list of contents

[1 Abstract 2](#_Toc163733157)

[2 The SAML web browsers SSO protocols 3](#_Toc163733158)

[2.1 Types of SSO 3](#_Toc163733159)

[2.2 Laws of Identity 3](#_Toc163733160)

[3 Formalising the Communication Channels 4](#_Toc163733161)

[3.1 Confidential channels 4](#_Toc163733162)

[3 References 6](#_Toc163733163)

# 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 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.

# The SAML web browsers SSO protocols

## Types of SSO

1. Where they are deployed:
   * Intranett or Enterprise SSO (ESSO);
   * Extranet or Multi-domain SSO;
   * Internet or Web SSO.
2. How they are deployed:
   * Simple SSO architecture;
   * Complex SSO architecture.
3. Types of Credentials Used:
   * Complex SSO with a single set of credentials;
   * Complex SSO with multiple sets of credentials.
4. Single sign-on Protocols:
   * Kerberos authentication Protocol;
   * Security Assertion Markup Language;
   * OpenID.

## 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.

# Formalising the Communication Channels

As the security of SAML SSO ultimately depends on the security of the transport protocols used to exchange the messages, special care must be paid in modelling the communication channels. We do this by constraining the behaviour of the intruder through a number of LTL formulae each modelling a specific security property that the underlying communication channel is expected to enjoy.

## Confidential channels

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

|  |  |
| --- | --- |
|  | (1) |
| where ch - the communication channel under consideration;  *p* denotes the principal (receiver) for whom the channel ch is confidential;  *A* signifies the sender of a message;  *B* denotes the receiver of a message;  *M* represents the message being exchanged. | | | |  |  |
|  | () |
| where b – receiver;  *a* – sender;  *m* – message;  *s* – signature;  *j2* denotes the transition of the system's state. | | | |  |  |
| where *RS* denotes the state of sending a message. | | | |  |  |
|  | | | |  |  |
| where *A0* and *B0* denote the sender and receiver, respectively, of the subsequent message;  *RS0* represents the subsequent state of sending another message;  M0 - is a message sent by another sender (A0) to another receiver (B0) in the same communication channel (ch) within the same communication context (RS0), where the original message M was sent. | | | |  |  |

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 table and figure below.

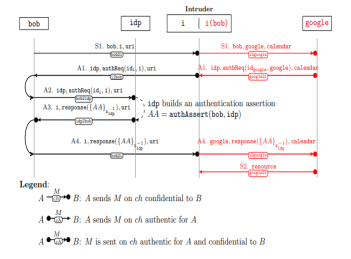


Figure 1 – Attack on the SAML-based SSO

Table 1 – Facts and their informal meaning

|  |  |
| --- | --- |
| Fact | Meaning |
| stater (j, a, es, s) | Principal a, playing role r, is ready to execute step j in session s of the protocol, and es is a list of expressions representing the internal state of a and thus affecting her future behaviour. |
| ik(m) | The intruder knows message m. |
| sent(rs, b, a, m, ch) | Principal rs has sent message m on channel ch to principal a pretending to be principal b. |
| rcvd(a, b, m, ch) | Message m (supposedly sent by principal b) has been received on channel ch by principal a, but a has not processed it yet. |
| c(n) | Term n is the current value of the counter used to construct fresh terms. This value is incremented every time a fresh term is used. |
| contains(db, m) | Message m is contained into set db. Sets are used, e.g., to share data between honest principals. |

# References

1. A. Armando, R. Carbone, and L. Compagna, “Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps,” Management of Computing and Information Systems]: Security and Protection—Authentication, vol. 1, pp. 1–9, 2008.
2. Y. Liu, D. He, and M. S. Obaidat, “Blockchain-based identity management systems: A review,” Journal of Network and Computer Applications, vol. 166, pp. 1–37, 2020.
3. V. Radha and D. H. Reddy, “A Survey on Single Sign-On Techniques,” Procedia Technology, vol. 4, pp. 134–139, 2012, doi: 10.1016/j.protcy.2012.05.019.