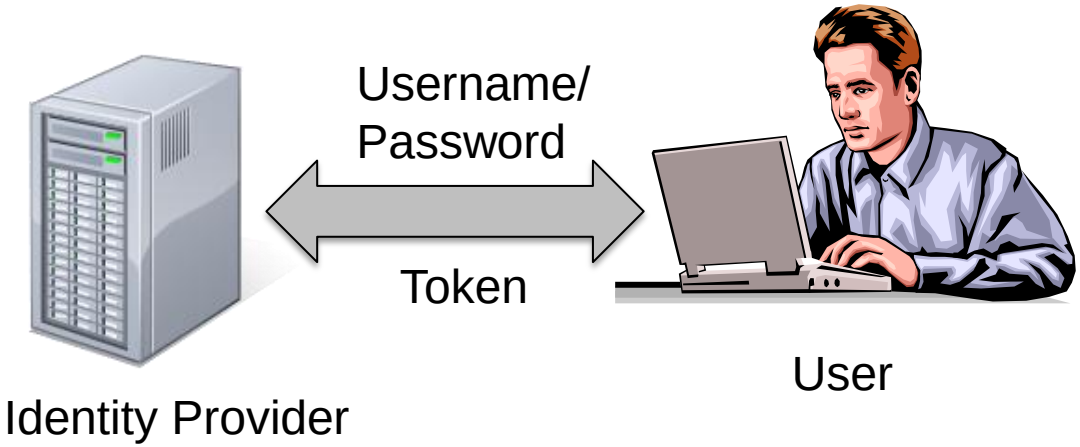
User

Service Provider 3

Service Provider 4

Service Provider 5

Single Sign-On



Service Provider 1

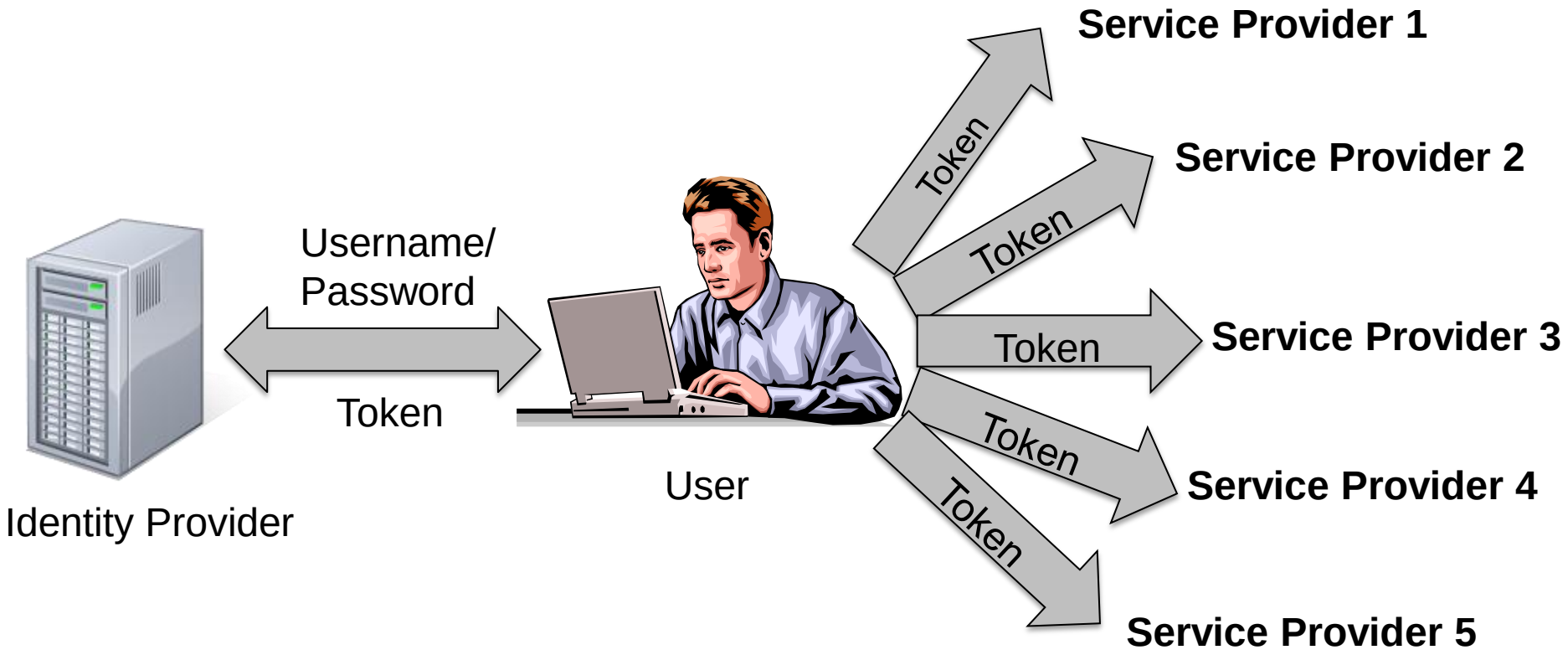
Service Provider 2

Service Provider 3

Service Provider 4

Service Provider 5

Single Sign-On



Analyzing SSO: Protocols

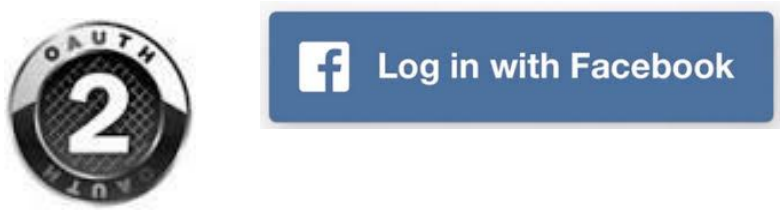
- SAML 2.0

Analyzing SSO: Protocols

- SAML 2.0
- OpenID

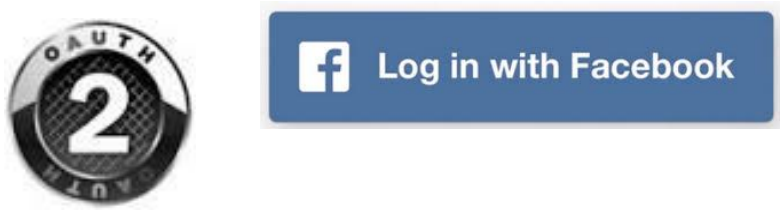
Analyzing SSO: Protocols

- SAML 2.0
- OpenID
- OAuth 2.0
  - MS Account
  - Facebook Connect



Analyzing SSO: Protocols

- SAML 2.0
- OpenID
- OAuth 2.0
  - MS Account
  - Facebook Connect
- OpenID Connect 1.0



Analyzing SSO: Protocols

- SAML 2.0
- OpenID
- OAuth 2.0
  - MS Account
  - Facebook Connect
- OpenID Connect 1.0
- BrowserID

Analyzing SSO: Protocols

- SAML 2.0
- OpenID
- OAuth 2.0
  - MS Account
  - Facebook Co
- OpenID Conn
- BrowserID

Analyzing SSO: Automated Analysis

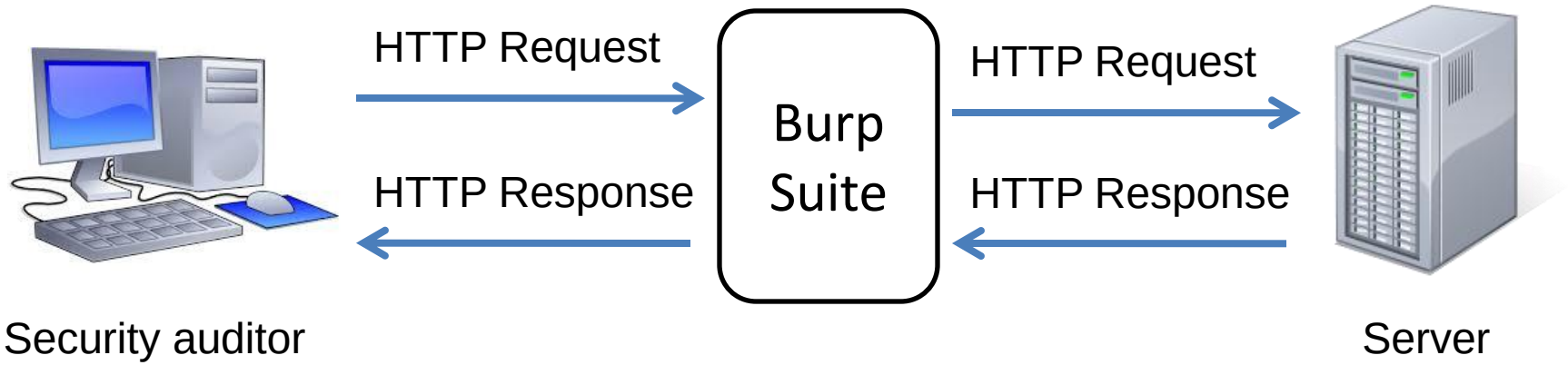
- Automated Analysis is insufficient
  - Existing tools analyze only one SSO protocol or small subset of exisiting attacks
  - Small deviations in the messages lead to false results
  - Only known attacks are detected
  - Extending the tools is insufficient or not possible
  - Changes in the specification are not implemented

Analyzing SSO: Automated Analysis

- Automated Analysis is insufficient
  - Existing tools analyze only one SSO protocol or small subset of exisiting attacks
  - Small deviations in the messages lead to false results
  - Only known attacks are detected
  - Extending the tools is insufficient or not possible
  - Changes in the specification are not implemented
- Security report: “No issues found”
  - There are no security issues?
  - The tool did not find any security issues?

Burp Suite

- Setup: Proxy HTTP Messages



DEMO

Any Questions?

EsPReSSO:

https://github.com/RUB-NDS/BurpSSOExtension