NETGEST

Network Identity, Grid-Enabled Services and Trust Networks

Mika Mustikkamäki, Juhani Niemelä

1. Network Identity -työpakettiin kontribuointi

NoCatAuth-ohjelmiston jatkokehitys WPKI-autentikointia varten, sekä RADIUS/WPKI -ympäristön integraatio ja konseptointi.

Network Identity -työpakettiin suunnattiin Wirlabin toimesta suurin yksittäinen panostus. Jo ennalta tutut teknologiat (SIP, RADIUS) nähtiin NetGest-projektinkin kannalta tärkeinä osa-alueina - RADIUS eritoten autentikoinnista, autorisoinnista ja mahdollisesta laskutustiedon keräämisestä puhuttaessa. RADIUS-protokollan sijoittuminen tämän päivän toimintakenttään operaattoreiden monipalveluisissa verkoissa on oleellinen ajuriprotokollan tukemisessa eri palveluissa edelleen.

Wirlabin aiemmassa tutkimuksessa saadut positiiviset kokemukset RADIUS-palveluiden toteuttamisessa ja soveltamisessa rohkaisivat tuomaan RADIUS-protokollan mukaan tutkimukseen myös Grid-palvelujen sovelluksena. Projektissa hyödynnetyssä NoCatAuth-palvelinohjelmistossa oli kehityskelpoinen RADIUS-tuki mukana, joten se nähtiin oivalliseksi alustaksi jatkokehitykselle. Lisäksi NoCatAuth vaikutti huomattavan vakaalta, ja tämä olettamus vahvistui myös kehitystyön kuluessa.

2. RADIUS/WPKI-autentikoinnin taustaa

Uudet tietoverkkoteknologiat mahdollistavat tänä päivänä hienojakoisen käyttäjien tunnistuksen verkkoihin liityttäessä. Teknologia nimeltä 802.1X toi (virtuaali)porttikohtaisen käyttäjien autentikoinnin niin langallisiin kuin langattomiinkin verkkoihin, ja esitteli samalla myös RADIUS-protokollan käytön autentikointimenetelmänä. Aiemmin RADIUS:ta oli käytetty pääasiassa modeemikäyttäjien autentikointiin, mutta protokolla sopii erittäin hyvin myös 802.1X:n kumppaniksi. RADIUS:ta tuetaan laajalti ja se on helposti laajennettavissa oleva protokolla.

802.1X ja RADIUS ovat nousseet keskeisiksi Wirlab Network Research Centerin tutkimuksessa, ja WPKI-teknologian soveltaminen langattomiin lähiverkkoihin ja niiden autentikointitapoihin nähtiin luonnollisena jatkumona aiemmin kertyneen tutkimustiedon kumuloitumisessa.

Viimeisen vuoden sisällä mobiililaitteissa on yleistynyt WIM-teknologia (WAP/Wireless Identity Module). Se mahdollistaa sertifikaatteihin perustuvan käyttäjien tunnistuksen ja verifioinnin erilaisiin mobiiliverkon palveluihin WIM mahdollistaa kuitenkin helposti myös cross-over palvelut perinteisen IP-verkon autentikointimenetelmien kanssa erityisten yhdyskäytävätuotteiden välityksellä. Eräs tällaisista tuotteista on Valimon Validator, ja siihen liittyvä RADIUS-autentikointimoduli. Sertifikaatit ovat henkilökohtaisia, ja ne tallennetaan erityiselle SIM-kortille, jonka nimitys vaihtelee operaattorikohtaisesti. NetGest-projektissa käytettiin Radiolinjan (nyk. Elisa) SWIM-kortteja (Secure Wireless Identity Module).

Ajatus RADIUS/WPKI-integraatiosta perustuu siihen, että käyttäjät voivat liittyä langattomiin lähiverkkoihin ja autentikoida itsensä antamatta salasanaa WWW-autentikoinnin yhteydessä. WPKI-autentikoinnin tarve tunnistetaan käyttäjätunnuksen domain-osasta ja välitetään mobiiliverkkoon. Käyttäjä verifioi kirjautumisensa henkilökohtaisella WPKI-PIN-koodillaan, joka vastaa normaalia käyttäjätunnus-salasanaparin salasanaa. Näin autentikoinnissa välitettävä salasanatieto voidaan turvata mobiiliverkon tarjoamilla tekniikoilla ja IP-verkossa eri palvelimien välillä välitettävä tieto on ei-sensitiivistä käyttäjätunnus-informaatiota.

3. NoCatAuth:in RADIUS- ja WPKI-kehitystyö

NoCatAuth:in tuki RADIUS-protokollalle oli aloitusvaiheessa hieman hajanainen. Tiettyjä ominaisuuksia oli toteutettuna, mutta osa niistä oli bugisia ja/tai keskeneräisiä. Lisäksi laskutustiedon keräämiseen käytettävä, IETF RFC 2866:den mukainen RADIUS accounting –toiminnallisuus oli kokonaan toteuttamatta. Koodia korjattiin ja verkosta löytyneitä patch-tiedostoja tuotiin ohjelman koodiin soveltuvin osin. Jokainen muutos testattiin erikseen, jotta voitiin olla varmoja kokonaisuuden toimivuudesta.

NoCatAuthin RADIUS-osuuteen tehtiin myös muita muutoksia. Tiettyihin domain-osiin päättyvät käyttäjätunnukset (.wpki, eli WPKI-autentikoinneissa käytetyt tunnukset) käsiteltiin eri tavoin ja niille ei suoritettu lainkaan accounting-tiedon keräämistä. Autentikointitiedot välittävälle RADIUS-palvelimelle, eli ns. RADIUS-proxy:lle WPKI-autentikointidomainit määriteltiin omana autentikointikäsittelijällä, mikä mahdollisti usean autentikointimenetelmän hoitamisen samalla proxy-palvelimella. Täten normaalit RADIUS-kyselyt voitiin autentikoida paikallisesti ja .wpki -päätteiset tunnukset ohjattiin autentikointia varten Valimon Validator -palveluun ja sieltä edelleen matkapuhelinoperaattorin verkkoon.

4. Integrointi ja konseptointi

RADIUS/WPKI-integraatio oli parannetulla NoCatAuth-palvelimella ja Valimon projektin käyttöön luovuttamalla Validator-palvelulla, sekä tarvittavilla mobiililaitteilla ja WPKI-SIM:eillä toteutettavissa. RADIUS-protokollan käyttö IP-verkkoon liittyvän asiakkaan

autentikoinnissa on tällä hetkellä yhteensopivin ja laajennettavin autentikointikonsepti. WPKI-varmenteiden käyttö mobiililaitteilla on myös tarpeeksi sujuvaa onnistuneen autentikointiprosessin aikaansaamiseksi.

Suurin osa RADIUS/WPKI -autentikointipalvelun konseptoinnin onnistumiseen vaikuttavista tekijäistä liittyy RADIUS- ja WPKI-autentikointipalvelimien oikeaan konfigurointiin ja palvelualustan mahdollisimman tarkkaan tuntemukseen.

Kun ns. RADIUS-edustapalvelin ottaa vastaan ensimmäisen autentikointipyynnön, välittää sen RADIUS-proxylle joka puolestaan välittää viestin edelleen Validatorille, ja tämä mobiiliverkkoon, autentikointisanoman vastineen saapumiseen vaikuttaa monta viivästyttävää tekijää. Suurin yksittäinen muuttuja on mobiililaitteen käyttäjän näppäilynopeus WPKI-varmenteen vastaanotossa ja kuittaamisessa. Testien mukaan RADIUS-edustapalvelimen on syytä odottaa ainakin 90 sekuntia ennen uudelleenlähetyksen aloittamista. Tässä ajassa alkuperäinen RADIUS-pyyntö on ehtinyt WPKI-yhdyskäytävälle, sieltä muunnettuna mobiiliverkkoon ja -laitteeseen ja käyttäjän allekirjoittamana takaisin.

Projektissa toteutetun palvelun tuominen olemassa oleviin ns. Public Access -langattomiin lähiverkkoihin olisi mahdollista nopeasti. Koska WLAN-operaattorit ovat toiminnallaan joka tapauksessa rajanneet suuren osan PA-verkkojen käyttäjistä business-käyttäjiin, ei WPKI-kykyisten mobiililaitteiden levinneisyyskään olisi pitkäkestoinen ongelma. Esimerkiksi suurin osa Nokian business-puhelinmalleista tukee "langaton lompakko" -ominaisuutta. WPKI-SIM:in vaihtaminen vanhan SIM-kortin tilalle on maksutonta. Koska RADIUS-viesteissä ei kulje sensitiivistä tietoa, autentikoinnin tietoturva hoituu kokonaan mobiiliverkon puolella. Puoltavia asioita löytyy runsaasti.

Viitteet

IEEE 802.1X: http://grouper.ieee.org/groups/802/1/pages/802.1X-rev.html
IETF RADIUS: http://www.ietf.org/rfc/rfc2865.txt?number=2865 ja
http://www.ietf.org/rfc/rfc2866.txt?number=2866
NoCatAuth: http://nocat.net/
SWIM: https://www.radiolinja.fi/go?section=tuotteet/liittyman_palvelut
&page=varmenne&lang=fi&side=2
WPKI: http://www.valimo.com/cgi-bin/fi/content.php?Level1=tuotteet