



Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:

Tuottajat

Ratkaisu

Ryhmät

Ongelma 2:

Sovellukset

Pääsylippu malli

MatTaFi projektin HAKA-pilotti

Matti Harjula

`matti.harjula@hut.fi`

Matematiikan ja systeemianalyysin laitos
Teknillinen korkeakoulu

15. tammikuuta 2008



Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:

Tuottajat

Ratkaisu

Ryhmät

Ongelma 2:

Sovellukset

Pääsylippu malli

1 Taustaa

2 Materiaalin tuottajat ongelmana

- Ratkaisu
- Ryhmät

3 Uusien sovellusten yksinkertaisempi kytkeminen

- Pääsylippu malli



MatTaFi projekti

Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:
Tuottajat

Ratkaisu
Ryhmät

Ongelma 2:
Sovellukset

Pääsylippu malli

- **Matematiikkaa** tietokoneavusteisesti kansallisesti \approx MatTaFi.
- Käytännössä verkko-oppimateriaaleja. Harjoitustehtäviä ja teoriaa verkossa. Kaikkea MathML esityksistä hyperkuutioiden pyörittely appletteihin.
- 5 yliopistoa ja 5 ammattikorkeakoulua. TKK, HY, TY, TAY, JOY, Stadia, TAMK, VAMK, Savonia-AMK, RAMK.
- Ideana kerätä tuotettua materiaalia yhteen paikkaan kaikkien käytettäväksi. Ja tarjota tukea teknisissä ratkaisuissa.



Paljon väkeä paljon ongelmia

Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:

Tuottajat

Ratkaisu

Ryhmät

Ongelma 2:

Sovellukset

Pääsylippu malli

- Materiaalin kerääminen yhteen paikkaan ei varsinaisesti ole ongelma, mutta sen muokkaus myöhemmin on.
- Tuottajien ja ylläpidon välillä käsittämätön määrä turhaa viestintää. Lisäksi viestinnän määrä nostaa kynnystä lähettää materiaalia.
- Tuottajille haluttaisiin antaa suoraan käyttöoikeudet, mutta oikeuksien hallinta organisaatioiden välillä. . .
- Lisävaikeustasona osa materiaalista halutaan pitää piilossa. Esim. vastaukset opiskelijoilta ja tehtävät maailmalta. . .



Lobby-portaali 1/2

Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:
Tuottajat

Ratkaisu
Ryhmät

Ongelma 2:
Sovellukset

Pääsylippu malli

- Portaali sivusto, jonka sivut ovat suoraan editoitavissa selaimen kautta.
- Käyttöoikeudet HAKA tunnusten ja attribuuttien perusteella.
- Erityisesti käyttäjäryhmien hallintaan panostettiin. Tavoitteena on että projektin kaikkien käyttäjäryhmien hallinta siirtyy portaaliin.
- Muina ominaisuuksina lokalisaatiota, matemaattisten kaavojen renderöintiä sekä hiukan RSS/blogi ominaisuuksia.



Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:
Tuottajat

Ratkaisu
Ryhmät

Ongelma 2:
Sovellukset

Pääsylippu malli

- Apache serveri. Postgres kanta.
- `mod_python` ja sen päällä Django¹ sovelluskehys.
- `mod_shib` paljastaa attribuutit Apachen serveri muuttujiin ja ne näkyvät suoraan Djangoon.
- Django valittiin lähinnä ominaisuuksien vuoksi. ORM, I18N ja sopivasti rajapintoja muokkausta varten. Djangoon valmiit ylläpitosivut olivat tietenkin suurin syy.

¹djangoproject.com



Käyttäjärühmien määrittely

Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:
Tuottajat

Ratkaisu
Ryhmät

Ongelma 2:
Sovellukset

Pääsylippu malli

Portaalin ryhmät määritellään täysin HAKA attribuuttien perusteella. Tällä hetkellä käytetään opiskelijanumeroa² ja käyttäjätunnusta³ jatkossa laajennetaan ehkä muihin attribuutteihin. Käytännössä näiden perusteella rakennetaan ehdot sille ketkä kuuluvat ryhmään. Esim:

- `op#=57591C AND id=*@hut.fi` tai `id=aharjula@hut.fi` kuvaa minut.
- `id=a*` OR `id=b*` poimii käyttäjiä (harjoitus)ryhmään tunnuksen alkukirjaimen mukaan.
- `id=aharjula@*...`
- `id=*` on tietenkin joskus tarpeen.
- Käytännössä ehdot saadaan nopeasti ja automaattisesti muodostettua ilmoittautumislistoista.

²`urn:mace:terena.org:schac:attribute-def:schacPersonalUniqueCo`

³`urn:mace:dir:attribute-def:eduPersonPrincipalName`



Käyttäjiryhmät...

Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:

Tuottajat

Ratkaisu

Ryhmät

Ongelma 2:

Sovellukset

Pääsylippu malli

- Ryhmien muokkaus edellyttää kuulumista ryhmän muokkaamisesta vastaavaan ryhmään. Opettajalle voidaan siis antaa oikeus virittää omia ja vain omia ryhmiään.
- Käyttäjät voivat tietenkin kuulua useaan ryhmään.
- Ryhmiin voidaan liittää parametreja, jotka välitetään sivuille ja sovelluksille käyttäjän tietojen mukana. Esim. sovelluksen admin-ryhmä eroaa muista ryhmistä lähinnä parametrien suhteen.



Muut sovellukset

Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:

Tuottajat

Ratkaisu

Ryhmät

Ongelma 2:

Sovellukset

Pääsylippu malli

MatTaFi projekti tuottaa ja ylläpitää erinäisiä verkkosovelluksia, jotka tarvitsevat autentikaatiota ja käyttäjien hallintaa.

Portaalista on tarkoitus tehdä etusivu näihin sovelluksiin.

- Tyypillisesti sovellukset ovat avointa lähdekoodia, mutta näin ei aina ole.
- Useimmiten kyseessä on PHP-sovellus ja kytkeminen Shibbolethiin on siten helppoa, mutta kun vastaan tulee jotain joka ei pyöri Apachen päällä tilanteesta tulee mielenkiintoinen.
- Käyttäjien hallinta näiden sovellusten kesken haluttaisiin yhtenäistää ja siirtää portaalin.
- Siispä sovellukset ”upotetaan” portaaliin ja portaali hoitaa autentikoitumisen.



Sovellusten kytkentä portaaliin

Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:

Tuottajat

Ratkaisu

Ryhmät

Ongelma 2:

Sovellukset

Pääsylippu malli

- Vältetään kaikki mahdolliset ongelmat sovelluksen ja Shibbolethin kytkennässä, ei kytketä niitä toisiinsa ollenkaan.
- Shibbolethin portaalille kertomat attribuutit välitetäänkin sovellukselle XML-tiedostossa, serverin tiedostojärjestelmän kautta. Jos sovellus pyörii eri serverissä niin NFS auttaa tilanteeseen.
- Portaali ohjaa käyttäjän sovellukseen HTTP redirectillä, jossa kerrotaan samalla sovellukselle mistä satunnaisesti nimetystä tiedostosta käyttäjän tiedot haetaan. Välimieshyökkäys on riski, mutta SSL turvaa tilannetta muuten.
- Oli sovelluksen ohjelmointikieli mikä tahansa sille löytyy XML-parseri ja jos ei niin tekstitiedoston lukeminen on ainoa tekninen vaatimus.



Pääsylippu

Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:

Tuottajat

Ratkaisu

Ryhmät

Ongelma 2:

Sovellukset

Pääsylippu malli

Välitettävä tiedosto toimii siis pääsylippuna sovellukseen ja pääsylippujen väärentäminen vaatii pääsyä tiedostojärjestelmään. Toisen henkilön lipun käyttäminen vaatii välimieshyökkäystä tai oikeaa arvausta täsmälleen oikealla hetkellä. Lippujen turvana on:

- Lyhyt voimassaoloaika. Eli ryöstö pitää tehdä nopeasti, alle 5min aikaa.
- Kertakäyttöisyys. Kun käyttäjä on käyttänyt lipun se tuhotaan, eli pitää ehtiä väliin ennen kuin redirecti portaalista sovellukseen ehtii perille.
- Isoja satunnaislukuja eri generaattoreista. Todennäköisyydet arvata äärimmäisen pieniä ellei tiedä generaattorien tilaa ja tyyppiä, sekä kellonaikaa.



Lobby

MatTaFi

Sisältö

Taustaa

Ongelma 1:

Tuottajat

Ratkaisu

Ryhmät

Ongelma 2:

Sovellukset

Pääsylippu malli

The End