



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

Committee Draft 01, 15 July 2005

Document identifier:

sstc-gross-sec-analysis-response-cd-01

Location:

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

Editors:

John Linn, RSA Security Inc. (jlinn@rsasecurity.com)
Prateek Mishra, Principal identity (pmishra@principalidentity.com)

Contributors:

Scott Cantor, Internet2

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>).

32 Table of Contents

33	1 Response to Analysis.....	3
34	1.1 Introduction.....	3
35	1.2 General Comments.....	3
36	1.2.1 Scope of SAML.....	3
37	1.2.2 Use of SSL/TLS.....	3
38	1.3 Evaluation of Protocol Steps.....	4
39	1.3.1 Step 1: Contact the Source Site.....	4
40	1.3.2 Step 2: Initiating the Redirect to the Destination Site.....	4
41	1.3.3 Step 3: Redirect to the Destination Site.....	4
42	1.3.4 Step 4: SAML Request.....	4
43	1.3.5 Step 5: SAML Response.....	4
44	1.3.6 Step 6: Response to the Browser.....	5
45	1.4 Evaluation of Cited Attacks.....	5
46	1.4.1 Connection Hijacking / Replay Attack.....	5
47	1.4.2 Man-in-the-Middle Attacks.....	5
48	1.4.2.1 Between B and S by DNS Spoofing.....	5
49	1.4.2.2 Other Man-in-the-Middle Attacks.....	5
50	1.4.3 HTTP Referrer Attack.....	5
51	1.5 Conclusions.....	5
52	2 References.....	6
53	Appendix A.Acknowledgements.....	7
54	Appendix B.Revision History.....	8
55	Appendix C.Notices.....	9

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 countermeasures 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.

96 **1.3 Evaluation of Protocol Steps**

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

98 **1.3.1 Step 1: Contact the Source Site**

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

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

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

112 **1.3.2 Step 2: Initiating the Redirect to the Destination Site**

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

119 **1.3.3 Step 3: Redirect to the Destination Site**

120 Use of an SSL/TLS secure channel, as recommended in the SAML 1.x and SAML 2.0 specifications,
121 serves as a defense against the described "Lack of Authentication" attack.

122 **1.3.4 Step 4: SAML Request**

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

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

131 **1.3.5 Step 5: SAML Response**

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

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

141 **1.3.6 Step 6: Response to the Browser**

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

146 **1.4 Evaluation of Cited Attacks**

147 **1.4.1 Connection Hijacking / Replay Attack**

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

151 **1.4.2 Man-in-the-Middle Attacks**

152 **1.4.2.1 Between B and S by DNS Spoofing**

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

155 **1.4.2.2 Other Man-in-the-Middle Attacks**

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

158 **1.4.3 HTTP Referrer Attack**

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

163 **1.5 Conclusions**

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

2 References

170

171

172

173

[Groß]

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

174

175

[SAMLBind10]

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

176

177

[SAML20-Binding]

Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005.

178 A. Acknowledgments

179 The editors would like to acknowledge the contributions of the OASIS Security Services Technical
180 Committee, whose voting members at the time of publication were:

- 181 • Conor Cahill, AOL
- 182 • John Hughes, (formerly) Atos Origin
- 183 • Hal Lockhart, BEA Systems
- 184 • Mike Beach, Boeing
- 185 • Rebekah Metz, Booz Allen Hamilton
- 186 • Rick Randall, Booz Allen Hamilton
- 187 • Ronald Jacobson, Computer Associates
- 188 • Gavenraj Sodhi, Computer Associates
- 189 • Thomas Wisniewski, Entrust
- 190 • Carolina Canales-Valenzuela, Ericsson
- 191 • Dana Kaufman, Forum Systems
- 192 • Irving Reid, Hewlett-Packard
- 193 • Guy Denton, IBM
- 194 • Heather Hinton, IBM
- 195 • Maryann Hondo, IBM
- 196 • Michael McIntosh, IBM
- 197 • Anthony Nadalin, IBM
- 198 • Nick Ragouzis, individual
- 199 • Scott Cantor, Internet2
- 200 • Bob Morgan, Internet2
- 201 • Peter Davis, Neustar
- 202 • Jeff Hodges, Neustar
- 203 • Frederick Hirsch, Nokia
- 204 • Senthil Sengodan, Nokia
- 205 • Abbie Barbir, Nortel Networks
- 206 • Scott Kiester, Novell
- 207 • Cameron Morris, Novell
- 208 • Paul Madsen, NTT
- 209 • Steve Anderson, OpenNetwork
- 210 • Ari Kermaier, Oracle
- 211 • Vamsi Motukuru, Oracle

- 212 • Brian Campbell, Ping Identity
- 213 • Darren Platt, Ping Identity
- 214 • Prateek Mishra, Principal Identity
- 215 • Jim Lien, RSA Security
- 216 • John Linn, RSA Security
- 217 • Rob Philpott, RSA Security
- 218 • Deepak Chopra, SAP
- 219 • Jahan Moreh, Sigaba
- 220 • Eve Maler, Sun Microsystems
- 221 • Ronald Monzillo, Sun Microsystems
- 222 • Emily Xu, Sun Microsystems
- 223 • Greg Whitehead, Trustgenix

Appendix B: Notices

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

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

236 **Copyright © OASIS Open 2005. All Rights Reserved.**

237 This document and translations of it may be copied and furnished to others, and derivative works that
238 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and
239 distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and
240 this paragraph are included on all such copies and derivative works. However, this document itself may
241 not be modified in any way, such as by removing the copyright notice or references to OASIS, except as
242 needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights
243 defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it
244 into languages other than English.

245 The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors
246 or assigns.

247 This document and the information contained herein is provided on an "AS IS" basis and OASIS
248 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY
249 WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR
250 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.