Lab 2.3

LaTeX

Sergey Sheff Semen Strebelev

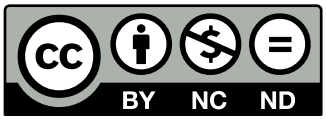
May 1, 2024

UNIVERSITAT DE BARCELONA

Institute of Informatics and Cybernetics
Samara University

Published by: Igor Gofman
Template by: Mario Vilar
AMS Classification (2020): 01A75, 00B50.

Samara, on May 1, 2024



Contents

Part I
Theory

I

Discovery of a Security Flaw in SAML 2.0 Web Browser SSO Profile Protocol

1.1 Abstract

Single-Sign-On (SSO) protocols enable companies to establish a federated environment in which clients sign in the system once and yet are able to access services offered by different companies. The scheme of SSO operation is shown in the figure 1.1. The OASIS Security Assertion Markup Language (SAML) 2.0 Web Browser SSO Profile is the emerging standard in this context. In this paper we provide formal models of the protocol corresponding to one of the most applied use case scenario (the SP-Initiated SSO with Redirect/POST Bindings) and of a variant of the protocol implemented by Google and currently in use by Google's customers (the SAML-based SSO for Google Applications). We have mechanically analysed these formal models with SATMC, a state-of-the-art model checker for security protocols. SATMC has revealed a severe security flaw in the protocol used by Google that allows a dishonest service provider to impersonate a user at another service provider. We have also reproduced this attack in an actual deployment of the SAML-based SSO for Google Applications.

1.2 Types of SSO

SSO types are categorized based on where and how they are deployed, the type of credentials they use, and whether they are single sign-on protocols:

1. Intranett or Enterprise SSO (ESSO);
2. Extranet or Multi-domain SSO;
3. Internet or Web SSO;
4. Simple/complex SSO architecture;
5. Complex SSO with a single(multiple) set(s) of credentials;
6. Kerberos authentication Protocol;
7. SAML;
8. OpenID.

1.3

Confidential channelsand laws of identity

We will now revisit the Cameron's law of identity, which is used in the later part of this paper:

- User Control and Consent;
- Minimal Disclosure for a Constrained Use;
- Justifiable Parties;
- Directed Identity;
- Pluralism of Operators and Technologies;
- Human Integration;
- Consistent Experience Across Contexts.

To illustrate the usage of the above constraints let us consider the SAML SSO and its security recommendations in matter of communication channels. Assumption (A1) requires that the message exchanges between C and SP are carried over unilateral SSL/TLS channels. As sumption (A2) imposes that the message from C to IdP is sent over a confidential channel, while the message from IdP to C is sent over a confidential and authentic channel. For each session s, this amounts to including the following constraints in C. Also take a look at the figure 1.2

1.4

SSO protocols: overview and comparison

Let's consider several of the most common SSO protocols and compare their main characteristics. The table Table 1.1 below summarizes some of the most popular SSO protocols and their brief descriptions.
When selecting an SSO protocol, consider your organization's requirements for security, compatibility with existing systems, and usability for users.

1.5

Confidential channels

A channel provides confidentiality if its output is exclusively accessible to given receiver. In our model this amounts to requiring that in every state if a fact, then has exclusive access to the channel. Thus, the condition that channel is confidential to principal can be formalised by the following formulas:

$$F(x) = \int_{-\infty}^{\infty} e^{-\frac{x^2}{2}} \cdot \left(\sum_{n=0}^{\infty} \frac{(2n)!}{n! \cdot 2^n} \cdot \sqrt{2\pi} \cdot x^n \right) dx$$

where

$F(x)$ — cumulative distribution function of a normal distribution,

e — base of the natural logarithm,

x — variable,

n — index of the summation.

$$\text{AES}(M, K) = \left(\sum_{i=1}^{10} S(\text{ShiftRows}(\text{SubBytes}(M \oplus K))) \cdot R_i \right) \oplus K$$

where

$\text{AES}(M, K)$ — result of AES encryption of message M with key K,

$S(\cdot)$ — substitution operation,

$\text{ShiftRows}(\cdot)$ — row shifting operation,

$\text{SubBytes}(\cdot)$ — byte substitution operation,

R_i — round key for round i,

$\oplus$ — bitwise exclusive OR operation.

Formulas (1.5) and (1.5) can be used to formalize the security and reliability requirements of an SSO system. They can be used to verify that the SSO system complies with certain standards and requirements, as well as to identify possible vulnerabilities and errors in the authentication and authorization process.

$$E(m, k) = (m \cdot k) \mod n$$

$$\text{SHA-256}(M) = H_0 \oplus H_1 \oplus H_2 \oplus H_3 \oplus H_4 \oplus H_5 \oplus H_6 \oplus H_7$$

1.6

Appendix

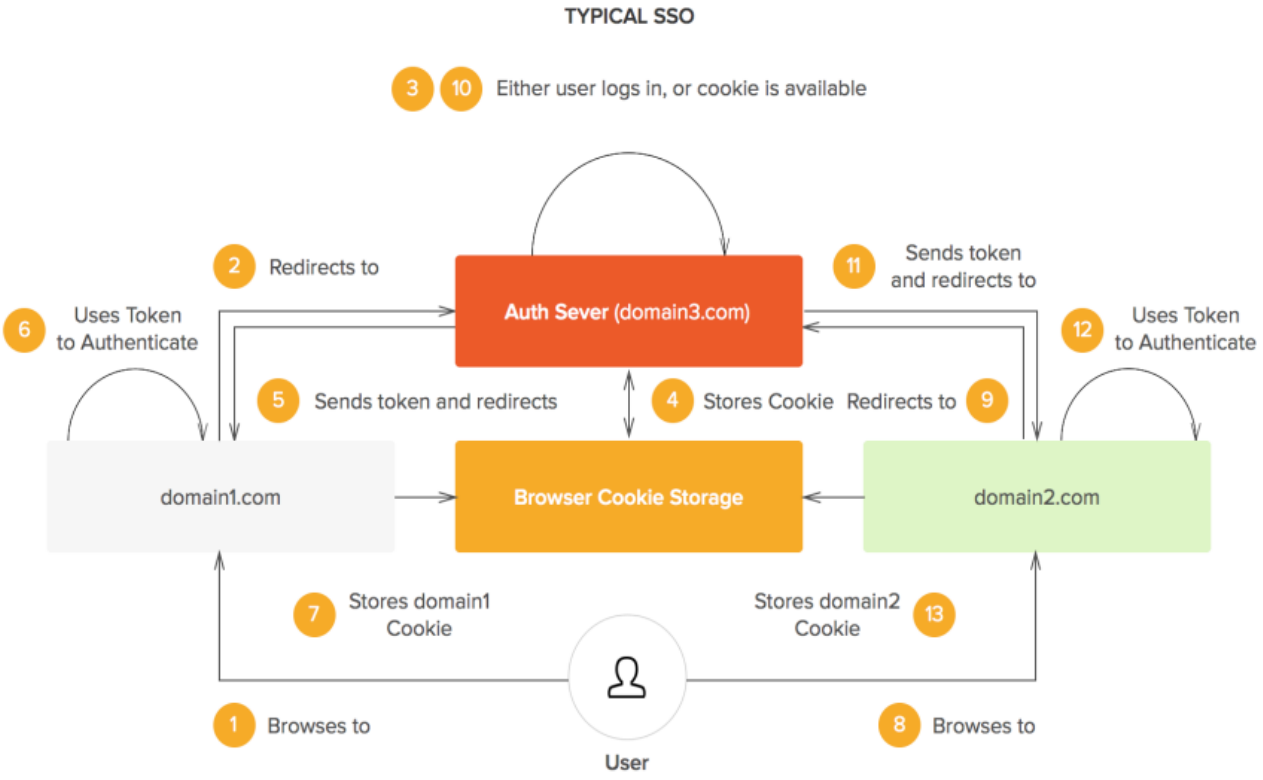


Figure 1.1: SSO execution scenario

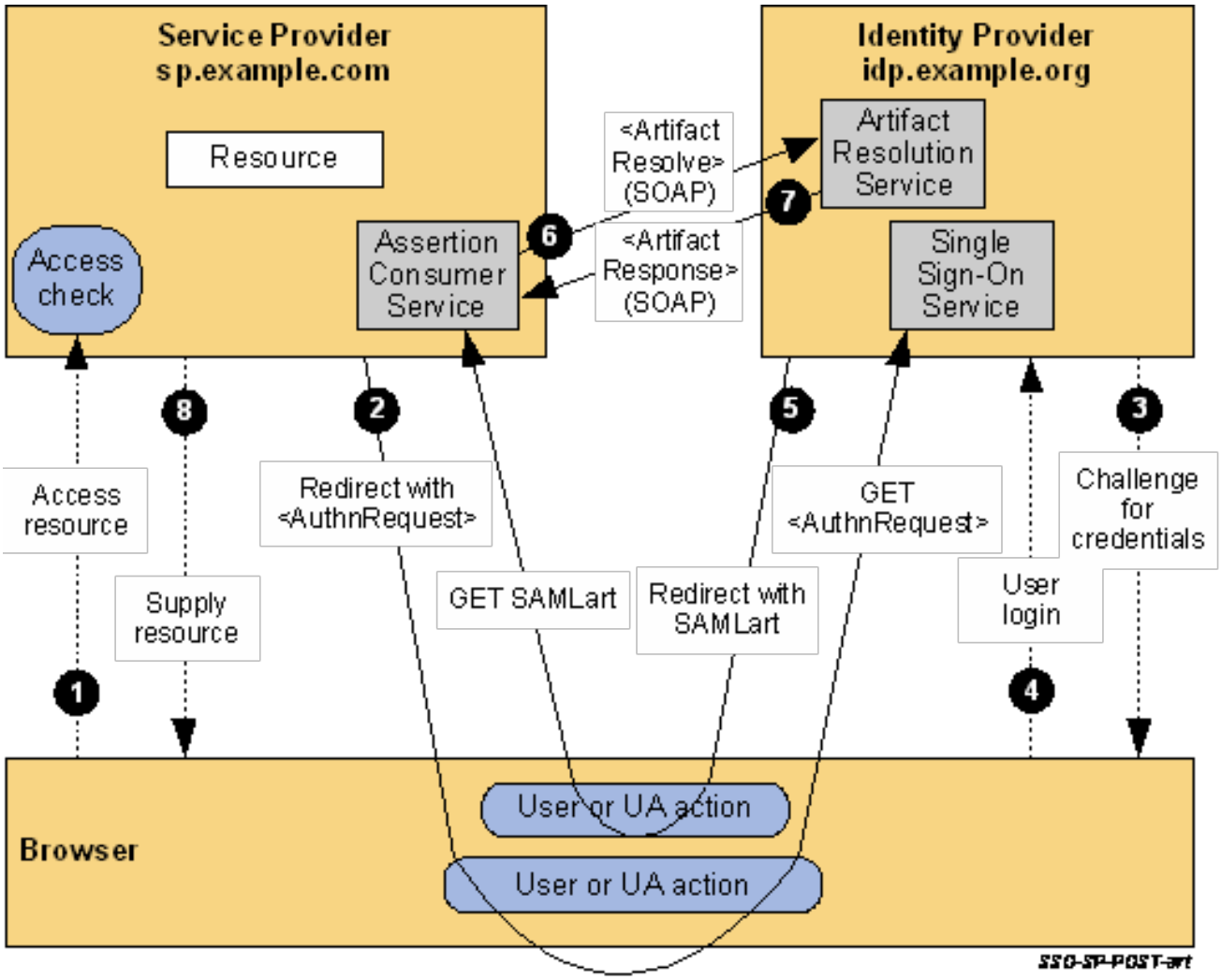


Figure 1.2: Attack on the SAML-based SSO

Protocol	Description	Use cases
SAML 2.0	Standard SSO protocol that uses XML for data exchange between service providers and identity providers.	Enterprise SSO, cloud-based applications, web-based applications, and mobile applications.
OAuth 2.0	Authorization protocol that allows users to grant access to their data without sharing their password.	Social media logins, third-party app access, and API authentication.
OpenID Connect	SSO protocol based on OAuth 2.0 that adds user authentication capabilities.	Web-based applications, mobile applications, and enterprise SSO.
WS-Federation	SSO protocol used in the Windows environment that allows users to access resources in different domains.	Enterprise SSO, web-based applications, and legacy applications.
CAS	SSO protocol used in the Java environment that allows users to access resources on different servers.	Web-based applications, enterprise SSO, and cloud-based applications.

Table 1.1: Comparison of Common Single Sign-On (SSO) Protocols