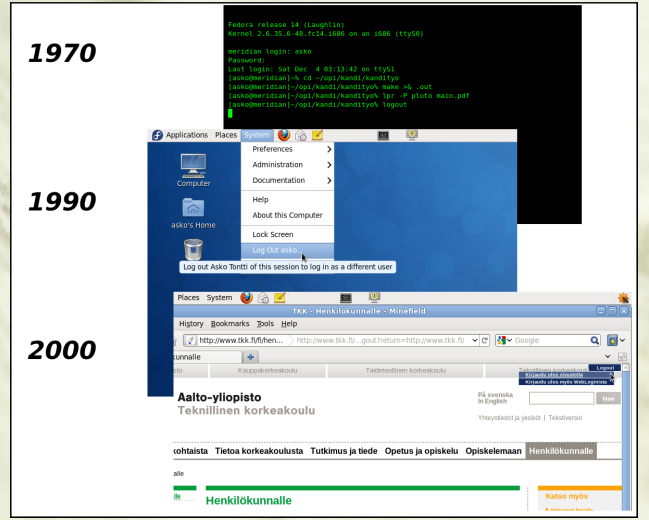
Uloskirjautuminen Shibbolethissa

Tunnistaminen Internetissä

Asko Tontti

7. - 9.12.2010 kandidaatinseminaari

Johdanto


1970
1990
2000
Fedora release 14 (Laughlin)
Kernel 2.6.35.6-48.fc14.i686 on an i686 (tty50)
meridian login: asko
Password:
Last login: Sat Dec 4 03:13:42 on tty51
[asko@meridian]~% cd ~/opi/kandi/kandityo
[asko@meridian]~/opi/kandi/kandityo% make >& .out
[asko@meridian]~/opi/kandi/kandityo% lpr -P pluto main.pdf
[asko@meridian]~/opi/kandi/kandityo% logout
Applications Places System
Preferences
Administration
Documentation
Help
About this Computer
Lock Screen
Log Out asko...
Computer
asko's Home
Log out Asko Tontti of this session to log in as a different user
Places System
TKK - Henkilökunnalle - Minefield
History Bookmarks Tools Help
Aalto-yliopisto
Teknillinen korkeakoulu
Tietoa korkeakoulusta
Tutkimus ja tiede
Opetus ja opiskelu
Opiskelemaan
Henkilökunnalle
Katso myös

Johdanto

- Palvelut ja sovellukset siirtyvät kiihtyvää vauhtia Internetiin
- Tunnistautumisesta on tullut tärkeämpi osa palveluita
  - Käyttäjien hallinta
  - Kertakirjautuminen (Single Sign-On, SSO)
  - Uloskirjautuminen
- Uloskirjautuminen ei ole yksinkertaista WWW-palveluissa
  - Tulemme näkemään: vielä olisi paljon tehtävää

SAML ja Shibboleth

- Security Assertion Markup Language (SAML)
  - Standardi tapa: organisaatiorajat ylittävä tunnistaminen
  - SAML 2.0 on nykyinen versio
  - http://saml.xml.org/
- Yliopistomaailmasta SAML2-pohjainen Shibboleth
  - TKK ja Haka-luottamusverkosto
  - http://shibboleth.internet2.edu/
- Shibbolethin komponentit
  - Identity Provider (IdP): tunnistustietojen tarjoaja
  - Service Provider (SP): palveluntarjoaja

Uloskirjautumisen ongelmia

- WWW:ssä käytetty HTTP-protokolla on tilaton
- Selaimet ja palvelut simuloivat tilallisuutta
  - Evästeet ja URL:t
  - Istunto: käyttäjää koskevat tilatiedot
- Uloskirjautuminen: tilan purkaminen
  - Pitää tapahtua luotettavasti ja turvallisesti
  - Muuten joku muu voi päästä käyttämään istuntoa
- Tietoturva ...

Tietoturva uloskirjautumisessa

- Käyttäjä voi esiintyä toisena henkilönä
  - Vahingossa tai tahallaan
  - Ongelmana erityisesti yhteiskäyttöisten tietokoneiden kanssa
- Suurin riski: SSO-istunnon väärinkäyttö
- Yksittäinen palvelu voi myös olla merkittävä riski
  - Esimerkiksi rahaa ja henkilötietoja käsittelevät palvelut

Uloskirjautumisen muodot

- Sovelluksen uloskirjautuminen
- SP:n uloskirjautuminen
- IdP:n uloskirjautuminen (SSO-istunto)
- Paikallinen uloskirjautuminen (Local Logout)
- Kertauloskirjautuminen (Global Logout, Single Logout, SLO)
- Osittainen uloskirjautuminen (Partial Logout)

Käytännössä

- Paikallinen: Sovellus + SP
- Kerta: Sovellukset + SP:t + IdP

Hakan ja SAML2:n uloskirjautuminen

- Hakan uloskirjautuminen
  - Shibboleth 1.x ei tue uloskirjautumista
  - Yleensä osittainen uloskirjautuminen
  - Ohje: Sulje WWW-selain
- SAML2:n uloskirjautuminen
  - Hauras ja monimutkainen
  - Shibboleth SP 2.x tukee, mutta IdP 2.x ei tue
- Vaihtoehdot epäyhteensopivat

Uloskirjautuminen käytännössä

- Tutustuimme TKK:lla paljon käytettyihin WWW-palveluihin
  - Nelliportaali, http://www.nelliportaali.fi/ (Haka)
  - Noppa, https://noppa.tkk.fi/
  - Oodi, https://oodi.aalto.fi/
  - Aalto Wiki, https://wiki.aalto.fi/ (Haka)
  - TKK:n henkilökuntasivut, http://www.tkk.fi/
- Tulos: Uloskirjautuminen ei toimi yhtenäisellä tavalla palveluissa

Yhteenveto tuloksista

	Menetelmä	Istunnot				Toimii
		Sovellus	SP	SSO	Muut SP:t	
Nelliportaali	Haka SLO	°	✓	✓	† °	ei
Noppa	Haka SLO	✓	✓	✓	† °	OK 1
Oodi	paikallinen	✓	°	°	°	ei
Wiki	SAML2 SLO	✓	✓	°	°	ei 2
Henkilökuntasivut	paikallinen	✓	✓	°	°	OK 3
	Haka SLO	✓	✓	✓	† °	

° istunto jää auki; ✓ istunto lopetettu; † ohje sulkea selain

1 kielivalinta vuotaa; 2 yhteensopivuusongelma

3 käyttäjä voi valita, mutta ymmärtääkö hän vaihtoehtojen eron?

Ratkaisuja havaittuihin ongelmiin

- Käyttöliittymät ja käyttäjien koulutus
- Sovelluksen muokkaus
- Kirjautumisen tilatiedot ja uloskirjautuminen
- CoSign-ohjelmiston erilainen näkökulma
- WWW-selaimissa evästeiden hallinnan kehittäminen
- Uusien WWW-tekniikoiden hyödyntäminen, esimerkiksi AJAX
- Yhtenäiset testauskäytännöt

KISS

Keep It Simple, Stupid!

Johtopäätökset

- Paras vaihtoehto: SAML-standardointityön jatkaminen
    - SAML2:n uloskirjautuminen on hauras ja monimutkainen
- HTML5:n standardointityö: evästeiden hallinnan kehittäminen
- Luottamusverkostoissa uloskirjautumisen ja testauksen painottaminen

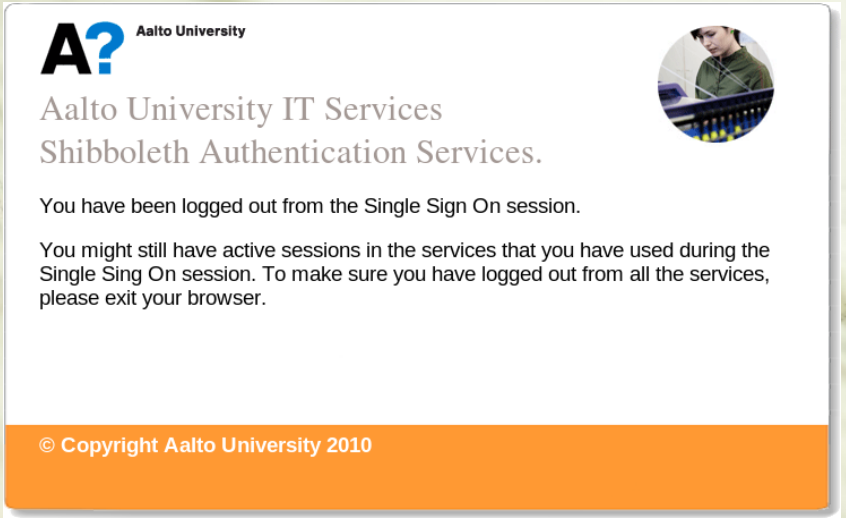
Merkittävimmät

Standardointityö ja testauskäytännöt

Yhteenveto

- Uloskirjautumisen toimiminen entistä tärkeämpää
- SAML2 on laajasti käytetty standardi tunnistautumisessa
- HTTP on tilaton, tilaa simuloidaan evästeillä
- Uloskirjautuminen ei toimi yhtenäisellä tavalla palveluissa
- Ratkaisuja: käyttäjien koulutus, käyttöliittymät, sovellusten muokkaus, evästeiden hallinta, istuntojen hallinta AJAX:lla, testaus ja standardointityö
- Johtopäätökset: tärkeimmäksi nousevat standardointityö ja testauskäytännöt

Logout


Aalto University
Aalto University IT Services
Shibboleth Authentication Services.
You have been logged out from the Single Sign On session.
You might still have active sessions in the services that you have used during the Single Sing On session. To make sure you have logged out from all the services, please exit your browser.
© Copyright Aalto University 2010