Tampereen yliopisto

Tuukka Tilsa

# PIKAVIESTINSOVELLUKSIEN TIETOTURVA

## Yksityiskäyttäjien tarpeet

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Kesäkuu 2021

# Tiivistelmä

Tuukka Tilsa: Pikaviestinsovelluksien tietoturva – yksityiskäyttäjien tarpeet
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Kesäkuu 2021

---

Pikaviestinsovellukset, kuten Whatsapp, Telegram ja Signal, ovat nousseet merkittäviksi kommunikaatiovälineiksi sähköpostin rinnalle sähköisessä viestinnässä, mutta niiden yksityisyydensuoja ja tietoturva ovat jääneet osin vähälle huomiolle. Tässä tutkielmassa tarkastellaan pikaviestinsovellusten tietoturvaa, yksityisyyttä ja käytettävyyttä maallikkokäyttäjien näkökulmasta.

Tutkimus on toteutettu kirjallisuuskatsauksena, jonka tavoitteena on selvittää nykyisten pikaviestinten toteutunut tietoturvan taso ja siihen vaikuttuvat syyt. Tutkimuskysymyksenä on “Miten pikaviestinsovelluksien tietoturva vastaa käyttäjien tarpeisiin?”. Käsiteltäviä teemoja ovat käyttäjien tarpeet ja tietotaito, pikaviestimien ominaisuudet, viestien salaus ja yksityisyyteen ja tietoturvaan kohdistuvat uhat. Lähdemateriaaliksi on valittu teemoja käsitteleviä tieteellisiä artikkeleita, kirjallisuutta ja konferenssijulkaisuja. Mukaan on otettu myös muuta sähköistä viestintää ja tietoturvaa yleisesti käsittelevää aineistoa.

Olennaisia yksityisyydenuhkia ovat valtiolliset toimijat sekä kaupalliset yritykset, joilla on motiivi kerätä mahdollisimman paljon tietoa käyttäjistä. Myös pikaviestimien välityksellä käydyt keskustelut ovat laajamittaisen joukkoseurannan kohteena. Monet pikaviestimet ovat kuitenkin toteuttaneet salausmenetelmiä, jotka estävät viestien sisällön joutumisen ulkopuolisten tietoon. Salaus ei kuitenkaan takaa käyttäjien anonymiteettiä eikä estä metatietojen keräystä. Metatiedoista voi selvitä mm. kenen kanssa ja koska käyttäjä on viestinyt, mikä on ongelmallista yksityisyydensuojan kannalta.

Tietoturvallisen viestinnän toteutuksessa ongelmaksi on osoittautunut, että kaikkien keskusteluun osallistuvien käyttäjien on valittava yhteensopiva sovellus ja omattava riittävä tietoturvaosaaminen sen käyttämiseksi. Pikaviestimien kehittäjät pyrkivät usein sitouttamaan käyttäjät omaan palveluunsa käyttämällä epäyhteensopivia protokollia. Tämä on johtanut käyttäjäkunnan sirpaloitumiseen ja useiden kilpailevien pikaviestinsovellusten syntymiseen.

Tutkimuksen tuloksena oli, että pikaviestimien tietoturvaominaisuuksille on olemassa perusteltu tarve ja nykyiset pikaviestimet tarjoavat toimivia ratkaisuja maallikkokäyttäjien tarpeisiin, olennaisimpana viestien salaus. Suuri osa käyttäjistä ei kuitenkaan aktiivisesti pyri ottamaan käyttöön edes näitä perusominaisuuksia. Syitä ovat tietoisuuden, tietotaidon ja motivaation puute sekä virheelliset käsitykset uhista ja niitä vastaan suojautumisesta. Osa viestimistä tarjoaa myös kehittyneempiä tietoturvaominaisuuksia, mutta käyttäjät eivät koe niitä tarpeellisiksi. Maallikkokäyttäjien käsityksissä on suuria eroja verrattuna tietoturva-asiantuntijoihin; maallikot eivät usko päästä päähän -salauksen toimivuuteen, kun taas asiantuntijat pitävät sitä vahvana suojana yksityisyydelle.

Avainsanat: pikaviestin, päästä päähän -salaus, tietoturva, yksityisyys, käytettävyys

# Sisällysluettelo

# 1 Johdanto

Valtaosa ihmisten viestinnästä tapahtuu sähköisesti pikaviestinsovellusten, kuten WhatsAppin, Telegramin tai Signalin kautta. Pikaviestimet ovat uusin sähköisen viestinnän toteutus, joka voidaan nähdä sähköpostin kehitysaskeleena. Ihmisten välisissä keskusteluissa käsiteltävät aiheet ovat usein luottamuksellisia, eikä keskusteluja ole tarkoitettu muiden osapuolten tietoon. Oikeutta yksityisyyteen pidetään perustavanlaatuisena ihmisoikeutena. Suomen perustuslaissa todetaan “Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton” (Suomen perustuslaki 731/1999 § 10). Viestin on kuitenkin oltava suljettu, eikä vapaasti luettavissa jotta sitä voidaan pitää luottamuksellisena. Suomen rikoslaissa määritellään viestisalaisuuden rikkominen seuraavasti: “Joka oikeudettomasti avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä…” (Rikoslaki 39/1889 § 3).

Fyysisten viestien yksityisyydessä ero suljetun kirjeen ja postikortin välillä on helppo hahmottaa. Toisessa viesti on vapaasti luettavissa matkalla määränpäähänsä, toisessa tapauksessa vaaditaan tietoisia toimia viestin lukemiseksi. Sähköisessä viestinnässä käyttäjän on paljon vaikeampi arvioida viestien luottamuksellisuuden astetta. Tarkka arvio vaatii asiantuntemusta ja syvällistä perehtymistä monimutkaisiin ja teknisiin aiheisiin. Jos käyttäjän tavoite on lähettää viestejä mahdollisimman sujuvasti, tietorvakysymykset saatetaan nähdä hidasteena ja haittana, tai ne voidaan sivuuttaa kokonaan.

Tietoturvasta puhuttaessa käsitellään usein salasanoja ja niiden käyttöä. Niillä on kuitenkin se etu, että yksittäinen käyttäjä voi parantaa käytänteitään muista riippumatta. Viestinnässä olennainen ominaispiirre ja lisähaaste on se, että kaikkien osapuolten on otettava käyttöön tarvittavat työkalut, jotta muun muassa viestien salaus on mahdollista. Salattu viesti ei täytä tehtäväänsä, jos vastaanottaja ei voi avata sitä, tai ei edes käytä samaa pikaviestintä.

Tämä tutkielma on tehty kirjallisuuskatsauksena, jonka tavoite on selvittää miten nykyiset pikaviestimet ja niiden tietoturva vastaavat maallikkokäyttäjien tarpeisiin. Tuloksena oli, että tietoturvalle on tarve ja nykyiset pikaviestimet tarjoavat toimivia,

suhteellisen helppokäyttöisiä tietoturvaratkaisuja. Käyttäjät eivät kuitenkaan ole tietoisia tietoturvakysymyksistä, tai eivät ole valmiita näkemään lisävaivaa hyvän tietoturvan saavuttamiseksi.

Tutkielman rakenne on seuraava: luvussa 2 esitellään tutkimuksen tavoitteet, käytetyt tutkimusmenetelmät ja aineisto. Luvussa 3 esitellään olennaisia käsitteitä. Luku 4 käsittelee käyttäjiä ja heidän asenteitaan ja tarpeitaan. Luvussa 5 käsitellään käyttäjien ja asiantuntijoiden tunnistamia uhkamalleja liittyen yksityisyyteen ja tietoturvaan. Luvussa 6 luvussa käsitellään lyhyesti tietoturvaominaisuuksien, kuten viestien salauksen toteutusta. Luvussa 7 tarkastellaan yleisten pikaviestimien tietoturvaominaisuuksia ja sitä, miten ne vastaavat käyttäjien tarpeisiin. Lisäksi arvioidaan miten hyvin tietoturva käytännössä toteutuu viestimiä käytettäessä. Luvussa 8 käydään läpi tietoturvan parantamisen haasteita. Luku 9 sisältää aihetta laajemmin eri näkökulmista käsittelevää keskustelua. Luvussa 10 kootaan yhteen tutkimuksen tulokset.

## 2 Tutkimuksen tavoite, menetelmä ja aineisto

Tässä tutkimuksessa selvitetään kirjallisuuslähteiden avulla millaisia asenteita ja näkemyksiä viestimien käyttäjillä on tietoturvasta, ja millaisia tarpeita heillä on. Tutkittava käyttäjäryhmä edustaa enemmistöä, jolla ei ole erityistä asiantuntemusta tietoturvasta. Tämän perusteella arvioidaan miten nykyiset pikaviestinsovellukset vastaavat näihin tarpeisiin. Erityisesti huomion kohteena on käytettävyys. Tutkimuskysymyksenä on “Miten pikaviestinsovelluksien tietoturva vastaa käyttäjien tarpeisiin?”.

On oleellista arvioida myös tietoturvan teknistä toteutusta, jotta voidaan arvioida kuinka hyvin sovellukset onnistuvat saavuttamaan tavoitteensa. Pääasiallinen toteutustapa on viestien salaus, jonka teknistä toteutusta käsitellään lyhyesti. Tässä tutkimuksessa keskitytään ainoastaan sovellusten tietoturvaan, eikä muihin ympäröiviin tekijöihin, kuten alustoihin, joilla sovelluksia käytetään.

Näkökulmana tutkimuksessa ovat yksityiskäyttäjät, jolla ei ole erityistä tietoturvaosaamista. Näin ollen organisaatioiden, kuten terveydenhuollon viestintää käsittelevä aineisto rajattiin pois. Tutkimuksessa ei myöskään käsitellä virallisesti salaiseksi luokiteltavaa kommunikaatiota, joka vaatii erityistä tietoturvaosaamista.

Tälläisiä voivat olla esimerkiksi henkilön toimenkuvaan liittyvä poliittinen, talous- tai sotilasaiheinen viestintä. Yksityiskäyttäjien joukkoon on kuitenkin luettu mukaan esim. journalistit ja aktivistit, joilla ei ole käytettävissään suurten organisaatioiden tietoturvaosaamista ja muita resursseja. Viestinnän sisältö voi olla kuitenkin erittäin arkaluontoista ja sen paljastuminen voi johtaa vakaviin seurauksiin, kuten vangitsemiseen.

Tutkielma on toteutettu kirjallisuuskatsauksena. Aineisto haettiin pääosin Tampereen yliopiston kirjaston Andor-palvelun kautta eri tietokannoista, pääasialliset lähteet olivat ScienceDirect, IEEE Xplore, Springer Link ja EBSCOhost.

Käytetyt hakusanat: *instant messaging, instant messenger, end-to-end encryption, usability, usable security, Edward Snowden, privacy.*

Lisäksi hakusanoihin yhdistettiin termejä *can't, won't, why* ja *problems with,* jolloin tulokseksi saatiin erityisesti aihepiirin ongelmia käsitteleviä tutkimuksia. Hakusanoissa Edward Snowden oli poikkeus yleiskäsitteistä, sillä hän on ollut keskeinen henkilö yksityisuudensuojan tarpeen tuomisessa julkisuuteen.

Tutkimukseen on otettu mukaan aineisto, jossa käsitellään nimenomaisesti pikaviestimiä ja niiden tietoturvaa. Tietoturvan käytettävyyden ja sähköisen viestinnän osalta mukaan on otettu aineistoa laajemmin, sillä rajaus pelkästään pikaviestinkontekstiin osoittautui liian tiukaksi. Tietoturvan käytettävyyttä käsittelevissä tutkimuksissa salasanat olivat selvästi yleisin käytetty esimerkki käytännön tietoturvatoteutuksesta kun tutkittiin käyttäjien toimintaa ja asenteita. Tässä tutkimuksessa on tehty oletus, että suhtautuminen tietoturvaan on yleistettävissä riippumatta tietystä toteutuksesta. Käyttäjän näkökulmasta olennainen ongelma on se, että hyvien tietoturvakäytäntöjen noudattaminen vaatii asiantuntemusta, aikaa ja vaivannäköä (Dencik & Cable, 2017; Theofanos, 2020). Tämä pätee myös pikaviestinten käytössä, missä tietoturva ja yksityisyys ovat vähintäänkin yhtä vaativa ja monimutkainen kokonaisuus.

Aikaisemmissa sähköisen viestinnän tietoturvan käytettävyystutkimuksissa on käsitelty erityisesti sähköpostiviestien salausta PGP-menetelmällä, kuten Whitten ja Tygar (1999) *t*utkimuksessaan *Why Johnny can't encrypt.* PGP kuitenkin osoittautui

liian vaikekäyttöiseksi maallikkokäyttäjille. Kun varsinaiset pikaviestimet alkoivat yleistyä 2000-luvun alussa, myös niiden tietoturvaan alettiin kiinnittää huomiota. Reaaliaikainen viestintä asetti kuitenkin salaukselle lisävaatimuksia, joita yksittäisten viestien salaukseen tarkoitettu PGP ei enää täyttänyt. Pikaviestimien tarpeisiin kehitettiin *Off-the-Record (OTR)* -salausmenetelmä, jolla oli potentiaalia levitä laajaan käyttöön, sillä se julkaistiin vapaasti käytettävänä kirjastona (OTR, 2021). Vaikka OTR-lisäosa oli tarjolla moniin pikaviestimiin, sekään ei vakiinnuttanut asemaansa käyttäjien enemmistön keskuudessa. OTR:n käytettävyyttä arvioivat tutkimukset totesivat myös OTR:n käytettävyydessä olevan suuria puutteita (Cohn-Gordon et al., 2017; Stedman et al., 2008; Unger et al., 2015). Ongelmat olivat osin samoja kuin PGP-salauksessa, kuten erityisesti käyttäjältä vaadittava asiantuntemus.

Pikaviestinten jatkunut yleistyminen henkilökohtaisessa viestinnässä on antanut mahdollisuuksia uusiin teknisiin sovelluksiin ja niiden tutkimiseen. Mm. Herzberg ja Leibowitz (2016) ovat käsitelleet viimeisimpien pikaviestimien salausominaisuuksia loppukäyttäjän näkökulmasta ja löytäneet edelleen useita kehityskohteita käyttävyydessä. Tietoturvasta on kuitenkin tulossa perusominaisuus, ja useimmat nykyiset pikaviestimet sisältävätkin perustasoisen viestien salaustoiminnallisuuden.

Pikaviestimet voidaan nähdä sähköpostin seuraajana henkilökohtaisessa viestinnässä ja mahdollisena alustana luottamukselliseen viestintään. Tällä perusteella sähköpostin käytettävyyttä ja tietoturvaa koskevat tutkimukset ovat relevantteja myös pikaviestimiä käsiteltäessä. Käyttäjien kokemat haasteet ovat hyvin samankaltaisia kaikessa sähköisessä viestinnässä.

Keskeisiä tutkimuksessa esiin nousseita teemoja olivat käyttäjien tietoisuuden ja tietotaidon puute, tietoturvan vaikeaksi koettu käytettävyys ja käyttäjäjoukkojen sirpaloituminen. Sirpaloitumisen syitä olivat viestimien keskinäinen epäyhteensopivuus ja käyttäjien haluttomuus muuttaa toimintaansa, kuten vaihtaa viestintäsovelluksesta toiseen.

# 3 Keskeiset käsitteet

Tutkielman aihealueeseen liittyy useita käsitteitä jotka voivat olla monitulkintaisia, tai joille ei ole vakiintunutta ja yksikäsitteistä suomenkielistä vastinetta. Tässä luvussa

määritellään mitä käytetyillä termeillä ja tarkoitetaan. Pääasiallinen konteksti on sähköinen viestintä kahden käyttäjän välillä.

## 3.1 Sähköinen viestintä, pikaviestimet ja sähköposti

Tässä tutkielmassa sekä sähköpostia että pikaviestimiä käsitellään sähköisen viestinnän alakategorioina, sillä loppukäyttäjän näkökulmasta molemmantyyppiset toteutukset palvelevat samaa tarkoitusta. Pikaviestimet voidaan nähdä sähköpostin seuraajana sähköisessä viestinnässä, vaikka tällä hetkellä molemmat ovat yleisesti käytössä rinnakkain. Tyypillisiä eroja toteutuksessa ja käyttötavoissa ovat:

**Sähköposti:** Sähköposti on korvannut erityisesti fyysisiä kirjeitä virallisten tahojen kanssa asioinnissa. Sen erityispiirre on laaja yhteensopivuus, sillä lähes kaikkien palveluntarjoajien sähköpostiosoitteista voi lähettää viestejä kaikkiin muihin osoitteisiin, toisin kuin eri pikaviestimien välillä. Sähköpostin heikkoutena on huono tietoturva, sillä valtaosa viesteistä lähetetään selkokielisinä ilman salausta.

Taulukko 1. Keskeisiä käsitteitä (Butterfield et al., 2016; Conti et al., 2016; Dencik & Cable, 2017; Kyberturvallisuuskeskus, 2021; NIST, 2021).

| **Englanninkielinen Käsite** | **Lyhenne** | **Suomenkielinen vastine** | **Määritelmä** |
|---|---|---|---|
| Cybersecurity, computer security | - | Tietoturva | Tietojen luottamuksellisuus, eheys ja käytettävyys. Tietojen tulee olla vain niiden käyttöön oikeutettujen saatavilla. |
| End-to-end encyption | E2EE, E2E-encryption | Päästä päähän -salaus, läpisalaus | Salausmenetelmä, missä viestien salausta ei pureta matkalla. |
| Public key encryption | | Julkisen avaimen salaus | Yleisesti käytetty salausmenetelmä jossa salaus ja salauksen purkaminen tapahtuvat eri avaimilla. |
| Pretty good privacy | PGP | . | Salausmenetelmä. Käytetty yleisesti mm. sähköpostiviestien salaamiseen. |
| Mass Surveillance | - | Joukkoseuranta | Laajamittainen tietojenkeräys jonka kohteena on esim. tietyn maan väestö. |
| Man-in-the-Middle | MitM | - | Hyökkääjä esiintyy keskustelun osapuolena saadakseen viestien sisällön tietoonsa. |

**Pikaviestin (IM, instant messenger):** Sovellus jolla käyttäjät voivat lähettää tekstimuotoisia viestejä toisilleen (Sutikno et al., 2016). Voi sisältää lisäominaisuuksia kuten kuvien ja videoiden lähettäminen, sekä video- ja äänipuhelut (Sutikno et al., 2016). Käytetään erityisesti yksityisiin ja epävirallisiin keskusteluihin. Toteutuksissa painotetaan yleensä reaaliaikaisuutta ja viestiketjut esitetään keskusteluina, joita on helpompi seurata kuin sähköpostiviestiketjuja. Sovelluksissa painotetaan mobiilikäyttöä erityisen paljon sähköpostiin verrattuna. Lisäksi pikaviestimet sisältävät usein lisätoimintoja, kuten emojia, tarroja, video- ja äänipuhelut ja kuvien ja videoiden jakaminen. Useat sovellukset tarjoavat helppokäyttöisen päästä päähän -salauksen.

Taulukkoon 1 on koottu keskeisimpiä tutkielmassa esiintulevia termejä, liittyen tietoturvaan, viestien salaukseen ja salauksen toteutukseen. Salauksen toimintaa ja sen toteutusta nykyisissä pikaviestimissä käsitellään tarkemmin luvuissa 6 ja 7.

## 3.2 Tietoturva ja yksityisyys

Viestiliikenteen suojaamiseen voidaan käyttää myös edistyneempiä menetelmiä kuin pelkkä viestien sisällön salaus. Joissain tapauksissa voi olla toivottavaa, että käyttäjää ei pystytä yksilöimään tai todistamaan viestin lähettäjän henkilöllisyyttä jälkikäteen. Tälläisiä viestinnän mahdollisia lisäominaisuuksia on listattu taulukkoon 2.

Käyttäjien enemmistölle passiivista tiedonkeruuta (joukkoseurantaa) rajoittavat toimet ovat riittävä tavoite. Aktiivisen hyökkääjän suorittamaa kohdennettua operaatiota vastaan puolustautuminen asettaa erityisen suuria vaatimuksia tietoturvan toteutukselle. Myös maallikkokäyttäjät voivat kuitenkin tarvita näitä ominaisuuksia esimerkiksi sanan- tai journalistisen vapauden varmistamiseksi tai vallitsevan poliittisen tilanteen johdosta. Hyvä tietoturva pyrkii minimoimaan vahingot myös siinä tapauksessa, että osa keskustelusta tai salauksesta on vaarantunut tai vuotanut. Salausta ei myöskään tule voida käyttää todisteena siitä, että tietty käyttäjä on lähettänyt jonkin viestin, koska ihmisten välisessä kommunikaatiossa on aina olemassa vastapuoliriski. Teknisillä ratkaisuilla ei voida vaikuttaa siihen, mitä keskustelun toinen osapuoli tekee saamallaan informaatiolla.

Taulukko 2. Viestinnän turvallisuusominaisuuksia (Unger et al., 2015).

| Ominaisuus | Vaikutus |
|---|---|
| **Luottamuksellisuus (Confidentiality)** | Ainoastaan tarkoitettu vastaanottaja voi lukea viestin. Palveluntarjoaja tai muu keskustelun ulkopuolinen taho ei pysty saamaan viestin sisältöä selville, vaikka saisi viestin haltuunsa salatussa muodossa. |
| **Eheys (Integrity)** | Yritykset muokata viestejä matkalla päätepisteiden välillä pystytään huomaamaan ja muokatut viestit hylkäämään. Osapuolet voivat luottaa vastaanotettujen viestien sisällön vastaavan lähetettyjä viestejä. |
| **Käyttäjän tunnistus (Authentication)** | Keskustelun osapuolet voivat varmistaa viestien lähettäjän. Tarjoaa mekanismin, jolla varmistetaan että viestien vastaanottajat pysyvät samoina joiden kanssa keskustelu on aikaisemmin aloitettu. |
| **Eteenpäin turvallisuus (Forward secrecy)** | Salausavainten paljastuminen ei mahdollista kaikkien edellisten viestien avaamista. Vuotanut avain paljastaa vain osan viestihistoriaa. |
| **Taaksepäin turvallisuus (Backward secrecy)** | Paljastunella avaimilla ei voida purkaa seuraavia salattuja viestejä. Käytetään myös termiä *future secrecy*. |
| **Kiistettävyys (Deniability)** | Jälkikäteen ei voida varmuudella osoittaa todeksi, että tietty käyttäjä on lähettänyt tietyn viestin tai osallistunut keskusteluun, vaikka osa salausavaimista ja viestihistoriasta olisi paljastunut. |
| **Anonymiteetin ylläpito (Anonymity Preserving)** | Viestintä ei heikennä käytetyn viestinkuljetusarkkitehtuurin tarjoamaa anonymiteettiä, eikä vuoda käyttäjien yksilöimisen mahdollistavia tunnisteita. |
| **Ryhmäkeskustelut (Group conversations)** | Käyttäjiä voidaan lisätä tai poistaa ilman uuden keskustelun aloittamista. Osallistujat voivat lukea keskusteluja vain siltä ajalta kuin he ovat olleet itse osallisina. |

# 4 Käyttäjät

Pikaviestinten käyttäjät ovat laaja ja heterogeeninen joukko. Pelkästään WhatsAppilla (2020) on yli kaksi miljardia käyttäjää maailmanlaajuisesti. Tässä luvussa perehdytään käyttäjien välisiin eroihin ja tietoturvan haasteisiin käyttäjien näkökulmasta.

Keskeisimpiä on tietoisuuden puute koko aihealueesta. Kaikki eivät ole tulleet edes ajatelleeksi, että viestinten käytössä olisi tarpeellista huolehtia myös yksityisyydestä ja tietoturvasta. Toinen vallitseva asenne on se, että tietoturvalla ja yksityisyydellä ei ole väliä, koska mahdollisia uhkia ei pidetä vakavina (Endeley, 2019;

Gerber et al., 2019). Osa käyttäjistä tiedostaa tarpeen toimia, mutta ei usko että on olemassa toimivia ratkaisuja, tai että heidän olisi mahdollista käyttää niitä (Renaud et al., 2014).

Renaud et al. (2014) tutkivat E2E-salauksen käyttämättä jättämisen syitä sähköpostissa. He jakoivat selitykset seitsemään eri luokkaan tietämyksen, motivaation ja osaamisen mukaan. Vaikka tutkimus käsittelee sähköpostia pikaviestimien sijaan, teen oletuksen, että löydökset ovat yleistettävissä myös muuhun sähköiseen viestintään kuten pikaviestimiin. Maallikkokäyttäjän kannalta viestien lähettämisen toteutus ei ole tässä yhteydessä olennainen. Taulukossa 3 on kuvattu käyttäjien seitsemän eri luokkkaa ja näiden tyypillinen suhtautuminen tietoturvaan ja yksityisyyteen.

Taulukko 3. Käyttäjien seitsemän luokkaa (Renaud et al., 2014; Volkamer et al., 2015).

| **Käyttäjän luokka** | **Suhtautuminen** |
|---|---|
| Ei yksityisyystietoisuutta | Ei ole lainkaan tietoinen siitä, että viestinnässä voi olla turvallisuusuhkia. |
| Tietoinen yksityisyyskysymyksistä, mutta ei huolestunut | ”Ei salattavaa” -asenne, ei pidä yksityisyyttä olennaisena oikeutena. Ei usko olevansa itse kohteena. |
| Huolestunut, mutta virheellisiä käsityksiä | Tunnistaa riskejä, mutta arvioi niiden suurusluokan väärin. Ei todenmukaista käsitystä uhista ja vastakeinoista. Esim. ei usko päästä päähän -salauksen toimivuuteen. |
| Tietoinen ja perehtynyt, mutta ei tarvetta toimia | Suhteellisen realistinen kuva riskeistä, mutta pitää turvattomienkin viestimien hyötyä suurempana kuin uhkia. Ei motivaatiota lisävaivan näkemiseen. |
| Huolestunut, hyvä ymmärrys, mutta ei tiedä miten toimia | Hahmottaa riskit kattavasti, mutta ei omaa riittävää tietotaitoa hallita uhkia. |
| Huolestunut, haluaa toimia, mutta ei kykene | Tietoinen riskeistä ja vastatoimista, mutta esimerkiksi viestinnän vastapuolet eivät suostu tietoturvatason noston vaatimiin toimiin. |
| Huolestunut, tietää mitä tehdä, mutta ei silti toimi | Valvontarealismi, näkee vallitsevan tilanteen muuttamisen toivottomana. Kokee turvallisuuden hinnan liian kovana (esim. melkein kaiken viestinnän lopettaminen). |

Taulukossa 3 nousevat esiin olennaisina teemoina tietotaidon puute ja tarpeeksi helppokäyttöisten tietoturvaratkaisujen puute. Tutkimuksen perusteellla käyttäjät eivät vastusta parempaa tietoturvaa, mutta suuri osa ei ole valmis näkemään lisävaivaa sen

saavuttamiseksi. Enemmistö käyttäjien luokista on kuitenkin huolestunut tietoturva- ja yksityisyyskysymyksistä. Mikäli ratkaisu on tarpeeksi helppokäyttöinen, mikään käyttäjien luokka ei vastusta tietoturvan parannusta. Tämän perusteella voidaan päätellä, että tietoturvalliselle viestinnälle on olemassa olennainen tarve.

Tietoturva-asiantuntijoiden ja maallikkokäyttäjien suhtauminen tietoturvaan poikkeaa toisistaan olennaisesti. Pikaviestimiin ja tietoturvaan liittyy paljon monimutkaisia teknisiä konsepteja, joiden opiskeluun ja ymmärtämiseen käyttäjät eivät ole motivoituneita.

**Maallikkokäyttäjä:** Sekä Gerber et al. (2018) että Dechand et al. (2019) tutkivat luottamusta WhatsAppia kohtaan ja totesivat, että käyttäjien luottamus on hyvin vähäistä. Syitä epäilevään asenteeseen oli monia. Merkittävä tekijä oli käyttäjien epätietoisuus salauksen yleisestä toimintaperiaatteesta ja sen toteutuksesta WhatsApp-viestimessä. Päästä päähän -salauksen (E2E) ei nähty antavan kattavaa suojaa urkkijoita vastaan, sillä osaavien tahojen kuten hakkerien tai valtiollisten toimijoiden uskottiin voivan avata ja lukea viestit matkalla. Vaikka salaus suojaisi viestejä matkalla, niin myös palveluntarjoajan (kuten WhatsApp) uskottiin voivan avata ja lukea viestit halutessaan.

Ainoastaan 25% Gerberin ja muiden (2018) tutkimukseen vastanneista uskoi, että WhatsApp on toteuttanut viestien salauksen toimivasti ja pelkästään käyttäjän etu motiivinaan. WhatsAppin kuuluminen Facebookin omistukseen oli luottamusta heikentävä tekijä. Käyttäjät kokivat myös liikentoimintamallin, käyttäjien tietojen käytön ja salauksen teknisen toteutuksen läpinäkymättömyyden ongelmalliseksi. Mahdollisiksi neutraaleiksi syiksi toimivan salauksen tarjomiseksi mainittiin kilpailu markkina-asemasta ja lakitekniset seikat, jotta WhatsApp ei olisi vastuussa käyttäjien lähettämistä viesteistä.

**Tietoturva-asiantuntija:** Olennainen ero asiantijoiden suhtautumisessa on se, että he luottavat toimivien teknisten ratkaisujen olevan mahdollisia. Monien pikaviestimien salauksessa käyttetty Signal-protokolla pystyy tosiallisesti tarjoamaam vahvan salauksen, minkä enemmistö käyttäjistä ei usko olevan mahdollista. (Cohn-Gordon et al., 2017) Peruskäyttäjät vaikuttavat uskovan, että salauksen murtaminen on melko vaivatonta siihen kykeneville toimijoille (Gerber et al., 2018). Asiantuntijat taas arvottavat usein salauksen ja muut yksityisyystyökalut sen mukaan, miten vaikeaa

suojauksen ohittaminen tai murtaminen on, eli miten paljon aikaa ja resursseja hyökkääjä joutuu käyttämään. Vallitseva konsensus asiantuntijoiden keskuudessa on se, että hyvin toteutetun salauksen murtaminen on vaikeaa tai mahdotonta jopa valtiollisille toimijoille. Tyypillisesti käyttäjä onkin järjestelmän heikoin lenkki.

Kuuluisa saksalainen Enigma-salausjärjestelmä onnistuttiin murtamaan juuri siksi, että sen käytössä ilmeni inhimillisiä virheitä (Thimbleby, 2016). Enigma oli myös *symmetrinen* järjestelmä, jossa viestin salaus ja purkaminen tapahtuivat samalla salausavaimella. Laite tai tiedot sen toiminnasta eivät missään tapauksessa saaneet päätyä vastapuolen haltuun, sillä se olisi vaarantanut koko järjestelmän turvallisuuden. Tätä salassapitoon perustuvaa turvallisuusmallia *(security by obscurity)* pidetään nykyään riittämättömänä. Auguste Kerckhoffs esitti jo vuonna 1883 periaatteen, jonka mukaan salausjärjestelmien turvallisuutta arvioitaessa on oletettava että uhkataho tietää järjestelmän toiminnasta kaiken, paitsi sen, mitä avaimia tiettyjen viestien salaamiseen on käytetty (Ince, 2013; Kerckhoffs, 1883). Tämä periaate tunnetaan myös Claude Shannonin esittämänä Shannonin maksimina; ”Vihollinen tuntee järjestelmän” (Shannon, 1949). Nykyiset asymmetriset salausmentelmät pyrkivät täyttämään tämän vaatimuksen.

Maallikkokäyttäjät näkevät julkiset ja avoimet toteutukset turvallisuutta heikentävänä seikkana. Myös ilmaisuus on luottamusta heikentävä asia. Maallikot uskovat vahvan salauksen olevan kallista ja salaista, eli päinvastaista tarjolla oleviin ratkaisuihin nähden. Näkemysero aiheuttaa perusteetonta epäluuloa salausta kohtaan ja vähentää motivaatiota sen käyttöönottoon, jos sen ei uskota toimivan. Toisaalta myöskään suljettuja ja salassapidettäviä ratkaisuja kehittävät palveluntarjoajat eivät näytä nauttivan käyttäjien luottamusta (Gerber et al., 2018). Maallikkokäyttäjän näkökulmasta voi vaikuttaa siltä, että hyviä ratkaisuja tietoturvan parantamiseen ei ole. Asiantuntijat sensijaan luottavat, että avoin, auditoitu ja hyvin toteutettu salaus toimii odotetulla tavalla. He kuitenkin näkevät tietoturvan saavuttamisessa muita ongelmia, kuten käyttäjien enemmistön heikon motivaation, palveluntarjoajien intressit jotka ovat ristiriidassa käyttäjien edun kanssa, sekä muut yksityisyyden uhat (Dencik & Cable, 2017). Pelkästään toimiva salaus ei välttämättä yksistään takaa kohtuullista yksityisyyttä.

Yksityisyys on paljon muutakin kuin pelkkä viestien salaus, asiantuntijat pitävät käyttäjien toimintaan liittyvää metadataa ja sen keräämistä merkittävänä yksityisyysriskinä, joka voi paljastaa lähes yhtä paljon kuin viestien sisältö (Fuchs & Trottier, 2017; Malekhosseini et al., 2018). Käyttäjien vapaaehtoisesti jakamia tietoja, kuten käyttäjäprofiileja ja tilannepäivityksiä voidaan yhdistää esimerkiksi tietoihin siitä kenelle viestejä on lähetetty. On olennaista huomioida, että viestien sisällön salaus ei tarjoa anonymiteettiä. Useat viestimet käyttävät esimerkiksi puhelinnumeroa käyttäjien yksilöimiseen. Tämä on vahva yksilöllinen tunniste, sillä puhelinnumero on yleensä tiukemmin sidottu henkilöön kuin esimerkiksi sähköpostiosoite, joita voi hankkia käyttöönsä varsin vapaasti.

# 5 Uhkamallit

Vuonna 2013 Yhdysvaltain tiedustelupalvelun NSA:n entinen työntekijä Edward Snowden paljasti NSA:n harjoittavan maailmanlaajuista joukkovalvontaa internetissä (Preibusch, 2015). Tunnetuin julkisuuteen nousseista ohjelmista oli nimeltään PRISM, jonka tavoitteena oli tarkkailla, kerätä ja tallentaa laajamittaisesti myös tavallisten ihmisten viestiliikennettä ja toimintaa internetissä. Tämä paljastus oli tärkeä, sillä aikaisemmin tietojenkeräyksen oli oletettu kohdistuvan lähinnä tahoihin, joilla on mm. poliittista tai taloudellista merkittävyyttä. (Dencik & Cable, 2017)

Jotta käyttäjät näkisivät tietoturvan ja yksityisyydensuojan tarpeellisena asiana, on oltava olemassa jokin uhka, jota vastaan he näkevät tarpeelliseksi suojautua. On merkittävää huomata, että osa käyttäjistä ei näe toimenpiteitä tarpeellisena, vaikka he olisivat tietoisia yksityisyydenluokkauksista.

Snowdenin paljastukset eivät kuitenkaan näyttäneet vaikuttavan merkittävästi internet-käyttäjien kiinnostukseen yksityisyyttä kohtaan, vaikka paljastuksista uutisoitiin laajasti valtamediassa. Preibusch (2015) tutki käyttäjien kiinnostusta yksityisyydensuojaan hakusanojen ja paljastuksiin liittyvien avainsanojen esiintymisen perusteella. Suuren yleisön mielenkiinto aihetta kohtaan hiipui nopeasti, eikä uutisoinnin voitu osoittaa muuttaneen ihmisten toimintatapoja. Tämä voi johtua siitä, että suuri osa käyttäjistä pitää pikaviestimiä lähtökohtaisesti epäluotettavimpana kuin tekstiviestejä tai puhelinverkon välityksellä toimiva äänipuheluja (Dechand et al., 2019).

Jotkin maat, kuten Pohjois-Korea, Kiina, Syyria, Yhdistyneet arabiemiirikunnat, Iran, Qatar ja Kuuba ovat kieltäneet vahvaa salausta käyttävät viestimet (Effi, 2020). Kielto implikoi valtioiden tavoitteena olevan pääsy kansalaisten yksityisiin tietoihin. Toinen mahdollinen tulkinta on se, että viestinten salaus ei ole triviaalisti murrettavissa tai kierrettävissä vaan tehokkain toimenpide on pyrkiä estämään salauksen käyttöönotto. Myöskään Snowdenin julkaisemien tietojen perusteella ei näytä siltä, että valtiolliset tahot pystyisivät murtamaan tehokkaina pidettyjä salauksia triviaalisti, vaan tietojen keräämisessä on käytetty muita keinoja (Fuchs & Trottier, 2017).

## 5.1 Eri uhkatyypit

Haastattelututkimusten perusteella käyttäjät osaavat nimetä suuren joukon mahdollisia uhkia, mutta käyttäjien ja asiantuntijoiden käsitykset eri uhkien vakavuudesta ja vastakeinojen toimivuudesta vaihtelevat huomattavasti. Taulukkoon 4 on kerätty yleisimpiä haastatteluissa ilmi tulleita uhkia. Tutkimuksissa haastateltiin eri ikäisiä käyttäjiä useista maista. Tutkimusten tavoitteet ja määritelmät olivat vaihtelevia, joten koostetta varten luokitteluja on jouduttu tulkitsemaan ja yhdistelemään. Jos tutkimuksessa on mainittu useita mahdollisia uhkien alakategorioita, on taulukkoon poimittu suurin esiintynyt prosenttiosuus.

Taulukko 4. Tietyn yksityisyyden uhan maininneiden vastaajien osuus.

| | **Tutkimus** | | | |
|---|---|---|---|---|
| **Uhka** | Dechand et al., (2019) N = 11 | Gerber et al., (2018) N=20 | Murata et al., (2017) N = 491 | Abu-Salma et al., (2017) N=60 |
| Kaupalliset yritykset | 40 % | 90 % | 86 % | 13 % |
| Internet-operaattorit ja palveluntarjoajat | 60 % | 90 % | ---- | 90 % |
| Valtiolliset toimijat | 53 % | 60 % | 39 % | 97 % |
| Hakkerit ja rikolliset | 60 % | 90 % | 56 % | 97 % |

Esiin tulleet uhat voidaan jaotella eri luokkiin Ungerin ja muiden (2015) esittelemän mallin mukaan seuraavasti:

*Paikalliset uhat:* Esim. Avoimien langattomien verkkojen tarjoajat. Fyysisesti läsnä oleva hyökkääjä.

*Globaalit uhat :* Hyökkäjät jotka pystyvät kontrolloimaan suuria osia internetin infrastruktuurista, kuten valtiolliset toimijat ja suuret internet-operaattorit.

*Palveluntarjoajat:* Tahot joiden hallinnoiman infrastruktuurin läpi viestiliikenne kulkee, ovat myös mahdollisia uhkia. Internet-operaattorit ja keskitettyä arkkitehtuuria käyttävät viestinsovellukset lukeutuvat tähän joukkoon.

Kategoriat eivät ole toisiaan poissulkevia, vaan useat uhat kuuluvat moneen kategoriaan (Unger et al., 2015). On myös mahdollista että hyökkääjä hyödyntää kaikkia kategorioita yhdessä. Edward Snowden kuvaa NSA:n käyttävän kaikkien kategorioiden keinoja operaatioissaan. NSA velvoittaa Internet-operaattorit ja yksityiset yritykset (kuten Microsoft, Google ja Facebook) jakamaan keräämänsä tiedot(Endeley, 2019). Internetin tietoliikennettä seurataan kokonaisvaltaisesti aina merenalaisten runkokaapeleiden valvontaan asti. Laajan internetliikenteestä kerätyn aineiston perusteella pyritään löytämään kohteita, jotka voidaan ottaa aktiivisen ja kohdennetun seurannan kohteeksi. (Bauman et al., 2014)

Valtioden tiedustelupalvelut tekevät myös yhteistyötä keskenään. Yksi tälläinen liittouma on *Five Eyes*, johon kuuluvat Yhdistynyt kuningaskunta, Yhdysvallat, Kanada, Australia ja Uusi-Seelanti (Bauman et al., 2014).

Vaikka urkintaa suorittavat tahot eivät saisi viestien sisältöä tietoonsa, myös viestien metadata voi paljastaa arkaluontaista tietoa (Malekhosseini et al., 2018). Hyökkääjä voi saada selville kenen kanssa käyttäjä on viestinyt, koska ja kuinka pitkään. Tietoja voidaan jakaa myös vapaaehtoisesti, kuten Whatsappin profiilin ja tila-viestien kautta. Tieto siitä, koska käyttäjä on ollut paikalla yhdessä muun metadatan kanssa voi mahdollistaa varsin tarkan kuvan luomisen käyttäjän toiminnasta.

## 5.2 Maallikkokäyttäjän riskiarvio

Viestisovellusten käyttäjät voi perustellusti olettaa, että usea toimija on motivoitunut keräämään tietoa heidän viestiliikenteestään. Valtiollinen tiedustelu ja palveluntarjoajien kaupalliset intressit ovat olennaisia tavoitteita. Ensisijainen uhka maallikkokäyttäjän yksityisyydelle näyttää olevan passiivinen tiedonkeruu, joka perustuu vapaaehtoisesti annettuihin tietoihin palvelujen käyttämisen yhteydessä ja salaamattoman viestinnän ja

sen metadatan keräämiseen (Bauman et al., 2014). Välittömät riskit ja seuraamukset eivät yleensä ole kriittisiä, sillä tiedonkeruun tavoitteena ei ole aktiivinen hyökkäys käyttäjää vastaan.

Vastatoimena vapaaehtoisen tiedon jakamisen rajottaminen ja viestiliikenteen salaaminen parantaa yksityisyyden astetta ja viestinnän luottamuksellisuutta huomattavasti. Salauksen käyttöönottaminen ei myöskään vaadi kohtuuttoman suurta vaivaa, sillä monet viestimet käyttävät salausta vakiona.

Siinä tapauksessa, että käyttäjällä on syytä epäillä voivansa joutua aktiivisen ja kohdennetun tiedustelutoiminnan kohteeksi, yleensä myös seuraamukset ovat vakavampia. Muun muassa journalistit, aktivistit ja poliittista- tai muuta arkaluontoista toimintaa harjoittavat henkilöt voivat olla jopa hengenvaarassa.

Korkean riskin toimintaan liittyvässä toiminnassa viestintävälineeksi tulisi valita erityisen vahvaa salausta käyttävä sovellus. Myös lisäominaisuudet kuten anonymiteetti, kiistettävyys ja mahdollisten tietovuotojen rajaus nousevat tärkeiksi ominaisuuksiksi. Myös metadatan paljastavuuteen pitää suhtautua huomattavasti tarkemmin.

# 6 Tietoturvan toteutus

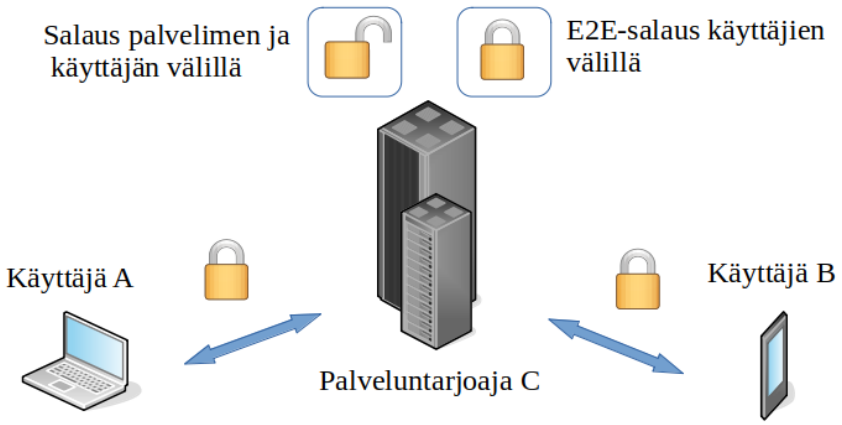
Olennaisin tavoite viestimien tietoturvassa on estää ulkopuolisia saamasta viestien sisältöä käsiinsä. Tämä on yleensä toteutettu salaamalla tekstimuotoiset viestit niin, että ainoastaan oikea vastaanottaja pystyy muuttamaan ne selkokieliseen muotoon.

Viestien salaus on mahdollista toteuttaa eri tavoilla. Symmetrisessä salauksessa sekä viestin salaamiseen että avaamiseen käytetään samaa salausavainta. Viestintäkäytössä on kuitenkin yleensä tarpeen vaihtaa salausavaimia käyttäjien kesken epäturvallista kanavaa (internetiä) pitkin. Tähän soveltuu paremmin Asymmetrinen salaus, jossa salaaminen ja purkaminen tapahtuu eri avaimilla. Käyttäjillä on salainen yksityisavain *(private key),* jolla puretaan viestit ja julkinen avain *(public key),* jolla voidaan salata käyttäjälle lähettävät viestit. Koska julkisella avaimella voidaan vain salata viestejä, mutta ei purkaa niitä, se voidaan lähettää vapaasti verkkoa pitkin. Mahdollinen hyökkääjä ei voi käyttää julkista avainta salattujen viestien murtamiseen.

Kaikkien viestimien salaustoteutuksia ei ole voitu arvioida, koska ne ovat suljettua koodia, joka ei ole julkisesti saatavilla. Arvioitaessa miten käyttökelpoisia toteutuksia on tällä hetkellä olemassa, voidaan esimerkkinä kuitenkin käyttää Open

Whisper Systemsin kehittämään Signal-protokollaa. Myös Whatsapp käyttää oman ilmoituksensa mukaan Signal-protokollan versiota. Signalille on tehty turvallisuusanalyysi ulkopuolisten asiantuntijoiden toimesta (Cohn-Gordon et al., 2017). Analyysissä protokollasta ei löydetty olennaisia heikkouksia, ja myös osan luvussa 5.1 mainituista lisäominaisuuksista arvioitiin toimivan.

Kuva 1 havainnollistaa päästä päähän -salauksen (*End-to-end encryption, E2E -salaus)* ja palvelin-asiakasohjelma -salauksen eroa. E2E-salauksessa viesti on salatussa muodossa koko matkan ajan ja vasta vastaanottaja voi purkaa sen omalla salausavaimellaan. Sen sijaan suppeaammassa asiakasohjelman ja palvelimen välisessä salauksessa viesti on myös salattu matkan aikana, mutta viestin salaus puretaan palvelimella ja salataan uudestaan ennen vastaanottajalle lähettämistä. Näin ollen viesti on luettavissa selkokielisenä palvelimella, mitä viestin sisällöstä kiinnostunut hyökkääjä voi käyttää hyväkseen. Tämäkin toteutus kuitenkin lisää tietoturvaa huomattavasti, sillä viestiliikenne on salattua väleillä AC ja CB, eikä kolmas osapuoli saa viestien sisältöä tietoonsa passiivisella tarkkailulla.




Kuva 1. Salatun viestin lähettäminen keskitetyn välityspalvelimen kautta. Kuvakkeet VRT Systems (CC BY 4.0).

E2E-salaus voidaan toteutaa eri tavoilla. Tietoturvan tason ja käytön helppouden kannalta olennaisia tapoja ovat:

*Opportunistinen päästä päähän -salaus:* Useimmat nykyiset viestimet ottavat salauksen käyttöön automaattisesti aina kun se on mahdollista, eli yleensä heti yhteyden luomisen jälkeen. Näin käyttäjän ei tarvitse itse muistaa ottaa salausta käyttöön joka

kerran kun viestintä aloitetaan. Joissain viestimissä, kuten WhatsAppissa salausta ei voi myöskään ottaa pois päältä.

*Varmennettu päästä päähän -salaus*: Kun salattu yhteys on luotu ensimmäisen kerran, tarvitaan vielä lisävaihe jossa varmistetaan, että keskustelun osapuolet ovat oikeat henkilöt joille viestit on tarkoitettu.

Nykyisissä viestimissä salatun yhteyden luominen on hyvin pitkälle automatisoitua, sillä sähköpostissa käytetty salausmenetelmä PGP osoitti, että keskivertokäyttäjälle useiden salausavainten manuaalinen käsittely ja muut toimenpiteet ovat liian työläitä (Whitten & Tygar, 1999).

Pelkästään vahva salaus ei tarjoa kattavaa tietoturvaa. Olennainen osa luottamuksellista viestintää on oikesta vastaanottajasta varmistuminen. Hyökkääjien ei tarvitse pystyä murtamaan viestien salausta, mikäli he voivat huijata lähettäjää ja esiintyä oikeana vastaanottajana. Tälläinen hyökkäys tunnetaan nimellä *MitM (Man-in-the-Middle).*(Conti et al., 2016; Unger et al., 2015). Vastatoimena voidaan käyttää käyttäjien todennusta salattua viestiyhteyttä luotaessa.

Vastaanottajan todentaminen varmistaa, että vain tarkoitettu vastaanottaja voi avata salatut viestit. Todennuksen käytännön ongelmana on kuitenkin se, että se vaatii käyttäjältä erityisiä toimenpiteitä (Unger et al., 2015). Käyttäjät eivät osaa hahmottaa todennuksen tärkeyttä, sillä opportunistinen salaus antaa heille virheellisen turvallisuudentunteen. Myöskään todennuksen toteutus ei ole riittävän käytettävä useimmissa sovelluksissa, vaan käyttäjät eivät onnistu todennuksessa edes opastettuina (Herzberg & Leibowitz, 2016). Tunnistautumiseen voidaan käyttää merkkijonoja tai kuvasarjoja joita käyttäjät vertaavat keskenään. Uusimpana versiona on tullut käyttöön QR-koodin skannaaminen älypuhelimen kameralla (Herzberg & Leibowitz, 2016). Tämä nopeuttaa ja helpottaa prosessia ja sitä kautta parantaa käytettävyyttä.

# 7 Viestimien tietoturvaominaisuudet

Markkinoilla on useita pikaviestimiä, jotka lupaavat samankaltaisia tietoturva-ominaisuuksia. Lähemmässä tarkastelussa voidaan kuitenkin todeta, että niiden toteutuksissa on olennaisia eroja. Olennainen ero on se, voidaanko totetus tarkistaa ulkopuolisen asiantuntijan toimesta. Esimerkiksi WhatsApp käyttää oman ilmoituksensa mukaan Signa-protokollaan perustuvaa salausta, mutta käyttäjä ei voi varmistua väitteen

paikkaansapitävyydestä. Taulukossa 5 vertaillaan pikaviestimien keskeisiä ominaisuuksia. Yhteenvetona voidaan todeta, että kaikki vertailussa mukana olevat viestimet tarjoavat vähintään viestien salauksen palvelimen ja asiakasohjelman välillä. Suurimmat erot pikaviestimien välillä ovat päästä päähän -salaus, lähdekoodin avoimuus ja salausmenetelmien tarkastus ulkopuolisen tahon toimesta.

Taulukko 5. Pikaviestimien tietoturvaominaisuudet (Sutikno et al., 2016).

| **Ominaisuus** | **WhatsApp** | **Telegram** | **Telegram (Secret Chat)** | **Signal** |
|---|---|---|---|---|
| Viestit salattu palvelimen ja asiakasohjelman välillä | √ | √ | √ | √ |
| Palveluntarjoaja ei voi lukea viestejä (E2E-salaus) | √ | - | √ | √ |
| Kontaktin henkilöllisyyden varmistus | √ | - | √ | - |
| Edistynyt henkilöllisyyden varmistus (esim. QR-koodin skannaus) | √ | √ | √ | √ |
| Vanhat viestit turvassa tietomurron sattuessa | √ | - | √ | √ |
| Avoin lähdekoodi asiakasohjelmassa | - | √ | √ | √ |
| Avoin lähdekoodi palvelimella | - | - | - | - |
| Kryptografia hyvin dokumentoitu | - | √ | √ | √ |
| Ulkopuolinen tarkastus | √ | √ | √ | √ |

## 7.1 Viestien salaus

Kaikissa tutkimuksessa mukana olleissa viestimissä oli jonkinlainen automatisoitu viestien salaus, mikä toimii hyvin yleisintä uhkakuvaa, eli kohdentamantonta joukkoseurantaa vastaan. Signal erottuu joukon parhaana, sillä sen viestien salaus on auditoitu ja todettu toimivaksi. Signalin asiakasohjelman toiminta on mahdollista tarkistaa lähdekoodia tutkimalla.

Kaikkien pikaviestimien, kuten Telegramin tai WhatsAppin koko toimintaa ei voida arvioida, koska lähdekoodi ja muut toteutuksen yksityiskohdat eivät ole saatavilla. Osa viestimistä tarjoaa myös edistyneempiä ominaisuuksia, kuten käyttäjien varmentamisen merkkijonoa vertailemalla tai skannaamalla QR-koodi toisen käyttäjän laitteelta.

### 7.2 Tietoturvaominaisuuksien käytettävyys

Kaikkien viestimien käytettävyydessä havaittiin kriittisiä ongelmia (Herzberg & Leibowitz, 2016). Ainoastaan Telegramissa päästä-päähän salauksen käyttöönotto vaati käyttäjältä toimenpiteitä, muissa opportunistinen salaus luodaan automaattisesti. Tunnistautumisen käytettävyys taas oli riittämätöntä (Herzberg & Leibowitz, 2016). Maallikot eivät ymmärrä miksi heidän pitäisi suorittaa tunnistautumisoperaatio, mitä siihen liittyvät ilmoitukset tarkoittavat, tai miten niihin pitäisi reagoida. Myös itse tunnistautumisoperaatiot ovat vaikekäyttöisiä ja virheherkkiä. Herzberg ja Leibowitz (2016) esittävät parannusehdotuksiksi yksinkertaistamista ja läpinäkyvyyden lisäämistä. Esimerkiksi tunnistautumisen tarve ja sen suorittamatta jättämisen seuraukset pitäisi kommunikoida nykyistä paremmin käyttäjille. Myös mahdollisuus valita tietoturvan taso keskustelukumppanin mukaan tapauskohtaisesti parantaisi käytettävyyttä (Herzberg & Leibowitz, 2016). Tunnistautumisen ongelmiin ehdotetaan yhtenä ratkaisuna pelillistämistä, joka tekisi operaatiosta mukavamman ja vähemmän virheherkän kuin pelkkien merkkijonojen vertailu (Herzberg & Leibowitz, 2016).

## 8 Esteet tietoturvan omaksumisessa

Käyttäjäryhmien sirpaloituminen ja viestimien keskinäinen yhteensopimattomuus ovat olennaisia ongelmia erityisesti pikaviestimien keskuudessa (Abu-Salma et al., 2017; Bala & Wasilczyk, 2017). Salatun sähköpostin etuna on yhteensopivuus tavallisen sähköpostin kanssa, jolla on jo vakiintunut asema. Käytännössä kuitenkin sähköpostisalauksen, kuten PGP, vaatima tietotaito on estänyt sen laajamittaisen yleistymisen (Whitten & Tygar, 1999). Käyttäjän näkökulmasta turvalliseen viestintään liittyykin edelleen olennaisia käytettävyysongelmia.

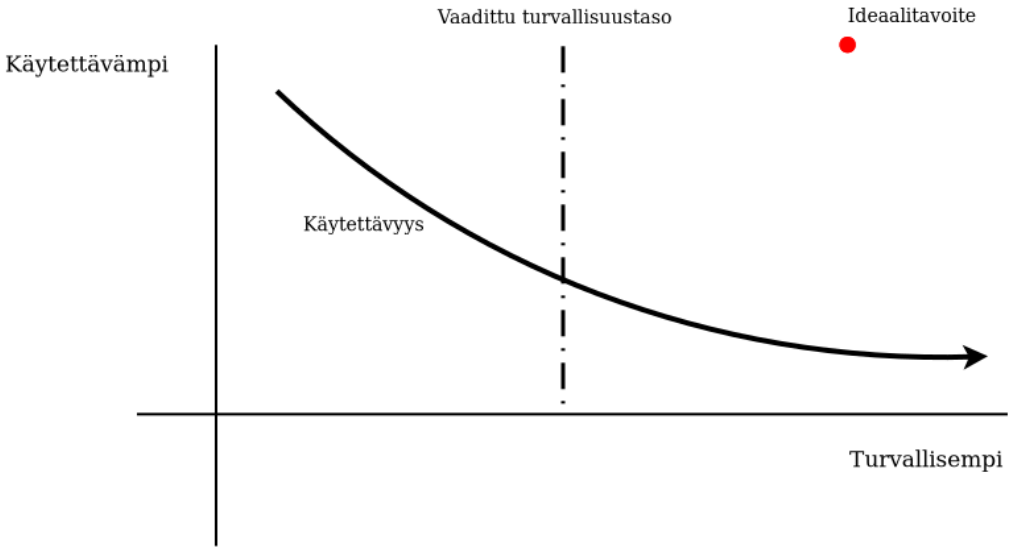
Käyttäjät ovat osin tietoisia yksityisyyden haasteista, mutta tilanne voidaan kokea liian lannistavana, vaikeana ja monimutkaisena jotta sille olisi mahdollista tehdä

mitään. Käyttäjät jatkavat viestimien käyttöä tiedostamistaan epäkohdista huolimatta, koska eivät näe tilanteen muuttamista realistisena. Dencik ja Cable (2017) nimittävät tätä suhtautumista *valvontarealismiksi*. Myös Gerber ja muut (2019) löysivät saman ilmiön omassa tutkimuksessaan. Käyttäjät kokevat joutuvansa valitsemaan yksityisyyden ja ihmissuhteiden ylläpitämisen välillä. Useimmat kokevat yhteydenpidon sosiaalisen piirinsä kanssa niin tärkeäksi, että ovat valmiita hyväksymään haittoja siinä onnistuakseen. Vaikuttaa siltä, että käyttäjät ovat taipuvaisempia valitsemaan vaihtoehdon, joka ei vaadi heiltä vaivannäköä, eli he luopuvat mieluummin yksityisyydestään kuin ponnistelisivat ottaakseen käyttöön tietoturvallisempia viestimiä (Dencik & Cable, 2017; Endeley, 2019).

Volkamerin ja muiden (2015) tutkimuksessa kävi ilmi myös, että käytettävällä laitteella oli vaikutusta suhtautumiseen. Osa käyttäjistä piti älypuhelimia nimenomaisesti puhelimina, eikä samantyyppisinä laitteina kuin kannettavia tai pöytämallisia tietokoneita. Tietokoneet nähtiin työvälineinä ja tärkeiden asioiden hoitamisen välineinä, mutta pääosin viestintään käytettäviin mobiililaitteisiin ei suhtauduttu samalla vakavuudella. (Volkamer et al., 2015)

Jos tietoturva vaatii käyttäjältä aktiivisia toimenpiteitä, sen koetaan usein haittaavan pääasiallista toimintaa, kuten viestin lähettämistä. Käyttäjät eivät myöskään ole yleisesti ottaen tietoisia viestien salauksen tarkasta toiminnasta, eivätkä luota pikaviestimien tarjoamaan tietoturvaan, jolloin sen käyttöönottoa ei nähdä erityisen hyödyllisenä (Gerber et al., 2018). Käytettävyys ja tietoturva näyttäytyvät kilpailevina tavoitteina. Tietoturvan lisääminen kuormittaa käyttäjiä huomattavasti, mikä heikentää järjestelmien käytettävyyttä olennaisesti (Theofanos, 2020). Maallikoiden näkökulmasta hyvä käytettävyys tarkoittaa sitä, että heiltä ei vaadita erityistä perehtymistä ja syvällistä ymmärtämistä seikoista, jotka eivät liity mitenkään ensisijaisen tavoitteen suorittamiseen. Tietoturvan parantaminen kuitenkin vaatii viitseliäisyyttä suorittaa oikeita toimia turvallisuuden parantamiseksi. Kaikki käyttäjät, jopa itse asiantuntijat ovat vaarassa lipsua hyvistä käytännöistä, sillä monimutkaisten järjestelmien käyttö muiden velvollisuuksien lisäksi on vaativaa ja voi aiheuttaa uupumusta (Benenson et al., 2015). Tämä voi näkyä huomion herpaantumisena ja pyrkimyksenä kognitiivisen kuorman vähentämiseen, kuten ilmoitusten ja varoitusten hyväksyminen lukematta, tai samojen salasanojen käyttönä useassa eri kohteessa (Benenson et al., 2015).

Kuvassa 2 esitetään yleistetty malli käytettävyyden ja turvallisuuden suhteesta tietojärjestelmissä. Kuva on koostettu useista eri lähteistä, joissa käsitellään tietoturvan asettamien vaatimusten vaikutusta käytettävyyteen (Abu-Salma et al., 2017; Benenson et al., 2015; Herzberg & Leibowitz, 2016a; Orman, 2015; Theofanos, 2020). ISO 9241-11 -standardin (SFS-EN ISO 9421-11, 2018) mukaan käytettävyys tarkoittaa sitä, että käyttäjä saavuttaa tavoitteensa tehokkaasti ja tyydyttävästi. Kuvan 2 yhteenvedossa käytettyjen lähteiden mukaan tietoturva nähdään pääasiallista tavoitetta haittaavana hidasteena, joka aiheuttaa turhautumista, kuormitusta ja epätietoisuutta. Turvallisuus voi vaatia esimerkiksi salasanojen vaihtamista määrävälein tai keskustelukumppanin identiteetin varmistamista. Näin ollen tosimaailman sovelluksissa on vaikea päästä ideaalitavoitteeseen, jossa viestintävälinä olisi erittäin turvallinen, mutta tästä ei aiheutuisi mitään haittaa tai lisätyötä käyttäjälle. Ideaalitavoite on esitetty pisteenä kuvan 2 oikeassa yläkulmassa, missä sekä käytettävyys, että turvallisuus ovat mahdollisimman suuret. Kuvassa 2 on asetettu prioriteetiksi tietyn vaaditun turvallisuustason saavuttaminen, mikä käytännössä määrittää käytettävyyden maksimitason. Tietoturvan vaatimat toimenpiteet koetaan usein lisätaakkana, joka haittaa varsinaisen tavoitteet saavuttamista, kuten viestien lähettämistä.




Kuva 2. Käytettävyyden ja turvallisuuden suhde

# 9 Keskustelu

Tulosten perusteella näyttää siltä, että hyvien tietoturvakäytänteiden noudattaminen vaatii käyttäjiltä vahvaa motivaatiota. Useimmat käyttäjät priorisoivat pääasiallisen tavoitteensa, joka on viestien lähettäminen mahdollisimman helposti. Viestimien käytön hyöty nähdään suurempana kuin mahdollinen yksityisyyden menetys.

Vaikka yksittäiset tietoturvan vaatimat toimenpiteet eivät olisi liian kuormittavia yksinään, niistä saattaa muodostua erittäin vaativia kokonaisuus. Yhdellä henkilöllä on usein hoidettavanaan sekä yksityinen tietoturvansa, sekä työ- tai opiskelupaikan vaatimukset. Erittäin moni tietotekniikkaa hyväksikäyttävä asia vaatii vähintään salasanojen hallintaa. Sähköposti, pikaviestimet, pankkiasiat, työ- ja opiskelupaikkojen järjestelmät vaativat kaikki salasanojen käyttöä. Hallittavia salasanoja saattaa olla satoja, joten monet käyttävät samaa salasanaa kaikkialla, vaikka tietävät sen olevan huono käytäntö (Theofanos, 2020). Useimmat käyttäjät kuitenkin priorisoivat helppokäyttöisyyden hyvin korkealle. Jos viestien salaus ei ole vakio-ominaisuus vaan vaatii erillistä viitseliäisyyttä, sitä ei oteta käyttöön. Tietoturvan parantaminen jää siis palveluntarjoajien vastuulle ja se on toteutettava käyttäjistä huolimatta. Mikäli tietoturvaominaisuudet ovat tarpeeksi helppokäyttöisiä, voidaan olettaa, että käyttäjät eivät lopeta viestimien käyttöä, vaan mukautuvat tilanteeseen. Vaikuttaa myös siltä, että turvallisuus on positiivinen asia viestimien markkinoinnissa, kunhan se ei vaadi käyttäjiltä ylimääräisiä toimia. Pelkkä opportunistinen salaus parantaa tietoturvaa merkittävästi maallikkokäyttäjän käyttöskenaarioissa.

Tietämättömyys ja virheelliset oletukset ovat suuri este salauksen yleistymiselle (Abu-Salma et al., 2017). Käyttäjät eivät ole valmiita näkemään vaivaa lisäturvaominaisuuden käyttämiseksi, jos he eivät usko niiden toimivan. On kuitenkin nähtävissä viiteitä siitä, että käyttäjät ovat valmiita panostamaan tietoturvaan tietyissä tilanteissa, kuten aivan lähipiirinsä kanssa kommunikoidessa. Samaa vaivaa ei olla valmiita näkemään satunnaisempien ja etäisempien osapuolien kanssa viestiessä. Näin ollen olisikin olennaista, että käyttäjät voivat valita halutun tietoturvan tason, niin että käytetty panostus pysyy kohtuullisella tasolla. Käytäntö, jossa salaus on automaattisesti käytössä ja käyttäjät voivat varmistaa toistensa henkilöllysyyden halutessaan, vaikuttaisi olevan käyttökelpoinen kompromissi.

Pikaviestimien epäyhteensopivuus on vakava ongelma. Toistaiseksi pikaviestimillä ei ole sähköpostia vastavaa, universaalisti käytössä olevaa, yhteensopivaa protokollaa. Yksi aikasemmista yrityksistä luoda yleinen ja avoin protokolla on Jabber-pikaviestimessä käytetty XMPP (Bala & Wasilczyk, 2017). Muun muassa Google, WhatsApp ja Facebook ovat käyttäneet XMPP-protokollan eri versioita omissa palveluissaan (Watkin & Koelle, 2016). Palveluntarjoajat eivät kuitenkaan ole käyttäneet standardoitua versiota, vaan kehittäneet omia muunnelmiaan ja lopettaneet XMMP-protokollan tukemisen palveluissaan.

Kehitteillä on kuitenkin uusia projekteja, joiden yhtenä tavoiteena on ehkäistä käyttäjäkannan sirpaloitumista. Uusimpia projekteja on The Matrix.org Foundationin avoimen lähdekoodin Matrix-protokolla, joka tarjoaa kehittäjille mahdollisuuden luoda sähköpostin tapaan yhteensopiva kommunikaatioverkosto (Matrix, 2021). Matrixilla ei ole rajoittavia lisenssejä, vaan protokolla on vapaasti kaikkien käytettävissä ja kuka tahansa voi tehdä muiden Matrix-toteutusten kanssa yhteensopivan sovelluksen. Tämä mahdollistaa viestinnän kaikilla laitteilla, joilla sähköpostikin toimii. Matrix tarjoaa myös kehittyneitä turvallisuusominaisuuksia ja sen käyttämät avoimet Olm- ja Megolm salausmenetelmät ovat Signalin tavoin auditoituja ja toimiviksi arvioituja (Cohn-Gordon et al., 2017; Hodgson & van der Hoff, 2016). Alustariippumattomuus on erittäin tärkeä tekijä viestintäprotokollan käyttökelpoisuuden kannalta. Sähköposti on edelleen yleisesti käytössä, vaikka sen tietoturvaominaisuudet, kuten PGP, eivät ole koskaan levinneet enemmistön käyttöön. Viestimen tulisikin toimia kaikilla yleisimmillä alustoilla, kuten Android, iOS, Windows, Linux ja macOS. Useimmat pikaviestimet tarjoavat jonkinlaisen web-version, vaikka natiivia sovellusta ei olisi saatavilla. Tämä ei kuitenkaan ole optimaalinen tilanne, sillä natiivien sovelluten puute lisää käyttäjäkunnan sirpaloitumista.

# 10 Yhteenveto

Tutkimuksen tuloksena oli, että paremmalle tietoturvalle ja yksityisyydelle on olemassa perusteltu tarve. Maallikkokäyttäjät eivät kuitenkaan ole tietoisia asiasta, tai eivät ole motivoituneita paneutumaan yksityisyydensuojaan ja tietoturvaan. Lisäksi käyttäjillä on paljon täysin vääriä käsityksiä salauksesta ja sen toiminnasta.

Kaikki yleisimmät pikaviestimet tarjoavat jonkinlaisen salauksen, osa jopa erittäin hyvin toteutetun. Automaattisesti toimiva salaus, joka ei vaadi käyttäjältä toimenpiteitä, parantaa tietoturvaa olennaisesti. Maallikkokäyttäjän kannalta suurin yksityisyydenuhka on passiivinen joukkoseuranta, jota vastaan päästä-päähän salaus toimii hyvin. Edistyneemmät tietoturvaominaisuudet, kuten käyttäjien identiteetin varmistus, ovat edelleen liian vaikeakäyttöisiä ja asiantuntemusta vaativia, jotta maallikot voisivat käyttää niitä onnistuneesti.

Pikaviestimien käytettävyydessä on edelleen kehittämistä. Niihin kaivataan selkeyttä ja läpinäkyvyyttä, jotta käyttäjät voivat muodostaa riittävän tilannekuvan ilman asiantuntijatasoista kokemusta. Käyttäjäkannan sirpaloituminen monien yhteensopimattomien viestimien kesken on suuri ongelma ja hidastaa parhaiden tietoturvaominaisuuksien yleistymistä.

## Lähdeluettelo


Butterfield, A., Ngondi, G. E., & Kerr, A. (2016). A Dictionary of Computer Science. *Oxford University Press.* http://10.1093/acref/9780199688975.001.0001.

Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017). Obstacles to the adoption of secure communication tools. *2017 IEEE Symposium on Security and Privacy (SP), 137–153.* https://doi.org/10.1109/SP.2017.65.

Bala, S., & Wasilczyk, T. (2017). Secure integration of multiprotocol instant messenger. *2017 IEEE International Conference on INnovations in Intelligent SysTems and Applications (INISTA), 495–500.* https://doi.org/10.1109/INISTA.2017.8001210

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: rethinking the impact of surveillance. *International Political Sociology, 8(2), 121–144.* https://doi.org/10.1111/ips.12048.

Benenson, Z., Lenzini, G., Oliveira, D., Parkin, S., & Uebelacker, S. (2015). Maybe poor Johnny really cannot encrypt: the case for a complexity theory for usable security. *Proceedings of the 2015 New Security Paradigms Workshop, 85–99.* https://doi.org/10.1145/2841113.2841120.

Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L., & Stebila, D. (2017). A formal security analysis of the Signal messaging protocol. *2017 IEEE European Symposium on Security and Privacy (EuroS P), 451–466.* https://doi.org/10.1109/EuroSP.2017.27.

Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man In The Middle Attacks. IEEE Communications Surveys Tutorials, 18(3), 2027–2051. https://doi.org/10.1109/COMST.2016.2548426.

Dechand, S., Naiakshina, A., Danilova, A., & Smith, M. (2019). In encryption we don't trust: the effect of end-to-end encryption to the masses on user perception. *2019 IEEE European Symposium on Security and Privacy (EuroS P), 401–415.* https://doi.org/10.1109/EuroSP.2019.00037.

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: public opinion and activist responses to the snowden leaks. *International Journal of Communication (19328036), 11, 763–781*.

Effi ry – Electronic Frontier Finland. (2020). *Lehdistötiedote:* Turvallista, yksityisyyttä suojaavaa, päästä päähän salattua viestintää. https://effi.org/turvallista-yksityisyytta-suojaavaa-paasta-paahan-salattua-viestintaa (Haettu 1.11.2020).

Endeley, R. E. (2019). End-to-end Encryption, Backdoors, and Privacy. *T.D., Capitol Technology University. In ProQuest Dissertations and Theses*. http://search.proquest.com/publiccontent/docview/2309795255/abstract/85135EA95FCF4BFCPQ/1

Fuchs, C., & Trottier, D. (2017). Internet surveillance after snowden: a critical empirical study of computer experts' attitudes on commercial and state surveillance of the internet and social media post-Edward Snowden. *Journal of Information, Communication and Ethics in Society, 15(4), 412–444.* https://doi.org/10.1108/JICES-01-2016-0004.

Gerber, N., Zimmermann, V., Henhapl, B., Emeröz, S., & Volkamer, M. (2018). Finally Johnny can encrypt: but does this make him feel more secure? *Proceedings of the 13th International Conference on Availability, Reliability and Security, 1–10.* https://doi.org/10.1145/3230833.3230859.

Gerber, N., Zimmermann, V., & Volkamer, M. (2019). Why Johnny fails to protect his privacy. *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), 109–118.* https://doi.org/10.1109/EuroSPW.2019.00019.

Herzberg, A., & Leibowitz, H. (2016). Can Johnny finally encrypt? evaluating e2e-encryption in popular IM applications. *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust, 17–28.* https://doi.org/10.1145/3046055.3046059.

Hodgson, M., & van der Hoff, R. (2016). Olm Cryptographic Review. *NCC Group Security Services, Inc*. www.nccgroup.com/globalassets/our-research/us/public-reports/2016/november/ncc_group_olm_cryptogrpahic_review_2016_11_01.pdf (Haettu 08.06.2021).

Ince, D. I. (2013). Kerchoff's principle. A Dictionary of the Internet. *Oxford University Press.* http://www.oxfordreference.com/view/10.1093/acref/9780191744150.001.0001/acref-9780191744150-e-4506 (Haettu 3.3.2021).

Kerckhoffs, A. (1883). La Cryptographie Militaire (Seconde partie). *Journal des sciences militaires, IX, 5–38.*

Kyberturvallisuuskeskus. (2021). Tietoturva. www.kyberturvallisuuskeskus.fi (Haettu 20.06.2021).

Malekhosseini, R., Hosseinzadeh, M., & Navi, K. (2018). Evaluation of users' privacy concerns by checking of their WhatsApp status. *Software: Practice & Experience, 48(5), 1143–1164.* https://doi.org/10.1002/spe.2565.

Matrix. (2021). Frequently Asked Questions. www.matrix.org (haettu 19.06.2021).

Molyneaux, H., Stobert, E., Kondratova, I., & Gaudet, M. (2020). Security matters … until something else matters more: security notifications on different form factors. *In A. Moallem (Ed.), HCI for Cybersecurity, Privacy and Trust (pp. 189–205). Springer International Publishing.* https://doi.org/10.1007/978-3-030-50309-3_13.

Murata, K., Adams, A. A., & Lara Palma, A. M. (2017). Following Snowden: a cross-cultural study on the social impact of Snowden's revelations. J*ournal of Information, Communication & Ethics in Society; Bingley, 15(3), 183–196.*

NIST. (2021). *Glossary.* The National Institute of Standards and Technology. Information Technology Laboratory, Computer Security Resource Center. https://csrc.nist.gov/glossary (Haettu 21.06.2021).

Orman, H. (2015). Why won't Johnny encrypt? *IEEE Internet Computing, 19(1), 90–94.* https://doi.org/10.1109/MIC.2015.16.

OTR. (2021). *Off-the-record Messaging.* https://otr.cypherpunks.ca/ (Haettu 24.06.2021).

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM, 58(5), 48–55.* https://doi.org/10.1145/2663341.

Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). Why doesn't Jane protect her privacy? *In E. De Cristofaro & S. J. Murdoch (Eds.), Privacy Enhancing Technologies (pp. 244–262). Springer International Publishing.* https://doi.org/10.1007/978-3-319-08506-7_13.

Rikoslaki 39/19.12.1889, *38 luku § 3:* Viestintäsalaisuuden loukkaus https://finlex.fi/fi/laki/ajantasa/1889/18890039001 (Haettu 15.10.2020).

SFS-EN ISO 9421-11. 2018. Ergonomics of human-system interaction. Part 11: usability: definitions and concepts. *Suomen Standardoimisliitto SFS ry. (ISO 9241-11:2018).* https://online-sfs-fi (Haettu 26.02.2021).

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal, 28(4), 656–715.* https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.

Stedman, R., Yoshida, K., & Goldberg, I. (2008). A user study of off-the-record messaging. *Proceedings of the 4th Symposium on Usable Privacy and Security, 95–104.* https://doi.org/10.1145/1408664.1408678.

Suomen perustuslaki 731/1.6.1999, *2 luku 10 §:* Yksityiselämän suoja. https://finlex.fi/fi/laki/ajantasa/1999/19990731 (Haettu 15.10.2020).

Sutikno, T., Handayani, L., Stiawan, D., Riyadi, M. A., & Subroto, I. M. I. (2016). Whatsapp, Viber and Telegram: which is best for instant messaging? *International Journal of Electrical and Computer Engineering; Yogyakarta, 6(3), 909–914.*

Theofanos, M. (2020). Is usable security an oxymoron? *Computer, 53(2), 71–74.* https://doi.org/10.1109/MC.2019.2954075.

Thimbleby, H. (2016). Human factors and missed solutions to Enigma design weaknesses. *Cryptologia, 40(2), 177–202.* https://doi.org/10.1080/01611194.2015.1028680.

Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I., & Smith, M. (2015). Sok: secure messaging. *2015 IEEE Symposium on Security and Privacy, 232–249.* https://doi.org/10.1109/SP.2015.22.

Volkamer, M., Renaud, K., Kulyk, O., & Emeröz, S. (2015). A socio-technical investigation into smartphone security. *In S. Foresti (Ed.), Security and Trust Management (pp. 265–273). Springer International Publishing.* https://doi.org/10.1007/978-3-319-24858-5_17.

Watkin, L., & Koelle, D. (2016). Practical XMPP. *Packt Publishing.*

WhatsApp. (2020) *Blog:* Two billion users -- connecting the world privately. https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately (Haettu 28.10.2020).

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: a usability evaluation of PGP 5.0. *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8, 14.*