Puheluiden ja viestinnän yksityisyys mobiililaitteissa

University of Oulu
Department of Information Processing Science
Bachelor's Thesis
Kimmo Paananen
9.3.2015

Tiivistelmä

Tutkimuksessa perehdyttiin internettiin kytkettyjen laitteiden puheluiden ja viestinnän yksityisyyteen ja tietoturvaan. Voimakkaasti yleistyneet VoIP-puhelut mahdollistavat helpon, monipuolisen ja edullisen viestinnän laitteiden välillä internetissä. VoIP-pohjaiseen kommunikaatioon liittyy kuitenkin yksityisyyteen ja turvallisuuteen liittyviä uhkia, aivan kuten kaikkeen julkisessa internetissä välitettävään liikenteeseen. Tässä tutkimuksessa selvitettiin VoIP-tekniikan perusteet, mistä tietoturvauhkat johtuvat ja miten uhkia voidaan torjua. Lisäksi tehtiin katsaus tarjolla oleviin valmiisiin palveluihin, ja vertailtiin tuotteiden ominaisuuksia niiden tarjoaman yksityisyydensuojan ja turvallisuuden näkökulmasta, huomioiden erityisesti palveluiden liitettävyys omiin sovelluksiin sekä mahdollisimman pienet käyttöönotto- ja käyttökustannukset.

Avainsanat
yksityisyydensuoja, tietoturva, salaus, matkaviestintä, VoIP, puhelut

Ohjaaja
Professori Petri Pulli

Lyhenteet

3GPP - 3rd Generation Partnership Project
AES - Advanced Encryption Standard
API - Application Programming Interface
CALEA - Communications Assistance for Law Enforcement Act
ETSI - European Telecommunications Standards Institute
HTTP - Hypertext Transfer Protocol
IEFT - Internet Engineering Taskforce
IMAP - Internet Message Access Protocol
IP - Internet Protocol
IPSec - Internet Protocol Security
MIME - Multipurpose Internet Mail Extensions
MitM - Man in the Middle
NSA - National Security Agency
OSI - Open Systems Interconnection
POP3 - Post Office Protocol version 3
VoIP - Voice over Internet Protocol
QoS - Quality of Service
QFD - Quality Function Deployment
RTCP – Real-time Control Protocol
RTP – Real-time Transport Protocol
SRTP - Secure Real-time Transport Protocol
SIP - Session Initiation Protocol
SIPS - SIP over TLS (Transport Layer Security)
SSL - Secure Sockets Layer
TCP - Transmission Control Protocol
TLS - Transport Layer Security
ZRTP – Zimmerman Real-time Transport Protocol

Sisältö

1. Johdanto

Yksityisyydensuoja internetin palveluissa ja ihmisten välisessä sähköisessä kommunikaatiossa on noussut merkittäväksi keskustelunaiheeksi viimeisen puolentoista vuoden aikana. Aikaisemminkin asia oli herättänyt keskustelua, mutta erityisesti entisen NSA-työntekijän Edward Snowdenin tekemät paljastukset Yhdysvaltain hallinnon suorittamasta massiivisesta verkkotiedustelusta on herättänyt mielenkiintoa viestinnän salaamista ja yksityisyyttä kohtaan. Samaan aikaan puhelut ja viestintä ovat siirtymässä yhä laajemmin internettiin ja IP-pohjaisiin palveluihin. IP-pohjaisuus mahdollistaa monipuolisen viestinnän kiinteällä hinnalla minne päin maailmaa tahansa, ja on edellytys myös sille, että viestintä ei ole enää ainoastaan puhelinvalmistajien ja teleoperaattorien hallinnassa, ja on täten myös vapaasti sovellusten salattavissa. Azfarin ja muiden (2014) tutkimuksessa osoitettiin, että monet suosituimmat VoIP- ja viestintäpalvelut jo salaavat liikenteensä, mutta sittemmin on osoittautunut, että esimerkiksi Skypellä on yhteyksiä NSA:han, ja Snowdenin paljastusten mukaan Skypen välittämää viestintää pystytään seuraamaan (The Guardian, 2013). Tältä pohjalta heräsi mielenkiinto tutkia, voiko yksityishenkilö tai pienyritys parantaa yksityisyyden-suojaansa ja suojata viestintänsä ulkopuoliselta salakuuntelulta ja tiedustelulta.

Tämä tutkielma käsittelee viestinnän ja erityisesti äänipuheluiden yksityisyyttä ja turvallisuutta internettiin kytketyissä mobiililaitteissa. Vastaavaa aiempaa tutkimusta, jossa vertaillaan ja analysoidaan valmiita tuotteita teoriaa vasten, ei ole kovin paljon, joten tässä on mahdollisuus saada aikaan uutta kiinnostavaa tietoa, jota voidaan hyödyntää suoraan ottamalla tuotteet käyttöön tai integroimalla niiden tarjoama palvelu omiin sovelluksiin.

Tutkimuksen tarkoituksena oli tutkia millaisia ratkaisuja puhe-, video- ja tekstiviestinnän salaamiseen on tarjolla mobiililaitteille ja erityisesti yksityishenkilön ja pienyrityksen näkökulmasta. Ensisijaisia kriteerejä haettavalle ratkaisulle ovat hinta, turvallisuuden taso, liitettävyys omiin järjestelmiin sekä käytön helppous. Tutkimuksessa selvitettiin perusteet IP-pohjaiselle puheviestinnälle, tietoturva-ongelmille ja viestinnän salaukselle, jonka jälkeen etsittiin ja vertailtiin valmiita tuotteita tai ratkaisuja, joilla salaus ja yksityisyys voidaan toteuttaa. Tutkimuskysymys on, onko yksityishenkilön tai pienyrityksen mahdollista suojata viestintänsä, kuinka tehokasta se on ja millaisia rahallisia, ajallisia tai teknisiä resursseja menetelmä mahdollisesti vaatii. Tutkimus perustuu kirjallisuustutkimukseen, jonka lisäksi haetaan, luokitellaan ja vertaillaan tarjolla olevia valmiita ratkaisuja kirjallisuustutkimuksessa löydettyjen kriteerien pohjalta.

2. Internetpuhelut, VoIP ja SIP

Internet telephony, ITP ja VoIP ovat usein rinnakkain käytettyjä termejä puhuttaessa internetin välityksellä toimivista puhelinpalveluista. Tässä tutkielmassa käytetään ensisijaisesti sanaa VoIP (Voice over Internet Protocol) tarkoittamaan internetin kautta yhdistettäviä ja siirrettäviä puheluita. Internet on hyvin pitkälle korvannut aiemmat digitaaliseen puheensiirtoon käytetyt suljetut järjestelmät, ja lähes kaikki langallinen ja langaton kommunikaatio on siirtymässä tai siirtynyt käyttämään avoimia internet-standardeja, jotka on kehittänyt Internet Engineering Task Force (IETF) (Sinnreich & Johnston, 2012, s. xxv). IEFT on väljästi organisoitu ryhmä toteuttajia, toimittajia, palvelun tarjoajia ja tutkijoita, jotka työskentelevät yhdessä ratkaistakseen internetin ongelmia, ja kehittävät uusia protokollia (Johnston, 2009, s. 18).

Perinteiset telekommunikaatioverkot ovat edelleen käytössä ja keräävät vielä rahaa operaattoreille, mutta ne kaikki tullaan tulevaisuudessa todennäköisesti korvaamaan IP-pohjaisilla palveluilla. Internet mahdollistaa myös joustavan tavan tuoda muita kommunikointitapoja, kuten pikaviestintä ja videopuhelut, puheluiden rinnalle. Internetissä älykkyys on sovelluksissa eikä laitteissa ja infrastruktuurissa, joten keskitettyä palveluidenhallintaa ei siis enää tarvita. (Sinnreich & Johnston, 2012, s. xxv.) Jotta VoIP-järjestelmän yksityisyydensuojaa ja turvallisuusuhkia voidaan käsitellä, täytyy jäsentää ensin teknologian perusteet. Tässä luvussa käsitellään olennaisimmat VoIP:iin liittyvät termit, protokollat ja teknologiset pääasiat.

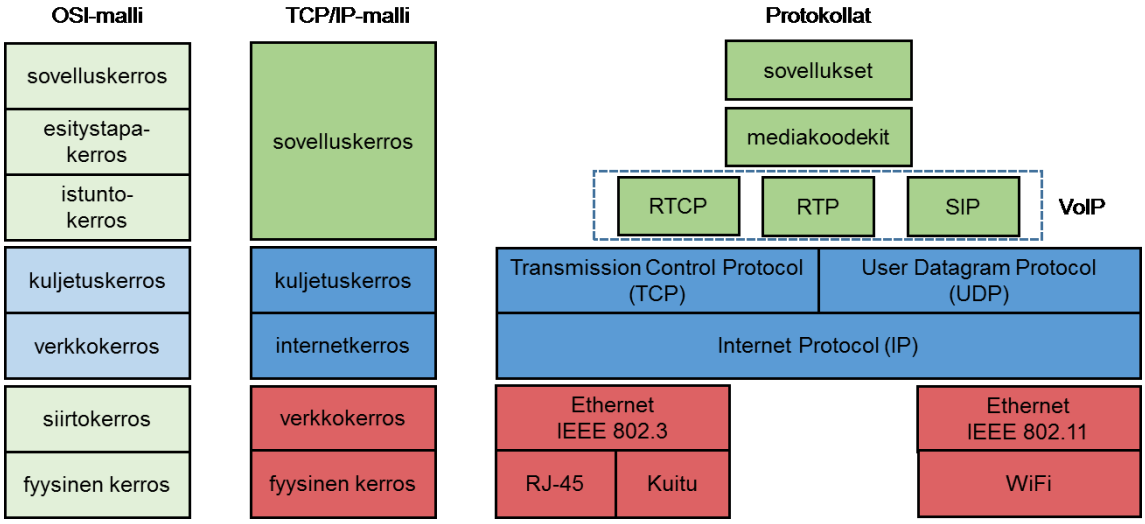
2.1 VoIP-teknologian perusteet

VoIP perustuu Internet Protokollan (IP) päälle rakennettuun teknologiaan. Dwivedi (2009) rinnastaa VoIP-puhelut muihin internetin tiedonsiirtomuotoihin. Samalla tavalla kuin tietokoneet normaalisti keskustelevat TCP/IP:n välityksellä lähettääkseen datapaketteja, VoIP:ssa lähetetään digitaalista ääntä ja videota paketteina. Samalla tavalla kuin dataa lähetetään erilaisilla protokollilla kuten HTTP, POP3, IMAP ja SMTP, VoIP:ssa käytetään omia äänen ja kuvan siirtoon tarkoitettuja protokollia kuten SIP (Session Initiation Protocol), H.323 ja RTP (Real-time Transport Protocol). Puhetta ja videoita lähetetään siis verkossa aivan samaan tapaan kuin dataa, hyödyntäen samaa fyysistä siirtotietä ja muita verkkokerroksia. Ainoastaan sovelluskerrokselle on määritelty puheensiirtoon ja sessionhallintaan liittyviä uusia protokollia. (Dwivedi, 2009, s. 9.)

Protokollat ja niiden suhde toisiinsa kuvataan yleensä pinona, jossa alimpana on fyysinen kerros ja ylimpänä sovellukset. Open Systems Interconnection Reference Model, eli OSI-malli kuvaa tiedonsiirtoprotokollien pinon seitsemässä kerroksessa. Kukin kerroksista käyttää yhtä alemman kerroksen palveluja ja tarjoaa palveluja yhtä kerrosta ylemmäs. Käytännön protokollapinot on kehitetty kuitenkin yleensä viisiportaisen TCP/IP-viitemallin suhteen, mutta molemmat mallit ovat kuvaus-tarkoituksessa yleisesti käytössä. (Kurose & Ross, 2013). Kuva 1 esittää, miten VoIP-protokollat sijoittuvat OSI-malliin ja TCP/IP-malliin.

Kuvasta nähdään, että VoIP-protokollat ovat TCP/IP-mallissa sovelluskerroksen protokollia, mutta tarkemmin eri kerrokset kuvaavassa OSI-mallissa ne kuuluvat

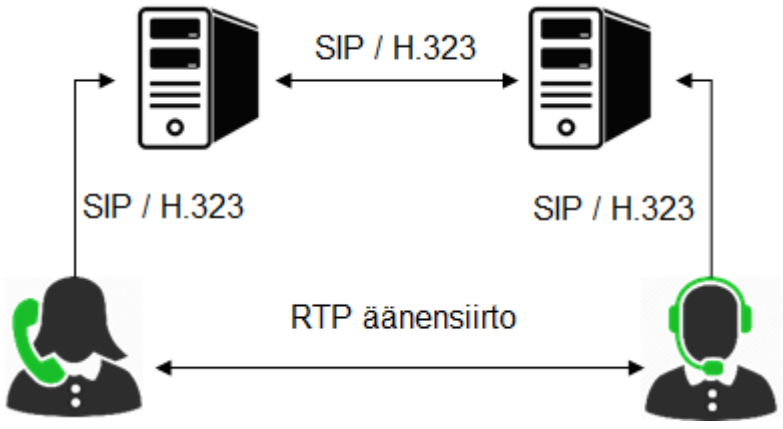
istuntokerrokseen, jonka päälle varsinainen VoIP-sovellus rakentuu esitystapa- ja sovelluskerroksille (Katz ja muut, 2006).



Kuva 1. VoIP-protokollat OSI- ja TCP/IP-mallissa.

VoIP-palvelu ja protokollat rakentuvat siis täysin olemassa olevien tavallisten kuljetuskerroksen protokollien päälle, eikä niitä varten ole tarvinnut kehittää mitään uutta protokollapinon alemmille kerroksille.

VoIP-puhelun muodostamiseen tarvitaan yleensä myös palvelimia kuten välityspalvelin ja rekisteri (SIP Proxy/Registrar) tai H.323 Gatekeeper/Gateway. Näistä tarkemmin myöhemmissä luvuissa, mutta yksinkertaistettuna palvelimia käytetään puhelun osapuolten löytämiseen, yhdistämiseen sekä puhelun muodostukseen ja hallintaan. Kun puhelu on saatu muodostettua, puhedata eli digitaalinen ääni siirretään RTP-mediaprotokollalla suoraan puhelun osapuolten välillä. (Dwivedi, 2009, s. 10.) Kuva 2 havainnollistaa protokollien käyttöä järjestelmän entiteettien välillä.



Kuva 2. VoIP-protokollat

Pääasialliset VoIP-puheluissa käytettävät protokollat ovat siis SIP, H.323 ja harvinaisempi IAX puhelujen yhdistämiseen ja muodostamiseen, sekä RTP median eli itse puheen siirtoon. Protokollat jakautuvat siis selkeästi sessio- ja mediaprotokolliin, joista ensimmäisillä muodostetaan ja hallitaan puhelua ja toisilla siirretään puhedataa (Dwivedi, 2009, s. 9.) Sinnreich ja Johnston (2012) mukaan RTP on oikeastaan ainoa nykyään käytössä oleva mediansiirtoprotokolla VoIP-puheluissa. SIP-protokollasta

puolestaan on tullut alan hallitseva standardi sessionhallintaan sekä VoIP-puheluissa että muussa viestinnässä. Käytännössä kaikki julkiset VoIP-palveluiden tarjoajat käyttävät SIP-protokollaa tai sen johdannaista sessionhallintaan, ja väittely SIP, H.323 ja muiden protokollien välisestä paremmuudesta on käytännössä käyty loppuun ja kuihtunut. (Sinnreich & Johnston, 2012, s. xxv.) Merkittävät globaalit toimijat kuten ETSI ja 3GPP ovat hyväksyneet ja ottaneet SIP-protokollan ja muut reaaliaikaviestintään liittyvät IEFT:n määrittelemät standardit käyttöön (Geneiatakis ja muut, 2005, s. 1). Voidaan siis sanoa, että SIP:stä on tullut niin merkittävä standardi alalle, että muita sessionhallintaprotokollia ei kannata enää tutkimuksissa edes käsitellä (Sinnreich & Johnston, 2012, s. xxv). Tässä tutkimuksessakin sivuutettiin muut protokollat kuin SIP sessionhallinnan osalta.

2.2 Monipuolinen viestintä ja lisäpalvelut

Läsnäolon hallinta (Presence) ja pikaviestintä (Instant Messaging, IM) ovat puheviestinnän lisäksi merkittävä osa nykyaikaisia VoIP-palveluita. Läsnäololla tarkoitetaan henkilön tai laitteen kykyä kommunikoida muiden kanssa ja välittää saavutettavuuden tasoja (Camarillo, 2001, s. 113). Se on siis muille jaettava tietoisuus siitä, onko henkilö tai laite läsnä, ja voidaanko häneen ottaa yhteyttä (Johnston, 2009, s. 189). Kun henkilön saavutettavuus on julkista, voidaan heti tietää, onko kyseinen henkilö käytettävissä vastaamaan puheluun tai pikaviestiin (Camarillo, 2001, s. 180). Pikaviestintä on merkittävä osa kommunikointia nykyään, ja erityisesti nuoremman sukupolven suosiossa (DigitalStrategyConsulting, 2014). Tietyissä tapauksissa pikaviestinnällä voidaan korvata puheviestintä, esimerkiksi kun vaaditaan hiljaisuutta tai, kun halutaan keskittyä useampaan asiaan yhtä aikaisesti. Pikaviestipalvelut mahdollistavat usein myös keskusteluryhmien muodostamisen, jolloin useampi kuin kaksi henkilöä voivat osallistua samaan keskusteluun (Porter, 2006). Yleensä sama sovellus yhdistää kaikki nämä peruspalvelut yhdeksi toimivaksi kokonaisuudeksi, jolla voidaan hoitaa kaikki kommunikaatiotarpeet.

2.3 Turvallisuuden perusteet ja palvelun laatu

VoIP-teknologiaan kohdistuu yksityisyydensuoja- ja turvallisuusongelmia samalla tavalla kuin mihin tahansa teknologiaan, jota käytetään siirtämään luottamuksellista tietoa verkon yli. Teknologian perusteet tuntien, voidaan käsitellä lyhyesti VoIP:iin liittyviä turvallisuusuhkia ja palvelun laatua. VoIP:ssa, kuten minkä tahansa verkossa toimivan palvelun yhteydessä, määrätyt asiat tulevat aina eteen puhuttaessa yksityisyydestä, turvallisuudesta ja tietoturvasta. Nämä ovat autentikointi (todennus), luvitus, saatavuus, luottamuksellisuus ja eheyden ylläpito (Dwivedi, 2009, s. 13).

Autentikointiprosessi useimmissa VoIP-toteutuksissa tapahtuu sessiotasolla. Kun asiakas liittyy palveluun tai muodostaa puhelun, autentikointi tapahtuu VoIP-sovelluksen ja palvelimen välillä. Mediaprotokolla, yleensä RTP, ei vaadi enää erillistä autentikointia, sillä se on hoidettu jo sessionmuodostusvaiheessa. (Dwivedi, 2009, s. 13.) SIP-palvelimien kanssa yleisesti käytetty Digest authentication ei ole kovin vahva autentikointimenetelmä ja siihen liittyy monia tietoturvariskejä, joita käsitellään tarkemmin luvussa kolme (Geneiatakis ja muut, 2005, s. 4).

Luvitusta voidaan käyttää lisänä turvallisuutta takaamassa. Voidaan esimerkiksi rajoittaa teknisin keinoin asiakkaiden liittymistä verkkoon. Tätä voi olla usein kuitenkin hankala toteuttaa käytännössä, jotta verkko pysyy joustavana ja käytettävänä. Luvituksella asetetut rajoitukset ovat usein myös helposti teknisesti ohitettavissa. Esimerkkejä luvituksesta ovat MAC-osoitteen (Media Access Control) perusteella

tapahtuva laitteiden suodatus ja URI-liitteen (Universal Resource Identifier) avulla tehty luvitus. (Dwivedi, 2009, s. 13.)

Saatavuus ja palvelun laatu ovat todella tärkeitä asioita VoIP-verkoissa. Ihmiset olettavat, että puhelut toimivat ja äänenlaatu on hyvä kun puhelua tarvitaan. Käyttäjien kärsivällisyys ei usein riitä kovinkaan kauan, jos palvelu on epäluotettava tai huonolaatuinen. Camarillon (2001) mukaan useimmille sovelluksille internetin ”paras yritys” palvelumalli toimii hyvin, kun verkko ei ole erityisen kuormittunut. VoIP-tyyliselle päästä-päähän liikenteelle kuormittunut verkko voi kuitenkin tuottaa ongelmia. Liikenteen jonoutuminen verkon solmuihin voi johtaa siihen, että viiveet kasvavat liian suuriksi, ja paketteja alkaa kadota. Kadonneet paketit ja viiveet johtavat palvelun laadun (Quality of Service, QoS) heikkenemiseen. Äänipuheluiden tapauksessa se tarkoittaa äänen puuroutumista, pätkimistä tai häviämistä. (Camarillo, 2001, s. 74.) Dwivedin mukaan VoIP-puheluiden kanssa voidaan käyttää tiettyjä QoS-menetelmiä, joiden avulla tietyn tyyppisille palveluille ja paketeille taataan tietty laatutaso. Monessa tapauksessa audiopaketit priorisoidaan verkossa datapakettien edelle. Myös puheen erottamista omaan virtuaaliseen verkkoonsa voidaan käyttää, mutta tämä ei ole kovin yleistä. (Dwivedi, 2009, s. 15.)

Luottamuksellisuus ja eheys ovat tärkeä osa palvelua, jotta käyttäjät voivat olla varmoja puheluidensa yksityisyydestä, ja että heidän puheluitaan ei salakuunnella, ja ne tulevat täydellisinä ja muuntelemattomina perille (Camarillo, 2001, s. 307). VoIP-liikenteen salaus voidaan tehdä sekä sessionhallinta- että mediansiirtotasoilla. Dwivedin (2009) mukaan yleensä pyritään salaamaan molemmat tasot, jolloin sekä session autentikointi-informaatio että varsinainen kommunikaatio salataan. Yleisimmät menetelmät VoIP-verkkojen salaamiseen ovat IPSec (Internet Protocol Security), SRTP (Secure Real-time Transport Protocol) sekä SSL (Secure Sockets Layer). IPSec-salaus on monimutkainen OSI-mallin verkkokerroksella toimiva salausmenetelmä, jota voidaan käyttää VoIP ja yleisesti IP-pohjaisen liikenteen turvaamiseen julkisissa tai epäluotettavissa verkoissa kuten internet. SRTP-protokollaa käytetään median eli itse puheen salaamiseen VoIP-puheluissa. SRTP hyödyntää yleensä AES-salausta (Advanced Encryption Standard). SSL-salausta käytetään VoIP-sessionhallinta protokollien paketointiin salattuun muotoon. (Dwivedi, 2009, s. 15.) Salausmenetelmiä käsitellään tarkemmin luvussa neljä.

3. Protokollat ja tietoturva

Lähes kaikki merkittävät VoIP-toteutukset perustuvat SIP-pohjaiseen sessionhallintaan ja RTP-perustaiseen mediansiirtoon. Jotta voidaan ymmärtää VoIP:iin ja siihen liittyviin protokolliin kohdistuvia tietoturvaongelmia, täytyy protokollien perusteet ja toiminta ymmärtää. Tässä luvussa esitellään SIP- ja RTP-protokollat ja niiden toiminta tarkemmin, sekä esitellään niihin spesifisesti liittyvät tietoturvaongelmat.

3.1 Sessionhallinta ja SIP-protokolla

SIP on sovellustason signalointiprotokolla multimediasessioiden luontiin, muokkaukseen ja lopettamiseen yhden tai useamman osallistujan kesken (Rosenberg ja muut, 2002). SIP-viesti voi olla pyyntö tai kuittaus pyynnölle, ja se kostuu aina otsikosta ja viestin sisällöstä. Tyypillinen SIP-pohjainen VoIP-ratkaisu sisältää neljä osaa: käyttäjäagentti (User agent), rekisteri (Registrar), uudelleenohjauspalvelin (Redirect server) ja välityspalvelin (Proxy server). Kuten muutkin samantyyliset internet-sovellusprotokollat, SIP noudattaa asiakas-palvelin arkkitehtuuria. Rekisteri ja välityspalvelimet hallinnoivat SIP-viestintää siten, että välityspalvelimen vastuulla on viestien reitittäminen kohteisiin, ja rekisteri käsittelee käyttäjäagenttien liittymistä järjestelmään sekä rekisteröintiä (Geneiatakis ja muut, 2005, s. 2). SIP-protokolla kuuntelee yleensä TCP tai UDP porttia 5060, mutta se voidaan asettaa myös muuhun haluttuun porttiin. Johnston (2009, s. 51-65) kuvaa eri osien tarkoitusta ja toimintaa seuraavasti:

Käyttäjäagentti (User agent) on joko ohjelmistopohjainen tai varsinainen laite, jossa on SIP/VoIP soitto-ominaisuus. Käyttäjäagentti muodostaa lähtevät ja hyväksyy tulevat puhelut.

Rekisteri (Registrar) rekisteröi käyttäjäagentit verkkoon ja niitä voidaan käyttää myös käyttäjien autentikointiin.

Uudelleenohjauspalvelin (Redirect server) hyväksyy SIP-pyynnöt ja palauttaa osoitteen johon käyttäjäagentin täytyy ottaa yhteyttä suorittaakseen loppuun pyyntönsä.

Välityspalvelin (Proxy server) välittää liikennettä käyttäjäagenttien ja muiden laitteiden tai sijaintien välillä. Niitä voidaan käyttää myös reititykseen ja autentikointiin. Välityspalvelimia voidaan käyttää myös VoIP-pakettien siirtämiseen verkon palomuurien yli.

SIP-protokolla on rakennettu samana tapaan kuin HTTP-protokolla. Molemmat perustuvat pyyntöihin ja vastauksiin, joilla toteutetaan määriteltyjä toimintoja (Dwivedi, 2009, s. 20). Johnston (2009, s. 73-85) esittää yleisimmät SIP-metodit ja niitä vastaavat toiminnot seuraavasti:

INVITE–metodia käytetään pyytämään toinen käyttäjäagentti puheluun. Se lähetetään agentilta toiselle, ja se voi kulkea useiden eri SIP-verkon laitteiden kautta.

REGISTER–pyyntö rekisteröi käyttäjäagentin rekisteripalvelimelle.

ACK–viesti lähetään käyttäjäagentilta toiselle vahvistamaan, että lähetetty viesti tuli perille. ACK on yleensä kolmas vaihe puhelunmuodostusprosessissa, jonka jälkeen itse median eli puhedatan siirto voi alkaa.

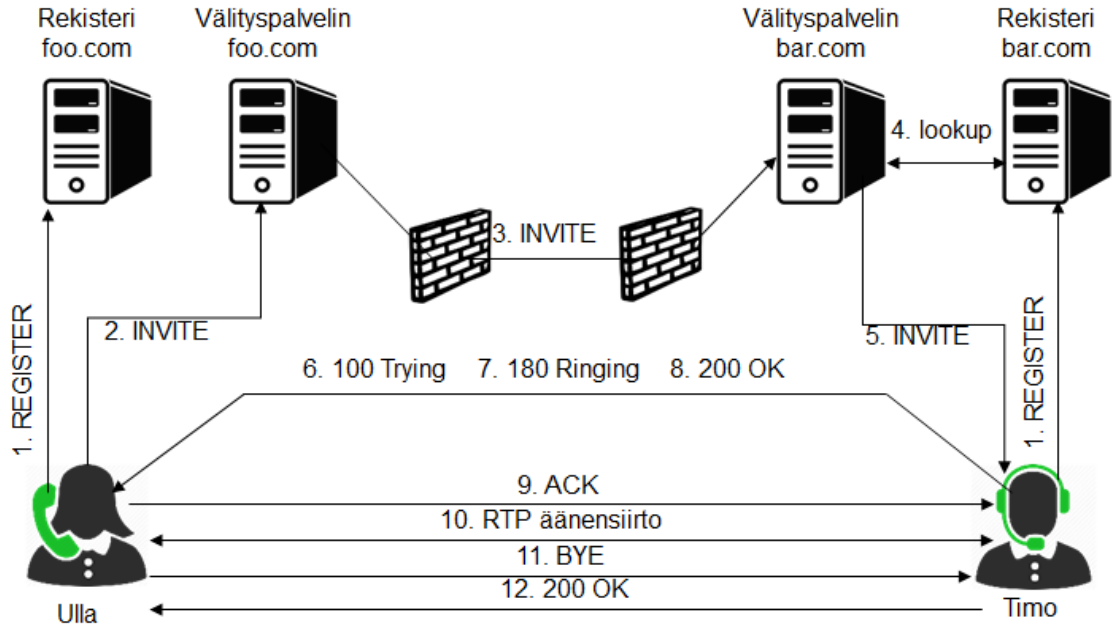
CANCEL–metodi peruuttaa olemassa olevan INVITE session. Käyttäjäagentti voi lähettää CANCEL -pyynnön myös hylätäkseen tulevan puhelun.

BYE–metodi katkaisee käynnissä olevan puhelun tai session.

OPTIONS–metodia käytetään käyttäjäagentin tai välityspalvelimen kyvykkyyksien eli tuettujen ominaisuuksien kyselyyn.

SIP-viestit koostuvat yleensä metodista ja kentistä kuten *To, From, Contact, Call-ID, CSeq, Content-Type* ja *Content-Length*. Näillä kentillä määritellään lähettäjä, vastaanottaja, IP-osoitteet, puhelun tunniste, viestien järjestys ja sisältö. Kaikki on perusmuodossaan tekstimuotoista ja selväkielistä, joten tietoturva on näissä ilman salausta olematon. (Dwivedi, 2009, s. 21.)

Kuvassa 3 esitetään esimerkki VoIP-puhelusta SIP-protokollaa käyttäen. Esimerkissä on kaksi käyttäjää (Ulla ja Timo), joiden välillä puhelu muodostetaan. Kuvaus perustuu Dwivedin (2009) esitykseen aiheesta.



Kuva 3. SIP-protokollan komennot.

Ensimmäisessä vaiheessa molempien käyttäjien käyttäjäagentit rekisteröityvät omille palvelimille käyttäen REGISTER-metodia. Autentikointi järjestelmään suoritetaan yleensä tässä vaiheessa. Toisessa vaiheessa Ulla aloittaa puhelun Timolle, jolloin Ullan käyttäjäagentti lähettää INVITE-pyynnön välityspalvelimelle. Palvelin välittää pyynnön mahdollisten palomuurien läpi Timon välityspalvelimelle, joka etsii Timon sijainnin verkossa, ja lähettää Ullan käyttäjäagentille 100 Trying-viestin ilmoittaen, että INVITE-pyyntö on vastaanotettu. Kun Timon käyttäjäagentti alkaa hälyttää, se lähettää Ullalle viestin 180 Ringing, ilmaisten että puhelin hälyttää. Kun Timo vastaa puheluun, hänen käyttäjäagenttinsa lähettää Ullalle viestin 200 OK, tarkoittaen, että puhelussa voidaan siirtyä äänensiirtoon. Ulla hyväksyy viestin ACK-metodilla, ja RTP-pohjainen

äänensiirto puhelussa alkaa. Puhelun lopetus tapahtuu lähettämällä BYE-metodi, jonka toinen osapuoli kuittaa OK-viestillä. (Dwivedi, 2009, s. 24.)

3.2 SIP-protokollaan liittyvät tietoturvauhkat

Protokollan tai sovelluksen turvallisuusanalyysi tehdään yleensä laatimalla lista mahdollisista uhkista, jonka jälkeen tutkitaan turvallisuusmekanismeja, joilla uhkia vastaan voidaan suojautua (Johnston, 2009, s. 311.) Monissa lähteissä kaksi uhkaa erottuu selvästi hallitsevimpina. Johnstonin (2009) ja muiden lähteiden mukaan kaksi suurinta uhkaa SIP- ja yleisesti internetviestintää kohtaan ovat palvelunesto- (Denial of Service, DoS) ja mies välissä (Man in the Middle, MitM) -hyökkäykset. Palvelunestohyökkäyksessä kolmas osapuoli yrittää keskeyttää tai estää protokollan tai palvelun toiminnan. Gupta & Shmatikov (2006) kuvaama esimerkki palvelunesto-hyökkäyksestä on pakettitulva (ATK-slangissa floodaus), jossa hyökkääjä lähettää valtavavan määrän IP-paketteja kohteeseen, jotka ylikuormittavat vastaanottavan kohteen paketteja käsittelevän laitteen tai sovelluksen. Tämä voidaan suorittaa vielä tehokkaammin myös useammalta koneelta kerralla, jolloin sitä kutsutaan hajautetuksi palvelunestohyökkäykseksi (Distributed Denial of Service, DDoS) (Gupta & Shmatikov, 2006.) Mies välissä -hyökkäyksessä tunkeudutaan kahden viestijäosapuolen väliin tarkoituksena muuttaa tai poistaa viestejä kommunikaatiosta, tai lisätä väliin uusia viestejä (Dwivedi, 2009, s. 38). Mies välissä -hyökkäys on vaikeampi toteuttaa kuin palvelunesto, sillä se vaatii hyökkääjältä pääsyn verkon solmuun, jonka kautta paketit kulkevat.

Muita mahdollisia, mutta ei niin yleisiä tietoturvauhkia ovat toisena esiintyminen, jossa hyökkääjä saa koneensa näyttämään SIP-käyttäjältä tai -serveriltä ja identiteettivarkaus, jossa hyökkääjä varastaa käyttäjän tunnukset, ja saa siten pääsyn toisen henkilön viestintään. Kaikki nämä uhkat pätevät puhelusessioiden muodostukseen, saatavuustiedon vaihtoon sekä pikaviestintään. (Johnston, 2009, s. 312.) Nämä uhkat eivät ole mitenkään erityisesti vain VoIP-puheluille ominaisia, vaan koskevat yhtä lailla kaikkea internetliikennettä.

3.3 Mediansiirto ja RTP-protokolla

RTP (Real-time Transport Protocol) on oikeastaan ainoa käytetty mediansiirtoprotokolla VoIP-puheluissa. Se kehitettiin alun perin mahdollistamaan reaaliaikainen ääntä, videota tai muuta dataa sisältävien datapakettien siirto IP-protokollan yli (Johnston, 2009, s. 273). RTP:n kanssa käytetään yleensä parina RTCP-protokollaa (Real-time Control Protocol) lähettämään signalointia ja kontrollidataa puhelun osapuolien välillä (Dwivedi, 2009, s. 73). RTP on verrattain yksinkertainen UDP-kuljetuskerrosta hyödyntävä protokolla, jonka periaatteet ovat hyvin samanlaiset kuin muillakin vastaavilla protokollilla. RTP-paketit sisältävät sekvenssinumeron, aikaleiman, tietosisällön sekä tietoa lähteestä (Camarillo, 2001, s. 71). Schulzrinnen (2004) mukaan aikaleimoja käytetään pakettien järjestelyyn soittopuskurissa, jolloin äänestä saadaan kelvollista, vaikka välistä puuttuisikin paketteja. Sekvenssinumeroita käytetään tunnistamaan pakettihävikkiä. RTP tarjoaa myös jonkun verran luotettavuutta median siirtoon, vaikka se hyödyntääkin UDP-protokollaa, mikä on sinänsä epäluotettava kuljetuskerroksen protokolla. RTCP:n käyttö RTP:n rinnalla mahdollistaa pakettihävikin tunnistamisen ja viiveiden kompensoinnin, jolloin huonoissa verkoissa voidaan käyttää esimerkiksi pienempää bittivirtaa (Porter, 2006, s. 167).

3.4 RTP-protokollaan liittyvät tietoturvauhkat

Dwivedin (2009) mukaan VoIP:iin liittyvät tietoturvauhkat liittyvät useimmiten median turvattomuuteen, eli RTP-liikenteen kaappaamiseen ja salakuunteluun. RTP-protokolla ei itsessään sisällä minkäänlaista salausta tai tarjoa yksityisyyttä, jonka vuoksi siihen kohdistuu monenlaisia turvallisuusriskejä. Vaikka usein käytetty Secure RTP (SRTP) sisältää salauksen, ei sitä aina kuitenkaan ole käytetty sen vaatimien suorituskyky tai käytettävyysongelmien takia. RTP on haavoittuvainen monille erityyppisille hyökkäyksille kuten kaappaus, muokkaus, salakuuntelu ja äänen manipulointi. RTP-protokollan käytössä oletetaankin yleensä, että turvallisuus tulee sen ulkopuolelta. (Dwivedi, 2009, s. 75.)

Dwivedin (2009) mielestä salakuuntelu, äänen injektointi ja palvelunesto ovat pahimmanlaatuisia yksityisyydensuojan uhkia ääni- ja videopuhelulle. Jos palvelu on salakuunneltavissa, sen käytöstä puuttuu luottamuksellisuus, joka on oleellinen osa äänipuheluita. Jos linjalle voidaan injektoida ylimääräistä ääntä, puhelun eheys ja koskemattomuus ovat uhattuina. Jos puhelut voidaan lopettaa tai estää, palvelun luotettavuus ja käyttövarmuus heikkenee. VoIP-puhelut ovat täysin vailla tietoturvaa ilman luottamuksellisuutta, eheyttä ja luotettavuutta (Dwivedi, 2009, s. 91).

3.4.1 Salakuuntelu

Salaamattomat RTP-paketit voidaan helposti kaapata ja tallentaa verkosta, aivan kuten mikä tahansa salaamaton internetliikenne. VoIP-puhelun tapauksessa muutaman satunnaisen paketin kaappaaminen ei yleensä avaa paljoakaan sensitiivistä informaatiota kaapparille, vaan käytännössä tarvitaan koko puhelun sisältävä pakettivirta, jotta siitä voidaan muodostaa kokonaisia keskusteluita. Tämä tekee VoIP-puhelun audion kaappaamisesta hieman hankalampaa kuin tavallisen dataliikenteen, mutta se on silti täysin mahdollista. Dwivedin (2009) mukaan työkalut kuten Cain & Abel sekä Wireshark tekevät RTP-audion kaappaamisesta jopa melkein helppoa. Näillä työkaluilla voidaan kaapata automaattisesti RTP-pakettisekvenssi ja tallentaa se suoraan oikeassa järjestyksessä kuunneltavaksi audiotiedostoksi. Tämä mahdollistaa sen, että kuka tahansa passiivinen salakuuntelija voi muutamalla klikkauksella kaapata ja salakuunnella salaamatonta VoIP-liikennettä omassa aliverkossaan. (Dwivedi, 2009, s. 76.)

Passiivisen salakuuntelun lisäksi RTP on haavoittuvainen myös aktiivisille hyökkäyksille. Käyttäen esimerkiksi Wireshark työkalua, voidaan haistella verkosta VoIP-liikennettä, ja sitten suorittaa aktiivisia hyökkäyksiä kuten äänen injektointi RTP-päätepisteeseen. Esimerkkinä Dwivedi (2009) käyttää pörssivälittäjien väliseen puheluun injektoitua viestiä, ”myy hintaan xx”, jolloin vastaanottaja erehdyksissään voi myydä osakkeita epäedulliseen hintaan ja menettää rahaa. Aktiiviset hyökkäykset ovat yleisesti ottaen huomattavasti vaikeampi toteuttaa kuin passiiviset, mutta niidenkin toteuttamiseen löytyy useita valmiita työkaluja ja menetelmiä. (Dwivedi, 2009, s. 82.)

3.4.2 Palvelunesto

Palvelunestohyökkäys voidaan Dwivedin (2009) mukaan kohdistaa myös RTP-protokollaan, vaikkakin se on huomattavasti helpompi suorittaa sessionmuodostus-protokollia vastaan. RTP-protokollaan kohdistettu palvelunestohyökkäys on kuitenkin vaikutuksiltaan jopa pahempi kuin SIP-protokollaan kohdistettu, koska RTP kontrolloi itse äänen siirtoa puhelussa (Dwivedi, 2009, s. 82). RTP-palvelunestohyökkäyksiä on kahta päätyyppiä: viestitulva, session purkaminen.

Viestitulvassa lähetetään olemassa olevan VoIP-puhelun osapuolille valtava määrä RTP-paketteja, jotka ne joutuvat käsittelemään. Tarkoituksena tällaisella hyökkäyksellä on saada palvelu tukkoon, kun se joutuu tarkastamaan jokaisen vastaanotetun paketin otsikkotiedot. Session purkaminen valheellisella tiedolla voi onnistua lähettämällä RTCP BYE -viesti puhelun toiselle osapuolelle, jolloin järjestelmä luulee, että puhelu täytyy lopettaa. RTCP BYE viesti ilmoittaa, että toinen osapuoli ei ole enää aktiivinen, ja RTP-yhteyttä ei pidä enää käyttää. (Dwivedi, 2009, s. 89-90.)

3.5 Viranomaisten harjoittama salakuuntelu ja vakoilu

Viranomaisten suorittama verkkovakoilu on myös mainittava tietoturvariskinä tai vähintäänkin yksityisyydensuojaan kohdistuvana loukkauksena. Perinteisten lanka- ja matkapuhelinten salakuuntelua on varmasti harjoitettu viranomaisten toimesta niin kauan kuin puhelimia on ollut olemassa. Tämähän on hyvä tapa päästä rikollisten jäljille, ja saada tietoa ja todisteita rikollisesta toiminnasta. VoIP-puheluiden yleistyminen sai viranomaiset etenkin Yhdysvalloissa toimimaan lainsäädännön puolesta, joka mahdollistaisi myös elektronisen viestinnän laajamittaisen salakuuntelun (Electronic Frontier Foundation, 2015b).

Yhdysvalloissa on vuodesta 1994 alkaen voimassa ollut Communications Assistance for Law Enforcement Act (CALEA) -laki velvoitti puhelin- ja internetoperaattoreita lisäämään järjestelmiinsä vuoteen 2007 mennessä valtiolliset salakuuntelulaitteet. Lakia on myöhemmin laajennettu koskemaan kaikkea viestintää sisältäen mm. VoIP-puhelut, sähköpostin, pikaviestipalvelut ja sosiaalisen median palvelut. CALEA -lain velvoittamana siis kaikki Yhdysvaltavalaiset palveluntarjoajat joutuvat tarjoamaan viranomaisille keinon järjestelmiensä salakuunteluun ja valvontaan. Näitä palveluja käyttävä joutuu siis tahtomattaan ja väistämättä valtiollisen salakuuntelun piiriin. (Wikipedia / CALEA, 2015.)

Yhdysvaltain turvallisuusviranomaiset kuten FBI ja NSA väittävät käyttävänsä salakuuntelumahdollisuuksia vain rikollisten, terroristien ja vastaavien jäljittämiseen. Edward Snowdenin vuotamat paljastukset NSA:n toiminnasta kuitenkin kertovat järjestelmällisestä ja laajalle levinneestä verkkotiedustelusta ja -vakoilusta, joka ylsi huomattavasti laajemmalle kuin yksittäisten rikollisten seuraamiseen (The Guardian, 2013). Valtiollinen salakuuntelumahdollisuus on rakennettu itse tuotteisiin ja palveluihin sisään, joten sen laajempi analysointi ei ole kovin hedelmällistä. Asian tiedostaminen voi kuitenkin ohjata käyttämään tuotteita, joihin valtiolliset vakoilutoimet eivät ulotu. Jää tietysti uskon varaan, onko tuotteen valinnalla vaikutusta lopputulokseen, jos salakuuntelu ulottuu kaikille verkon osa-aluille, ja tiedustelulla on käytettävissä käytännössä rajattomat resurssit esimerkiksi salausten purkamiseen.

4. VoIP-palvelun turvaaminen

VoIP-palvelun turvaaminen ja liikenteen salaaminen on tärkeää, jotta tärkeät neuvottelut, tiedot ja kommunikaatio siirtyvät ja pysyvät yksityisinä. Organisaatioille ja yksityishenkilöille turvallisuus tarkoittaa yleensä tiedostojen, tietokantojen, sähköpostien ja muiden digitaalisten tallenteiden turvallista säilyttämistä ja käsittelyä, mutta puheliikenne voi olla aivan yhtä suuri turvallisuusriski. Salaamattoman VoIP-puhelun sisältö on helposti kaapattavissa ja tallennettavissa, ja puhelunmuodostusta voidaan häiritä tai ohjata väärään paikkaan mikäli sessionhallintaa ei ole suojattu. Se että VoIP-palvelua käytetään vain organisaation sisällä, ei ole myöskään mikään tekosyy käyttää suojaamatonta palvelua. Suojaukseen ja salaukseen löytyy menetelmiä, jotka on todettu toimiviksi, joten nykyään ei voida mitenkään hyväksyä salaamatonta ratkaisua hankaluuden, hinnan tai teknisten syiden takia.

4.1 Sessionhallinnan turvaaminen

Sessionhallinnan turvaaminen keskittyy tässä tutkimuksessa luonnollisesti SIP-protokollaan. SIP-määrittely ei itsessään sisällä minkäänlaista turvamekanismia, vaan sen sijaan suositellaan käyttämään muita hyvin tunnettuja ja hyväksi havaittuja internet-turvamekanismeja (Geneiatakis ja muut, 2005, s. 5). Rosenberg ja muut (2002) ehdottaa seuraavia menetelmiä käytettäväksi: HTTP digest authentication, Transport Secure Layer (TLS), SIP over SSL (SIPS), IP security (IPsec) ja Secure MIME (S/MIME). Palvelujen kehittäjille on jätetty valinnanvapaus valita näistä toimivin ja sopivin menetelmä omiin sovelluksiinsa. IEFT:n dokumentti *Security Mechanism Agreement for the Session Initiation Protocol RFC 3329*, käsittelee turvallisuusaspekteja monelta kantilta nimenomaan sovelluskehittäjän näkökulmasta, ja auttaa valitsemaan sopivia menetelmiä SIP-protokollan turvaamiseen (Arkko ja muut, 2003).

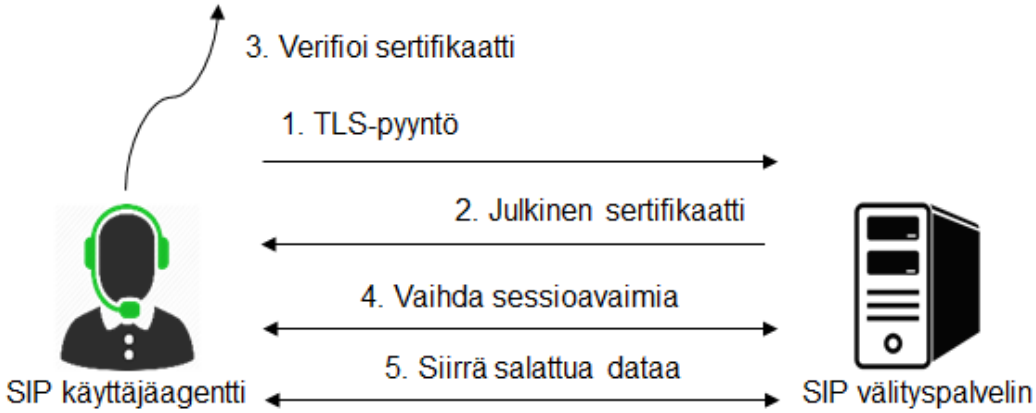
SIP-protokollassa käytetty autentikointitapa on HTTP digest authentication, joka ei ole kovin turvallinen, ja on haavoittuvainen perinteiselle sanakirjahyökkäykselle. Termi sanakirjahyökkäys saa nimensä siitä, että murto-ohjelmalle annetaan lista salasanoista, joita hyökkäyksessä testataan peräkkäin. Ohjelma käy läpi koko listan (esim. sanakirjan) ja testaa olisiko joku sanoista oikea salasana. Yhdistettynä huonoihin salasanoihin tai siihen, että jotkut SIP-toteutukset käyttävät vain neljän numeron pin-koodia salasanana, tekevät SIP-sessionhallinasta haavoittuvaisen hyökkäyksille (Dwivedi, 2009. s. 180).

Autentikointiongelmaan ja muihin SIP-protokollaan liittyvien turvallisuusongelmien ratkaisuun auttaa SIP over SSL (SIPS), jonka avulla voidaan salakirjoittaa sessioprotokollan data SIP-käyttäjäagentilta SIP-välityspalvelimelle. Edelleen SIP-välityspalvelin voi käyttää TLS:ää seuraaviin siirtymiin, jolloin voidaan varmistaa, että koko reitti SIP-asiakkaalta toiselle on päästä päähän salattu. (Dwivedi, 2009. s.181.) Kuvassa 4 esitetään TLS-session muodostus SIP-protokolaan turvaamiseksi.

Dwivedi (2009) kuvaa TLS-autentikointiprosessin seuraavilla askeleilla, jotka ovat samat kuin kuvassa 4.

1. Käyttäjäagentti ottaa yhteyden välityspalvelimelle muodostaakseen TLS-session
2. Välityspalvelin vastaa julkisella sertifikaatilla

3. Käyttäjäagentti validoi sertifikaatin samalla tavalla kuin Web-sivujen sertifikaatit varmistetaan.
4. Käyttäjäagentti ja välityspalvelin vaihtavat sessioavaimia salatakseen ja purkaakseen SIP-session liikenteen.
5. Välityspalvelin muodostaan yhteyden toiseen välityspalvelimeen ja muodostaa TLS-session sen kanssa salatakseen seuraan siirtymän liikenteen.



Kuva 4. TLS-session muodostus.

4.2 Mediansiirron turvaaminen

Secure RTP (SRTP) on protokolla, joka lisää salauksen, luottamuksellisuuden ja koskemattomuuden varsinaiseen puheliikenteeseen eli mediansiirtoon VoIP-puheluissa, jotka käyttävät RTP:tä ja RTCP:tä. Turvallisuus perustuu siihen, että SRTP salaa kryptaamalla RTP-paketin varsinaisen hyötykuorman, eli paketteina siirrettävän puheen (Porter, 2006, s. 413). RTP-otsikkotietoja ei salata, koska verkon päätepisteet kuten reitittimet ja kytkimet tarvitsevat niitä tietoja välittäessään paketteja. SRTP-paketit näyttävät itse asiassa täysin samanlaisilta kuin RTP-paketit, koska vain sisältö on salattu (Dwivedi, 2009. s.181).

SRTP hyödyntää AES-salausta (Advanced Encryption Standard) salakirjoitus-järjestelmänä. AES on symmetrinen lohkosalausmenetelmä, jossa salaus ja purkaminen tehdään useiden kierrosten läpi. Salauskierrosten lukumäärä riippuu käytetyn avaimen pituudesta (128-bittinen, 192-bittinen tai 256-bittinen). AES-salausta pidetään jokseenkin murtamattomana, ja se on yksi yleisimmin käytetyistä ja luotettavimmista salaustavoista. (Yksityisyydensuoja, 2015).

ZRTP on RTP:n laajennus, joka soveltaa Diffie-Hellman (DH) avainsopimusta SRTP-paketteihin, tarjoten avaimenhallintapalvelut VoIP-puhelumuodostukseen kahden päätepisteen välillä (Gupta & Shmatikov, 2006). Se keskittyy ainoastaan mediansiirron turvaamiseen, eikä liity mitenkään sessionhallinnan suojaamiseen. ZRTP luo osapuolten välille yhteisen salaisuuden, jota käytetään luomaan salausavaimet. ZRTP on periaatteiltaan samankaltainen kuin PGP-salaus (Pretty Good Privacy), ja sen tavoitteena on varmistaa, että mies välissä -hyökkäystä ei voi tapahtua kahden päätepisteen välillä (Dwivedi, 2009. s.184). ZRTP:n tarkemmat yksityiskohdat eivät sisälly tähän tutkimukseen. Zimmerman ja muut (2011) määrittelemä RFC 6189 kuvaa menetelmän yksityiskohtaisesti.

4.3 Yksityisyydensuojan ja tietoturvan toteutuminen

VoIP-palvelun turvaaminen ei ole helppo tehtävä, mutta se on erittäin tärkeä, jotta palveluiden yksityisyys, turvallisuus, käytettävyys ja uskottavuus saadaan riittävän hyväksi. TLS, SIPS, SRTP ja ZRTP tekniikoiden käyttöönotto voi olla hankala ja monimutkainen tehtävä, mutta niiden avulla voidaan merkittävästi vähentää hyökkäysmahdollisuuksia VoIP-palveluun. Salauksen toteutus sekä sessionmuodostus- että mediakerroksille mahdollistaa vähintään yhtä hyvän tietoturvan tason kuin perinteisissä puhelinverkoissa.

Salausmenetelmät kuten TLS ja SSL ovat olleet perusvaatimuksia Web-liikenteessä jo vuosikausia, ja niiden käyttöön löytyy valmis infrastruktuuri. VoIP puolella tämä ei ole välttämättä vielä itsestäänselvyys, ja epäyhteensopivuus tuotteiden välillä asettaa esteitä salauksen joustavaan käyttöönottoon. Verkon palomuurit, välityspalvelimet ja muut elementit voivat entisestään vaikeuttaa VoIP-liikenteen salaamista. Myös verkkoelementteihin sisäänrakennettu tuki VoIP-protokollille on monesti edelleen puutteellista.

5. Ratkaisujen evaluointi ja valintakriteerit

Tässä luvussa tarkastellaan tarjolla olevia valmiita viestintäratkaisuja, ja pyritään valitsemaan käyttötarkoitukseen sopivin palvelu. Käyttötarkoitus saadaan muista Oulun yliopiston Sähkö- ja tietotekniikan laitoksella meneillä olevista tutkimuksista, joissa tutkitaan ja rakennetaan tukijärjestelmiä vanhusten ja näkövammaisten avustamiseksi, ja heidän turvallisuuttaan lisäämään. Käyttötarkoituksen pohjalta laadittiin lista ominaisuuksista, jotka ratkaisun täytyisi toteuttaa, ja sellaisia joiden olemassaolo tuo tuotteeseen lisäarvoa. Sopivin ratkaisu valittiin käyttämällä Pugh Concept Selection Process -menetelmää (Pugh, 1981), joka perustuu laajempaan Quality Function Deployment (QFD) -metodologiaan (Cohen, 1997).

Tarjolla olevia palveluita voidaan arvioida monelta kantilta. Tämän tutkimuksen tarkoituksena oli etsiä ratkaisua erityisesti yksityishenkilöiden, pienyritysten ja edellä mainittujen käynnissä olevien tutkimusten näkökulmasta. Turvallisuutta arvioitaessa käytetään avuksi myös Dwivedi (2009), esittelemää tapaa auditoida VoIP-palveluita. Siinä laaditaan kysymyslista, jonka vastausten kautta arvioidaan palvelun turvallisuutta eri osa-alueilla. Tässä tutkimuksessa otetaan kantaa myös palvelun integroitavuuteen omiin sovelluksiin, joten lähdekoodien avoimuus ja ohjelmointirajapinnan (API) saatavuus, jonka kautta palvelua voidaan käyttää, on asetettu yhdeksi ratkaisua puoltavaksi kriteeriksi.

5.1 QFD evaluoinnin apuvälineenä

QFD eli Quality Function Deployment on menetelmä, joka soveltuu strukturoiduksi apuvälineeksi toimimaan päätöksenteon tukena. Sitä käytetään useimmiten tuotekehityksessä, johdossa ja markkinoinnissa tuomaan esille asiakkaan ääni vaatimuksien ja odotusten muodossa. QFD voi auttaa organisaatiota kohdentamaan huomionsa uuden tai olemassa olevan tuotteen tai palvelun ominaisuuksiin, tai auttaa etsimään vaihtoehtoisia ratkaisuja. QFD:n tuloksena saadaan graaffeja ja matriiseja, joita on tarkoitus käyttää tuotteen tai palvelun kehittämiseen ja valintojen tekemiseen. Menetelmä on alun perin kotoisin Japanista, jossa Yoji Akao ja Shigeru Mizuno kehittivät sen alun perin 1960-luvun alussa. (Cohen, 1997.)

QFD sisältää useita erilaisia työkaluja ja menetelmiä, joita voidaan soveltaa käyttötarpeesta riippuen. Tässä tutkimuksessa oli tarkoitus löytää vaihtoehtoisista valmiista ratkaisuista käyttötarpeeseen parhaiten soveltuva, joten QFD menetelmään liittyvistä työkaluista valittiin Pugh Concept Selection Process -menetelmä. Se on Stuart Pughin keksimä päätöksenteon matriisimenetelmä, kvantitatiivinen tekniikka, jonka avulla voidaan asettaa konsepteja paremmuusjärjestykseen vaatimusten tai moniulotteisten vaihtoehtojen perusteella (Burge, 2009). Päätöksentekoa varten menetelmässä luodaan valintamatriisi, jossa riveinä ovat vaatimukset ja sarakkeina evaluoitavat kandidaatit. Jokaiselle vaatimukselle voidaan antaa myös painotuskerroin, jos halutaan painottaa valinnassa erityisesti tiettyjä osa-alueita.

Kuva 5 esittää esimerkkiä valintamatriisista. Symboleilla plus (+), miinus (-) ja (s) kuvataan vaatimuksen toteutumista verrattaessa kandidaattia referenssituotteeseen. Yksi kandidaateissa valitaan referenssituotteeksi tai ns. perustasoksi, joihin muita verrataan.

Yleensä referenssituotteeksi valitaan nykyinen ratkaisu tai jo aiemmin hyvin tunnettu konsepti (Burge, 2009).

	Vaihtoehdot			
Vaatimukset	**Painotus**	**1**	**2**	**3**
Vaatimus 1	**10**	s	s	-
Vaatimus 2	**2**	s	s	s
Vaatimus 3	**4**	s	+	+
∑+		**0**	**1**	**1**
∑-		**0**	**0**	**1**
∑s		**3**	**2**	**1**
Painotettu summa		**3**	**6**	**-5**

Kuva 5. Esimerkki Pugh valintamatriisista.

Lopputulosta tulkittaessa voidaan tarkastella plussien ja miinusten määriä, tai painotettua summaa, jossa on laskettu yhteen plussat ja miinukset ja kerrottu tulokset painotuskertoimilla (Burge, 2009). Paras vaihtoehto on periaatteessa se, jonka painotettu summa on suurin.

5.2 Vaatimusten luokittelu ja selitykset

Turvallisten puhelu- ja viestintäpalvelujen hakua ja vertailua varten valittiin joukko vaatimuksia, joiden avulla ratkaisuja vertailtiin. Ideaalinen ratkaisu toteuttaisi kaikki vaatimukset ja saisi täydet pisteet valintamatriisissa. Painotukset on valittu niin, että valitun käyttötarkoituksen kannalta olennaiset vaatimukset saavat suuremman painotuksen kuin toiset.

5.2.1 Tietoturva vaatimukset

Tietoturvavaatimuksia kirjattiin neljä kappaletta. Sessionhallinnan suojaus ja äänensiirron salaus ovat aivan oleellinen osa VoIP-palvelun turvallisuutta. Kokonaisturvallisuutta arvioitaessa otetaan näiden lisäksi huomioon tuotteen mahdollinen tilanne valtiollisessa salakuuntelussa.

1. Sessionhallinta suojattu: Sessionhallinta on suojattu TLS tai SIPS menetelmällä. Tämä on yksi tärkeimpiä asioita arvioitaessa tietoturvaa, joten painoarvo on 10.
2. Äänensiirto salattu: Mediansiirto on suojattu SRTP/ZRTP protokollilla. Tämä on myös yksi tärkeimpiä asioita arvioitaessa tietoturvaa, joten painoarvo on 10.
3. Äänensiirto päästä-päähän salattu: Mediansiirto on suojattu päästä-päähän, niin että sitä voi missään vaiheessa kaapata salaamattomana tuntematta avaimia. Tuo lisäparannusta yksityisyyden suojaan, joten painoarvo on 5.
4. Kokonaisturvallinen: Tämän vaatimuksen toteuttaa, jos tuote on teknisesti turvallinen ja todennäköisesti ei ole valtiollisen salakuuntelun piirissä. Valtiollisen salakuuntelun mahdollisuutta voidaan vaan spekuloida, joten tälle annettiin vähäisempi painoarvo 7.

5.2.2 Ominaisuudet

Toivottavia ominaisuuksia vaatimuksiin kirjattiin myös neljä kappaletta. Monissa palveluissa oli paljon muitakin ominaisuuksia, kuin tässä listatut, mutta käyttötarkoituksen kannalta niillä ei ollut merkitystä, joten niitä ei otettu vaatimuksiin mukaan.

1. Äänipuhelut: Painoarvo 10
2. Videopuhelut: Painoarvo 10
3. Pikaviestit: Painoarvo 5
4. Läsnäolo: Painoarvo 1

5.2.3 Liitettävyys

Liitettävyydellä tarkoitetaan palvelun käyttämistä omista sovelluksista. Tämä voidaan käyttää integroimalla lähdekoodit suoraan tai käyttämällä ohjelmisto ohjelmointirajapinnan, eli API:n (Application Programming Interface) kautta. Avoin lähdekoodi saa tässä vertailussa paljon painoarvoa, koska sen kautta voidaan myös tarkistaa tietoturvaratkaisujen toteutukset luotettavaksi, sekä varmistu siitä, että ohjelmistoissa ei ole vakoilun tai salakuuntelun mahdollistavia takaportteja.

1. Avoin lähdekoodi: Painoarvo 10
2. Liitettävyys omiin sovelluksiin (API): Painoarvo 8

5.2.4 Tuetut alustat

Tuettujen alustojen vaatimuksiin laitettiin suosituimmat mobiililaitteiden ja pöytätietokoneiden käyttöjärjestelmät. Kaikille alustoille annettiin sama painoarvo 5. Valitut alustat vertailuun ovat:

1. Android
2. iOS
3. Windows Phone
4. Linux
5. OSX
6. Windows

5.2.5 Käytettävyys ja hinta

Käytettävyys on hyvin subjektiivinen asia, ja sille ei asetettu tässä vertailussa suurta painoarvoa. Hinta vaatimuksena tarkoitti tässä vertailussa käytännössä ilmaista, sillä käyttötarkoitus ja kohderyhmä eivät pysty eivätkä yleensä halua käyttää rahaa tällaisen palvelun hankkimiseen ja käyttöön.

Käytettävyys: Painoarvo 3
Hinta: Painoarvo 3

6. Tarjolla olevat ratkaisut

Ratkaisuja arvioitaviksi VoIP-palveluiksi etsittiin internetin avulla. Etsinnässä käytettiin avuksi Google hakukonetta ja aiheeseen vihkiytyneitä sivustoja. On silti täysin mahdollista, että joitakin mielenkiintoisia ja käyttökelpoisia salauksen toteuttavia VoIP-palveluita jäi löytämättä. Tässä kappaleessa listataan löydetyt ratkaisut ja kerrotaan niistä perustiedot, joista selviää lähde, tuetut alustat, lisensointimalli ja tuetut palvelut. Jokaisesta on myös lyhyt kuvaus, jonka perusteella voi saada nopeasti kuvan, minkälaisesta palvelusta on kyse.

Turvaominaisuuksia arvioitiin toimittajien itsensä antamien tietojen perusteella, sekä etsimällä tietoa internetistä. Electronic Frontier Foundation (EFF) on tehnyt myös taulukon, jossa on arvioitu palveluiden pikaviestinnän turvallisuutta seitsemän kriteerin perusteella (Electronic Frontier Foundation, 2015a). Tästä kerätyt arviot on esitelty tuotteen yhteydessä, ja näitä tietoja käytettiin etenkin palvelun kokonaisturvallisuuden arvioinnissa luvun 7. valintamatriisissa.

6.1 Ostel

Ostel on avoimeen lähdekoodiin perustuva palvelu päästä-päähän salattujen puhelujen mahdollistamiseen. Ostel on testiympäristö The Guardian Project -nimiselle avoimen lähdekoodin projektille, jonka tavoitteena on käyttää ilmaisia avoimia protokollia, standardeja ja ohjelmistoja mahdollistamaan turvallisen puheviestinnän mobiililaitteissa. Ostel asiakassovelluksia on lähes kaikille alustoille ja myös työpöytäympäristöön, ja useimmat sovellukset ovat ilmaisia ja avoimeen lähdekoodiin perustuvia. Ostel projekti ylläpitää myös omaa ilmaista palvelinta, jonka kautta puheluja voidaan muodostaa. (Ostel, 2015).

Yritys: The Guardian Project
Ominaisuudet: puhelut, pikaviestit, videopuhelut tulossa
Tuetut alustat: Android, iOS, Blackberry, Linux, OSX, Windows
Turvaominaisuudet: päästä-päähän salaus, useita servereitä, avoimen lähdekoodin asiakas ja palvelin
Turvallisuusarvio: teknisesti turvallinen: kyllä, kokonaisturvallinen: kyllä, valtiollinen salakuuntelu aktiivista: epätodennäköistä
Lisenssi ja standardit: käyttää avoimen lähdekoodin standardeja, ei kaupallista tai suljettua koodia
Liitettävyys: API, avoin lähdekoodi
Käytettävyys: kohtalaisen helppo
Hinta: ilmainen, iOS versio maksaa 6.99 USD
Kotimaa: Yhdysvallat
Web sivut: https://guardianproject.info/ ja https://ostel.co/

6.2 Linphone

Linphone on avoimeen lähdekoodiin perustuva VoIP-puhelinsovellus, joka mahdollistaa ilmaisen kommunikaation internetissä ääni- ja videopuheluilla sekä pikaviesteillä. Linphone käyttää standardia SIP-protokollaa, ja sitä voi käyttää periaatteessa minkä

tahansa VoIP-operaattorin palvelinten kanssa. Linphone ylläpitää myös itse omaa palvelintaan. Linphone on suhteellisen vanha ja monia kehitysvaiheita nähnyt projekti, sillä sitä on kehitetty jo vuodesta 2001. (Linphone, 2015).

Yritys: Linphone Open Source project, Belledonne Communications
Ominaisuudet: puhelut, videopuhelut, pikaviestit
Tuetut alustat: Android, iOS, Windows Phone, Blackberry, OSX, Windows, selain
Turvaominaisuudet: päästä-päähän salaus, vapaasti valittava serveri, avoimen lähdekoodin asiakas ja palvelin
Turvallisuusarvio: teknisesti turvallinen: kyllä, kokonaisturvallinen: kyllä, valtiollinen salakuuntelu aktiivista: epätodennäköistä
Lisenssi ja standardit: käyttää avoimen lähdekoodin standardeja, ei kaupallista tai suljettua koodia
Liitettävyys: API, avoin lähdekoodi
Käytettävyys: kohtalaisen helppo
Hinta: ilmainen
Kotimaa: Yhdysvallat
Web sivut: https://www.linphone.org

6.3 Redphone

Whisper Systemsin tavoitteena on tehdä salatusta viestinnästä mahdollisimman helppoa. Palvelu on rakennettu avoimen lähdekoodin päälle, jota tukee suuri joukko avoimen lähdekoodin kehittäjiä. Whisper Systemsillä on myös tiimi, joka on erikoistunut Redphone tuotteen tekemiseen. Applen mobiililaitteisiin tuotteen nimi on Signal. (Open Whisper Systems, 2015).

Yritys: Whisper Systems
Ominaisuudet: puhelut, pikaviestit
Tuetut alustat: Android, iOS
Turvaominaisuudet päästä-päähän salaus, avoimen lähdekoodin asiakas
Turvallisuusarvio: teknisesti turvallinen: kyllä, kokonaisturvallinen: kyllä, valtiollinen salakuuntelu aktiivista: epätodennäköistä
Lisenssi ja standardit: käyttää avoimen lähdekoodin standardeja, ei kaupallista tai suljettua koodia
Liitettävyys: lähdekoodin kautta, ei dokumentoitu
Käytettävyys: helppo
Hinta: ilmainen
Kotimaa: Yhdysvallat
Web sivut: https://whispersystems.org/

6.4 Silent Circle

Silent Circle on palvelu joka mahdollistaa salatun viestinnän internetissä. Palvelu on kaupallinen ja maksullinen, eikä sisällä avointa lähdekoodia. Yritys väittää, että se ei anna suoraan tietoja Yhdysvaltain hallitukselle, mutta pyynnöstä luovuttaa tietoja, jos pyynnöt ovat kohtuullisia. Tutkimuksen kirjoittamisen aikana palvelu on laajentunut ja sisältää nykyään myös kokonaisturvallisen Android puhelimen. (Silent Circle, 2015).

Yritys: Silent Circle
Ominaisuudet: puhelut, videopuhelut, pikaviestit
Tuetut alustat: Android, iOS, Windows
Turvaominaisuudet:

Turvallisuusarvio: teknisesti turvallinen: kyllä, kokonaisturvallinen: kyllä, valtiollinen salakuuntelu aktiivista: epätodennäköistä
Lisenssi ja standardit: käyttää avoimen lähdekoodin standardeja, ei kaupallista tai suljettua koodia
Liitettävyys: ei
Käytettävyys: helppo
Hinta: maksullinen, 120 USD / vuosi
Kotimaa: Sveitsi
Web sivut: https://www.silentcircle.com/

6.5 Skype

Skype on ilmainen palvelu, joka tarjoaa todella helpot puhelut, videopuhelut ja viestinnän, ja lisäksi maksulliset puhelut normaaleihin (ei VoIP) puhelimiin. Skype ei perustu avoimeen lähdekoodin eikä avoimiin protokolliin, eikä se ole yhteensopiva muiden VoIP-palveluiden kanssa. (Skype, 2015). Toisin kuin useimmat muut VoIP-sovellukset, Skype on teknisesti vertaisverkko-ohjelma. Skypen liikenne on sinänsä osoitettu salatuksi ja turvalliseksi, mutta Skype on nykyään Microsoftin omistuksessa, ja on Yhdysvaltain hallituksen tiedustelun kohteena.

Yritys: Microsoft
Ominaisuudet: puhelut, videopuhelut, pikaviestit, läsnäolo, ruudunjakaminen, soitto oikeisiin puhelimiin, tekstiviestit
Tuetut alustat: Android, iOS, Windows Phone, Linux, OSX, Windows
Turvaominaisuudet: salattu liikenne, ei päästä-päähän salausta
Turvallisuusarvio: teknisesti turvallinen: kyllä, kokonaisturvallinen: kyllä, valtiollinen salakuuntelu aktiivista: todennäköistä
Lisenssi ja standardit: suljettu järjestelmä, jonka turvaominaisuuksista ei ole tarkkaa tietoa. NSA:lla pääsy järjestelmään PRISM:n kautta.
Liitettävyys: API, puutteellinen
Käytettävyys: helppo
Hinta: ilmainen, puhelut oikeisiin puhelimiin ja tekstiviestit maksullisia
Kotimaa: Yhdysvallat
Web sivut: https://www.skype.com/

6.6 Google Hangouts

Google Hangouts on Googlen kehittämä viestintäpalvelu, jolla voi tehdä puheluita ja videopuheluita sekä lähettää pikaviestejä. Se on yhtiön aikaisempien palveluiden Google+ Messengerin ja Talkin seuraaja. Palvelu on käytettävissä netin kautta selaimella ja Google Chrome selainlaajennoksena sekä Android ja iOS sovelluksina. (Google+ Features, 2015.)

Yritys: Google
Ominaisuudet: puhelut, videopuhelut, pikaviestit, läsnäolo, tiedostonlähetys
Tuetut alustat: Android, iOS, Chrome OS, selain
Turvaominaisuudet: salattu liikenne, ei päästä-päähän salausta
Turvallisuusarvio: teknisesti turvallinen: kyllä, kokonaisturvallinen: ei, valtiollinen salakuuntelu aktiivista: todennäköistä
Lisenssi ja standardit: suljettu järjestelmä, jonka turvaominaisuuksista ei ole tarkkaa tietoa. NSA:lla pääsy järjestelmään PRISM:n kautta.
Liitettävyys: API
Käytettävyys: helppo

Hinta: ilmainen, puhelut oikeisiin puhelimiin ja tekstiviestit maksullisia
Kotimaa: Yhdysvallat
Web sivut: http://www.google.com/+/learnmore/hangouts/

7. Ratkaisujen vertailu, arviointi ja johtopäätökset

Vertailua varten luotiin kuvan 6 valintamatriisi käyttäen luvussa viisi esiteltyä Pugh Concept Selection Process -menetelmää. Matriisissa ovat sarakkeina haetut tuotekandidaatit ja riveinä aikaisemmin käsittelyt vaatimukset. Vaatimuksille on annettu myös painotukset, joiden perusteella niiden paremmuutta tai huonommuutta perustasoon verrattuna arvostetaan. Vasemmanpuoleisena ratkaisuvaihtoehdoista on Skype, joka on valittu vertailun referenssituotteeksi ja perustasoksi, joihin muita verrataan. Se saa siis kaikista vaatimuksista merkinnän (s), ja tämän tasoin ylity tai alitus merkitään symboleilla (+/-). Skype valittiin perustasoksi, koska sen käyttöä oli tutkittu tutkimusryhmässä aikaisemmin, ja siitä oli muutenkin parhaat tiedot ennestään.

Pugh valintamatriisi VoIP-sovelluksille

		Ratkaisuvaihtoehdot					
Vaatimukset	**Painotus**	**Skype**	**ostel.co**	**Linphone**	**Redphone**	**Cilent Circle**	**Google**
Kokonaisturvallinen	**7**	s	+	+	+	s	s
Sessionhallinta suojattu	**10**	s	s	s	s	s	s
Äänensiirto salattu	**10**	s	s	s	s	s	s
Äänensiirto päästä-päähän salattu	**5**	s	+	+	+	+	s
Äänipuhelut	**10**	s	s	s	s	s	s
Videopuhelut	**10**	s	-	s	-	-	s
Pikaviestit	**5**	s	s	s	s	s	s
Läsnäolo	**1**	s	-	-	s	-	s
Avoin lähdekoodi	**10**	s	+	+	s	s	s
Liitettävyys sovelluksiin	**8**	s	+	+	s	s	+
Käytettävyys	**3**	s	-	-	-	-	s
Android tuki	**5**	s	s	s	s	s	s
iOS tuki	**5**	s	s	s	s	s	s
Windows Phone tuki	**5**	s	-	s	-	-	s
Linux tuki	**5**	s	s	s	-	-	s
OSX tuki	**5**	s	s	s	-	-	s
Windows tuki	**5**	s	s	s	-	s	s
Hinta	**3**	s	s	s	s	-	s
∑+		**0**	**4**	**4**	**2**	**1**	**1**
∑-		**0**	**4**	**2**	**6**	**7**	**0**
∑s		**18**	**10**	**12**	**10**	**10**	**17**
Painotettu ∑+		**0**	**30**	**30**	**12**	**5**	**8**
Painotettu ∑-		**0**	**19**	**4**	**33**	**32**	**0**
Summa yhteensä		**18**	**21**	**38**	**-11**	**-17**	**25**
Sijoitus		**4.**	**3.**	**1.**	**5.**	**6.**	**2.**

Kuva 6. Pugh valintamatriisi valituille tuotekandidaateille.

Valintamatriisin perusteella paras ratkaisuvaihtoehto on Linphone. Se sai miinuspisteitä ainoastaan läsnäolo-ominaisuuden puutteesta ja vertailutuotetta huonommasta käytettävyydestä. Sen alustatuki ja liitettävyys omiin sovelluksiin ovat erinomaisia, ja avoimen lähdekoodin ansiosta sitä voi tarpeen mukaan myös muokata omiin tarpeisiin sopivaksi. Tietoturvaratkaisut ovat myös tarkastettavissa lähdekoodista, jos halutaan olla varmoja, että toteutukset ovat varmasti asiallisia. Lisäksi Linphonen tietoturvaominaisuudet ovat vertailutuotetta paremmat. Se sisältää äänen päästä-päähän salauksen, ja ansaitsee myös kokonaisturvallisuudesta pisteitä. Linphone ei palveluna ainakaan suoraan luovuta tietoa viranomaisille, eikä sitä velvoita CALEA-laki niin kuin suurtyrityksiä ja teleoperaattoreita.

Vertailussa toiseksi tuli Google Hangouts. Siitä ei puuttunut oikeastaan mitään ominaisuuksia, ja sen vahvuus vertailutuotteeseen verrattuna oli liitettävyys omiin sovelluksiin, sillä Google Hangouts tarjoaa API:n, jonka avulla sen toiminallisuus voidaan liittää omiin sovelluksiin. Tietoturvan taso ei ole korkein mahdollinen, ja Google on Yhdysvaltalaisena suuryrityksenä sitoutunut myös CALEA-ohjelmaan. Hangouts ei myöskään käytä mitään avoimia standardeja, eivätkä toteutukset ole suljetun lähdekoodin vuoksi puolueettomasti tarkastettavissa.

Kolmanneksi tuli avoimeen lähdekoodin perustuva Ostel. Se sai miinuspisteitä laitetuesta ja ominaisuuksista, vaikka turvallisuuspuoli on erittäin hyvin kunnossa. Avoimen lähdekoodin tuotteiden käytettävyys ei ole myöskään suuryritysten tekemien tuotteiden tasolla, ja Ostelin käytettävyys ja helppous ovat vielä aika kaukana Skypen ja Google Hangoutsin loppuun asti hiotusta helppoudesta.

Tämän vertailun perusteella yksityishenkilölle ja pienyrittäjälle voisi suosittaa Linphone tuotetta. Etenkin jos on tarkoitus integroida palvelu omiin sovelluksiin, on Linphone erittäin hyvä vaihtoehto. Tiukasti yksityisyydestään kiinnipitävälle se on myös hyvä ratkaisu, sillä kaikki tietoturvaominaisuudet perustuvat avoimiin hyvin tunnettuihin standardeihin, ja koodi on tarvittaessa helposti auditoitavissa. Satunnaiselle käyttäjälle, joka arvostaa helppoutta, ovat suuryritysten tuotteet Skype ja Google Hangouts hyviä valintoja. Niiden kanssa yksityisyyden suoja ei yllä samalle tasolle kuin Linphonella ja Ostelilla, mutta arvostuksista riippuen voi olla silti monelle riittävä. Vertailun kaksi muuta tuotetta RedPhone ja Silent Circle eivät ole aivan yhtä suositeltavia. RedPhonea vaivaa huono alustatuki, eikä liitettävyys omiin sovelluksiinkaan ole kovin helppoa. Silent Circle taas maksullisena ja kuitenkin varsin suppeasti eri alustoilla tuettuna järjestelmänä jää vertailun hännille.

8. Yhteenveto

Tässä tutkimuksessa tarkasteltiin internetin välityksellä toimivien puheluiden ja viestinnän yksityisyyttä sekä tietoturvaa. Turvallisuusongelmiin liittyvien asioiden ymmärtäminen vaati VoIP-protokollien perusteiden ja toiminnan selvittämistä. VoIP-liikenteeseen liittyviä tietoturvaongelmia tunnistetiin useita, ja osoittautui, että niiden torjuminen ei ole välttämättä helppoa mutta erittäin tärkeää. Avoimien standardien kuten TLS, SIPS, SRTP ja ZRTP hyödyntäminen voi kuitenkin merkittävästi vähentää tietoturvariskejä sekä parantaa yksityisyydensuojaa, ja auttaa tarjoamaan jopa erittäin hyvän turvallisuuden ja yksityisyyden tason.

Valmiista ratkaisuista tehty selvitys ja vertailu antoivat positiivisen kuvan VoIP-palveluiden tietoturvan tasosta tänä päivänä. Kaikki vertailun kandidaatit sisälsivät liikenteen salauksen ja muita turvaominaisuuksia. Positiivista oli löytää myös kaksi täysin avoimeen lähdekoodiin perustuvaa tuotetta, jotka olivat myös erittäin hyviä ja toimivia. Tutkimuksen perusteella suurten yritysten isolla rahalla tehdyille huipputuotteille on myös vaihtoehtoja. Tietoturvan näkökulmasta avoin lähdekoodi on kuitenkin valtava etu, sillä se mahdollistaa tietoturvan puolueettoman, avoimen ja jatkuvan arvioinnin.

Tutkimuskysymykseen palattaessa voidaan siis todeta, että tämän tutkimuksen perusteella näyttäisi, että yksityishenkilön tai pienyrityksen on mahdollista suojata viestintänsä tehokkaasti ja edullisesti. Yksityisyyttä ja tietoturvaa parantavia tuotteita on hyvin tarjolla, ja ne ovat varsin valmiita kokonaisuuksia. Viimeaikojen paljastukset salakuuntelusta, vakoilusta ja tietoturvan puutteessa varmasti lisäävät kiinnostus tämän kaltaisiin tuotteisiin, joten varmasti tulemme näkemään uusia tuotteita ja palveluita yksityisyyttämme parantamaan.

Aiheesta voisi tehdä myös jatkotutkimusta, jossa voisi esimerkiksi selvittää tuotteiden todellista tietoturvaa altistamalla niitä erilaisille hyökkäyksille, tai tutkia miten hyvin vertailussa valitut tuotteet todella onnistuvat liikenteen salaamisessa. Myös näiden palvelujen tarjoama palvelunlaatu (QoS) oikeassa käytössä herättää kysymyksiä. Jatkotutkimuksessa voisi selvittää miten ne toimivat todellisessa käytössä mobiililaitteissa ja vaihtelevan laatuisissa verkoissa.

Lähteet

Arkko, J., Torvinen, V., Camarillo, G., Niemi A., & Haukka T. (2003). *Security Mechanism Agreement for the Session Initiation Protocol RFC 3329.* IETF

Azfar, A., Choo, K., & Liu, L. (2014). *A study of ten popular android mobile VoIP applications: Are the communications encrypted?* 4858-4867.

Burge, S. (2009), *The System Engineering Tool Box – Pugh Matrix.* Lainattu 3.2.2015, saatavilla: http://www.burgehugheswalsh.co.uk/uploaded/documents/Pugh-Matrix-v1.1.pdf

Camarillo, G. (2001). *SIP demystified.* McGraw-Hill Education.

Cohen, L. (1997). *Quality Function Deployment, How to make QFD work for you*. Addison-Wesley.

DigitalStrategyConsulting (2014). *Voice calls to be replaced by instant messaging?* Lainattu: 2.1.2015, saatavilla: http://www.digitalstrategyconsulting.com/intelligence/2014/08/voice_calls_to_be_replaceced_by_instant_messaging.php

Dwivedi, H. (2009). *Hacking VoIP: Protocols, attacks, and countermeasures.* No Starch Press.

Electronic Frontier Foundation (2015a). *Secure Messaging Scorecard*. Lainattu 14.2.2015, saatavilla: https://www.eff.org/secure-messaging-scorecard

Electronic Frontier Foundation (2015b). *The Communications Assistance for Law Enforcement Act (CALEA) of 1994*. Lainattu 3.2.2015, saatavilla: https://www.eff.org/issues/calea

Geneiatakis, D., Kambourakis, G., Dagiuklas, T., Lambrinoudakis, C. & Gritzalis, S. (2005). SIP security mechanisms: A state-of-the-art review. *Proceedings of the 5th International Network Conference, INC 2005,* 147-155.

Google+ Features (2015). *Hangouts - Bring your conversations to life with photos, emoji, and even group video calls for free.* Lainattu 14.2.2015, saatavilla: http://www.google.com/+/learnmore/hangouts/

The Guardian, 2013. *Microsoft handed the NSA access to encrypted messages*. Lainattu 12.12.2015, saatavilla: http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Gupta, P. & Shmatikov, V. (2007). *Security analysis of voice-over-IP protocols*. Proceedings of the 20th IEEE Computer Security Foundations Symposium. 2007, IEEE Computer Society, 49-63.

Johnston, A. B. (2009). *SIP: Understanding the session initiation protocol.* Artech House, Incorporated.

Katz, D., Lukasiak, T., Gentie, R. & Meyer, W. (2006). *Design Your own VoIP Solution with a Blackfin Processor – Add Enhancements Lates.* Analog Devices Dialogue, Volume 40 – 2006. Lainattu 8.2.2015, saatavilla: http://www.analog.com/library/analogDialogue/archives/40-04/blackfin_voip.html

Kurose, J., Ross, K. (2013). *Computer Networking – A Top-Down Approach.* Pearson.

Linphone – Open source VoIP Project (2015). *About Linphone.* Lainattu 14.2.1015, saatavilla: http://www.linphone.org/about.html

Open Whispersystem (2015). *About us.* Lainattu 14.2.2015, saatavilla: https://whispersystems.org/about/

Ostel (2015). *About Ostel.* Lainattu 14.2.2015, saatavilla: https://ostel.co/about

Porter, T. (2006). *Practical VoIP security*. Rockland, Mass: Syngress

Pugh, S. (1981). *Concept selection: a method that works*. Hubka, V. (ed.), Review of design methodology. Proceedings international conference on engineering design, March 1981, Rome. Zürich: Heurista, 1981, 497 – 506

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Spark, R., Handley, M. & Schooler, E. (2002), *Session Initiation Protocol, RFC 3261,* IETF

Silent Circle (2015). *Mobile Privacy Solutions.* Lainattu 14.2.2015, saatavilla: https://silentcircle.com/services

Schulzrinne, H. (2004). *Internet Telephony.* Columbia University.

Sinnreich, H. & Johnston, A. B. (2012). *Internet communications using SIP: Delivering VoIP and multimedia services with session initiation protocol*. Wiley.

Skype (2015). *About Skype.* Lainattu 14.2.2015, saatavilla: http://www.skype.com/en/about/

Wikipedia (2015). *Communications Assistance for Law Enforcement Act.* Lainattu 1.2.2015, saatavilla: http://en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act

Yksityisyydensuoja (2015). *Tietojen salaaminen.* Lainattu 15.2.2015, saatavilla: https://www.yksityisyydensuoja.fi/tietojen-salaaminen

Zimmerman, P., Johnston, A. & Callas, J. *ZRTP: Media Path Key Agreement for Unicast Secure RTP RFC 6189.* IEFT.