

Julkisten pääsyalueiden välinen verkkovierailu

TTKK/Tietoliikennetekniikan laitos

Sami Keski-Kasari

samikk@cs.tut.fi

Karri Huhtanen

karrih@cs.tut.fi

Taustaa

- Lisääntyvät WLAN- ja pääsyaluepalvelut vaativat käyttäjän autentikointia
- Projektihenkilökunnan, luennoijien ja opiskelijoiden liikkuvuus aiheuttaa haasteita
 - Luentosaleissa ja kokoustiloissa tarvittavat verkkoyhteydet vaativat käyttäjätunnuksien jakoa -> työllistää ylläpitoa
 - Erilaiset autentikointitavat sekoittavat käyttäjiä ja saattavat vaatia käyttäjiltä erillisiä ohjelmia

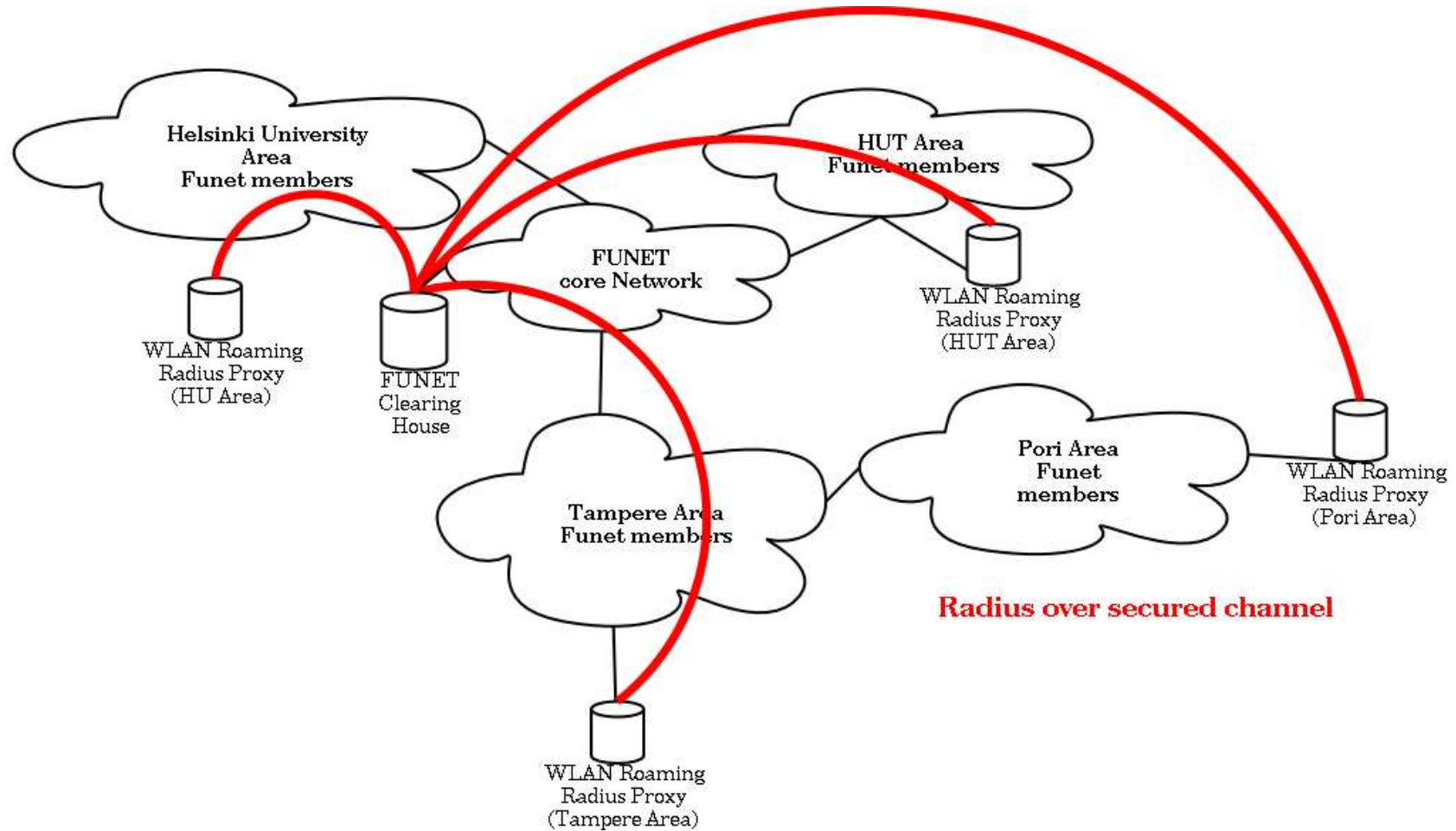
Taustaa

- Yhteisellä rakenteella ja käyttäjätunnistusmenetelmillä mahdollista hyödyntää käyttäjän kotiverkon autentikointipalvelimia
 - Ylläpidon työmäärä vähenee
 - Käyttäjät saavat suuremman pääsyalueen
 - Palveluiden käyttö helpottuu

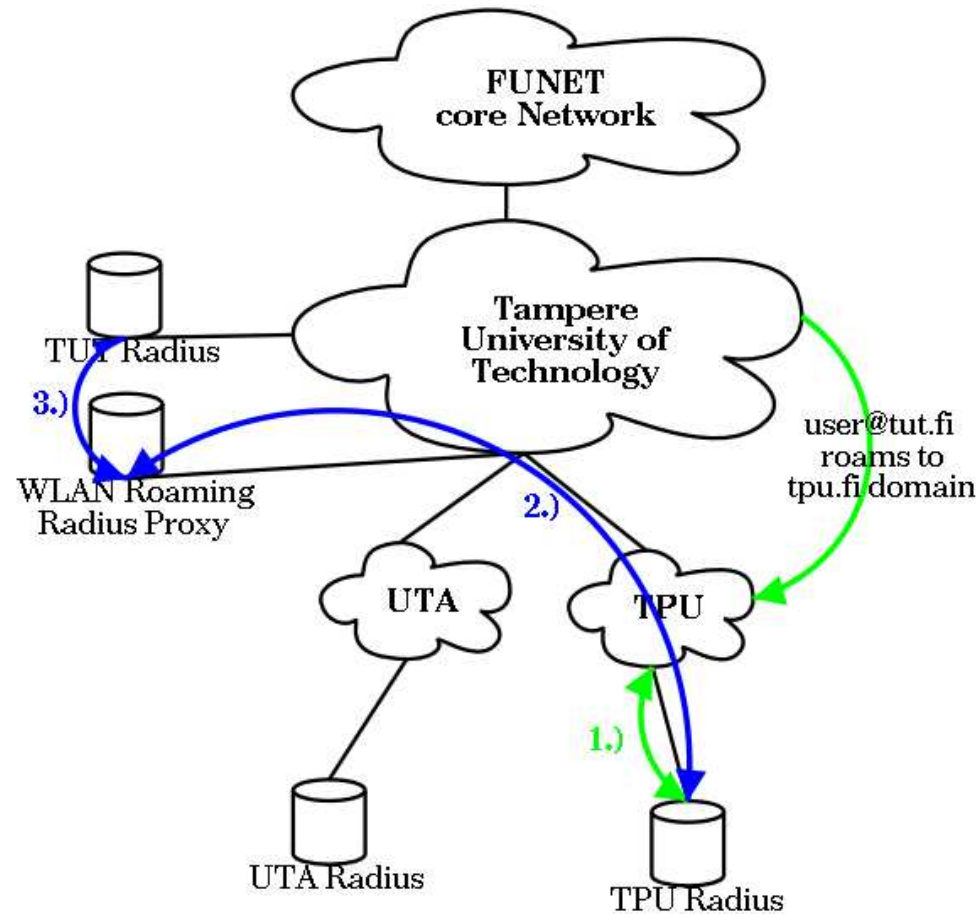
Teoria

- Mahdollista toteuttaa RADIUS-protokollan proxy-toiminnolla
 - Käyttäjätunnus muotoa username@realm
 - Realmien perusteella ohjataan autentikointipyyntö oikealle RADIUS-palvelimelle
 - Toimii kaikilla toteutuksilla, jotka käyttävät RADIUS:ta autentikointiin
 - RADIUS-protokollalla mahdollista kerätä tilastotietoa, jolloin käyttäjä voidaan tarvittaessa jäljittää

Esimerkki hierarkiasta



Alueellinen verkkovierailu

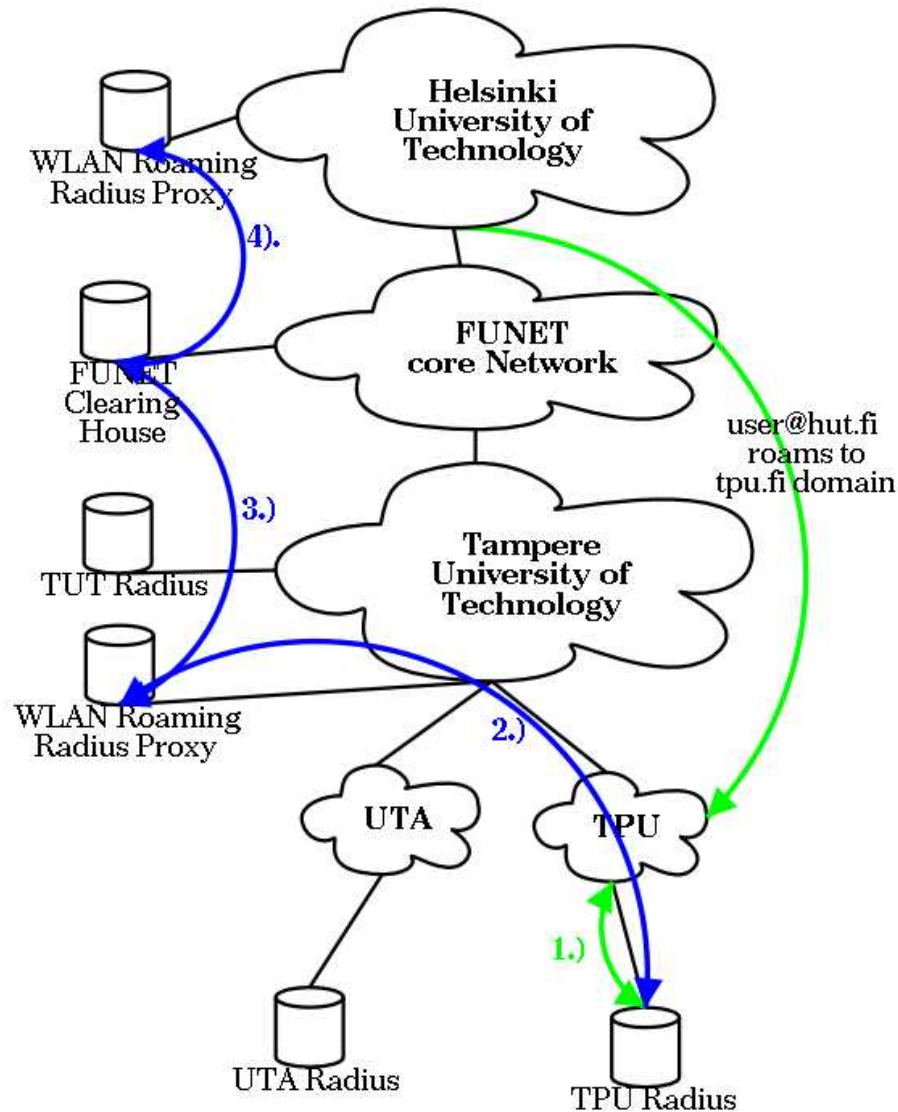


1.) Public Access Authentication System sends username user@tut.fi and password to TPU Radius.

2.) TPU Radius distinguishes the domain tut.fi from username. This is not a local domain, so TPU Radius forwards request to WLAN Roaming Radius Proxy

3.) WLAN Roaming Radius Proxy forwards the TPU Radius request to domain handling tut.fi domain i.e. TUT Radius. The response to authentication request is transmitted back via the same route as the requests.

Eri alueiden välinen verkkovierailu



1.) Public Access Authentication System sends username `user@hut.fi` and password to TPU Radius.

2.) TPU Radius distinguishes the domain `hut.fi` from username. This is not a local domain, so TPU Radius forwards request to WLAN Roaming Radius Proxy

3.) WLAN Roaming Radius Proxy forwards the TPU Radius request to the FUNET clearing house.

4.) FUNET Clearing House knows all WLAN roaming domains and their respective WLAN Roaming Radius Proxies. The FUNET Clearing House forwards the Radius request to the WLAN Roaming Radius Proxy handling `hut.fi` domain.

The response to authentication request is transmitted back via the same route as the requests.

Autentikointi ja sen tietoturva

WWW-pohjainen

- Laite on jo jollain tasolla verkossa
- HTTPS pakollinen tietoturvan saavuttamiseksi
- Hop-by-Hop tietoturva
- Vaatii selaimen
- Toimii normaali RADIUS-palvelimen kanssa

IEEE 802.1X

- Portti/Virtuaaliportti-kohtainen autentikointi
- EAP ja tunneloidut EAP variaatiot mahdollistavat end-to-end tietoturvan
- Vaatii tuen käyttäjän laitteelta
- Vaatii tuen RADIUS-palvelimelta

Tarvittava laitteisto

- Normaali RADIUS-palvelin riittää, koska proxy-ominaisuus on rfc:ssä määritelty, mahdollisesti tarvitaan IEEE 802.1X tuki.
- Proxy-moodissa toimivat RADIUS-palvelimet mahdollisimman yksinkertaisia
- ”Äly” sijaitsee jokaisen organisaation RADIUS-palvelimessa, esim. IEEE 802.1X.
- Alueelliset proxy-palvelimet esim. FUNET:n POP:eissa.
- FUNET Clearing House Proxyn avulla yhdistetään Euroopan verkot FUNET-verkkoon

Muita saavutettavia etuja

- Tilastotiedon keräys, jota voi myöhemmin käyttää muuhun tutkimukseen
 - Verkkovierailevien käyttäjien määrä
 - Yleisimmin vierailut kohteet
 - Käyttäjäprofiilit
- Mahdollista myöhemmin soveltaa operaattoriympäristöön

Tilanne tällä hetkellä

- Suomessa
 - Testiyhteys TTKK:n ja WirLab:in (sjoki.uta.fi) välillä toiminnassa.
- Euroopassa
 - SURFnet ja UNINETT rakentamassa verkkojaan samalla menetelmällä.
 - Tarkoitus olisi TERENA:n puitteissa luoda testiyhteys ainakin SURFnet:n ja TTKK:n välille.

Tulevaisuus

- Autentikoituminen mahdollista myös HST-kortilla
- Mahdollista luoda Euroopan-laajuinen pääsyverkko
 - Missä tahansa Euroopassa liikkuesssa tietää pääsevänsä sähköposteihinsa/Internetiin kiinni menemällä lähimpään yliopistoon

Keskustelua

- Löytyykö FUNET:n jäsenorganisaatioista mielenkiintoa aiheeseen?
- Poliittisia ongelmia?
- Juridisia ongelmia?
- Toteutuksellisia ongelmia?
- Muita ongelmia?
- Jatko?