SSTC Response to "Security Analysis of the SAML Single Sign-on Browser/Artifact Profile"

Working Draft 01, 24 January 2005

Document identifier:

sstc-gross-sec-analysis-response-01

Location:

http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

Editors:

John Linn, RSA Security Inc.

Prateek Mishra, Principal identity

Contributors:

TBD

Abstract:

Thomas Groß's paper, "Security Analysis of the SAML Single Sign-on Browser/Artifact Profile" (19th Annual Computer Security Applications Conference, Las Vegas, December 2003) **[Groß]** analyzes aspects of SAML V1.0. This document provides a response to that analysis on behalf of the OASIS Security Services Technical Committee (SSTC).

Status:

No scheduled updates are planned to this document following publication, but corrections and clarifications may be incorporated at a later date if discussion warrants.

Committee members should submit comments and potential errata to the security-services@lists.oasis-open.org list. Others should submit them by filling out the web form located at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security. The committee will publish on its web page (http://www.oasis-open.org/committees/security) a catalog of any changes made to this document as a result of comments.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights web page for the Security Services TC (http://www.oasis-open.org/committees/security/ipr.php).

Table of Contents

1 Response to Analysis

1.1 Introduction

The SSTC would like to thank Thomas Groß for this paper's detailed examination of aspects of the SAML V1.0 specifications. We concur with the paper's assessment of SAML as an important standardized example of an identity management protocol, and appreciate the author's description of the evaluated Browser/Artifact profile specification as "generally a well-written protocol" and "one of the most carefully designed browser-based protocols in federated identity management". Particularly given SAML's importance and deployment, and the concerns and constraints attendant to operation in browser-based environments, we also concur with the appropriateness and value of careful and formalized security evaluation. As the paper notes, protocols like SAML represent a new type of target for security analysis methodologies, and we encourage work in this area.

In response to the paper's analysis, the SSTC has incorporated some changes into the SAML V2.0 specifications. Specifically, Section 3.6.5.2 of [SAML20-Binding]   recommends additional counter-measures against threats identified in Section 6.5 (One-request property of the SAML artifact) and Section 6.6 (HTTP Referrer Tag) of [Groß]**.**

We believe, however, that some of the points raised in the analysis warrant clarification or correction, and therefore present our responses within this document.

1.2 General Comments

This section discusses general issues, which arise in multiple places within the paper.

1.2.1 Scope of SAML

In evaluating SAML protocol flows, it is important to distinguish steps that are within the scope specified by SAML from steps that are performed in conjunction with SAML but which are outside its scope per se. SAML protocols and implementations are designed to operate in a broader context, in conjunction with other protocols and mechanisms. Examples include protocols such as HTTP and SSL, as well as mechanisms for authentication and session management as found in most web and application servers.

The SSTC believes that it is appropriate and useful to identify areas in which SAML depends on other components and mechanisms for functional and/or security purposes, but that evaluation of such components and mechanisms is properly distinct from evaluation of SAML itself. Further, a dependency by SAML on a function or security services that is appropriately provided outside SAML need not, in the SSTC's view, constitute a flaw in the SAML specification.

1.2.2 Use of SSL/TLS

As the paper notes in its conclusion, "Most implementations will simply use SSL/TLS channels with unilateral authentication, which complicates or prevents man-in-the-middle and replay attacks." Indeed, proper use of SSL/TLS, which the SAML specifications recommend, can render many of the described attacks moot or impractical. It is the SSTC's intent and recommendation, as stated in both the SAML 1.x and SAML 2.0 specifications, that the Web SSO Browser/Artifact profile be used in conjunction with SSL/TLS, except for particular deployment environments where comparable protection is obtained through other means. We note, also, that SAML contemplates deployment of SSL/TLS with unilateral authentication (based on server-side certificates), in addition to the anonymous and bilateral cases considered in Section 4 of the paper.

1.3 Evaluation of Protocol Steps

This section comments on the analysis of protocol steps as presented within Section 6 of the paper.

1.3.1 Step 1: Contact the Source Site

Clearly, it is important for browser users to authenticate the sites they access before performing sensitive transactions with those sites, whether in SAML or non-SAML environments. The connection to a site's inter-site transfer URL, although a precursor to SAML-supported SSO, is not itself within the scope of SAML-defined protocols though it is part of the overall operational scenario described in conjunction with the use of those protocols.

Regarding the "Message Format" attack as described in this section, more discussion would be valuable to clarify the exploits that might be possible as a result of accumulating artifacts and repeating selected protocol steps. The behavior as discussed could also be reasonably described to be characteristic of the HTTP protocol and its usage and does not seem to be specific to SAML SSO.

Regarding the "User Tracking" discussion, the means through which source sites determine whether a particular user session has already been authenticated is (as the paper recognizes) not specified within SAML, and may vary in different implementations and deployments. As a result, it cannot be comprehensively evaluated within the scope of SAML protocols.

1.3.2 Step 2: Initiating the Redirect to the Destination Site

SAML implementations can maintain information bases enabling them to determine the appropriate URL for artifact delivery; it need not be determined solely based on hostname. Within the SAML V2.0 specifications, for example, metadata elements provide a means for this information to be represented and published. Further, it is worth noting that access to a misdelivered artifact is necessary but in itself insufficient to obtain the assertion to which it corresponds, as the artifact's issuer is expected to perform validation checks when an attempt is made to resolve the artifact.

1.3.3 Step 3: Redirect to the Destination Site

Use of an SSL/TLS secure channel, as recommended in the SAML 1.x and SAML2,0 specifications, serves as a defense against the described "Lack of Authentication" attack.

1.3.4 Step 4: SAML Request

Regarding the "Specification of the Source Site Lookup" discussion, Section 4.1.1.8 of [SAMLBind10] describes the intended ID lookup procedure; the paper's conclusion that lookups cannot be successfully performed on this basis appears unclear, and further clarification would be helpful.

Regarding the "One-request Property of the SAML Artifact" discussion, the source site indeed enforces the property that a given artifact can only be resolved once. As the artifact source is responsible for the associated assertion, we consider it an appropriate entity to perform this enforcement. The exposure associated with pending, unresolved artifacts is somewhat mitigated by the intent that artifact lifetimes are to be short.

1.3.5 Step 5: SAML Response

Regarding the "One-request Property of the SAML Artifact" discussion, we agree that correct implementation of the one-time use constraint is important, as is correct implementation of all other security-related aspects of the SAML specifications. Specific implementation issues and strategies lie below the architectural level of the SAML specifications. To provide additional assurance for the one-time use constraint, the SAML V2.0 specifications include (Section 3.6.5.2 of [SAML20-Binding]) provisions for destination-side enforcement in addition to the currently specified source-side enforcement.

Regarding the "Multiple Services on One Host" discussion, it was not intended that the granularity of artifact transfer would be constrained to hostnames. If multiple services with different assurance levels coexist on the same host, they could be separately identified and represented with different credentials.

1.3.6 Step 6: Response to the Browser

While within the overall operational scenario, this step lies outside the scope of SAML-defined protocols. Per the "Specification of this Step" discussion, it is true that the same connection as discussed in Step 3 would ordinarily be used to return this response; as noted above, the SSTC recommendation is for that connection to be protected using SSL/TLS.

1.4 Evaluation of Cited Attacks

1.4.1 Connection Hijacking / Replay Attack

As the last sentence in the section describes as a solution to the attack described, "One can also use a secure channel B <-> D in steps 3 and 6, which provides freshness and replay prevention." The recommended use of SSL/TLS provides such a channel, as Section 8 of the paper acknowledges.

1.4.2 Man-in-the-Middle Attacks

1.4.2.1 Between B and S by DNS Spoofing

As noted above, initial authentication of S to the user's browser is outside the scope of SAML-specified protocols.

1.4.2.2 Other Man-in-the-Middle Attacks

Per the second paragraph in this section of the paper, note that use of SSL/TLS authentication is recommended for the steps described.

1.4.3 HTTP Referrer Attack

Consistent with the recommendation in the "Possible Solutions" discussion, SAML 2.0 includes provisions for destination-side enforcement of one-time artifact use within the SAML V2.0 specifications. In contexts where active referrals are unacceptable an implementation of the Web SSO profile using the HTTP POST binding (Section 3.5 of [SAML20-Binding]) provides an alternative choice .

1.5 Conclusions

The SSTC believes that the Groß paper provides an important service by evaluating security characteristics of SAML protocols and environments, and values and encourages work in this area. We observe, however, that the recommended use of SSL/TLS secure channels provides an effective countermeasure to most of the attacks identified in the paper. Further, the SAML V2.0 specifications, include additional recommendations, and clarifications to enhance defenses against certain attacks identified by [Groß].

2 References

[Groß]   T. Groß, *Security Analysis of the SAML Single Sign-on Browser/Artifact Profile*, 19th Annual Computer Security Applications Conference, Las Vegas, December 2003.

[SAMLBind10]   *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML),* OASIS Standard, 5 November 2002.

[SAML20-Binding]   *Bindings for the OASIS Security Assertion Markup Language (SAML),* V2.0 Committee Draft 03, 14 December 2004

178 # Appendix A.Acknowledgements

179 TBD

180 # Appendix B.Revision History

181 *[This appendix is optional, but helpful. It should be removed for specifications that are at OASIS Standard*
182 *level.]*

Rev	Date	By Whom	What
00	2004-07-08	John Linn	Initial version
01	2005-01-24	Prateek Mishra and John Linn	First update

Appendix C.Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.