With Great Power Comes Great Pwnage

Area41 Security Conference
Zürich, June 10th 2016
antoine.neuenschwander@compass-security.com
roland.bischofberger@compass-security.com
Hello

Roland Bischofberger  
IT Security Analyst  

Compass Security Schweiz AG  
Werkstrasse 20 | Postfach 2038 | CH-8645 Jona  
T: +41 55 214 41 70 | F: +41 55 214 41 61  
roland.bischofberger@compass-security.com

Antoine Neuenschwander  
IT Security Analyst  

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

antoine.neuenschwander@csnc.ch  
T: +41 55 214 41 68  
F: +41 55 214 41 61

www.compass-security.com

© Compass Security Schweiz AG
Agenda

- Introduction to SAML
- Use-Cases
- Protocol Details
- SAML Attacks
- Demo
- Remediation
Introduction: SAML

WEB

Security Assertion Markup Language

Crossdomain

Single Sign-On

Such wow!
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: IG B2B BrokerGate

941 Brokers, 4295 Users

21 Insurers (13 online)
Broker portal as Service Providers
Use-Case: IG B2B BrokerGate

941 Brokers, 4295 Users

21 Insurers (13 online)
Broker portal as Service Providers

SAM L 2.0 IdP

SAML 2.0
IdP
Use-Case: IG B2B BrokerGate

Logins per Month

User Accounts

Jan 13
Mrz 13
Mai 13
Jul 13
Sep 13
Nov 13
Jan 14
Mrz 14
Mai 14
Jul 14
Sep 14
Nov 14
Jan 15
Mrz 15
Mai 15
Jul 15
Sep 15
Nov 15
Use-Case: SWITCHaai

University

Webmail

Student Admin

eLearning

Home Organization

Hospital

Library

Where are you from?

ejournals

Research DB
Use-Case: SWITCHaai

SWITCH

# Home Organizations

Interfederation enabled

© Compass Security Schweiz AG  www.compass-security.com  Slide 11
Use-Case: SWITCHaai

On Average: 52 SAML authentication requests per minute
SAML 2.0 FUNDAMENTALS
SAML – The Overall Picture

**Profiles**
Combinations of assertions, protocols, and bindings to support a defined use case

**Bindings**
Mappings of SAML protocols onto standard messaging and communication protocols

**Protocols**
Requests and responses for obtaining assertions and doing identity management

**Assertions**
Authentication, attribute, and entitlement information

SAML profiles define how the SAML assertions, protocols, and bindings are combined and constrained to provide greater interoperability in particular usage scenarios, e.g. Web Browser SSO Profile

Bindings specify how the various messages can be carried over underlying transport protocols, e.g. HTTP redirect or POST

SAML defines a number of protocol messages, e.g. authentication request, artifact resolution or single logout

With an **Assertion** a IdP confirms to a SP the identity of a subject including the used authentication method
Web Browser SSO Profile

SP-Initiated SSO with Redirect and POST Bindings

1. Access resource
2. Redirect with <AuthnRequest>
3. GET using <AuthnRequest>
4. User login
5. Signed <Response> in HTML form
6. POST signed <Response>
7. Supply resource

Service Provider
sp.example.com

Assertion Consumer Service

Identity Provider
idp.example.org

Resource

Single Sign-On Service

User or UA action

Browser

User or UA action

© Compass Security Schweiz AG  www.compass-security.com
Web Browser SSO Profile (Artifact)

SP-Initiated SSO with POST/Artifact Bindings

1. Supply resource
2. Redirect with <AuthnRequest>
3. Challenge for credential
4. User login
5. Redirect with SAMLart
6. GET SAMLart
7. Artifact Resolution Service
8. Access resource

Service Provider sp.example.com
Identity Provider idp.example.org

Browser
User or UA action
Security Assertion

SAML Assertion

Version
AssertionID
IssueInstant

Issuer
IdP EntityID

Subject
NameID
Userld

Conditions
NotBefore
NotAfter

AudienceRestriction
SP EntityID

AuthnStatement
AuthInstant

AuthnContext
AuthnContextClassRef

Attribute

Digital Signature
X.509 Signing Certificate
Signature Algorithm, Transforms
Digest
Sig Value
XML Signature

1. **Assertion**
2. **c14n**
3. **XML**
4. **sha1**
5. **Digest**
6. **rsa**
7. **Signature**
8. **rsa**
9. **Secure Certificate**
10. **Checkmark**
SAML ATTACKS
SAML Attacks

Technologies

- SAML
- XML Signatures
- X.509 Certificates
The road to hell is paved with SAML Assertions

Posted on Τετ 27 Απριλίου 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.
SAML Attacks - SAML

- Log out other users due to a guessable IDs
- Replay an eavesdropped SAML Message
  - Google for Messages, Stack Overflow
SAML Attacks - XML

- Signature Exclusion (simply delete Signature)

- XML Signature Wrapping
SAML Attacks - XML

✿ Normal Message

```
Root
  Assertion
    id=23
    saml:Subject
      Signature
        SignedInfo
          Reference
            URI=23
```
Manipulated Message (XSW)
SAML Attacks – Certificate Tampering

Precondition: Certificate is embedded in the message

- «clone» a certificate, generate new key material
- Use a certificate signed by other official CA
- Use a revoked certificate
Demo Exploit

Found in June 2015 by Compass Security

using **SAM L POST-Binding**

not matching all attributes of the **X.509 certificate embedded**

in the assertion **against the certificate from the identity provider (IdP)**
Demo Exploit

SAML

STOP

SAML

INTEGRITY

SAML

INTEGRITY
SAMLRaider Extension for Burp

https://github.com/SAMLRaider/SAMLRaider
Demo Exploit

BLACK CAT

HACKER
REMEDIATIONS
SAML Attacks - Mitigation

- **Configuration:**
  - Use artifact binding (no content on client)
  - 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
Questions?

Credits and Links:

Emanuel Duss, Bachelor Thesis and SAML Raider

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

SAML Raider on Github:
https://github.com/SAML Raider/SAML Raider