With Great Power Comes Great Pwnage

Yverdon, November 3rd 2016
roland.bischofberger@compass-security.com
emanuel.duss@compass-security.com

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

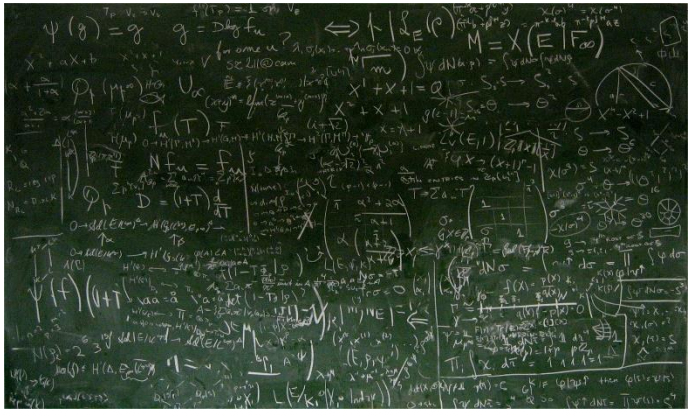
Hello

- Emanuel Duss
- Roland Bischofberger

- Security Analysts at Compass Security Schweiz

Agenda

- Introduction to SAML
- Use-Cases
- Protocol Details



- SAML Attacks
- Demo
- Remediation

WEB

Security

Crossdomain

Assertion

Single Sign-On

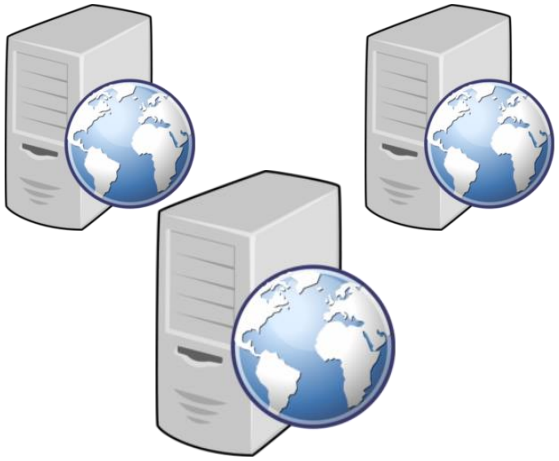
Markup

Such wow!

Language

Introduction: Components

Client / User
Entity that wants to assert a particular identity



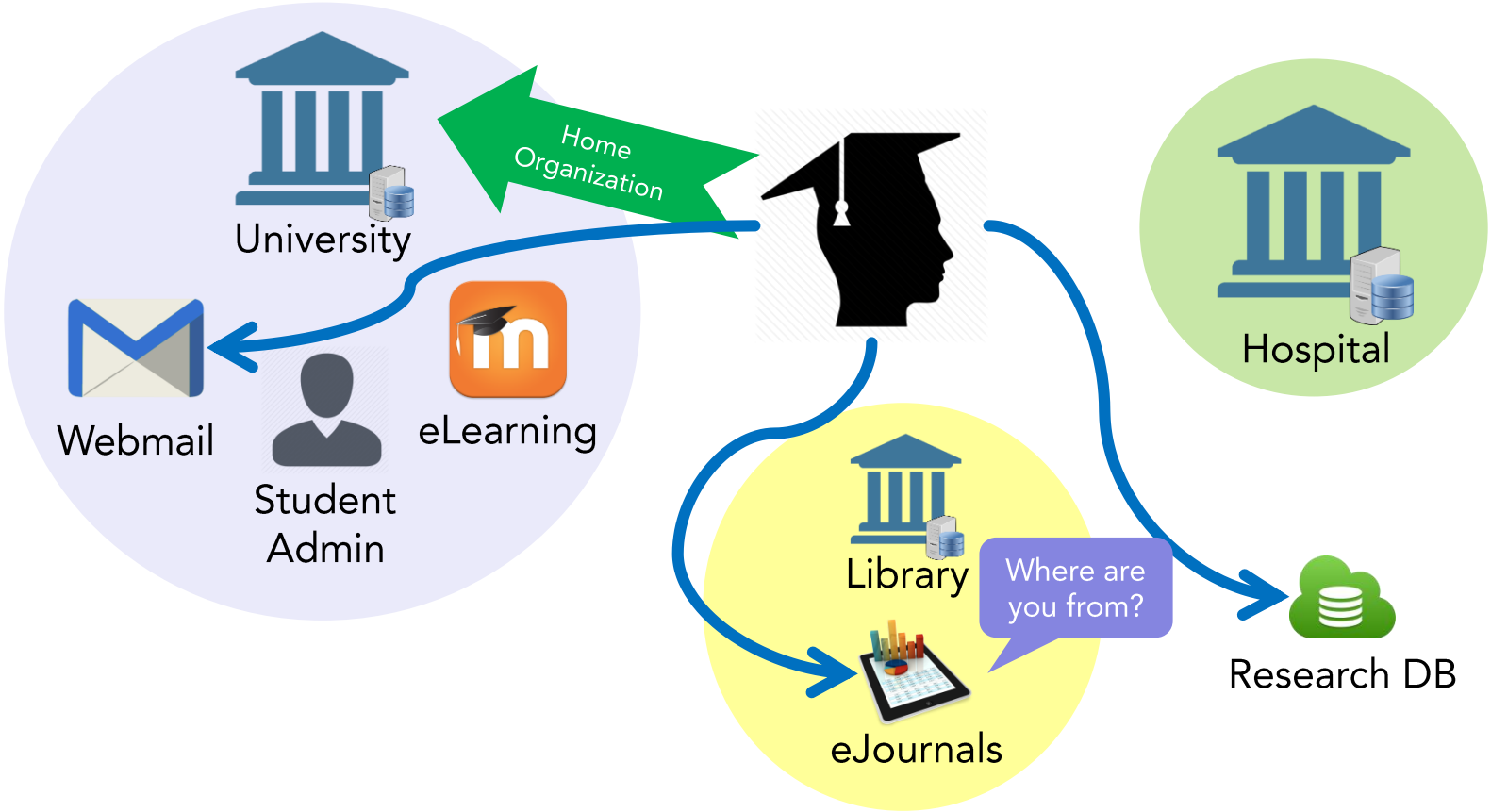
Identity Provider (IdP)
- Checks the identity of subjects
- Issues SAML assertions
- Provides the result to SPs

Service Providers (SP)
- Provides services to subjects
- Trusts the identification from the IdP based on the assertions it receives

USE-CASES

Use-Case: SWITCHaai

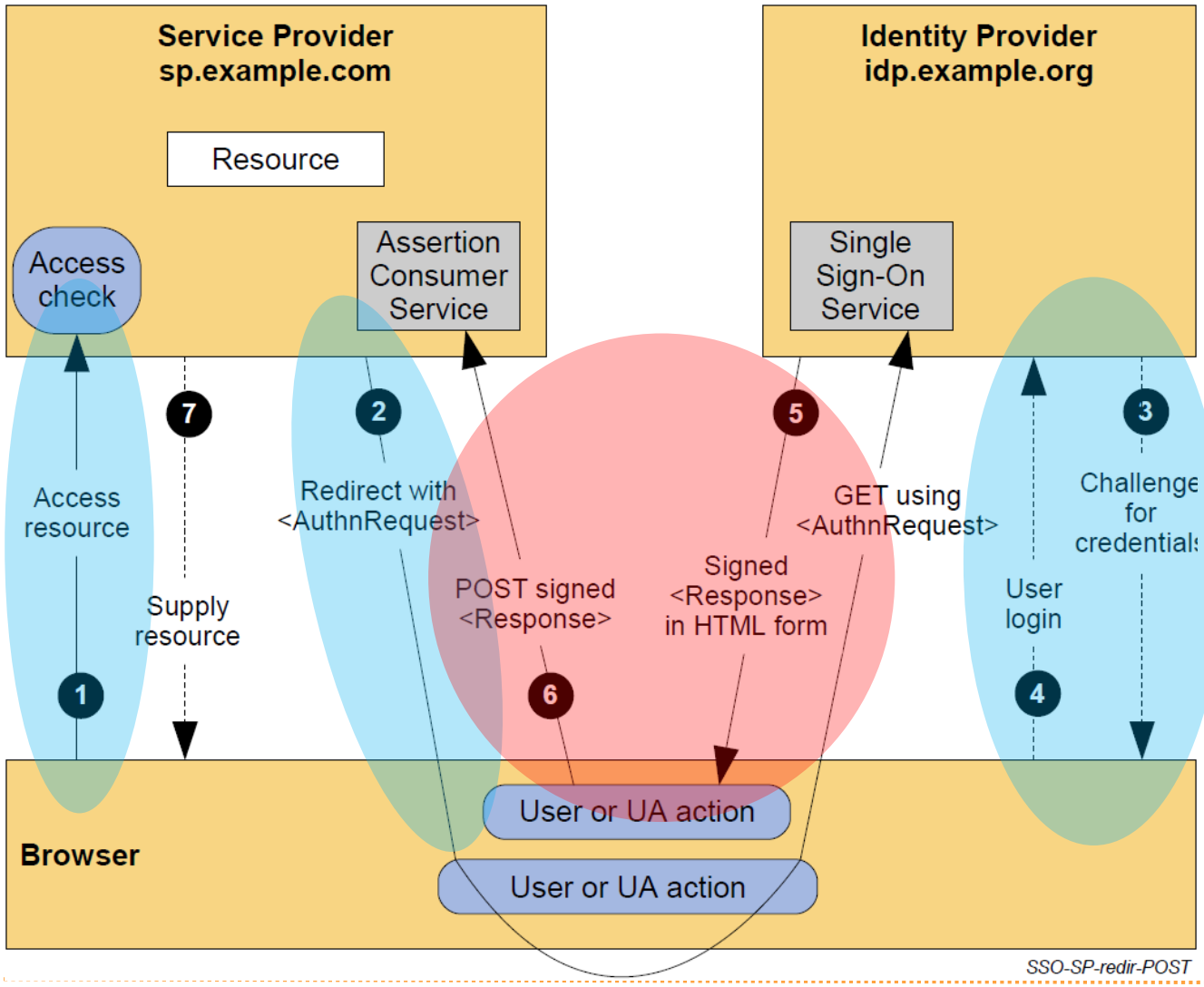
SWITCH



SAML 2.0 FUNDAMENTALS

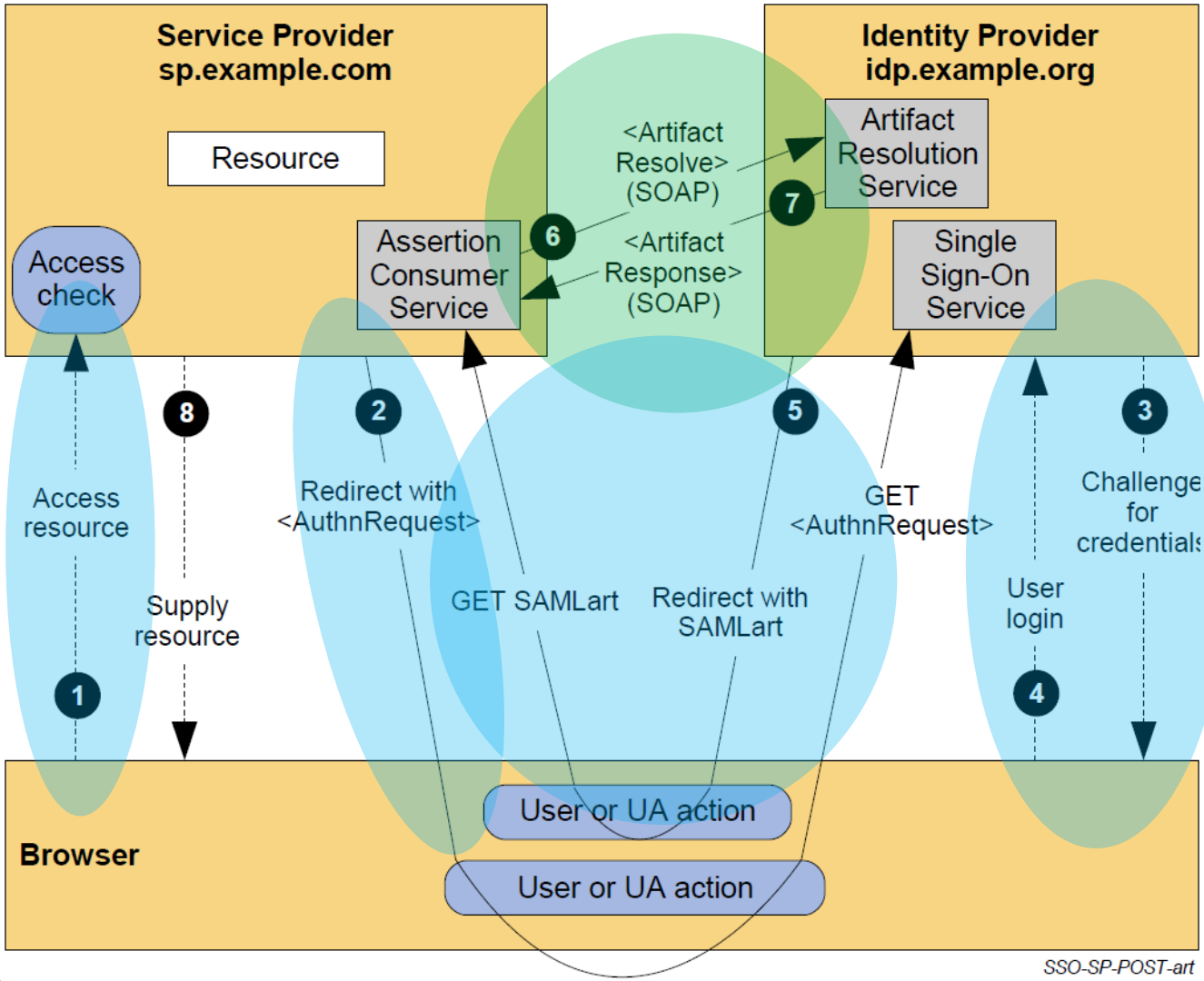
Web Browser SSO Profile

SP-Initiated SSO with Redirect and POST Bindings

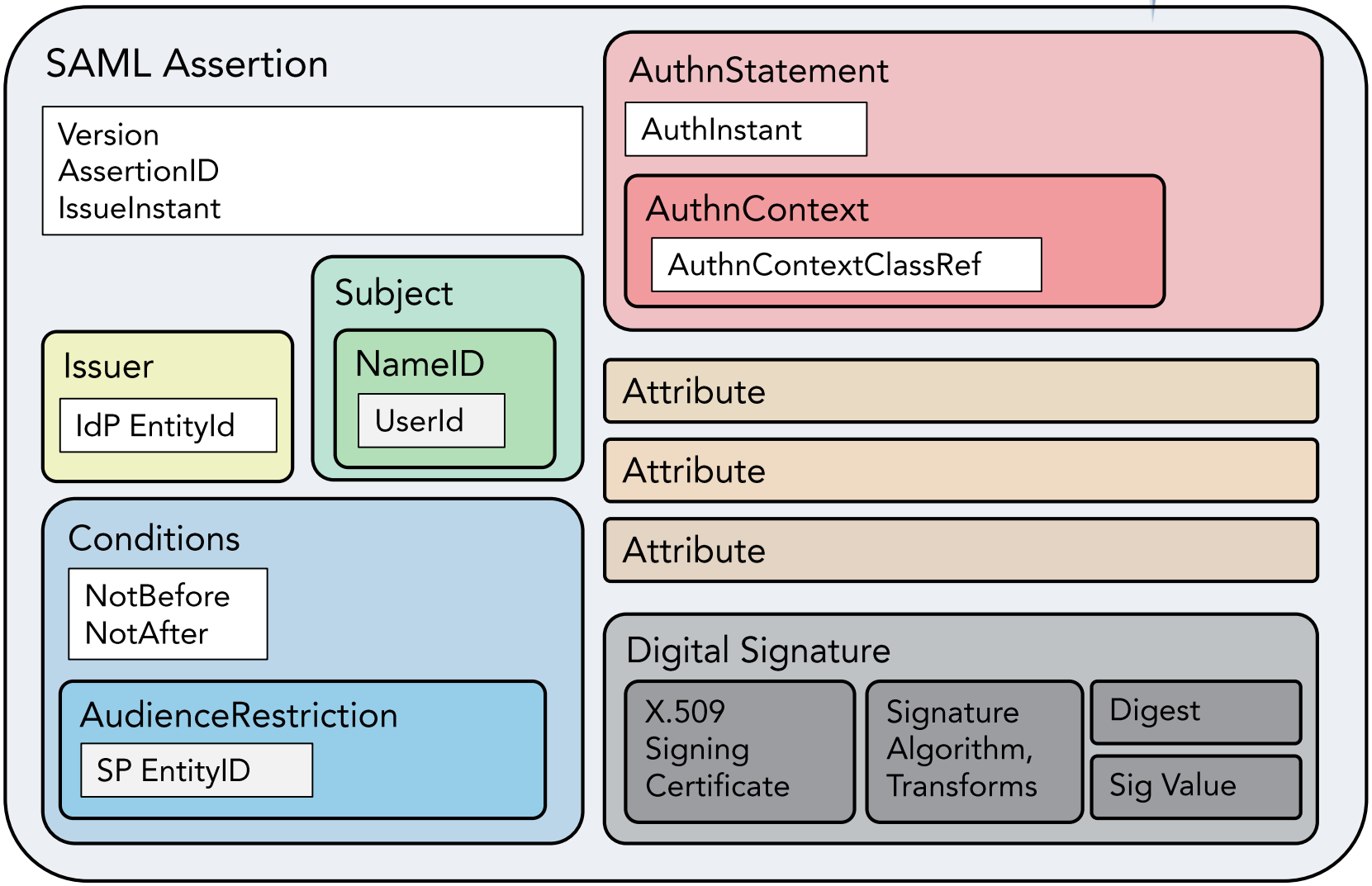


Web Browser SSO Profile (Artifact)

SP-Initiated SSO with POST/Artifact Bindings



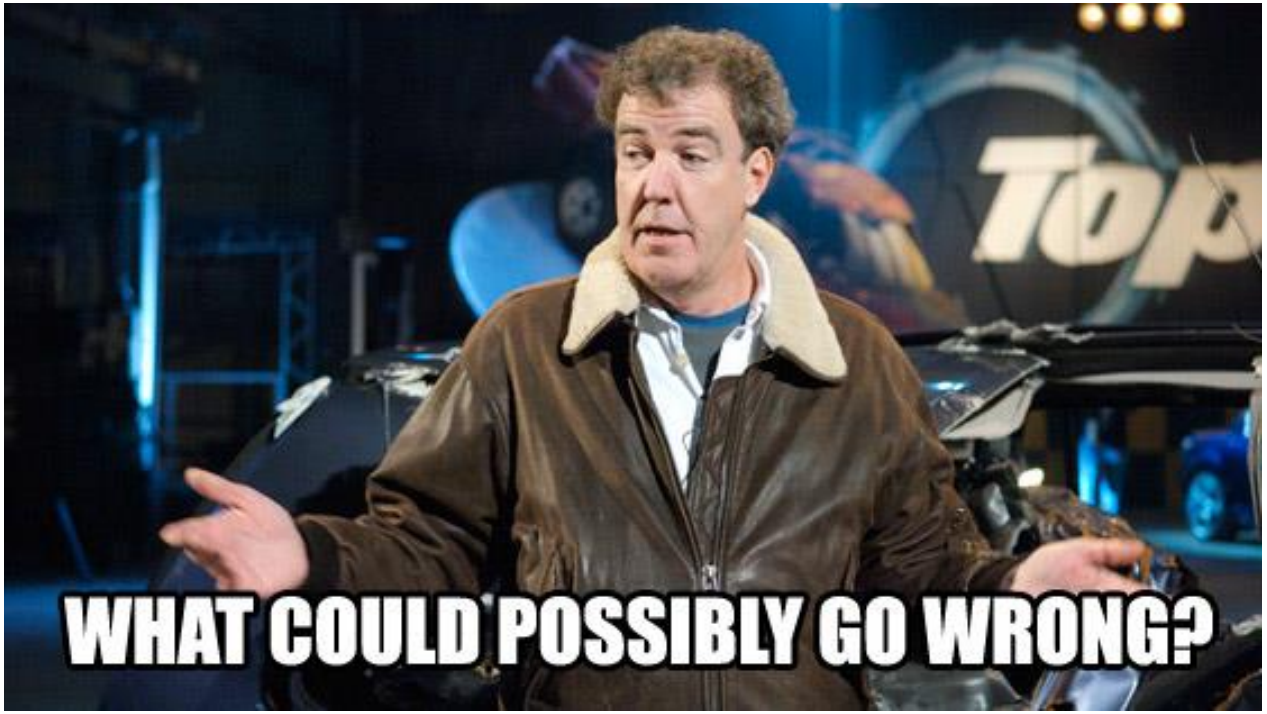
Security Assertion



SAML ATTACKS

Technologies

- SAML
- XML Signatures
- X.509 Certificates



Security is hard

about

geocreepy

HOME | ARCHIVES | CATEGORIES | TAGS | ATOM

The road to hell is paved with SAML Assertions

Posted on Τετ 27 Απρίλιος 2016 in bounty

TL;DR

A vulnerability in Microsoft Office 365 SAML Service Provider implementation allowed for cross domain authentication bypass affecting **all** federated domains. An attacker exploiting this vulnerability could gain unrestricted access to a victim's Office 365 account, including access to their email, files stored in OneDrive etc.

This vulnerability was jointly discovered by Klemen Bratec from Šola prihodnosti Maribor, and Ioannis Kakavas from Greek Research and Technology Network and this blog post is cross-posted here and on Klemen's blog.

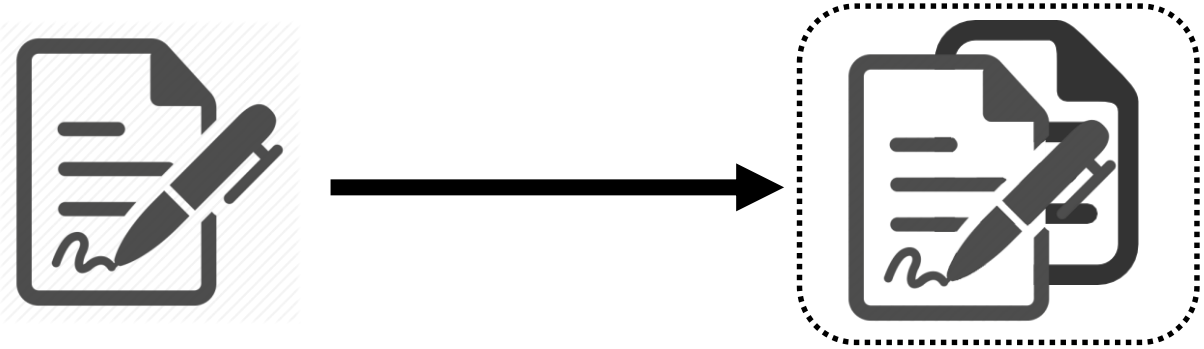
Microsoft fixed the vulnerability within **7 hours** of our report and handled the disclosure process admirably.

http://www.economyofmechanism.com/office365-authbypass.html

SAML Attacks - XML

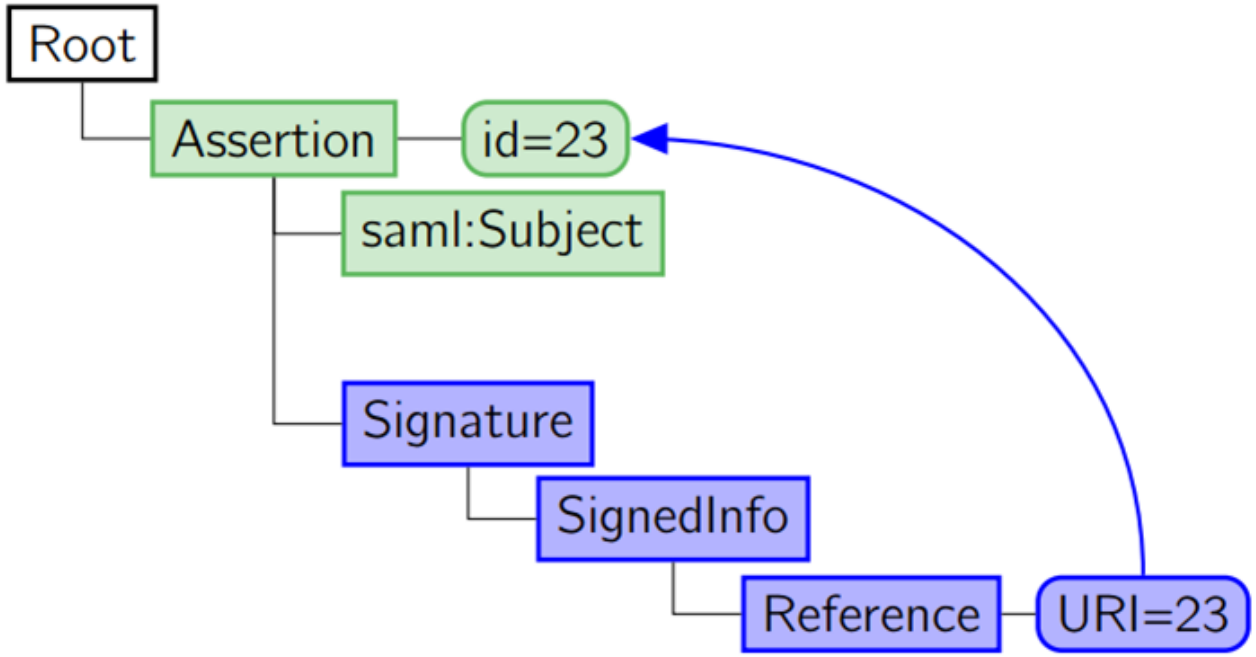
- Signature Exclusion (simply delete Signature)

- XML Signature Wrapping
  - Paper «On Breaking SAML: Be Whoever You Want to Be», 2012



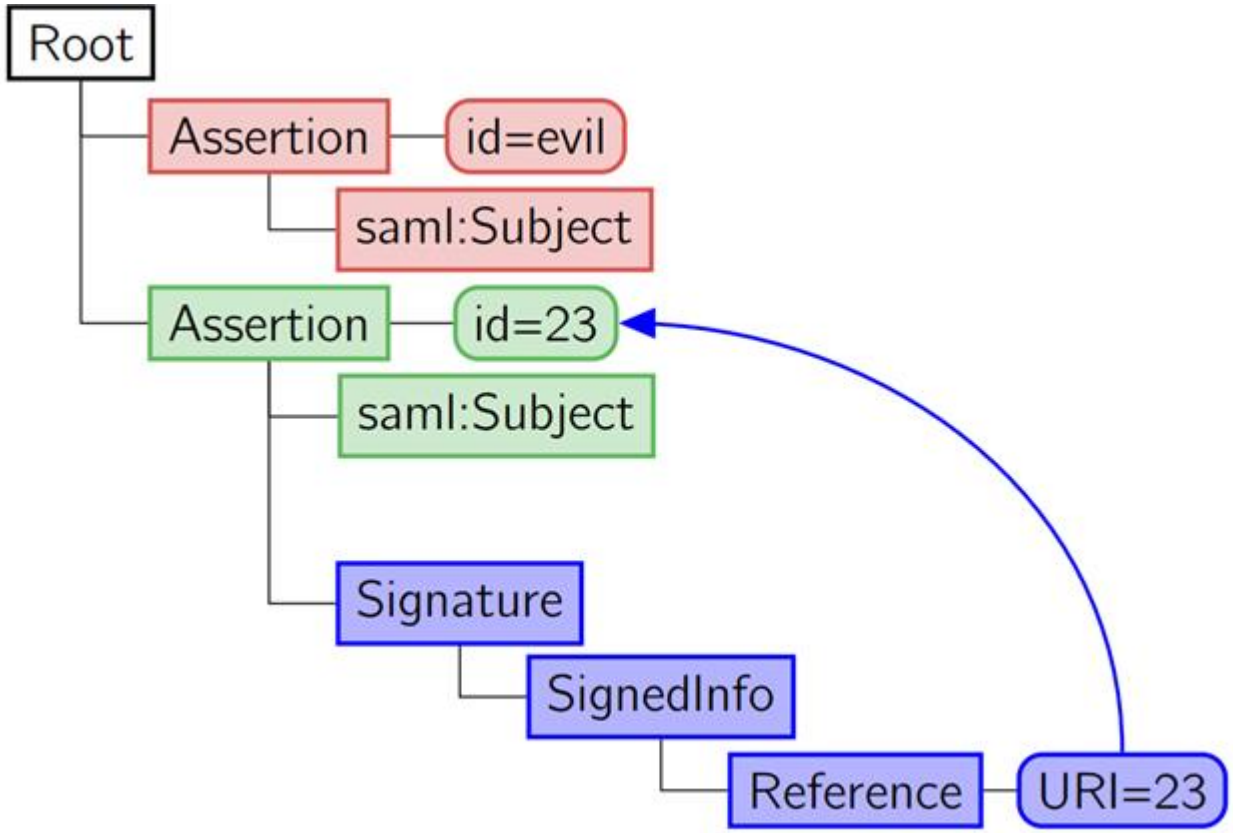
SAML Attacks - XML

- Normal Message



SAML Attacks - XML

- Manipulated Message (XSW)



SAML Attacks – Certificate Tampering

Precondition: Certificate is embedded in the message

- Official certificate
- «clone» a certificate, generate new key material
- Use a certificate signed by other official CA
- Use a revoked / expired certificate

Demo Exploit

Found in June 2015 by Compass Security

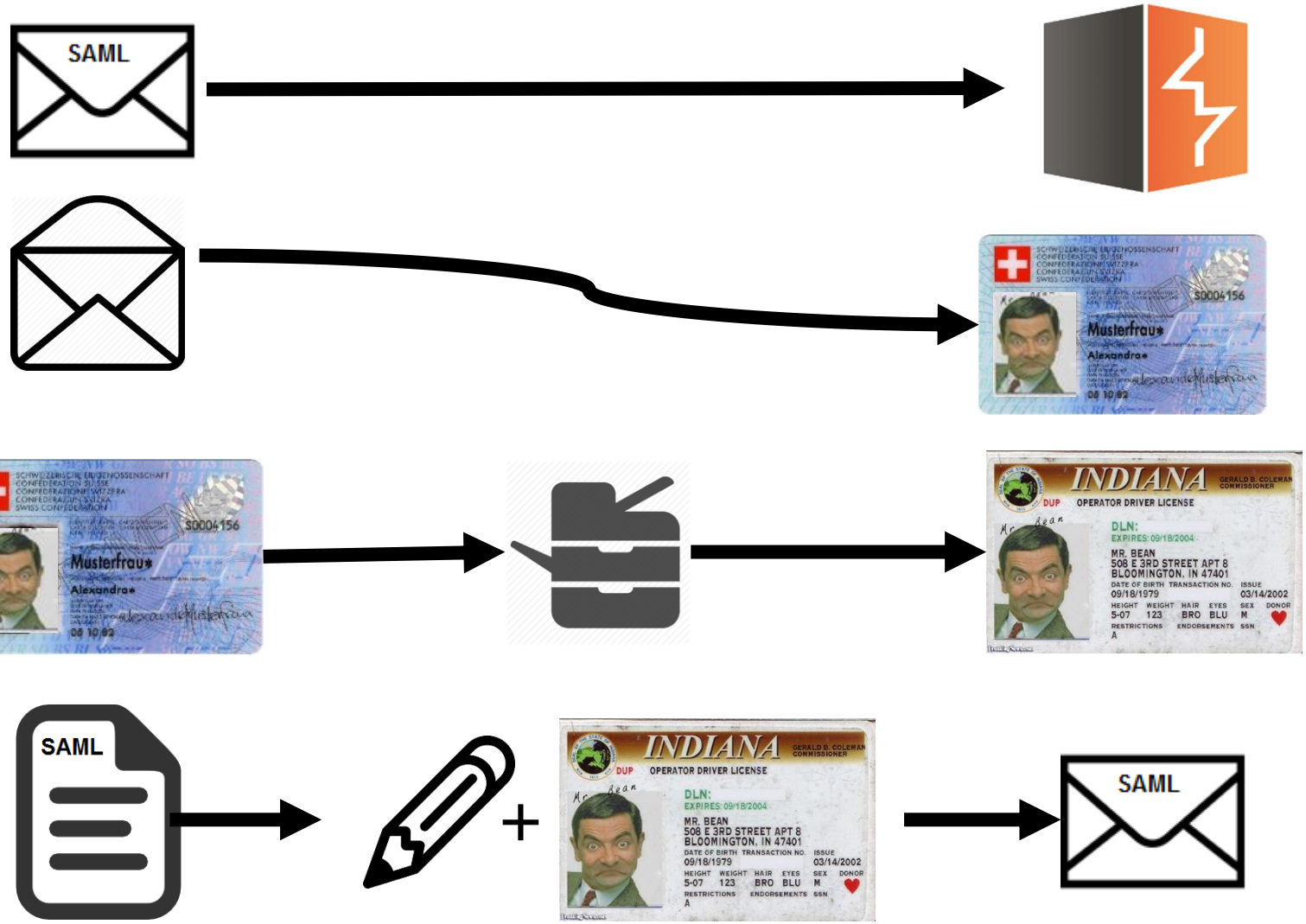
Using SAML POST-Binding

Validated the signature with the embedded certificate

Embedded certificate not correctly compared to local one (IdP certificate)

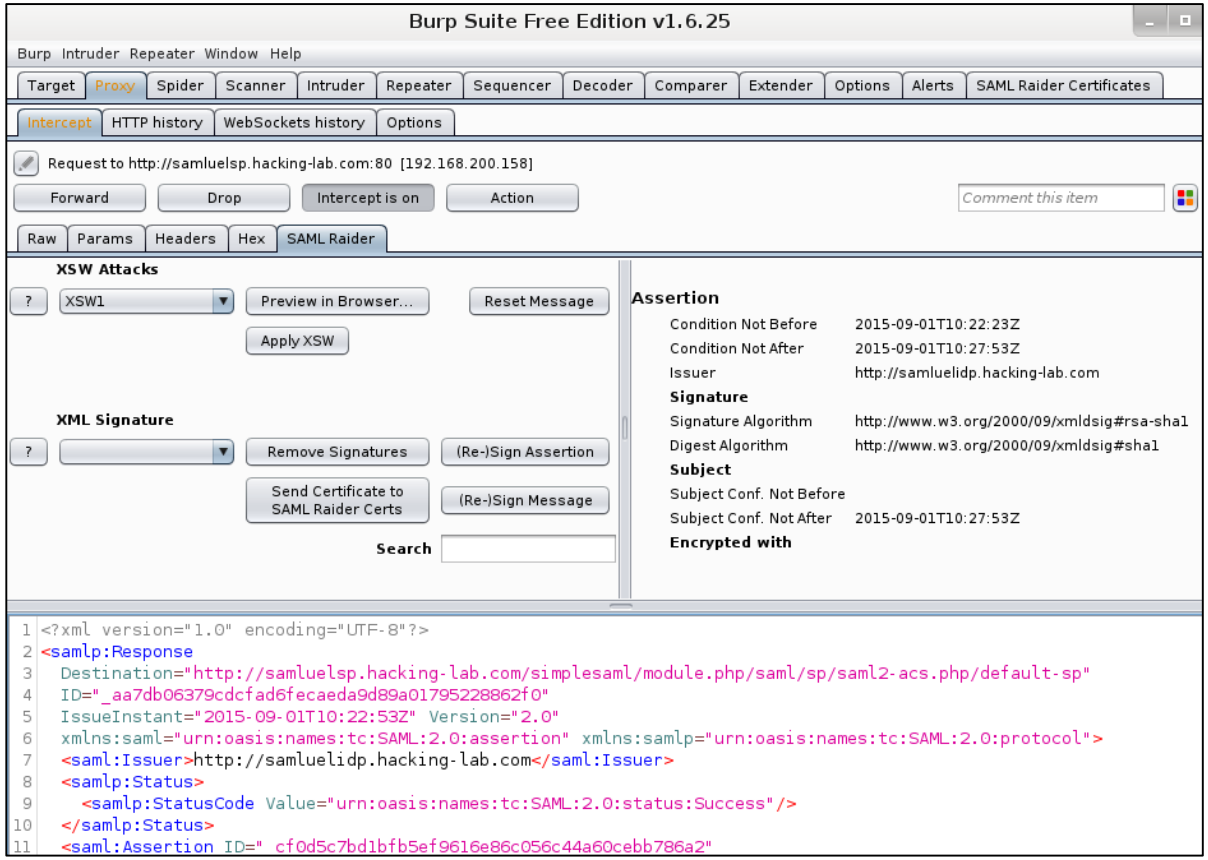
Sign assertion with arbitrary content by using self generated key material

Demo Exploit



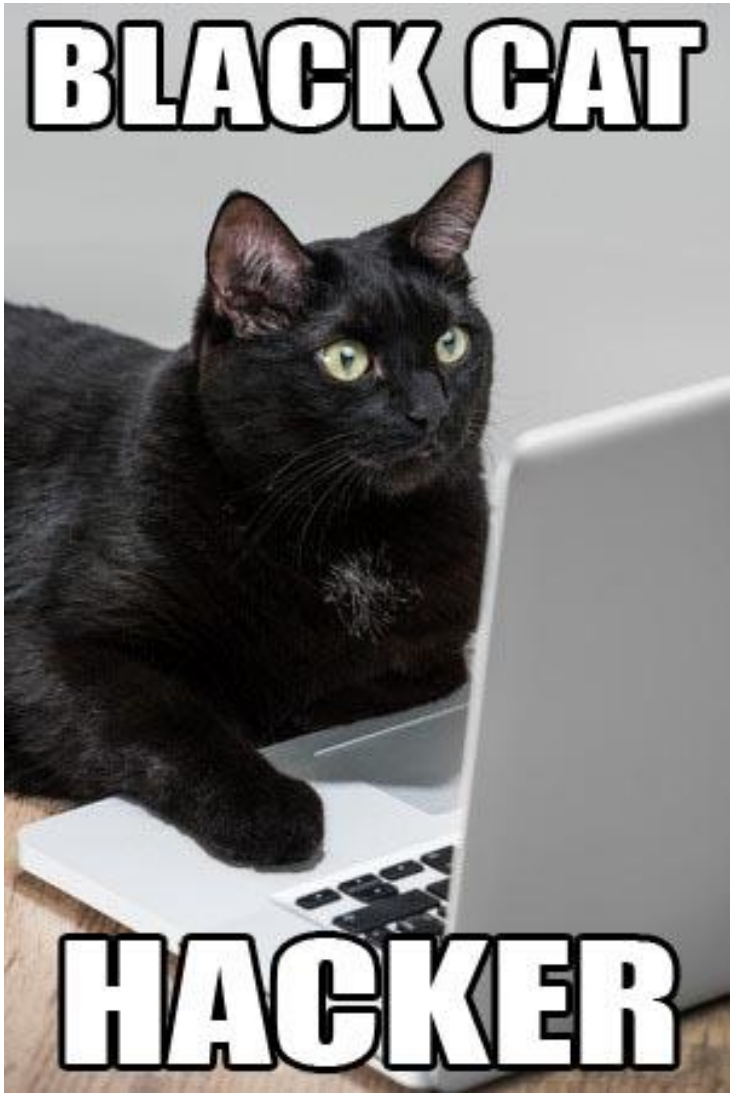
SAMLRaider

SAMLRaider Extension for Burp



https://github.com/SAMLRaider/SAMLRaider

Demo Exploit



REMEDIATIONS

SAML Attacks - Mitigation

- Configuration:
  - Use artifact binding (IdP sends assertion directly to SP)
  - If POST-binding is necessary:
    - Use encrypted messages
- Implementation:
  - Only process signed XML tree (delete other content)
  - Use key material on the SP or IdP and not embedded keys
- Testing: Test your Implementation (with SAMLRaider ;-))

Questions?

Links:

Bachelor Thesis:
https://eprints.hsr.ch/464/

SAMLRaider on Github:
https://github.com/SAMLRaider/SAMLRaider

SAMLRaider in BApp Store:
https://portswigger.net/bappstore/


COMPASS
SECURITY