



Dnro 278731/04
Päätösno 40393/04

REAALIAIKAISET INTERNET-PALVELUT JA SIP RETIISI -PROJEKTI

2.1.2004 – 31.12.2005

LOPPURAPORTTI

Marjatta Jokisuu, koulutusjohtaja
Mika Mustikkamäki, IT-suunnittelija
Pekka Raisio, vanhempi suunnittelija
Tampereen yliopisto, Täydennyskoulutus-
keskuksen Seinäjoen toimipaikka /Wirlab
Kari Virtanen
Tietoliike Virtanen

Tampereen yliopiston täydennyskoulutuskeskus, TYT

Seinäjoen toimipaikka

PL 147 (Keskuskatu 34), 60101 Seinäjoki

Puh. +358 6 4211400, fax +358 6 4141 354, <http://www.sjoki.uta.fi/tyt>, <http://wirlab.net>

Sisältö

Tiivistelmä	2
<i>1. Taustaa</i>	<i>4</i>
<i>2. Tavoitteet</i>	<i>4</i>
<i>2. Projektin tuloksia</i>	<i>5</i>
2.1. Teknologisia tuloksia / TYT -osaprojekti	5
2.2. Teknologisia tuloksia / TTY-osaprojekti	8
2.3. Teknologisia tuloksia / VY - osaprojekti	8
3. Tulosten arviointia liiketoimintanäkökulmasta	9
<i>4. Tutkimustyön tulosten hyödyntäminen</i>	<i>10</i>
<i>5. Tutkimustyön tulosten julkistaminen ja muu tiedottaminen</i>	<i>11</i>
<i>6. Kansainvälinen yhteistyö ja sen hyödyntäminen</i>	<i>11</i>
<i>7. Tutkimustyön toteutuminen</i>	<i>11</i>
<i>7. Projektin jatkotoimet</i>	<i>12</i>
Liitteet / Osaraportit	13

REAALIAIKAISET INTERNET-PALVELUT JA SIP – RETIISI

Tiivistelmä

Projektissa keskityttiin erityisesti tietoliikenneteknologioiden kehittämiseen ympäristöihin, joissa keskeisiä elementtejä ovat reaaliaikaisuus ja eri medioiden (ääni, kuva, liikkuva kuva) käyttömahdollisuus. Projektissa oli tavoitteena saada operaattoreille ja tietoliikenneverkkojen suunnittelijoille tutkittua tietoa siitä, miten on mahdollista toteuttaa turvallinen ja vakaa multimedian vaatimukset täyttävä laaja tietoverkkojärjestelmä ja sen avulla nopeuttaa multimedian hallittua käyttöönottoa koko Internetissä. Projektissa tuotettiin kuusi osaraporttia.

Projektissa rakennettiin vikasietoisen SIP-palvelun kehitys- ja tutkimusympäristö, jossa SIP-palveluiden kahdennus onnistui tyydyttävästi. Tietokantojen kahdennuksesta pystyttiin siirtymään replikointiin käyttäen MySQL 4.1- sarjan tietokantasovellusta. SIP-välityspalvelin, RADIUS-autentikointipalvelin sekä muut keskeiset osat hajautettiin useammalle palvelinalustalle. Varmennuksen lisäksi hajautusratkaisulla voidaan toteuttaa myös perus- kuormantasaustoiminnot. Jatkokehitystä vaatii replikoinnin siirtäminen operaattoritason tuotantoympäristöön, mutta MySQL-tietokantaan tullut replikointiominaisuus todettiin kuitenkin jo melko helpoksi konfiguroida käyttöön SIP-palvelinympäristöön.

CallManager- ja SER-tutkimuksen osalta projektin tutkimusympäristössä pystyttiin hyödyntämään SER:in "trusted peer" -ominaisuutta, jonka avulla CallManagerilta tullut SIP-signalointi voitiin välittää edelleen SER:in avulla ilman SIP-viestien erillistä autentikointia. Tämä mahdollisti CallManagerin "SIP Trunk" -signalointiominaisuuden käytön ympäristössä, jossa SIP-välityspalvelin haluttiin integroida olemassaolevaan, CallManagerilla toteutettuun Voice over IP - palveluun.

NAT-osoitekäännösten ja palomuurien osalta selvitettiin parhaita käytäntöjä SIP-signaloinnin ja RTP-median läpiviemiseksi. Erityisen tärkeässä asemassa toimivuuden takaamiseksi on päätelaitteiden (so. SIP-puhelimien) ominaisuudet. Palomuurien ja myös NATin osalta eräs tärkeimmistä ratkaisuista on ns. MediaProxyn käyttö. NATiin liittyen STUN-protokollan todettiin olevan kelvoton tapa ohittaa käännökset nykyaikaisissa SIP- ympäristöissä.

Projektissa kehitettiin avointa 802.1x -autentikointiohjelmistoa Linuxiin. Tavoitteena oli mahdollisimman yksinkertaisen käyttöliittymän sekä käytettävyyden tarjoaminen, jolloin eri autentikointimetodien hallinta sekä konfiguraatitiedostojen muokkaus on käyttäjälle mahdollisimman yksinkertaista. Erityisesti projektissa keskityttiin laajentamaan olemassaolevaa ohjelmistoa uusilla autentikointitavoilla. Uusia EAP-metodeja olivat PEAP, EAP-GTC ja OTP.

Reaaliaikaisen median (erityisesti ääni ja video) kuljettaminen tietoverkossa on monisyinen vaatimusten ja ongelmien vyyhti. Viiveet, viiveen vaihtelut, palomuurit ja NAT-osoitekäännökset ovat vain osa mahdollisista ongelmista. Muita tekijöitä ovat erilaiset videoneuvottelujärjestelmät ja niiden teknologiat, joten järjestelmien

käytössä ollaan toimivuuden suhteen hyvin paljon tuotteiden valmistajien armoilla. Käytännön testeissä parhaaksi tavaksi ohittaa osoitekäänökset ja palomuurit osoittautui VPN-tunneleiden käyttö ja tietoliikenteen virtualisointi sen avulla. Eräs tapa hyödyntää tunnelia on perustaa VPN-palvelu reaaliaikaisia mediapalveluja tarjoavan organisaation omaan verkkoon ja siten suojata tietoliikenne.

Projektissa tehdyn tutkimustyön tulosten perusteella voidaan arvioida, että SIPin siirtyminen ja käyttöönotto on nykyisten ja tulevien verkkoratkaisujen toimivuuden kannalta turvallista ja perusteltavaa. SIP on osoittautunut oikeaksi valinnaksi, koska se on toimiva signaalintiprotokolla operaattoreiden palvelujen integroijana, monien eri multimediasovellusten pohjana ja tietoturvallisten ratkaisujen kehityksessä. SIP lisää operaattoreiden tuotevalikoimaa ja vahvistaa jo rakennettujen verkkojen ja verkkopalveluiden markkinointia. Lisäksi SIP on koko ajan kehittyvä ja se perustuu IETF RFC- standardeihin, joka takaa yhteensopivuuden tietoverkkojen muun kehityksen kanssa.

Wirlab-projekteissa kehitetty ja laajan kansainvälisen kehitystyön kohteena oleva Kphone -ohjelmistopuhelin on osoitus siitä, että kaikki RFC:n määrittelemät ominaisuudet voidaan toteuttaa SIP -Clientissa. Kphonen ominaisuuksia voi päätelaitteiden hankintavaiheessa käyttää vertailupohjana arvioitaessa SIP-puhelinten ominaisuuksia. Projektissa testattu, vahvojen standardien perusteella rakennettu SIP- ympäristö palvelee välittömästi myös mobiilikäyttäjiä. WLAN-alueella operaattori voi näin tarjota kaikki SIPin tuomat hyödyt myös heille.

Olemassaolevien järjestelmien hyödyntäminen ja järjestelmien hallittu kehittäminen on tarkoituksenmukaista sekä teknologisesti että taloudellisesti. Projektissa toteutettiin malli, jolla SIP-puhelimet ja Call Manager-puhelimet saadaan toimimaan keskenään. Cisco Call Manager on monien laajojenkin VoIP -ympäristöjen käytössä oleva keskus. Malli antaa palvelujen ja verkkoympäristöjen rakentajille mahdollisuuden jatkaa olemassaolevien Call Manager-ratkaisujen kehittämistä.

Retiisi -projekti toteutettiin ryhmäprojektina, jota koordinoi Tampereen yliopisto, Täydennyskoulutuskeskuksen Seinäjoen toimipaikka. Muut tutkimusosapuolet olivat Tampereen teknillinen yliopisto / DMI/ Tietoliikennetekniikan laitos ja Vaasan yliopisto, Seinäjoen toimipiste. Projektin teknologisenä johtajana toimi TkT Juha Heinänen, TutPro Oy. Projekti toteutettiin Seinäjoella ja Tampereella Wirlab – verkkotutkimuskeskuksen testiympäristöissä 2.1.2004 – 31.12.2005. Projektia rahoittivat Tekes ja yritysrahoittajina Alajärven Puhelinosuuskunta, Vaasan Läänin Puhelin Oy ja Cygate Networks Oy.

1. Taustaa

Reaaliaikaiset internet-palvelut ja SIP –Retiisi –projekti on Seinäjoella käynnistetyn ja vuonna 2001 toimintansa aloittaneen Wirlab-verkkotutkimuskeskuksen kuudes laaja yleinen tutkimushanke. Wirlabin toiminnan perusta on konsortiopohjainen yhteistyö, jossa on mukana yliopistojen ja korkeakoulujen tutkimusyksiköitä sekä tietoliikennealan yrityksiä. Verkkotutkimuskeskuksen painopiste on tulevaisuuden tiedonsiirtotekniikoissa ja kohdealueena erityisesti mobiiliverkon täydentäminen uusilla langattomilla tekniikoilla, puhepalveluiden toiminta erilaisten verkkojen yhdistelmissä sekä wlan-verkkojen uudet sovellukset ja palvelumahdollisuudet. Wirlabilla on käytössään monipuoliseen testaukseen soveltuva tietoverkko-ympäristö, johon on tarpeen mukaan mahdollisuus liittää osia myös yhteistyö-osapuolten verkoista ja laitteista. Yleisten tutkimushankkeiden lisäksi Wirlab-verkkotutkimuskeskus toteuttaa tutkimustuloksia soveltavia yritys- tai yritysryhmäkohtaisia kehittämishankkeita.

Wirlabin tutkimustoiminnalla pyritään tuottamaan uutta ja kumuloituvaa tutkimustietoa tulevaisuuden tietoverkko- ja tiedonsiirtoteknologioista ja tietoliikennejärjestelmistä. Wirlabin tutkimuksen peruserätyyteenä on tähdätä avoimiin mutta samalla turvallisiin tietoliikenne- ja verkkoratkaisuihin.

2. Tavoitteet

Reaaliaikaiset internet-palvelut ja SIP –projektin tutkimussuunnitelma rakentui Wirlabissa aikaisemmin toteutettujen tutkimusprojektien tulosten jatkokehittämiseen ja hyödyntämiseen. Projektissa keskityttiin erityisesti tietoliikenneteknologioiden kehittämiseen ympäristöihin, joissa keskeisiä elementtejä ovat reaaliaikaisuus ja eri medioiden (ääni, kuva, liikkuva kuva) käyttömahdollisuus.

Projektissa oli tavoitteena saada operaattoreille ja tietoliikenneverkkojen suunnittelijoille tutkittua tietoa siitä, miten on mahdollista toteuttaa turvallinen ja vakaa multimedian vaatimukset täyttävä laaja tietoverkkojärjestelmä ja sen avulla nopeuttaa multimedian hallittua käyttöönottoa koko Internetissä. Tavoitetta tukevia teknologioita kehitettäessä korostuvat vaihtoehdot tasoista, joilla eri protokollia voidaan tukea. Tutkimuksen tavoitteena oli ratkaista millä tasoilla ja millä laitteilla missäkin tapauksessa olisi parasta tai jopa pakollista toteuttaa esimerkiksi SIP-tuki, NAT-tuki, RTP-palvelu ja palomuurien tuoma turva. Tavoitteena oli myös paljastaa ne vaikeudet ja ongelmat, joita tulee esiin sovitettaessa perinteisiä tietoverkkoratkaisuja ja multimedian vaatimuksia yhteen mm. reaaliaikaisuuden ja tietoturvan osalta. Teknologisina tavoitteina oli selvittää eroja SIP- ja H323-toteutusten välillä sekä selvittää SIP-palvelujen toteutumista tietoverkoissa, joissa on palomureja ja NAT-palveluja. Tavoitteena oli myös tutkia RTP-palvelujen (Real Time Transmission Protocol) sijoittamisvaihtoehtoja tietoverkkoon turvaamaan tietoliikenne yritysverkoista julkiseen verkkoon ja myös yritysverkkojen välillä.

Projektin laaja sisältöalue jaettiin kolmeen osaprojektiin, joille nimettiin vastuuorganisaatiot ja –tutkijat. Projektia koordinoiva Tampereen yliopisto, TYT/Wirlab vastasi osaprojektista, jossa tutkittiin Internetin reaaliaikaisten palvelujen mahdollisuuksia parantaa multimediatoteutuksien laatutasoa sekä RTP-proxyn mahdollisuuksia turvata liikenne yritysverkoista julkiseen verkkoon ja yritysverkkojen välillä. Tavoitteena oli rakentaa malli, jolla H323- ja SIP-protokollia toteuttavista ympäristöistä voidaan suunnitella toimiva kokonaisuus. Osaprojektissa selvitettiin eri SIP-palvelujen toteutusmahdollisuudet palomureja ja NAT-palveluja sisältävissä tietoverkoissa.

Tampereen teknillinen yliopisto /DMI/ Tietoliikennetekniikan laitos vastasi osaprojektista, jossa keskityttiin reaaliaikapalveluiden tietoturvaominaisuuksien tutkimiseen. Siinä oli tavoitteena kehittää käyttäjän autentikoinnin apuvälineeksi Linux-käyttäjärjestelmään ohjelmisto, jonka avulla IEEE 802.1X-autentikointi ja sen päällä toimivat EAP-variaatiot ja dynaamiset WEP-avaimet saadaan helposti käyttöön.

Vaasan yliopiston Seinäjoen toimipiste vastasi osaprojektista, jossa testattiin ja analysoitiin eri videoneuvottelujärjestelmiä käytännön kuormituksella erilaisia aktiivilaitteita ja palveluja sisältävissä tietoverkoissa. Tavoitteena oli kehittää analysointimenetelmää testaustulosten raportointiin.

2. Projektin tuloksia

Reaaliaikaiset internet-palvelut ja SIP –projektin tulokset ovat tavoitteiden mukaisesti ensisijaisesti teknologisia tuloksia, osittain jopa lähellä perustutkimustakin olevia. Niiden tarkoituksena on antaa operaattoreille ja tietoliikenneverkkoja suunnitteleville yrityksille teknologista tietämystä, jonka pohjalta yritykset voivat kehittää liiketoimintamallejaan ja tuotteitaan omiin tuotantoympäristöihinsä. Tuloksia on yksityiskohtaisemmin raportoitu kuudessa osaraportissa (suluissa osaprojektin vastuutaho) ; Palomuurit ja NAT SIP-palvelun rakentamisessa (TYT), Vikasietoinen SIP-ympäristö (TYT), Cisco CallManager ja SER (TYT), Tut1x802.1x Supplicant (TTY) ja Tut1x –projektin laajennus (TTY) sekä Palomuurien ja NATin tuomat haasteet neuvottelujärjestelmien käytössä (VY). Osaraporteista erityisesti ensin mainittuun, “Palomuurit ja NAT SIP-palvelun rakentamisessa” on koottu suosituksia ja ohjeita tarkoituksena tukea yritysten teknologista kehittämistoimintaa.

2.1. Teknologisia tuloksia / TYT -osaprojekti

Projektin aikana rakennettu vikasietoisen SIP-palvelun kehitys- ja tutkimusympäristö saatiin toimimaan melko hyvin. Tietokantojen kahdennuksesta pystyttiin siirtymään replikointiin käyttäen MySQL 4.1- sarjan tietokantasovellusta. Replikoinnin siirtämisessä operaattoritason tuotantoympäristöön on kuitenkin vielä kehitysaskelia otettavana, sillä laite- tai ohjelmistoviasta selviämistä ei pystytty osoittamaan 100% toimivaksi eri testatuilla MySQL-kehitysversioilla. Usein testitilanteissa kävi niin, että tietokantadataa hävisi tai tietokannan eri osia

korruptoitui siten, ettei niitä voitu enää klusterointia käyttämällä palauttaa toimintaan. MySQL-tietokantaan tullut replikointiominaisuus todettiin kuitenkin melko helpoksi konfiguroida käyttöön tutkitun SIP-palvelinympäristön kannalta. Tämän voidaan katsoa rohkaisevan operaattoreita järjestelmän käyttöönottoon sekä teknisestä että liiketaloudellisesta näkökulmasta, sillä vika- ja ongelmatilanteista selviäminen vaatii huomattavasti vähemmän ylläpitohenkilökunnan käsityötä perinteiseen tietokantojen master/ slave-kopiointiin verrattuna, jolloin järjestelmän oletettava saavutettavuus on parempi.

Varsinainen SIP-palveluiden kahdennus onnistui muuten tyydyttävästi. SIP-välityspalvelimen, RADIUS-autentikointipalvelimen, sekä muiden keskeisten osien hajauttaminen useammalle kuin yhdelle palvelinalustalle toimi, kuten alunperin suunniteltiin. Varmennuksen lisäksi tutkimustulosten valossa on oletettavaa, että hajautusratkaisulla voidaan toteuttaa myös perus- kuormantasaustoiminnot. Nämä saavutetaan etenkin RADIUS-palvelinten ja tietokantojen hajauttamisella eri palvelimille. Kuormantasauksella voidaan SIP-palveluissa ymmärtää esimerkiksi useiden yhtäaikaisten, yksittäistä SIP-välityspalvelinta ylikuormittavien kyselyiden jakaminen RADIUS-pyynnöillä niin, että kukin yksittäinen autentikointipyyntö ohjataan sattumanvaraisesti (round-robin, ks. periaatteet esim. [1]) hajautetussa ympäristössä oleville palvelimille. Jatkokehityskysymykseksi tuotantoympäristöjen kannalta jäi kesken olevien autentikointipyyntöjen tai SIP-dialogien siirtäminen toiselle palvelimelle, mikäli alkuperäinen palvelin lakkaa vastaamasta. Tutkittaessa mahdollisuuksia selvittää tällaisesta vikatilanteesta todettiin, että yleisesti on luotettava sovelluskerroksen hallitsemiin uudelleenlähetyksiin ja -yrityksiin, kun alkuperäinen viesti katoaa kesken toiminnon suorittamisen. Tälläkin on kuitenkin rajoituksensa, joten esim. RADIUS- autentikoinnissa on tietty määrä (konfiguroitavia) asetuksia, joilla voidaan itse hallita uudelleenyritysten ja timeout-parametrien arvoja.

CallManager- ja SER-tutkimuksen osalta saavutettiin kaikki asetetut tavoitteet, eli projektin tutkimusympäristössä pystyttiin hyödyntämään SER:in "trusted peer" - ominaisuutta, jonka avulla CallManagerilta tullut SIP-signalointi voitiin välittää edelleen SER:in avulla ilman SIP-viestien erillistä autentikointia. Tämä mahdollisti CallManagerin "SIP Trunk" -signalointiominaisuuden käytön ympäristössä, jossa SIP-välityspalvelin haluttiin integroida olemassaolevaan, CallManagerilla toteutettuun Voice over IP -palveluun.

NAT-osoitekäännösten ja palomuurien osalta tutkimuksessa selvitettiin erityisesti SIP-signaloinnin ja RTP-median (ääni, video) asettamia vaatimuksia em. laite- ja ohjelmistototeutuksille. Tutkimuksessa selvitettiin erityisesti parhaita käytäntöjä signaloinnin ja median läpiviemiseksi sellaisissa ympäristöissä, joista löytyy osoitekäännöksiä ja/tai palomureja. Erityisen tärkeässä asemassa toimivuuden takaamiseksi on päätelaitteiden (so. SIP-puhelimien) ominaisuudet. Symmetrinen signalointi ja media, eli toisin sanoen lähettävien ja vastaanottavien tietoliikenneporttien vastaavuus on ominaisuus, joka vaaditaan kaikilta nykyaikaisilta päätelaitteilta. Symmetrisen signaloinnin avulla voidaan ohittaa useita NAT-ongelmia, sillä NAT-osoitekäännös perustuu usein nimenomaan osoite- ja portti-translaatioon lähdeporttien perusteella. Palomuurien (ja myös NATin) osalta eräs tärkeimmistä ratkaisuista on ns. MediaProxyn käyttö. MediaProxy on välityspalvelin, jolla voidaan hoitaa kahdenvälisen mediasession välitys palo-

muurin yli, sekä myös sellaiset tilanteet joissa käytettävää NAT-osoitekäännöstä ei voida muuten ohittaa. MediaProxyn käyttö edellyttää luonnollisesti sitä, että se sijaitsee osoitekäännösten ja/tai palomuurin julkisella puolella, jossa se on mahdollista saavuttaa muista Internet- osoitteista käsin. MediaProxy vaatii toimiakseen myös päätelaitteiden symmetrisen signaloinnin.

Tutkimuksessa todettiin lisäksi NATiin liittyen STUN-protokollan olevan kelvoton tapa ohittaa käännökset nykyaikaisissa SIP- ympäristöissä. Suurin ongelma STUNin käytössä on se, ettei se ymmärrä lainkaan symmetrisiä NAT-translaatioita. Edelleen tutkimuksessa todettiin, että viime aikoina yleistyneet ns. älykkäät NATit ovat ehkäpä huonoin tapa hoitaa signaloinnin ja median välitys translaatioiden yli. Toteutukset älykkäistä NATeista on todettu käytännössä olevan itse asiassa käänteisiä haluttuun toimintaansa nähden, ja rikkovat yleensä signaloinnin ja median välityksen kokonaan. Mikäli tuotantoympäristöissä on tarpeen käyttää älykkäitä NAT-laitteita, Retiisi-projekti suosittelee SIPin standardin signalointiportin vaihtamista esimerkiksi 5061:ksi 5060:n sijaan. Tällaisella yksinkertaisella porttimuutoksella älykkäät NATit eivät osaa enää tunnistaa SIP-liikennettä.

RTP-median (ääni, video) verkossa viennin kannalta CallManager ja käytetty SIP-palvelinympäristö ovat samalla lähtöviivalla suhteessa NAT- osoitekäännösten ja palomuurien suhteen. Signaloinnissa tutkimushetkellä SIPiin oli saatavilla jo useita käyttöä helpottavia ratkaisuja, joita CallManager-järjestelmiin ei suoranaisesti tarjottu (esimerkiksi edellä mainitut signalointi-, MediaProxy-, ja STUN-toteutukset). Tästä lähtökohdasta käsin voidaan todeta, että SIPiin siirtyminen ja käyttöönotto on nykyisten ja tulevien verkkoratkaisujen toimivuuden kannalta turvallista ja perusteltavaa. Koska SIP-signaloinnin välittäminen verkossa ei kuormita toteutustapansa vuoksi verkon rakennetta yhtä paljon kuin H.323-protokollaan perustuvat ratkaisut, voidaan erilaisia Quality Of Service -tapoja käyttäen keskittyä nimenomaan RTP-liikenteen häiriöttömään kuljettamiseen multimediasessioiden osapuolien välillä. Tämä tosiasia on osaltaan keventämässä verkonsuunnitteluun liittyvää problematiikkaa ja auttaa reaaliaikaisten palveluiden käyttöönottoa.

Projektin yhtenä osana kehitettiin myös KPhone-ohjelmistopuhelinta ja sen Windows-käyttöjärjestelmän yhteensopivuutta. Kehitys tapahtui Qt-ohjelmointiympäristön päällä, perustuen Qt-versioihin 3.0 ja 4.0. Aiemman Qt-version kanssa ongelmaksi muodostuivat verkko- ja äänirajapinnan ohjelmointivaikeudet, sillä KPhone-toteutus haluttiin saada toimimaan puhtaasti Qt:n kanssa, ilman Windowsin omien ohjelmistorajapintojen käyttöä. Tämä mahdollisuus toteutui vasta Qt:n 4.0.1-versiossa, jossa em. verkko- ja äänirajapinnat Windowsin suhteen tulivat vasta kunnolla toteutettuina. Windows-version ohjelmoinnissa kohdattiin myös muita haasteita, johtuen erityisesti Qt:n ja Windows-versioiden lisenssien välisestä luonteesta.

Avoimen kehitysympäristön käyttämisestä Windowsin päällä muodostuu erityinen haaste KPhonen tapauksessa, kun valmis koodi halutaan saattaa GPL-lisenssin alaiseksi myös kaupallisella käyttöjärjestelmäalustalla. Koska Microsoftin Visual C++ -ympäristö ei toimi yhdessä GPL-lisenssin alaisen Qt:n kanssa, käyttöön

otettiin avoimen lähdekoodin C++-kehitysympäristö Code::Blocks [1]. Sitä pystyttiin soveltamaan onnistuneesti koodin kääntämiseen Qt:n 4.0-version Meta Object Compilerin kanssa. Ensimmäiset toimivat versiot Windows-KPhonesta saatiin rekisteröitymään SIP-välityspalvelimelle joulukuussa 2005, ja kehitys jatkuu Qt-ympäristön jatkokehityksen myötä. Erityisesti KPhone-Windows -kehitys mahdollistaa avoimen SIP-päätelaitteen käytön tulevaisuudessa TYT/Wirlabin tutkimus- ja kehityshankkeissa.

2.2. Teknologisia tuloksia / TTY-osaprojekti

TTY:llä kehitettiin Retiisi-projektin puitteissa avointa 802.1x (ks. esim. [2]) -autentikointiohjelmistoa Linuxiin (Tut1x, [3]). Lähtökohtana oli mahdollisimman yksinkertaisen käyttöliittymän sekä käytettävyyden tarjoaminen, jolloin eri autentikointimetodien hallinta sekä konfiguraatitiedostojen muokkaus on käyttäjälle mahdollisimman yksinkertaista. Erityisesti projektissa keskityttiin laajentamaan olemassaolevaa ohjelmistoa uusilla autentikointitavoilla. Uusia EAP-metodeja olivat PEAP, EAP-GTC ja OTP. Esimerkki varmenteisiin perustuvan TLS-autentikoinnin konfiguraatiosta:

```
user_cert = "/etc/tut1x/user-cert.pem";
user_key = "/etc/tut1x/user-key.pem";
root_cert = "/etc/tut1x/cacert.pem";
cert_password = "whatever";
interface = "eth0";
username = "md5user";
auth_method = "tls";
```

Tulokset osaprojektista olivat tyydyttäviä. PEAP-toteutus tehtiin IETF-draftin numero kuusi mukaisesti, sillä uudemman versio seitsemän toteutukseen tarvittavia laitteistoja ei ollut Retiisi-projektin aikana saatavilla. Myös TTY:n testilaitteissa esiintyneet ongelmat rajoittivat jonkin verran virheiden kartoitusta ja korjaamista.

2.3. Teknologisia tuloksia / VY - osaprojekti

Reaaliaikaisen median (erityisesti ääni ja video) kuljettaminen tietoverkossa osoittautui monisyiseksi vaatimusten ja ongelmien vyyhdiksi. Viiveet, viiveen vaihtelut, palomuurit ja NAT-osoitekäännökset ovat vain osa mahdollisista median kuljettamista vaikeuttavista tekijöistä. Erilaiset videoneuvottelujärjestelmät käyttävät lukuisia erilaisia tietoliikenneporttien avaruuksia, joiden konfiguroiminen manuaalisesti kaikkiin palomuuereihin ja muihin liikennöintiä rajoittaviin laitteisiin on lähes mahdotonta. Joistain (kaupallisista) tuotteista on myös lähtökohtaisesti vaikea saada selville käytettäviä portteja. Näin ollen ko. järjestelmien käytössä ollaan toimivuuden suhteen hyvin paljon tuotteiden valmistajien armoilla. Tietyissä kaupallisissa tuotteissa on kuitenkin hyvin pitkälle kehitettyjä ominaisuuksia, joilla em. ongelmia voidaan ohittaa ja estää.

Käytännön testeissä parhaaksi tavaksi ohittaa osoitekäännökset ja palomuurit osoittautui VPN-tunneleiden käyttö. VPN-tunnelilla tietoliikenneyhteys voidaan virtualisoida kulkemaan pisteestä A pisteeseen B siten, että liikenne kohteelle C näyttää tulevan B:ltä alkuperäisen lähettäjän, eli A:n sijaan. VPN-tunneleissa pisteiden A ja B väliin luodaan siis suojattu "putki", joka on salattu jollain vahvalla menetelmällä (esim. 3DES [4] tai AES [5]). Kun tietoliikenne kuljetetaan tällaisen putken läpi kohteelle, kohdellaan IP-paketteja täysin tunnelin B-osan verkon sääntöjen mukaisesti. Eräs tapa hyödyntää tunnelia on siis perustaa VPN-palvelu reaaliaikaisia mediapalveluja tarjoavan organisaation omaan verkkoon, terminoida kaikki kyseisiä mediapalveluja käyttävät tähän VPN-pisteeseen, ja hyväksyä sen jälkeen liikenne kaikkialta oman verkon luotetuista osista mediapalveluita tarjoavalle palvelimelle.

[1] Remote Access Dial In User Service, IETF RFC2865, <http://www.ietf.org/rfc/rfc2865.txt>

[1] <http://en.wikipedia.org/wiki/Code::Blocks>

[2] <http://www.ieee802.org/1/pages/802.1x.html>

[3] <http://atm.tut.fi/tut1x/>

[4] <http://en.wikipedia.org/wiki/3DES>

[5] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[1] <http://en.wikipedia.org/wiki/Code::Blocks>

3. Tulosten arviointia liiketoimintanäkökulmasta

Perinteisen lankapuhelinverkon markkinat eivät enää kasva ja operaattoreiden liiketoiminta on rajusti muuttumassa. Puhelujen siirtyminen IP-pohjaiseen verkkoon on väistämätön. Siirryttäessä IP-liikenteeseen mahdollisuudet laajenevat, koska puheliikenne on kiinteä osa IP-verkkojen kokonaiskehitystä. Retiisi-tutkimuksen ansiosta operaattorit ovat valmiimpia soveltamaan uutta tekniikkaa liiketoiminnassaan. Tieto ja osaaminen takaavat itsenäisemmät valinnat ja uusia palveluja voidaan rakentaa suunnitelmallisemmin. Retiisi-tutkimusprojektin tärkein valinta oli keskittyminen SIP- signaalointiprotokollaan. SIP on osoittautunut oikeaksi valinnaksi, koska sen vahvuus, esimerkiksi operaattoreiden palvelujen integroijana, monien eri multimediasovellusten pohjana ja tietoturvallisten ratkaisujen kehityksessä, on toimiva. SIP kehittyy koko ajan ja jatkaa turvallisella IETF RFC- standardien tiellä, joka takaa yhteensopivuuden tietoverkkojen muun kehityksen kanssa. Kehityksessä ajoissa mukana olleet operaattorit voivat huokaista helpotuksesta, koska yksi kehityksen vaihe on jäänyt kustannuksista pois, kun he ovat suoraan siirtyneet SIP- protokollan käyttäjiksi.

SIP lisää operaattoreiden tuotevalikoimaa ja vahvistaa jo rakennettujen verkkojen ja verkkopalveluiden markkinointia.

Operaattorit tarjoavat yksityisiä ja yrityksiä palvelevia laajakaistayhteyksiä. Palvelun käyttäjillä on mahdollista valita yhteyden nopeus. SIP puhelupalvelun voi tarjota lisäominaisuutena kaikilla käytössä olevilla nopeuksilla. Hankintavaiheessa SIP- puhelinten ominaisuuksia voi arvioida vertaamalla niitä Wirlabin projekteissa

kehitettyyn, Retiisi-projektissa lisäominaisuuksia saaneeseen ja laajasti levinneeseen KPhoneen. KPhone on operaattoreille toimiva esimerkki heidän keskustellessaan laitetoimittajien kanssa uusista SIP-puhelinmalleista. KPhone on osoitus siitä, että kaikki RFC:n määrittelemät ominaisuudet voidaan toteuttaa SIP -Clientissa. Vertailun kautta tehdyt oikeat valinnat säästävät huomattavasti aikaa ja kustannuksia.

WLAN -alueella SIPin päällä toimivat kännykät, merkkejä esimerkiksi Zyxel ja Nokia, laajentavat SIP -palvelujen hyödyn myös liikkuville käyttäjille. Retiisi-projektissa testattujen vahvojen standardien perusteella rakennettu SIP- ympäristö palvelee välittömästi myös kännykkäkäyttäjiä. WLAN- alueella kännykkäkäyttäjälle operaattori voi näin tarjota kaikki SIPin tuomat hyödyt.

Cisco Call Manager on monien laajojenkin VoIP -ympäristöjen keskus. Retiisi-projektissa toteutettu malli, miten SIP-puhelimet ja Call Manager-puhelimet saadaan toimimaan keskenään, antaa rakentajille mahdollisuuden rauhassa jatkaa kehitystä purkamatta vanhempia Call Manager-ratkaisuja. Asiakastytyväisyys säilyy eikä tule turhia kustannuksia jatkuvista muutostöistä.

Projektiin otettiin case-tyyppiseksi tutkimuskohteeksi videoneuvottelupalvelujen kehittäminen. Projektissa päästiin aloittamaan pohjan rakentaminen myös videoneuvottelujen siirtämiseksi täysin SIPin päälle.

Kaikkiaan ollaan todella menossa siihen suuntaan, että henkilöllä on yksi osoite, johon yhteydenotto voi olla puhelu, sähköposti, pyyntö videoneuvotteluun, IM (Instant Message = SIP tekstiviesti) tai palvelu voi viestittää operaattorin asiakkaan halukkuudesta tai mahdollisuudesta kommunikoida (presence). Ja kun Enum yhdistää vielä eri palveluntarjoajat niin käyttäjien yhteydenotot pysyvät koko ajan liikennettä hidastavien puhelinkeskusten ulkopuolella. Operaattoreille on projektissa syntynyt malli, jolla operaattorit voivat siirtyä sujuvasti uuteen palvelurakenteeseen käyttämällä rinnalla jo aikaisemmin valittuja tuotteita.

4. Tutkimustyön tulosten hyödyntäminen

Retiisi -projektista saatavia tuloksia voidaan hyödyntää sekä Wirlabin yritysosaapuolien että alan perustutkimuksen ja sovellusten puitteissa. Projektin tuloksia on esitelty yhteistyöyrityksille projektin aikana demoina ja tarjottu mahdollisuuksia olla mukana kehitystyössä testiympäristöissä. Kehitystuloksia on myös välittömästi siirretty osapuolten omiin ympäristöihin tutkittavaksi ja edelleen kehitettäväksi.

Tuloksia on hyödynnetty myös Seinäjoen yliopistokeskuksen ucs.fi -verkkoympäristön kehittämisessä, jolloin on pystytty rakentamaan eräänlainen testi- ja tuotantoympäristöjen välimuoto. Se on tukenut erityisesti tutkimusyksiköiden yhteistyötä ja osaprojektien yhteyksiä, tuloksia on kyetty testaamaan erilaisilla käyttäjäryhmillä ja lisäksi ympäristöä, teknologioita ja kehitysnäkymiä on yleisellä tasolla voitu esitellä myös ulkopuolisille yrityksille ja organisaatioille.

Tutkimusympäristöä tuloksineen voidaan hyödyntää Informaatioteknologian maisterikoulutusohjelmassa, jossa on käynnistymässä opinnäytetyövaihe. Koulutuksen järjestää TYT/Seinäjoki yhdessä Tampereen yliopiston tietojenkäsittelytieteen laitoksen kanssa. Yhteistyöstä korkea-asteen koulutuksessa ja mahdollisesti myös t&k-toiminnassa on käyty keskusteluja myös Seinäjoen ammattikorkeakoulun informaatio- ja kommunikaatioteknologian yksikön kanssa.

Projektin aikana on käynnistynyt kaksi yritysprojektia, joissa projektin tuloksia edelleen hyödynnetään sekä teknologisella kehitystyöllä että liiketoimintamallien ja palvelutuotteiden kehittämisellä. Lisäksi on valmisteltu laajahkoa alueellista kehittämishanketta sekä yritysryhmähanketta, joissa molemmissa tutkimus- ja kehitystyö pohjautuu keskeisesti myös tässä projektissa tuotettuihin tuloksiin.

5. Tutkimustyön tulosten julkistaminen ja muu tiedottaminen

Tutkimustyöstä ja projektin etenemisestä kokonaisuutena on tiedotettu ennen kaikkea rahoittajille ja muille yhteistyökumppaneille. Projektin yritysrahoittajilla on ollut nimettynä yhteyshenkilöt, joiden kanssa vuorovaikutus ja sen mukana projektin tuloksista syntyvä tiedonvälitys on ollut viikottaista.

Projektin sisältöjä ja tuloksia on esitelty yrityskäynneillä tai Wirlabin laboratoriotiloissa useille yrityksille ja laitoksille, jotka suunnittelevat omien tietoverkkoympäristöjensä teknologista uudistamista tai kehittämistä.

Projektin osaraportit ovat esillä Wirlabin kotisivuilla <http://www.wirlab.net/julkaisut.html>.

6. Kansainvälinen yhteistyö ja sen hyödyntäminen

Projektissa on jatkunut kansainvälinen yhteistyö aktiivisena verkkopohjaisena vuorovaikutuksena alan globaalien kehittäjäverkostojen kanssa. Tutkimuksen ohjauksessa ja fokuksinnissa on hyödynnetty kansainvälisiä tutkimustuloksia ja kehitystyötä.

7. Tutkimustyön toteutuminen

Tutkimustyössä lähdettiin liikkeelle rahoituspäätösten ja sopimusten solmimisen myötä. Selkeän tutkimussuunnitelman ansiosta tutkimustyö lähti ripeästi etenemään ja painottui projektin alkupuoliskolle. TTY:n ja VY:n osaprojektit olivat päätuloksiltaan käytännöllisesti katsoen valmiita jo keväällä 2005. Resurssien mukaan ja omien asiantuntijaverkostojensa tuella kukin osaprojekti fokusoiti tutkimustyötään ja kokonaisuutena projekti eteni varsin hyvin tutkimussuunnitelman mukaisesti. Erityisesti TYTin ja VY:n osalta projektia tuki samanaikaisesti menossa ollut Seinäjoen yliopistokeskuksen verkkoympäristön kehittämishanke, jota joiltain osin pystyttiin hyödyntämään käytännön testauksissa.

Projekti lähti liikkeelle osaprojektien määrittelyillä, jonka jälkeen kukin niistä eteni pääsääntöisesti omaan tahtiinsa. Projektin johtoryhmän kokouksissa käsiteltiin kunkin osaprojektin eteneminen ja lisäksi TkT Juha Heinänen ohjasi projektin teknologiaryhmää koko projektin ajan. TYTin ja Vaasan yliopiston tutkimuksia varten rakennettiin testiympäristö, joka perustui molempien yksiköiden omille testiverkko- ja laiteympäristöille ja niiden yhdistämiselle projektin tavoitteiden mukaisesti. Ympäristöjen rakentamisen jälkeen käynnistettiin testaukset ja analyysit ja niiden pohjalta tuotettiin ohjeistusta SIP-palvelujen toteutuksesta palomuuereja ja NAT-palveluja sisältävissä tietoverkoissa, Call Managerin käytöstä sekä erilaisten videoneuvottelujärjestelmien toimivuudesta ja erityisesti Access Grid –kehityksestä.

Projektin tutkimustyöstä ovat vastanneet Tampereen yliopiston TYT/Wirlab, Vaasan yliopiston Seinäjoen toimipiste ja Tampereen teknillisen yliopiston DMI/tietoliikennetekniikan laitos. Projektin koordinoinnista ja projektihallinnosta on vastannut Tampereen yliopisto, TYT/Seinäjoki.

Projektikoordinaatorina ja TYTin vastuulla olleesta tutkimuskokonaisuudesta ovat vastanneet Mika Mustikkamäki, Veli Pajula, Pekka Raisio ja Jouni Vuorela (v. 2004) sekä projektihallinnosta Juhani Niemelä (v. 2004) ja Marjatta Jokisuu. Lisäksi on ostopalveluna hankittu projektin teknologinen ohjaus TkT Juha Heinäselältä / TutPro Oy ja osaprojektien ja yritys yhteistyön koordinointityö Kari Virtaselta /Tietoliike Virtanen ja Kari Rajalalta / R-Trade Oy (v. 2004).

Tampereen teknillisen yliopiston tietoliikennetekniikan laitoksen osaprojektista ovat vastanneet professori Jarmo Harjun johdolla tutkija Ilkka Karvinen sekä tekniikan ylioppilaat Jouni Honkala, Antti Laiti ja Petri Niemi.

Vaasan yliopiston Seinäjoen yksikön osaprojektista on vastannut suunnittelija Lassi Ylikojola yhdessä yksikön johtajan Tuomas Rouhunkosken kanssa.

Projektin hyväksytty kustannusarvio oli 331 293 euroa. Projektiosapuolet ovat raportoineet kertyneiksi kustannuksiksi 369 594 euroa. Ylitykset ovat kertyneet palkoista ja ostopalveluista, joka osoittaa, että projektin tutkimusosapuolet ovat halunneet panostaa asiantuntijatyöhön jopa suunniteltua enemmän. Projektin rahoituksesta Tekesin osuus oli 262 000 euroa ja yritysosapuolten Vaasa Läänin Puhelin Oy, Cygate Networks Oy ja Alajärven Puhelinosuuskunta yhteensä 69 293 euroa. Rahoitukset toteutuvat täysimääräisinä. Projektissa on tehty kolme kustannustilitystä ja raportointia Tekesille 31.12.04, 30.6.05 ja 31.12.05. Johtoryhmä on kokoontunut viisi kertaa 3.9.04, 22.11.04, 21.1.05, 26.8.05 ja 16.12.05. Projektin ohjaus on tapahtunut osapuolten jatkuvan yhteistyön ja noin joka toinen kuukausi tapahtuneiden teknologiaryhmän projektikokousten avulla.

7. Projektin jatkotoimet

Tutkimus- ja kehitystyö jatkuu erityisesti IP-teknologioiden parissa, painopisteinä edelleen SIP- ja WLAN- teknologiakehitys ja niiden hyödyntäminen yritysten liiketoiminnassa, liiketoimintastrategioissa ja palvelu- ja tuotekehityksessä. Projektin päättyessä on menossa kaksi projektia ja valmisteluvaiheessa myös

kaksi hanketta, joissa projektin tuloksia hyödynnetään ja käytetään erityisesti liiketoiminta- ja teknologiastrategioiden kehittämisen pohjana. Näissä hankkeissa panostetaan teknologisten tulosten ohella osaamisen lisäämiseen ja uusien teknologioiden laajempaan esittelyyn erilaisille käyttäjä- ja hyödyntäjätahoille. Seinäjoen yliopistokeskuksen verkkoympäristön rakentamisessa ja kehittämisessä projektin tuloksia on voitu hyödyntää ja soveltaa lähes tuotantoympäristössä koko projektin ajan ja myös sen kehitystyö jatkuu edelleen.

Liitteet / Osaraportit

Palomuurit ja NAT SIP-palvelun rakentamisessa (TYT)

Vikasietoinen SIP-ympäristö (TYT)

Cisco CallManager ja SER (TYT)

Tut1x802.1x Supplicant (TTY)

Tut1x –projektin laajennus (TTY)

Palomuurien ja NATin tuomat haasteet neuvottelujärjestelmien käytössä (VY)