JULKAISUJA 2/2018

Sähköisen viestinnän salaus- ja suojausmenetelmät

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Liikenne- ja viestintäministeriön julkaisuja
2/2018

Sähköisen viestinnän salaus- ja suojausmenetelmät

Liikenne- ja viestintäministeriö, Helsinki 2018

Liikenne- ja viestintäministeriö

ISBN PDF 978-952-243-546-0:

Helsinki 2018

Kuvailulehti

Julkaisija	Liikenne- ja viestintäministeriö		7.3.2018
Tekijät	Kimmo Halunen, Jani Suomalainen, Sami Lehtonen, Anni Karinsalo ja Visa Vallivaara		
Julkaisun nimi	Sähköisen viestinnän salaus- ja suojausmenetelmät		
Julkaisusarjan nimi ja numero	Liikenne- ja viestintäministeriön julkaisuja 2/2018		
Diaari/hankenumero		Teema	
ISBN PDF	978-952-243-546-0	ISSN PDF	1795-4045
URN-osoite	http://urn.fi/URN:ISBN:978-952-243-546-0		
Sivumäärä	72	Kieli	Suomi
Asiasanat	Tietoturva, tietoturvastrategia, sähköinen viestintä, yksityiselämän suoja, luottamuksellisen viestin suoja, salausteknologia, salausmenetelmät		

Tiivistelmä

Osana digitaalisen liiketoiminnan kasvuympäristön rakentamista koskevaa hallituksen kärkihanketta parannetaan kansalaisten luottamusta digitaalisiin palveluihin. Tämän kärkihankeen yhtenä keskeisenä toimenpiteenä on laadittu kansallinen tietoturvastrategia, jolla pyritään lisäämään kaupallisten tiedon salaus- ja suojausmenetelmien tarjontaa ja käyttöä sisämarkkinoilla.

Salaus- ja suojausmenetelmien merkitys on kasvanut digitalisaatiokehityksen myötä. Salausmenetelmien käytöllä voidaan kasvattaa kuluttajien luottamusta digitaalisiin palveluihin. Markkinoilla saatavilla olevien salausteknologioita hyödyntävien tieto- ja viestintäpalveluiden määrä jatkuvasti kasvanut.

Tässä raportissa esitetään katsaus sähköisen viestinnän salaus- ja suojausmenetelmistä, niihin liittyvistä mahdollisuuksista sekä riskeistä. Selvityksessä kuvataan myös salaus- ja suojausteknologioiden kehittymisen tulevaisuuden näkymiä.

Raportin keskeisimmät johtopäätökset ovat, että salausteknologioilla on suuri merkitys sähköisen viestinnän suojaamiseksi. Viestinnän suojaamiseksi on suositeltavaa käyttää päästä päähän salattuja ja tiedon eheyden varmentavia viestintämenetelmiä. Takaporttien eli tahallisesti heikennettyjen salausmenetelmien vaatimista voidaan pitää ykistyiselämän suojalle sekä tietoturvallisuudelle haitallisena.

Kustantaja	Liikenne- ja veistintäministeriö
Painopaikka ja vuosi	Lönnberg Print & Promo, 2018
Julkaisun myynti/jakaja	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Presentationsblad

Utgivare	Kommunikationsministeriet		7.3.2018
Författare	Kimmo Halunen, Jani Suomalainen, Sami Lehtonen, Anni Karinsalo och Visa Vallivaara		
Publikationens titel	Kryptering och skydd av elektronisk kommunikation		
Publikationsseriens namn och nummer	Kommunikationsministeriets publikationer 2/2018		
Diarie-/projektnummer		Tema	
ISBN PDF	978-952-243-546-0	ISSN PDF	1795-4045
URN-adress	http://urn.fi/URN:ISBN:978-952-243-546-0		
Sidantal	72	Språk	Finsk
Nyckelord	informationssäkerhet, informationssäkerhetsstrategi, elektronisk kommunikation, skyddet för privatlivet, skyddet av förtroliga meddelanden, krypteringsteknik, krypteringsmetod		

Referat

Ett led i regeringens spetsprojekt för att skapa en tillväxtmiljö för digital affärsverksamhet går ut på att förbättra medborgarnas förtroende för digitala tjänster. Som en central åtgärd i detta spetsprojekt har man utarbetat en nationell informationssäkerhetsstrategi för att på den inre marknaden öka utbudet och användningen av kommersiella metoder för kryptering och skydd av data.

Betydelsen av olika metoder för kryptering och skydd av data har vuxit i takt med att digitaliseringen har utvecklats. Genom att använda kryptering kan vi öka konsumenternas förtroende för digitala tjänster. Ute på marknaden växer det antal informations- och kommunikationstjänster som tillämpar krypteringstekniker ständigt.

I denna rapport ges en överblick över olika metoder för kryptering och skydd av elektronisk kommunikation samt de möjligheter och risker som är förknippade med dem. Dessutom beskrivs framtidsutsikterna för utvecklingen av olika krypterings- och skyddstekniker.

De viktigaste slutsatserna av rapporten är att krypteringsteknikerna är av stor betydelse vid skyddet av elektronisk kommunikation. För att garantera en skyddad kommunikation rekommenderas kommunikationsmetoder som är krypterade från början till slut och som säkrar att informationen är oföränderlig. Att kräva ”bakdörrar”, alltså avsiktligt försvagade krypteringsmetoder, kan på det hela taget anses vara skadligt för informationssäkerheten.

Förläggare	Kommunikationsministeriet
Tryckort och år	Lönnberg Print & Promo, 2018
Beställningar/ distribution	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi

Description sheet

Published by	Ministry of Transport and Communications		7 March 2018
Authors	Kimmo Halunen, Jani Suomalainen, Sami Lehtonen, Anni Karinsalo and Visa Vallivaara		
Title of publication	Encryption and protection methods in electronic communications		
Series and publication number	Publications of the Ministry of Transport and Communications 2/2018		
Register number		Subject	
ISBN PDF	978-952-243-546-0	ISSN PDF	1795-4045
Website address (URN)	http://urn.fi/URN:ISBN:978-952-243-546-0		
Pages	72	Language	Finnish
Keywords	Information security, information security strategy, electronic communication, protection of private life, confidentiality, encryption technology, encryption methods		

Abstract

As part of the Government Programme's key project concerning the creation of a digital growth environment, an effort will be made to increase the population's trust in digital services. As one of the central actions of this key project, a national information security strategy has been drawn up. The strategy aims to increase the provision and use of encryption and protection methods for commercial data in the domestic market.

The significance of encryption and protection methods has grown with the development of digitalisation. The use of encryption methods can increase consumer trust in digital services. The number of information and communication services available on the market that utilise encryption technologies is growing.

This report includes a review of encryption and protection methods for electronic communication, as well as the related possibilities and risks. The report also describes the future outlook for the development of encryption and protection technologies.

The report shows that encryption technologies play an enormous role in the protection of electronic communication. In order to protect communication, the use of end-to-end encryption and communication methods that guarantee the integrity of data are recommended. A requirement for back doors, meaning weakened encryption methods, can be considered harmful to right to privacy and information security.

Publisher	Ministry of Transport and Communications
Printed by (place and time)	Lönnberg Print & Promo, 2018
Publication sales/ Distributed by	Distribution by: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi

Sisältö

LUKIJALLE

Osana digitaalisen liiketoiminnan kasvuympäristön rakentamista koskevaa hallituksen kärkihanketta parannetaan kansalaisten luottamusta digitaalisiin palveluihin. Tämän kärkihankeen yhtenä keskeisenä toimenpiteenä on laadittu kansallinen tietoturvastrategia, jolla pyritään lisäämään kaupallisten tiedon salaus- ja suojausmenetelmien tarjontaa ja käyttöä sisämarkkinoilla.

Salaus- ja suojausmenetelmien merkitys on kasvanut digitalisaatiokehityksen myötä. Salausmenetelmien käytöllä voidaan suojata sähköisen viestinnän luottamuksellisuutta, kuten viestien sisältöä sekä välitystietoja. Viestinnän luottamuksellisuuden turvaaminen on tärkeää, sillä yksityisyyden suoja ja viestinnän salaisuuden loukkaamattomuus ovat perustuslaissa suojattuja perusoikeuksia. Julkisen vallan tehtävänä onkin aktiivisesti edistää perusoikeuksien, kuten yksityisyyden suojan ja viestinnän luottamuksellisuuden, toteutumista.

Viestinnän luottamuksellisuuden lisäksi salausmenetelmillä voidaan huolehtia myös tiedon eheydestä, joka tulevaisuudessa voi olla useiden palveluiden laadun ja turvallisuuden kannalta hyvin keskeistä. Esimerkiksi automaattista liikennettä tullaan tulevaisuudessa ohjaamaan digitaalista tietoa hyödyntämällä. Tämän tiedon aitouden ja muuttumattomuuden varmistaminen on keskeistä liikenneturvallisuuden varmistamiseksi.

Salausmenetelmien käytöllä voidaan kasvattaa kuluttajien luottamusta digitaalisiin palveluihin. Markkinoilla saatavilla olevien salausteknologioita hyödyntävien tieto- ja viestintäpalveluiden määrä on jatkuvasti kuluttajien lisääntyneen kysynnän seurauksena kasvanut. Tästä ovat esimerkkinä useat pikaviestintäsovellukset, joissa oletusarvoiseti käytetään päästä-päähän salausta. Yhä suurempi osa kuluttajista onkin lyhyen ajan sisällä siirtynyt käyttämään perinteisten puheluiden tai tekstiviestien sijasta pikaviestintäsovelluksia, joissa viestintä pystytään paremmin suojaamaan ulkopuolisilta.

Teknologian tutkimuskeskus VTT Oy on laatinut tämän selvityksen liikenne- ja viestintäministeriön toimeksiannosta. Selvityksessä esitetyt johtopäätökset ovat selvityksen toteuttajien, eivätkä välttämättä edusta liikenne- ja viestintäministeriön näkemyksiä. Selvitys ei myöskään ole aukoton kuvaus sähköisen viestinnän salaus- ja suojausmenetelmistä.

Maija Rönkä
Tammikuu 2018

1 Raportin yhteenveto

Perustuslain 10 §:ssä turvataan yksityisyyden suoja ja viestinnän salaisuuden loukkaamattomuus. Julkisen vallan tehtävänä on aktiivisesti edistää perusoikeuksien, kuten yksityisyyden suojan ja viestinnän luottamuksellisuuden, toteutumista. Digitalisoituva maailma luo uusia haasteita monien näiden oikeuksien toteutumiselle. Osana digitaalisen kasvuympäristön rakentamista koskevaa hallituksen kärkihanketta parannetaan kansalaisten luottamusta digitaalisiin palveluihin. Näin ollen mm. viestinnän luottamuksellisuuden varmentamiseksi tarvittavien salaus- ja suojausmenetelmien ominaisuuksia on hyvä arvioida.

Tässä tutkimuksessa selvitettiin viestinnän salausmenetelmien ominaisuuksia, markkinoita ja niihin liittyviä mahdollisia riskejä. Tutkimuksen ulkopuolelle rajattiin puhtaasti tiedon säilytykseen (ns. data at rest) liittyvät salausmenetelmät ja palvelut.

Tutkimuksessa käytiin läpi erilaisia viestinnän salaukseen liittyviä protokollia, ohjelmistoja ja sovelluksia. Verkossa tapahtuvan viestinnän salaamisessa havaittiin kaksi päätasoa: verkkotaso ja sovellustaso. Molemmilla tasoilla salauksen voi toteuttaa eri menetelmillä. Varsinaiseen päästä päähän salaukseen vaaditaan usein sovellustason salaussovellus, mutta myös verkkotason salaus on tarpeellista.

Viestittävän tiedon lisäksi salausmenetelmillä voidaan varmistua myös tiedon muuttumattomuudesta. Viestintään liittyvän metadatan (viestin osoitetiedot, ajanhetki jne.) salaamiseen on myös joitakin menetelmiä, mutta ongelmana se on huomattavasti vaikeampi kuin sisällön salaaminen. Kuitenkin useimmissa nykyisissä keskitetyissä pikaviestinsovelluksissa (esim. Whatsapp, Signal) suurin osa tästä metadatasta ei näy palvelun ulkopuolelle verkkoliikenteestä. Eli verkkoliikenteestä voidaan vain päätellä, että käyttäjä on tietyllä ajanhetkellä yhteydessä palveluntarjoajaan, mutta ei sitä, kenen kanssa tämän palvelun sisällä kommunikoidaan.

Viestinnän salaukseen liittyviä riskejä on useita. Salausmenetelmät voivat murtua monella eri tasolla ja useilla tavoilla. Tällaisen haavoittuvuuden vakavuuteen vaikutta-

vat kyseisen menetelmän tai sovelluksen levinneisyys, käyttötarkoitus sekä erilaisten käyttäjien tai käyttäjäryhmien omat riski- ja uhka-arviot.

Raportin lopputuloksissa on useita johtopäätöksiä ja suosituksia koskien salausmenetelmiä ja niihin liittyvää teknologiaa sekä osaamista ja sen kehittämistä. Yksikäsitteistä suositusta yhden menetelmän tai sovelluksen käyttämiseen ei voida antaa, koska käyttäjiä ja käyttötarkoituksia on niin monia.

Lisäksi ns. takaporttien vaatimista salausmenetelmiin ja sovelluksiin ei voida pitää suositeltavana toimintamallina. Takaportit eli salausmenetelmien tahallinen heikentäminen eivät poista vahvaa salausta sitä haluavien saatavilta, mutta asettaa tavalliset käyttäjät ja heidän viestintänsä alttiiksi monenlaisille uhille.

Käyttäjille voidaan suositella päästä päähän salattujen viestimien käyttämistä, mutta avainten ja käytetyn viestisovelluksen turvallisuudesta on pidettävä samalla huolta. Kansallisella tasolla osaamisen huoltovarmuus salausmenetelmien osalta on huomioitava ja lisäksi on suositeltavaa muodostaa ohjeita ja arviointeja, joita erilaisten salausmenetelmien käyttäjät voivat hyödyntää. Ohjeiden tulisi olla saatavilla kansantajuisesti.

Tulevaisuuden näkymissä korostuu salausmenetelmien ja -sovellusten nopea kehitys sekä niiden mahdollisuudet esim. IoT -ympäristössä. Myös kvanttitietokoneiden ja kvanttilaskennan muodostamat riskit on hyvä huomioida tulevia salausmenetelmiä ja -sovelluksia valittaessa.

2 Johdanto

2.1 Tehtävänanto ja tutkimuksen taustaa

Perustuslain 10 §:ssä turvataan yksityisyyden suoja ja viestinnän salaisuuden loukkaamattomuus. Julkisen vallan tehtävänä on aktiivisesti edistää perusoikeuksien, kuten yksityisyyden suojan ja viestinnän luottamuksellisuuden, toteutumista. Viime vuosina on kuitenkin käynyt ilmi, että erityisesti tietoliikenneverkoissa tapahtuvaa viestintää voidaan helposti tarkkailla eri toimijoiden taholta. Tämä on tarkoittanut myös kasvavaa kiinnostusta viestinnän salaamiselle ja toisaalta myös viranomaisten osalta kiinnostusta mahdollisesti päästä käsiksi salatun liikenteen sisältöön.

Osana digitaalisen kasvuympäristön rakentamista koskevaa hallituksen kärkihanketta parannetaan kansalaisten luottamusta digitaalisiin palveluihin. Osana tätä kärkihanketta liikenne- ja viestintäministeriön johdolla on laadittu kansallinen tietoturvastrategia [1], jolla pyritään lisäämään kaupallisen tiedon salaus- ja suojausmenetelmien tarjontaa ja käyttöä sisämarkkinoilla. Strategian toimeenpanolla kehitetään myös päätelaitteiden, käyttöjärjestelmien, selainten, hakukoneiden, viestintäsovellusten, pilvipalveluiden ja muiden keskeisten tieto- ja viestintäteknisten hyödykkeiden tietoturvaominaisuuksia. Strategisin toimenpitein parannetaan myös digitaalisten hyödykkeiden tietoturvaominaisuuksien yhteentoimivuutta, läpinäkyvyyttä sekä todennettavuutta.

Tässä tutkimuksessa selvitettiin viestinnän salausmenetelmien ominaisuuksia, markkinoita ja niihin liittyviä mahdollisia riskejä. Tutkimuksen ulkopuolelle rajattiin puhtaasti tiedon säilytykseen (ns. data at rest) liittyvät salausmenetelmät ja palvelut.

3 Salausmenetelmien ominaisuudet ja markkinat

Salausmenetelmillä tarkoitetaan tässä raportissa sellaisia algoritmeja ja protokollia, joiden avulla käyttäjä tai ohjelmisto voi pyrkiä suojaamaan viestinnän luottamuksellisuuden ja eheyden. Salauksella tarkoitetaan viestin muokkaamista niin, että sen sisällön luottamuksellisuus tai eheys voidaan varmistaa. Lisäksi salauksella voidaan tukea muiden tarpeellisten tietoturvaominaisuuksien toteutumista.

3.1 Yleistä salausmenetelmistä

Salausmenetelmien päämääränä on varmistaa viestinnän luottamuksellisuuden ja/tai eheyden säilyminen viestin kulkiessa lähettäjältä vastaanottajalle. Tätä tarkoitusta varten voidaan käyttää lukuisia erilaisia menetelmiä. Menetelmän valinta riippuu monista eri vaatimuksista ja siitä, mitä salauksella halutaan saavuttaa. Vaatimukset voivat olla teknisiä (esimerkiksi suorituskykyyn tai salauksen turvallisuuden tasoon liittyviä) sekä lainsäädännöllisiä (esim. viranomaisten vaatimat takaportit tai tiedon turvaluokitukseen liittyvät vaatimukset). Takaportilla tarkoitetaan salausmenetelmään suunnitelmallisesti luotua heikkoutta, jonka avulla esim. viranomaiset pääsevät purkamaan salauksen tarvittaessa. Tällaiset takaportit ovat usein vuotaneet myös muualle kuin viranomaiskäyttöön tai niissä on havaittu heikkouksia (esim. Clipper-siru Yhdysvalloissa ja siihen liittyvä heikkous [2]).

Salausmenetelmien yhteydessä ajatellaan usein kahta osapuolta Ainoa ja Reinoa (engl. Alice ja Bob), jotka haluavat viestiä luottamuksellisesti *epäluotettavan* kanavan yli (ks. Kuva 1). Kanava voi olla mikä tahansa viestikanava, jossa oletetaan, että joku pahantahtoinen toimija Eeva (engl. Eve) haluaa päästä käsiksi Ainon ja Reinon viesteihin. Eevalla voidaan ajatella olevan mahdollisuudet kuunnella Ainon ja Reinon välistä kanavaa ja mahdollisesti (uhkamallista riippuen) myös muokata viestejä ennen kuin ne saapuvat Ainolta Reinolle tai toisin päin.

Jotta Aino ja Reino voivat kommunikoida luotettavasti ilman, että Eeva saa selville tai pääsee muokkaamaan viestejä, Aino ja Reino voivat käyttää salausmenetelmiä. Salausmenetelmissä vaaditaan osapuolilta aina *salausavain* ja salausmenetelmien teho perustuu siihen, että tämä avain on vain Ainon ja Reinon tiedossa. Tällöin Eeva ei pääse salakuuntelemaan eikä muokkaamaan Ainon ja Reinon välistä viestintää.

Kuva 1 Yleiskuva salauksesta viestinnässä

Yleisesti ottaen salausmenetelmät voidaan jakaa kahteen kategoriaan: *symmetrisiin* ja *asymmetrisiin* menetelmiin. Asymmetriset menetelmät tunnetaan myös *julkisen avaimen* menetelminä. Tällaisissa järjestelmissä salaaminen tapahtuu vastaanottajan julkisen avaimen avulla. Lähettäjän tulee saada tämä avain tietoonsa ja näiden avainten välittämiseen on useita tapoja. Hyvin usein käyttäjän ohjelmisto ja kommunikaatiojärjestelmä hoitavat avainten välittämisen ja varmentamisen ilman käyttäjän apua (verkkoselaimet ja useimmat salatut pikaviestinpalvelut), mutta joissakin järjestelmissä käyttäjän tulee itse olla aktiivinen avaimen hakemisessa ja käyttöönotossa (esim. PGP, Pretty Good Privacy, ks. Luku 3.2.2.2). Avain voi tulla viestinnän osana ns. *sertifikaatin* mukana tai se voidaan hakea erillisestä luettelosta (esim. keybase.io). On myös olemassa menetelmiä, joissa julkinen avain voidaan muodostaa ohjelmiston

toimesta käyttäjän identiteettiin liittyvästä tiedosta (esim. sähköpostiosoite tai nimi) (engl. Identity Based Encryption).

Salauksen purkamista varten vastaanottajalla on yksityinen, salainen avain, jonka avulla vastaanottaja voi purkaa tätä kyseistä avainta vastaavalla julkisella avaimella salatun viestin. On tärkeä huomata, että nämä kaksi avainta ovat eri avaimet ja vain juuri oikean yksityisen avaimen haltija voi purkaa salatun viestin. Julkisella avaimella salauksen purkaminen ei onnistu.

Symmetriset järjestelmät edustavat perinteistä salausta, jossa lähettäjällä ja vastaanottajalla molemmilla on yhteinen salainen avain, jonka avulla he voivat sekä salata että purkaa salattuja viestejä. Tämä on myös Kuvan 1 esittämä tilanne. Näistä tällä hetkellä yleisimmin käytetty on AES (Advanced Encryption Standard) [3], joka on jo 1990-luvun lopulla kehitetty ja edelleen turvallinen lohkosalausalgoritmi.

Salauksen lisäksi sekä symmetrisillä että asymmetrisillä menetelmillä voidaan myös varmistua viestien muuttumattomuudesta eli eheydestä. Menetelmät eivät ole samoja kuin viestejä salattaessa, mutta ne hyödyntävät samoja tai saman tyyppisiä avaimia. Tällöin viestin vastaanottaja voi varmistua viestin muuttumattomuudesta sekä viestin lähettäjän ”identiteetistä”. Symmetrisen salauksen tapauksessa on syytä huomata, että kolmas osapuoli ei voi varmentua siitä, kenen avaimella viesti on varmistettu. Tämä johtuu siitä, että kaikilla salattuun viestintään osallistuvilla osapuolilla on käytössään sama salainen avain.

Julkisen avaimen järjestelmissä vahvistus voidaan rakentaa digitaalisen allekirjoituksen muodossa, jolloin kuka tahansa voi varmistaa viestin allekirjoituksen julkisen avaimen avulla. Tämä varmennus tapahtuu yleensä ohjelmallisesti, jolloin järjestelmä tai ohjelmisto suorittaa tarkistuksen ja hyväksyy allekirjoituksen vain, mikäli tarkistus onnistuu. Käyttäjän ei tarvitse yleensä tehdä mitään toimenpiteitä, ellei järjestelmä sitten halua käyttäjän päättävän jatkotoimista silloin, kun tarkistus epäonnistuu.

Edellä mainittuja menetelmiä voidaan toteuttaa hyvin erilaisilla tavoilla ja tässä raportissa ei mennä teoreettisten toteutusten yksityiskohtiin. Ylätasolla voidaan todeta, että symmetristä salausta voidaan toteuttaa jono- ja lohkosalausalgoritmien avulla, joista molemmista löytyy sekä turvallisia että turvattomia ratkaisuja ja toteutuksia. Julkisen avaimen menetelmät taas pohjautuvat vaikeisiin matemaattisiin ongelmiin, joiden pohjalta niiden turvallisuus voidaan johtaa. Näistäkin löytyy hyvin eritasoisia toteutuksia. Lisäksi nykyisten julkisen avaimen menetelmien pohjana olevat matemaattiset ongelmat ovat sellaisia, joiden murtamiseen *kvanttitietokone* voi antaa merkittävää etua. Tämän vuoksi mm. Yhdysvaltojen standardointilaitos NIST (National Institute of Standards and Technology) on käynnistänyt kilpailun, jossa etsitään julkisen avaimen menetelmiä, joiden murtamisessa kvanttitietokoneesta ei olisi suurta apua. Lisää kvantti-

tietokoneista ja niihin liittyvistä salausmenetelmistä on kerrottu tämän raportin osioissa 6.1.2 ja 6.3.3.

3.1.1 Salausmenetelmien ominaisuudet

Salausmenetelmillä on edellä mainittujen yleisten ominaisuuksien lisäksi joukko tarkempia ominaisuuksia, joita ne voivat toteuttaa. Osalle näistä käsitteistä ei ole vielä vakiintunutta suomenkielistä termiä, joten tässä esitetään myös englanninkieliset termit.

Sessio on yleensä lyhytkestoinen ajanjakso, jonka aikana kommunikoivat osapuolet vaihtavat viestejä (tai vain yhden viestin). Avaintenvaihto (engl. key exchange) tarkoittaa prosessia, jonka aikana kommunikoivat osapuolet sopivat yhteisestä avaimesta, jolla varsinainen viestintä salataan. Sessioavaimella (engl. session key) tarkoitetaan avainta, joka on voimassa vain yhden session ajan. Pitkäkestoinen avain (engl. long term key/secret, master key) on taas avain, joka on voimassa pitkiäkin aikoja (jopa vuosia). Yleensä nykyiset salausmenetelmät pyrkivät siihen, että tällä pitkäkestoisella avaimella hoidetaan vain aivan ensimmäinen avaintenvaihto ja tämän jälkeen käytetään erilaisia sessioavaimia.

Perfect forward secrecy tarkoittaa sitä, että pitkän aikavälin avain ei paljastuessaan aiheuta aikaisempien (sessioavainten) luottamuksellisuuden vaarantumista eivätkä eri viestien sessioavaimet paljasta aiempia sessioavaimia. Backward secrecy taas tarkoittaa että nykyinen sessioavain ei ole paljastunut liikennettä kuuntelevalla hyökkääjälle vaikka aikaisempi sessioavain tai pitkän aikavälin avain olisikin vuotanut.

Kiistämättömyys tarkoittaa sitä, että lähettäjä ei voi jälkeenpäin kiistää lähettäneensä viestiä. Tämä vaatii yleensä julkisen avaimen menetelmän, jossa myös kolmannet osapuolet voivat varmistaa esimerkiksi allekirjoituksia. On hyvä huomata, että tämä ominaisuus ei ole mitenkään itsestään selvästi kaikkien sovellusten tavoitteena. Esimerkiksi Off The Record (OTR) viestintäprotokolla nimenomaisesti toteuttaa viestinnän kiistettävästi, jolloin käytännössä session päätyttyä viesteistä ei voida tuottaa varmoja todisteita siitä, onko joku viestinnän osapuoli lähettänyt tietyn viestin.

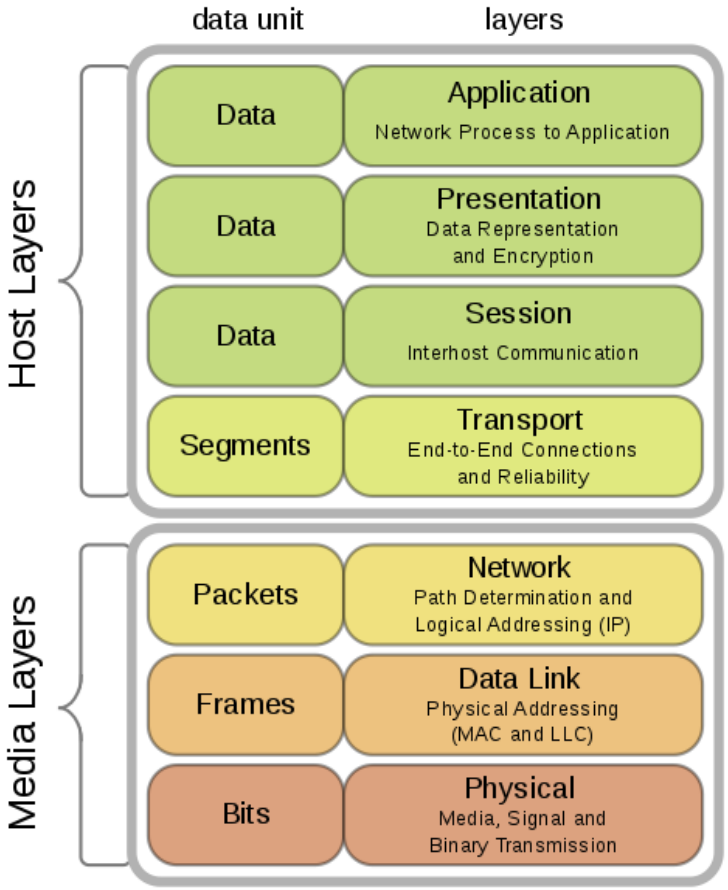
3.2 Eri verkon kerrosten salausmenetelmiä

Salausmenetelmiä tarvitaan turvaamaan monenlaisia viestintäsovelluksia. Esimerkiksi salauksella suojataan kahdenvälistä viestintää (puhetta, videoneuvotteluja, sähköposteja sekä pikaviestejä), ihmisten ja palveluiden sekä laitteiden välistä viestintää (www, sosiaalinen media, tiedostojen jako, kodin laitteet jne.) sekä myös laitteiden välistä viestintää (tiedon kerääminen antureiden avulla, ajoneuvojen liittäminen infrastruktuuriin, kriittisen infrastruktuurin valvonta ja ohjaus).

Viestinnän salaus voidaan toteuttaa monella eri verkon tasolla. ISO/OSI standardi jakaa verkon seitsemään eri kerrokseen ja TCP/IP -mallissa verkko jaetaan neljään kerrokseen. Näistä viestinnän salaamisen kannalta relevanteimmat kerrokset ovat ISO/OSI:n mukaiset verkkokerros ja sovelluskerros (Network ja Application Layer, ks.Kuva 2). Yksinkertaistaen voidaan kuva 2 mukaan ajatella, että tärkein ero salauksessa menee juuri Media ja Host -tasojen välissä. Suurin osa viestinnän salaamisen algoritmeista toimii jommallakummalla näillä tasoilla. Kuitenkin verkon jokaiselle tasolle on määritelty omia viestintäprotokollia ja niistä jokaisella voidaan toteuttaa myös salausmenetelmiä.

Hieman yksinkertaistaen voidaan sanoa, että mitä ylemmällä verkon kerroksella salaus on toteutettu, sitä lähemmäksi käyttäjää viesti tulee salattuna ennen salauksen purkamista. Edelleen on hyvä huomata, että eri verkon kerrosten salausmenetelmillä on kuitenkin merkitystä kyseisellä verkon tasolla toimivien laitteiden välisen kommunikaation turvaamisessa. Loppukäyttäjälle nämä ovat usein kuitenkin näkymättömiä, sillä viestinnän käyttäjä toimii yleensä sovelluskerroksessa toimivan sovelluksen kanssa.

Tässä osiossa esitellään tärkeimmät menetelmät (eli yleisesti ottaen protokollat), joilla salausta toteutetaan näissä kerroksissa. Yksittäistä protokollaa voidaan toteuttaa useissa eri sovelluksissa, joita käsitellään myöhemmissä osioissa ja vastaavasti yksittäinen sovellus voi salauksessa hyödyntää useampia eri protokollia.



Kuva 2. OSI / ISO standardin verkkokerrokset

Salauksen yhteydessä puhutaan usein myös *päästä päähän salauksesta* (engl. end-to-end encryption). Tällä tarkoitetaan sitä, että salaus suoritetaan lähettävän laitteen toimesta ja puretaan vasta vastaanottajan laitteessa. Tällöin viestiä kahden pään välillä välittävät laitteet ja järjestelmät eivät kykene purkamaan salausta ja lukemaan viestin sisältöä. On hyvä huomata, että joskus päästä-päähän salaus toimii nimenomaan kyseisen verkon kerroksen tasolla päästä päähän. Eli verkkotasolla päästä päähän salattu viesti salataan vasta kun se muutetaan verkkoon lähetettäviksi paketeiksi ja puretaan mahdollisesti jo ennen kuin vastaanottajan sovellus (sovellustasolla) käsittelee viestiä. Sovellustason päästä päähän salaus taas salaa viestin sovelluksessa ennen kuin se lähetetään verkkoon ja lopullinen salaus puretaan vasta vastaanottajan sovelluksessa.

3.2.1 Verkkotason salaus

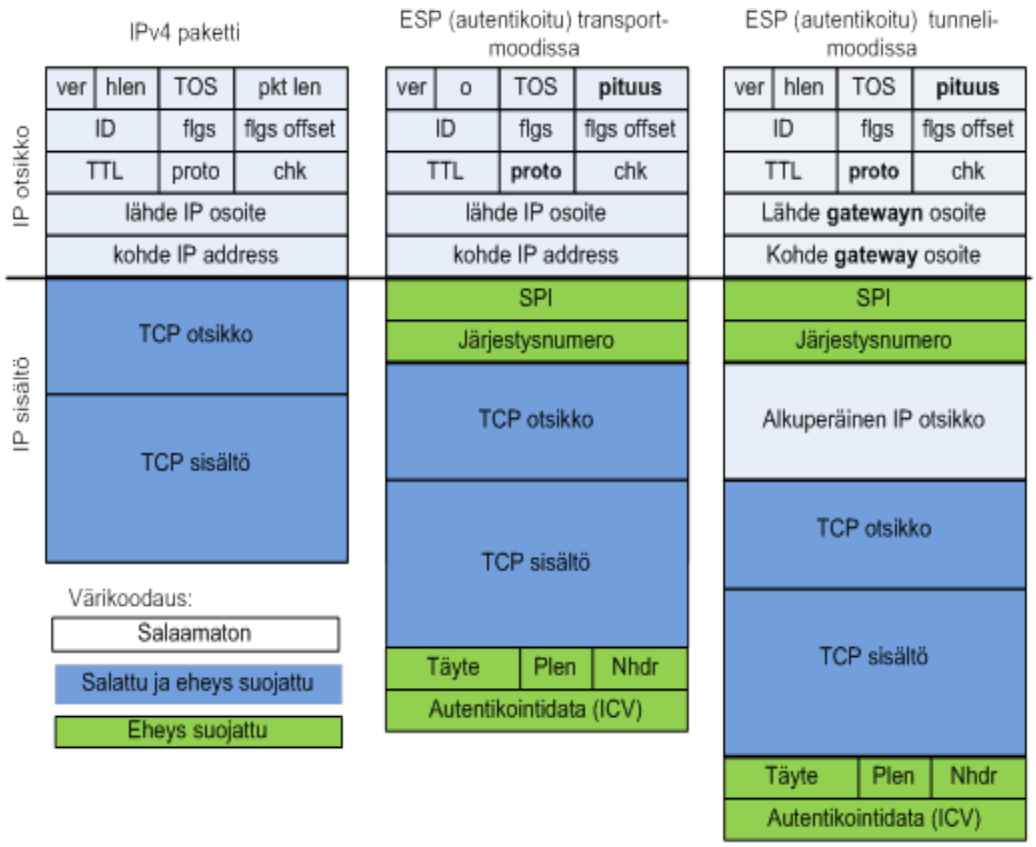
Verkkotason salauksella tarkoitetaan yleensä pakettien sisällön salaamista niiden liikkuessa verkossa. Karkeasti ottaen salaus tapahtuu ennen viestien lähettämistä verkkoon ja se puretaan vastaanottavassa päässä heti viestipakettien saavuttua.

3.2.1.1 IPsec

IPsec (Internet Protocol Security) [4] on tietoturvaprotokollaperhe, joka määrittelee mekanismit (arkkitehtuurin, pakettirakenteet ja avaintenneuvotteluprotokollat) Internet Protokollien (IPv4, IPv6) suojaamiselle. Standardia on myös laajennettu tukemaan ryhmäavaintenhallintaa ja multicast-paketteja [5]. Keskeisiä protokollia ovat:

- ESP (Encapsulated Security Payload) [6] - menetelmä pakettien salaamiseksi ja optionaalisesti myös autentikoimiseksi
- AH (Authentication Header) [7] - menetelmä pakettien eheyden ja autenttisuuden varmistamiseen
- IKE (Internet Key Exhange) [8] [9] - protokolla ESP:n ja AH:n käyttämien kryptografisten avainten sopimiseen

Protokollat voivat hyödyntää erilaisia kryptografisia algoritmeja. ESP ja AH protokollia voidaan käyttää kahdessa moodissa: transport ja gateway. Esimerkiksi kuva 3:ssa on EPS protokollan mukaiset rakenteet IP paketeille. Transport-moodi on tarkoitettu kahden IPsec:iä itsessään tukevien laitteiden kommunikointiin ja IP paketin sisältö (payload) korvataan salatulla sovelluksen (esim. TCP) paketilla ja autentikointidatalla. Gateway-moodissa paketit välitetään gateway-koneiden välillä ja alkuperäiset IP-otsikkotiedot korvataan gateway-koneiden tiedoilla.

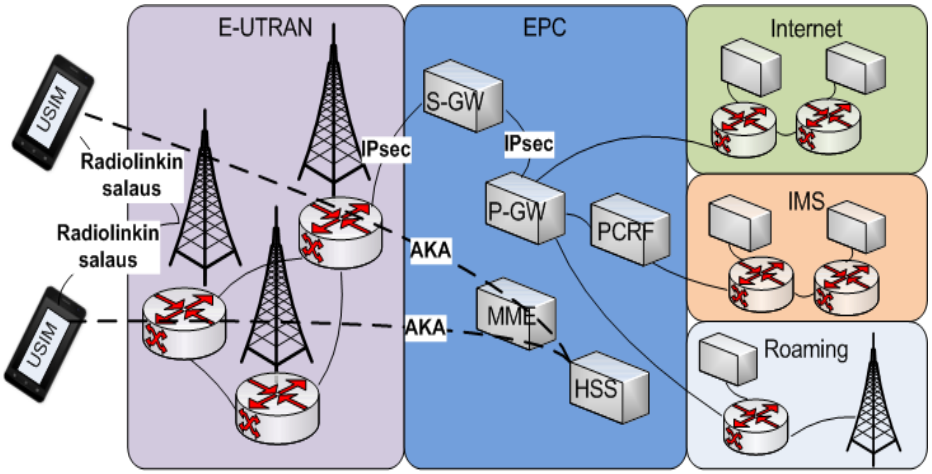


Kuva 3. ESP protokollan mukaiset pakettirakenteet IP pakettien salaamiseen ja tunnistamiseen ([6] [10])

IPsec protokollia pidetään turvallisina, mutta standardit ja käytännön toteutukset ovat kompleksisia ja yhteyksien muodostaminen ja konfiguroiminen on työlästä. Tyypillisesti IPsec:iä käytetään muodostamaan laitteiden välille virtuaalisia yksityisiä verkkoja (Virtual Private Network, VPN), joiden avulla voidaan siirtää turvallisesti usean eri sovelluksen dataa. IPseciä käytetään paljon runkoverkoissa ja esimerkiksi matkapuhelinverkkojen kommunikointi operaattorin komponenttien välillä on suojattu sillä.

3.2.1.2 Matkapuhelinverkkojen salaus

Matkapuhelinverkkojen tietoturvamenetelmät suojaavat radiolinkin ylittävän sekä runkoverkoissa kulkevan kommunikaation luottamuksellisuuden ja eheyden sekä mahdollistavat tunnistautumisen verkkojen ja globaalisti liikkuvien laitteiden välillä. Tietoturva-arkkitehtuuri on perusmuodossaan säilynyt samankaltaisena, mutta menetelmät ja algoritmit ovat kehittyneet standardisukupolvien mukana. Esimerkiksi kuva 4 esittelee tyypillisen arkkitehtuurin neljännen sukupolven verkoille ja siinä korostetaan salaukseen liittyviä standardoituja menetelmiä: radiolinkin salausta, ydinverkkoyhteyksien suojaamista VPN-tunneleilla (IPsec) ja tunnistautumista (Authentication and Key Agreement - AKA).



Kuva 4: Neljännen sukupolven verkkoarkkitehtuurin tietoturvamenetelmät [14] [71]

Matkapuhelinten toinen sukupolvi (GSM) tarjosi useita vaihtoehtoisia algoritmeja radiorajapinnan salaamiseen ja määritteli menetelmän käyttäjien tunnistamiseksi. Algoritmit olivat alun perin salaisia, mutta niiden toiminta pystyttiin selvittämään ja niitä vastaan on tehokkaat hyökkäykset. GSM-protokollassa tunnistaminen perustuu SIM-kortteilla jaettuihin autentikoitumisavaimiin. Päätelaitteet tunnistautuvat palvelevassa verkossa olevaan MME (Mobile Management Entity) palveluun, joka hyväksyy käyttäjät kotiverkon HSS (Home Subscriber Server) komponentilta saatujen käyttäjätietojen perusteella.

GSM:ssä vain päätelaitteet tunnistetaan. Päätelaitteen käyttämää verkkoa ei tunnisteta, mikä jättää GSM:än alttiiksi väärille pahantahtoisille tukiasemille. Autentikointiprotokollat A3 ja A8 generoivat laitteille tilapäiset avaimet ja tunnisteet SIM-korteilla olevista (Ki) avaimista. Protokollien käyttämä COMP128 algoritmin ensimmäinen versio on altis mm. kloonaushyökkäyksille [11]. GPRS liikenteen suojaamiseen on kehitetty

omat (GPRS Encryption Algorithm - GEA) menetelmät, jotka perustuvat samoihin algoritmeihin kuin puhelinliikenteen suojaaminen.

Kolmas sukupolvi (UMTS) [12] toi mukanaan turvallisemmat USIM-kortit sekä kaksisuuntaisen tunnistautumismenetelmän, joka perustuu MILENAGE autentikointi- ja avaintengenerointialgoritmeihin [13]. Myös salaus- ja eheyden suojausalgoritmit uudistettiin UMTS:ään (ks. Taulukko 1).

Neljäs sukupolvi (4G) eli LTE (Long Term Evolution) määrittelee kolme vaihtoehtoista (Taulukko 1:ssä esiteltyä) algoritmia päätelaitteen ja tukiaseman välisen liikenteen suojaukseen [14]. Lisäksi 4G:ssä, kuten aiemmissakin sukupolvissa, on “Null” salaus (EEA-0) eheys (EIA-0) vaihtoehdot, joissa data lähetetään suojaamattomana.

Taulukko 1. Salaus- ja eheysalgoritmit eri matkapuhelinsukupolvissa

Sukupolvi	**Algoritmi**	**Kuvaus**
2G	GSM Encryption Algorithm (A5/1,2,3,4)	Jonosalausalgoritmeja, joista A5/1 julkaistiin USA:n ja Euroopan markkinoille sekä heikennetty A5/2 muille markkinoille. Jo suunnitteluvaiheessa menetelmien vahvuutta (avainten pituutta) heikennettiin keinotekoisesti valtioiden toimesta [15]. A5/3 (64 bittisellä avaimella) ja A5/4 (128 bittinen avain) on myös 3G:ssä käytetty KASUMI. Kaikkia algoritmeja vastaan on myös esitelty tehokkaat hyökkäykset [16] [17]. A5/1 voidaan kryptoanalyysillä murtaa sekunnissa muutaman minuutin kuuntelun jälkeen.
3G	KASUMI (UEA1 ja UIA1) [18]	Lohkosalain, joka käyttää operoi 128 bittisillä avaimilla ja 64 bittisillä lohkoilla. Algoritmin on osoitettu olevan murrettavissa ”related key” hyökkäyksellä [17].
	SNOW [19]	Jonosalain, joka salaa 32 bittisiä sanoja 128 tai 256 bittisillä avaimilla nopeasti. Snow on mahdollisesti altis ”related key” hyökkäyksille [20].
4G	SNOW 3G (128-EEA1 ja 128-EIA1) [19]	Jonosalain, jota on päivitetty UMTS:stä LTE:hen. Myös tämä versio voi olla altis ”related key” hyökkäyksille [20].
	AES (128-EEA2) [21] ja AES CMAC (128-EIA2) [22]	AES on lohkosalain, jota CMAC moodissa käytetään luomaan autentikointikoodi (MAC) salatusta viestistä eli EIA2 implisiittisesti myös salaa viestit.
	ZUC (128-EEA3 ja 128-EIA3) [23] [24]	Jonosalain, joka on kehitetty Kiinassa pääasiassa Kiinan markkinoille.

Tutkimusta, joka pyrkii nostamaan tulevaisuuden (5G/6G) verkkojen salauksen ja tietoturvan tasoa sekä mahdollistamaan uudenlaisten sovellusten, radioteknologioihin ja laitteiden käyttämisen, esitellään luvussa 6.

3.2.1.3 SSH

Secure shell (SSH) [25] on tietoturvaprotokolla, jonka avulla voidaan luoda päästä-päähän suojattuja yhteyksiä Internetin ylitse. SSH:n tyypillisiä sovelluksia ovat laitteiden etäkäyttö (merkkipohjaisen konsolin kautta), turvallisten tunnelien muodostaminen sovelluksien välille sekä tiedostojen kopiointi. SSH tukee useita vaihtoehtoisia salaus- ja eheyden suojausalgoritmeja ja määrittelee avaintenhallintaan ja laitteiden tunnistamiseen vaihtoehtoisia (mm. julkisiin avaimiin tai salasanoihin) perustuvia protokollia.

3.2.1.4 Älykkään liikenneverkoston viestinnän salaus (C-ITS)

Nykyaikana useat ajoneuvot ovat jo monin tavoin toisiinsa yhteydessä. Lähitulevaisuudessa ne ovat myös vuorovaikutuksessa toistensa sekä ympäröivän maailman kanssa ja tämä liikenne tullaan suojaamaan Euroopassa EU:n C-ITS (*Cooperative Intelligent Transport Systems*) strategian mukaisesti. Älykkään liikenneverkoston toimijoita (*ITS-stations*) ovat älyajoneuvot ja älykäsinfrastruktuuri (*roadside units*), jotka kaikki luovat omat avainparinsa noudattaen *ISO/IEC 14516-2* standardia [26].

Yhdellä avainparilla tehdään sekä todennetaan digitaalisia allekirjoituksia ja toista käytetään symmetristen avainten sekä MAC avaimen (Message Authentication Code) luomiseen. EU:n viranomaiset pitävät yllä listaa kaikkien toimijoiden sertifikaateista (*European Certificate Trust List),* josta voidaan todentaa allekirjoitukset. Oletus salausalgoritmi on ECIES & AES128. Oletus allekirjoitusalgoritmi on *ECDSA & SHA256*. Vuoteen 2022 mennessä SHA256 vaihtuu SHA384 algoritmiksi, jossa on hankalampi löytää törmäyksiä, eli samoja tiivistearvoja/allekirjoituksia.[1]

Älykkään liikenneverkon salauksissa huomionarvoista on myös se, että nimenomaan viestien muuttumattomuuden (eli eheyden) takaaminen saattaa olla tärkeämmässä roolissa kuin varsinainen salaaminen. Esimerkiksi erilaisten sensorien tapauksessa nimenomaan eheys on suuressa roolissa. C-ITS strategiassa on painotettu jonkin verran ketteryyttä salausmenetelmien käyttöönotossa, mikäli nykyisin käytetyistä löytyy heikkouksia. Toinen mielenkiintoinen älykkääseen liikenteeseen liittyvä aihe on yhteensopivuus, sillä esimerkiksi Euroopassa ja Yhdysvalloissa mm. salaukseen liitty-

[1] https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf

vät ohjeistukset ja standardit ovat hieman toisistaan poikkeavat. Yhteensopivuuden takaaminen on nostettu yhdeksi merkittäväksi yhteistyön aiheeksi tällä saralla. [27]

3.2.2 Sovellustason salaus

Sovellustason salaus mahdollistaa oikein toteutettuna todellisen päästä päähän salatun yhteyden. Tämä tarkoittaa, että viesti salataan ennen kuin se poistuu sovelluksesta muun järjestelmän edelleen lähetettäväksi vastaanottajalle. Tämän jälkeen viesti etenee verkossa vastaanottajan laitteeseen ja (yleensä samaan) sovellukseen, jossa viesti puretaan ja esitetään vastaanottajalle. Verkkotason salaukseen verrattuna vahvuus on se, että salattu viesti on lähtökohtaisesti vain yhden sovelluksen käytössä. Verkkotason salaus puretaan yleensä aiemmin, jolloin salaamattomaan viestintään on mahdollista päästä käsiksi myös muiden kuin viestin käsittelyyn tarkoitetun ohjelman.

On hyvä huomata, että verkkotason ja sovellustason salausta voidaan käyttää yhtä aikaa. Tämä on joskus myös tarpeellista, sillä eri verkon kerrosten salausmenetelmät torjuvat erilaisia uhkia ja kaikkia uhkia ei ole välttämättä mahdollista torjua vain yhden kerroksen salausmenetelmällä. Erityisesti yhteyden varmentamisen on hyvä tapahtua monilla eri tasoilla, jopa silloin, kun varsinaista salausta ei käytetäkään.

3.2.2.1 TLS ja HTTPS

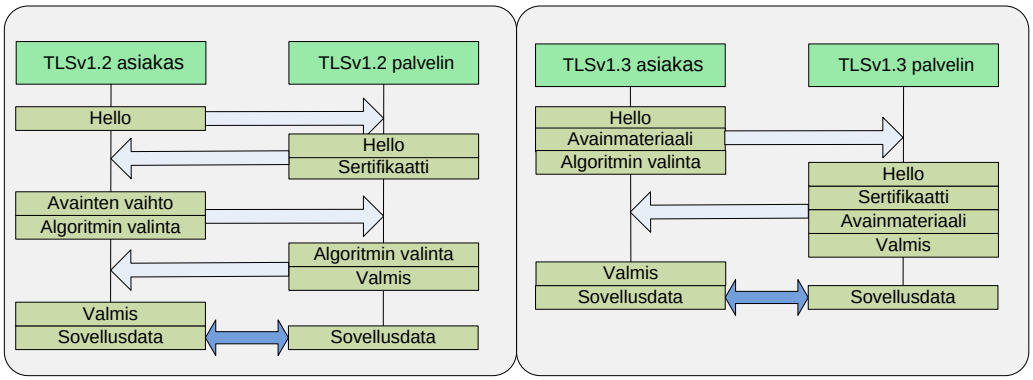
Transmission Layer Security (TLS) [27], aiemmin Secure Socket Layer (SSL), on salausprotokolla, jota käytetään yleisesti eri sovellusten Internet-tietoliikenteen päästä-päähän suojaamiseen. TLS on asiakas-palvelin malliin perustuva protokolla, joka määrittelee kättelykäytännöt laitteiden välisen sessioavaimen neuvotteluun ja käytettyjen salausmenetelmien sopimiseen. TLS standardi tukee suurta määrää vaihtoehtoisia algoritmeja avainten sopimiseen ja salaukseen (sekä lohko- että jonosalaimia) sekä eheyden turvaamiseen. Osa näistä on hyviä ja turvallisia ja osa taas huonoja eivätkä tarjoa enää riittävää suojaa.

WWW-palvelut ja selaimet ovat ehkä tyypillisimpiä TLS:ää käyttäviä sovelluksia. Menetelmät TLS:än hyödyntämiseksi HTTP-protokollan kanssa on määritelty HTTPS (HTTP over TLS) protokollassa [29]. HTTPS hyödyntää palvelinten tunnistuksessa julkisen avaimen infrastruktuuria. Järjestelmän heikkoutena on pidetty [30] sitä, että HTTPS:än soveltajat (selainten toimittajat) hyväksyvät suuren määrän luotettuja osapuolia (certification authority, CA), joiden myöntämien sertifikaattien perusteella palvelut tunnistetaan. Suurelle listalle voi mahtua epäluotettavia CA:ita minkä takia käyttäjä ei välttämättä tunnista joutuneensa hyökkäyssivustolle. Toteutuksissa on myös havaittu virheitä (esim. [31, 32]), jotka ovat mahdollistaneet hyökkäykset. Lisäksi jotkut luo-

tetutkin CA:t ovat joutuneet hyökkäysten kohteeksi ja näin hyökkääjät ovat päässeet käsiksi näiden avaimiin[2].

TLS-protokollaa käytetään myös yleisesti VPN-tunnelointiratkaisuna. TLS-VPN toimii sovellustasolle ja huolehtii täten yhteyden luotettavuudesta ja pakettien katoamisista aiheutuvat ongelmat (jota esim. IPsec-VPN:ät eivät tee). TLS:n käyttöä VPN:issä ei ole standardoitu, joten kaikki ratkaisut eivät välttämättä ole keskenään yhteensopivia.

TLS on yhteysorientoitunut menetelmä, joka on tarkoitettu erityisesti TCP-kommunikaatioprotokollan suojaamiseen ja joka sopii siten pitempien kommunikaatiosessioiden ja suurempien datamäärien siirtämiseen. TLS on kättelyineen ja virheenkorjausominaisuuksineen kuitenkin raskas. Nykyisin käytössä oleva TLS versio on 1.2. Versio 1.3 [28] on tällä hetkellä standardoinnin kohteena ja tulee muun muassa määrittelemään uusia algoritmeja ja poistamaan heikkoja. Uuden protokollan kättelyvaihe (jota havainnollistettu yksinkertaistetussa Kuva 5:ssä) on myös nopeutumassa ja yksinkertaistumassa, kun sovellusliikennettä voidaan lähettää heti, kun asiakaspuoli saa ja hyväksyy palvelimelta tulleen vastauksen alkuperäiseen pyyntöön.



Kuva 5. Tietoturvayhteyksien muodostaminen TLS v1.2:ssa ja v1.3:ssa [27] [28]

Reaaliaikaisiin kommunikointisovelluksiin (kuten videoneuvottelut), joissa palvelun laatu voi vaihdella, tai lyhyeen satunnaisesti tapahtumaan viestintään, joka on tyypillistä esim. ja esineiden internetissä (IoT), TLS on raskas. Yksittäisten pakettien suojaamiseen (erityisesti UDP-kommunikointiprotokollaa) varten on kehitetty Datagram Transmission Layer Security (DTLS) protokolla [33], joka hyödyntää TLS:än avainten-hallintamenetelmiä ja salausalgoritmeja mutta jossa sovellus joutuu itse huolehtimaan

[2] https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/

pakettien saapumisjärjestyksien, katoamisien ja koon vaihtelusta aiheutuvat ongelmat. DTLS soveltuu myös multicast-kommunikaatioarkkitehtuureihin. Pakettien häviämistä sietävien reaaliaikaisten videokommunikaatiosovelluksia varten taas on kehitetty SRTP (Secure Real Time Transport Protocol) [34].

3.2.2.2 PGP – Pretty Good Privacy

PGP (Pretty Good Privacy) on ensimmäisiä julkisesti saataville tulleita salausohjelmistoja. Sen kehitystyön aloitti vuonna 1991 Phil Zimmermann ja sen ympärille on rakennettu myös standardi (OpenPGP, RFC 4880). PGP:n avulla voidaan salata (ja allekirjoittaa) lähes mitä tahansa, joten sen sovelluskohteena ei ole pelkästään viestintä vaan myös tiedostojen jne. salaaminen. Kuitenkin yksi sen suurimpia käyttökohteita on perinteisesti ollut sähköpostiviestien allekirjoittaminen ja salaaminen.

Vaikka osa alkuperäisen PGP-standardin mahdollistamista salausmenetelmistä (esim. SHA-1 [35]) on todettu heikoiksi ja riittämättömiksi, PGP:tä on laajennettu viimeisen vuosikymmenen aikana niin, että siinä voidaan hyödyntää moderneja salausmenetelmiä, kuten elliptisten käyrien salausta. PGP:n suurin heikkous on käytettävyydessä. Huolimatta siitä, että julkisten avainten löytäminen on esimerkiksi keybase.io – palvelun kautta tullut huomattavasti helpommaksi, on PGP:n käyttäminen edelleen hankalaa ja virhealtista keskivertokäyttäjälle.

Yleisiä virheitä ovat julkisen ja yksityisen avaimen sekoittaminen ja yksityisen avaimen julkaiseminen, johon jopa suuret yritykset voivat sortua[3]. Lisäksi nykyisin kommunikoinnin siirtyessä saman käyttäjän laitteelta toiselle (pöytäkone, työpuhelin, oma puhelin), tapahtuu usein tilanteita, joissa avaamiseen tarvittava PGP-avain ei olekaan laitteella, jolla esimerkiksi sähköpostiviestiä avataan. Kiireellisissä kommunikaatiotilanteissa tämä aiheuttaa tilanteita, joissa viestintä päätetään lähettää salaamattomana ja näin ollen tietoturva vaarantuu.

PGP:ssä avainten hallinta onkin siirretty lähes kokonaan käyttäjille. Tämä on erittäin hajautettu rakenne, ns. luottamusverkosto (engl. Web of Trust), jossa käyttäjät allekirjoituksillaan vahvistavat toisten käyttäjien avaimia ja niihin liittyviä identiteettejä. Toisaalta tästä aiheutuu suuri kuormitus käyttäjille ja tämä johtaa usein myös aiemmin mainittuihin ongelmiin salauksen käytettävyyden kanssa. Lisäksi PGP-avainten pitkä käyttöikä ja vahva linkitys käyttäjän identiteettiin voi olla ongelmallista yksityisyyden suojan suhteen. Tiettyyn julkiseen avaimeen yhdistyvän salaisen avaimen hallussapito on voimakas todiste siitä, että haltija on myös kyseisen julkisen avaimen identiteetin (joka voi olla esim. sähköpostiosoite, nimimerkki) takana.

---

[3] https://arstechnica.com/information-technology/2017/09/in-spectacular-fail-adobe-security-team-posts-private-pgp-key-on-blog/

3.2.2.3 S/MIME – Secure/Multipurpose Internet Mail Extensions

S/MIME on RSA[4] Data Security -yrityksen kehittämä tapa salata sähköpostia ja siihen liittyviä liitetiedostoja. Nykyisin protokolla on IETF:n standardointiprosessissa, jota varten S/MIME:en liittyen on useita RFC -dokumentteja (3369, 3370, 3850 ja 3851). S/MIME:n avulla voidaan toteuttaa viestin salaus ja autentikointi. Lisäksi julkisen avaimen protokollien avulla voidaan toteuttaa myös lähetetyn viestin kiistämättömyys eli viestin lähettäjä ei voi myöhemmin kiistää lähettäneensä viestiä.

S/MIME:ä voidaan hyödyntää sähköpostiohjelmissa, mutta tämä vaatii avainpareihin liittyvien sertifikaattien käyttöä. Jotkut ohjelmistot eivät kykene näitä hyödyntämään. Lisäksi ongelmana on se, että avainten (tai niihin liittyvien salasanojen) kadotessa salattuja viestejä ei enää pysty avaamaan. Tämä ongelma on tosin lähes kaikissa salausta toteuttavissa järjestelmissä muodossa tai toisessa.

S/MIME:ssä avainten hallinta perustuu keskitettyyn julkisen avaimen ratkaisuun, joten samankaltaista työmäärää ei aiheudu käyttäjälle, kuin PGP:n tapauksessa. Toisaalta tämä tekee siitä melko jäykän ratkaisun eikä se juurikaan nauti suosiota suurten organisaatioiden ulkopuolella.

3.2.2.4 Signal (protokolla)

Signal on Open Whisper Systemsin kehittämä protokolla, joka toimii lähinnä pikaviestintään. Sen avulla voidaan salata tekstipohjainen viestintä, puhe- sekä videoyhteydet. Lisäksi protokolla tarjoaa mahdollisuuden salattuihin ryhmäviesteihin. Signal-protokolla ei kuitenkaan suojaa viestinnän metadataa. Metadatalla tarkoitetaan viestin välittämiseen ja viestisovelluksen käyttämiseen liittyvää tietoa eli sitä, kenelle viestitään, mihin aikaan, missä paikassa ja vaikkapa lähetetyn datan määrää. Tämän datan hyödyntäminen on mahdollista eri sovelluksissa ja sitä käytetään mm. mainosten kohdentamiseen ja muuhun käyttäjän profilointiin.

Signal on nykyisin erittäin suosittu protokolla, johon liittyy myös samanniminen pikaviestinsovellus. Itse protokollaa hyödynnetään kuitenkin laajemmin kuin vain kyseisessä sovelluksessa. Esimerkiksi Whatsappin salaus perustuu Signal-protokollaan. Protokolla itsessään on avoin ja sillä pyritään takaamaan hyvin vahva turvallisuus viestinnässä. Protokolla on myös auditoitu vuonna 2016 ja tulokset olivat hyvin lupaavia [36]. Protokollasta ei löytynyt mitään erityisiä tietoturva-aukkoja. Toisaalta protokollaa on päivitetty tuon auditoinnin jälkeen, joten siltä osin tuo vuoden 2016 auditointi ei kata kaikkea. Kuitenkin Signal on tällä hetkellä *de facto* standardi, jota käytetään

[4] RSA lyhenne tulee samannimisen salausmenetelmän keksijöiden sukunimistä (Rivest, Shamir ja Adleman), jotka ovat myös yrityksen perustajia.

useissa sovelluksissa ja sen avoimuuden vuoksi sitä voidaan arvioida (ja arvioidaan) tarvittaessa jatkuvasti.

3.2.3 Viestinnän metadatan salaaminen

Viestinnän metadatan salaamisella (tai piilottamisella) pyritään siihen, että viestien sisällön lisäksi salataan mahdollisimman hyvin myös se, ketkä (tai mitkä laitteet) verkossa kommunikoivat keskenään, kuinka usein, mihin aikaan jne. Metadatan avulla voidaan tehdä hyvin vahvoja päätelmiä viestinnästä ja henkilöiden (tai laitteiden) ominaisuuksista, liikkumisesta, asuin- ja työpaikoista ja jopa viestinnän sisällöstä.

Pienissä verkoissa on periaatteessa mahdollista salata suurin osa metadatasta järjestämällä kommunikaatio niin, että viestejä lähetetään jatkuvasti tasaisin väliajoin, jokainen verkon solmu lähettää aina viestin kaikille muille ja nämä viestit ovat aina vakiokokoisia. Lisäksi jokaisen solmun tulisi olla aina yhteydessä verkkoon. Luonnollisesti koko internetin skaalalla tällainen järjestely ei ole mahdollista. Tällaisia verkkoja voisivat olla muutaman henkilön/laitteen muodostamat verkot, joissa viestintä tapahtuu vain näiden henkilöiden/laitteiden välillä.

Käytännössä internetissä verkkoliikennettä seuraamalla voidaan päätellä monia asioita viestinnästä, vaikka sisältö olisikin salattua. Viestinnän metadataa ei lähtökohtaisesti salata, sillä se sisältää tietoa siitä, mihin viestinnän tulee kulkea. Verkossa viestintä tapahtuu pakettien välityksellä. Nämä paketit kulkevat yleensä useiden eri laitteiden kautta lähettäjältä vastaanottajalle, jolloin jokaisen välittävän laitteen tulee tietää viestin määränpää, jotta paketit päätyvät oikeaan osoitteeseen. Lisäksi paketeissa on paljon tietoa siitä, mihin sovellukseen ko. viesti liittyy, sillä vastaanottajan järjestelmän tulee voida ohjata paketin tietosisältö oikean sovelluksen käyttöön (sähköposti, verkkoselain, pikaviestin jne.).

Useimmissa nykyisissä keskitetyissä pikaviestinsovelluksissa (esim. Whatsapp, Signal) suurin osa tästä metadatasta ei näy palvelun ulkopuolelle verkkoliikenteestä. Eli verkkoliikenteestä voidaan vain päätellä, että käyttäjä on tietyllä ajanhetkellä yhteydessä palveluntarjoajaan, mutta ei sitä, kenen kanssa tämän palvelun sisällä kommunikoidaan. Viestinnän osapuolet eivät siis paljastu verkkoliikenteestä ulkopuoliselle tarkkailijalle eikä myöskään viestintä, mikäli sisältö on salattu. Palveluntarjoaja luonnollisesti näkee tämän tiedon ja eri palveluntarjoajat säilyttävät ja hyödyntävät tätä hyvin eri tavoin. Esimerkiksi Signal ei tallenna tätä tietoa eikä hyödynnä sitä mainontaan, kun taas Whatsapp tallentaa ja hyödyntää tätä tietoa.

Edelleen viestinnän metadata on arvokasta myös sovelluksia tarjoavien yritysten kannalta. Usein nämä yritykset pystyvät näkemään viestinnästä käyttäjien välisen sosiaalisen verkoston (kuka on yhteydessä keneen ja kuinka paljon). Tämä itsessään on jo

melko arvokasta tietoa ja mikäli tähän on mahdollista lisätä tietoja käyttäjien mieltymyksistä jne. voidaan tätä hyödyntää mainonnassa. Tällainen mahdollisuus on silloin, kun viestimessä käytetty käyttäjätunnus on helposti kytkettävissä muiden palveluiden käyttäjätunnuksiin. Esimerkiksi pysyvä sähköpostiosoite tai puhelinnumero ovat hyviä tunnisteita. Tällöin viestien sisällön ollessa salaamatonta profilointi on vielä helpompaa ja tarkempaa, mutta ”pelkän” metadatan avullakin voidaan saada paljon tietoa käyttäjistä.

Yksi merkittävä yksityiskohta on myös se, että monilla yrityksillä on käytössään profiileja myös sellaisista henkilöistä, jotka *eivät käytä itse* ko. palvelua. Lisäksi käyttäjien profiileihin voidaan lisätä myös sellaista dataa, jota käyttäjä itse ei ole palvelun käyttöön antanut. Tämä data saadaan usein muilta palvelun käyttäjiltä ja heidän laitteistaan sosiaalisen verkoston kautta. [5]

3.2.3.1 Sekoitusverkot

Sekoitusverkko (engl. mix network) on järjestelmä, jossa verkon kommunikaatiota pyritään sekoittamaan mahdollisen tarkkailijan varalta. Ensimmäisiä tutkimuksia sekoitusverkoista internetympäristössä on julkaistu jo 1980-luvulla [37] ja kehitystä on tapahtunut näihin päiviin saakka.

Tällä hetkellä tunnetuin ilmentymä sekoitusverkosta on The Onion Router (Tor) -verkko[6]. Tor-verkossa viestipaketit välitetään kryptografisesti salattujen otsikkotietojen avulla eri verkon pisteiden kautta lopulliseen määränpäähän. Näin peitetään suora yhteys kommunikoivien osapuolten laitteiden tai sovellusten välillä. Paketit matkaavat Tor-verkon sisällä ja poistuessaan verkosta lopulliseen määränpäähän vastaanottajalle näyttäytyy liikenne kuin se tulisi viimeisestä Tor-verkon solmusta eikä alkuperäisestä lähetysosoitteesta.

Tor-verkkoa voidaan käyttää siihen tarkoitukseen kehitetyllä verkkoselaimella (Tor Browser Bundle) tai viestisovelluksella, joka käyttää viestien välitykseen Tor-verkkoa. Lisäksi joissakin käyttöjärjestelmissä hyödynnetään oletusarvoisesti Tor-verkkoa (esim. Qubes OS, Tails) verkkoliikenteen reitittämisessä.

Tor-verkko ei kuitenkaan tarjoa täydellistä anonymiteettiä. Joissakin tapauksissa viestien alkuperä on voitu selvittää ja tätä tietoa on hyödynnetty mm. FBI:n toimesta. Spesifimpiin tarkoituksiin kehitettyjä sovelluksia ovat mm. Vuvuzela [38] ja Sphinx [39], joissa pyritään luomaan sovellustason sekoitusverkko viestien välittämiselle.

---

[5] Esimerkkinä Facebook https://www.digitaltrends.com/social-media/what-exactly-is-a-facebook-shadow-profile/
[6] https://www.torproject.org

Tor-verkon käyttäminen sekä joissain tapauksissa myös varsinaisten VPN-sovellusten (Virtual Private Network) on kielletty tai rajoitettu joissakin maissa. Ainakin Venäjän uusi laki[7] sekä Kiinassa esitetyt suunnitelmat[8] ovat tämän suuntaisia. Myös joissakin EU-maissa, kuten esimerkiksi Ranskassa[9], on esitetty vastaavia ajatuksia, mutta varsinaista kieltoa ei ole kirjattu lakiin asti. Myös Turkissa on ainakin ajoittain rajoitettu Tor-verkon käyttöä[10].

Toinen Tor-verkkoa vastaava anonymisointityökalu on I2P (Invisible Internet Project)[11], joka on saatavilla useimmille tunnetuille käyttöjärjestelmille. Protokolla pyrkii samoihin tavoitteisiin Tor-verkon kanssa, mutta toteutus on yksityiskohdiltaan erilainen eivätkä nämä kaksi menetelmää ole yhteensopivia (eli käyttäjän tulee valita, kumpaa anonymisointityökalua käyttää viestinnässään). Tätä protokollaa hyödyntäviä kommunikaatiosovelluksia on joitakin mm. sähköpostille ja erilaisille chat-sovelluksille. Myös tavallinen verkkoselain voidaan asettaa hyödyntämään I2P:tä. Jotkut lohkoketjuihin perustuvat ns. kryptovaluutat, kuten Monero, hyödyntävät I2P:tä anonymiteetin saavuttaakseen.

3.3 Viestintä ja salausmenetelmät

Salausmenetelmien markkinat ovat muuttuneet viime vuosina. Teknologisia ratkaisuja on saatavilla kuluttajille ja kuluttajien suosimat palvelut ovat kasvavissa määrin ottaneet käyttöön vahvoja salausmenetelmiä. Esimerkiksi EFF:n (Electronic Frontier Foundation) raportti vuoden 2017 alusta esittää, että jo puolet verkon liikenteestä on salattua[12]. Tässä esittelemme joitakin tuotteita ja palveluja, joiden avulla viestintäänsä voi salata. Viestintämenetelmien salaustasoon vaikuttavia ominaisuuksia on esitetty tarkemmin vertailumuodossa Taulukossa 2.

Yleisesti, viestintämenetelmien turvallisuuteen salausnäkökulmasta tarkasteltaessa vaikuttaa esimerkiksi sellaiset seikat, kuin miten ja minne viestit tallennetaan, (esimerkiksi paikallisesti vs. pilveen), ja missä vaiheessa (kuten viestien kuljetuksessa ja/tai viestien tallennuksessa) ja minkälaista salausta on käytetty.

---

[7] https://themoscowtimes.com/news/russian-law-banning-anonymous-online-surfing-comes-into-effect-59434
[8] https://www.extremetech.com/internet/252174-china-will-reportedly-ban-personal-vpns-close-great-firewall-loophole-february
[9] https://arstechnica.com/tech-policy/2015/12/france-looking-at-banning-tor-blocking-public-wi-fi/
[10] https://turkeyblocks.org/2016/12/18/tor-blocked-in-turkey-vpn-ban/
[11] https://geti2p.net/en/
[12] https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web

3.3.1 Pikaviestinsovellukset

Yksi suosituimpia tapoja viestiä tänä päivänä ovat erilaiset verkon yli käytettävät pikaviestinsovellukset. Näillä on tällä hetkellä miljardeja käyttäjiä ja niitä käytetään niin yksityiseen kuin yhteisölliseen viestintään. Laaja yleistason katsaus eri viestisovelluksiin ja salausmenetelmiin on tehty viime vuonna [40]. Tässä raportissa listaamme yleisimmät keskittyen sellaisiin, jotka ovat tällä hetkellä vielä aktiivisessa käytössä kuluttajapuolella tai joita kehitetään edelleen. Lisäksi käymme läpi niiden eroja. Erinomaiset listaukset pikaviestinsovelluksista[13], niiden protokollista[14] ja niiden eroista löytyy myös Wikipediasta.

IRC (Internet Relay Chat) on Jarkko Oikarisen vuonna 1988 kehittämä viestisovellus ja -protokolla, joka määriteltiin virallisemmin ensimmäisen kerran 1993 RFC 1459 -dokumentissa [41]. IRCissä keskustelut on mahdollista käydä erilaisilla kanavilla, joissa useat käyttäjät voivat osallistua keskusteluun yhtäaikaisesti. Myös yksityisviestien lähettäminen on mahdollista käyttäjien välillä.

Lähtökohtaisesti IRCissä ei ole salausta eikä viestinnän alkuperän ja muuttumattomuuden varmennusta. IRCiä on kuitenkin mahdollista käyttää TLS:n yli, jolloin salaus ja autentikaatio voidaan toteuttaa TLS:n keinoin.

Snapchat on pikaviestijärjestelmä kuvien ja videopätkien lähettämistä varten. Aiemmin viestit olivat kertakäyttöisiä, eli kun vastaanottaja avasi viestin, se näkyi käyttäjälle lyhyen aikaa ja sen jälkeen tuhoutui palvelimelta. Nykyisin viestien pysyvyyttä pystyy säätelemään. Kuitenkin avaamaton viesti tallentuu 30 päiväksi Snapchatin palvelimelle. Snapchat ei takaa päästä-päähän salausta. Viestit lähetetään salattuna, mutta esimerkiksi tekstimuotoiset viestit eivät ole salattuja.

Facebook Messenger ja Googlen Allo-sovellukset ovat ohjelmia pikaviestintään. Kumpikin käyttää päästä-päähän salausta, mutta ei oletuksena. Käyttäjän tulee siis itse asettaa salaus päälle sovelluksesta ennen viestien lähettämistä.

Slack on vuonna 2013 perustettu pilvipalvelupohjainen viestintäjärjestelmä yhteisökäyttöön. Siinä on ominaisuuksia sekä julkiselle että yksityiselle keskustelulle ja integrointimahdollisuus useiden muiden sovellusten kanssa, mahdollistaen kustomoidun palvelun omalle yhteisölle. Slack ei käytä päästä-päähän salausta, mutta lähettää ja tallentaa viestit salattuna.

[13] http://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients
[14] https://en.wikipedia.org/wiki/Comparison_of_instant_messaging_protocols

Skype on monipuolinen ja erittäin yleinen viestintäalusta. Se on paitsi ääni- tai videoyhteyttä käyttäva konferenssijärjestelmä, myös pikaviestijärjestelmä. Skype on rakenteeltaan peer-to-peer järjestelmä joka käyttää 256-bittistä AES:sta salaamaan viestiliikennettä kahden Skype-clientin välillä, tai TLS:ää Skype-clientin ja Skypen pilvipalvelimen välillä.

Ricochet on pikaviestinjärjestelmä joka käyttää Tor-verkkoa viestintään. Se luo salatun palvelun, mihin viestinnän osapuolet voivat osallistua ja mihin lähettää viestejään. Tällä estetään se, että jommankumman IP-osoite tai sijainti paljastuisi.

Tor Messenger on pikaviestinmentelmä, joka käyttää luonnollisesti myös Tor-verkkoa salattuun viestintään.

Briar on pikaviestinpalvelu, joka ei käytä myöskään keskitettyä palvelinta viestien välittämiseen, vaan viestit kulkevat lähettäjältä vastaanottajalle suoraan Tor-verkon kautta. Jos ja kun internet-yhteys katkeaa, yhteys synkronoituu joko Bluetoothin tai Wi-fin kautta uudelleen. Tällä turvataan viestinnän katkeamattomuus.

iMessage on Applen IPhone-puhelimien keskinäinen viestintämenetelmä. Se käyttää päästä-päähän salausta. Uusin käyttöjärjestelmäversio iOS11 mahdollistaa, että keskenään synkronoidut omat laitteet muodostavat keskenään avainpareja eikä edes Applella ole mahdollisuutta aukaista viestejä iCloudista.

Muita vastaavia viestintäsovelluksia ovat esimerkiksi Silent Phone (salatut puhelut ja viestit), Telegram (salatut teksti-ja chatviestit) ja TextSecure (salatut puhelut ja tekstiviestit).

EFF on mitannut eri sovellusten turvallisuutta ja yksityisyyden suojaa. Heidän uusin mittauksensa on vielä työn alla, mutta vanha antaa kuvan siitä, mitä ominaisuuksia EFF:n mielestä tulisi mitata viestinnän turvallisuutta arvioitaessa[15]. Valitettavasti osa tuon tutkimuksen tiedoista on jo vanhentunut eikä tuota voi enää tällä hetkellä pitää luotettavana arviona eri sovellusten turvallisuudesta. Suosittelemme seuraamaan tuon tutkimuksen kehitystä ja lopputuloksia.

3.3.2 Internetpuhelusovellukset

Skypellä pystyy myös puhumaan Internetin yli. Skype on rakenteeltaan peer-to-peer järjestelmä joka käyttää 256-bittistä AES:sta salaamaan viestiliikennettä, mutta ei tarjoa päästä-päähän salausta. Salaus tapahtuu siis vain verkkotasolla.

[15] https://www.eff.org/node/82654

WhatsApp on sovellus pikaviestien ja puhelujen välittämiseen internetin yli. WhatsApp käyttää päästä päähän salaukseen Signal-protokollaa. Tällöin myös puhelinviestintä on salattua.

Avoimeen lähdekoodiin perustuva puhelu- ja pikaviestijärjestelmä Signal (viestisovellus on nimeltään Wire) käyttää ZRTP-protokollaa puhelujen muodostamiseen. Signal soveltuu sekä iOS:ille että Androidille.

Facetime on internetpuhelujärjestelmä Applen omille tuotteille. Puhelut ovat päästä päähän salattuja.

Facebookin Messengerillä voi myös soittaa salattuja puheluja internetin yli.

Viber on maailmalla suhteellisen suosittu järjestelmä sekä salattujen viestien että puhelujen välittämiseen internetin yli.

3.3.3 Sähköposti

Arkaluontoisimmat sähköpostit ja sähköpostien liitetiedostot pitäisi salata jollain menetelmällä, erityisesti yritysten on otettava huomioon tietosuoja (GDPR,General Data Protection Regulation)-asetuksen asettamat henkilötietojen liikutteluun kohdistuvat vaatimukset. Valitettavasti useimmat sähköpostiohjelmistot eivät oletuksena salaa sähköpostiliikennettä. Sähköpostin päästä-päähän salaukseen käytettäviä sovelluksia ovat esimerkiksi PGP -pluginit, sekä Preveil ja EezyKeyz. Eezykeyz perustuu AES ja RSA- salausteknologioihin, ja käyttää niin kutsuttua moniavainsalausteknologiaa. Niin Preveil- kuin EezyKeyz-sovellus soveltuu Android ja iOS-käyttöjärjestelmille sekä Outlookille. Myös erityinen puhelinmalli, ToughMobile on kehitetty turvalliseen tietojenkäsittelyyn.[16]

Selainpohjaisissa sähköpostiratkaisuissa (kuten esim. Gmail) salaus toteutetaan nykyisin verkkotasolla HTTPS-protokollan avulla. Eli viestintä on viestien verkossa liikkuessa salattua. Tällöin kuitenkin sähköpostipalveluntarjoaja, kuten esim. Google, pääsee halutessaan näkemään viestien sisällön palvelimillaan.

3.3.4 Puheluiden salaaminen

Puhelujen salaukseen käytettävät mekanismit ovat yleensä palveluntarjoajakohtaisia, koska isot toimijat, kuten Google, Skype ja Apple, mielellään sitouttavat asiakkaansa tällä tavalla omaan alustaansa. Niinpä yleiskäyttöisten puhelujen salausmekanismien

16 https://www.bittium.com/BittiumToughMobile#security

kehitys on jäänyt suhteellisen pieneksi. Puhelinsovelluksia, joilla voi käydä salattuja puheluja ovat esimerkiksi Signal- Whatsapp- ja Telegram, mutta ne vaativat vastaanottajalta samaa sovellusta. CryptoPhone[17] tarjoaa useita Android-pohjaisia puhelinmalleja viestinnän ja puhelujen salaamiseen. Se käyttää AES-256 ja Twofish-protokollia salaukseen.

3.3.5 VPN-sovellukset

Markkinoilla on useita erilaisia VPN-sovelluksia, sekä ilmaisia että maksullisia, avoimeen lähdekoodiin perustuvia että suljettuja. Näissä on kussakin omat hyvät ja huonot puolensa: yleensä maksamalla hiukan saa enemmän yksityisyyttä. Lähtökohtaisesti VPN-palveluntarjoajalla on erittäin hyvä näkyvyys käyttäjän verkkoliikenteeseen, sillä salaus toteutetaan usein verkkotasolla käyttäjän laitteesta VPN-palveluntarjoajan järjestelmään, jossa salaus voidaan purkaa ja viestintään liittyviä tietoja voidaan tallettaa palveluntarjoajan järjestelmään.

3.4 Yhteenveto ja johtopäätöksiä

Erilaisia laitteita ja sovelluksia kommunikointiin tulee jatkuvasti lisää. Näiden turvallisuus- ja salausominaisuuksien seuraaminen on tärkeää. Menetelmien ja sovellusten turvallisuuden ajanmukainen arviointi on olennainen osa myös laajemmin kyberturvallisuuden varmistamista yhteiskunnan kaikilla tasoilla.

1. **On hyvä pitää osaamista ja teknologiaan liittyvää kehitystä myös Suomessa.** Salausmenetelmistä ja viestinnän salaukseen liittyvistä tuotteista voi tulla hyvinkin kriittisiä huoltovarmuuden ja kansalaisyhteiskunnan toimivuuden kannalta. Tällä hetkellä suuri osa erilaisista viestintäpalveluista ja niihin liittyvistä salausmenetelmistä kehitetään ja toteutetaan Suomen ulkopuolella. Suomalaisia ratkaisuja voidaan hyvin hyödyntää myös globaalisti ja toisaalta maailmalla olevien ratkaisujen arvioiminen vaatii myös kansallista osaamista.
2. **Globaalin kehityksen seuraaminen.** Esimerkiksi EFF:n raportista on tulossa uusi versio ja lisäksi myös monet muut julkiset ja yksityiset tahot julkaisevat erilaisia raportteja salausmenetelmiin liittyen. Näistä esimerkkinä ENISA:n raportti [42] sekä Viron tietoturvaviranomaisten julkaisema raportti [43]. Näiden ja vastaavien raporttien kautta salausmenetelmien ja viestinnän salaussovellusten kehityksen seuraaminen ja annettujen suositusten arvioiminen sekä toteuttaminen on suositeltavaa.

17 http://www.cryptophone.de/

3. **Ohjeiden ja arviointien julkaiseminen.** Julkisen tahon tekemien arviointien julkaiseminen sekä näiden arviointien pohjalta tehtävien ohjeistusten tekeminen on yksi mahdollinen tapa edistää salaustuotteiden markkinoita.

4 Salausmenetelmien purkaminen

Lähtökohtaisesti salausmenetelmien purkaminen voi perustua tekniseen kyvykkyyteen (tai salausmenetelmän heikkouteen) tai lainsäädännön asettamiin vaatimuksiin. Lainsäädännön asettamat vaatimukset ovat yleensä selviä siinä mielessä, että ne on kirjattu lakiin. Tekniset mahdollisuudet voivat olla yleisesti tunnettuja tai vielä tuntemattomia (esimerkiksi tuntemattomat haavoittuvuudet sovelluksissa ja protokollissa).

4.1 Lainsäädännön mahdollisuudet

Perustuslain 10 § 2 momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Salausmenetelmien purkamista on lakisääteisesti rajoitettu. 1.1.2015 voimaan tullut tietoyhteiskuntakaari (7.11.2014/917) korvasi aikaisemman lain eräiden suojauksen purkujärjestelmien kieltämisestä (30.11.2001/1117). Salausmenetelmien purkamista käsittelee erityisesti tietoyhteiskuntakaaren 32 luku.

Tietoyhteiskuntakaaren 269 § 4 momentin mukaan Viestintävirastolla on oikeus suojauksen purkujärjestelmien yhteensopivuuden varmistamiseksi antaa määräyksiä niiden teknisistä ominaisuuksista.

Tietoyhteiskuntakaaren (7.11.2014/917) 32 luku käsittelee suojausta ja suojauksenpurkujärjestelmiä. Sen 269§ 2 momentin mukaan “Sellaisen suojauksen purkujärjestelmän tai sen osan oikeudeton hallussapito, käyttö, valmistaminen, maahantuonti, kaupanpito, vuokraus, levittäminen, myynninedistäminen, asentaminen ja huolto on kielletty, jonka ensisijaisena käyttötarkoituksena on teknisen suojauksen oikeudeton purku ja mahdollistaa pääsy suojattuun televisiolähetykseen, radiolähetykseen tai vastaanottajan henkilökohtaisesta pyynnöstä toimitettavaan etäpalveluun.”Lisäksi rikoslain 38 luvun 8 b §:ssä määritellään suojauksen purkujärjestelmärikos.

Salauksen purkamista on oikeuskäytännössä käsitelty mm. CSS:n (Content Scrambling System -DVD-elokuvissa käytetty yksinkertainen ja algoritmisesti epäonnistunut

salaus) osalta Helsingin hovioikeudessa (22.05.2008/1427), jolloin rikosnimikkeenä oli teknisen toimenpiteen loukkausrikkomus. Hovioikeuden tulkinnan mukaan myös CSS oli lain tarkoittama tehokas toimenpide. Vastaajat jätettiin rangaistukseen tuomitsematta, mutta oikeudenkäyntikulut jäivät vastaajien vahingoksi. Sekä tekoaikaan että asiaa käsiteltäessä voimassa oli vielä sähköisen viestinnän tietosuojalaki (16.6.2004/516).

Parhaillaan Suomessa valmistellaan tiedustelua koskevaa lainsäädäntöä. Hallituksen esitystä ei vielä ole annettu eduskunnalle. Työryhmien mietinnöt niin siviilitiedustelusta (8/2017) kuin sotilastiedustelusta ovat kuitenkin valmistuneet. [44] [45] Mietinnöissä on kartoitettu myös muiden maiden tiedustelua koskevaa lainsäädäntöä.

Kansainvälisesti eri maiden lainsäädännöissä ei yleensä juurikaan oteta kantaa, voiko tiedustelussa saatua salattua viestiä purkaa. Toisaalta se on lähinnä akateeminen kysymys, koska tehokasta salausta ei käytännöllisesti katsoen pysty purkamaan. Jos mahdollisuus purkaa viestejä haluttaisiin taata, voitaisiin tietysti edellyttää vain heikkojen salausjärjestelmien tai vaihtoehtoisesti viranomaiskäyttöön tarkoitettujen takaporttien lisäämistä.

Maailmalla tämä on hiljattain noussut esiin esimerkiksi Yhdysvaltain varaoikeusministeri Rod Rosensteinin esittämänä ns. "Responsible encryption" -ratkaisuna[18], jossa tosiasiallisesti tehokasta ja toimivaa salausta ei sallita käyttäjille. Sen kantava ajatus on, että salaus olisi tehokasta ja turvallista, mutta viranomaisilla olisi aina hallussaan viestin purkamiseen tarvittavat avaimet. Electronic Frontier Foundation on laatinut hyvän vastineen[19] Rosensteinin ajatelmille, mutta tiivistetysti merkittävimmät teknologiset ongelmat ovat:

1. tällainen keskitetty järjestelmä ei estä rikollisia käyttämästä erilllisiä päästä-päähän salaavia viestintäjärjestelmiä, jolloin viranomaisten pääsy ei toteudukaan
2. salausavainten keskittäminen tuottaa merkittävän turvallisuusriskin kaikkien järjestelmää käyttävien viestinnän tietoturvalle

Ranskassa tehokkaat salausmenetelmät olivat aikaisemmin (ennen vuotta 2004) kiellettyjä, kunnes LCEN[20] ne rajoitetusti salli käyttöön. Paraikaa Ranskassa kuitenkin

[18] Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy, Annapolis, MD, 10.10.2017, https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval

[19] Kurt Opsahl, Deputy Attorney General Rosenstein's "Responsible Encryption" Demand is Bad and He Should Feel Bad – Legal Analysis, EFF 10.10.2017, https://www.eff.org/deeplinks/2017/10/deputy-attorney-general-rosensteins-responsible-encryption-demand-bad-and-he

[20] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164

valmistellaan taas lakia, joka velvoittaisi operaattorit purkamaan omat salauksensa.[21] Takaporttien[22] vaatimusta on valmisteltu monissa maissa (mm. Saksassa[23]) vaikka siitäkin on todettu, että se todennäköisesti aiheuttaa enemmän vahinkoa kuin hyödyttää. [46]

Kaavailtuun suomalaiseen tiedustelulakiin ei olla lisäämässä yrityksille velvoitetta asentaa palveluihinsa takaportteja tai luovuttaa viranomaisille salausavaimia. Myös puolustusministeriön mietinnössä todetaan, että Suomen kansainvälisen kilpailukyvyn sekä Suomen houkuttelevuuteen investointikohteena voisi vaikuttaa, jos ICT-alan yritykset velvoitettaisiin heikentämään tuotteidensa tai palveluidensa luuotettavuutta vaatimalla salausavaimia luovuttamista, takaporttien lisäämistä tai muuten salaustuotteita rajoittamalla.

Ehdotuksessa sotilastiedustelulaiksi (so. mietintö) sen 88 §:ssä säädettäisiin mahdollisuudesta käyttää reserviläisiä (ei varusmiehiä) näiden ollessa asevelvollisuuslain mukaisessa palveluksessa. Perusteluosassa mainitaan tuon pykälän 1 momentin sisältävän myös salauksen purun.

4.2 Tekniset mahdollisuudet eli miten salausmenetelmät murtuvat?

Riskien ymmärtämiseksi on hyvä aluksi tehdä katsaus siihen, millä eri tavoilla salausmenetelmät voivat murtua. Kaikki heikkoudet ja murrot eivät ole yhtä vakavia. Lisäksi eri käyttäjäryhmissä ja käyttötarkoituksissa löydettyjen heikkouksien vakavuus voi vaihdella.

4.2.1 Raaka laskentateho

Yksinkertaisin tapa murtaa salaus on käydä läpi kaikki vaihtoehdot mahdollisille avaimille. Koska äärimmäisen suurella todennäköisyydellä vain oikea avain tuottaa ”järkevän” tuloksen, kun salaus puretaan, voidaan oikea avain tunnistaa tulkitsemalla purettu viesti. Tämän vuoksi salausmenetelmissä vaaditaan, että eri avainvaihtoehtoja on enemmän kuin mitä nykyisillä tietokoneilla voidaan mielekkäästi kokeilla sopivassa ajassa. Yleisesti ottaen tämä tarkoittaa vähintään 128 bitin mittaisia avaimia symmetrisessä salauksessa ja vastaavan tietoturvatason avaimia julkisen avaimen järjestel-

[21] https://m.iltalehti.fi/digi/2016030821235296_du.shtml
[22] https://definitions.uslegal.com/b/backdoor/
[23] https://www.bleepingcomputer.com/news/government/germany-preparing-law-for-backdoors-in-any-type-of-modern-device/

missä. Yleensä julkisen avaimen järjestelmissä tarvitaan pidempiä (enemmän bittejä) avaimia kuin symmetrisissä järjestelmissä, jotta saavutetaan sama tietoturvan taso.

Jotkin vanhat salausmenetelmät, kuten esim. DES (Digital Encryption Standard), eivät tue näin pitkiä avaimia ja näin ollen ne voidaan murtaa nykyisin ilman mitään erityistä heikkoutta puhtaasti raa'an laskentatehon (engl. Brute force) avulla riittävän hyvällä laitteistolla. Laskentatehoon perustuu myös osaltaan vuonna 2015 havaittu FREAK-haavoittuvuus[24], jossa tietoisesti heikennettyihin, ns. vientikäyttöön (engl. export grade) tarkoitettuihin julkisen avaimen menetelmiin voitiin hyökätä suhteellisen tehokkaasti ja edullisesti käyttämällä nykyään helposti saatavilla olevaa laskentatehoa pilvestä. Aiemmin tällaisen laskentatehon ajateltiin olevan vain valtiotason toimijoiden saatavilla, mutta Mooren laki ja aika olivat tehneet tehtävänsä. Lisäpontta kyseiselle heikkoudelle antoi se, että viestintäprotokolla mahdollisti tällaiseen heikkoon salaukseen siirtymisen viestinnän ns. kättelyvaiheessa (engl. Handshake), jossa osapuolet selvittävät viestinnän parametrejä, kuten mm. salauksessa käytettävät algoritmit. Useissa tapauksissa oli mahdollista saavuttaa tämä heikompi salaus, mikäli palvelin tarjosi vain näitä heikkoja vaihtoehtoja käyttäjän järjestelmälle.

Yleisesti ottaen lähes kaikki salauksen murtamismenetelmät vaativat jonkin verran raakaa laskentatehoa. Hyökkäyksen tehokkuus riippuukin yleensä siitä, kuinka pieneksi tämän vaatimuksen kyseinen haavoittuvuus alentaa. Ja siitä, mitä reunaehtoja murtamismenetelmä asettaa. Monet menetelmät vaativat hyvin paljon muistia ja esikäsittelyä, mutta ovat tämän jälkeen nopeasti toteutettavissa. Toiset hyökkäykset saattavat vaatia jonkinlaista yhteyttä palvelimeen. Erilaisia reunaehtoja on monenlaisia ja murtamismenetelmän teho riippuu siitä, kuinka vaikea ne kaikki on toteuttaa yhtäaikaisesti. Murtamismenetelmän hyvyyttä voidaan tällöin arvioida sen suhteen, kuinka paljon etua raa'an laskentatehon menetelmään verrattuna saavutetaan.

4.2.2 Salauksen teoreettisen pohjan murtaminen

Ylimmällä tasolla voidaan ajatella salauksen teoriaa ja menetelmien teoreettista pohjaa. Tällä tasolla heikkouksien löytäminen on melko harvinaista ja tämän tason heikkoudet pyritään löytämään ennen kuin menetelmä otetaan laajempaan käyttöön. Tämän vuoksi salausmenetelmien teoreettisen pohjan tulisi olla mahdollisimman avointa, jotta asiantuntijat voivat arvioida menetelmää ja löytää teoriatason heikkoudet mahdollisimman varhaisessa vaiheessa.

Esimerkkinä edellisestä voidaan mainita vaikkapa alkuperäinen ns. *oppikirja Diffie-Hellman* -avaimenvaihto, jossa osapuolet käyttävät julkisen avaimen menetelmää

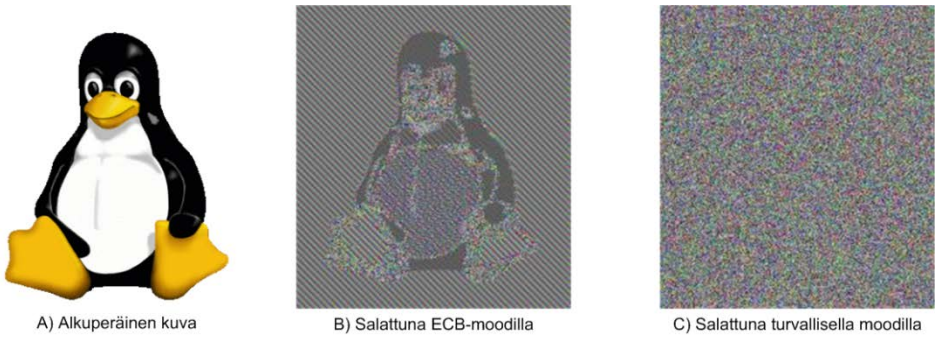
[24] https://censys.io/blog/freak

sopiakseen yhteisestä avaimesta. Tämä menetelmä ei sellaisenaan suojaa avaimenvaihtoa ns. *välimieshyökkäystä* vastaan. Välimieshyökkäyksessä hyökkääjä kuuntelee ja muokkaa alkuperäisten osapuolten viestintää niin, että hyökkääjä sopii eri avaimet kummankin osapuolen kanssa ja osapuolten viestiessä toisilleen purkaa ja uudelleen salaa viestit. Hyökkääjä pystyy näin siis lukemaan osapuolten välisen viestinnän. Oppikirja Diffie-Hellman -menetelmässä osapuolet eivät varmistu millään tavoin siitä, että heidän välissään ei ole ketään muokkaamassa avaimenvaihtoa. Tämän vuoksi nykyisin Diffie-Hellman -menetelmää on muokattu niin, että osapuolet varmistavat (autentikoivat) toistensa identiteetin ennen kuin hyväksyvät sovitun avaimen.

Osa erilaisten menetelmien teoriaan liittyvistä heikkouksista ei aiheuta käytännön tasolla ongelmia salauksen suhteen. Tästä esimerkkinä on AES, jolle tunnetaan teoreettinen ”heikkous”, jonka avulla hyvin erityisessä tapauksessa hyökkääjä voi saada jonkin verran etua AESin murtamiseen ideaaliin tilanteeseen verrattuna. Hyökkäyksen vaatima alkutilanne on kuitenkin melko keinotekoinen ja hyökkääjän saama etu niin pieni, että tästä ei ole käytännössä mitään hyötyä hyökkääjälle eikä AESia ole koskaan murrettu missään käytännön sovelluksessa tätä heikkoutta hyödyntäen.

Toinen esimerkki tällaisesta teoreettisesta heikkoudesta on lohkosalaajissa mahdollinen ECB (Electronic CodeBook) -moodi, joka ei tarjoa nykyisin riittäväksi katsottavaa suojaa edes teoriassa. Tätä moodia voidaan kuitenkin edelleen käyttää, mikäli sovelluksen toteuttajilla ei ole käsitystä salauksen tietoturvan teoriasta ja siitä, mikä tekee tietyistä moodeista turvallisia ja mikä ei. Esimerkki tästä löytyy Kuvasta 6[25], jossa sama kuva on salattu kahdella eri lohkosalausmoodilla, joista toinen on ECB ja toinen turvallinen. Teoriassa ECB:tä voitaisiin käyttää tilanteissa, joissa tarvitsee salata *vain yksi lohko* (yleensä 256 -1024 bittiä) dataa yhdellä avaimella. Tällaisia tilanteita tulee vastaan nykyisin erittäin harvoin.

[25] Kuvien alkuperät: A) Larry Ewing (https://en.wikipedia.org/wiki/File:Tux.jpg), B) & C) Dr Juzam (https://en.wikipedia.org/wiki/File:Tux_ecb.jpg & https://en.wikipedia.org/wiki/File:Tux_secure.jpg)



Kuva 6 Kuvan salaaminen kahdella eri lohkosalauksen moodilla

Yleisesti ottaen teoreettisen hyökkäyksen uhka on usein hyvin pieni ja vaikka sen vaikutus onkin hyvin suuri, ovat muut tavat murtaa salaus huomattavasti yleisempiä. Käytännössä siis salaus murtuu jollain muulla, kuin teorian tasolla. Vaikutus on kuitenkin sama, eli haluttu tavoite viestinnän tietoturvan suhteen jää saavuttamatta.

4.2.3 Väärä uhkamalli

Salaus voi murtua myös väärän uhkamallin valinnan vuoksi. Tällöin turvallista ja hyvää menetelmää käytetään oikein, mutta järjestelmää vastaan kohdistuu uhka, jolta salausmenetelmä ei suojaa. On hyvä huomata, että eri käyttäjillä ja käyttäjäryhmillä voi olla hyvin poikkeavat uhkamallit, joten yksi ratkaisu ei välttämättä sovi kaikille.

Esimerkkinä voidaan ajatella vaikkapa viestinnän eheyttä ja digitaalista allekirjoitusta. Digitaalisella allekirjoituksella viestinnän eheys voidaan varmistaa erinomaisen hyvin ja tarkoitukseen sopivia menetelmiä ja sovelluksia on saatavilla useita. Digitaalisella allekirjoituksella voidaan myös varmistua viestin kiistämättömyydestä. Eli allekirjoittaja ei voi kiistää jälkikäteen allekirjoitustaan.

On kuitenkin tilanteita, joissa halutaan varmistua viestinnän eheydestä, mutta mahdollistaa viestinnän kiistettävyys. Esimerkkinä voi olla vaikkapa viestintäsovellus, jossa halutaan, että viestejä ei voida jälkikäteen käyttää viestijöitä vastaan, mutta on tärkeää, että viestit säilyvät muuttumattomina viestinnän aikana. Tällöin digitaalisten allekirjoitusten käyttäminen aiheuttaa ongelmia, koska ne ovat kiistämättömiä. Ja tällaisessa tapauksessa sorrutaan väärän uhkamallin käyttämiseen.

Monet salausmenetelmät perustuvat luotettuun osapuoleen, joka toimittaa tunnistetiedot ja avaimet kommunikoiville tahoille. Internet-selaimet luottavat suureen sertifiointiauktoriteettien joukkoon ja matkapuhelin verkoissa tunnistaminen perustuu USIM-kortteihin, jotka tulevat älykorttien valmistajilta puhelin operaattorien välityksellä. Nä-

mä luotetut tahot voivat kuitenkin pettää, joko tahallaan tai huolimattomuuttaan. Esimerkiksi vuonna 2015 uutisoitiin [47] kunka salaisia avaimia oli vuotanut yhdeltä USIM-valmistajalta tiedustelupalveluille.

4.2.4 Väärä käyttötarkoitus

Yksi merkittävä virhelähde on turvallisen salausmenetelmän käyttäminen väärään tarkoitukseen. Käytetään siis vaikkapa menetelmää, joka takaa luottamuksellisuuden (esim. perinteinen salaus) tilanteessa, jossa halutaan suojata viestinnän eheys tai toisin päin. Tämän kaltaisessa tapauksessa virheen paljastuttua ei yleensä ole mitään takeita siitä, saadaanko haluttu viestinnän tietoturvatavoite toteutettua vai ei.

Esimerkkinä väärästä käyttötarkoituksesta ja sen aiheuttamista ongelmista voidaan mainita vaikkapa vuoden 2013 Adoben salasanamurto, jossa kymmenien miljoonien käyttäjien salasanat vuotivat Adoben järjestelmästä[26]. Tällaiset murrot eivät ole mitenkään poikkeuksellisia ja niitä on tapahtunut aiemmin ja myös Adoben tapauksen jälkeen. Tapauksesta tekee merkittävän se, että paljastuneet salasanat oli suojattu salausmenetelmällä, jota ei oltu suunniteltu tätä tarkoitusta varten.

Salasanat suojataan yleensä kryptografisen *hash-funktion* avulla ja salasanan lisäksi käytetään myös ns. *suolaa* eli lisättyä satunnaisuutta, jotta mahdollinen sama salasana ei johda samaan lopputulokseen. Hash-funktio soveltuu hyvin tähän tarkoitukseen, sillä se antaa aina vakiomittaisen vastauksen salasanan pituudesta riippumatta ja tämä vastaus on hyvin satunnainen ja vaihtuu merkittävästi vaikka salasana poikkeaisi toisesta vain vähän. Lisäksi hash-funktio on yksisuuntainen eli saadusta tuloksesta on vaikeaa päätellä alkuperäistä salasanaa. Tällä tavoin suojatuista salasanoista ei pysty päättelemään, mikä on salasanan pituus eikä sitä, mitkä salasanat ovat lähellä toisiaan.

Adobe käytti tietokannassaan salasanojen suojaamiseen lohkosalaajaa sekä lisäksi sellaista käyttömoodia, joka tuottaa aina samalla avaimella salatusta tiedosta täsmälleen saman salakirjoituksen (jo aiemmin esitelty ECB-moodi). Koska kyseinen salausmenetelmä paljastaa aina myös salatun viestin pituuden, Adoben tietokannassa olleista salatuista salasanoista voitiin päätellä niiden pituus ja se, mitkä salasanat ovat samoja tai sisältävät samoja osia. Tämän lisäksi käyttäjien itse määrittämät vihjeet (salasanan unohtuessa) olivat salaamattomina samassa tietokannassa. Salasanojen arvaamisesta tuli siis lähinnä ristisanatehtävää vastaava ongelma[27].

[26] https://www.geekwire.com/2013/report-adobe-breach-hit-150-million-usernames-passwords/
[27] Verkosta löytyy sivusto, joka käyttää tietokantaa ristisanatehtävien muodostamiseen: https://zed0.co.uk/crossword/

4.2.5 Implementaatiovirhe

Salausmenetelmät toteutetaan samaan tapaan elektroniikkaa ja ohjelmointia hyödyntäen kuin muutkin digitaaliset laitteet ja ohjelmistot. Näin ollen salaussovelluksista löytyy myös implementaatiovirheitä eli ns. bugeja. Nämä virheet voivat johtaa siihen, että salauksella tavoiteltu turvallisuus menetetään.

Kaikki salaussovelluksissa olevat virheet eivät aiheuta tietoturvan vaarantumista. Lisäksi virheitä on hyvin eritasoisia. Yksittäinen virhe voi koskettaa yksittäistä sovellusta ja sen tiettyä versiota, jolloin tältä ongelmalta voi välttyä käyttämällä jotain toista versiota ja/tai toista sovellusta. Tällaisen virheen aiheuttama riski riippuu siitä, kuinka laajalle ko. sovellus on levinnyt.

Nykyisin ohjelmistoja rakennetaan hyvin usein erilaisten ohjelmointikirjastojen avulla. Yksittäinen kirjasto saattaa esiintyä useissa kymmenissä eri ohjelmistoissa, joten tällaisessa kirjastossa esiintyvällä virheellä on usein laajempi vaikutus kuin yksittäisen ohjelman virheellä. Edelleen ei ole aina varmuutta, että kaikki kirjastoa hyödyntävät ohjelmistot ja niiden kehittäjät saavat tietoa tästä virheestä, jotta pystyisivät päivittämään oman ohjelmistonsa.

Salausmenetelmiin liittyvä keskeinen kirjasto on OpenSSL[28]. Jo kyseisen kirjaston verkkosivuilta voidaan huomata, että viimeisin ilmoitus löydetystä virheestä on 2.11.2017. Kyseessä ei ole vakava virhe, mutta OpenSSL:stä on vuosien saatossa löydetty useita hyvin vakavia virheitä. Esimerkiksi kuluvana vuonna on löytynyt virhe, joka voi mahdollistaa salaisten RSA-avainten saamisen haltuun[29]. Toinen hyvin tunnettu haavoittuvuus on Heartbleed [31, 32], joka antoi hyökkääjille pääsyn OpenSSL:ää käyttävien HTTPS palvelimien suojatulla muistialueella oleviin avaimiin ja tietoihin. Kun heikkous havaittiin vuonna 2014, jopa yli puolet suosituimmista Internet-palveluista oli sille alttiina [48].

Edelleen salausmenetelmät viestinnässä toimivat erilaisten kommunikaatioprotokollien yli. Salausmenetelmät voivat murtua myös näissä kommunikaatioprotokollissa ja niiden toteutuksissa ilmenevien virheiden kautta. Hyvä esimerkki tästä on Wi-Fi-yhteyksissä käytetty salausprotokolla WPA2 ja siihen liittyvä virhe, jonka avulla voidaan tämä salaus murtaa[30]. Protokollatason virheet ovat hyvin ongelmallisia, sillä protokollat ovat usein standardoituja ja täten käytössä hyvin monessa laitteessa ja ohjelmistossa. Tämän tyyppisen virheen laajuus on usein erittäin suuri.

---

[28] https://www.openssl.org (luettu 4.12.2017)
[29] https://nvd.nist.gov/vuln/detail/CVE-2017-5681 (luettu 4.12.2017)
[30] https://www.krackattacks.com

Kaikkiin implementaatiovirheisiin liittyy olennaisesti päivittäminen ja päivitysten saatavuus. Eri ohjelmistot ja laitteet päivittyvät eri tavoin eikä usein ole mitään varmuutta siitä, onko tietty virhe päivittynyt kaikkialla. Tämä yhdistettynä siihen, että monet virheet vaikuttavat useisiin eri ohjelmistoihin ja että erilaisia ohjelmistoja salaukseenkin liittyen on saatavilla melko paljon, tekee vaikeaksi hahmottaa tiettyyn ohjelmistoon liittyvät riskit tai tiettyyn tavoitteeseen parhaiten sopivan ratkaisun löytämisen.

4.2.6 Satunnaisuuden puuttuminen

Kaikki salausmenetelmät tarvitsevat satunnaisuutta, jotta ne olisivat turvallisia. Tätä satunnaisuutta hyödynnetään yleensä avaimien luomisessa. Nykyaikaisissa tietokoneissa satunnaisuuden keräämisestä huolehtii usein laitteen käyttöjärjestelmä. Käyttöjärjestelmä tarjoaa sitten eri sovelluksille mahdollisuuden hyödyntää tätä satunnaisuutta esimerkiksi salausmenetelmiä käytettäessä.

Mikäli satunnaisuus on jostain syystä puutteellista eli liian arvattavaa, voi luoduissa avaimissa esiintyä säännönmukaisuuksia, jotka vaarantavat niitä hyödyntävien salausmenetelmien turvallisuuden. Esimerkkinä tästä on ongelmat RSA-salauksen avaimien luomisessa [49]. Lisäksi tällaiset ongelmat ovat johtaneet hyvin ongelmallisiin tilanteisiin mm. Viron sähköisten henkilökorttien kanssa[31].

4.2.7 Sivukanavat

Sivukanavalla tarkoitetaan salausmenetelmien yhteydessä epäsuoraa tapaa saada tietoa järjestelmästä. Sivukanavan avulla voidaan joissakin tapauksissa murtaa salausmenetelmiä. Yleisimmät sivukanavat liittyvät salausmenetelmissä tapahtuvan laskennan ajoituksiin sekä järjestelmän (yleensä mikrosirun) tuottaman lämmön tai sähkömagneettisen säteilyn mittaamiseen. Kuitenkin erilaisia sivukanavia on monenlaisia ja ne voivat liittyä esimerkiksi virheiden käsittelyyn.

Verkkoliikenteeseen liittyvänä esimerkkinä sivukanavasta voidaan käyttää ns. padding oracle[32] -hyökkäystä, jossa hyödynnetään salausmenetelmään kuuluvaa täydennysdatan (engl. padding) lisäystä sekä salauksen ja eheyden varmistamisen aiheuttamia erilaisia virhetiloja ja ilmoituksia. Hyökkäyksen avulla voidaan PKCS#5 -tyyppisesti täydennetty, tietyllä lohkosalausmoodilla salattu viesti purkaa lähettämällä hienovaraisesti muokattuja versioita viestistä kohteeseen (yleensä palvelinkone), joka vastaa onko viesti validi vai epävalidi. Toistamalla tätä menetelmää riittävän monta kertaa koko viestin sisältö voidaan purkaa (muutama tavu kerrallaan) ilman, että viestin sa-

[31] https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/
[32] http://blogs.microsoft.co.il/linqed/2010/09/19/padding-oracle-aspnet-vulnerability-explanation/

laamiseen käytettyä avainta tiedetään. Tosin hyökkäys ei paljasta käytettyä avainta, joten se pitää toistaa uusien viestien osalta samanlaisena. Nykyisissä järjestelmissä ja toteutuksissa juuri tämä hyökkäys on otettu huomioon, mutta erilaisia muunnelmia ja niistä johtuvia ongelmia on ollut myös viime aikoina ja esimerkiksi OpenSSL:stä on löytynyt padding oracle -tyyppinen heikkous vielä vuonna 2015[33] ja edelleen TLS:stä on löytynyt vastaavanlainen haavoittuvuus vielä aivan äskettäin[34].

Lisäksi sivukanavina voidaan pitää myös virheiden tahallista injektointia järjestelmään. Tämän tyyppiset hyökkäykset vaativat usein enemmän aikaa kuin monet muut ja lisäksi myös mahdollisesti fyysistä pääsyä järjestelmään. Verkkoliikenteen tapauksessa tämän kaltaiset skenaariot ovat usein hyvin epätodennäköisiä, mutta esimerkiksi älykorttien tapauksessa hyvinkin realistisia. Edelleen riippuen hyökkääjän tarkoitusperistä ja salauksen käyttötarkoituksesta näinkin aggressiiviset hyökkäykset ja murtomenetelmät voivat tulla kyseeseen.

4.2.8 Käyttäjän virhe

Viimeisenä, mutta ei suinkaan vähäisimpänä, salaus voidaan murtaa käyttäjän virheen toimesta. Tässä raportissa emme pureudu tähän ongelmaan, sillä tällaisia virheitä on mahdotonta käydä kattavasti läpi ja lisäksi nämä ongelmat eivät yleensä liity itse salausteknologiaan. Tästä huolimatta voidaan todeta, että eri sovellukset ovat hyvin eri tasolla käytettävyyden suhteen ja huono käytettävyys johtaa usein käyttäjän virheisiin tai sellaisiin tietoisiin käyttömalleihin, jotka vaarantavat salauksen toimivuuden.

Lähtökohtaisesti teorian tasolla salausmenetelmät pyritään suunnittelemaan turvallisiksi myös huolimattomien tai jopa pahantahtoisten käyttäjien suhteen. Käytännössä toteutukset mahdollistavat salauksen murtumisen käyttäjän virheen toimesta lähes aina. Lisäksi käyttäjä voi toimia salaussovelluksen ulkopuolella sillä tavoin, että salausmenetelmä tai -sovellus ei voi tähän vaikuttaa. Tästä on esimerkkinä luottamuksellisten tietojen kopioiminen ja säilyttäminen salaamattomana vaikka paperisina tai USB-tikulla ja näiden hukkaaminen tai väärin hävittäminen[35].

[33] https://www.openssl.org/news/secadv/20160503.txt
[34] https://robotattack.org (13.12.2017)
[35] Yksi viimeaikainen esimerkki: https://arstechnica.com/information-technology/2017/10/man-finds-usb-stick-with-heathrow-security-plans-queens-travel-details/

5 Salauspalveluihin liittyvät riskit

Salauspalveluihin liittyvät riskit voidaan jaotella karkeasti saatavuuteen, eheyteen ja luottamuksellisuuteen liittyviin riskeihin. Kartoituksessamme tarkastelemme yleisimpiin menetelmiin ja sovelluksiin liittyviä riskejä. Arvioimme myös riskien vaikuttavuutta.

5.1 Yleisen tason riskit

Yleisellä tasolla viestinnän salausmenetelmien riskit kohdistuvat saatavuuteen ja kiistämättömyyteen sekä mahdollisesti lakeihin.

5.1.1 Salaus ja saatavuus

Salauksella ei perinteisesti pyritä saavuttamaan mitään etua viestinnän saatavuuden suhteen. Luonnollisesti voidaan toki ajatella, että ilman riittävää salausta koko viestintä voidaan jättää toteuttamatta, koska riskit viestinnän muiden tavoitteiden osalta kasvavat liian suuriksi. Esimerkiksi arkaluontoisen tiedon saattaminen verkon yli vastaanottajalle saattaa vaatia riittävän turvallista salausmenetelmää, jotta tieto voidaan siirtää.

Saatavuuteen liittyvät riskit salauksen suhteen syntyvät kuitenkin yleensä siitä, että salattua tietoa ei kyetä enää avaamaan vastaanottajan toimesta. Tällainen tilanne syntyy usein niin, että salaamiseen käytetty avain on kadotettu eikä sitä voida enää palauttaa. Salausavain on voitu suojata salasanalla, joka on unohtunut tai se on talletettu esim. muistitikulle, joka on kadonnut eikä avaimesta ole muita kopioita. Esimerkiksi nykyisin erittäin suosittu kryptovaluutta Bitcoin [50] on tunnettu siitä, että Bitcoin-osoitteeseen liittyvän salaisen avaimen kadottaminen johtaa kyseisessä osoitteessa olevien Bitcoinien pysyvään menettämiseen.

Saatavuuteen liittyvien riskien ymmärtämiseksi tulee ymmärtää käytetyn salausmenetelmän ja erityisesti sovelluksen *avaintenhallintamekanismi* eli se, miten salaamisessa käytetyt avaimet luodaan, jaetaan, varmennetaan, talletetaan ja tarvittaessa hävitetään. Erilaiset ratkaisut tuovat myös erilaisia uusia riskejä muita tavoitteita kohtaan.

Esimerkiksi avainten säilytys luotettavan kolmannen osapuolen toimesta (engl. Key escrow) on tapa mahdollistaa kadonneiden avainten palauttaminen ottamalla yhteyttä tähän kolmanteen osapuoleen. Tällöin kuitenkin tämän osapuolen tulee nauttia kaikkien kommunikoivien osapuolten luottamusta ja tällaisesta tahosta tulee myös erittäin houkutteleva kohde erilaisten hakkereiden ja tiedustelupalveluiden näkökulmasta.

Osaltaan saatavuuteen liittyvä riski on viranomaisten pääsy salattuun viestintään. Kuten eri tahojen toimesta on esitetty, viranomaisilla on tarpeita päästä tutkimaan salatun viestinnän sisältöä. Nykyiset salausmenetelmät eivät kuitenkaan tue tämän tapaisia järjestelyjä silloin, kun kyse on päästä päähän salatusta viestinnästä. Kuitenkin viestinnän sisältöön voidaan päästä käsiksi muita reittejä kuin verkkoviestinnän salaus murtamalla (tai sitä heikentämällä). Viestintä on selväkielisenä viestivien osapuolten päätelaitteilla. Lisäksi useat viestisovellukset mahdollistavat viestinnän tallentamisen palveluntarjoajan pilvipalveluun, jossa viestintä ei enää välttämättä ole salattuna ja josta se voidaan oikeuden päätöksellä luovuttaa viranomaisille.

5.1.2 Salaus ja kiistämättömyys

Toinen yleisen tason riski salaukseen liittyen on kiistämättömyys. Kiistämättömyys ei ole yksiselitteisesti hyvä tai huono ominaisuus viestinnässä. On paljon käyttötapauksia, joissa kiistämättömyyttä ei missään nimessä voida sallia, kuten esimerkiksi digitaaliset allekirjoitukset vaikkapa pankkiasioiden yhteydessä. Yhtä lailla on myös tapauksia, joissa kiistämättömyys on perusteltu ominaisuus, joka järjestelmän tulee toteuttaa. Esimerkiksi anonyymi viestintäsovellus, jossa mahdollisesti kaapattuja tai muuten selvitettyjä viestejä ja niiden sisältöä ei voida osoittaa pitävästi tietyn viestintään osallistuneen osapuolen lähettämiksi.

Salauksen avulla voidaan toteuttaa molempia tavoitteita. Kuten aiemmin mainittu, julkisen avaimen järjestelmällä toteutetut allekirjoitukset eivät ole kiistettävissä, mikäli yksityinen avain voidaan yhdistää tiettyyn henkilöön. Usein esimerkiksi PGP-avaimet ovat vahvasti yhdistettävissä tiettyihin sähköpostiosoitteisiin, jotka edelleen voivat olla esim. työ- tai opiskelupaikkaan sidoksissa ja näin vahvasti henkilökohtaisia. Tällaisella avaimella tehty allekirjoitus on hyvin vaikea henkilön kiistää jälkeenpäin.

Toisin päin salaus voidaan rakentaa kiistettäväksi. Yksinkertaisimmillaan tämä toteutuu tavallisessa symmetrisessä salauksessa. Koska molemmilla (tai kaikilla) osapuolilla on sama avain, ei voida pitävästi osoittaa, kuka on tietyn viestin lähettänyt pelkän salausavaimen avulla. Luonnollisesti muita tietolähteitä hyväksikäyttäen selvittäminen voi olla mahdollista. Luvussa 3.2.3 on esitelty muutamia menetelmiä, jotka pyrkivät häivyttämään myös tämän mahdollisuuden.

5.1.3 Salaus ja lainsäädäntö

Salattua viestintää voidaan myös pitää lain näkökulmasta ongelmallisena silloin, kun viestinnän sisällöllä voisi olla merkitystä esimerkiksi rikosasian tms. käsittelyssä. Mikäli salauksessa käytettyjä avaimia ei saada käyttöön, on usein vaikea tai jopa mahdotonta saada viestinnän sisältöä selville. Joissakin tapauksissa viestinnän sisältö voidaan selvittää viestintäpalveluntarjoajan avulla esimerkiksi siinä tapauksessa, että muuten salatusta viestinnästä on tehty varmuuskopioita (salaamattomina) palveluntarjoajan järjestelmään.

Lainsäädännöllä voidaan koettaa velvoittaa epäiltyjä avaamaan viestien tai muun datan salaus, mutta tämä ei ole mitenkään ongelmatonta. Esimerkiksi Isossa-Britanniassa voidaan tuomita vankeuteen jopa viideksi vuodeksi, mikäli epäilty ei paljasta salasanaansa (tai muuta avainta) salattuihin tietoihin pääsemiseksi[36]. On kuitenkin menetelmiä, joissa viestit poistuvat järjestelmästä tietyn ajan jälkeen eikä niitä enää voida välttämättä palauttaa edes salasanan avulla. Edelleen salasanat voivat unohtua tai salaukseen käytetty avain voi kadota (esim. USB-tikun mukana) ja tällöin epäilty ei voi toteuttaa tuota vaatimusta avainten paljastamisesta.

5.2 Yksityiskohtaisempi riskikartoitus

Tarkemmassa riskikartoituksessa katsotaan erityisesti tiettyjen sovellusten ja protokollien riskejä salauksen ja viestinnän näkökulmasta. Lisäksi esitetään lyhyesti yleisempien riskien osalta mahdollisia hallintakeinoja.

Vuonna 2015 Unger *et al.* [51] tekivät kattavan kartoituksen kuluttajille suunnatuista turvallisista viestisovelluksista. He tunnistivat kolme korkean tason tavoitetta turvalliselle viestinnälle. Ensimmäinen on *luottamuksen muodostaminen*, jolla tarkoitetaan sitä, miten käyttäjät voivat varmistua siitä, että kommunikaatio tapahtuu vain ja ainoastaan sovittujen osapuolten välillä. Toinen ominaisuus on *keskustelujen turvallisuus*. Tämä pitää sisällään viestien ja viesteihin liittyvän informaation salaamisen ja varmentamisen sekä näihin liittyvät kryptografiset menetelmät sekä tarvittavat avainten vaihdot. Kolmas ominaisuus on *viestinnän yksityisyyden suoja*, jolla tarkoitetaan niitä menetelmiä, joilla viestit välitetään osapuolten välillä ja näihin menetelmiin liittyviä, viestinnän metadataa suojaavia mekanismeja.

Jokaisessa tavoitteessa on turvallisuuteen, käytettävyyteen ja käyttöönottoon liittyviä ominaisuuksia, joita arvioidaan. Lisäksi jokaiselle tavoitteelle on määritelty ns. perus-

[36] http://www.itpro.co.uk/126891/encryption-law-could-mean-jail-time

taso, joka on saavutettavissa ilman käyttäjälle näkyviä toimenpiteitä. Muita menetelmiä verrataan tähän perustasoon. Vaikka kehitystä on jonkin verran tapahtunut tuon tutkimuksen julkaisun jälkeen, voidaan edelleen todeta, että täydellistä ratkaisua mihinkään kolmeen ongelmaan ei ole vielä kehitetty. Perustason ratkaisut tarjoavat vain heikon turvallisuuden tai yksityisyyden tason, vaikkakin usein parhaan tai lähes parhaan käytettävyyden. Useat muut menetelmät eivät tarjoa yhtä hyvää käytettävyyttä eivätkä mitkään yksittäiset menetelmät tarjoa kaikkia turvallisuus- ja yksityisyysetuja.

Alla esitetään löydöksiä eri salausmenetelmien ja -sovellusten ominaisuuksista ja riskeistä. Laajempi ja tarkempi esitys eri pikaviestinsovellusten turvallisuusominaisuuksista löytyy Wikipediasta[37].

Taulukko 2: Suosituimpien viestinsovellusten salausominaisuuksia

Sovellus	Salaus oletuksena	Avoin lähdekoodi	Hajautettu palvelinrakenne	Kerättävä data	Yhteyden varmennus	Forward secrecy	Salaus ryhmäkeskustelulissa	Salaus tiedostonjaossa	Asynkroninen	Viestien salaus laitteessa
Briar	Kyllä	Sovellus	Kyllä	Ei tallenna	Kyllä	Kyllä	Kyllä	Ei	Ei	Kyllä
Facebook Messger	Ei	Sovellus osittain	Ei	Profiili ja kontaktit	Kyllä	Kyllä	Ei (vaikka ryhmäkeskustelut mahdollisia)	–	Kyllä	Kyllä
Google Allo	Ei	Sovellus osittain	Ei	–	Ei tietoa	Kyllä	Optio	–	Kyllä	–
iMessage	Ei (optio)	Ei	Ei	–	Ei	Ei	Optio	Kyllä	Kyllä	–
Signal	Kyllä	Sovellus & palvelin	Ei	Vain profiilidata (salattu sovelluksessa)	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Skype	Vain palvelimelle	Ei	–	–	Ei	Ei	Sama kuin oletuksena	Sama kuin oletuksena	Ei	Ei
Sähköposti	Ei (optio)	Riippuu sovelluksesta	Ei	Riippuu sovelluksesta	Ei	Ei	Optio	Optio	Kyllä	Riippuu sovelluksesta
Telegram	Ei	Sovellus	Ei	Profiili ja kontaktit, ei metadataa	Kyllä	Kyllä, mutta hidas	Ei (vaikka ryhmäkeskustelut mahdollisia)	Kyllä	Ei	Optio
Whatsapp	Kyllä	Sovellus osittain	Ei	Profiili, metadata ja kontaktit	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Ei

[37] https://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients#Secure_messengers

Taulukko 2 sisältää suosituimpien viestinsovellusten ominaisuuksia. Taulukosta voidaan nähdä, onko päästä päähän salaus käytössä oletuksena ja onko sovelluksen ja palvelintoteutuksen lähdekoodi avointa. Kerättävä data on jaettu kolmeen kategoriaan: *profiilidata*, joka on käytännössä vain käyttäjän antama käyttäjänimi sekä mahdollinen kuva; *metadata*, joka tarkoittaa viestinnän metadataa sekä *kontaktit*, joka tarkoittaa sovelluksessa ja mahdollisesti laitteessa (esim. puhelin) olevien yhteystietojen keräämistä.

Jotkut sovellukset mainostavat myös mahdollisuutta ”estää” kuvankaappauksia sekä sovelluksesta automaattisesti poistuvia viestejä. Nämä menetelmät eivät kuitenkaan tarjoa suojaa kuin käytännössä vahingossa tapahtuvia kuvankaappauksia ja viestien poistamatta jättämisiä vastaan. Haluttaessa näitä rajoituksia voidaan kiertää esim. ottamalla kameralla kuva puhelimen näytöstä tai kopioimalla viestin teksti toiseen sovellukseen ennen viestien poistumista.

Kuten taulukosta voidaan huomata, sähköpostille ei ole oikeastaan yhtä yhteistä sovellusta, jota voidaan arvioida. Eri sovellukset toimivat hyvin eri lailla ja salaus on usein vain verkkotasolla ja päästä päähän sovellustason salaus vaatii erityisiä ohjelmistoja. Tällaisia ovat mm. Preveil[38] sekä suomalainen EezyKeyz[39]. Myös F-Secure tarjoaa lisäosaa Outlook-ohjelmistoon. Lisäosan avulla viestin voi lähettää salattuna. Lisäksi myös PGP ja S/MIME -tyyppiset ratkaisut ovat mahdollisia. Monet selainpohjaiset sovellukset tarjoavat verkkotason salauksen HTTPS:n kautta.

Huomionarvoista on myös, että esimerkiksi nuorten suosima Snapchat-sovellus ei tarjoa tietoa siitä, käyttääkö se salausta viestinnässä, vaikka muuten tuo esille mm. automaattisesti häviävät viestit.

[38] https://www.preveil.com
[39] https://eezykeyz.eu

Taulukko 3: Viestintään liittyviä riskejä ja niiden hallintakeinoja

Riski	Esiintymistapa	Luottamuksellisuus	Eheys	Saatavuus	Verkkotason hallintakeinot	Sovellustason hallintakeinot
Viestintälaitteen katoaminen	Varkaudet, unohtamiset jne.	Vaarantuu	Mahdollisesti vaarantuu	Vaarantuu	Ei sovellu	Viestien salaaminen päätelaitteessa. Viestien varmuuskopiointi (salattuna).
Viestinnän luvaton lukeminen	Verkkovalvonnalle altistuminen, suojaamattomien yhteyksien käyttäminen	Vaarantuu	Vaarantuu	Ei yleensä	Suojatut verkkoyhteydet (Wi-Fi ja matkapuhelinverkot), molemminpuolinen tunnistautuminen verkon ja päätelaitteen välillä	Päästä päähän salatut viestiyhteydet, viestinnän osapuolten identiteetin varmistaminen
Viestien muuttaminen	Välimieshyökkäys, erilaiset haittaohjelmat	Vaarantuu	Vaarantuu	Ei yleensä	Suojatut ja autentikoidut verkkoyhteydet (Wi-Fi ja matkapuhelinverkot), molemminpuolinen tunnistautuminen verkon ja päätelaitteen välillä	Päästä päähän salatut ja autentikoidut yhteydet,
Yksityisyyden suoja metadatalle	Metadataa keräävät sovellukset, verkkovalvonta	Mahdollisesti vaarantuu	Ei yleensä	Ei yleensä	Sekoitusverkkojen ja VPN-yhteyksien hyödyntäminen	Anonyymit viestipalvelut sekä mahdollisesti sekoitusverkkoja hyödyntävät sovellukset
Verkkosensuuri	Yhteyksien estäminen joko kohdennetusti tai laajamittaisesti	Ei yleensä	Mahdollisesti	Vaarantuu	Sekoitusverkkojen ja VPN-yhteyksien hyödyntäminen	Anonyymit viestipalvelut sekä mahdollisesti sekoitusverkkoja hyödyntävät sovellukset. Julkisten kanavien hyödyntäminen salattuna.
Salauksen käyttämättömyys	Salausta ei ole tarjolla järjestelmässä tai sen käyttäminen ei onnistu	Vaarantuu	Vaarantuu	Vaarantuu	Mahdollisimman automaattiset ohjelmalliset ratkaisut esim. selaimen lisäosat[40]	Käyttäjäystävälliset viestintäsovellukset, joissa salaus oletusarvoisesti päällä

[40] Mm. HTTPS everywhere https://www.eff.org/https-everywhere mahdollistaa hyvin automaattisen salauksen käyttöönoton verkkoselailussa.

Taulukkojen 2 ja 3 avulla voi löytää muutamia sovelluksia ja muita menetelmiä, joilla viestintään liittyviä riskejä voi hallita ja koettaa poistaa. Kuitenkaan esimerkiksi taulukon 2 tilanne ei ole staattinen sillä sovelluksista voi löytyä uusia haavoittuvuuksia ja niitä päivitetään jatkuvasti sekä näitä haavoittuvuuksia vastaan että uusia ominaisuuksia varten.

5.3 Yhteenveto ja johtopäätöksiä

Salausmenetelmien käyttöön viestinnässä liittyy riskien lisäksi hyvin oleellisesti uhka-arviot. Koska erilaisissa viestintätilanteissa ja eri käyttäjillä ja käyttäjäryhmillä on hyvin erilaiset tarpeet ja vaatimukset salaukselle, ei yksittäistä, kaikenkattavaa ratkaisua ole mahdollista esittää. Valittujen menetelmien tulee perustua rationaaliseen uhka-analyysiin. Luonnollisesti tavallinen käyttäjä ei välttämättä kykene aina tekemään hyviä ratkaisuja. Hyvillä ohjeistuksilla voidaan kuitenkin auttaa käyttäjiä tekemään turvallisia valintoja viestinnässään.

1. **Yksittäistä ja yksiselitteisesti parasta ratkaisua ei ole.** Eri viestintäsovellusten salausmenetelmät lähtevät erilaisista lähtökohdista ja tavoitteista. Näin ollen käytetyn sovelluksen tulee perustua käyttäjän omaan riskiprofiiliin ja -arvioon ja näihin parhaiten sopivan menetelmän ja sovelluksen valintaan.
2. **Kehitystä on seurattava ja mahdollisia ohjeita päivitettävä.** Yksittäisistä sovelluksista ja kokonaisista protokollista ja jopa salausmenetelmistä voi löytyä yllättäviä heikkouksia, jotka voivat vaarantaa halutut tavoitteet. Täten näiden sovellusten ja menetelmien jatkuva seuraaminen ja niihin liittyvien ohjeiden ja johtopäätösten päivittäminen on tärkeää.
3. **Suomalaisille käyttäjille suunnatut ohjeet.** Suomalaisille tavallisille viestinnän käyttäjille suunnatut ohjeet olisivat hyvin tärkeät. Ohjeita voi myös jakaa hieman erilaisille riskiryhmille. Tällaisia ratkaisuja löytyy verkosta jo muutamia[41] ja näiden mallien pohjalta voidaan rakentaa myös suomalaiset ohjeet.
4. **Aina kun mahdollista käytä päästä päähän salattua ja viestinnän eheyden varmistavaa menetelmää.** Nykyään päästä päähän salatun viestinnän varmistavia viestisovelluksia on useita ja niiden käytettävyys on hyvällä tasolla. Tämänkaltaisen viestimen käyttö alkaakin olla jo ns. peruskyberhygieniaa. Lisäksi on hyvä varmistua viestien muuttumattomuudesta matkalla lähettäjältä vastaanottajalle. Viestien muuttumattomuus kannattaa varmistaa myös salaamattoman viestinnän yhteydessä.

[41] https://www.wired.com/2017/12/digital-security-guide/ sekä https://securityplanner.org/#/

5. **Varmista avainten oikeellisuus.** Useat sovellukset tarjoavat mahdollisuuden varmistaa avainten oikeellisuus. Tätä mahdollisuutta on hyvä käyttää ja varmistaa avainten oikeellisuus ennen viestinnän aloittamista.
6. **TLS-protokollaa verkkotason liikenteen suojaamiseen käytettäessä RSA-salausta tulisi välttää.** Sekä historialliset että viimeaikaiset löydökset osoittavat, että TLS:n RSA-salauksesta löytyy herkemmin heikkouksia kuin muista julkisen avaimen menetelmistä, joita TLS:ssä voidaan käyttää. Näin ollen on parempi ottaa käyttöön näitä muita menetelmiä aina kun se vain on mahdollista. Myös muissa yhteyksissä RSA-salauksen käyttämisen turvallisuutta tulee arvioida.

6 Tulevaisuuden näkymiä

Viimeisten vuosikymmenten aikana salaustuotteiden markkinat ja käyttötarkoitukset ovat muuttuneet valtavasti. Aiemmin lähinnä valtiotason toimijoille saatavilla olevat salausmenetelmät ovat nyt osana jokaisen tietoverkkoa käyttävän ihmisen arkea. On myös käynyt selväksi, että näitä menetelmiä on hyödyllistä käyttää, sillä viestinnän sisällön selvittäminen verkossa on huomattavan helppoa, mikäli salausta ei käytetä. Lisäksi viestejä voidaan helposti muokata, mikäli viestinnän eheydestä ei huolehdita oikein.

Miten eri palvelut kehittyvät tulevaisuudessa ja mitä uusia salausmenetelmiä kehitetään ja tuodaan markkinoille? Tässä osiossa esittelemme muutamia tulevaisuuden teknologioita ja mahdollisia kehityssuuntia salausmenetelmiin liittyen.

6.1 Tulevaisuuden kommunikaatio- ja laskentateknologiat

6.1.1 5G, 6G ja niin edelleen

Viidennen sukupolven (5G) standardeja matkapuhelinverkoille kehitellään parhaillaan. Standardointityö on keskittynyt 5G:hen liittyvien tietoturvahaasteiden kartoitukseen [52] eikä salaukseen liittyviä uusia standardeja ole esitelty. Yksi tärkeä trendi 5G:ssä on mahdollistaa erilaisten radioverkkojen liittäminen yhteen runkoverkkoon. Tällöin myös avaintenhallinta voisi noudattaa 3GPP:n standardeja ja infrastruktuureja, kun taas salauksessa voitaisiin hyödyntää erilaisille radioverkoille optimoituja menetelmiä. 5G pyrkii myös tukemaan paremmin uusia sovelluksia ja laitteita. Esimerkiksi 5G pyrkii tarjoamaan yhteyksiä automatisoituville kulkuneuvoille (jotka tarvitsevat lyhyitä vasteaikoja), IoT-laitteille (joille energiatehokkuus on kriittistä) ja kriittiselle infrastruktuurille (jolle saatavuus on taattava). Tämä tarkoittaa tietoturvamenetelmien differointia ja kustomointia sovellus- tai asiakaskohtaisesti hyödyntämällä esimerkiksi verkon virtualisoinnin mahdollisuuksia.

5G tai 6G verkkojen tietoturvan kehityksessä pyritään myös vastaamaan tiedossa oleviin heikkouksiin nykyisissä verkoissa. Nykyiset verkot vuotavat esimerkiksi tietoa käyttäjien sijainneista, sillä päätelaitteiden tunnisteita (IMSI, GUTI) lähetetään radioverkossa salaamatta. Tähän on ehdotettu ratkaisuksi asymmetrisiä salausmenetelmiä [53]. Nykyisistä salausmenetelmistä puuttuvat myös perfect forward secrecy ja kvanttiresistiivisyys ominaisuudet.

6.1.2 Kvanttitietokoneet ja kvanttilaskenta

Kvanttitietokoneiden kehittäminen on tuonut uuden uhkan salausmenetelmiä vastaan. Riittävän edistyneet ja tehokkaat kvanttitietokoneet voivat murtaa lähes kaikki tällä hetkellä yleisimmin käytössä olevat julkisen avaimen salausmenetelmät [54]. Lisäksi kvanttitietokoneet jonkin verran heikentävät symmetristen algoritmien vahvuutta [55] ja näin pakottavat salausratkaisut esimerkiksi avainpituuksien kaksinkertaistamiseen. Arviot salausta murtavan kvanttitietokoneen valmistumisajasta vaihtelevat kymmenestä vuodesta [56] vuosikymmeniin tai siihen ettei sellaista koskaan valmistu. Kvanttitietokoneen mahdollistamaan salauksen murtamiseen on kuitenkin varauduttava ja salausmenetelmien on oltava kvanttitietokoneen kestäviä ennen sen valmistumista, sillä liikenne voidaan tallentaa ja murtaa myöhemmin. Yhdysvaltalaisen standardointijärjestelmän NISTin kilpailu [57] korvaavien julkisen avaimen menetelmien löytämiseksi on parhaillaan käynnissä. Lupaavia menetelmiä on olemassa, mutta menetelmien vahvuuden varmistaminen sekä klassisia että kvanttikoneeseen perustuvia kryptananalyysimenetelmiä vastaan vaatii vielä paljon työtä tietoturvayhteisöltä. Lisäksi menetelmien suorituskykyä ja energiatehokkuutta pyritään parantamaan.

6.1.3 Fyysisen kerroksen hyödyntäminen

Fyysisen kommunikointikerroksen ominaisuuksien käyttäminen salausmenetelmien vahvistamiseen ja korvaamiseen on myös aktiivinen tutkimusalue. Radiokanava sisältää paljon satunnaisuutta muuttavassa ympäristössä olevien signaalinkulkuun vaikuttavien esteiden ja häiriölähteiden takia. Tätä satunnaisuutta pystytään käyttämään hyväksi kryptografisten avainten generoimisessa [58, 59, 60] ja kontrolloitaessa kenellä on pääsy fyysisen kerroksen signaaleihin [61, 62]. Lisäksi fyysisen kerroksen menetelmillä (esim. fingerprinting [63], distance bounding [64, 65]) voidaan todentaa laitteen maantieteellistä sijaintia.

6.2 Lainsäädännön ja markkinoiden kehitys

Tulevaisuudessa viestinnän salausmenetelmiin vaikuttavat myös sekä säädösilmapiirin että markkinoiden kehityskulut. Näiden yhteisvaikutusta on vaikea ennustaa, mutta muutamia kehityskulkuja voidaan arvioida ja niiden näkymiä esittää.

6.2.1 Säädösilmapiirin kahtiajakoisuus

Kuten jo luvussa 5.1.3 esitettiin, lainsäädäntö ja salausmenetelmät voivat muodostaa eräänlaisen riskitekijän. Tällä hetkellä lainsäätäjien ja päättäjien taholta tulevat viestit salaukseen ja yksityisyyden suojaan ovat osaltaan ristiriitaisia. Yhtäällä on EU:n yleinen tiesuoja-asetus ja vastaavat yksityisyyden suojaa korostavat säädökset, jotka osaltaan asettavat vaatimuksia myös viestinnän salausmenetelmiä kohtaan. Toisaalta useat eri tahot, mm. jotkut Ranskan ja Saksan ministerit, Yhdysvaltojen tiedusteluviranomaiset sekä EU:n oikeuskomissaari, ovat pyrkineet argumentoimaan tarvetta luoda salausmenetelmiä, jotka ovat vahvoja, mutta jotka voidaan tarvittaessa avata viranomaisten toimesta.

Vasta-argumenttina useat johtavat salausmenetelmien asiantuntijat julkaisivat lausunnon [66], jossa edellä mainitun kaltaisen salausmenetelmän luominen ja turvallinen käyttöönotto todetaan liian riskialttiiksi. Yksinkertaistaen voidaan sanoa, että tällainen järjestelmä ja sen mahdollistama pääsy käsiksi kaikkeen salaukseen olisi liian houkutteleva kohde hakkereille ja tiedustelupalveluille, jotta sen turvallisuus voitaisiin taata. Lisäksi on huomattava, että nykyiset salausmenetelmät ovat yleensä avoimiin ja julkisiin tuloksiin pohjautuvia, joten kuka tahansa voi niistä tehdä oman toteutuksen. Edelleen ilman täysin kattavaa ja aukotonta kansainvälistä säädöstä, salausmenetelmät voitaisiin toteuttaa siellä, missä lainsäädäntö ei niitä estä.

6.2.2 Viestinnän metadatan salaaminen

Toinen salausmenetelmien markkinoihin liittyvä kehityskulku on metadatan salaaminen. Tällä hetkellä sisällön salaaminen päästä päähän näyttää yleistyvän ainakin pikaviestimien osalta, kuten Taulukko 2 kertoo. On oletettavaa, että myös muun kommunikaation osalta sisällön salaaminen yleistyy ja myös verkkotasolla HTTPS ja muut salausta tukevat protokollat tulevat yleistymään.

Viestinnän metadatan salaaminen sovellus- ja verkkotasoilla on vielä huomattavan paljon harvinaisempaa. Siihen ei ole vielä monia sovelluksia (laajimmalle levinnyt lienee Tor), sovellusten käytettävyys ei ole vielä kovin hyvällä tasolla ja lisäksi monista sovelluksista löytyy heikkouksia, jotka mahdollistavat metadatan keräämisen ja käyttäjien yksityisyyden suojan murtamisen. Tällä saralla tutkimusta ja kehitystyötä

tarvitaan vielä huomattavan paljon. Myös erilaiset parantuneet analytiikkamenetelmät tekevät metadatan ja viestinnän yksityisyyden suojan suojaamisesta haastavaa.

6.2.3 IoT ja salaus

IoT -laitteiden tuleminen markkinoille muodostaa lisähaasteen salausmenetelmille. Haastetta aiheuttaa niin laitteiden pienet resurssit (ja tähän liittyvien salausmenetelmien kehitys ks. luku 6.3.2) kuin myös se, että monille käyttäjille ei enää ole selvää, mitkä laitteet kommunikoivat ja millä tavoin. Näin ollen myös mahdollinen viestinnän suojaaminen näiden laitteiden osalta saattaa jäädä vaillinaiseksi.

Yhtenä jo nyt esiintyvänä kehityssuuntana voidaan nähdä keskitettyjen turvallisuusratkaisuiden markkinat. Esimerkiksi F-Securen Sense -laitteen avulla voidaan turvata useita erillisiä IoT-laitteita. Myös EU:n seitsemännen puiteohjelman SECURED-projektissa[42] toteutettiin samantyylisiä ratkaisuja.

Tulevaisuudessa IoT-laitteiden viestinnän salausmenetelmiä tullaan kehittämään ja myös uudenlaisia ratkaisuja tullaan näkemään, sillä kehitys salaus- ja suojausmenetelmien saralla tapahtuu valitettavan usein vasta, kun nykyisin käytössä olevista havaitaan heikkouksia. Tässä on myös yksi mahdollisuus osoittaa edelläkävijyyttä ja kehittää salausmenetelmiä, jotka toimivat hyvin IoT-maailmassa.

6.3 Salausmenetelmien kehitys

Salausmenetelmät kehittyvät jatkuvasti ja varsinkin teoriaa viedään jatkuvasti eteenpäin monilla osa-alueilla. Yksi tämän hetken haasteista onkin tuoda näitä teoriatuloksia käytäntöön kehittämällä niistä riittävän tehokkaita ja toimivia sovelluksia ja hyödyntämällä niitä erilaisissa protokollissa.

6.3.1 Homomorfinen salaus

Homomorfisella salauksella (engl. Homomorphic encryption) tarkoitetaan salausta, jolla salatulle datalle voidaan suorittaa laskentaoperaatioita *purkamatta salausta*. Tällöin vaikkapa pilvipalveluntarjoajalle voidaan toimittaa esim. paikkatieto ja haluttu kysely (lähin ravintola) salattuina ja palveluntarjoaja voi laskea kyseiselle paikalle halutun tiedon saamatta tietoon sitä, mikä paikka oli kyseessä ja mitä kyselyssä etsittiin. Vaikka tämän tyyppinen salaus liittyy enemmän talletetun datan kuin viestintädatan

[42] https://www.secured-fp7.eu

suojaamiseen, on homomorfisella salauksella valtavasti mahdollisuuksia useilla eri sovellusalueilla.

Tällä hetkellä homomorfinen salaus on liian tehotonta, jotta sitä voitaisiin käyttää kaikkeen dataan ja kaikissa palveluissa. Kuitenkin ensimmäisiä sovelluksia aiheeseen liittyen on jo olemassa mm. biometrisessä tunnistautumisessa [67] [68].

6.3.2 Kevyet salausmenetelmät

Kevyillä salausmenetelmillä (engl. Lightweight encryption) tarkoitetaan yleensä menetelmiä, jotka ovat tehokkaita ja turvallisia myös laskuteholtaan hyvin rajallisissa laitteissa, kuten pienissä sensoreissa. Esineiden internetin myötä tulee paljon lisää laitteita, jotka kommunikoivat internetin yli. Tämän kommunikaation turvaaminen vaatii kehitystä kevyiden salausmenetelmien saralla.

Korkealla tasolla on nähtävissä kaksi tapaa mahdollistaa tehokkaat ja toimivat salausmenetelmät myös IoT-ympäristössä. Ensimmäinen on kehittää tapoja tehostaa nykyisiä salausmenetelmiä ja niiden toimivuutta. Yksi askel tähän suuntaan on esimerkiksi Intelin AES-salausta tukevat ns. natiivikäskyt (engl. Native instructions, AES-NI) prosessoreissa. Näiden avulla AES-salaus on huomattavan tehokasta toteuttaa näissä prosessoreissa. Tämän suuntaista kehitystä on mahdollista jatkaa ja näin tuoda vahva salaus myös IoT-maailmaan.

Toinen kehityssuunta on tuoda käyttöön aivan uusia, nimenomaisesti vähäresurssisille laitteille suunnattuja salausmenetelmiä. Tällaisia menetelmiä on kehitetty useita, mutta niiden käyttöönotto ei ole vielä kovinkaan laajamittaista. Kasvava tarve tämänkaltaisille ratkaisuille voi kuitenkin tuoda muutosta ja saada aikaan sekä uusia ratkaisuja että laajempaa käyttöä vanhoille ratkaisuille. Tällöin myös näiden menetelmien analysointi ja mahdollisten heikkouksien löytäminen muodostuu tärkeäksi tutkimusaiheeksi.

6.3.3 Kvanttilaskennan kestävät salausmenetelmät

Kuten jo kappaleessa 6.1.2 todetaan, kvanttilaskentaa varten tarvitaan uusia salausmenetelmiä. Tämän menetelmäkehityksen seuraaminen ja siihen tarvittaessa vaikuttaminen on tärkeä valmistauduttaessa tulevaan. Lisäksi on hyvä huomata, että tällä hetkellä ehdotetut kvanttilaskennan kestävät salausmenetelmät ovat usein vähemmän tehokkaita tai vaativat enemmän muistia ja/tai kommunikaatiokaistanleveyttä kuin aikaisemmat menetelmät. Näin ollen tämä kehitys kulkee ainakin tällä hetkellä vastakkaiseen suuntaan kuin kevyet salausmenetelmät.

On kuitenkin oletettavaa, että näitäkin menetelmiä voidaan kehittää tehokkaammiksi. Tulevaisuuden kehityksen kannalta onkin oleellista, kuinka lähelle nykyisiä menetelmiä nämä voidaan tuoda ja lisäksi kuinka paljon pienten laitteiden ja sensoreiden laskentateho kehittyy. Mikäli nämä kaksi kehityskulkua kohtaavat, voidaan kvanttilaskennan kestäviä menetelmiä tuoda myös pieniin laitteisiin. Edelleen täysin toinen kysymys on, missä määrin näitä tarvitaan IoT-laitteissa ja mikäli kehitys ei tuo riittävän tehokkaita menetelmiä ja laitteita, niin muodostuuko tästä suurta riskiä.

6.3.4 Salausmenetelmät ja verkkoliikenteen valvonta

Yksi merkittävä syy viestinnän salaamisen kysynnän kasvulle on ollut eri tahojen havahtuminen siihen, että verkkoviestintää on melko helppoa valvoa ja että tätä mahdollisuutta on hyödynnetty laajamittaisesti valtiotason toimijoiden toimesta. Lisäksi monet muut tahot voivat tarkkailla viestintää ja tehdä johtopäätöksiä sen sisällön ja metadatan perusteella. Tämän kehityksen vastavoimana voidaan nähdä mm. pikaviestimien sisällön salaaminen sekä yleisemmin verkkoliikenteen salaamiseen tähtäävät projektit, kuten Let's Encrypt[43].

Koska aihe on ajankohtainen nyt myös Suomessa, niin salausmenetelmien käyttäminen ja niiden tarjoaman suojan ymmärtäminen on tärkeää. Lisäksi myös globaalisti eri tahojen kiinnostus ja tarve päästä käsiksi verkkoliikenteestä saatavaan tietoon kasvaa. Salaaminen ei automaattisesti suojaa kaikkea viestintään liittyvää informaatiota, kuten esimerkiksi metadataa. Lisäksi on näyttöä siitä, että salatustakin liikenteestä voidaan tehdä yksityisyyttä rikkovia johtopäätöksiä, ainakin IoT-laitteiden tapauksessa [69]. Esimerkiksi unirytmiä valvovan laitteen liikenteen määrästä ja ajankohdasta voitiin päätellä, milloin henkilö käy nukkumaan, vaikka itse data oli salattua. Valvontakameran liikenteestä taas voitiin päätellä, milloin kamera havaitsi liikettä.

Tässä suhteessa on nähtävissä kehitystä, jossa salausmenetelmien avulla pyritään suojaamaan viestintää ja yksityisyyttä ja toisaalta erilaisten laitteiden ja sensorien sekä niiden tuottaman tiedon analysoinnin kautta yksilöistä ja viestinnästä voidaan tehdä tarkempia analyysejä salauksesta huolimatta. Tavoitteena on tietenkin, että ihmiset voivat valita keiden kanssa tietoa viestinnästään ja viestinnällään jakavat ja että salausmenetelmät mahdollistavat tämän varmistamisen. Myös siinä tapauksessa, että jokin taho aktiivisesti pyrkii saamaan luvatta tietoa käyttöönsä.

[43] https://letsencrypt.org

6.3.5 Salausmenetelmäosaamisen tarpeen kasvu

Koska salausmenetelmät tulevat lisääntyvissä määrin olemaan avainasemassa monissa digitalisaatiokehityksen vaiheissa, tulee näiden menetelmien ymmärtäminen ja soveltaminen olemaan tärkeää. Tämä tarkoittaa sitä, että salausmenetelmäosaamista tulee kehittää ja mahdollisesti laajentaa niin Suomessa kuin kansainvälisestikin. Ymmärrystä salausmenetelmien toiminnasta ja niiden rajoituksista tulisi löytyä tavallisilta kuluttajiltakin, jotta he voivat tehdä hyviä valintoja viestinnän suojaamiseksi. Lisäksi syvällisempää osaamista vaaditaan erilaisten laitteiden ja ohjelmistojen kehittäjiltä ja suunnittelijoilta, jotta näihin osataan valita oikeat menetelmät takaamaan riittävän turvallisuuden.

Osaamisen kehittäminen kansallisella tasolla on pitkäjänteistä toimintaa, joka lähtee jo koulumaailmasta. Salausmenetelmien osaaminen vaatii matematiikan ja ohjelmoinnin osaamista ja ymmärrystä sekä tietenkin kiinnostusta alaa kohtaan. Tämän lisäksi osaamista vaaditaan lähes kaikilla yhteiskunnan aloilla niin yksityisellä kuin julkisellakin sektorilla. Oman haasteensa osaamisen kehittämiseen ja osaajien houkuttelemiseen Suomeen muodostaa se, että yleisellä tasolla kyberturvallisuuden osaajista nähdään tällä hetkellä sekä EU:n että maailman tasolla erittäin suurta puutetta. Tähän joukkoon kuuluvat myös salausmenetelmien osaajat ja heidänkin kysyntänsä ylittää tarjonnan tällä hetkellä.

6.4 Yhteenveto ja johtopäätöksiä

Tulevaisuudessa salausmenetelmien kysyntä viestinnässä tulee kasvamaan ja niitä halutaan käyttää entistä moninaisempiin tarkoituksiin hyvin erilaisissa ympäristöissä. Vain seuraamalla salausmenetelmien ja erilaisten sovellusten kehitystä voidaan myös Suomessa varmistaa edellytykset perustuslain 10§:n mukaiseen yksityisyyden suojaan viestinnässä. Myös suomalaista osaamista tällä alalla on hyvä kehittää ja hyödyntää eri yhteiskunnan ja liiketoiminnan alueilla.

1. **Ei takaportteja salausmenetelmiin.** Salausmenetelmiin lain voimalla esitetyt rajoitukset ja takaportit eivät ole ratkaisu salauksen mahdollisesti muodostamiin ongelmiin viranomaisten tiedonsaannissa. Takaportteja ei voida toteuttaa sillä tavoin, että ne mahdollistaisivat salausmenetelmien turvallisen käytön.
2. **Suomalaisen salausmenetelmäosaamisen tasosta tulee pitää huolta.** Koska matematiikan osaamisesta ollaan huolissaan tekoälyn suhteen, niin tässä on toinen osa-alue, jossa matematiikan ja teoreettisen tietojenkäsittelyn sekä insinööriosaamisen tulee olla hyvällä tasolla. Li-

säksi tämä tukee myös kyberturvallisuusstrategiassa [70] esitettyjä osaamisen kehittämiseen liitettyjä tavoitteita.

3. **Edelläkävijyyttä myös salausmenetelmien osaamisessa.** Suomi on edelleen langattomien verkkojen kommunikaatioratkaisuissa (5G jne.) maailman ykkösmaita. Tätä edelläkävijyyttä tulee vaalia ja siihen tulee sisällyttää myös riittävä salausmenetelmien ja laajemminkin tietoturvan osaaminen.
4. **Kvanttilaskennan huomioiminen salausratkaisuissa.** On tärkeä seurata mm. NIST:n standardointia tässä aiheessa ja myös Suomessa valmistautua siirtymään uusien vaatimusten mukaisen salauksen hyödyntämiseen. Erityisesti pitkän aikavälin digitaalisissa allekirjoituksissa kannattaa huomioida mahdollinen kvanttilaskennan tuoma riski.

7 Johtopäätöksiä ja suosituksia

Viestinnän salaamiseen ja suojaamiseen on olemassa lukuisia erilaisia menetelmiä ja sovelluksia. Koska erilaisissa tilanteissa tarvitaan erilaisia ominaisuuksia salaukselta, yhtä yksittäistä menetelmää tai sovellusta ei voida esittää ratkaisuksi kaikkiin ongelmiin.

Raportissamme olemme esittäneet useita johtopäätöksiä ja suosituksia. Esitetyt johtopäätökset ja suositukset voidaan jakaa kolmeen osioon: Yleisiin, viestinnän salaamiseen liittyviin sekä kansalliseen toimintaan liittyviin johtopäätöksiin. Alla esitellään yhteenveto tutkimuksen johtopäätöksistä.

7.1 Tutkimuksen yleiset johtopäätökset

1. **Yksittäistä ja yksiselitteisesti parasta ratkaisua ei ole.** Eri viestintäsovellusten salausmenetelmät lähtevät erilaisista lähtökohdista ja tavoitteista. Näin ollen käytetyn sovelluksen tulee perustua käyttäjän omaan riskiprofiiliin ja -arvioon ja näihin parhaiten sopivan menetelmän ja sovelluksen valintaan.
2. **Ei takaportteja salausmenetelmiin.** Salausmenetelmiin lain voimalla esitetyt rajoitukset ja takaportit eivät ole ratkaisu salauksen mahdollisesti muodostamiin ongelmiin viranomaisten tiedonsaannissa. Takaportteja ei voida toteuttaa sillä tavoin, että ne mahdollistaisivat salausmenetelmien turvallisen käytön.
3. **Ohjeiden ja arviointien julkaiseminen.** Julkisen tahon tekemien arviointien julkaiseminen sekä näiden arviointien pohjalta tehtävien ohjeistusten tekeminen on yksi mahdollinen tapa edistää salaustuotteiden markkinoita.
4. **Kehitystä on seurattava ja mahdollisia ohjeita päivitettävä.** Yksittäisistä sovelluksista ja kokonaisista protokollista ja jopa salausmenetelmistä voi löytyä yllättäviä heikkouksia, jotka voivat vaarantaa halutut ta-

voitteet. Täten näiden sovellusten ja menetelmien jatkuva seuraaminen ja niihin liittyvien ohjeiden ja johtopäätösten päivittäminen on tärkeää.

5. **Globaalin kehityksen seuraaminen.** Esimerkiksi EFF:n raportista on tulossa uusi versio ja lisäksi myös monet muut julkiset ja yksityiset tahot julkaisevat erilaisia raportteja salausmenetelmiin liittyen. Näistä esimerkkinä ENISA:n raportti [42] sekä Viron tietoturvaviranomaisten julkaisema raportti [43]. Näiden ja vastaavien raporttien kautta salausmenetelmien ja viestinnän salaussovellusten kehityksen seuraaminen ja annettujen suositusten arvioiminen sekä toteuttaminen on suositeltavaa.

7.2 Viestinnän salaamiseen liittyvät johtopäätökset

1. **Aina kun mahdollista käytä päästä päähän salattua ja viestinnän eheyden varmistavaa menetelmää.** Nykyään päästä päähän salatun viestinnän varmistavia viestisovelluksia on useita ja niiden käytettävyys on hyvällä tasolla. Tämänkaltaisen viestimen käyttö alkaakin olla jo ns. peruskyberhygieniaa. Lisäksi on hyvä varmistua viestien muuttumattomuudesta matkalla lähettäjältä vastaanottajalle.
2. **Varmista avainten oikeellisuus.** Useat sovellukset tarjoavat mahdollisuuden varmistaa avainten oikeellisuus. Tätä mahdollisuutta on hyvä käyttää ja varmistaa avainten oikeellisuus ennen viestinnän aloittamista.
3. **TLS-protokollaa käytettäessä RSA-salausta tulisi välttää.** Sekä historialliset että viimeaikaiset löydökset osoittavat, että TLS:n RSA-salauksesta löytyy herkemmin heikkouksia kuin muista julkisen avaimen menetelmistä, joita TLS:ssä voidaan käyttää. Näin ollen on parempi ottaa käyttöön näitä muita menetelmiä aina kun se vain on mahdollista.
4. **Kvanttilaskennan huomioiminen salausratkaisuissa.** On tärkeä seurata mm. NIST:n standardointia tässä aiheessa ja myös Suomessa valmistautua siirtymään uusien vaatimusten mukaisen salauksen hyödyntämiseen. Erityisesti pitkän aikavälin digitaalisissa allekirjoituksissa kannattaa huomioida mahdollinen kvanttilaskennan tuoma riski.

7.3 Kansalliseen toimintaan liittyvät johtopäätökset

1. **Suomalaisen salausmenetelmäosaamisen tasosta tulee pitää huolta.** Koska matematiikan osaamisesta ollaan huolissaan tekoälyn suhteen, niin tässä on toinen osa-alue, jossa matematiikan ja teoreettisen tietojenkäsittelyn sekä insinööriosaamisen tulee olla hyvällä tasolla. Lisäksi tämä tukee myös kyberturvallisuusstrategiassa [70] esitettyjä osaamisen kehittämiseen liitettyjä tavoitteita.
2. **Edelläkävijyyttä myös salausmenetelmien osaamisessa.** Suomi on edelleen langattomien verkkojen kommunikaatioratkaisuissa (5G jne.) maailman ykkösmaita. Tätä edelläkävijyyttä tulee vaalia ja siihen tulee sisällyttää myös riittävä salausmenetelmien ja laajemminkin tietoturvan osaaminen.
3. **Suomalaisille käyttäjille suunnatut ohjeet.** Suomalaisille tavallisille viestinnän käyttäjille suunnatut ohjeet olisivat hyvin tärkeät. Ohjeita voi myös jakaa hieman erilaisille riskiryhmille. Tällaisia ratkaisuja löytyy verkosta jo muutamia[44] ja näiden mallien pohjalta voidaan rakentaa, myös suomalaiset ohjeet.
4. **Suomalaisten tuotteiden kehitystä tulee tukea.** Salausmenetelmistä ja viestinnän salaukseen liittyvistä tuotteista voi tulla hyvinkin kriittisiä huoltovarmuuden ja kansalaisyhteiskunnan toimivuuden kannalta. On hyvä pitää osaamista ja teknologiaan liittyvää kehitystä myös Suomessa. Suomalaisia ratkaisuja voidaan hyvin hyödyntää myös globaalisti.

[44] https://www.wired.com/2017/12/digital-security-guide/ sekä https://securityplanner.org/#/

8 Lähteet

[1] Liikenne- ja viestintäministeriö, ”Maailman luotetuinta digitaalista liiketoimintaa,” 2016.

[2] M. Blaze, ”Protocol failure in the escrowed encryption standard,” tekijä: *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, 1994.

[3] United States National Institute of Standards and Technology (NIST)., ”Announcing the ADVANCED ENCRYPTION STANDARD (AES),” Federal Information Processing Standards Publication 197 , 2001.

[4] S. Seo ja K. Kent, ”Security Architecture for the Internet Protocol. IETF Specification,” 2005. [Online]. Available: http://tools.ietf.org/html/rfc4301.

[5] B. Weis, G. Gross ja D. Ignjatic, ”Multicast Extensions to the Security Architecture for the Internet Protocol. IETF Specification,” 2008. [Online]. Available: http://tools.ietf.org/html/rfc5374.

[6] S. Kent, ”IP Encapsulating Security Payload (ESP). IETF Specification,” 2005. [Online]. Available: http://tools.ietf.org/rfc/rfc4303.txt.

[7] S. Kent, ”IP Authentication Header. IETF Specification,” 2005. [Online]. Available: http://tools.ietf.org/html/rfc4302.html.

[8] D. Harkins ja D. Carrel, ”The internet key exchange (IKE). IETF specification,” 1998. [Online]. Available: http://tools.ietf.org/html/rfc2409.html.

[9] C. Kauffman, ”Internet Key Exchange (IKEv2) Protocol. IETF specification,” 2005. [Online]. Available: https://tools.ietf.org/html/rfc4306.

[10] S. Friedl, ”An Illustrated Guide to IPsec,” 2005. [Online]. Available: http://www.unixwiz.net/techtips/iguide-ipsec.html.

[11] W. Goldberg, ”GSM cloning,” 2002. [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/gsm.html.

[12] G. M. Køien, ”An introduction to access security in UMTS,” *IEEE Wireless Communications,* osa/vuosik. 11, nro 1, pp. 8-18, 2004.

[13] 3GPP, ”TS 35.205 V14.0.0. 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and,” 2017. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/35_series/35.205/35205-e00.zip.

[14] 3GPP, ”TS33.401. System Architecture Evolution (SAE). Security architecture.,” 2015. [Online].

[15] R. Anderson, ”A5 (Was: HACKING DIGITAL PHONES),” 1994. [Online]. Available: https://groups.google.com/forum/#!msg/uk.telecom/TkdCaytoeU4/Mroy719hdroJ.

[16] ”Cracking GSM A5 protocol,” 2008. [Online]. Available: https://www.scribd.com/document/7227619/Cracking-a5-THC-Wiki.

[17] O. Dunkelman, N. Keller ja A. Shamir, ”A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony,” 2010. [Online]. Available: https://eprint.iacr.org/2010/013.

[18] 3GPP, ”TR 35-202. KASUMI specification,” 2017. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/35_series/35.202/35202-e00.zip.

[19] 3GPP, ”TS 35.215. Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications.,” [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/35_series/35.215/35215-e00.zip.

[20] A. Kircanski ja A. M. Youssef, ”IET Information Security 5.4,” 2011.

[21] NIST, ”Advanced Encryption Standard (AES) (FIPS PUB 197),” 2001. [Online]. Available: Advanced Encryption Standard (AES) (FIPS PUB 197).

[22] M. Dworkin, ” Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication,” NIST Special Publication 800-38B, 2005.

[23] ETSI/SAGE , ”Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3,” 2001.

[24] G. Orhanou ja S. El-Hajji, ”The New LTE Cryptographic Algorithms EEA3 and EIA3,” *Appl.Math,* osa/vuosik. 7, nro 6, pp. 2385-2390, 2013.

[25] T. Ylönen ja C. Lonvick, ”The Secure Shell (SSH) Protocol Architecture. IETF specification,” 2006. [Online]. Available: https://tools.ietf.org/html/rfc4251.

[26] ISO/IEC 14516-2, *Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services,* ISO/IEC, 2002.

[27] T. Dierks ja E. Rescorla, ”The Transport Layer Security (TLS) Protocol. Version 1.2. IETF specification,” 2008. [Online]. Available: https://tools.ietf.org/html/rfc5246.

[28] E. Rescorla, ”The Transport Layer Security (TLS) Protocol Version 1.3. draft-ietf-tls-tls13-21. IETF standars draft,” 2017. [Online]. Available: https://tools.ietf.org/html/draft-ietf-tls-tls13-21.

[29] E. Rescorla, ”HTTP Over TLS. IETF specification,” 2000. [Online]. Available: https://tools.ietf.org/html/rfc2818.

[30] S. Schoen, ”New Research Suggests That Governments May Fake SSL Certificates,” 2012. [Online]. Available: https://www.eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl.

[31] Cyberoam, ”OpenSSL Heartbleed Vulnerability Fix. Security Advisory,” 11 4 2014. [Online]. Available: https://kb.cyberoam.com/default.asp?id=2909&SID=&Lang=1&hglt=Heartbleed.

[32] E. Limer, ”How Heartbleed Works: The Code Behind the Internet's Security Nightmare,” 4 9 2014. [Online]. Available: https://gizmodo.com/how-heartbleed-works-the-code-behind-the-internets-se-1561341209.

[33] E. Rescorla ja N. Modadugu, ”Datagram Transport Layer Security Version 1.2. IETF specification,” 2012. [Online]. Available: https://tools.ietf.org/html/rfc6347.

[34] M. Baugher, D. McGrew, M. Naslund ja N. K. Carrara E., ”The Secure Real-time Transport Protocol (SRTP). IETF specification,” 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3711.txt.

[35] M. Stevens, ”New collision attacks on SHA-1 based on optimal joint local-collision analysis,” tekijä: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2013.

[36] K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt ja D. Stebila, ”A Formal Security Analysis of the Signal Messaging Protocol,” Cryptology ePrint Archive, 2016.

[37] D. Chaum, ”Untraceable electronic mail, return addresses, and digital pseudonyms,” *Communications of the ACM,* osa/vuosik. 24, nro 2, pp. 84-90, 1981.

[38] J. Van Den Hooff, D. Lazar, M. Zaharia ja N. Zeldovich, ”Vuvuzela: Scalable private messaging resistant to traffic analysis,” tekijä: *Proceedings of the 25th Symposium on Operating Systems Principles*, 2015.

[39] G. Danezis ja I. Goldberg, ”Sphinx: A compact and provably secure mix format,” tekijä: *Security and Privacy, 2009 30th IEEE Symposium on*, 2009.

[40] K. Ermoshina, F. Musiani ja H. Halpin, ”End-to-end encrypted messaging protocols: An overview,” tekijä: *International Conference on Internet Science*, 2016.

[41] J. Oikarinen ja D. Reed, ”Internet Relay Chat Protocol,” Internet Engineering Task Force, 1993.

[42] European Union Agency for Network and Information Security, ”Algorithms, key size and parameters report - 2014,” 2014.

[43] Republic of Estonia - Information System Authority, ”Cryptographic Algorithms Lifecycle,” 2016.

[44] Sisäministeriön julkaisu 8/2017, ”Siviilitiedustelulakityöryhmän mietintö,” 2017.

[45] Puolustusministeriö, ”PLM Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi,” 2017.

[46] House Judiciary Committee - Encryption Working Group, ”Encryption Working Group Year-End Report,” 2016.

[47] J. Schaill ja J. Begley, ”The Great SIM heist - How spies stole the keys to the encryption castle,” 19 2 2015. [Online]. Available: https://theintercept.com/2015/02/19/great-sim-heist/.

[48] Z. e. a. Durumeric, ”The matter of heartbleed,” tekijä: *Proceedings of the 2014 Conference on Internet Measurement Conference*, 2014.

[49] M. Barbulescu, A. Stratulat, V. Traista-Popescu ja E. Simion, ”RSA Weak Public Keys available on the Internet,” tekijä: *International Conference for Information Technology and Communications*, 2016.

[50] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system,* 2008.

[51] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg ja M. Smith, ”SoK: secure messaging,” tekijä: *Security and Privacy (SP), 2015 IEEE Symposium on*, 2015.

[52] 3GPP, ”TR 33.899. Study on the security aspects of the next generation system. V. 1.3.,” 2017. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/33_series/33.899/33899-130.zip.

[53] M. N. V. Khan, ”Concealing IMSI in 5G Network Using Identity Based Encryption,” tekijä: *International Conference on Network and System Security* , 2017.

[54] P. Shor, ”Polynomial-time algorithms for prime factorization and discrete logarithms,” *SIAM review,* osa/vuosik. 41, nro 2, pp. 303-332, 1999.

[55] L. Grover, ”Quantum mechanics helps in searching for a needle in a haystack,” *Physical review letters,* 1997.

[56] R. Juskalian, ”Practical Quantum Computers,” *MIT Technology Review,* osa/vuosik. 120, nro 2, pp. 77-81, 3/4 2017.

[57] National Institute of Standards and Technology, ”Post-Quantum Cryptography Standardization,” 2017. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization.

[58] J. H. A. &. Y. R. Hershey, ”Unconventional cryptographic keying variable management,” *IEEE Transactions on Communications,* osa/vuosik. 43, nro 1, pp. 3-6, 1995.

[59] B. K. A. M. A. &. Y. B. Azimi-Sadjadi, ”Robust key generation from signal envelopes in wireless networks,” tekijä: *2007*, Proceedings of the 14th ACM conference on Computer and communications security.

[60] S. T. W. M. N. Y. C. &. R. A. Mathur, ”Radiotelepathy: extracting a secret key from an unauthenticated wireless channel,” tekijä: *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008.

[61] L. &. W. A. Ozarow, ”Wire-tap channel II,” *Advances in Cryptology,* pp. 33-50, 1985.

[62] H. &. V. A. Mahdavifar, ”Achieving the secrecy capacity of wiretap channels using polar codes,” *IEEE Transactions on Information Theory,* osa/vuosik. 57, nro 10, pp. 6428-6443, 2011.

[63] B. Z. D. &. C. S. Danev, ”On physical-layer identification of wireless devices,” *ACM Computing Surveys,* osa/vuosik. 45, nro 1, 2012.

[64] S. B. a. D. Chaum, ”Distance-bounding protocols,” tekijä: *Advances in Cryptology (EUROCRYPT’93)*, 1994.

[65] C. a. M. A. Dimitrakakis, ”Distance-Bounding Protocols: Are You Close Enough?,” tekijä: *IEEE Security & Privacy*, 2016.

[66] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. A. Specter ja D. J. Weitzner, ”Keys under doormats: mandating insecurity by requiring government access to all data and communications,” *Journal of Cybersecurity,* osa/vuosik. 1, nro 1, pp. 69-79, 2015.

[67] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama ja T. Koshiba, ”Packed homomorphic encryption based on ideal lattices and its application to biometrics,” tekijä: *International Conference on Availability, Reliability, and Security*, 2013.

[68] K. Halunen ja V. Vallivaara, ”Secure, Usable and Privacy-Friendly User Authentication from Keystroke Dynamics,” tekijä: *Nordic Conference on Secure IT Systems*, 2016.

[69] N. Apthorpe, D. Reisman ja N. Feamster, *A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic,* Arxiv, 2017.

[70] Valtioneuvoston periaatepäätös 24.1.2013, ”Suomen kyberturvallisuusstrategia,” 2013.

[71] L. M., A. I., Y. M., G. A., A. A. B. ja E. M. d. Oca, ”Leveraging LTE security with SDN and NFV.,” tekijä: *IEEE 10th International Conference on Industrial and Information Systems (ICIIS)*, 2015.

[72] T. Taubert, ”More Privacy, Less Latency. Improved Handshakes in TLS version 1.3,” 2015. [Online]. Available: https://timtaubert.de/blog/2015/11/more-privacy-less-latency-improved-handshakes-in-tls-13/. [Haettu 27 11 2017].