TEKNILLINEN KORKEAKOULU
Informaatio- ja luonnontieteiden tiedekunta
Tietotekniikan tutkinto-ohjelma

Pikaviestinnän tietoturva

Ongelmat, vaihtoehdot ja ratkaisut

Kandidaatintyö

Olli Jarva

Tietotekniikan laitos
Espoo 2009

TEKNILLINEN KORKEAKOULU
Informaatio- ja luonnontieteiden tiedekunta
Tietotekniikan tutkinto-ohjelma

KANDIDAATINTYÖN
TIIVISTELMÄ

Tekijä:	Olli Jarva	
Työn nimi:	Pikaviestinnän tietoturva – Ongelmat, vaihtoehdot ja ratkaisut	
Päiväys:	1. toukokuuta 2009	**Sivumäärä:** 6 + 36
Pääaine:	Tietoliikenneohjelmistot	**Koodi:**
Vastuuopettaja:	prof. Lauri Savioja	
Työn ohjaaja:	TkL Sanna Suoranta	

Työssä tarkastellaan pikaviestintäjärjestelmän tietoturvassa huomioon otettavia asioita teoriatasolla, luodaan lyhyt katsaus tärkeimpiin nykyisiin pikaviestintäjärjestelmiin ja tarkastellaan joitain turvallisempia järjestelmiä.

Työ on toteutettu kirjallisuustutkimuksena. Joidenkin pikaviestintäverkkojen toimintaa on seurattu kuuntelemalla ohjelman verkkoliikennettä.

Lähes kaikki yleisesti käytetyt pikaviestintäjärjestelmät kärsivät keskitettyjen palvelimien muodostamasta ongelmasta. Suurimmat järjestelmät eivät salaa tai muuten suojaa viestiliikennettä. Viestinnän luottamuksellisuuden säilymisen kannalta turvallisia pikaviestintäjärjestelmiä on olemassa, mutta kynnys käyttöönottoon voi olla melko suuri. Totutuista järjestelmistä ei haluta siirtyä pois. OTR mahdollistaa luottamuksellisen viestinnän, mutta ei esimerkiksi ryhmäkeskusteluita. SILC toteuttaa normaalikäytön ominaisuus- ja tietoturvavaatimukset.

Avainsanat:	pikaviestintä, pikaviestintäjärjestelmä, tietoturva, cia
Kieli:	Suomi

Alkulause

Kiitos työn ohjaajalle ja lukuisille oikolukijoille. Ilman kommentteja ja parannusehdotuksia työ olisi huomattavasti huonompi.

Työn uusin versio löytyy osoitteesta `http://olli.jarva.fi/kandi.pdf`.

Espoossa 26. huhtikuuta 2009

Olli Jarva

Käytetyt lyhenteet

AES	Advanced Encryption Standard; symmetrinen salausalgoritmi
AIM	AOL Instant Messenger; AOL:n pikaviestintäpalvelu
AOL	American Online; Yhdysvaltojen suurin internetyhteyksien tarjoaja
CIA	Confidentiality, Integrity, Availability; luottamuksellisuus, eheys, saatavuus
DCC	Direct Client-to-Client; suora asiakkaidenvälinen viestinvälitys, IRC:n laajennus
DoS	Denial of Service; palvelunestohyökkäys
GSM	Global System for Mobile Communications; matkapuhelinverkkotekniikka
HMAC	keyed-Hash Message Authentication Code; avaimellinen tarkistussumma
HTTP	Hypertext Transfer Protocol; hypertekstin siirtoprotokolla
HTTPS	Hypertext Transfer Protocol Secure; salattu hypertekstin siirtoprotokolla
IM	Instant Messaging; pikaviestintä
IRC	Internet Relay Chat; tosiaikainen keskustelusovellus
ISO	International Organization for Standardization; kansainvälinen standardoimisorganisaatio
MD5	Message Digest algorithm; tiivistealgoritmi
MSN	The Microsoft Network; Microsoftin verkkopalveluita tarjoava portaali

NIST	National Institution of Standards and Technology; Yhdysvaltojen kansallinen standardoimisorganisaatio
OTR	Off-the-Record Messaging; pikaviestintäverkoissa toimiva tiedon salausjärjestelmä
OSCAR	Open System for Communication in Realtime; AIM:n pikaviestintäprotokolla
PGP	Pretty Good Privacy; julkisten avainten salausjärjestelmä, pääasiassa sähköpostikäytössä.
RSA	Rivest-Shamir-Adleman; epäsymmetrinen salausalgoritmi.
SHA	Secure Hash Algorithm; tiivistealgoritmi.
SILC	Secure Internet Live Conferencing; turvallinen tekstipohjainen konferenssijärjestelmä
SIM	Subscriber Identity Module; matkapuhelinverkon käyttäjän tunnistusmoduuli
SIMPLE	Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions; SIP-protokollan pikaviestintälaajennus
SIP	Session Initiation Protocol; istunnon luontiprotokolla
SMS	Short message service; tekstiviestipalvelu
TLS	Transport Layer Security; yleinen tiedon salausjärjestelmä
UMAC	Message Authentication Code using Universal Hashing; avaimellinen tiedon tarkistussumma
UMTS	Universal Mobile Telecommunications System; kolmannen sukupolven matkapuhelinverkkotekniikka
XML	Extensible Markup Language; laajennettava merkintäkieli
XMPP	Extensible Messaging and Presence Protocol; yleinen vapaa XML-pohjainen pikaviestintäprotokolla

Sisältö

Luku 1

Johdanto

Sähköisellä pikaviestinnällä tarkoitetaan sähköisten viestien välittämistä kahden tai useamman ihmisen ryhmässä. Pikaviestinnän luonteeseen kuuluu viestien välitön siirto vastaanottajalle; esimerkiksi sähköpostia ei tästä syystä katsota pikaviestinnäksi. Useimmat pikaviestintäjärjestelmät välittävät myös toisen tai toisten osapuolten läsnäolotietoja. Pikaviestintä on vähemmän interaktiivista kuin esimerkiksi puhuminen, joten viestintä vaatii vähemmän huomiota.

Pikaviestintäjärjestelmät ovat saaneet alkunsa lähinnä vapaa-ajan toiminnan tarpeista, mutta käyttö yritysmaailmassa on lisääntynyt voimakkaasti. Yrityskäytön turvallisuus- ja toimivuusvaatimukset ovat lähes poikkeuksetta korkeampia kuin vapaa-ajan käytössä. Arkaluontoisten tietojen ja yrityssalaisuuksien siirtäminen turvattomasti voi tuoda huomattavia taloudellisia ja oikeudellisia vastuita ja seuraamuksia.

Tämä työ keskittyy suosituimpien järjestelmien tietoturvaongelmiin ja olemassa oleviin turvallisiin vaihtoehtoihin. Käyttöliittymien ja protokollien yksityiskohdat sekä salaus- ja suojausmenetelmien syvällinen analyysi on rajattu työn ulkopuolelle. Lisäksi huomioon on otettu ainoastaan tekstipohjainen viestintä. Äänen ja kuvan turvallisessa siirrossa on erilaisia teknisiä haasteita, muun muassa vaatimus erittäin pieniin viiveisiin ja siirrettävän tiedon sopivaan pakkaamiseen[1].

Järjestelmäkatsaukseen valitut pikaviestintäjärjestelmät on valittu suuntaa antavilla tiedoilla markkinaosuuksista ja markkinoiden kasvuarvioista. Lisäksi osa järjestelmistä - SILC, OTR, tekstiviestit ja IRC - on valittu teknologiakatsauksen laajentamiseksi. SILC, OTR ja IRC ovat käyttäjämääriltään marginaalisia verrattuna suuriin pikaviestintäjärjestelmiin.

[1]Esimerkiksi Wright et al. (2007) kertovat äänen siirron salauksen ongelmista.

Luku 2

Tietoverkkojen tietoturva

2.1 Toimintaympäristö ja -oletukset

Tietoverkoissa - erityisesti langattomissa verkoissa - hyvä perusoletus on liikenteen julkisuus: ei voida sulkea pois mahdollisuutta, että joku salakuuntelee ja tallentaa verkkoliikenteen analysoitavaksi[1]. Suurten tietomäärien automaattinen analysointi tietokoneilla on lähes ilmaista. Tietoverkoissa ei päde esimerkiksi perinteisellä postilla välitettyjä tietoja koskeva yleinen oletus siitä, että kenelläkään ei ole motivaatiota eikä resursseja viestien keräämiseen ja käsittelyyn. Tekstimuotoisesta tiedosta voidaan nykytekniikalla helposti tunnistaa automaattisesti henkilökohtaisia tietoja - osoitteita, luottokorttinumeroita, tuttavia jne. - esimerkiksi identiteettivarkauksien toteuttamiseen.

Tietojärjestelmien heikoin lenkki on usein järjestelmää käyttävä ihminen tai ihmiset. Ihmiset vastustavat muutosta, ja pyrkivät tekemään asioita vanhojen tapojen mukaisesti (Trader-Leigh, 2002). Muutosten vastustaminen hankaloittaa toiminnan kehittämistä. Ihmisillä on vahva luontainen halu auttaa toisia ihmisiä, vaikka auttaminen edellyttäisi sääntöjen rikkomista. Järjestelmän käyttäjiä vastaan hyökkäämisestä käytetään termiä *social engineering*. Esimerkkejä ihmisten luontaisen auttamisen halun hyväksikäytöstä on runsaasti: huolellisesti suunniteltuja ja toteutettuja teknisiä suojauksia on kierretty saamalla ihmiset auttamaan hyökkääjää normaalilta kuulostavissa tehtävissä. (Mitnick ja Simon, 2003)

Henkilökohtainen internetin käyttö yleistyy koskemaan tärkeämpiä ja henkilökohtaisempia asioita. Esimerkiksi Suomessa kehitetään aktiivisesti sähköistä asiointia. Samalla internetin kautta välitettäväksi siirtyy yhä tärkeämpää tietoa. Yrityk-

[1] Tietokoneelle saapuvan tietoliikenteen salakuuntelu on erittäin helppoa. Ks. esim. `http://www.wireshark.org/` , verkkoliikenneanalysaattorin verkkosivu, viitattu 15.3.2009.

sissä tietoverkkojen käyttö kasvaa mm. alhaisten kustannusten vuoksi kattamaan yhä enemmän myös liiketoiminnalle kriittisiin asioihin liittyvää kommunikointia. Valtaosa yrityksien sisäisistä pikaviestintäkeskusteluista käsittelee monimutkaisia työhön liittyviä asioita (Isaacs et al. 2002 ja Handel ja Herbsleb 2002). Samaan aikaan tietokoneiden suorituskyky kasvaa, ja tekoäly sekä erilaiset automaattiset analysointityökalut kehittyvät (Cassimatis et al., 2006). Ihmisten ymmärrys tietoverkoissa tapahtuvan tiedon analysoinnin erilaisesta luonteesta esimerkiksi fakseihin tai puhelimiin verrattuna ei välttämättä kehity vastaavasti.

Järjestelmiä suunniteltaessa ja käyttöön otettavia järjestelmiä valittaessa tulisi olettaa, että järjestelmää vastaan tullaan hyökkäämään. Usein ihmiset vastustavat muutosta, joten jo käyttöön otetun järjestelmän vaihtaminen uuteen voi olla vaikeaa. Hyökkääjät voivat olla järjestelmän käyttäjiä, kolmansia osapuolia tai jopa järjestelmän toimittajia. Esimerkiksi järjestelmän toimittajan työntekijöitä on voitu lahjoa salakuuntelemaan ja välittämään eteenpäin kilpailevan yrityksen viestintää.

2.2 Tietoturvan osa-alueita

Tietoturvan systemaattinen analysointi on vaikeaa ja hyvin monitahoista. Tietokonejärjestelmissä ja -verkoissa hyökkääjien riskit ovat perinteisiin rikollisuuteen verrattuna minimaalisia. Hyökkääjä voi sijaita maantieteellisesti missä tahansa. Hyökkäyksiä voidaan helposti automatisoida, eikä suurten tietomäärien kerääminen ja käsitteleminen ole vaikeaa tai kallista. Tietoturvan analysointimalleista CIA on yksinkertaisin ja yleisimmin käytetty. CIA on lyhenne termeistä confidentiality (luottamuksellisuus), integrity (eheys) ja availability (saatavuus). Tietoturva on kokonaisuus, joka muodostuu kompromissista eri kriteerien välillä. Täydellistä luotettavuutta ei voida saavuttaa, jos tieto on saatavilla. Toisaalta täydellinen saatavuus tekee tiedon luottamuksellisuuden varmistamisesta vaikeaa tai jopa mahdotonta.

ISO-standardi 27002 (ISO/IEC, 2005) määrittelee johdannossa tiedon varsin laajasti:

> "Tieto voi olla tulostettuna tai kirjoitettuna paperille, tallennettuna elektronisesti, siirretty postilla tai elektronisesti, näytetty filmillä tai puhuttu."

Tässä työssä keskitytään pääasiassa elektronisesti tallennettuun ja elektronisesti siirrettyyn tietoon.

Standardi määrittelee luottamuksellisuuden, eheyden ja saatavuuden seuraavasti:

> "Luottamuksellisuus on sen varmistamista, että tieto on vain niiden käsiteltävissä, joilla on oikeus tietoon."
>
> "Eheys on tiedon ja tiedon käsittelymenetelmien oikeellisuuden ja täydellisyyden varmistamista suojautumalla luvattomilta muokkauksilta."
>
> "Saatavuus tarkoittaa, että tieto ja tietoon liittyvät resurssit ovat auktorisoitujen käyttäjien käytettävissä tarvittaessa."

Calder ja Watkins (2005) kertovat kirjassaan ISO 27002:n käytöstä ja yritysten tietoturvan kehittämisestä yleisesti. Reid et al. (2005) kertovat pinnallisesti CIA-mallin käytöstä tietoturvan analysoinnissa.

Luottamuksellisuudella tarkoitetaan tiedon yksityisyyttä ja yksityisyyden säilymistä. Luottamuksellisuus on toteutunut, jos tieto on ja on ollut vain niiden henkilöiden saatavilla, joille se on tarkoitettu. Esimerkki luottamuksellisuusongelmasta on onnistunut tiedon salakuuntelu. Tiedonsiirron luottamuksellisuutta voidaan kehittää tiedon salauksella tai siirtotien muulla suojaamisella. Myös päätelaitteiden turvallisuudesta on huolehdittava. Siirron ajaksi täydellisesti salatun tiedon luottamuksellisuus ei toteudu, jos salakuuntelija voi tarkastella tietoa esimerkiksi käyttäjän näyttöä kuvaavan kameran välityksellä.

Tiedon eheys tarkoittaa osapuolten välillä välitetyn tiedon muuttumattomuutta. Tieto on siirretty riittävän samanlaisena lähettäjältä vastaanottajalle. Eheys ei välttämättä tarkoita tiedon siirtämistä täysin samanlaisena - esimerkiksi äänen pakkaus muuttaa ääntä - vaan sisällön muuttumattomuutta. Esimerkki eheyden ongelmista on tiedon muokkaus: tietoa voidaan muokata myös saamatta selville sisältöä. Myös väärällä identiteetillä esiintyminen on eheysongelma. Tärkein keino eheyden säilyttämiseen on siirtotien turvaaminen. Eheys voidaan todeta kryptografisilla tarkisteilla. Usein tehokkain keino identiteetin väärentämisen estämiseen on sisäänkirjautumisprosessin turvallinen ja toimiva toteuttaminen. Lisäksi sisäänkirjautuneen käyttäjän istunnon kaappaaminen tulee estää. Käyttäjien väliseen kommunikointiin tarvitaan autentikointi, joko järjestelmän tuottamana tai suoraan käyttäjien välisenä.

Saatavuus on tiedon saamista oikeaan aikaan luotettavasti. Vaikka tieto olisi luottamuksellista ja eheää, tiedon saaminen vastaanottajalle on kriittinen tekijä missä tahansa tiedonsiirtojärjestelmässä. Esimerkiksi onnistunut palvelunestohyökkäys (Denial of Service, DoS) on haitta saatavuudelle. Saatavuutta voidaan parantaa esimerkiksi palveluita tarjoavien järjestelmien hajauttamisella ja kahdentamisella.

2.3 Kryptografian perusteet

Anderson (2001, luvussa 5) antaa lyhyen katsauksen kryptografiaan. Kryptografiset algoritmit jaotellaan tiedon eheyden tarkistamiseen (tarkistussummat) ja luottamuksellisuuden toteuttamiseen (tiedon salaus). Tiedon salaus jaotellaan symmetrisiin ja epäsymmetrisiin algoritmeihin. Eräs merkittävä kryptografian sovellus on lähettäjän identiteetin varmentaminen. Reid et al. (2005) esittävät kattavan tiivistelmän salauksen käytöstä tietoturvan parantamiseen. Lähes kaikki salausalgoritmit ja -protokollat perustuvat algoritmin lisäksi algoritmiin syötettävään salaisuuteen. Kerckhoffsin aksiooman mukaan salausalgoritmin toimivuus tai luotettavuus ei kärsi, vaikka algoritmi julkaistaisiin, jos salausavain pysyy salaisena (Kerckhoffs, 1883).

2.3.1 Salausalgoritmit

Symmetrisessä salauksessa tarvitaan jaettu avain osapuolten välille. Lähettäjä salaa tiedon jaetulla avaimella. Vastaanottaja purkaa salauksen samalla algoritmilla ja samalla avaimella. Yhdysvaltojen liittovaltion standardoimisorganisaation (National Institute of Standards and Technology, NIST) kansalliseksi standardiksi hyväksymä Advanced Encryption Standard (AES) on mahdollisesti eniten käytetty symmetrinen salausalgoritmi (Barker, 2001).

Epäsymmetrinen eli julkisen avaimen salaus perustuu julkiseen ja yksityiseen avaimeen. Julkisella avaimella salatun tiedon salaus voidaan purkaa ainoastaan sitä vastaavalla yksityisellä avaimella. Esimerkiksi lähinnä sähköpostien salauksessa käytetyssä PGP:ssä (Pretty Good Privacy) lähettäjä salaa tiedon julkisella avaimella, ja vastaanottaja purkaa tiedon julkista avainta vastaavalla yksityisellä avaimellaan (Garfinkel, 1996). Vastaavasti PGP:ssä yksityisellä avaimella allekirjoitetun tiedon eheys (allekirjoittajan identiteetti) voidaan tarkistaa yksityistä avainta vastaavan julkisen avaimen avulla (Garfinkel, 1996). Julkisen avaimen järjestelmässä tiedon vastaanottaja voi levittää julkista avaintaan vapaasti, sillä julkisella avaimella ei voida purkaa salattua tietoa. RSA (Rivest et al., 1977) on mahdollisesti tunnetuin epäsymmetrinen salausalgoritmi.

Symmetrinen salaus on huomattavasti julkisen avaimen salausta nopeampaa (Menascé, 2003), esimerkiksi Reid et al. (2005) toteavat nopeuseron olevan noin tuhatkertainen. Suurten tietomäärien siirrossa ja korkeaa suorituskykyä vaativissa järjestelmissä voidaan vaihtaa jaettu salaisuus julkisen avaimen salausjärjestelmällä ja siirtyä käyttämään symmetristä salausta varsinaiseen tiedonsiirtoon.

2.3.2 Tiivistealgoritmit

Tiivistealgoritmit luovat tyypillisesti suhteellisen lyhyen tarkistussumman alkuperäisestä tiedosta, tiedon sormenjäljen. Tiivistealgoritmit ovat yksisuuntaisia, eli tarkistussumma sisältää huomattavasti vähemmän informaatiota kuin alkuperäinen tieto. Hyvästä tarkistussummasta voidaan palauttaa vain koko alkuperäinen tieto arvaamalla ja tarkistamalla, täsmääkö tarkistussumma. Tiivistealgoritmissa on puutteita, jos osittaisen arvauksen oikeellisuus voidaan tarkistaa. Yleisimmät algoritmit ovat SHA (Secure Hash Algorithm) ja MD5 (Message Digest). Esimerkiksi MD5 tuottaa 128-bittisen tiivisteen mistä tahansa syötteestä (Rivest, 1992). Stallings (2006, luku 11.4) esittelee tarkistussummien laskemista ja käyttöä laajemmin.

Hyvin yleinen käyttö tarkistussummille on salasanojen tallennus. Esimerkiksi palveluntarjoajalle riittää mahdollisuus tarkistaa annetun salasanan oikeellisuus, salasanan tietäminen ei yleensä ole tarpeellista. Tarkistussumman avulla voidaan todeta tiedon eheys laskemalla tarkistussumma uudelleen ja vertaamalla aikaisemmin laskettuun. Menetelmä on melko varma, mutta ei täydellinen. Stevens (2007) esittelee menetelmän halutun MD5-tarkistussumman tuottavan merkkijonon muodostamiseen. Vastaavilla hyökkäyksillä voi olla mahdollista muuttaa osia tiedoista ilman tarkistussumman muuttumista (Stevens et al., 2007). SHA-algoritmeista on useita versioita, joista SHA-0 on murrettu (Manuel ja Peyrin, 2008). SHA-1 on murrettu teoreettisella tasolla (Wang et al., 2005), mutta todellisuudessa toimivia hyökkäyksiä ei toistaiseksi ole. SHA-2:ta pidetään toistaiseksi turvallisena.

2.3.3 Osapuolen identiteetin varmentaminen

Pelkkä viestin sisällöstä otettu tarkistussumma suojaa viestiä ainoastaan tahattomilta muokkauksilta. Yleisesti käytetyt salaus- ja tarkistussummien laskentaalgoritmit ovat julkisia - Kerckhoffin aksiooman mukaisesti ei ole syytä yrittää pitää algoritmia salaisena - joten viestin muokkaaja voi laskea muokatulle viestille tarkistussumman uudelleen.

Tiedon eheyden ja lähettäjän identiteetin varmentaminen jaetulla salaisuudella on erittäin yksinkertaista. Lähettäjä luo viestin A, liittää viestiin jaetun salaisuuden B ja laskee A+B:stä tarkistussumman C. Vastaanottajalle lähetetään viesti A ja tarkistussumma C. Vastaanottaja liittää vastaanotettuun viestiin yhteisen salaisuuden B, laskee vastaavasti tarkistussumman ja vertaa saatua tulosta välitettyyn tarkistussummaan C. Salaisuuden lisäystä tarkistussummaan kutsutaan suolaukseksi (salting). Useissa sovelluksissa välitettävään pakettiin lisätään yksi-

löllinen numero U (tarkistussumma C lasketaan merkkijonosta A+B+U, vastaanottajalle välitetään A, U ja C) viestien uudelleenlähetysten tunnistamiseksi ja estämiseksi. Yksilöllisen numeron U valitseminen ja siirto on tehtävä huolellisesti. Jos hyökkääjä voi valita käytettävän numeron, uudelleenlähetysten estäminen ei ole mahdollista.

Kryptografialla toteutettua viestin aitouden ja osapuolen identiteetin varmistamista kutsutaan sähköiseksi allekirjoitukseksi. Viestin identiteetin ja eheyden varmentamiseen on valmiita menetelmiä, muun muassa HMAC (keyed-Hash Message Authentication Code, Krawczyk et al. 1997) ja UMAC (Message Authentication Code using Universal Hashing, Krovetz 2006). Stallings (2006, luku 11.3) antaa lisätietoa autentikointiviestien käytöstä.

Luku 3

Pikaviestinnän tietoturva

3.1 CIA-malli pikaviestinnässä

3.1.1 Salakuuntelu

Pikaviestinnän mahdollisesti tärkein ja yksikäsitteisin tietoturvaongelma on viestien luottamuksellisuuden puute: osapuolten välillä välitettyjen viestien salakuuntelu. Sekä yksityishenkilöt että yritykset siirtävät pikaviestintäverkoissa salaista tai yksityistä tietoa, joka väärinkäytettynä voi aiheuttaa henkisiä, taloudellisia tai oikeudellisia haittoja. Pikaviestintäverkossa välitettyjen keskusteluiden luottamuksellisuudesta huolehtiminen on helppoa oikein valitulla ja toteutetulla salausjärjestelmällä. Usein suurin ongelma on osapuolten välisen turvallisen avaintenvaihdon toteuttaminen.

Salakuuntelu voi olla mahdollista myös viestinvälityksen päätepisteissä. Salakuuntelun estämiseksi tulee suojata myös käyttäjien tietokoneet ja fyysinen ympäristö. Paraskin salaus on turhaa, jos hyökkääjä voi asentaa kameran kuvaamaan käyttäjän näyttöä. Vakavammissa järjestelmissä, esimerkiksi sotilaskäytössä, täytyy kiinnittää huomiota elektronisten laitteiden lähettämään säteilyyn (Kuhn ja Anderson, 1998).

3.1.2 Viestien muokkaaminen

Keskustelussa kaikkien viestien siirtyminen muuttumattomana perille on selvästi tärkeää. Lisäksi keskusteluun ei ole saanut ilmestyä ylimääräisiä viestejä. Viestinnän eheys ei ole toteutunut, jos viestejä on voitu muokata: viestien tulee siirtyä muuttumattomina lähettäjältä vastaanottajalle. Mikäli viesti muuttuu, muutos

täytyy olla mahdollista tunnistaa luotettavasti. Yksittäisen viestin puuttuminen tai keskusteluun lisätty viesti voi muuttaa koko keskustelun sisällön, vaikka kaikki muut viestit olisi välitetty perille täysin muuttumattomina. Viestin onnistunut muokkaaminen, lisääminen tai poistaminen ei välttämättä edellytä onnistunutta viestien sisällön selvittämistä. Muokkaaminen voidaan tunnistaa kryptografisilla tarkistussummilla. Samoilla menetelmillä voidaan tunnistaa lisätyt ja poistetut viestit. Yksinkertaisimmillaan lähettäjä lisää viestiin yksilöllisen numeron, tiedon edellisen lähetetyn viestin numerosta ja allekirjoittaa koko lähetettävän viestin. Vastaanottaja voi edellisen viestin numerosta tarkistaa, onko keskustelusta lisätty tai poistettu viestejä.

3.1.3 Toisena henkilönä esiintyminen

Toisena henkilönä esiintyminen on ongelma välitettävien viestien luottamuksellisuudelle ja järjestelmän eheydelle. Viestin lähettäjä voi kertoa toisena henkilönä esiintyvälle luottamuksellista tietoa, ja vastaavasti toisena henkilönä esiintyvä voi käyttää väärin vastaanottajan luottamusta. Pikaviestintäkeskustelut vastaavat mielikuvana usein esimerkiksi puhelimessa keskustelua, joten toisen osapuolen sanomiin asioihin luotetaan. Normaalissa pikaviestinnässä väärän henkilön voi tunnistaa vain kirjoitustyylistä. Esimerkiksi kirjoitusvirheiden matkiminen on helppoa. Puhelimessa tunnistamiseen on käytettävissä myös huomattavasti yksilöllisemmät äänensävyt ja yleinen keskustelutyyli (Doddington, 1985). Toisena henkilönä esiintymistä on vaikea estää luotettavasti ilman järjestelmän ulkopuolista luotettavaa kolmatta osapuolta tai erillistä kommunikointia. Luotettava kolmas osapuoli voi olla esimerkiksi valtio[1]. Erillinen kommunikointi voi olla esimerkiksi henkilökohtaisesti vastapuolen tapaaminen tai puhelimessa äänestä tunnistaminen. Joissain salaus- ja viestintäjärjestelmissä - esimerkiksi PGP (Pretty Good Privacy) ja OTR (Off-the-Record Messaging) - avaintenvaihtoon voidaan käyttää vastapuolen salausavaimen sormenjäljen[2] vaihtamista turvallisella välitystiellä tai etukäteen sovittua jaettua salaisuutta (Garfinkel 1996 ja Alexander ja Goldberg 2007, kts. 3.1).

[1] Esimerkiksi Suomessa on mahdollista hankkia sähköinen henkilökortti, jolla voi mm. allekirjoittaa tietoja. Katso esimerkiksi verkkosivu sähköisestä henkilökortista, www.fineid.fi (viitattu 29.3.2009).

[2] Esimerkki salausavaimen sormenjäljestä on 0A090D88 A83B1047 1C4E4783 C690CC76 089E4781. Sormenjälki yksilöi avaimen melko luotettavasti.

3.1.4 Palvelun estyminen

Asiakas-palvelin-arkkitehtuurilla toimivat pikaviestintäverkot ovat riippuvaisia keskitetyn palvelimen verkkoyhteydestä ja toiminnasta[3]. Jos palvelimeen tulee vika tai palvelimen ja verkon käyttäjän välinen verkkoyhteys katkeaa, palvelun saatavuudessa on ongelma.

Saatavuutta voidaan parantaa palvelinten, palveluiden ja verkkoyhteyksien kahdentamisella, hajauttamisella ja sovellustason vikasietoisuutta parantamalla. Vikasietoinen asiakasohjelma voi esimerkiksi osata vaihtaa käytettävää palvelinta automaattisesti, jos yhteys käytössä olevaan palvelimeen katkeaa. Vastaavasti palvelinohjelmistojen tulisi toimia vaikka esimerkiksi yksittäinen autentikointipalvelin lakkaisi toimimasta. Palvelun saatavuuden varmistamisessa olennaista ovat myös fyysiset ratkaisut: tilojen fyysisestä turvallisuudesta (kulunvalvonnasta, vartioinnista jne.) on huolehdittu, palvelimet kestävät yksittäisten osien hajoamisen ja huoltoja voidaan suorittaa ilman käyttökatkoja.

Saatavuuden varmistamisessa on otettava huomioon myös palvelunestohyökkäykset (Denial of Service, DoS). Esimerkiksi viestien välitys tai autentikointi voi olla mahdollista estää kuormittamalla sopivia järjestelmän komponentteja liikaa. Esimerkiksi kirjautumispalvelin pystyy tarkistamaan vain rajallisen määrän kirjautumisia tietyssä ajassa. Jos kirjautumispalvelimen jonot kasvavat liian suuriksi, palvelin saattaa kaatua tai asiakasohjelmat keskeyttävät kirjautumisen (aikakatkaisu). Kirjautumispalvelimen käytön estyminen estää uusien käyttäjien kirjautumisen, mutta ei välttämättä estä jo käynnissä olevaa kommunikointia verkossa.

3.2 Muita näkökulmia pikaviestinnän tietoturvaan

3.2.1 Välitettyjen viestien eheys jälkikäteen

Mahdollisuus kiistää tai todistaa viestin lähetys tai vastaanottaminen voi olla hyvin olennainen ominaisuus viestintäjärjestelmälle. Jos viestissä on esimerkiksi hyväksytty sopimus tai sopimusehtoja, riitatapauksessa viestien aitouden todistaminen on erittäin tärkeää. Toisaalta sille, joka haluaa kiistää hyväksyneensä sopimuksen mahdollisuus viestien lähettämisen ja sisällön kiistämiseen on erittäin olennaista. Mahdollisuus osoittaa luotettavasti, että viestin tarkoitettu vastaanottaja vastaanotti viestin voi olla tärkeää mm. ilmoituksen edellyttävissä asioissa

[3]Myös vertaisverkkoperiaatteella toimivia pikaviestintäverkkoja on tutkittu, esimerkiksi Rao ja Singhal (2007).

(kirjattua kirjettä vastaava järjestelmä).

Viestien lähettäjä ja sisällön alkuperäisyys voidaan varmistaa viestien kryptografisella allekirjoittamisella. Esimerkiksi PGP:llä allekirjoitetusta viestistä voidaan tarkistaa lähettäjä ja viestin aitous (Garfinkel, 1996). Vastaavasti OTR:ssä viestien vastaanottaja voi vastaanottaessa olla varma lähettäjän ja viestin sisällön aitoudesta, eheydestä ja luottamuksellisuudesta - jos vastapuolen tunnistus on suoritettu luotettavasti. Järjestelmän käyttämän salausjärjestelmän ominaisuuksiin kuuluu kuitenkin tietojen kiistämisen mahdollisuus. Jälkikäteen on mahdotonta osoittaa luotettavasti, kuka viestin lähetti tai mikä lähetetyn viestin todellinen sisältö oli. (Borisov et al., 2004)

3.2.2 Salauksen turvallisuus jälkikäteen

Hyvä salausjärjestelmä on turvallinen myös jälkikäteen. Jos hyökkääjä voi tallentaa viestiliikenteen ja murtaa salauksen kohtuullisessa ajassa, luottamuksellisuudessa on vakavia puutteita. Vastaavasti hyvän viestinvälityksen salausjärjestelmän peruspiirteeksi voidaan lukea välitettyjen viestien luottamuksellisuus, vaikka hyökkääjä saisi haltuunsa yksityisen avaimen esimerkiksi varastetun tietokoneen mukana. Esimerkiksi OTR:n salausjärjestelmä on suunniteltu pitämään välitetyt viestit luottamuksellisina, vaikka hyökkääjä saisi haltuunsa viestinvälityksen osapuolten yksityiset avaimet (Borisov et al., 2004).

Eräs klassinen hyökkäysmenetelmä on siirrettävien tietojen salakuuntelu, tallentaminen ja lähettäminen uudelleen (Aura, 1997). Hyökkääjä voi esimerkiksi salakuunnella autentikointiviestit ja lähettää viestit jälkikäteen uudelleen, ilman tarvetta viestien todellisen sisällön tai salasanan selvittämiseen. Salaus- ja siirtojärjestelmän täytyy tunnistaa ja hylätä uudelleenlähetetyt paketit luotettavasti. Uudelleenlähetysten tunnistusta toteutettaessa protokollan suunnittelija törmää helposti tarpeeseen minimoida siirrettävä tieto. Tiedon määrää minimoitaessa erilaiset uudelleenlähetyshyökkäykset tulevat helpommin toteutettaviksi. Yksinkertaisin toteutus uudelleenlähetyksiltä suojautumiseen on yksilöllisen numeron liittäminen lähetettävään pakettiin. Palvelimen täytyy määrätä pakettien aloitusnumero. Tyypillisesti numeroa kasvatetaan yhdellä jokaista uutta pakettia lähetettäessä.

3.2.3 Näkökulmien priorisointi

Erilaisissa ympäristöissä tulee ottaa huomioon erilaisia asioita ja näkökulmia. Esimerkiksi sotilaskäytössä viestintäjärjestelmissä ei riitä viestien sisällön salaaminen. Jos järjestelmän salakuuntelija pystyy päättelemään viesteistä ajan, lä-

hettäjän ja vastaanottajan - esimerkiksi taistelussa oleva yksikkö lähettää viestin tykistölle - järjestelmän käytön turvallisuus on hyvin kyseenalaista (Sterling, 2007). Vastaavaa ongelmaa ei yleensä ole yrityskäytössä - paitsi väärinkäytöksissä. Jos työnantaja pystyy selvittämään pikaviestintäliikenteestä työntekijän, joka on puhunut arkaluontoisia tietoja sisältäneen lehtijutun kirjoittajan kanssa, pikaviestintäjärjestelmän tietoturvassa voi katsoa olevan - ainakin käyttäjän kannalta - puutteita. Vastaavasti hyvin salaisen tiedon välityksessä luottamuksellisuus voi olla tärkeämpää kuin tiedon saatavuus, hyvin kiireellisessä tiedossa tiedon eheys ja saatavuus voi olla tärkeämpää kuin luottamuksellisuus. Esimerkiksi palohälytystä lähettäessä saatavuus voi olla tärkeämpää kuin luottamuksellisuus.

3.2.4 Päivitykset

Tietoturvapäivitykset ovat olennainen osa tietokoneohjelman elinkaarta. Pikaviestintäjärjestelmät ovat laajoja kokonaisuuksia[4], joten virheiden olemassaolo ja löytyminen on melko todennäköistä (Glass 2008 ja Mamone 1984). Kaupallisissa järjestelmissä käyttäjän kannalta ongelmaksi saattaa muodostua tuen loppuminen, mikäli tuotteen toimittaja päättää lopettaa päivitysten tarjoamisen. Vapaan lähdekoodin järjestelmissä ongelmien korjaaminen tai korjauttaminen on mahdollista.

Eräs ratkaisu kaupallisten ohjelmien ylläpidon jatkuvuuden varmistamiseksi on lähdekoodin turvatalletus (source code escrow). Talletuksessa kolmas osapuoli säilyttää lähdekoodin. Tallentaja ja ohjelman toimittaja sopivat, koska lähdekoodi voidaan luovuttaa ja kenelle. Lähdekoodi voidaan esimerkiksi luovuttaa nimetyille suurille asiakkaille, jos toimittaja menee konkurssiin tai toimittaa vakavaan tietoturvaongelmaan korjauksia liian hitaasti. (Freibrun, 2007). Suomessa esimerkiksi Helsingin seudun kauppakamari tarjoaa talletuspalvelua.

Myös pikaviestintäverkoissa leviää aktiivisesti matoja (worms). Monet madot leviävät lähettämällä itseään tiedostonsiirtoina tai viesteinä, joissa kehotetaan avaamaan linkki. Osa madoista levittää itseään käyttämällä hyväkseen asiakasohjelmista löytyneitä haavoittuvuuksia. Ohjelmointivirheistä johtuvien haavoittuvuuksien korjaamisessa toimittajan tarjoamien päivitysten saaminen on kriittistä. (Mannan ja van Oorschot, 2005)

[4]Esimerkiksi avoimen monissa pikaviestintäverkoissa toimivan pikaviestintäohjelma Pidginin version 2.5.5 kommunikointikirjasto on hieman yli 200000 riviä ohjelmakoodia. Pidginin käyttöliittymä on 100000 riviä ohjelmakoodia. Pidginin kotisivu, www.pidgin.im (viitattu 25.4.2009).

3.2.5 Muut ongelmat

Työn tietoturva-analyysi on rajattu kattamaan pääasiassa vain verkkoliikenne, mutta pelkkä verkkoliikenteen suojaaminen ei tee järjestelmästä turvallista. Täydellisesti suojattu ja toimiva viestien välitys ei tee päätepisteistä - asiakasohjelmista - täydellisiä. Monet asiakasohjelmat tarjoavat mahdollisuuden välitettyjen viestien kirjoittamiseen lokitiedostoihin. Useimmissa järjestelmissä lokitiedostojen salaus ei ole mahdollista ilman erillistä ohjelmaa. Asiakasohjelmien tallentamia tietoja täytyy joko rajoittaa tai suojata muilla keinoilla. Vaikka lokitietoja ei tallennettaisi, järjestelmän turvallisuus on vaarantunut, jos hyökkääjä voi katsoa käyttäjän olan yli näyttöä tai esimerkiksi asentaa oman salakuunteluohjelman päätelaitteeseen[5]. Verkkoturvallisuuden lisäksi täytyy huolehtia päätelaitteen ja käyttöympäristön fyysisestä turvallisuudesta, käyttäjän luotettavasta autentikoinnista, käyttöjärjestelmän päivityksistä, mahdollisesti levysalauksesta ja virustorjunnasta yms.

[5]Erilaisten valmiiden käyttäjältä piilossa toimivien kirjoituksen tallennusohjelmien löytäminen ja omien ohjelmien tekeminen on erittäin helppoa. Kts. esim. `http://sourceforge.net/projects/pykeylogger/` (viitattu 15.3.2009).

Luku 4

Katsaus pikaviestintäjärjestelmiin

Esiteltäviä järjestelmiä valittaessa on tehty ero pikaviestintäohjelmien ja pikaviestintäjärjestelmien välille. Esimerkiksi Microsoftin messenger -verkkoa on mahdollista käyttää kolmannen osapuolen ohjelmilla, jotka yleensä toimivat virallisia ohjelmia vastaavasti[1]. Tämä työ käsittelee pikaviestintäverkkoja ja virallisia asiakasohjelmia. Muita asiakasohjelmia esitellään tarvittaessa.

Katsaukseen on valittu suurimmat pikaviestintäverkot[2], eli AIM, Microsoftin Messenger ja Skype, sekä mahdollisesti huomattavasti kasvava Google Talk. IRC on käyttäjämäärältään marginaalinen, mutta iältään poikkeuksellinen. Jarkko Oikarinen julkaisi protokollan dokumentaation (Oikarinen ja Reed, 1993) vuonna 1993, useita vuosia ennen muiden nykyään käytössä olevien verkkojen julkaisua[3]. SILC on otettu mukaan katsaukseen tietoturvallisuuden puolesta kaikki tarpeet parhaiten kattavana järjestelmänä. OTR:ää on mahdollista käyttää missä tahansa pikaviestintäverkossa tiedon salaukseen. Tekstiviestit eivät suoranaisesti ole internetissä toimiva pikaviestintäjärjestelmä, mutta tekstiviestejä pidetään usein täysin turvallisena tapana siirtää tietoja.

Kandidaatintyön rajallisen laajuuden vuoksi paljon käytetyistä protokollista esi-

[1]Esimerkiksi Pidgin (http://www.pidgin.im/ , pikaviestintäasiakasohjelman verkkosivu, viitattu 22.3.2009) osaa muodostaa yhteyden Skypeä lukuunottamatta kaikkiin tässä työssä käsiteltyihin pikaviestintäverkkoihin.

[2]Google Insights (www.google.com/insights/) antaa aikaväliltä 3/2008-3/2009 järjestelmien vertailuluvuiksi seuraavaa: Microsoft Messenger 69, Skype 52, Aim 20, ICQ 19, IRC 15. Samalla asteikolla Facebookin vertailuluku on yli 1200. Esimerkiksi Choi ja Varian (2009) esittelee suosion ennustamista hakutuloksilla.

[3]Oikarisen alkuperäinen IRC tuli käyttöön jo vuoden 1988 loppupuolella (http://www.irc.org/history_docs/jarkko.html , viitattu 28.3.2009).

merkiksi XMPP (Extensible Messaging and Presence Protocol, Saint-Andre 2004a ja Saint-Andre 2004b) ja SIMPLE (Session Initiation Protocol (SIP, Rosenberg et al. 2002) for Instant Messaging and Presence Leveraging Extensions, Campbell et al. 2002) on jätetty tarkastelun ulkopuolelle. Sekä XMPP että SIMPLE ovat yleiskäyttöisiä viestinvälityksen ja läsnäolo- ja sijaintitiedon välitysprotokollia. Ominaisuuksiltaan molemmat protokollat vastaavat esimerkiksi AIMin ja Microsoftin Messengerin toiminnallisuutta.

4.1 MSN Messenger ja Windows Messenger

MSN Messenger on Microsoftin pikaviestintäjärjestelmän kuluttajille suunnattu versio kun taas Windows Messenger on tarkoitettu yrityskäyttöön (Groth ja Philbin, 2004). Windows Messenger on esiasennettuna Windows XP -tietokoneissa, joten kynnys käyttöönottoon on hyvin alhainen. Tunnus luodaan itse yksinkertaisella rekisteröinnillä, jossa ilmoitetaan käyttäjätunnus, haluttu salasana ja salasanan palautuskysymys. Valmiista vaihtoehdoista valittavia kysymyksiä on esimerkiksi "äidin syntymäpaikka"tai "ensimmäisen lemmikin nimi". Unohtuneen salasanan palautuskysymykseen vastaamalla pystyy vaihtamaan salasanan. Tämä on ongelmallista, sillä sosiaalisista verkoista saatavilla tiedoilla voi löytää hyviä arvauksia tai vastauksia palautuskysymyksiin (Rabkin, 2008). Samalla käyttäjätunnuksella ja salasanalla kirjaudutaan sisään pikaviestintäverkkoon, sähköpostiin ja muihin Microsoftin LiveID-palvelun tukemiin järjestelmiin.

Windows Messengerissä ja MSN Messengerissä kaikki tiedonsiirto, myös videokuva, ääni ja siirrettävät tiedostot, välittyy palveluntarjoajan palvelimen kautta. Microsoftin yrityksille tarkoitettu dokumentti Windows Messengerin ja MSN Messengerin eroista väittää Windows Messengerin tiedonsiirron olevan salattua (Groth ja Philbin, 2004). Viestinvälitys Messenger-verkkoon on salaamaton sekä Windows XP Windows Messengerillä, että Pidginillä. Liite B antaa esimerkin viestinvälityksestä. Viestinvälitys oli vastaavaa kummallakin asiakasohjelmalla. Liitteessä A on esitelty verkkoliikennetallenteiden rakennetta ja rajoituksia.

Windows Live Messengerillä yhteys on salattu ainoastaan palvelimen ja asiakasohjelman välillä, joten siirrettävä tiedon salaus puretaan palvelimella ja salataan uudelleen ennen lähetystä. Järjestelmä ei varoita lähettäjää, vaikka yhteys vastaanottajaan olisi salaamaton. Viestien tallennus lokitiedostoihin on mahdollista, mutta tallennettavia tietoja ei voi salata.

4.2 Skype

Skype on vertaisverkkoprotokollaa käyttävä puhe-, video- ja pikaviestintäverkko. Verkossa on keskitetyt palvelimet käyttäjien sijainnin, kirjautumistietojen ja profiilien tallennukseen, mutta asiakasohjelmien välinen viestintä on suoraa päästä päähän salattua. Skypen teettämässä kryptologiaan keskittyneessä tietoturva-analyysissä ei ollut huomautettavaa tietojen salauksesta (Berson, 2005). Skype-verkkoon voi rekisteröityä vapaasti. Rekisteröinnissä syötetään perustiedot ja sähköpostiosoite. Sähköpostiosoitteella ja käyttäjätunnuksella voi tilata sähköpostiin uuden salasanan unohtuneen tilalle. Sisään verkkoon kirjaudutaan käyttäjätunnuksella ja salasanalla. Yhteyksien muodostus ja autentikointi verkossa tapahtuu Skypen avainpalvelimen jokaiselle käyttäjälle luomilla vahvoilla sertifikaateilla (Berson, 2005).

Skypellä on mahdollista soittaa ja vastaanottaa puheluita Skype-verkon lisäksi perinteisistä puhelinverkoista erillisen palvelun kautta. Puhelinverkon salakuuntelu on viranomais- ja operaattoritasolla helppoa ja yksinkertaista. Skypen käyttäjä voi asettaa saapuvat puhelut välitettäväksi perinteiseen puhelinverkkoon. Välityksestä salaamattomaan verkkoon ei kerrota soittajalle.

Riippumattomissa tutkimuksissa (esimerkiksi Perényi ja Molnár 2007 ja Rossi et al. 2008) on parhaimmillaan pystytty suorittamaan vain korkean tason liikenneanalyysiä: jo Skype-liikenteen tunnistaminen muusta liikenteestä on osottautunut ongelmalliseksi. Migliardi et al. (2008) esittelee menetelmän luotettavan liikenteen tunnistamisen estämiseen.

4.3 AOL Instant Messenger (AIM)

AOL Instant Messenger (AOL, 2009a) on American Onlinen (AOL) pikaviestintäjärjestelmä. AOL on yksi suurimmista Yhdysvalloissa toimivista internetoperaattoreista. AOL tarjoaa pikaviestintäjärjestelmää internet-liittymiensä yhteydessä ohjelmistopaketin mukana, ja ehti suurista toimijoista pikaviestintämarkkinoille ensimmäisenä (vuonna 1997), joten järjestelmällä on suuri käyttäjäkanta historiallisistakin syistä. AIM käyttää protokollana OSCAR:ia (open system for communication in realtime). AIM-verkkoon voi rekisteröityä vapaasti. Sisään kirjaudutaan rekisteröinnissä valitulla käyttäjätunnuksella ja salasanalla. AIM:n salasana palautetaan syöttämällä julkinen käyttäjätunnus tai sähköpostiosoite. Järjestelmä lähettää salasanan palautuslinkin rekisteröinnin yhteydessä annettuun sähköpostiin.

AOL Instant Messengerin tiedonsiirto on salaamatonta, lukuunottamatta sisään-

kirjautumisen salasanoja (liite C). AIM Pro on parannettu versio, joka sisältää mm. verkkoliikenteen salauksen ja video- ja äänipuhelut (AOL, 2009b). Vaikka AIM Pro on suunnattu yrityskäyttöön, yksityiskäyttöä ei ole estetty tai rajoitettu. Liikenne välitetään AOL:n ylläpitämän palvelimen kautta. Välitetyt viestit voi tallentaa lokitiedostoihin automaattisesti, mutta tallennettuja viestejä ei voi salata.

4.4 Google Talk

Google Talkin markkinaosuus on toistaiseksi suhteellisen pieni, mutta Google tarjoaa pikaviestintäohjelman sisältävää Google-sovellukset-pakettia myös yrityskäyttöön (Google, 2009a). Google Talk on XMPP-pohjainen (Extensible Messaging and Presence Protocol, Saint-Andre 2004b) pikaviestintäohjelma, joka on integroitu myös Googlen Gmail-selainsähköpostiin (webmail). Asiakasohjelmassa on pikaviestinnän lisäksi mahdollisuus äänipuheluiden soittamiseen internetin välityksellä. XMPP-protokollaa käytettäessä - eli aina erillisellä asiakasohjelmalla - TLS-salauksen (Transport Layer Security, Dierks ja Rescorla 2006) käyttö on pakollista (Google, 2009b). Gmail-liitännäistä käytettäessä salaus ei aina ole käytössä (liite D). Järjestelmä ei anna lähettäjälle mahdollisuutta selvittää, onko vastaanottajan yhteys palvelimeen salattu.

Googlen käyttäjätilien avaaminen on vapaata. Samalla tunnuksella käytetään kaikkia Googlen tarjoamia palveluita, mm. pikaviestintää, sähköpostia, verkkotunnusten hallintapalveluita ja mainontapalveluita. Sisäänkirjautuminen tapahtuu käyttäjätunnuksella ja salasanalla. Verkkosivuille kirjautuminen suoritetaan erillisen salatun kirjautumispalvelun kautta, vaikka varsinainen verkkopalvelu ei olisi salattu. Myös Gmail-pikaviestintäliitännäistä käytettäessä käyttäjätunnus ja salasana välitetään erillisen salatun yhteyden kautta.

Ääni, video ja tiedostot siirretään suoraan asiakasohjelmien välillä. Erikoisena ominaisuutena Google Talk -asiakasohjelmassa on mahdollisuus estää vastapuolta tallentamasta keskustelun sisältöä, tosin ominaisuus toimii ainoastaan Googlen asiakasohjelmilla (Google, 2009c). Esimerkiksi Gmail-liitännäistä käytettäessä keskustelujen sisältö tallennetaan automaattisesti Googlen palvelimille, ellei tallentamista ole poistettu käytöstä. Google Talk -ohjelman sijaan on mahdollista käyttää muita XMPP:tä tukevia asiakasohjelmia samaan pikaviestintäverkkoon yhdistämiseen.

4.5 Internet Relay Chat (IRC)

Internet Relay Chat (IRC) on useisiin palvelimiin perustuva tekstipohjainen avoin pikaviestintäprotokolla. Asiakasohjelmat muodostavat yhteyden yhteen palvelimeen verkossa. Palvelimet välittävät viestin toiselle käyttäjälle reititystaulujen perusteella. Protokolla on hyvin yksinkertaista ja selväkielistä (liite E). (Oikarinen ja Reed, 1993). Internetissä on lukuisia IRC-verkkoja, joita ei ole yhdistetty toisiinsa[4].

Protokollan alkuperäinen määrittely ei huomioi salausta mitenkään. Myöhemmistä versioista (esim. Kalt 2000) löytyy mainintoja salauksen merkityksestä, mutta ei määrittelyä salauksen toteuttamisesta. Käytännössä useat palvelin- ja asiakasohjelmistot tukevat TLS-salausta. Palvelinten välisiä yhteyksiä ei välttämättä ole salattu. Lähettäjällä ei ole keinoa varmistaa, välitetäänkö viestiä salaamattomana. Eräs yleisesti tuettu IRC:n lisäosa on suora asiakkaiden välinen yhteys (Direct Client Connection, Rollo ja Mesander 1994). DCC:ssä palvelimen kautta neuvotellaan suora yhteys asiakasohjelmien välille. Yhteysneuvottelun jälkeen asiakasohjelmien väliset DCC-viestit eivät kulje palvelimen kautta. Protokollassa ei ole suojausta välimieshyökkäyksiin (man-in-the-middle), joten palvelin voi DCC-yhteyspyyntöä muokkaamalla huijata asiakasohjelmat ottamaan yhteyden kolmannen osapuolen kautta.

IRC perustuu järjestelmänä avoimuuteen: useimpiin verkkoihin yhdistettäessä ei suoriteta minkäänlaista autentikointia[5]. Kahdella käyttäjällä ei voi olla samaan aikaan samaa käyttäjätunnusta (nick), mutta vain harvoissa IRC-verkoissa käyttäjätunnuksen voi rekisteröidä vain omaan käyttöön. Normaalisti kuka tahansa voi valita toisen käyttäjän käyttämän käyttäjätunnuksen[6], jos tunnus ei valintahetkellä ole verkossa käytössä. Kuka tahansa voi perustaa kanavia (keskusteluhuoneita). Kanaville pääsyä voi rajoittaa esimerkiksi käyttäjän IP-osoitteen perusteella tai kanavakohtaisella salasanalla.

4.6 Secure Internet Live Conferencing (SILC)

Secure Internet Live Conferencing (SILC) on turvallisuusnäkökulmasta suunniteltu pikaviestintäprotokolla. SILC, kuten mm. IRC, on avoin protokolla, jonka turvallisuutta ja toimivuutta kuka tahansa voi tutkia ja tarkastella. Oletuksena

[4]Ks. esim. IRC-verkkojen hakukone, www.searchirc.com (viitattu 26.3.2009).

[5]Useat palvelinohjelmistot tukevat autentikointia, mutta verkon ylläpitäjän on toteutettava rekisteröinti ja käyttäjätunnusten ylläpito erillisessä järjestelmässä, esimerkiksi LDAP:ssa.

[6]Oikea käyttäjä tunnistetaan käyttäjätunnuksen, tietokoneen osoitteen ja etäkäyttäjätunnuksen perusteella, esimerkiksi nick!ojarva@vipunen.hut.fi.

kaikki viestit salataan vain asiakasohjelman ja palvelimen välillä, joten palvelin pystyy lukemaan viestien sisällön. Protokollassa ja asiakasohjelmissa on tuki salaukseen lähettäjän ja vastaanottajan välillä, jolloin verkon palvelimet tietävät ainoastaan viestin lähettäjän ja kohteen, eivät sisältöä. Asiakasohjelmat autentikoivat palvelimet palvelimen salausavaimen sormenjäljellä. Vastaavasti asiakasohjelmat voivat autentikoida muita verkon käyttäjiä käyttäjien julkisen salausavaimen sormenjäljellä. Sormenjälkien tarkistuksella vältetään kaikkien luottaman kolmannen osapuolen autentikointipalvelimen tarve. Samaa verkkoa voivat käyttää usean eri organisaation ihmiset ilman tarvetta luottaa verkon ylläpitäjään. (Riikonen, 2003)

SILC määrittelee sertifikaatit tai yhteisen salasanan kirjautumistavaksi (Riikonen, 2003). SILC-verkon ei tarvitse vaatia kirjautumista. Verkon ylläpitäjän vastuulla on huolehtia sertifikaattien luomisesta, allekirjoittamisesta ja ylläpidosta. Verkkoon kirjautumisen autentikointi ei välttämättä autentikoi käyttäjiä toisilleen, mutta toisen käyttäjän voi keskusteluyhteyttä muodostaessa autentikoida salausavaimen sormenjäljellä.

SILC on teorian tasolla hyvin turvallinen ja normaalit pikaviestinnän tarpeet täyttävä, mutta käytännössä heikkotasoiset asiakasohjelmat ja hyvien yrityskäyttöön soveltuvien ohjelmien puuttuminen ovat lähes täysin estäneet SILC:n käytön. Käyttäjille salausavainten sormenjälkien vaihtamisesta ei ole välittömiä tai näkyviä hyötyjä, joten tarkistaminen saatetaan kokea työlääksi, hankalaksi ja turhaksi. Tiedostojen ja multimedian siirto on toteutettu protokollassa dokumentaatiossa, mutta käytännössä asiakasohjelmat tukevat tiedostojen siirtoa huonosti. Tukea esimerkiksi näytön sisällön jakamiseen tai ääni- ja kuvapuheluihin ei ole, eikä niitä ole teknisesti mahdollista toteuttaa järjestelmään. SILC ei ratkaise keskustelulokien suojaamisen ongelmaa.

4.7 Off-the-Record Messaging (OTR)

Off-the-Record Messaging (OTR) ei ole pikaviestintäverkko tai verkkoprotokolla, vaan salausjärjestelmä, jonka viestit siirretään minkä tahansa muun pikaviestintäverkon kautta. Järjestelmä toteuttaa vaivattomasti salauksen lähettäjältä vastaanottajalle. Mahdollinen salakuuntelija tai esimerkiksi käytettävän pikaviestintäverkon palvelin näkee ainoastaan salatut viestit, ei viestin sisältöä. Eheyden säilyttämiseksi osapuolten tulee tarkistaa vastapuolen salausavaimen sormenjälki tai vaihtaa jaettu salaisuus, jolla autentikointi voidaan suorittaa (Alexander ja Goldberg, 2007, kts. 3.1 ja 4). Oikein käytettynä OTR takaa tiedon luottamuksellisuuden, vastapuolen identiteetin, viestien kiistämisen mahdollisuuden (repudiation) ja vanhojen keskusteluiden luottamuksellisuuden, vaikka hyökkää-

jä saisi jonkin osapuolen yksityisen avaimen selville. Vastapuolelle lähetettyihin viesteihin ei lisätä allekirjoitusta, joten lähettäjä voi aina kiistää vastaanottajan väittämän viestin sisällön. Keskustelun aikana viesti siirretään turvallisesti, ja vastaanottaja voi olla varma lähettäjän identiteetistä. Käsitellyistä protokollista poikkeuksellisena OTR tarjoaa ainoastaan kahden ihmisen välistä viestinvälitystä. Keskusteluhuoneissa tai -kanavilla OTR:ää ei voi käyttää. (Borisov et al., 2004)

OTR ei tarjoa keskustelulokien suojaamiseen mitään ratkaisua. Lokien luottamuksellisuudesta ja eheydestä on huolehdittava muilla järjestelyillä.

4.8 Tekstiviestit

Tekstiviestit ovat suhteellisen kalliita verrattuna yleensä täysin ilmaiseen internetin kautta tapahtuvaan pikaviestintään. Viestien toimitusajat ja toimitusluotettavuus vaihtelevat huomattavasti maittain (Clements, 2003). Tekstiviestijärjestelmässä viestit välitetään palveluntarjoajan ylläpitämän viestikeskuksen kautta vastaanottajalle tai vastaanottajan operaattorin viestikeskukseen. Verkkoliikenne päätelaitteen (tyypillisesti matkapuhelimen) ja tukiaseman välillä on salattu salaisella algoritmilla. Tekstiviestien sisältöä ei salata, ja viesti säilytetään ja siirretään salaamattomana viestikeskuksessa ja operaattorin verkon sisällä. (Siddique ja Amir, 2006)

Tekstiviestejä pidetään suhteellisen turvallisena menetelmänä luottamuksellisten viestien välitykseen. Esimerkiksi kirjautumistietojen siirtäminen tekstiviesteillä on yleistä. Turvallisuus perustuu erilliseen siirtotiehen: jos osa tiedoista välitetään internetin kautta ja osa tekstiviestillä, salakuuntelijan täytyy onnistua usean itsenäisen järjestelmän salakuuntelussa. Teleoperaattorien järjestelmät alkavat kuitenkin vaihtua täysin erillisistä suljetuista järjestelmistä käyttämään hyvin kustannustehokasta internetiä siirtotienä, jolloin myös järjestelmään kohdistuvat riskit ja hyökkäykset lisääntyvät.

Guinierin (1997) mukaan GSM:n (Global System for Mobile Communications) turvallisuustarpeiksi on määritetty viestinnän anonymiteetti, käyttäjän autentikointi operaattorille, sekä viestinvälityksen ja tietoliikenteen luottamuksellisuus. Yleisesti kaikki edellä mainitut tarpeet ovat yhä täytettyjä. Esimerkiksi Siddique ja Amir (2006) esittävät joitain GSM-verkoissa toimivia hyökkäyksiä. Suuri osa nykyisistä päätelaitteen ja tukiaseman välillä tapahtuvista hyökkäyksistä on korjattu Universal Mobile Telecommunications System -verkoissa (UMTS). Olennaisimpana erona UMTS lisää kaksisuuntaisen autentikoinnin: verkko varmistaa puhelimen (SIM-kortin) aitouden ja puhelin tukiaseman.

Tekstiviesteissä lähettäjä on ainoastaan lähettäjän määrittämä kenttä viesteissä, joten lähettäjätietojen väärentäminen on triviaalia. Normaalisti esimerkiksi matkapuhelimet kirjoittavat lähettäjäkentän sisällön automaattisesti lähettäjän puhelinnumeroksi. Verkossa lähettäjän identiteetin väärentäminen on hyvin helppoa, mutta vastaanottajan identiteetin varastaminen on erittäin haastavaa ilman SIM-kortin (Subscriber Identity Module, käyttäjän tunnistuskortti) varastamista tai vakoiluohjelman asentamista vastaanottajan puhelimeen. Viestinvälitykseen ja päätelaitteen ja tukiaseman väliseen siirtotiehen liittyvien turvallisuusongelmien lisäksi matkapuhelimiin kohdistettujen hyökkäysten määrä on voimakkaassa kasvussa, mm. älypuhelimiin kohdistuvina viruksina ja matoina (Ruitenbeek et al., 2007). Älypuhelinten internet-yhteydet ja käyttäjien ymmärtämättömyys esimerkiksi ohjelmien asentamisen tietoturvariskeistä lisää huomattavasti mahdollisuuksia haitta- tai vakoiluohjelmien leviämiseen.

4.9 Yhteenveto pikaviestintäjärjestelmistä

Esitellyistä pikaviestintäjärjestelmistä Microsoftin Messenger, AIM ja Google Talk ovat hyvin samankaltaisia. Skype käyttää kaikessa viestinnässä vahvaa salausta, mutta on suljettu järjestelmä, joten esimerkiksi lähdekoodin tarkastelu tai takaovien (backdoor) etsiminen ei ole mahdollista. IRC on avoimuuteen perustuva salaamaton järjestelmä, josta SILC on parannettu versio. OTR toimii minkä tahansa pikaviestintäverkon kanssa ylimääräisenä asiakasohjelmien välisenä salauskerroksena.

Keskitetty palvelin tarjoaa keskitetyn sijainnin salakuunteluun ja tietojen muokkaamiseen. Toisaalta keskitetyllä palvelimella voidaan esimerkiksi torjua monia asiakasohjelmiin kohdistuvia hyökkäyksiä tehokkaasti. Esimerkiksi AIM esti asiakasohjelmasta löydetyn puskuriylivuotohaavoittuvuuden hyväksikäytön estämällä palvelimilta haavoittuvuutta hyväksikäyttävien viestien välityksen (Hindocha ja Chien, 2003). Ennen uuden asiakasohjelman version julkaisemista ja jokaisen asiakasohjelman päivitystä haavoittuvuutta hyväksikäyttävä virus olisi voinut levitä käytännössä kaikille AIMia käyttäville tietokoneille.

Taulukko 4.1 tiivistää pikaviestintäjärjestelmistä salauksen, palvelinrakenteen ja mahdollisuuden oman palvelimen käyttöön. Lisäksi taulukko näyttää, voiko järjestelmän ylläpitäjä salakuunnella viestejä. Merkintä X tarkoittaa ominaisuuden täyttymistä. Viiva (-) tarkoittaa, että ominaisuutta ei ole.

Taulukko 4.1: Tiivistelmä pikaviestintäjärjestelmistä

Järjestelmä	Autentikointi salattu	Viestintä salattu	Keskitetty palvelin	Oma palvelin	Salakuuntelu
AIM	X	-	X	-	X
AIM Pro	X	X	X	-	X
MSN Messenger	X	-	X	-	X
Windows Messenger	X	-	X	X	X
Google Talk	X	X[1]	X	-	X
Skype[2]	X	X[3]	-	-	-[3]
IRC	?[4]	?[4]	X	X	X[5]
SILC	X	X	X	X	-[6]
Tekstiviestit	X[7]	X[8]	X	-	X
OTR	X	X			-

[1]Asiakasohjelmalla yhteys on salattu, mutta selaimella käytettäessä salausta ei oletuksena ole.

[2]Yrityksen oma salainen protokolla.

[3]Yhteydet on salattu käyttäjien välillä. Keskitetty palvelin muodostaa yhteyden ja varmistaa identiteetin, joten palvelinta hallinnoivan tahon toiminen välimiehenä huomaamattomasti on mahdollista (Berson, 2005).

[4]Yhteys on salaamaton. Asiakasohjelman ja palvelimen välinen yhteys on mahdollista salata. Palvelinten välisiä yhteyksiä ei välttämättä ole salattu.

[5]Protokollassa on DCC-laajennus (Direct Client-To-Client, suora asiakkaiden välinen yhteys), jossa asiakasohjelmat viestivät suoraan keskenään, optionaalisella salauksella.

[6]Oletuksena palvelin tietää viestin sisällön. Protokolla tukee suoraa asiakasohjelmien välistä salausta sekä yksityisviesteissä että keskusteluryhmissä. (Riikonen, 2003)

[7]Puhelimen autentikointi verkkoon SIM-kortilla on salattu.

[8]Viestintä puhelimen ja tukiaseman välillä on salattu, mutta viestintä operaattorin verkossa ja viesti viestikeskuksessa ei ole.

Luku 5

Pohdinta ja yhteenveto

Pikaviestintäjärjestelmän tietoturvan analysointi on monikäsitteinen ongelma. Viestinnän yksityisyyden suojan kannalta paremmissa järjestelmissä on usein käytettävyysongelmia. Lisäksi olemassa olevissa turvallisemmissa järjestelmissä, esimerkiksi OTR:ssä ja SILC:ssä, on huomattavasti vähemmän ominaisuuksia: ei puheen tai videon välitystä, tiedostojen siirtäminen on ongelmallista ja OTR:stä puuttuu kokonaan ryhmäkeskustelumahdollisuus. Selkeää pakkoa vahvan salauksen käyttöön on harvoin, eikä mahdollisen salakuuntelun aiheuttamia ongelmia ja riskejä oteta huomioon ennen ensimmäisiä suuria vahinkoja. Käytettävyydestä ja ominaisuuksista ei tingitä - eikä ole syytäkään tinkiä - ennen todellisia tarpeita tietoturvan kehittämiseen. Esimerkiksi monissa normaaleissa arkikeskusteluita vastaavissa pikaviestintäkeskusteluissa konkreettista tarvetta tietojen luottamuksellisuuteen ei ole.

Suomessa yksityiskäytössä viestinnän yksityisyyden suojaa - nk. kirjesalaisuutta - pidetään itsestäänselvyytenä. Postissa, puheluissa ja muussa perinteisessä viestinnässä yksityisyyden suoja on ollut erittäin vahvaa ja kiistämätöntä. Automaattista tallentamista, tiedon analyysiä ja valvontaa ei ole ollut mahdollista tehdä, eikä uusien menetelmien riskejä siksi ymmärretä. Viisitoista vuotta sitten esimerkiksi yrityksen luottamuksellisia tietoja, luottokortin numero tai verkkopankin salasanat lähetettiin postilla täysin suojaamattomina - mahdollisuus siihen, että posti kadotti kirjeen oli olemassa, mutta riski tietojen joutumisesta vääriin käsiin oli olematon. Nykyään samoja tietoja lähetetään pikaviestintäverkoissa tai sähköpostilla, jolloin monien tärkeiden tietojen etsiminen ja hyväksikäyttäminen voidaan suorittaa täysin automaattisesti.

Yritysympäristöissä suuri osa yrityksen tiedoista on luottamuksellisia, ja siksi myös välitettyjen viestien sisällön tulisi olla luottamuksellisia. Toisaalta ehdoton viestinnän osapuolten välinen luottamuksellisuus ei välttämättä ole yrityksen

kannalta hyvä ratkaisu. Yrityksen näkökulmasta tietojen keskitetty tallentaminen voi olla olennaista esimerkiksi väärinkäytösten selvittämisessä. Mahdollisuus osoittaa tallennetuista viesteistä viestien muuttumattomuus voi asioita sovittaessa olla tärkeää (non-repudiation). SILC:ssä on mahdollista valita osapuolten välinen salaus (palvelin ei tiedä viestin sisältöä) tai mahdollisuus keskitettyyn tallentamiseen (palvelin purkaa ja salaa kaikki viestit). Lisäksi SILC mahdollistaa lähetettävän viestin allekirjoittamisen yksityisellä avaimella niin, että vastaanottaja voi jälkikäteen osoittaa viestin aitouden ja lähettäjän identiteetin. Mikään suurista pikaviestintäverkoista ei tue viestin lähettäjän ja aitouden todistamista, ja esimerkiksi OTR:n ominaisuuksiin kuuluu erityisesti viestien kiistämisen mahdollisuus.

Teknisesti nykyisiä järjestelmiä luotettavampia ja turvallisempia pikaviestintäjärjestelmiä on olemassa. Turvallisempien järjestelmien käyttäjien vähyys, käytettävyysongelmat, tiedon puute, ymmärtämättömyys ja konkreettisen tarpeen puuttumisen lisäksi mahdollisesti suurin este teknisesti parempien järjestelmien käyttöönotolle ja käyttämiselle lienee ihmisille luontainen muutosten vastustaminen (Trader-Leigh, 2002). Ongelmaa voidaan yleensä pienentää merkittävästi esittelemällä riittävät perustelut muutosten tarpeellisuudelle (Bovey ja Hede, 2001).

Nykyään käytössä olevista järjestelmistä on syytä mahdollisuuksien mukaan valita salausta käyttävä järjestelmä, esimerkiksi Google Talk. Tietoa siirtäessä tulisi etukäteen miettiä, kuinka luottamuksellista tieto on. Luottamuksellista tietoa tulisi siirtää vain riittävän turvallista siirtotietä: vahvalla salauksella autentikoidulle vastapuolelle (OTR) tai erillisellä siirtotiellä (henkilökohtaisesti tai esimerkiksi postilla). Yritysten sisäisessä käytössä sisäisen pikaviestintäpalvelimen käyttöönotto voi olla järkevää riskien vähentämiseksi. Erillisenä pikaviestintäjärjestelmänä SILC on protokollana ominaisuuksiltaan mahdollisesti kattavin: avoin, vahva autentikointi ja salaus, viestin allekirjoittamisen mahdollisuus (mutta ei velvoitetta) sekä asiakkaalta asiakkaalle salatut viestit ja keskusteluryhmät, jotka eivät edellytä luotettavia palvelimia luottamuksellisen tiedon turvalliseen välitykseen. SILC:n erittäin olennainen puute on asiakas- ja palvelinohjelmien taso ja ominaisuudet.

Kirjallisuutta

Chris Alexander ja Ian Goldberg. Improved user authentication in off-the-record messaging. *WPES '07: Proceedings of the 2007 ACM workshop on Privacy in electronic society*, sivut 41–47, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-883-1. doi: http://doi.acm.org/10.1145/1314333.1314340.

Ross Anderson. *Security Engineering - A Guide to Building Dependable Distributed Systems*. Wiley, 2001. ISBN 0-471-38922-7. 3. painos.

AOL. Instant Messenger - AIM, 2009a. URL `http://dashboard.aim.com/aim`. AOL Instant Messenger. Viitattu 13.2.2009.

AOL. AIM Pro, 2009b. URL `http://aimpro.premiumservices.aol.com/`. Viitattu 22.3.2009.

Tuomas Aura. Strategies against Replay Attacks. *CSFW '97: Proceedings of the 10th IEEE workshop on Computer Security Foundations*, sivu 59, Washington, DC, USA, 1997. IEEE Computer Society. ISBN 0-8186-7990-5.

Elaine Barker. FIPS 197, Advanced Encryption Standard (AES), 2001. URL `http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf`. Viitattu 25.3.2009.

Tom Berson. Skype Security Evaluation. Tekninen raportti, Anagram Laboratories, 2005. URL `http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf`. Viitattu 13.4.2009.

Nikita Borisov, Ian Goldberg ja Eric Brewer. Off-the-record communication, or, why not to use PGP. *WPES '04: Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, sivut 77–84, New York, NY, USA, 2004. ACM. ISBN 1-58113-968-3. doi: http://doi.acm.org/10.1145/1029179.1029200.

Wayne Bovey ja Andrew Hede. Resistance to Organizational Change: the role of defence mechanisms. *Journal of Managerial Psychology*, 16(7):534–549, 2001. doi: 10.1108/EUM0000000006166.

Alan Calder ja Steve Watkins. *A Manager's Guide to Data Security and BS 7799/ISO 17799*. Kogan Page, Limited, 2005. ISBN 978-074-9444-14-3.

B. Campbell, J. Rosenberg, H. Schulzrinne, C. Huitema ja D. Gurle. Session Initiation Protocol (SIP) Extension for Instant Messaging. RFC 3428 (Proposed Standard), joulukuu 2002. URL `http://www.ietf.org/rfc/rfc3428.txt`.

Nicholas Cassimatis, Erik Mueller ja Patrick Henry Winston. Achieving Human-Level Intelligence through Integrated Systems and Research. *AI Magazine*, 27 (2):12–14, 2006. ISSN 0738-4602-2006.

Hyunyoung Choi ja Hal Varian. Predicting the Present with Google Trends, 2009. URL `http://www.google.com/googleblogs/pdfs/google_predicting_the_present.pdf`. Viitattu 4.4.2009.

Tom Clements. SMS – Short but sweet. 2003. URL `http://developers.sun.com/mobility/midp/articles/sms/`. Viitattu 20.3.2009.

T. Dierks ja E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4346 (Proposed Standard), huhtikuu 2006. URL `http://www.ietf.org/rfc/rfc4346.txt`. Obsoleted by RFC 5246, updated by RFCs 4366, 4680, 4681.

George Doddington. Speaker recognition - Identifying people by their voices. *Proceedings of the IEEE*, 73(11):1651–1664, 1985. ISSN 0018-9219.

Eric Freibrun. Source Code Escrow Agreements - Balancing the Interests of Users and Vendors. 2007. URL `http://www.freibrun.com/articles/articl15.htm`. Viitattu 19.3.2009.

Simson Garfinkel. *PGP: Pretty Good Privacy*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 1996. ISBN 156-5-920-98-8.

Robert L. Glass. Two Mistakes and Error-Free Software: A Confession. *IEEE Software*, 25(4):96, 2008. ISSN 0740-7459. doi: http://dx.doi.org/10.1109/MS.2008.102.

Google. Google: Google-sovellukset, 2009a. URL `http://www.google.com/a/enterprise/`. Google-sovellukset-palvelun esittelysivu. Viitattu 28.2.2009.

Google. Google: Open Communications - Google Talk for Developers - Google Code, 2009b. URL `http://code.google.com/intl/fi-FI/apis/talk/open_communications.html`. Google-sovellukset-pakettiin kuuluvan Google Talk -järjestelmän API:n esittelysivu. Viitattu 28.2.2009.

Google. Google Talk - Chat History Saving, 2009c. URL `http://www.google.com/talk/chathistory.html`. Viitattu 21.3.2009.

Lorie Groth ja Kevin Philbin. Windows Messenger 5.1: Windows Messenger vs MSN Messenger: What's the Difference?, 2004. URL `http://www.microsoft.com/downloads/details.aspx?FamilyID=5e921409-d143-45ca-9a1c-7636a7cbca9e`. Viitattu 12.3.2009.

Mark Handel ja James Herbsleb. What is chat doing in the workplace? *CSCW '02: Proceedings of the 2002 ACM conference on Computer supported cooperative work*, sivut 1–10, New York, NY, USA, 2002. ACM. ISBN 1-58113-560-2. doi: http://doi.acm.org/10.1145/587078.587080.

Neal Hindocha ja Eric Chien. Malicious Threats and Vulnerabilities in Instant Messaging, 2003. URL `http://www.symantec.com/avcenter/reference/malicious.threats.instant.messaging.pdf`. Viitattu 10.4.2009.

Ellen Isaacs, Alan Walendowski, Steve Whittaker, Diane J. Schiano ja Candace Kamm. The character, functions, and styles of instant messaging in the workplace. *CSCW '02: Proceedings of the 2002 ACM conference on Computer supported cooperative work*, sivut 11–20, New York, NY, USA, 2002. ACM. ISBN 1-58113-560-2. doi: http://doi.acm.org/10.1145/587078.587081.

ISO/IEC. ISO/IEC 27002:2005: Information technology - Security techniques - Code of practice for information security management, 2005.

Christophe Kalt. Internet Relay Chat: Server Protocol. RFC 2813 (Informational), huhtikuu 2000. URL `http://www.ietf.org/rfc/rfc2813.txt`.

Auguste Kerckhoffs. La Cryptographie Militaire. *Journal des Sciences Militaires*, 9:5–38, 1883.

Hugo Krawczyk, Mihir Bellare ja Ran Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104 (Informational), helmikuu 1997. URL `http://www.ietf.org/rfc/rfc2104.txt`.

Theodore Krovetz. UMAC: Message Authentication Code using Universal Hashing. RFC 4418 (Informational), maaliskuu 2006. URL `http://www.ietf.org/rfc/rfc4418.txt`.

Markus. Kuhn ja Ross Anderson. Soft tempest: Hidden data transmission using electromagnetic emanations. *Proceedings of the Second International Workshop on Information Hiding*, sivut 124–142, London, UK, 1998. Springer-Verlag. ISBN 3-540-65386-4.

Salvatore Mamone. Error free code: is it attainable? *SIGPLAN Notices*, 19(3): 57–60, 1984. ISSN 0362-1340. doi: http://doi.acm.org/10.1145/948576.948586.

Mohammad Mannan ja Paul C. van Oorschot. On instant messaging worms, analysis and countermeasures. *WORM '05: Proceedings of the 2005 ACM workshop on Rapid malcode*, sivut 2–11, New York, NY, USA, 2005. ACM. ISBN 1-59593-229-1. doi: http://doi.acm.org/10.1145/1103626.1103629.

Stéphane Manuel ja Thomas Peyrin. Collisions on SHA-0 in One Hour. sivut 16–35, 2008. doi: http://dx.doi.org/10.1007/978-3-540-71039-4_2.

Daniel Menascé. Security Performance. *IEEE Internet Computing*, 7(3):84–87, 2003. ISSN 1089-7801. doi: http://dx.doi.org/10.1109/MIC.2003.1200305.

Mauro Migliardi, Roberto Podesta, Matteo Tebaldi ja Massimo Maresca. Hiding Skype VoIP calls from parametric identification. *e-Forensics '08: Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, sivut 1–6, ICST, Brussels, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). ISBN 978-963-9799-19-6.

Kevin Mitnick ja William Simon. *The art of Deception: Controlling the human element of security*. Wiley, 2003. ISBN 978-0-7645-4280-0.

Jarkko Oikarinen ja Darren Reed. Internet Relay Chat Protocol. RFC 1459 (Experimental), toukokuu 1993. URL `http://www.ietf.org/rfc/rfc1459.txt`. Updated by RFCs 2810, 2811, 2812, 2813.

Marcell Perényi ja Sándor Molnár. Enhanced Skype traffic identification. *ValueTools '07: Proceedings of the 2nd international conference on Performance evaluation methodologies and tools*, sivut 1–9, ICST, Brussels, Belgium, Belgium, 2007. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). ISBN 978-963-9799-00-4.

Ariel Rabkin. Personal knowledge questions for fallback authentication: security questions in the era of Facebook. *SOUPS '08: Proceedings of the 4th symposium on Usable privacy and security*, sivut 13–23, New York, NY, USA, 2008. ACM. ISBN 978-1-60558-276-4. doi: http://doi.acm.org/10.1145/1408664.1408667.

Ravi Rao ja Sandeep Singhal. P2P-IM: A P2P Presence System for the Internet. *P2P '07: Proceedings of the Seventh IEEE International Conference on Peer-to-Peer Computing*, sivut 233–234, Washington, DC, USA, 2007. IEEE Computer Society. ISBN 0-7695-2986-0.

Randall C. Reid, Richard G. Platt ja June Wei. A teaching module to introduce encryption for web users. *InfoSecCD '05: Proceedings of the 2nd annual conference on Information security curriculum development*, sivut 60–65, New York, NY, USA, 2005. ACM. ISBN 1-59593-261-5. doi: http://doi.acm.org/10.1145/1107622.1107636.

Pekka Riikonen. SILC Protocol White Paper, 2003. URL `http://silcnet.org/docs/silc_protocol.pdf`. SILC-protokollan tiivis esittely. Viitattu 1.3.2009.

Ronald L. Rivest. The MD5 Message-Digest Algorithm. RFC 1321 (Informational), huhtikuu 1992. URL `http://www.ietf.org/rfc/rfc1321.txt`.

Ronald L. Rivest, Adi Shamir ja Leonard M. Adleman. Cryptographic communications system and method, 1977. US Patent nr 4,405,829.

Troy Rollo ja Ben Mesander. The Client-To-Client Protocol (CTCP): Appendix A: a Description of the DCC protocol, 1994. URL `http://www.irchelp.org/irchelp/rfc/ctcpspec.html`. Viitattu 15.3.2009.

J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley ja E. Schooler. SIP: Session Initiation Protocol. RFC 3261 (Proposed Standard), kesäkuu 2002. URL `http://www.ietf.org/rfc/rfc3261.txt`. Updated by RFCs 3265, 3853, 4320, 4916, 5393.

Dario Rossi, Silvio Valenti, Paolo Veglia, Dario Bonfiglio, Marco Mellia ja Michela Meo. Pictures from the Skype. *SIGMETRICS Perform. Eval. Rev.*, 36(2):83–86, 2008. ISSN 0163-5999. doi: http://doi.acm.org/10.1145/1453175.1453191.

Elizabeth Van Ruitenbeek, Tod Courtney, William H. Sanders ja Fabrice Stevens. Quantifying the Effectiveness of Mobile Phone Virus Response Mechanisms. *DSN '07: Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, sivut 790–800, Washington, DC, USA, 2007. IEEE Computer Society. ISBN 0-7695-2855-4. doi: http://dx.doi.org/10.1109/DSN.2007.78.

Peter Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Core. RFC 3920 (Proposed Standard), lokakuu 2004a. URL `http://www.ietf.org/rfc/rfc3920.txt`.

Peter Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence. RFC 3921 (Proposed Standard), lokakuu 2004b. URL `http://www.ietf.org/rfc/rfc3921.txt`.

S. Muhammad Siddique ja Muhammad Amir. GSM Security Issues and Challenges. *SNPD-SAWN '06: Proceedings of the Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, sivut 413–418, Washington, DC, USA, 2006. IEEE Computer Society. ISBN 0-7695-2611-X. doi: http://dx.doi.org/10.1109/SNPD-SAWN.2006.42.

William Stallings. *Cryptography and Network Security*. 2006. ISBN 0-13-187316-4. 4. painos.

Christopher Sterling. *Military Communications*. ABC-CLIO, 2007. ISBN 1-8510-9732-5.

Marc Stevens. Fast Collision Attack on MD5. Diplomityö, Eindhovenin teknillinen yliopisto, 2007. URL `http://www.win.tue.nl/hashclash/On%20Collisions%20for%20MD5%20-%20M.M.J.%20Stevens.pdf`. Viitattu 14.3.2009.

Marc Stevens, Arjen Lenstra ja Benne de Weger. Chosen-prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities, 2007. URL `http://www.win.tue.nl/hashclash/EC07v2.0.pdf`. Viitattu 14.3.2009.

Karyn Trader-Leigh. Case study: identifying resistance in managing change. *Journal of Managerial Psychology*, 15(2):138–155, 2002. doi: 10.1108/09534810210423044.

Xiaoyun Wang, Yiqun Lisa Yin ja Hongbo Yu. Finding Collisions in the Full SHA-1, 2005. URL `http://people.csail.mit.edu/yiqun/SHA1AttackProceedingVersion.pdf`. Viitattu 10.4.2009.

Wireshark Foundation. Wireshark, 2009. URL `http://www.wireshark.org/`. Verkkoanalysaattorin internetsivu. Viitattu 24.3.2009.

Charles Wright, Lucas Ballard, Fabian Monrose ja Gerald Masson. Language identification of encrypted voip traffic: Alejandra y roberto or alice and bob? *SS'07: Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, sivut 1–12, Berkeley, CA, USA, 2007. USENIX Association. ISBN 111-333-5555-77-9.

Liite A: Verkkoliikennetallenteista

Tietoliikenteen tallentamiseen on käytetty Wiresharkia (Wireshark Foundation, 2009). Liikenne on tallennettu työasemalta paikallisesti, mutta vastaavaa tallentamista ja analysointia voisi suorittaa esimerkiksi verkon reitittimellä tai WLAN-liikennettä salakuuntelemalla. Tietoliikennelistauksiin on valittu vain esimerkkejä pikaviestintäprotokollaan kuuluvista paketeista. Pakettien tiedoista on poistettu ylimääräisiä otsaketietoja. Hakasuluissa olevat tiedot ovat muokattuja, esimerkiksi "[message]"on oikeassa liikenteessä viestin sisältö.

Muiden liitteiden tietoliikennelistaukset on automaattisesti analysoitu selväkielisiksi. Esimerkiksi kappaleessa 4.5 esitellyn IRC:n saapuva yksityisviesti (PRIVMSG) näyttää analysoimattomana seuraavalta:

```
4500 0093 0f47 4000 3306 4dfc c059 7b0f E....G@.3.M..Y{.
c2c5 ebf3 1a0b 8d58 272d ccf3 5002 1270 .......X'-..P..p
8018 21f0 35cd 0000 0101 080a 3eff ebcc ..!.5.......>...
6132 0148 3ab4 6d6d 6f75 217a 6f6d 1275 ‘3.E:nick!ident@
406f 6d70 7075 2e6d 6f64 6565 6d69 6e63 hostname.domain.
732e 7475 712e 6689 2010 5949 514d 5327 fi.PRIVMSG.mynic
2227 786b 626c 7461 233a                k.:message
```

Paketti esitetään analysoituna muodossa

```
-> TCP, Src Port: 23090, Dst Port: 6667, Seq: 101, Len: 40
    :[nick]![ident]@[hostname.domain.fi] PRIVMSG [buddynick] :[message]
```

Liite E esittelee IRC-protokollan liikennettä analysoituna.

Liite B: Windows Messengerin verkkoliikennettä

```
-> TCP, Src Port: 10957, Dst Port: 1863, Seq: 19, Len: 81
  CVR 5 0x0409 winnt 5.1 i386 MSMSGS 4.7.3001 WindowsMessenger \\
    [loginname@mydomain.fi]

<- TCP, Src Port: 1863, Dst Port: 10957, Seq: 14, Len: 110
  CVR 5 1.0.0000 1.0.0000 1.0.0000 http://msgr.dlservice.microsoft.com \\
    http://download.live.com/?sku=messenger

[...]

<- TCP, Src Port: 1863, Dst Port: 10957, Seq: 316, Len: 38
  USR 7 OK [loginname@domain.fi] [myname] 1 0

<- TCP, Src Port: 1863, Dst Port: 10957, Seq: 934, Len: 21
  LSG 0 Individuals 0

<- TCP, Src Port: 1863, Dst Port: 10957, Seq: 969, Len: 37
  LST [buddy1nick@domain1.fi] [buddy1name] 11 1

<- TCP, Src Port: 1863, Dst Port: 10957, Seq: 1006, Len: 41
  LST [buddy2nick@domain2.fi] [buddy2name] 11 0

[...]

<- TCP, Src Port: 1863, Dst Port: 10964, Seq: 92, Len: 122
  MSG [sender@address.fi] [sendernick] 87
  MIME-Version: 1.0
  Content-Type: text/x-msmsgscontrol
  TypingUser: [sender@address.fi]

<- TCP, Src Port: 1863, Dst Port: 10964, Seq: 214, Len: 165
  MSG [sender@address.fi] [sendernick] 129
  MIME-Version: 1.0
  Content-Type: text/plain; charset=UTF-8
  X-MMS-IM-Format: FN=Segoe%20UI; EF=; CO=0; CS=1; PF=0

  [Viestin sisältö]
```

Liite C: AOL Messengerin verkkoliikennettä

```
TCP, Src Port: 10667, Dst Port: 5190, Seq: 11, Len: 44
    FNAC: Family: AIM Signon (0x0017), Subtype: Sign-on (0x0006)
  AIM Signon, Sign-on
    Buddy Name: [myname]


TCP, Src Port: aol, Dst Port: 10667, Seq: 11, Len: 28
    FNAC: Family: AIM Signon (0x0017), Subtype: Sign-on Reply (0x0007)
  AIM Signon, Sign-on Reply
    Signon challenge: 3099327296

TCP, Src Port: 10667, Dst Port: 5190, Seq: 55, Len: 131
    FNAC: Family: AIM Signon (0x0017), Subtype: Logon (0x0002)
  AIM Signon, Logon
    TLV: Screen name
        Value: [myname]
    TLV: Password Hash (MD5)
    TLV: Client language
        Value: en

TCP, Src Port: 5190, Dst Port: 10676, Seq: 3827, Len: 946
    FNAC: Family: AIM Buddylist (0x0003), Subtype: Oncoming Buddy (0x000b)
  AIM Buddylist Service, Oncoming Buddy
    Buddy: [buddy1nick]
    Online since: [logintime]

TCP, Src Port: 10676, Dst Port: 519, Seq: 1089, Len: 65
    FNAC: Family: AIM Messaging (0x0004), Subtype: Outgoing (0x0006)
  AIM Messaging, Outgoing
    Buddy: [buddy1nick]
    Message: [outgoingmessage]

TCP, Src Port: 5190, Dst Port: 10676, Seq: 6725, Len: 1185
    FNAC: Family: AIM Messaging (0x0004), Subtype: Incoming (0x0007)
  AIM Messaging, Incoming
    Buddy: [buddy1nick]
    Message: [incomingmessage]
```

Liite D: Google Talk -liikennekaappaus

```
-> TCP, Src Port: 19770, Dst Port: 80, Seq: 1251, Len: 213
  POST /mail/channel/bind?at=[ID]&VER=6&it=2&SID=[ID]&t=1
  Host: mail.google.com
  Content-Type: application/x-www-form-urlencoded; charset=UTF-8
  Content-Length: 35
  application/x-www-form-urlencoded
     count=1&req0_type=cf&req0_focused=1

-> TCP, Src Port: 19807, Dst Port: 80, Seq: 6288, Len: 1237
  POST /mail/?ui=2&ik=[SID]&view=invite&ivit=1&ivem=[othernick%40gmail.com]
  Host: mail.google.com
  Content-Type: application/x-www-form-urlencoded
  Content-Length: 2411
  application/x-www-form-urlencoded

-> TCP, Src Port: 19812, Dst Port: 80, Seq: 13560, Len: 1177
  GET /mail/photos/[othernick%40gmail.com]?1&rp=1&pld=1
  Host: mail.google.com

-> TCP, Src Port: 19821, Dst Port: 80, Seq: 2406, Len: 324
  POST /mail/channel/bind?at=[ID]&VER=6&it=32&SID=[ID]&t=1
  Host: mail.google.com
  Content-Type: application/x-www-form-urlencoded; charset=UTF-8
  application/x-www-form-urlencoded
     count=1&req0_type=m&req0_to=[othernick%40gmail.com]&req0_id=[ID] \\
       &req0_text=[viestin teksti]&req0_chatstate=active

-> TCP, Src Port: 19823, Dst Port: 80, Seq: 4997, Len: 217
  POST /mail/channel/bind?at=[ID]&VER=6&it=16404&SID=[ID]&t=1
  Host: mail.google.com
  Content-Type: application/x-www-form-urlencoded; charset=UTF-8
  application/x-www-form-urlencoded
     count=1&req0_type=cf&req0_focused=1
```

Liite E: IRC-protokollan verkkoliikennettä

```
-> TCP, Src Port: 25090, Dst Port: 6667, Seq: 1, Len: 50
    USER [name] [computer hostname] [server address] :[client version]

-> TCP, Src Port: 25090, Dst Port: 6667, Seq: 51, Len: 13
    NICK [nick]

-> TCP, Src Port: 25090, Dst Port: 6667, Seq: 109, Len: 20
    PRIVMSG [buddynick] :[message]

<- TCP, Src Port: 6667, Dst Port: 25090, Seq: 5030, Len: 46
    :[buddynick]![buddyident]@[buddyhost] PRIVMSG [nick] :[incoming message]

-> TCP, Src Port: 25090, Dst Port: 6667, Seq: 129, Len: 17
    PING 1237918031

<- TCP, Src Port: 6667, Dst Port: 25090, Seq: 5076, Len: 49
    :[server address] PONG [server name] :1237918031

-> TCP, Src Port: 25090, Dst Port: 6667, Seq: 176, Len: 26
    JOIN #[channel name]

<- TCP, Src Port: 6667, Dst Port: 25090, Seq: 5194, Len: 231
    :[nick]![my ident]@[my hostname] JOIN :#[channel name]
    :[server address] 353 [my nick] = #[channel name] :@[other nicks]
    :[server address] 366 [my nick] #[channel name] :End of /NAMES list.
```