

How the SAMLtrace Firefox add-on can be useful



SWITCH

Thomas Lenggenhager
thomas.lenggenhager@switch.ch

Berne, 13 August 2015

Motivation

- What really happens after...
 - ...picking the Home Organisation in the Discovery Service and the IdP presenting the login screen?
 - Some HTTP redirects and the SP issues a SAML authentication request
 - ...providing user consent and getting into the web application?
 - The IdP posts a SAML authentication assertion to the SP and the SP redirects you to the web application

In action...

The screenshot shows a web browser window titled "SAML tracer". The interface includes a toolbar with "Clear", "Autoscroll", and "Filter resources" buttons, and "Export" and "Import" icons. A list of HTTP requests is displayed, with the third request highlighted in orange and labeled "SAML".

The detailed view of the selected request shows the following information:

- Method: GET
- URL: `https://aai-logon.vho-switchaai.ch/idp/profile/SAML2/Redirect/SSO?SAMLRequest=jZJdT8IwFib%2FytL7rduQDxtGgnAhCQph0wtvTNsdWJPSzp4O9N87GBq8IV737fOc87Zj5Htds2njK7OBjwbQB597bZCdDzLSOMMsR4XM8D0g85Ll06clS6OYlc56K60mwRQRnFfWzKzBZg8uB3dQE142y4xU3tfIKOXeOyUaD%2BFBwRFcxLmK8Ki8rCJZ0bxSQLgNvooQLT1ZUrpe5QUJ5ulYyvCT4ArHVajtzproUNmw45yILUqVNW2H2yoNF84GSuVAeprnKxIs5h15H0pIkt6Ap3x0z2MxFOVgC1sQcTmsQxGLNobYwMKg58ZnJI2TfhiPwiQtkh7r37079IOE60sHD8qUyuxuFya6ELLHoliH3W6v4PC8Vxsgk%2FGpdnYWu6uHuI3lP%2B2TyT%2B7xt%2Bux%2FTK2Ol9twqFvO1lUp%2BBVOt7XHmgHvISELopLvy99NMvgE%3D&RelayState=cookie%3A1439387982_8877 HTTP/1.1`
- Host: `aai-logon.vho-switchaai.ch`
- User-Agent: `Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0`
- Accept: `text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8`
- Accept-Language: `en-US,en;q=0.5`

The SAML payload is shown in the following XML format:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://attribute-viewer.aai.switch.ch/Shibboleth.sso/SAML2/POST"
  Destination="https://aai-logon.vho-switchaai.ch/idp/profile/SAML2/Redirect/SSO"
  ID="_7cell36a2a89a0b7bd6fefeb0d8c7b0b"
  IssueInstant="2015-08-12T13:59:42Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0"
  >
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://attribute-viewer.aai.switch.ch
/shibboleth</saml:Issuer>
  <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

Spotting SAML related errors...

```
http Parameters SAML
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://attribute-viewer.aai.switch.ch/Shibboleth.sso/SAML2/POST"
  Destination="https://aai-logon.vho-switch.ch/idp/profile/SAML2/Redirect/SSO"
  ID="_7ce1136a2a89a0b7bd6fefeb0d8c7b0b"
  IssueInstant="2015-08-12T13:59:42Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0"
>
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://attribute-viewer.aai.switch.ch
/shibboleth</saml:Issuer>
  <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

- Without access to the IdP or SP log files, e.g.
 - AssertionConsumerServiceURL=
"https://attribute-viewer.aai.switch.ch/Shibboleth.sso/SAML2/POST"
must match with SP metadata
 - IssueInstant="2015-08-05T13:26:32Z"
must be within 3 minutes of actual time

Where to get it?

- UNINETT in Norway wrote SAMLtracer
 - <https://github.com/UNINETT/SAML-tracer/>
 - <https://github.com/UNINETT/SAML-tracer/releases/download/samltracer-0.3/samltracer-0.3.xpi>
- No magic involved 😊
SAMLtracer can't decrypt the EncryptedAssertion of a SAML response