Wed 10.15am SantaClara

Scribing Template --Wed., Nov 13, 2013 at 10.15am -- Santa Clara Room

TOPIC: Testing SAML Solutions and etc

CONVENER: Roland Hedberg

SCRIBE: Jim Fox

# of ATTENDEES: 8

MAIN ISSUES DISCUSSED:

Roland has own SAML idp implementation. Difficult to figure out how to implement from the documentation.
Also involved in openidconnect development and verification. Developed test tool to verify that an implementaton is correct in its implementation. SAML seems not to have such a test tool.
Developed a test tool to verify that an IdP (or SP) actually works according the SAML spec. and federation policies.
Also verify that attribute release to entity categories is correct.
Third, verify that an IdP really does what is necessary to provide an advertised authn mechanism.
Fourth, when something doesn't work, how to identify why? Without phone calls.
Many sites don't allow test userids on production systems, so automated login test not possible.
Univ Wash does allow them. Makes continual monitoring possible.
People who acquire an SP, for example, want to know that the SP has a valid SAML implementation before purchase.
Don't know who would do any certification.
End to End test is very useful. hit sp, go to idp, return to sp, look for attributes.
Roland's test also inspects the SAML messages for correctness.
Can exxamine an IdP for each protocol it claims to support in metadata.
Should also be able to verify IdP-initiated login requests.
Available on github: https://github.com/rohe/saml2test

Roland has own SAML idp implementation. Difficult to figure out how to implement from the documentation.

Also involved in openidconnect development and verification. Developed test tool to verify that an implementaton is correct in its implementation. SAML seems not to have such a test tool.

Developed a test tool to verify that an IdP (or SP) actually works according the SAML spec. and federation policies.

Also verify that attribute release to entity categories is correct.

Third, verify that an IdP really does what is necessary to provide an advertised authn mechanism.

Fourth, when something doesn't work, how to identify why? Without phone calls.

Many sites don't allow test userids on production systems, so automated login test not possible.

University of Washington does allow them. Makes continual monitoring possible.

People who acquire an SP, for example, want to know that the SP has a valid SAML implementation before purchase. Don't know who would do any certification.

End to End test is very useful. hit SP, go to IdP, return to SP, look for attributes.

Roland's test also inspects the SAML messages for correctness. Can examine an IdP for each protocol it claims to support in metadata. Should also be able to verify IdP-initiated login requests.

Roland's code is available on github: https://github.com/rohe/saml2test

ACTIVITIES GOING FORWARD / NEXT STEPS:

If slides are used in the session, please ask presenters to convert their slides to PDF and email them to acamp-info@incommon.org