SLO: Single Log-out

Inedible cookies, sticky sessions and false hopes

SWITCH

Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Zurich, 5. May 2009

From the shib-users mailinglist

[…] I was going through the documents and haven't come across the steps for implementing SLO in shibboleth. Is it possible. If yes then how ?

[…] I've been reading th
lists archives a
Shib

I
a
a

d how the global logout is
d on shibboleth.
w can I spread the logout on all idp of the federation ?

Answer:
Yes, Logout will be possible
but it has a lot of limitations!

[…] So when I go back to my Google Apps, I am still logged in.

Usability and user experience issues?

What does a user expect when clicking on logout?

- Logout only from this single application?
  - Is of little use because of Single Sign On
- Logout from all applications where logged in? Which?
  - Also from Google Mail, eBay and other non AAI applications?

Therefore:

- User must understand consequences of logout
  - Must know that he currently is signed in to a single sign-on (SSO) system and what will result from clicking on logout
- User must always know if logout has completely succeeded
  - Otherwise they may assume that it has and leave the computer allowing some one else to erroneously access a service

Basics: Logged in vs Logged out

What defines if a user is logged in via AAI/application?

- 🍪 Shibboleth session cookie
- 🍪 Application session cookie (optional)
  - Some application only check if user was authenticated via AAI

What is necessary to log out a user?

- Delete Shibboleth and application cookies (front-channel)
  - Only possible when user’s browser is involved
    → Administrative logout not possible
- Or delete session information on server (back-channel)
  - Only possible if user’s Shibboleth sessionID is known in application
    → Implies adaptation of application

The two flavors of logout

Local logout

- User’s session is deleted only for one Service Provider
  - Not of much use due to Single Sign-On (SSO)
  - Or “egoistic” if IdP session also is bilaterally deleted but all other SP’s session are still intact.

Global logout = Single Log Out (SLO)

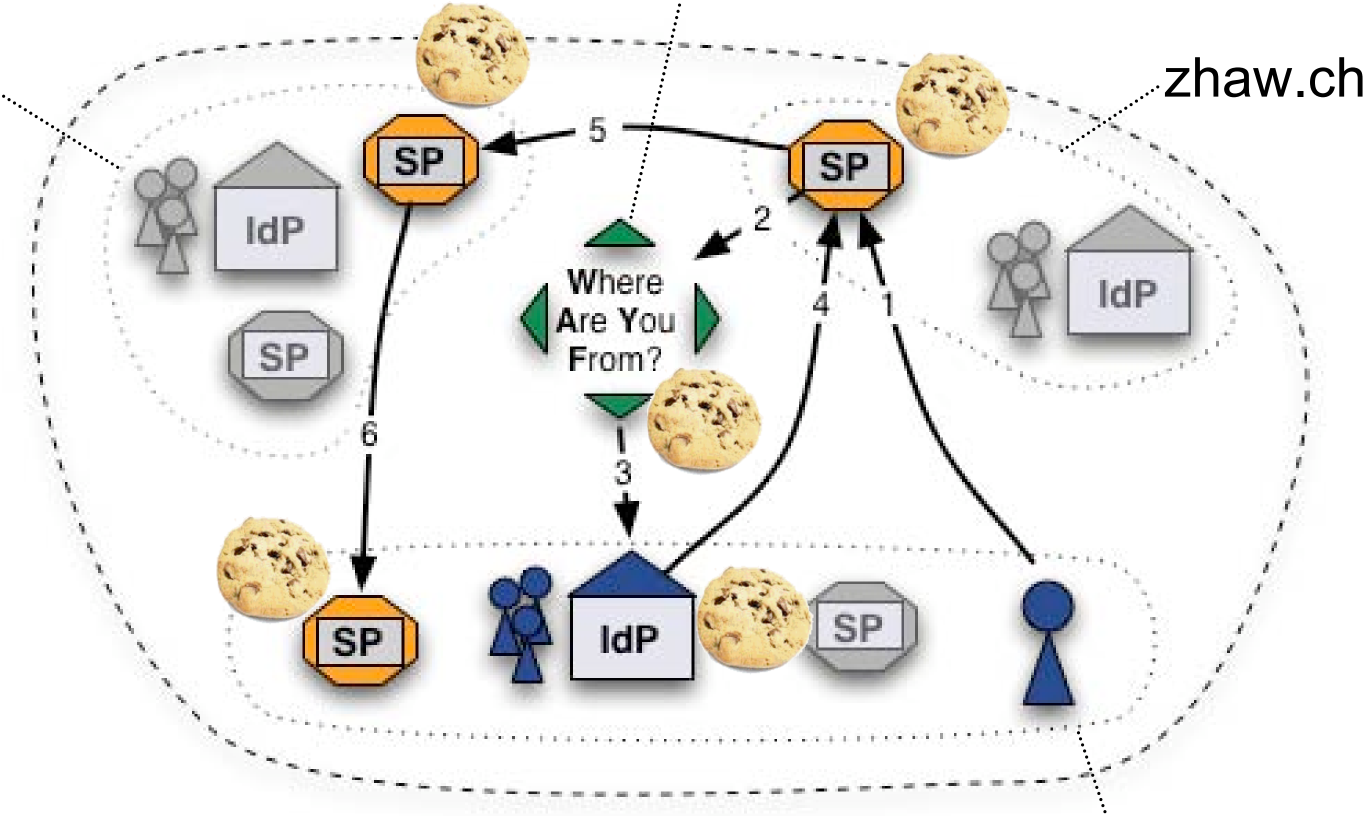
- User’s SSO session deleted on IdP and **all** SPs
  - For authentication methods like HTTP Basic Auth or some external authentication systems, the IdP cannot destroy the SSO session!
    - ❑ Only safe way for logout is to close the web browser!

Example SLO Scenario

wayf.switch.ch

ethz.ch

zhaw.ch



uzh.ch

- 5 AAI Sessions = 5 AAI Cookies
  - 1 at IdP (uzh.ch)
  - 3 at SPs (zhaw.ch, ethyz.ch, uzh.ch) but applications also have a cookie…
  - 1 at WAYF/DS (wayf.switch.ch)

How to get rid of sessions?

- SP “just” needs to delete all cookies that identify session
  - Impossible for Service Provider because cookies probably are for different domains or hosts

- Redirect browser to each SP, IdP and WAYF in order to delete cookies (front-channel logout)
  - What happens if one host is down? User is stranded

- Use IFRAMES to send browser to all components
  - Solves some of the technical issues but administrative logout (force logout of a malicious user) still is not possible

Current state of SLO in Shibboleth

SLO requires:

- SAML 2 (Shibboleth 2)
- built-in username/password authentication method (no CAS!)

- **Shibboleth Service Provider 2.1**
  - Supports local and global logout
- **Shibboleth Identity Provider 2.1/2.2**
  - Support neither local nor global logout
  - Development will probably start soon

- **Adapted Applications:**
  - Worldwide there are less than 10 applications that already are ready to support SAML 2 logout (incl. Moodle, ILIAS, Resource Registry)

But nevertheless…

… Single Logout most probably will be arriving in one of the next Identity Provider releases this year.

(Probably 2.3)

BUT with quite a few …

… Technical Limitations

SLO will work only for:

- Shibboleth 2 SPs/IdPs (SAML 2 required)

- Some of the built-in authentication systems at IdP
  - Basically, only the built-in UsernamePassword handler…
  - No CAS, pub-cookie, X509, HTTP Basic Auth will work

- Service Providers must have configured <Notify>
  - To inform application of logout via back-channel

- Adapted web applications via back-channel requests
  - This involves some work on your side …

Preparing application for logout

- **Either solely rely on SP's session management or …**
  - No own session management in application
  - Also has advantage of consistent session timeout

- **adapt application with session index and callback script**
  - Application needs to know which application session needs to be deleted getting only a Shibboleth SessionID as input
  - User's cookie still will exist but cannot be mapped anymore to a local session on server ⇒User is logged out
  - Example PHP script on:

    🌍 https://spaces.internet2.edu/display/SHIB2/NativeSPNotify

  - Already implemented for Resource Registry, Moodle, ILIAS

(Sad) Conclusion

Single Logout will work only in some cases reliably!

The only safe ways to log out from all applications are:

- to **delete all session cookies**
  - Have fun explaining an average user how to to this with his browser
  - Won’t log you out if authenticated via Basic Auth, X.509 certificates, …
- or the recommende way: **close the web browser**!
  - Quickest, most reliable and easiest way to explain
  - Also logs users off from PayPal etc. :-)
- In detail:

https://spaces.internet2.edu/display/SHIB2/SLOIssues