Successful SAML V1.1 Interop Lab at RSA2004 Conference

The SAML V1.1 Interop Lab at RSA2004

```
Date: Mon, 1 Mar 2004 09:55:34 -0500
From:      "Philpott, Robert" <rphilpott@rsasecurity.com>
To:        "'saml2004@cfrq.net'" <saml2004@cfrq.net>,
           "'security-services@lists.oasis-open.org'"
<security-services@lists.oasis-open.org>,
           "'saml-dev@lists.oasis-open.org'" <saml-
dev@lists.oasis-open.org>
Subject:   The SAML V1.1 interop lab at RSA2004 was a
fantastic success!
```

Hi folks,

For those of you that couldn't attend, I thought I'd pass along some news regarding the SAML interoperability lab we held during the RSA2004 conference. The lab was hosted by RSA and sponsored by the General Services Administration (GSA) of the US government and by Sun Microsystems, who provided 19" LCD monitors for everyone to use. Once I update the interop spec, I'll also post it and the press event slides to the SSTC repository.

Executive Summary

We had 11 vendors participating in the interop. We also had Enspier Technologies participating under contract to GSA. The vendors that participated in the event were Computer Associates, DataPower Technology, Entegrity Solutions, Entrust, Hewlett-Packard, Oblix, OpenNetwork, Ping Identity, RSA Security, Sun Microsystems, and Trustgenix.

There were 2 key goals for the interop. First, we wanted to demonstrate SAML 1.1 interoperability for both Web SSO profiles and for general queries. The other main goal was to show an interoperable implementation of the GSA eGov program's eAuthentication architecture that builds on top of SAML. Also, given that the major change for SAML 1.1 dealt with improving XML DSIG interoperability, we certainly wanted to demonstrate this in the process.

In my view, this exercise was an absolutely stunning success! I offer my congratulations to every vendor that participated. It was truly an honor to work with such a talented group of engineers and supporting cast. When we were done, every vendor had successfully completed everything they had planned to accomplish. This was no small feat.

The Details

The general concept of the web SSO demo was to let a visitor to the booth sit at any vendor's display, start the demo at the portal or any of the asserting party or relying party web sites, use either of the SAML Web SSO profiles to gain access to an application at a relying party, and then use Web SSO to gain access to any other application at another relying party. We wanted to accomplish this using either a "generic SAML" or the eAuthentication demo use case.

All vendors except DataPower implemented the Web SSO use cases, providing both the SAML 1.1 Web SSO Profile and eAuthentication demo scenarios. All of these vendors supported the Browser/Artifact Profile and all but two supported the Browser/POST Profile. Enspier provided a portal that implemented the additional exchanges defined by the eGov program's eAuthentication architecture. Each vendor implemented the AP and RP sides of these exchanges during the lab. The portal was also enhanced to support the generic SAML demo as well.

The SAML query use case was demonstrated by DataPower who implemented a simple web services-based demo utilizing SAML 1.1 Attribute Queries to the RSA Attribute Authority.

The general plan was to begin testing on Sunday morning and finish by Tuesday evening. A press and analyst event was scheduled first thing Wednesday morning with a private demo for them. This was to be followed by public demonstrations all day on Wednesday and Thursday. Our lab consisted of tables around the perimeter of a 20x20 foot booth on the conference exhibit hall floor. Since the exhibit hall was open beginning on Monday evening, we had curtains put up outside the tables so we could work in relative privacy (this invoked several Wizard of Oz comments about the man behind the curtain J). With most vendors sending 2 to 4 people to the lab, you can understand that things were pretty cramped at times, but we all made the best of it. The curtains came down Tuesday at 5pm once the exhibit hall closed. After sharing a pizza dinner, we all continued testing/debugging until our 10pm cutoff time. I thought it was great to see how lots of folks that had already completed their tests stuck around with their systems to help the others finish up.

With respect to the Web SSO demo, doing just the SAML asserting-party-site-first "click-through" testing of all vendors testing both BAP and BPP against all other vendors would have been a very good accomplishment. But we didn't stop there. We also did a "generic SAML" version of a portal-site-first and an application-site-first scenario, passing the web SSO "TARGET" parameter between sites.

And of course, since the lab was being sponsored by GSA, we also implemented 6 additional scenarios (BAP and BPP starting at 3 different sites) for the eAuthentication architecture. Thus, most vendors had over 100 test cases to run. We had a couple of late nights, but by Wednesday morning, everyone was ready.

The press event included opening remarks and introductions by Scott McGrath from OASIS, followed by comments from Steve Timchak from the GSA about why they wanted to sponsor the event and the importance of open standards to the GSA. I then presented a few slides on the history and current work of the SSTC and a quick discussion of the demo they would see. It was difficult for me to tell how many of the attendees were actually press and analysts (anyone care to venture a guess?), but it seemed well attended, especially considering a ferocious rain storm that hit SF and snarled traffic in town.

The exhibit hall was open 10am-5pm on Wednesday and Thursday. Traffic to the booth was very steady and at times very hectic. We had some excellent publicity during the conference, with moderators at the conference sessions reminding session attendees to come check us out. As Steve Anderson put it, the first 3 days were mentally exhausting and the last 2 days were physically exhausting. I know it's going to take me a few days to recover!

The interop testing proved that the SSTC's goal of producing a quality SAML V1.1 specification that improved interoperability was convincingly achieved. We found no defects in the V1.1 standard. One minor point of confusion did arise over why the spec requires that the value of a samlp:Status element must always be prefixed with a namespace declaration for the SAML protocol namespace. We can discuss whether we wish to change or clarify this on an upcoming SSTC call. But that was pretty much it.

Well, that's about all I can think of to say at this point. If others would like to provide their thoughts on the event, please do so!

Rob Philpott
RSA Security Inc.
The Most Trusted Name in e-Security
Tel: 781-515-7115
Mobile: 617-510-0893
Fax: 781-515-7020
Email: rphilpott@rsasecurity.com