OASIS SSTC: SAML Security Considerations

draft-sstc-sec-consider-00

10-Aug-2001

Jeff Hodges
Prateek Mishra
Bob Morgan
Tim Moses
Evan Prodromou

(I included folks' names here if they have an email msg in the list of relevant msgs below and some of that thinkin' and/or wordin' might be incorp'd herein.)

Revision History

Revision	Date	Author	What
00	xx-Aug-2001	Jeff Hodges	Created.

1 Introduction

This document describes and analyzes the security properties of the Security Assertions Markup Language. The intent is to provide..

- input back into the design of SAML itself, as-presently-specified by the documents listed in section 6.1 below,
- architects, implementors, and reviewers of SAML-based systems information about..
    - what threats, thus security risks, a SAML-based system is subject to,
    - what security risks the SAML architecture addresses, and how it does so,
    - those it does not address,
    - recommendations on mitigating those risks

2 Background and Motivation

Communication between computer-based systems is subject to a variety of threats, and thus have associated risk, depending upon a host of factors including the nature of the communications, the nature of the communicating systems, the communication medium(s), the communication environment, the end-system environments, etc. See section 3 of [sec-cons-03] for an overview of threats inherent in the Internet (and intranets, by implication).

SAML is intended to aid deployers in establishing security contexts for application-level computer-based communications within and/or between security domains. This document comprises and in-depth analysis and assessment of the security afforded by SAML.

See section 2 of [sec-cons-03] for an overview of Communications Security and Systems Security. The former is directly applicable to the design of SAML. The latter is of interest mostly in the context of SAML's threat models. It is worthwhile to note that SAML itself is intended to address the "endpoint authentication" (in part, at least) aspect of Communications Security, and also the "unauthorized usage" aspect of Systems Security.

3 Overview

Some example SAML deployments are shown in Figures 1-?.

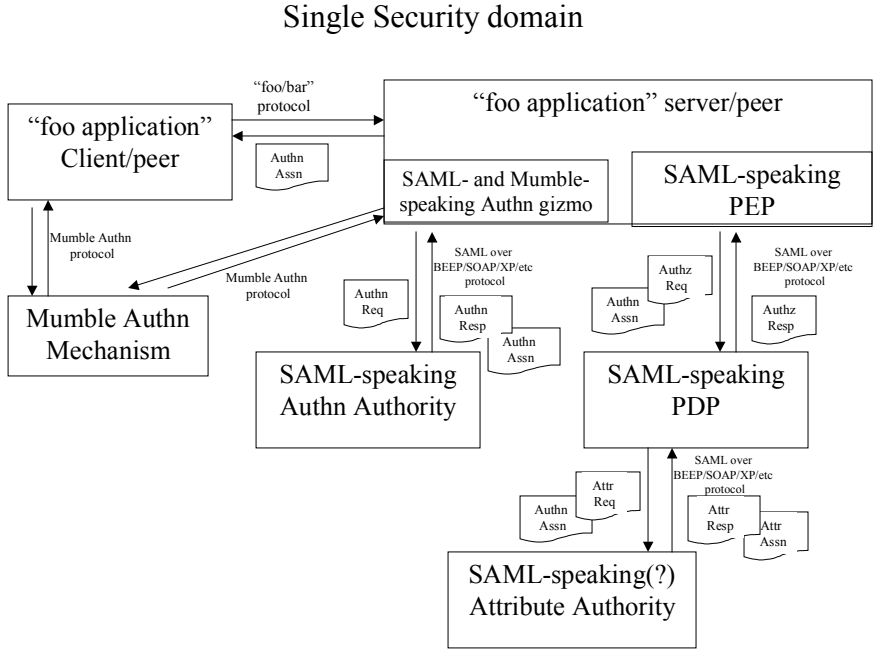


Figure 1: somewhat bogus overview illustration

3.1 Threat Models

From section 5 of [sec-cons-03]..

Authors MUST describe

1. which attacks are out of scope (and why!)
2. which attacks are in-scope
   2.1 and the protocol is susceptable to
   2.2 and the protocol protects against

SAML's overall threat models (see section 3 of [sec-cons-03]) are composed of…

[TBD]

4 Use-case Analyses

In this section, we examine SAML's use-cases from a security perspective. This helps put SAML into an overall context such that we can methodically examine it in detail. Concrete analysis then occurs in the following section.

4.1 Use Case 1: Web Browser-based Single Sign-on

4.1.1 Scenario 1-1: Single Sign-on, Pull Model

[This item will likely be addressed by the discussion in section 5.3.1.1 below.]

4.1.2 Scenario 1-2: Single Sign-on, Push Model

[This item will likely be addressed by the discussion in section 5.3.1.1 below.]

4.1.3 Scenario 1-3: Single Sign-on, Third-Party Security Service

4.2 Use Case 2: Authorization Service

4.2.1 Scenario 2-1: Application Chain

4.3 Use Case 3: Back Office Transaction

4.3.1 Scenario 3-1: Back Office Transaction

4.3.2 Scenario 3-2: Back Office Transaction, Third-Party Security Service

4.3.3 Scenario 3-3: Intermediary Add

4.4 Use Case 4: User Session

4.4.1 Scenario 4-1: Single Sign-on, User Session

5 Analyses of SAML Specifics

This section offers a detailed analysis of SAML in the context of specific assumptions and threats.

[These email messages have *useful* content (that should be extractred and incorporated) and/or hints for the material in this section (this list is not exhaustive)…

Note on Digital Signing in SAML (was RE: The XML Security Gap (wa sRe: XML Encryption Working Draft))
http://lists.oasis-open.org/archives/security-services/200106/msg00167.html
..and all the msgs having a subject of "*Note on Digital Signing in SAML".

RE: Note on Digital Signing in SAML (re-send)
http://lists.oasis-open.org/archives/security-services/200107/msg00008.html

RE: Note on Digital Signing in SAML (re-send)
http://lists.oasis-open.org/archives/security-services/200107/msg00015.html

Defective sign & encrypt vis-a-vis SAML?
http://lists.oasis-open.org/archives/security-services/200107/msg00059.html

Minutes of Bindings Con-Call, July 12
http://lists.oasis-open.org/archives/security-bindings/200107/msg00020.html

protocol bindings
http://lists.oasis-open.org/archives/security-bindings/200107/msg00029.html

..an exercise that the putative “we” need to do is methodically go thru the archives of the list(s) and extract relevant info for inclusion in this doc (see above)

]

5.1 SAML Assertions

5.2 SAML Protocol

5.2.1 SAML Protocol Bindings

5.2.1.1 HTTP

5.2.1.2 SOAP 1.1

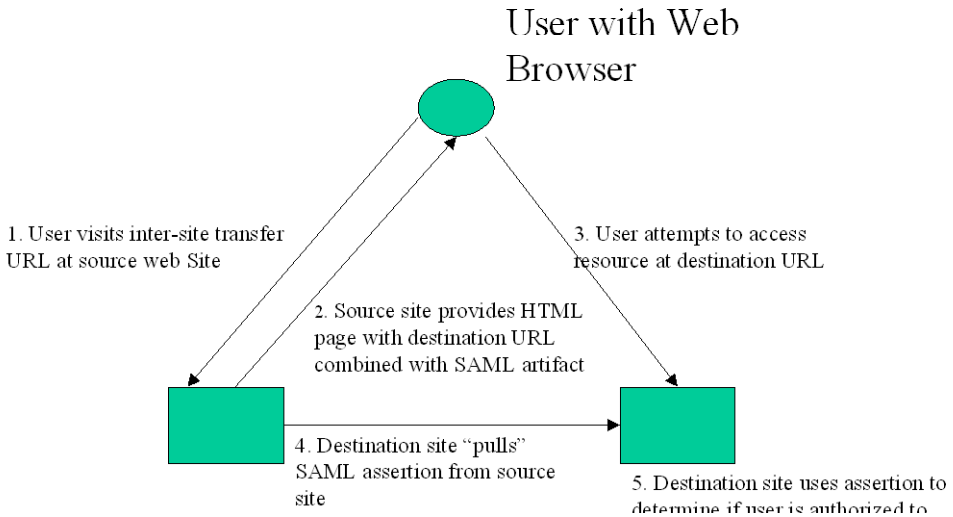
5.2.1.3 BEEP

[TBD]

5.3 Profiles of SAML

175 #### 5.3.1.1 Web Browser

Figure 1: Single Sign-On (web browser)



176

177 Given the illustration (above) and description in [bindings-model-04] of the Web Browser
178 Proflile of SAML, we have the following interaction steps..

179 0. (not directly illustrated) The user authenticates at the source web site

180 1. user's browser accesses (via HTTP) the source web site as-specified by the "inter-site
181 tranfer URL"

182 2. source site returns HTML page with a destination URL combined with a SAML artifact

183 3. user directs her browser to attempt to access resource (via HTTP) at destination site
184 specified by destination URL

185 4. Destination site "pulls" SAML assertion from source site (via SAML Request message
186 over some protocol).

187 5. Destination site uses assertion to determine if user is authorized to access destination
188 resource.

189

190 Each step in the interaction described above must be appropriately secured.

191

192 0. The user authenticates at the source web site

This could be accomplished using any authn mechanism supported by, or over HTTP, or whatever protocol the user's system is using to contact the source system entity (aka source web site). The key notion is that the source system entity MUST be able to ascertain that it is the same authenticated client system entity that it is interacting with in the next interaction step. One way to accomplish this is for these initial steps to be performed using TLS as a session layer underneath the protocol being used for this initial interaction (likely HTTP).

1. user's browser accesses (via HTTP) the source web site as-specified by the "inter-site tranfer URL"

2. source site returns HTML page with a destination URL combined with a SAML artifact

3. user directs her browser to attempt to access resource (via HTTP) at destination site specified by destination URL

4. Destination site "pulls" SAML assertion from source site (via SAML Request message over some protocol).

5. Destination site uses assertion to determine if user is authorized to access destination resource.

5.3.1.2 SOAP

6 References

6.1 SAML Specification Documents

[core-12] Security Assertions Markup Language: Core Assertion Architecture
http://www.oasis-open.org/committees/security/docs/draft-sstc-core-12.pdf

[core-discussion-01] SAML Assertion Schema Discussion (non-normative)
http://www.oasis-open.org/committees/security/docs/draft-sstc-core-discussion-01.pdf

[protocol-discussion-01] SAML Protocols Schema Discussion (non-normative)
http://www.oasis-open.org/committees/security/docs/draft-sstc-protocol-discussion-01.pdf

[bindings-model-04] Oasis Security Services Bindings Model
http://www.oasis-open.org/committees/security/docs/draft-sstc-bindings-model-04.pdf

[saml-reqs-01] Oasis Security Services Use Cases And Requirements
http://www.oasis-open.org/committees/security/docs/draft-sstc-saml-reqs-01.pdf

6.2 Normative References

[xml-dsig] XML-Signature Syntax and Processing, W3C Candidate Recommendation 19-April-2001.
http://www.w3.org/TR/2001/CR-xmldsig-core-20010419/

[saml-glossary] OASIS Security Services TC Glossary
http://www.oasis-open.org/committees/security/docs/draft-sstc-glossary-01.pdf

6.3 Supplementary Documents

[xml-encyption] XML Encryption Syntax and Processing, WG Working Draft 26 June 2001.
http://www.w3.org/TR/xmlenc-core/

[sec-cons-03] Guidelines for Writing RFC Text on Security Considerations
http://www.ietf.org/internet-drafts/draft-rescorla-sec-cons-03.txt

[ebXML-Risk] ebXML Technical Architecture Risk Assessment v1.0
http://www.ebxml.org/specs/secRISK.pdf

[ebXML-MSS] Message Service Specification: ebXML Transport, Routing & Packaging
Version 1.0
(chapter 12 specifically)
http://www.ebxml.org/specs/ebMS.pdf

[Prudent] Prudent Engineering Practice for Cryptographic Protocols
http://citeseer.nj.nec.com/abadi96prudent.html

[Robustness] Robustness principles for public key protocols
http://citeseer.nj.nec.com/2927.html

Appendix A

Appendix B