OULUN AMMATTIKORKEAKOULU

Markku Korkiakoski

Muuttuva viranomaislaajakaista

Päätelaitteen tietoturva

Muuttuva viranomaislaajakaista

Päätelaitteen tietoturva

Markku Korkiakoski
Opinnäytetyö
Syksy 2016
Teknologialiiketoiminnan tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Teknologialiiketoiminnan tutkinto-ohjelma

Tekijä: Markku Korkiakoski
Opinnäytetyön nimi: Muuttuva viranomaislaajakaista - Päätelaitteen tietoturva
Työn ohjaaja: Hannu Päätalo
Syksy 2016 Sivumäärä: 57 + 2

Opinnäytetyö kuvaa viranomaisviestinnässä käytetyn teknologian murrosta ja sen mukanaan tuomia haasteita. Se pyrkii lähestymään valittua aihetta kaupallisen teknologian ja siihen pohjautuvan teorian kautta. Opinnäytetyön tavoitteena on tuoda esille toisaalta nykyisten päätelaitteiden haavoittuvuudet ja toisaalta pyrkiä vastaamaan mahdolliseen huoleen uusien päätelaitteiden tietoturvatason riittämättömyydestä viranomaislaajakaistassa. Osana kokonaisuutta käsitellään myös yleisesti erilaisia vaihtoehtoja viranomaislaajakaistan toteuttamiseen ja näiden mahdollista vaikutusta kokonaisratkaisuun.

Lähestyminen on pohdiskeleva ja teknisen ratkaisun sijaan opinnäytetyö esittää keskeisten riskien hallintaan soveltuvaa menettelyä ja pyrkii tuomaan esille kokonaiskuvan ongelmanratkaisun tueksi. Opinnäytetyö käsittelee uhkakuvien kenttää yleisesti, eikä ole myöskään tarkoituksen mukaista syventyä jokaiseen mainittuun uhkakuvaan laaja-alaisesti esittämällä yksityiskohtaisia varautumismenetelmiä kuhunkin haasteeseen.

Opinnäytetyö hyödyntää lähdemateriaalia sekä kaupallisista teknologioista että myös viranomaiskentästä. Opinnäytetyö esittää keskeisimmät pääkohdat turvallisempaan kommunikaatiomalliin ja pyrkii myös tuomaan esille mahdolliset osa-alueet, jotka tarvitsevat lisäselvityksiä.

Avainsanat: LTE, Viranomaisviestintä, Päätelaite

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Industrial Management

Author: Markku Korkiakoski
Title of thesis: Mobile Broadband in Public Safety – Security in Handheld
Supervisor: Hannu Päätalo
Fall 2016 Number of pages: 57 + 2

This Master's Thesis aims to describe the change that is happening in Public Safety communication globally. Traditionally, public safety communities have learned to trust the voice centric communication, provided through narrowband technology. Now these same communities have noticed also the limitations of current technology and are planning to utilize new and enhanced possibilities of broadband data. This thesis covers the basics of the evolution in mobile communication as well as the basics of technologies currently used in public safety communication. This is essential for readers to better understand the magnitude of change that broadband data is bringing in to public safety users. Focus of the thesis is still in the security threats and potential mitigation approaches of those. Threats and mitigations are mainly brought from studies carried out in consumer segment but also public safety perspective is present.

Instead of focusing on the deep technical solutions for each possible threat, this thesis aims to provide more holistic view. It is crucial to understand that security is holistic approach and not something that can be added later. This "security by design" is also the main outcome of this thesis. It is important for readers to understand the main differences between the two segments, consumer and public safety. Where consumer can decide where and how to access the data, the public safety user is bound to observe the security policy their organization hopefully have. Together with added security in the device, this policy is one key element in holistic security approach.

As an outcome, this thesis also tries to emphasize the importance of future studies in public safety segment.

Keywords: LTE, Public Safety, Broadband

SISÄLLYS

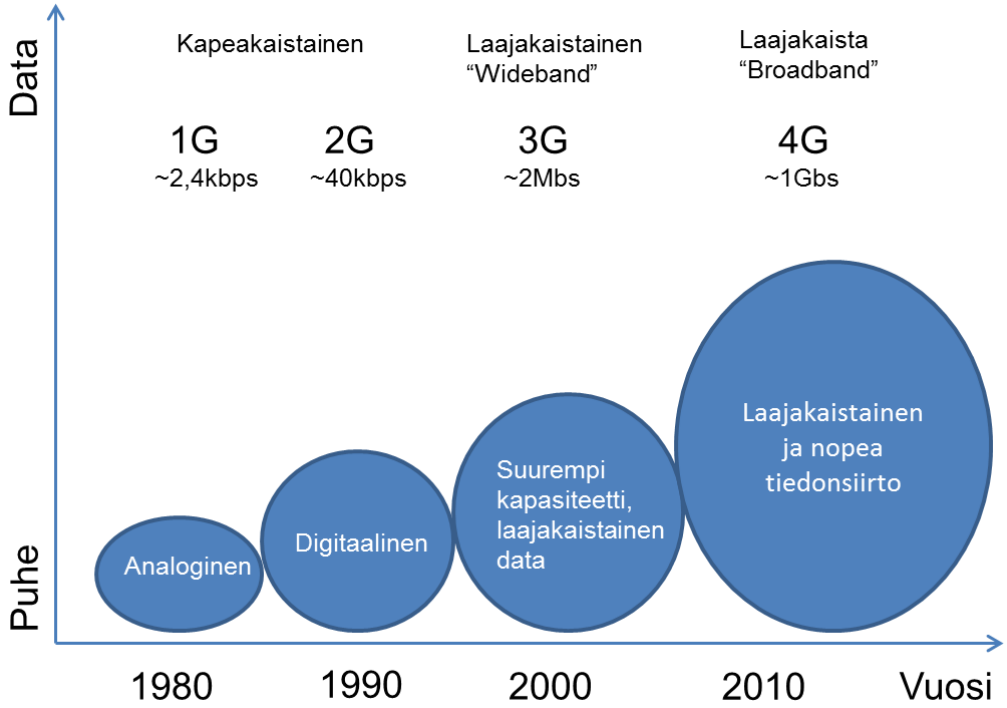
LYHENTEET

3GPP	3rd Generation Partnership Program
AAA	Authentication – Authorization – Accounting
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
CCBG	Critical Communications Broadband Group
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DMO	Direct mode operation
DoS	Denial of Service
E2E	End to End
EAP	Extensible authentication protocol
ENISA	European Union Agency for Network and Information Security
ESMCP	Emergency Services Mobile Communications Programme
EPS	Evolved Packet System
ESN	Emergency Services Network
ETSI	European Telecommunications Standards Institute
ETL	ENISA Threat Landscape
FCC	Federal Communications Committee
FDMA	Frequency Division Multiple Access
FICORA	Finnish Communications regulatory authority
HPUE	High Power User Equipment
HST	Henkilön Sähköinen tunnistaminen
IP	Internet Protocol
LMR	Land Mobile Radio
LTE	Long Term Evolution
MCPTT	Mission Critical Push To Talk
NATO	North Atlantic Treaty Organization
P25	Project 25

PIN	Personal Identification number
Prose	Proximity services
SHA	Secure hash algorithm
TCCA	TETRA and Critical Communications Association
TDMA	Time Division Multiple Access
TEE	Trusted Execution Environment
TETRA	Terrestrial Trunked Radio
Ue	User equipment
UICC	Universal Integrated Circuit Card

1 JOHDANTO

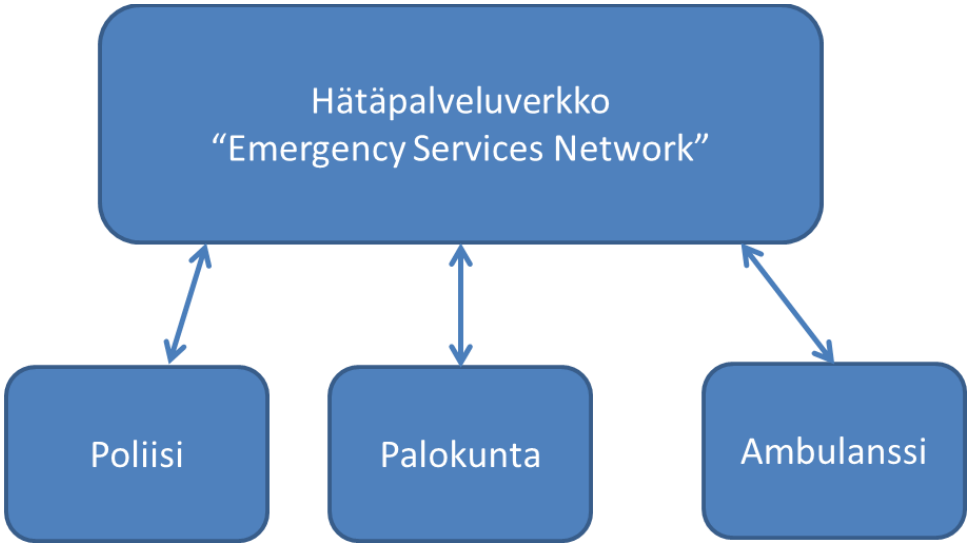
Langaton kommunikaatioteknologia on kehittynyt vuosien saatossa niin kuluttajilla kuin viranomaisillakin. Alkujaan pelkästään puheen siirtämiseen tarkoitetut järjestelmät ovat, varsinkin viime aikoina, kehittyneet voimakkaasti datakeskeisiin palveluihin. Tästä kehityksestä hyvänä esimerkkinä voidaan käyttää matkapuhelimia ja niiden kehityskaarta.



KUVA 1. Matkapuhelinkommunikaation evoluutio (Fumiuki 2001, 57)

Kuvasta 1 voimme todeta tiedonsiirtokapasiteetin kasvaneen huomattavasti eri kehitysasteiden välillä. Tämä kehitys on mahdollistanut esimerkiksi matkapuhelimen kehityksen pelkästään puhepohjaisesta teknologiasta aina nykyisiin älypuhelimiin. Tähän kehitykseen on vaikuttanut eri palveluiden, kuten internetin, saatavuus kannettaviin päätelaitteisiin. Samalla päätelaitteet ovat monimuotoistuneet ja mahdollistavat erilaisten, innovatiivisten käyttötapausten luomisen. Hyvänä esimerkkinä uudenlaisesta käyttötapauksesta voidaan mainita paikannusteknologian hyödyntäminen peleissä (Wikipedia, Pokémon Go 2016).

Tässä opinnäytetyössä keskitytään langattoman teknologian yhteen erityisalueeseen, viranomaisviestintään. Ja sen alla erityisesti osa-alueeseen, joka kattaa niin kutsutun hätäpalveluverkon (Kuva 2)



KUVA 2. Opinnäytetyön tarkastelualue viranomaisviestinnässä (Emergency Service Network, ESN)

Viranomaisviestintä on tässä valitussa kohderyhmässä tähän saakka toteutettu kapeakaistaisilla ja yleensä viranomaisille suunnitelluilla teknologioilla. Näiden teknologioiden päätarkoitus on mahdollistaa sekä turvallinen kommunikaatio (ryhmäkommunikaatio ja myös ilman verkkoa tapahtuva kommunikaatio), että luotettava palvelu. Palvelun saatavuuden ja luotettavuuden vaatimukset viranomaisteknologioille ovat yleensä merkittävästi tiukemmat verrattuna kaupalliseen teknologiaan. Siinä missä osa kaupallisista palveluista saattaa toimia ilman saatavuustakuuta, on viranomaisille pystyttävä takaamaan palvelu myös kriisitilanteissa. Osana palveluiden luotettavuutta on kyky tarjota ratkaisuja salakuuntelua tai jopa häirintää vastaan.

Nykyiset viranomaisteknologiat ovat palvelleet käyttäjien tarpeita erittäin hyvin ja käytetyt palvelut ovat olleet joiltakin osin jopa edellä kaupallisia teknologioita. Kehitys kuluttajapuolella on kuitenkin ollut merkittävästi nopeampaa kuin viranomaisteknologioissa ja siellä pystytäänkin nykyisin tarjoamaan kokonaan uudentyyppisiä palveluita käyttäjille. Esimerkiksi sosiaalisen median myötä tilannekuvaa pystytään välittämään

tehokkaasti laajalle käyttäjäkunnalle, samalla toki sisällön merkitys ja lähdekritiikin riittävä ymmärtäminen korostuvat.

Vaikka puheen merkitys viranomaisviestinnässä on edelleen tärkeä, on sen rinnalle nousemassa uusia käyttökohteita, kuten reaaliaikainen tilannekuva, video ja erilaiset ryhmäsovellukset, unohtamatta aiemmin mainittua sosiaalisen median hyödyntämistä. Näiden palveluiden käyttö nykyisissä, kapeakaistaisissa viranomaisteknologioissa on kuitenkin osin jopa mahdotonta. Tärkeimmät tunnistetut toiminnot ja niiden vaatima kapasiteetti viranomaisverkossa voidaan jakaa esimerkiksi alla esitetyn taulukon mukaisesti (Peltola 2011, 17).

TAULUKKO 1. Viranomaiskommunikaation tärkeimmät toiminnot ja niiden kapasiteetti-tarve (Peltola 2011)

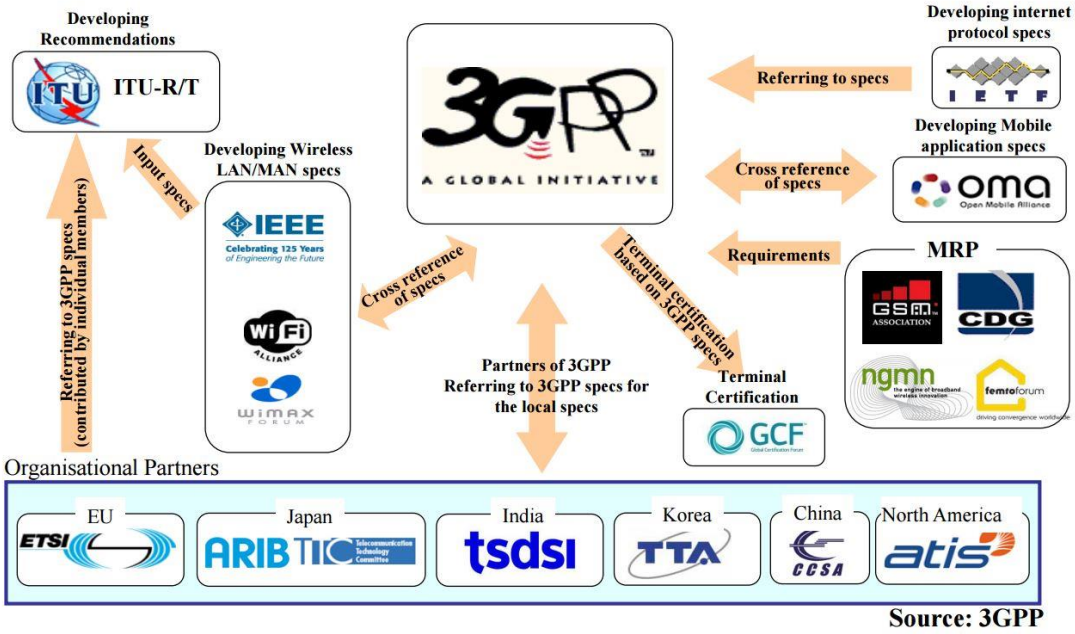
Ryhmäpuhelu	Kapeakaistainen data
Info- ja hälytysviestit	Kapeakaistainen data
Statusviestit	Kapeakaistainen data
Sähköposti	Kapea/laajakaistainen data
Paikannuspalvelu	Kapeakaistainen data
Kuvat	Kapea/laajakaistainen data
Tietokantahaut	Kapeakaistainen data
Videolähetys	Laajakaistainen/Laajakaistadata
Internet	Laajakaistadata
Tuki liikkuvalle johtamiselle ja ohjaukselle	Laajakaistainen/Laajakaistadata

Peltola toteaa tutkimuksessaan, että taulukossa 1 esitettyjä tietoja tulee arvioida myös kokonaisuuden kannalta, eikä pelkästään yksittäisen päätelaitteen näkökulmasta. Esimerkiksi paikkatiedon puolesta kapeakaistainen teknologia voi olla hyvinkin riittävä yksittäiselle päätelaitteelle, mutta järjestelmän kannalta usean päätelaitteen tuottama paikkatieto voi olla liikaa.

Viranomaisryhmittymät ja kansalliset valvontaviranomaiset ovat havahtuneet tunnistettuihin haasteisiin nykyisessä, kapeakaistaisessa teknologiassa, ja useat maat ovatkin siirtymässä kohti kaupallista laajakaistaisempaa teknologiaa. Yhtenä perusteena kaupallisen teknologian hyödyntämisessä on myös tavoiteltu kustannussäästö. Tämä peruste pohjautuu oletukseen, että kaupallisen teknologian tuomat suuret käyttäjämäärät ja avoin standardointi tuovat mukanaan halvempia päätelaitteita, edullisempia verkkoratkaisuja ja myös useampia toimijoita.

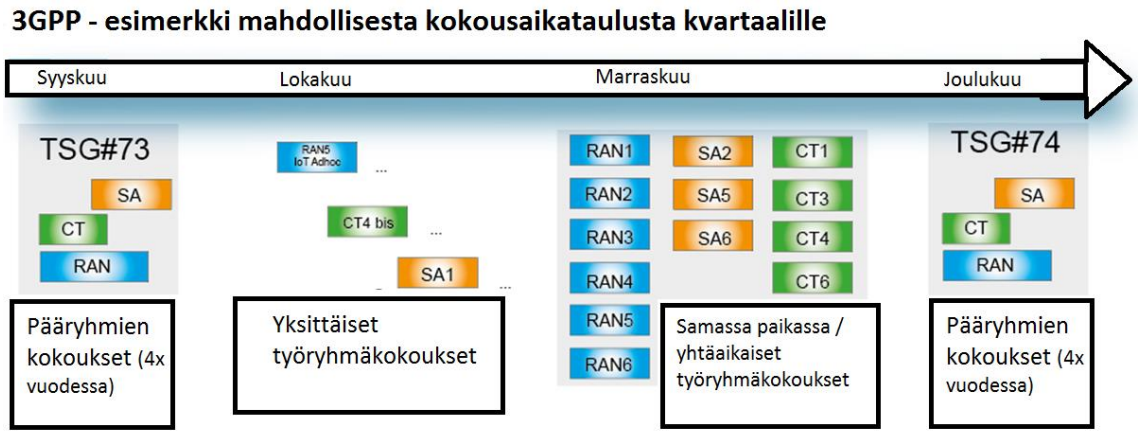
Kansainvälinen tietoliikennestandardointi on hyvin voimakkaasti keskittynyt 3GPP:n (3rd Generation Partnership Project) alle. Tämä yhteenliittymä koostuu seitsemästä telekommunikaatioon suuntautuneesta standardointijärjestöstä ja niihin kuuluvista jäsenistä. Standardointijärjestöt edustavat eri maita tai maanosia ja niistä käytetään 3GPP:n

yhteydessä lyhennettä OP (Organizational Partner). Yksittäinen jäsen voi olla mikä tahansa laillinen yritys. Näiden lisäksi 3GPP tekee yhteistyötä eri sidosryhmien kanssa, jotta standardien sisältö vastaisi paremmin loppukäyttäjien ja yhteisöiden tarpeita.



KUVA 3. 3GPP ja sen sidosryhmät (3GPP 2016, Viitattu 14.11.2016)

Kuvasta 3 käy ilmi 3GPP:n laaja sidosryhmäverkosto ja eri alueilla toimivat standardointijärjestöt. Jo pelkästään organisaatioiden lukumäärästä on helppo todeta tämän kokonaisuuden oleva hyvin laaja ja osin myös tästä johtuen 3GPP:n toimintamalli pyrkii olemaan tarkasti kontrolloitu. Jokainen uusi toiminto, joka määritellään 3GPP:ssä, sidotaan tiettyyn toimitukseen. Näistä toimituksista käytetään nimitystä Release. Releasen sisältökokonaisuus pyritään määrittelemään siten, että se muodostaa selkeän kokonaisuuden ja tyypillisesti yhden kokonaisuuden määrittelyyn varataan noin 18 kuukautta. Työ itsessään tapahtuu aihealueiden pohjalta määriteltyjen työryhmien kautta. Näiden työryhmien organisoituminen puolestaan tapahtuu sovittujen kokousten kautta. Kuva 4 esittää mahdollisen kokousaikataulun yhdelle vuosineljännekselle. Eri työryhmät on kuvassa merkitty omilla lyhenteillään, eikä niiden tarkempi avaaminen ole olennaista tämän opinnäytetyön kannalta.

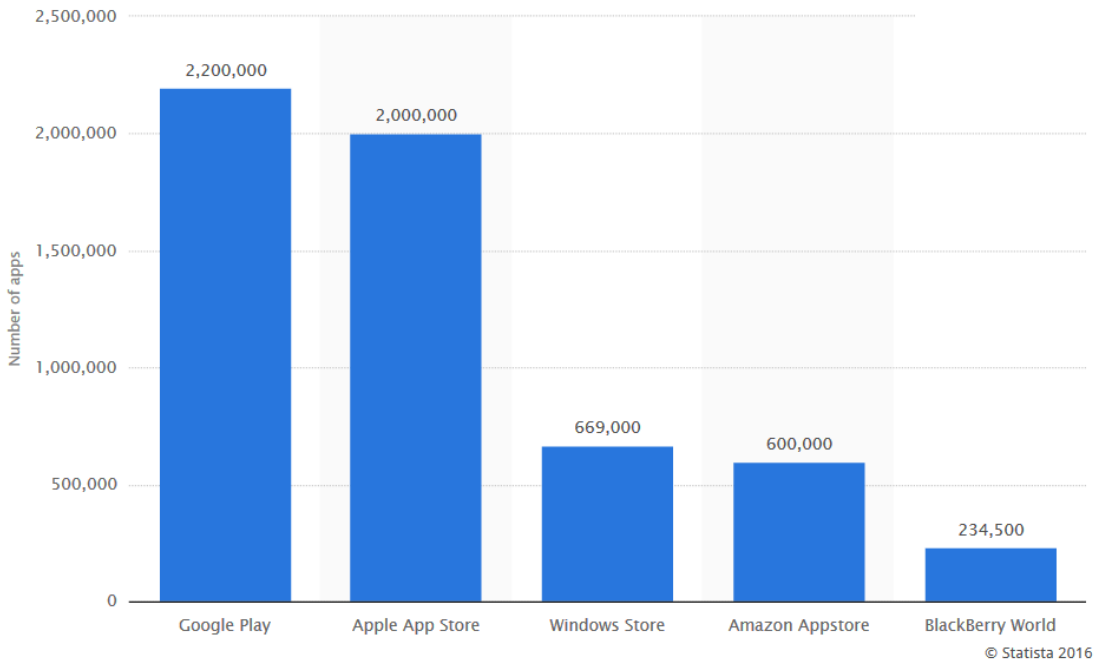


KUVA 4. Esimerkki 3GPP:n mahdollisesta kokousaikataulusta yhdelle kvartaalille (3GPP 2016, Viitattu 14.11.2016)

Vahvimpana vaihtoehtona kaupallisista teknologioista pidetään juuri 3GPP:n (3rd Generation Partnership Project) määrittelemää Long Term Evolution (LTE) teknologiaa (3GPP, 2016). LTE on ensimmäinen 3GPP:n määrittelemä 4G-teknologia. Kuten aiemmin opinnäytetyössä esitettiin, eri kehitysvaiheet kuvataan Generaatioina ”G” ja näiden eri vaiheiden, 1G – 4G, yhtenä suurimmista eroista on tiedonsiirtokyvykkyyden kasvaminen. Suurempi tiedonsiirtokyvykkyys mahdollistaa nopeampien ja myös useampien palveluiden käyttämisen. Useat maat ja viranomaisyhteisöt ovatkin jo valinneet LTE:n heidän tulevaisuuden viranomaisteknologiaksensa ja samalla toimijat ovat pyrkineet vaikuttamaan standardin kehittymiseen ja siten varmistamaan sen sopivuuden viranomaiskentässä. On syytä huomioida, että LTE on kehitetty kuluttajatuotteisiin, eikä se pidä lähtökohtaisesti sisällään viranomaisille tyypillisiä toimintoja saati vaatimuksia. Tämä lisääntynyt tarve on huomioitu 3GPP Release 11 työstä alkaen, tuomalla juuri viranomaisille suunniteltuja ominaisuuksia kaupalliseen teknologiaan. Näistä esimerkkeinä Release 11 oleva High Power UE (HPUE), joka mahdollistaa tavallista suuremman lähetystehon parantaen siten laitteen kuuluvuutta. Releaset 12 ja 13 tuovat puolestaan mukanaan Proximity Services -toiminnon (ProSe) joka mahdollistaa viranomaisille tyypillisen laitteesta laitteeseen (D2D) kommunikaation sekä verkko-ohjattuna että ilman matkapuhelinverkon kuuluvuutta. Release 13 määrittelee myös Mission Critical Push To Talk (MCPTT) toiminnon, joka vastaa nykyistä viranomaisten käytössä olevaa ryhmäpuhelua.

Siirtyminen kaupalliseen teknologiaan ei ole välttämättä suoraviivaista, vaan se tulee vaatimaan lisää merkittäviä panostuksia sekä kansainväliseen standardointiin, että kommunikaatioarkkitehtuurin ja päätelaitteisiin (Peltola 2011). Kaupallisten teknologioiden mahdollisina hyötyinä voidaan pitää niiden globaalia saatavuutta ja oletettua hintaeroa suljettuihin teknologioihin. Näiden etujen lisäksi viranomaisyhteisöjen tulee ymmärtää uuden teknologian mukanaan tuomat riskit, kuten lisääntyvä tarve tietoturvalle.

Kaupallisessa kuluttajateknologiassa päätelaitteen tietoturvasta huolehtiminen jää usein loppukäyttäjän vastuulle. Erilaiset verkkopohjaiset palvelut, sosiaalisen median ohjelmistot ja jopa pelit tuovat mukanaan kirjavan valikoiman tietoturvauhkia. Näiden lisäksi käytössä olevan käyttöjärjestelmän tuomat haavoittuvuudet tuovat oman ongelmakenttänsä kuluttajille. Eri ohjelmat vaativat käyttäjältä pääsyoikeuksia laitteen tietoihin ja hyvin usein niitä ohjelmille myönnetäänkin ilman tarpeellista harkintaa. Tämä saattaa johtaa myös tilanteeseen, jossa esimerkiksi käyttäjän päätelaitteessa olevat yhteystiedot päätyvät toisten tietämättä kolmansille osapuolille. Käyttäjälle on tarjolla valtava määrä erilaisia ohjelmia ja on usein hyvin haastavaa selvittää, mitkä ohjelmat ovat mahdollisia haittaohjelmia ja mitkä turvallisia asentaa. Kuva 5 esittää sovellusten määrän eri kauppapaikoissa.



KUVA 5: Eri ohjelmakauppojen sisältö määrällisesti kesäkuussa 2016 (Statista 2016a, Viitattu 14.11.2016)

Vaikka eri kauppapaikkojen ylläpitäjät pyrkivät valvomaan saatavilla olevien ohjelmien laatua ja niiden tietoturvaa, ohjelmien määrä kasvaa kiihtyvällä vauhdilla ja samalla myös hankaloituu ylläpitäjien valvonta.

Opinnäytetyö kuvaa nykyisen teknologiaympäristön ja antaa yleiskuvan tulevaisuuden suunnitelmista eri alueilla. Yleiskuvan sekä nykytilanteen kuvaaminen auttaa lukijaa muodostamaan käsityksen viranomaiskentän laajuudesta ja sen mahdollisista käyttäjämääristä. Tämä kokonaiskäsitys auttaa myös ongelmakentän hahmottamisessa.

2 TAVOITE JA KÄYTETYT TUTKIMUSMENETELMÄT

Opinnäytetyön tavoitteena on tuoda esille toisaalta nykyisten päätelaitteiden haavoittuvuudet ja toisaalta pyrkiä vastaamaan mahdolliseen huoleen uusien päätelaitteiden tietoturvatason riittämättömyydestä viranomaislaajakaistassa. Lähestyminen on pohdiskeleva ja teknisen ratkaisun sijaan opinnäytetyö esittää keskeisten riskien hallintaan soveltuvaa menettelyä ja pyrkii tuomaan esille kokonaiskuvan ongelmanratkaisun tueksi.
Opinnäytetyö käsittelee uhkakuvien kenttää yleisesti, eikä ole tarkoituksen mukaista syventyä jokaiseen mainittuun uhkakuvaan laaja-alaisesti esittämällä yksityiskohtaisempia varautumismenetelmiä kuhunkin haasteeseen. Opinnäytetyössä tarkastellaan lähemmin pienempää joukkoa esitetyistä uhkakuvista. Näiden tarkasteluun valittujen uhkakuvien valintaperusteena ovat sekä omakohtainen kokemus viranomaistoimijoiden uhkakuvakentästä, että lähteenä käytetyt julkaisut.

Opinnäytetyö lähestyy aihetta aluksi kartoittamalla nykytilanteen ja kuvaamalla sen mahdolliset rajoitukset ennen siirtymistä varsinaiseen tutkimuskenttään. Muuttuvan viranomaislaajakaistan yhtenä haasteena on, että se ei vielä ole käytössä laajamittaisesti, joten saatavilla oleva lähdemateriaali perustuu pääosin teoriaan ja kaupallisiin referensseihin. Kaupallinen referenssi tässä yhteydessä tarkoittaa samankaltaisuuksien etsimistä toisesta toimintaympäristöstä, esimerkiksi kuluttajatuotteista. Tämä lähestyminen on ongelmallista siitä syystä, että kuluttajatuotteiden toimintaympäristö poikkeaa vaatimusten osalta varsin merkittävästi viranomaisympäristöstä eikä samoja lainalaisuuksia pystytä välttämättä suoraan siirtämään ympäristöstä toiseen. Näiden eroavaisuuksien käsittely luo kuitenkin pohjan haastekentän ymmärtämiselle ja toimii myös siltana kohti viranomaiskentän hahmottamista. Myös yhteneväisyyksiä toimintaympäristöjen kesken löytyy ja ne on pyritty kuvaamaan opinnäytetyössä soveltuvin osin.

Opinnäytetyö käsittelee uuden teknologian tuomia haasteita ja erityisesti tietoturvaan liittyviä uhkakuvia lähinnä päätelaitteen näkökulmasta, mutta siinä otetaan myös huomioon eri vaihtoehtoja viranomaislaajakaistan toteuttamiseen ja niiden tuomia vaikutuksia kokonaisratkaisuun. Opinnäytetyö pyrkii käsittelemään viranomaislaajakaistan ja erityisesti siihen liittyvien päätelaitteiden tietoturvaa erilaisten tunnistettujen uhkakuvi-

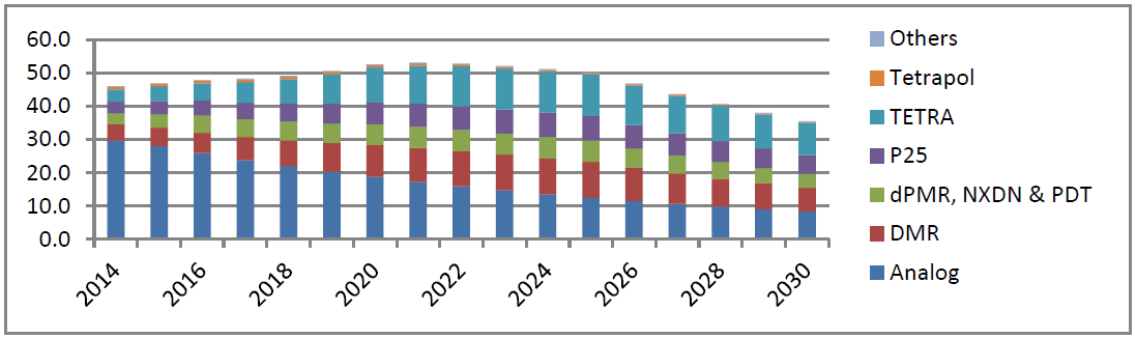
en kautta. Uhkakuvat pohjautuvat kansainvälisiin lähteisiin ja raportteihin pääasiassa kuluttajatuotteisiin liittyvistä uhkakuvista sekä tunnistetuista haavoittuvaisuuksista. Tunnistettujen uhkakuvien yhteydessä on myös pyritty esittämään mahdollisia menetelmiä kyseisten uhkakuvien torjumiseen.

Opinnäytetyössä tehdyn tutkimuksen perustana on käytetty kuluttajatuotteisiin pohjautuvaa lähdemateriaalia ja opinnäytetyö myös lähtee siitä olettamuksesta, että samoja aiheita käsitellään viranomaislaajakaistan yhteydessä. Olettamus pohjautuu omakohtaiseen kokemukseen eri viranomaisten kanssa käydyistä keskusteluista ja viranomaisyhteisön julkiseen tavoitteeseen hyödyntää kaupallista teknologiaa tulevassa viranomaislaajakaistassa (Wendelken 2013). Julkisuudessa nämä eri toimialueet ja niiden sisältämät uhkakuvat sekoitetaan usein ja se on omiaan aiheuttamaan lisää epätietoisuutta tai jopa virhearvioita toimialuekohtaisesti. Vaikka samoja uhkakuvia onkin olemassa ja niitä myös käsitellään tässä opinnäytetyössä, on tarpeen ymmärtää eri toimialueiden erot ja yhteneväisyydet laaja-alaisemmin.

3 VIRANOMAISVIESTINTÄ

Viranomaisviestintäteknologiat keskittyvät nykyisin varmistamaan luotettavan puheenvälityksen niin verkon kuuluvuusalueella, kuin myös sen ulkopuolella. Vaikka puhe tuleekin pysymään kriittisenä elementtinä viranomaisilla, ovat sen rinnalle nousemassa erilaiset datakeskeiset palvelut. Näistä lupaavina esimerkkeinä ovat reaaliaikaisen videokuvan välittäminen tapahtumapaikalta ja sosiaalisen median hyödyntäminen. Videokuvan ja muiden mahdollisten datapalveluiden vaatimuksena on riittävä datanopeus ja palvelun yleinen laatu. Nykyisten järjestelmien haasteena on kapeakaistaisuus, joka rajoittaa datanopeuden suhteellisen alhaiseksi. Viranomaisyhteisö onkin kääntänyt katseensa laajakaistateknologian suuntaan ja näistä selkeästi yleisempänä pidetään LTE-teknologiaa (3GPP 2013). Useat maat ovatkin valinneet LTE:n tulevaksi teknologiakseen viranomaisverkkoihin ja myös kattojärjestö TETRA and Critical Communications Association (TCCA) on asettunut tukemaan tätä tavoitetta (Tetratoday 2012). Seuraavissa kappaleissa esitellään yleisimmät nykyisin käytössä olevat viranomaisviestintäteknologiat sekä niiden tarjoamat datanopeudet.

LMR (Land Mobile Radio) on yleisesti käytetty termi kuvaaman kommunikaatiojärjestelmää, jota käytetään välittämään Push to Talk (PTT) -tyyppistä puhetta esimerkiksi viranomaisviestinnässä. LMR pitää sisällään useita eri teknologioita, joita tullaan tarkemmin käsittelemään seuraavissa kappaleissa. Kuva 6. esittää eri teknologioitten käyttäjämäärät maailmanlaajuisesti ja myös antaa ennusteen tulevaisuudesta. Viranomaisviestintä on hitaasti muuttuva kenttä ja LMR tulee vielä toistaiseksi kasvamaan, mutta siirtyminen uuteen, laajakaistateknologiaan on jo alkamassa.



KUVA 6. LMR Market Size (SNS Research 2015)

3.1 TETRA

TETRA eli Terrestrial Trunked Radio on yleisesti käytetty teknologia viranomaisviestinnässä erityisesti Euroopassa, Lähi-idässä sekä Aasiassa. TETRA on ollut sallittu myös Pohjois-Amerikassa vuodesta 2012 lähtien, mutta sen levinneisyys on siellä toistaiseksi vähäistä. European Telecommunication Standardisation Institute (ETSI) julkaisi ensimmäisen version TETRA -standardista jo vuonna 1995 (TandCCA 2016) ja sitä on kehitetty siitä lähtien. TETRA on erityisesti viranomaisille kehitetty teknologia, joka tukee heille keskeisimpiä toiminnallisuuksia, kuten ryhmäpuheluja sekä laitteesta laitteeseen (DMO) kommunikaatiota, sisäänrakennettuna.

TETRA on kapeakaistainen teknologia jossa yksittäisen kanavan kaistanleveys on tyypillisesti 25kHz ja maksimi datanopeus 28,8 kbits/s (Vehkalahti 2008), mutta TETRA Enhanced Data Service (TEDS) tarjoaa mahdollisuuden aina 150kHz saakka luoden teoreettisen datanopeusmaksimin 538kbit/s. Ensimmäisen vaiheen toteutuksissa kaistanleveytenä tullaan todennäköisesti käyttämään 50kHz, joka mahdollistaa teoreettisen 150kbits/s datanopeuden. Todellinen käyttäjälle näkyvä datanopeus on kuitenkin noin 80kbits/s (Hytera 2016).

Tietoturva on olennainen osa viranomaisviestintää ja myös TETRA tarjoaa siihen sisäänrakennettuja toteutuksia (Duan 2013, 41). korkealla tasolla TETRA tarjoaa käyttäjän tunnistamisen, E2E salauksen ja myös ilmarajapinnan salauksen. TETRA-teknologia on edelleen käytössä ja uusia verkkoja sekä rakennetaan, että otetaan käyttöön vielä usean vuoden ajan. On arvioitu, että TETRA-teknologian käyttäjiä olisi vuonna 2020 maailmanlaajuisesti noin 10,4 miljoonaa.

3.2 Project 25

Project 25 tai APCO 25 on varsinkin Pohjois-Amerikassa käytetty viranomaisteknologia. Sen kehitystyö aloitettiin jo 1989 ja tavoitteena oli saada uusi digitaalinen teknologia, joka toimisi myös yhdessä jo käytössä olleen analogisen teknologian kanssa. P25

on kapeakaistainen teknologia, joka mahdollistaa 9,6kbits/s maksimidatanopeuden (Tait 2010). Vaikka P25 on vanhempi teknologia kuin esimerkiksi TETRA, sen käyttäjämäärän arvioidaan silti kasvavan tulevien vuosien aikana, saavuttaen noin 6,6 miljoonan käyttäjän rajan vuonna 2020.

3.3 TETRAPOL

TETRAPOL on digitaalinen järjestelmä, joka kilpailee TETRA:n kanssa. TETRAPOL on suosittu erityisesti Ranskassa, jossa se otettiin käyttöön jo vuonna 1992. Siinä missä TETRA käyttää TDMA (time division multiple access) menetelmää, perustuu TETRAPOL FDMA (frequency division multiple access) menetelmään. Molempien järjestelmien puutteena on rajallinen kapasiteetti datan hyödyntämiseen. TETRAPOL on hyvin kapeakaistainen teknologia, jonka datanopeus on rajallinen, ainoastaan 7,6kbits/s (Ofcom 2016). TETRAPOL käyttäjiä on noin 800 000 ja tämän määrän arvioidaan lähtevän laskuun vuoden 2020 jälkeen.

3.4 Yhteenveto

Kuten edellä on kuvattu, nykyiset viranomaisviestintäteknologiat ovat puhekeskeisiä ja toimivatkin siinä luotettavasti. Niissä kaikissa on kuitenkin yhteinen heikkous, datanopeus (taulukko 2). Nykyisten rajoitteiden vuoksi viranomaiset joutuvat paikoin hyödyntämään erillistä päätelaitetta ja kaupallista verkkoa päästäkseen käsiksi joihinkin datapalveluihin. Tämä rajoite luo ylimääräisen hankaluuden viranomaisten toiminnalle ja samalla se myös luo tarpeettoman tietoturvariskin. Turvatakseen riittävän datanopeuden nyt ja tulevaisuudessa on viranomaisille käytännössä ainoana vaihtoehtona ottaa käyttöön laajakaistaisempi teknologia.

TAULUKKO 2. Käytettyjen teknologioiden datanopeudet

Teknologia	Kaistanleveys	Datanopeus
P25	12.5 kHz	9.6 kbits/s
TETRAPOL	12.5 kHz	7.6 kbits/s
TETRA	25 kHz	28.8 kbits/s
TEDS	150 kHz	150 kbits /s (max), 80 kbits/s (todellinen
LTE	20 MHz	100 Mbits/s ->

3.5 Viranomaislaajakaista

Viranomaistahot, kansalliset viestinnän säätelystä vastaavat tahot ja eri sidosryhmät ovat yleisesti asettuneet tukemaan LTE–teknologiaa seuraavana viranomaisviestinnän evoluutiona. Tahtotilana on tuoda viranomaisviestintää tukevat toiminnallisuudet kaupalliseen teknologiaan. Tämä lähestymistapa mahdollistaa teoriassa halvemmat päätelaitteet, laajemman tarjonnan sekä jatkumon teknologiatarjonnassa. Samalla se myös mahdollistaa nykyistä huomattavasti paremman kyvykkyyden hyödyntää datapohjaisia palveluita. Verrattuna nykyisten viranomaisteknologioiden tarjoamaan, maksimissaan kymmenien kilobittien datanopeuteen, LTE on omassa luokassaan tarjoten yli 100Mbits/s datanopeuksia (3GPP 2016).

LTE tarjoaa jo lähtökohtaisesti sisäänrakennettuja tietoturvatoiminnallisuuksia, kuten käyttäjän tunnistamisen UICC (Universal Integrated Circuit Card) välityksellä. Käyttäjän tunnistaminen on olennainen osa LTE verkon kokonaistietoturvaa ja sen mekanismi on kuvattu tarkemmin alla olevassa kaaviossa (Kuva 7).

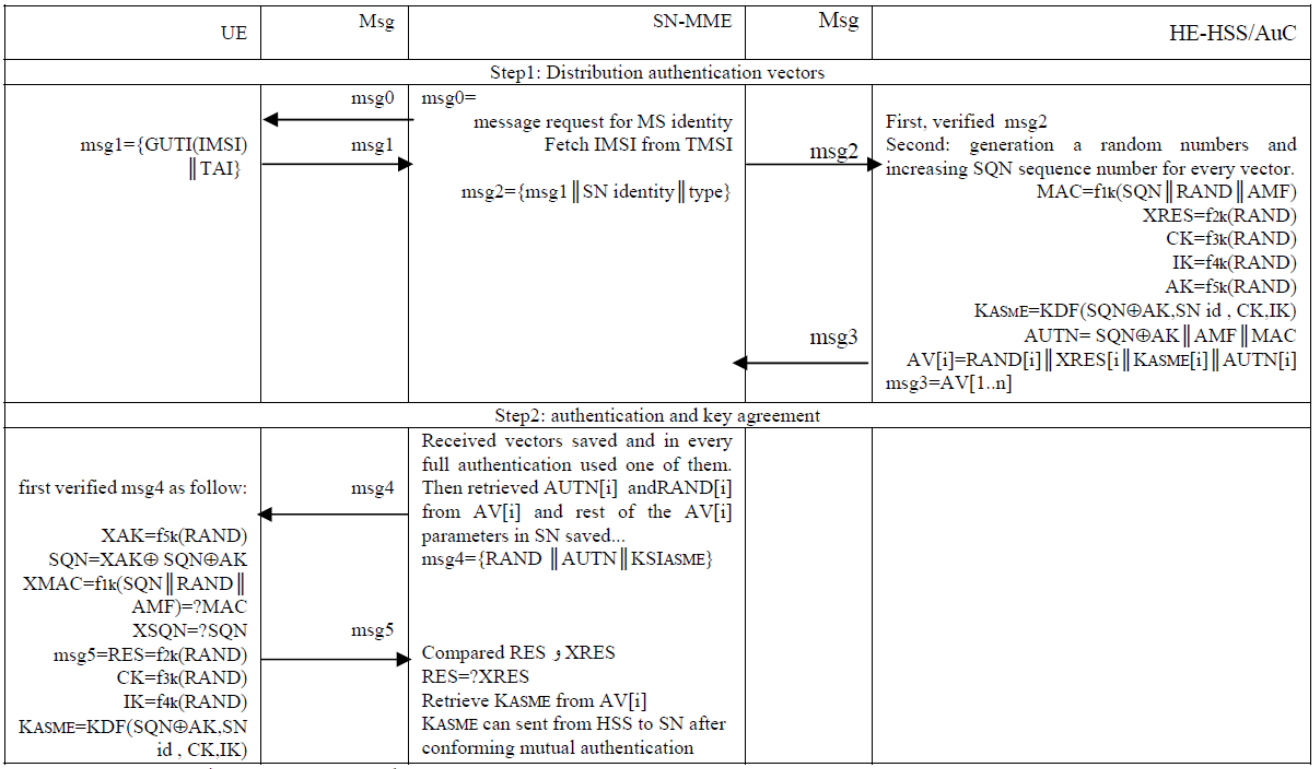


Fig. 4. EPS-AKA procedure

KUVA 7: EPS-AKA menettely (Purkhiabani & Salahi 2012).

EPS-AKA (Evolved Packet System Authentication and Key Agreement) on menetelmä, joka sisältyy LTE:n osana olevaan EAP (Extensible Authentication Protocol) tunnistamiskehikkoon. EPS-AKA pohjautuu niin kutsuttuun haaste-vastaus (challenge-response) tunnistamismenettelyyn. Yksinkertaistettuna tässä menettelyssä toinen osapuoli esittää kysymyksen, johon toisen osapuolen on kyettävä vastaamaan. Menetelmän mahdollisina heikkouksina tai uhkakuvina voidaan pitää käyttäjäidentiteetin paljastumista ja palvelunestohyökkäyksiä (Abdrabou, Elbayoumy, & El-Wanis 2015). Näitä uhkakuvia tarkastellaan opinnäytetyön kappaleessa 5. Käyttäjän tunnistamisen lisäksi LTE -standardi tarjoaa suojausmekanismin ilmarajapinnan suojaukseen ja turvallisen tavan välittää informaatio radioverkon ja runkoverkon välillä (Cichonski & Frankin 2015). Uusimmissa versioissa LTE-standardiin ollaan tuomassa myös tietoturvaratkaisuja esimerkiksi turvallisempaan PTT-kommunikaatioon.

Pääasiallinen standardointi LTE–teknologialle ja sen evoluutioille tapahtuu 3GPP:n ja sen jäsenorganisaatioiden kautta. Viranomaistahot ovat pyrkineet tuomaan tarkennettuja vaatimuksia 3GPP:n käsittelyyn ja sitä kautta tuleviin standardin julkaisuihin.

3.6 Toteutusvaihtoehdot

Vaikka viranomaislaajakaistan teknologiasta ollaan julkisesti yhtä mieltä, sen toteutusvaihtoehdot vaihtelevat merkittävästi eri maissa. Riippuen muun muassa sisämarkkinoista, taajuusallokaatiosta sekä markkina-alueen koosta mahdolliset toteutustavat voidaan jakaa neljään päävaihtoehtoon:

- Hybridiverkko
- Dedikoitu verkko
- Yhteiskäyttö kaupallisessa verkossa
- Jaettu radioverkko

Nämä pääryhmät jakautuvat mahdollisiin aliryhmiin, mutta tässä opinnäytetyössä keskitytään ainoastaan pääryhmiin ja niiden tuomiin haasteisiin. Jaetulla verkolla ja yhteiskäytöllä tarkoitetaan tässä opinnäytetyössä sellaista käyttöä, jossa jo olemassa olevaa verkkoa hyödynnetään rinnakkain kuluttajien kanssa.

3.6.1 Hybridiverkko

Hybridiratkaisussa pyritään hyödyntämään jo olemassa oleva viranomaisviestintäverkko ja tuomaan viranomaislaajakaista ja sen mahdolliset palvelut käyttöön vaiheittain. Viranomaislaajakaista voi olla tässä mallissa myös erillinen, ainoastaan viranomaisille rakennettu laajakaistaverkko, mutta tämän opinnäytetyön yhteydessä laajakaistaverkko tarkoittaa kaupallista verkkoa.

Useissa tapauksissa nykyinen järjestelmä toimii luotettavasti tärkeimmän, eli puhelunmuodostamisen mahdollistajana, eikä tätä välttämättä haluta muuttaa nopealla aikataululla. On myös mahdollista, että nykyinen viranomaisjärjestelmä on suhteellisen nuori ja siihen liittyvät perustamiskustannukset pyritään hyödyntämään pidemmällä aikajänteellä. Tästä syystä erillisen, rinnakkaisen järjestelmän pystyttäminen ei ole perusteltua. Mallin etuna voidaan pitää erityisesti aloituskustannusten selkeämpää suunniteltavuutta ja palveluiden tuomista hallitusti loppukäyttäjille.

3.6.2 Dedikoitu verkko

Yksi vaihtoehtoinen ratkaisu viranomaislaajakaistalle on oma, ainoastaan viranomaiskäyttöön rakennettu Dedikoitu LTE-verkko. Tämä malli vaatii oman taajuusalueen, joka on määritelty ainoastaan viranomaisten käyttöön. Erillinen viranomaisjärjestelmä vaatii tuekseen sekä uuden runkoverkon että radioverkon ja mallin haasteena voidaankin pitää sen suhteellisen suuria perustamiskustannuksia. Toisaalta pelkästään viranomaisille rakennettavan verkon hyötynä on sen mahdollisuus määritellä toteutus vastaamaan ainoastaan viranomaisten tarpeita. Lähtökohtaisesti tämä malli tarjoaa parhaat mahdollisuudet kokonaistietoturvan hallintaan.

3.6.3 Yhteiskäyttö kaupallisessa verkossa

Jaetussa mallissa viranomaislaajakaista hyödyntää kaupallista verkkoa joko kokonaan tai tuomaan lisäkapasiteettia tarvittaessa. Mallin etuina voidaan pitää suhteellisen nopeaa käyttöönottoa ja hallittuja perustamiskustannuksia. Yleisenä haasteena monessa maassa on kuitenkin verkon kattavuus versus viranomaisten vaatimukset. Samoin käyttäjien priorisointi ja viranomaiskäyttöä tukevat verkon vahvistamiset tuovat omia erityispiirteitä, jotka tulee huomioida palveluita suunniteltaessa. Mikäli viranomaiskäyttäjille pyritään takaamaan varmatoimiset palvelut kaupallisessa verkossa, saattaa se johtaa palveluiden saatavuuden laskuun kuluttajilla.

Osittaisessa jakamisessa viranomaiset hyödyntävät oman LTE-verkon ja kaupallisen LTE-verkon yhdistelmää. Tämä malli mahdollistaa lähestymistavan, jossa kaupallista infrastruktuuria käytettäisiin alentamaan perustamiskustannuksia määritellyissä verkon osissa tai vaihtoehtoisesti tuomaan lisäkapasiteettia viranomaisverkon kuormittuessa. Tämä vaihtoehtoinen malli vaatii oman viranomaisille rakennetun LTE-verkon ja taajuuden määrittelyn.

3.6.4 Jaettu radioverkko

Yhtenä toteutusvaihtoehtona on malli, missä viranomaisilla on jaettu radioverkko yhdessä kaupallisen operaattorin kanssa. Tässä mallissa viranomaiset hyödyntävät kaupal-

lisen operaattorin olemassa olevaa verkkoa ja varsinkin sen tarjoamaa radioverkkoa. Tässä vaihtoehdossa viranomaisille toteutetaan oma runkoverkko, joka mahdollistaa eriytettyjen palveluiden hallinnoinnin muusta käyttäjäkunnasta radioverkon ollessa yhteinen. Mallin etuna voidaan pitää nopeampaa sekä kustannustehokkaampaa palveluiden aloittamista verrattuna dedikoituun verkkoon ja toisaalta parempaa viranomaispalveluiden hallittavuutta verrattuna jaettuun kaupalliseen verkkoon. Yksi mallin haasteista on sama kuin kokonaan jaetussa verkossa: palveluiden laadun sekä saatavuuden varmistaminen myös kuluttajille.

3.7 Suunnitellut viranomaislaajakaistamallit eri maissa

Viranomaislaajakaista on herättänyt paljon huomiota kansainvälisesti ja eri maat ja toimijat ovat esitelleet suunnitelmia heille sopivasta laajakaistaratkaisusta. Osa suunnitelmista on edelleen esitysten tasolla, mutta muutamia konkreettisia ohjelmia on jo aloitettu.

3.7.1 Suomi

Suomi on esitellyt niin kutsutun viiden askeleen mallin viranomaislaajakaistan tuomiseksi kansalliseen käyttöön (Vinkvist, Pesonen & Peltola 2014). Malli rakentuu olemassa olevan TETRA-järjestelmän ympärille siten, että se säilyttää viranomaisille kriittiset toiminnot, kuten puheen, TETRA-järjestelmässä ja pyrkii tuomaan liikkuvanlaajakaistan vaiheittain käyttäjille. Suunniteltu käyttöönottomalli on hybridimalli ja toteutuksen on suunniteltu jakautuvan usealle vuodelle. Mallissa on tavoitteena siirtää nykyiset viranomaispalvelut uuteen laajakaistaan vaiheittain.

3.7.2 Yhdysvallat

Yhdysvallat on esimerkki dedikoidusta viranomaisverkosta. Yhdysvallat on allokoinut maanlaajuisen taajuuskaistan pelkästään viranomaiskäyttöön ja tavoitteena on rakentaa uusi LTE-teknologiaa hyödyntävä kommunikaatioverkko (Newcombe 2014, viitattu 13.10.2016). Kongressi on myöntänyt hankkeelle rahoitusta noin 7 miljardia dollaria, joka toimii perustana verkon aloituskustannuksille. Lopullinen summa tulee olemaan

huomattavasti korkeampi, jopa useita kymmeniä miljardeja. On mahdollista, että verkkoratkaisu tulee hyödyntämään paikoin myös kaupallista verkkoa, mutta ainoastaan valikoiduilta osin. Lähestymistapa johtaa siihen, että päätelaitteiden tulee tukea tätä valittua taajuutta.

3.7.3 Iso-Britannia

Iso-Britannia tulee hyödyntämään kaupallista LTE-verkkoa ja varsinkin sen tuomaa radioverkkoa viranomaislaajakaistassa. Heidän tavoitteensa on tuoda viranomaisten vaatimat toiminnallisuudet osaksi jo toiminnassa olevaa kaupallista LTE-radioverkkoa mutta samalla he lisäävät omia runkoverkon elementtejä viranomaisille. Tätä tavoitetta varten on luotu viranomaisohjelma ESMCP (Home Office 2015), joka koordinoi viranomaishanketta kansallisesti. Iso-Britannian lähestymistapa eroaa esimerkiksi Yhdysvaltojen vastaavasta myös päätelaitteiden suhteen. Koska tavoitteena on käyttää jo olemassa olevia kaupallisia taajuuksia, erillistä päätelaitevarianttia ei välttämättä tarvita. Toki viranomaisvaatimukset kussakin maassa tulevat asettamaan erikoisvaatimuksia toimittajille.

3.7.4 Etelä-Korea

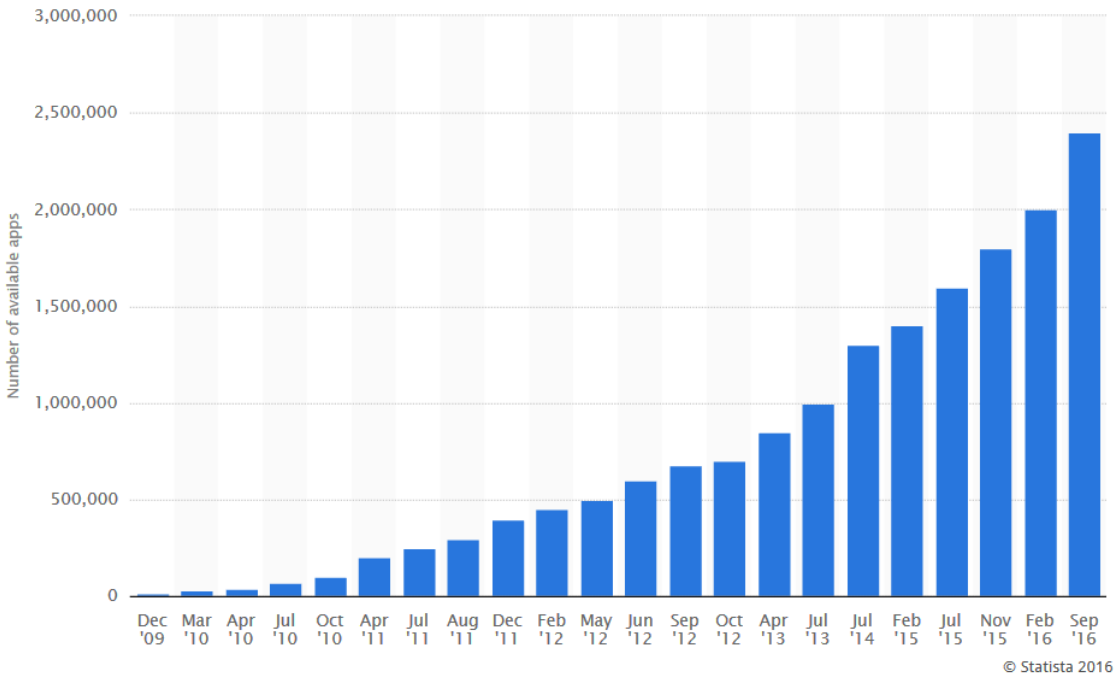
Etelä-Korean lähestyminen on lähellä Yhdysvaltojen valitsemaa ratkaisua ja he ovat määritelleet viranomaisille oman taajuuskaistan (Zilis 2014). Kehitystyö Koreassa on jo hyvässä vauhdissa ja ensimmäiset pilottihankkeet on aloitettu valikoitujen loppukäyttäjien kanssa (Wendelken 2015).

3.8 Uhkakuvat

Yhteistä kaikille aiemmin kuvatuille vaihtoehdoille on käytetty teknologia, LTE, ja tavoite hyödyntää datan käyttöä viranomaissovelluksissa. Tämä muutos on merkittävä ja kun otetaan huomioon viranomaiskäyttäjien mahdollisuus käsitellä arkaluontoista tietoa ja todennäköistä pääsyä keskitettyihin järjestelmiin, tuo muutos mukanaan uusia haas-

teita myös päätelaitteiden tietoturvalle. Tämä opinnäytetyö pyrkii kuvaamaan näitä uusia haasteita ja mahdollisia menetelmiä niihin varautumiseen.

Nykyinen tilannekuva kaupallisesta maailmasta antaa osin ehkä liiankin negatiivisen näkymän päätelaitteiden tietoturvatasoon. Saamme lukea lähes viikoittain uusista tietoturvamurroista tai salakuuntelutapauksista. Nämä uutiset ovat omiaan luomaan osin vääristynyttäkin kuvaa päätelaitteiden turvallisuudesta. On syytä huomioida, että päätelaitteiden tietomurrot eivät suoraan perustu käytettyyn kommunikaatioteknologiaan, tässä tapauksessa LTE-teknologiaan, vaan useimmiten tunnettuihin tietoturvahaavoittuvuuksiin esimerkiksi käyttöjärjestelmässä tai käytetyissä taustajärjestelmissä sekä sosiaalisen tiedonkeruun hyödyntämiseen. Uudet käyttöjärjestelmäpohjaiset ekosysteemit, kuten Android ja IOS, ovat luoneet kasvavan tarjonnan loppukäyttäjille suunnatuille ohjelmistoille. Pelkästään Androidille suunniteltujen ohjelmien määrä Googlen ylläpitämässä virallisessa ohjelmistojen kauppapaikassa on kasvanut räjähdysmäisesti. Näiden lisäksi käyttäjille on tarjolla valtava määrä ohjelmia muiden kauppapaikkojen, kuten Amazonin tai GetJarin kautta. Kuva 8 havainnollistaa Google Play–kauppapaikassa olevien ohjelmien lukumäärän kasvun.



KUVA 8. Ohjelmien määrä Google Play 2009 – 2016 (Statista 2016b)

Tietoturvayhtiö Symantec arvioi vuonna 2013 tehdyssä tutkimuksessa, että 17% kaikista Androidiohjelmista on itse asiassa haittaohjelmia (Tynan 2015). Symantec jaottelee haittaohjelmat kolmeen pääkategoriaan (Taulukko 3):

- Malware – haittaohjelmat, jotka pitävät sisällään viruksia, matoja tai troijalaisia hevosia
- Grayware – ohjelmat, jotka eivät suoraan pidä sisällään viruksia, mutta jotka voivat olla erittäin häiritseviä tai jopa haitallisia käyttäjälle (esimerkiksi hakkerointi-, vakoilu- tai mainosohjelmistot)
- Madware – ohjelmat, jotka lisäävät mainoksia esimerkiksi käyttäjän kuva-albumiin, vaihtavat soittoääniä tai pakottavat näytölle notifikaatioita

Symantec on myöhemmin päivittänyt analyysiaan ja vuonna 2015 he ovat analysoineet 71% enemmän ohjelmia kuin edellisenä vuonna ja huomasivat yli kolminkertaisen (230%) kasvun haittaohjelmien määrässä (Symantec 2016, 14).

TAULUKKO 3. Analysoitujen Android ohjelmien suhde haittaohjelmiin (Symantec 2016)

	2013	**2014**	**2015**
Analysoidut sovellukset	6,1 miljoonaa	6,3 miljoonaa	10,8 miljoonaa
Tunnistettu Malwareksi	0,7 miljoonaa	1,1 miljoonaa	3,3 miljoonaa
Tunnistettu Graywareksi	2,2 miljoonaa	2,3 miljoonaa	3,0 miljoonaa
Grayware, joka myöhemmin tunnistettu Madwareksi	1.2 miljoonaa	1,3 miljoonaa	2,3 miljoonaa
Malware määritelmä	Ohjelma ja tiedostot, jotka on suunniteltu tekemään haittaa		
Grayware määritelmä	Ohjelmat, jotka eivät sisällä viruksia, mutta voivat olla ärsyttäviä tai jopa haitallisia käyttäjälle. Esimerkiksi mainosohjelmistot		

Madware määritelmä	Aggressiiviset menetelmät, joilla pyritään vaikuttamaan tai muuttamaan päätellaitteen asetuksia siten, että niihin saadaan esimerkiksi mainoksia.

Uuden datapohjaisen järjestelmän ja kaupallisten teknologioiden hyödyntämisen myötä, viranomaispäätelaitteiden tietoturvauhkien voidaan olettaa olevan hyvin samankaltaisia kuluttajalaitteiden kanssa. ENISA:n tekemän raportin mukaan (Belmonte, Marinos & Rekleitis 2016) vuonna 2015 15 merkittävimmän uhkakuvan joukossa olivat muun muassa (Kuva 9):

- Haittaohjelmat (sijalla 1.)
- Verkon kautta kohdistuva uhka (sija 2.)
- Verkko-ohjelmistojen kautta kohdistuva uhka (sija 3.)
- Palvelunestohyökkäys (sija 5.)
- Laitteen katoaminen (sija 6.)
- Uhka sisältäpäin (sija 7.)
- Identiteettivarkaus (sija 12.)
- Kybervakoilu (sija 15.)

Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	➲	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	➲	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓
11. Insider threat	➲	11. Data breaches	➲	↓
12. Information leakage	↑	12. Identity theft	➲	↑
13. Identity theft/fraud	↑	13. Information leakage	↑	↓
14. Cyber espionage	↑	14. Ransomware	↑	↑
15. Ransomware/ Rogueware/Scareware	↓	15. Cyber espionage	↑	↓

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1: Overview and comparison of cyber-threat landscapes 2015 and 2014

KUVA 9: Yleiskuva kyber-uhista (Belmonte & al. 2016. s.7)

Kuten myös aiemmin esitetyn Symantecin tekemän jaottelun pohjalta voimme todeta, nämä ylätason kategoriat jakaantuvat kukin pienempiin osa-alueisiin, muodostaen huomattavan laajan uhkakuvakentän. Edellä mainittujen uhkakuvien rajapinnat yhtyvät myös päätelaitteisiin. Osa uhkakuvista vaikuttaa suoraan päätelaitteeseen ja osa epäsuorasti, mutta kuitenkin siten, että päätelaitteen ja sen käyttäjän voidaan katsoa olevan pääkohde. Uhkakuvien avulla pyritään tunnistamaan merkittävimmät riskit ja myös luomaan niille kohdistetut varautumiskeinot. NATO Cooperative Cyber Defence Centre of Excellencen tekemässä tutkimuksessa (Blumbergs, Braccini, Diez, Farar, Pissanidis, &Väisänen 2015) eri lähteisiin pohjautuvia uhkakuvia analysoimalla on pystytty tunnistamaan yhteisiä riskejä erityisesti kannettaville päätelaitteille. Tutkimuksessa käytetty kohderyhmä on rajattu ylempiin virkamiehiin ja päättävässä asemassa oleviin loppukäyttäjiin. Tämä rajaus näkyy myös osittain tutkimuksessa käytettyjen riskien sekä uhkakuvien määrittelyssä. Huolimatta lähteenä käytetyn tutkimuksen märittelemästä raja-

tusta kohderyhmästä, voimme silti tunnistaa yhteisiä riskejä laajemmin loppukäyttäjäryhmien kesken. Tutkimuksessa tunnistettiin valittuun käyttäjäryhmään kohdistuvia uhkakuvia seuraavasti (Blumbergs et al. 2015):

- Tietovuoto
- Laitteen luvaton käyttö
- Luvaton fyysinen tunkeutuminen laitteen muistiin
- Fyysinen murtautuminen laitteeseen
- Luvaton laitteen etäkäyttö
- Sosiaalinen manipulointi
- Verkkohuijaukset
- Tietoturvapäivitysten puutteellisuus, niiden puuttuminen ja turvallinen välitys
- Laitteen murtaminen ja muuttaminen (Rooting)
- Maineen menettäminen (henkilökohtainen, poliittinen tai organisaatiollinen)
- Palvelunestohyökkäys (DoS)

Seuraavassa luvussa käsitellään valittuja uhkakuvia tarkemmin ja pyritään ymmärtämään niiden mahdollisia ennaltaehkäiseviä menetelmiä.

4 UHKAKUVAT JA NIIHIN VARAUTUMINEN

Erilaiset uhkakuvat näyttelevät isoa roolia uusia viranomaisteknologioita valittaessa. Joissakin tapauksissa uhkakuvat sekä riskit syntyvät käyttäjien tai yhteisön tietämättömyydestä, mutta toisaalta loppukäyttäjät eivät myöskään välttämättä tiedosta omien valintojensa merkitystä tietoturvan kokonaisvaltaisuudelle Mikäli aihetta ei ymmärretä tarpeeksi hyvin, voidaan helposti synnyttää mielikuva vakavastakin riskistä, vaikka todellisuudessa saattaa hyvin olla kyse ainoastaan epätietoisuudesta. Samaan aikaan laadukaskin tietoturvaratkaisu päätelaitteessa ei välttämättä suojele käyttäjän tekemiltä virheiltä.

Uhkakuvien ymmärtäminen ja niihin varautuminen on olennainen vaihe kokonaisturvallisuuden muodostamisessa. Seuraavissa luvuissa lähestytään tärkeimpiä uhkakuvia ja pyritään tunnistamaan mahdolliset vaikuttamiskeinot.

4.1 Haittaohjelmat

Kannettavien päätelaitteiden lisääntyessä myös mobiilihaittaohjelmien määrä kasvaa ja niiden merkitys korostuu. Vuonna 2015 mobiilihaittaohjelmien määrä kasvoi lähes 50% edellisvuoteen verrattuna, ylittäen 8 miljoonan rajan (Belmonte & al. 2016, 19). Suurin osa, noin 95% mobiilihaittaohjelmista kohdistuu Android käyttöjärjestelmään. Haittaohjelmat itsessään jakaantuvat pienempiin osa-alueisiin, kuten

- Ei-toivottu ohjelmisto (44%)
- Adware (19%)
- Troijalaiset (12%)
- Trojan.sms (8%)
- Trojan.spy (7%)

Näiden lisäksi mm. erilaiset kiristysohjelmat ovat lisänneet suosiotaan rikollisten keskuudessa. Viranomaispäätelaitteille haittaohjelmat ovat todellinen uhkakuva ja niiden ehkäisyyn tulee varautua kattavasti.

Verkon kautta tapahtuvat hyökkäykset ovat tässä yhteydessä pääasiassa haitallisten ohjelmien levittämistä saastuneiden verkko-osoitteiden välityksellä ja käsitellään siksi osana haittaohjelmien kokonaisuutta.

Nykyisin osa toiminnallisista ohjelmista voidaan suorittaa hyödyntäen verkossa olevia resursseja tai ne voivat jopa sijaita verkossa. Tämä avaa mahdollisuuden haittaohjelmien levittämiseen tai jopa mahdolliseen tietomurtoon esimerkiksi käyttäjätietoja hyödyntämällä.

Viranomaisyhteydessä tähän uhkaan varautumisen voidaan katsoa painottuvan käyttäjäprosessien määrittelemiseen ja ohjeistuksen kouluttamiseen. Tyypillisesti viranomaisjärjestelmät ja niiden sisällä suoritettavat ohjelmat ovat sekä valvottuja että varta vasten viranomaisille kehitettyjä. Nykyisin on kuitenkin yhä enemmän nähtävissä julkisen verkon ja sen mahdollistamien sosiaalisten palveluiden hyötykäyttö myös viranomaisten keskuudessa. Päätelaitteessa pystytään tarvittaessa määrittelemään sekä sallitut palvelut että sallitut yhteysverkot.

4.2 Haittaohjelmien ennaltaehkäisy ja niihin varautuminen

Haittaohjelma monelta osin nojaa tunnettuihin tietoturvahaavoittuvuuksiin ja siten sen riskikenttä on alati muuttuva. Tärkeänä varautumiskeinona on jatkuva ohjelmiston ylläpito sekä päivittäminen, mutta myös esimerkiksi ohjelmiston ajo-oikeuksien rajaaminen. Esimerkiksi viranomaispäätelaitteissa voidaan sallia ainoastaan tunnettujen ohjelmistojen asentaminen ja suorittaminen. Tämän tyyppisessä mallissa, jossa sallittuja ohjelmistoja valvotaan palveluntarjoajan toimesta, voidaan toisaalta ajautua epätoivottuun tilanteeseen, jossa käyttäjät tuntevat päätelaitteen tai järjestelmän liian kankeaksi ja tekevät jopa mahdollisesti osan toiminnoista henkilökohtaisten päätelaitteiden tai kaupallisten sovellusten välityksellä.

Päätelaitteen ohjelmiston ja sen integriteetinhallinannan lisäksi tulee varmistaa mahdollisimman laaja tunnistamismekanismi haittaohjelmille unohtamatta toimintamekanismeja tietomurron varalle. Uusia haittaohjelmia luodaan kiihtyvällä vauhdilla ja niiden luontia helpottamaan on saatavilla jopa omia ohjelmistotyökaluja (F-Secure 2014). Tä-

mä alati muuttuva ja massiivinen toimintaympäristö asettaa haasteita haittaohjelmien reaaliaikaisille tunnistamismekanismeille.

4.3 Palvelunestohyökkäys

Palvelunestohyökkäykset voidaan jakaa karkeasti kahteen pääkategoriaan, hajautettuun palvelunestohyökkäykseen (Distributed Denial of Service, DDos) ja palvelunestohyökkäykseen (Denial of Service, DoS). Molempien hyökkäysten yhtenä tavoitteena on lamauttaa kohteena oleva palvelu tai palvelin. Palvelunestohyökkäyksiä voidaan hyödyntää myös esimerkiksi haittaohjelmien levittämisessä.

Palvelunestohyökkäys eroaa hajautetusta palvelunestohyökkäyksestä siten, että siinä kohteena olevaa palvelua kuormitetaan yhdeltä palvelimelta ja tyypillisesti yhden internetyhteyden kautta. Hajautetussa palvelunestohyökkäyksessä hyödynnetään useiden koneiden ja internetyhteyksien verkkoa ja nämä ovat usein globaaleja hyökkäyksiä. Hajautetussa palvelunestohyökkäyksessä voidaan hyödyntää jo saastuneita koneita ja palvelimia. Näiden torjuminen on huomattavasti haastavampaa kuin yksittäisen palvelimen ja yhteysosoitteen hyökkäyksissä. Kuten aiemmin mainittiin, yhtenä osana palvelunestohyökkäyksiä on saastuneitten koneiden, eli botnettien hyödyntäminen ja niiden luominen haittaohjelmien avulla.

4.4 Laitteen katoaminen

Päätelaitteiden yleistyminen ja niiden toiminnallisuuksien lisääntyminen muodostavat enenevissä määrin kasvavan huolen niiden joutumiselle väärin käsiin. Laitteen menettäminen voi johtua sekä inhimillisestä erehdyksestä että suunnitellusta varkaudesta. Molemmissa tapauksissa laitteen etähallinta on erityisen tärkeää ja siitä tulee huolehtia jo osana järjestelmän kokonaisvaatimuksia ja toimintamalleja.

Laitteen suojaaminen pelkästään etähallinnalla ei kuitenkaan välttämättä ole riittävä. Etähallinta ja sen hyödyntäminen vaatii tyypillisesti verkkoyhteyden, joten mikäli laite on joutunut vääriin käsiin, sen etähallinta voidaan estää pelkästään rajoittamalla verkkoyhteydet. Tätä uhkakuvaa käsitellään tarkemmin myöhemmissä luvuissa.

4.5 Uhka sisältäpäin

Sisältä päin tulevat, käyttäjiin kohdistuvat uhkakuvat ovat iso ja myös luontainen osa kyberturvaa. Välttämättä kyseessä ei ole tahallinen tietovuoto, vaan kyseessä voi olla inhimillinen virhe tai käyttäjän huolimattomuus. Tähän uhkakuvaan liittyvien hyökkäysvektorien määrä on suuri, koska siinä pystytään hyödyntämään useita mahdollisia hyökkäysmetodeja. Käyttäjiin kohdistuvissa metodeissa voidaan hyödyntää esimerkiksi tunnistettuja heikkouksia käytetyissä tietoturvamenetelmissä tai jopa heikkouksia päätelaitteiden sekä järjestelmien käytettävyydessä. Mikäli käyttäjät kokevat järjestelmän käytettävyyden heikoksi, se saattaa ajaa heidät joko käyttämään vaihtoehtoisia (mutta ei sallittuja) järjestelmiä tai jopa jättämään noudattamatta sovittuja menetelmiä. Esimerkkinä voidaan käyttää tapausta, jossa Yhdysvaltojen virassa oleva ulkoministeri käytti henkilökohtaista sähköpostiaan virallisessa kommunikoinnissa (O'Harrow 2016).

Suojautuminen näitä uhkakuvia vastaan on hyvin haasteellista. Uhkakuva itsessään tulee ymmärtää laajana kokonaisuutena, joka koostuu useista mahdollisista rajapinnoista, joita puolestaan voidaan hyödyntää mahdollisessa hyökkäyksessä. Tämä tarkoittaa sitä, että myös uhkakuvaan varautuminen ja sen torjunta koostuu useista osa-alueista. Päätelaitteen näkökulmasta yhtenä keskeisenä osa-alueena onkin sen käytettävyys. Samoin kuin uhkakuva ja siihen varautuminen, myös laitteen käytettävyys on monien tekijöiden summa. Laitteeseen kirjautuminen ja käyttäjän tunnistaminen tulisi tehdä mahdollisimman helpoksi, jotta vältyttäisiin houkutukselta ohittaa tietoturvallinen toimintamalli.

4.6 Identiteettivarkaus

Identiteettivarkauden ja sen mahdollisen hyödyntämisen merkitys tulee kasvamaan kannettavien päätelaitteiden sekä niiden mahdollistamien palveluiden yleistyessä. Voidaan olettaa, että kannettavalla päätelaitteella, kuten älypuhelimella, on mahdollista päästä käsiksi kokonaisjärjestelmään. Tämä avaa uusia mahdollisuuksia kybervakoilulle, vahingonteolle ja luonnollisesti arkaluontoisen materiaalin varastamiselle. Identiteettivarkaudessa käyttäjän tietoja voidaan käyttää hyväksi, kun pyritään murtautumaan järjestelmään ulkoa käsin. On myös mahdollista, että ulkopuolinen taho esiintyy varastetulla identiteetillä ja pyrkii sen avulla luomaan luottamuksellisen suhteen järjestelmän muihin

käyttäjiin. Identiteettivarkaudelta suojautuminen koostuu käyttäjän tietojen salauksesta ja niihin liittyvien menetelmien ja toimintamallien noudattamisesta.

4.7 Kybervakoilu

Kybervakoilu on enenevissä määrin kasvava uhka kybermaailmassa. Jo nykyiset päätelaitteet ja applikaatiot raportoivat, käyttäjän hyväksymänä, eri sensoreiden tuottamaa dataa verkkoon. Tämä data saattaa sisältää esimerkiksi paikkatietoa, jota pystytään puolestaan hyödyntämään vakoilutarkoituksiin. Digitalisaation myötä käyttäjien fyysisiä tunnistetietoja, kuten sormenjälkiä, iiris-skannauksia ja muita biometrisiä tunnisteita tallennetaan tietopankkeihin ja myös joissain tapauksissa päätelaitteisiin. Sama tietopankki pystyy pitämään sisällään myös laajoja asiakas- tai henkilötietokantoja. Tällaiset keskitetyt tietokannat ovat yleensä hyvin suojattuja, mutta myös samalla hyvin houkuttelevia kohteita kyberrikollisille. Esimerkiksi Yhdysvaltojen julkisen sektorin henkilötietokantaan tehdyn tietomurron (Forsythe & Sanger 2015) yhteydessä noin 21,5 miljoonan henkilön tiedot joutuivat vääriin käsiin.

Kybervakoilun yhtenä osa-alueena on salakuuntelu. Tämä voi olla joko rikollisten tai muiden ei-sallittujen intressiryhmien suorittamaa vakoilua tai viranomaisen suorittamaa tutkimusta. Salakuuntelu itsessään voidaan suorittaa usealla tasolla kommunikaatioverkossa ja tätä vastaan suojautuminen päätelaitteen näkökulmasta voidaan rajata käytettyyn puheensalaukseen.

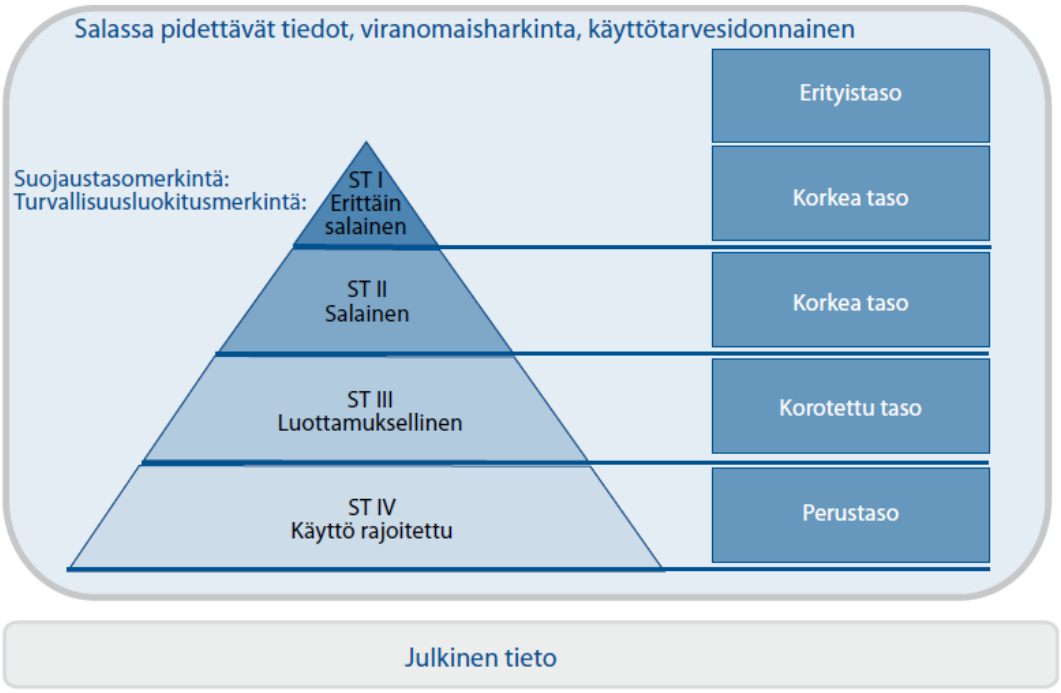
.

5 ANALYYSI

Julkisuudessa esiin tulevat väärinkäytökset ja jo tapahtuneet tietovuodot ovat omiaan lisäämään epävarmuutta uutta teknologiaa kohtaan. Kyseessä voi olla osin julkisuuspeli, osin tietämättömyys mutta myös aito huoli teknologiaa kohtaan. On kuitenkin syytä muistaa, että uhkakuvien ymmärtäminen on avain turvalliseen kommunikaatioon ja teknologian hyödyntämiseen viranomaiskäytössä. Osa tunnistetuista uhkakuvista liittyy voimakkaasti kaupalliseen verkkoon ja sitä hyödyntäviin ohjelmistoihin, eivätkä välttämättä ole sellaisenaan merkityksellisiä toimialueensa ulkopuolella. Viranomaisverkot ovat parhaimmillaan omia kokonaisuuksia, joten niiden hallinta voidaan myös keskittää ja jopa osin eristää valituista palveluista. Tämän tyyppinen verkonhallinnan eriyttäminen mahdollistaa lähtökohtaisesti turvallisemman toimintaympäristön verrattuna avoimeen verkkoon. Voidaan myös olettaa, että viranomaisten käyttötapaukset eroavat normaalikuluttajasta ja tietyt, pelkästään viranomaisille suunnatut palvelut, nousevat keskiöön. Esimerkkinä voidaan pitää viranomaisviestinnässä käytettyä Push To Talk (PTT) -kommunikaatiomenetelmää. Siinä missä kuluttaja nojaa joko Internet Protokollan (IP) yli tapahtuvaan, kaupalliseen sovellukseen (esimerkiksi Skype) tai standardoituun teknologiaan perustuvaan puheeseen (esimerkiksi GSM), käyttävät viranomaiset laajasti ryhmäkommunikaatiota ja sen tuomia palveluita. Viranomaislaajakaistassa nämä ryhmäkommunikaatiopalvelut ovat tyypillisesti heitä varten suunniteltuja, joten turvallisuustekijät on lähtökohtaisesti pyritty ottamaan huomioon jo suunnittelun alkuvaiheissa.

Viranomaisten ja virastojen järjestelmävaatimuksissa on myös mahdollista vaatia korkeamman tietoturvatason toteutusta. Suomessa tämän kaltainen kriteeristö tunnetaan nimellä KATAKRI (Puolustusministeriö 2015) Se pitää sisällään kolme (3) eri suojaustasoa (ST), jotka voidaan hyväksyä KATAKRI:n määritelmien mukaisesti (Kuva 10):

- ST II
  Korkean suojaustason vaatimukset
- ST III
  Korotetun suojaustason vaatimukset
- ST IV
  Perustason vaatimukset



KUVA 10. Suojaustasot, Vahti – ohje 2012 (Valtiovarainministeriö 2012, 27)

Nämä vastaavat pääosin Euroopan komission määrittelemiä luokituksia (Euroopan Komissio 2005).

- TRES SECRET UE/EU TOP SECRET
  Tätä luokitusta sovelletaan ainoastaan sellaiseen tietoon ja aineistoon, jonka luvaton käyttö saattaisi vahingoittaa poikkeuksellisen vakavasti Euroopan unionin tai sen yhden tai useamman jäsenvaltion olennaisia etuja

- SECRET UE
  Tätä luokitusta sovelletaan ainoastaan sellaiseen tietoon ja aineistoon, jonka luvaton käyttö saattaisi vahingoittaa vakavasti Euroopan unionin tai sen yhden tai useamman jäsenvaltion olennaisia etuja

- CONFIDENTIEL UE
  Tätä luokitusta sovelletaan ainoastaan sellaiseen tietoon ja aineistoon, jonka luvaton käyttö saattaisi vahingoittaa Euroopan unionin tai sen yhden tai useamman jäsenvaltion olennaisia etuja

- RESTREINT UE
  Tätä luokitusta sovelletaan ainoastaan sellaiseen tietoon ja aineistoon, jonka luvaton käyttö saattaisi haitata Euroopan unionin tai sen yhden tai useamman jäsenvaltion olennaisia etuja

On huomioitavaa, että Top Secret tasoa ei virallisesti käytetä teknologiahyväksynnöissä. Myöskään KATAKRI ei määrittele ST I tason, erittäin salaisen ympäristön, kriteeristöä. Suomessa tietoturvahyväksynnöistä vastaa Viestintävirasto (FICORA).

5.1 Päätelaitteen joutuminen vääriin käsiin

On mahdollista, että päätelaite joutuu vääriin käsiin joko inhimillisen erehdyksen tai tahallisen varkauden johdosta. Tämän tyyppisessä tilanteessa on tärkeää, että sekä päätelaitteen tietoturva että siihen rakennettu oheisjärjestelmä pystyvät reagoimaan tapahtuneeseen. Päätelaite olisi hyvä suunnitella siten, että se kestää mahdolliset sisäänpääsy yritykset, niin ohjelmiston kautta tapahtuvat kuin myös mahdollisen fyysisen murtautumisen.

Ohjelmistopohjaisen varautumisen perustana on vahva tunnistamismekanismi käyttäjille. Tyypillisesti kuluttajapäätelaitteissa käytetään eripituisia, käyttäjäkohtaisia tunnuslukuja, mutta myös biometrinen tunnistus on valtaamassa alaa. Tästä esimerkkinä on sormenjälkeen pohjautuvan tunnistamisen yleistyminen päätelaitteissa. Riippuen viranomaiskentän vaatimuksista on mahdollista, että käyttäjältä vaaditaan kaksivaiheinen tunnistaminen. Tätä kaksivaiheisen tunnistamisen menetelmää on kuvattu tarkemmin luvussa 6.1.2.

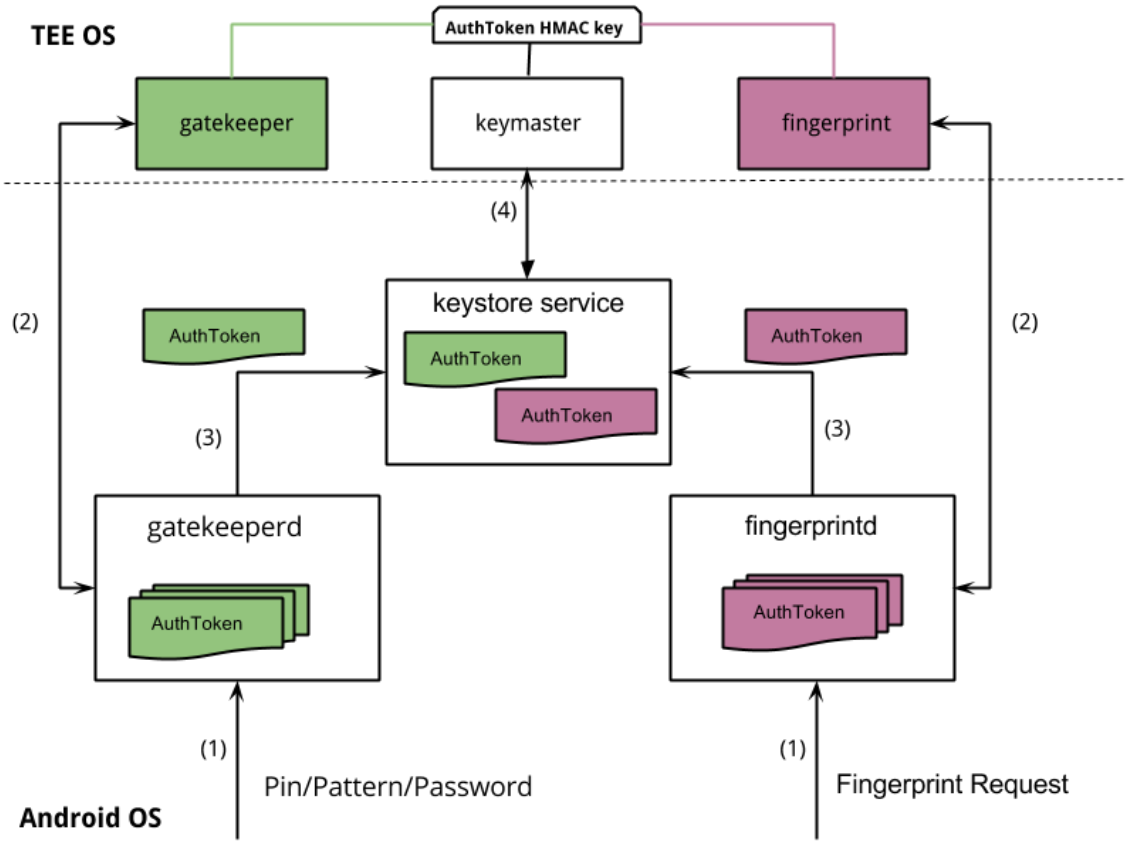
5.1.1 Authentication – Authorization - Accounting

Käyttäjän tunnistamiseen ja käyttöoikeuksien luovuttamiseen liitetään yleisesti AAA–prosessi. Lyhenne tulee englannin sanoista Authentication – Authorization – Accounting. Kyseessä oleva terminologia kattaa käyttäjän tunnistamisen, käyttöoikeuksien tarkistamisen ja palveluihin mahdollisesti liittyvän datan statistiikan.

Prosessin ensimmäinen osa, käyttäjän tunnistaminen pohjautuu usein määriteltyyn salasanaan, PIN (personal identification number) numeroon tai biometriseen tunnisteeseen. Jokainen edellä mainittu tunniste tulee olla yksilöllinen ja käyttäjäkohtainen. Tyypillisesti laitteen ensimmäisen käynnistyksen yhteydessä tai palautettaessa tehdasasetukset, järjestelmä alustetaan vastaanottamaan käyttäjätunnisteen luominen.

Android 6.0 alustassa käyttäjä määrittelee itselleen tunnisteen (PIN, kuvio, salasana, biometrinen tunniste), jonka pohjalta järjestelmä luo 64 bittisen, satunnaisen turvallisen käyttäjätunnisteen (User SID, user secure identifier). Tämä SID toimii käyttäjän tunnisteena järjestelmään ja sitä käytetään myös varattuna merkkinä käyttäjän salattuun materiaaliin ja se on salausteknisesti linkitetty käyttäjän luomaan salasanaan. Mikäli käyttäjä haluaa vaihtaa omat tunnistetietonsa, hänen täytyy ensin pystyä antamaan nykyiset tunnisteensa. Onnistuneen tunnistamisen myötä aiemmin luotu SID voidaan linkittää uuteen tunnisteeseen. Tämä mahdollistaa sen, että käyttäjä voi hyödyntää jo olemassa olevia avaimiaan myös tunnisteen vaihdon jälkeen. Mikäli käyttäjä ei anna nykyisiä tunnisteita, hän menettää jo luodun SID:n ja siihen liittyvät avaimet. Tämä menetelmä ei ole yleensä sallittu muille kuin järjestelmän ylläpitäjille ja se ei myöskään näy loppukäyttäjille.

Seuraavassa kaaviossa kuvataan käyttäjätunnisteen luominen Android 6.0 käyttöjärjestelmässä.



KUVA 11. Android Security – Authentication (Android 2016)

Yllä oleva kaavio (Kuva 11) esittää käyttäjän tunnistamisen Android 6.0 alustassa. Tämän pohjana on, että käyttäjä on jo luonut yksilöllisen tunnisteensa. Kaaviossa oleva numerointi kuvaa prosessin vaiheet.

1. Käyttäjä antaa yksilöllisen PIN-numeron, kuvion, salasanan tai käyttää sormenjälkilukijaa, mikäli laitteessa on sellainen. Riippuen menetelmästä järjestelmän aliosat suorittavat pyynnön joko Gatekeeper (salasana) tai Fingerprint (sormenjälki) palveluille. Käyttöjärjestelmä sisältää erillisen suojatun alueen, TEE (trusted execution environment), joka huolehtii avainten käsittelystä.
    - Mikäli kyseessä on salasana, PIN tai määritelty kuvio, gatekeeperd lähettää sen omalle vastinparilleen TEE-ympäristössä, joka puolestaan huolehtii autentikoinnista ja lähettää allekirjoitetun AuthTokenin takaisin Android OS:lle.
    - Mikäli kyseessä on sormenjälkitunnistus, toiminnon käynnistää fingerprintd, joka välittää tiedon TEE:ssa sijaitsevalle vastinparilleen.
2. Kun joko gatekeeperd tai fingerprintd on vastaanottanut allekirjoitetun AuthTokenin, välittää se sen eteenpäin keystorage palvelulle. Gatekeeperd myös pitää huolen, että keystorage palvelu on tietoinen järjestelmän lukituksesta ja mahdollisesta salasanan vaihdoksesta
3. Keystorage palvelu välittää AuthTokenin Keymaster palvelulle ja varmistaa AuthTokenit yhteisellä avaimella. Keymaster tekee päätöksen avainten luotettavuudesta Tokenin varmenteen aikaleimasta ja määrittää, voidaanko ohjelmille antaa lupa käyttää avainta.

Avaintenhallinta ja niiden luomisessa käytetyt algoritmit luovat perustan turvalliselle käyttäjän tunnistamiselle. Laitteen ja sen käyttöjärjestelmän tulee varmistaa, että avaimet eivät päädy laitteesta ulos. Myös avainten ja taulukoiden luontiin käytettyjen salausalgoritmien tulisi olla riittävän vahvoja, jotta niiden murtaminen olisi mahdollisimman aikaa vievää. Esimerkiksi aiemmin kuvatussa Android 6.0 käyttöjärjestelmän käyttäjän tunnistamisessa käytetään SHA (Secure Hash Algorithm) menetelmällä luotua 256 bittistä taulukkoa AuthTokenin allekirjoituksessa. SHA ei varsinaisesti ole salausalgoritmi, vaan sitä voidaan käyttää luomaan yksilöllinen tunniste annetun sisällön pohjalta. Tätä tunnistetta voidaan puolestaan hyödyntää tiedon varmentamisessa. Tiedon salaami-

sen voidaan puolestaan käyttää salausalgoritmeja, näistä yleisimmät voidaan jakaa kahteen pääluokkaan:

1. Symmetriset menetelmät

Symmetrisissä menetelmissä salauksen luomiseen käytetään määriteltyä salaista avainta tai lähdettä. Symmetrisissä menetelmissä sekä salaukseen, että sen purkamiseen vaaditaan sama avain. Vaikka salauksesta itsestään voidaan luoda hyvinkin turvallinen, voi avaintenhallinnassa tulla haasteita. Mikäli avain päätyy tunnetuksi, voidaan päästä käsiksi salattuun tietoon ja myös luoda salattua tietoa järjestelmään esimerkiksi sekaannuksen aikaansaamiseksi. Myös tilanteissa, joissa on paljon käyttäjiä ja käyttäjäryhmiä, voi pelkkään symmetriseen salaukseen pohjautuva menetelmä osoittautua rajalliseksi. Yleisimpiä symmetrisen salauksen algoritmejä ovat (OWASP 2015):

- DES
  Data encryption standard on jo osin vanhentunut standardi, joka käyttää 56 bitin mittaista avainta. Nykyisillä laskutehoilla DES on auttamatta liian helppo murrettava.
- 3DES
  3DES hyödyntää suoraan DES-standardia, mutta se mahdollistaa kolme eri avainmittaa:168, 112 ja 56.
- AES
  Advanced Encryption Standard on laajasti käytössä oleva salausmenetelmä, joka mahdollistaa 128, 192 ja 256 bitin mittaisen avaimen. Voidaan arvioida, että tämän hetkisten laskentatehojen avulla 256 bittisen salauksen murtaminen veisi aikaa kauemmin kuin nykyinen tunnettu universumin ikä (Mohit 2012).

2. Epäsymmetriset menetelmät

Epäsymmetrisistä menetelmistä voidaan käyttää myös termiä Public/Private Key Cryptography. Menetelmässä käytetään kahta eri avainta; toista tiedon salaamiseen ja toista sen avaamiseen.. Toinen avaimista on julkinen ja sitä voidaan jakaa muille käyttäjille, mutta yksityiseksi määritellystä avaimesta on syytä huolehtia tarkasti. Yleisimpiä epä-

symmetrisen salauksen menetelmiä ovat PGP (Pretty Good Privacy) sekä SSL (Secure Socket Layer) (Wikipedia 2016).

5.1.2 Kaksivaiheinen tunnistaminen

Kaksivaiheinen tunnistaminen on yksittäistä salasanaa tai PIN koodia varmempi menetelmä käyttäjän tunnistamiseen. Sen pohjana on lähestyminen, jossa käyttäjältä vaaditaan esimerkiksi pankkikortti (jotain mitä sinulla on) ja PIN koodi (jotain mitä tiedät) ennen kuin toiminto voidaan aloittaa. Tavalliselle kuluttajalle pankkiautomaatti on helppo esimerkki kaksivaiheisesta tunnistamisesta. Toinen helposti lähestyttävä esimerkki on Googlen käyttämä menetelmä sähköpostipalveluun kirjautumiseen. Siinä käyttäjä syöttää salasanansa (jotain mitä tiedät) jonka jälkeen palvelu lähettää erillisen koodin käyttäjän ennalta määrittelemään puhelinnumeroon (jotain mitä sinulla on). Turvallisuussyistä käytetty koodi ei ole kahta kertaa samanlainen.

Molemmissa esimerkeissä voidaan huomata, että esimerkiksi salasanan tai PIN-koodin menettäminen ei välttämättä suoraan johda sähköpostien tai jopa tilitietojen menettämiseen. Kaksivaiheiseen menetelmään voidaan sitoa myös esimerkiksi biometrinen tunniste, kuten sormenjälki tai erillinen tunnistekortti. Tämäntyyppinen henkilön sähköinen tunnistaminen (HST) on käytössä muun muassa joissakin valtionhallinnon järjestelmissä.

5.1.3 Authorization - varmentaminen

Osana käyttäjän määrityksiä on käyttöoikeuksien luominen ja niiden hallinnointi. Kuluttajatuotteissa käyttäjällä on merkittävät oikeudet omaa päätelaitetta kohtaan. Käyttäjä pystyy muokkaamaan asetuksia, asentamaan uusia ohjelmia ja luovuttamaan tietoja niin halutessaan. Voidaan olettaa, että viranomaispäätelaitteiden hallintamekanismi eroaa merkittävästi normaalista kuluttajapäätelaitteesta tässä suhteessa. Yhtenä olennaisena osana viranomaispäätelaitteen kokonaisturvallisuutta on sen etähallinta ja myös valmius mukauttaa käyttäjäasetuksia. On mahdollista, että viranomaispäätelaiteella on useampia käyttäjiä ja näiden käyttäjäprofiilit voivat erota toisistaan myös pääsyoikeuksien puolesta. Tietyissä tapauksissa osa palveluista voi olla sallittuja ainoastaan rajatulle käyttäjä-

kunnalle, mutta päätelaite voi silti olla käytössä myös muilla käyttäjillä. Näissä tapauksissa käyttäjäprofiilin hallintaan tulee kiinnittää erityistä huomiota ja on todennäköisesti jopa tarpeen vaatia useamman askeleen tunnistaminen ennen palvelun sallimista.
Mikäli päätelaite on joutunut väärin käsiin, nousevat sekä käyttäjäoikeudet että laitteen etähallinta merkittävään rooliin.

Käyttäjäoikeuksilla voidaan rajata jo lähtökohtaisesti ne ohjelmat, joita laitteessa voidaan suorittaa. Tämä sulkee pois mahdollisuuden asentaa esimerkiksi vakoilutarkoituksiin kehitettyjä ohjelmia tai muuten muokata laitteen sisältöä. Android päätelaitteille on olemassa useita mahdollisia tapoja ladata uusia sovelluksia, mutta mikäli käyttäjälle sallitaan ainoastaan valikoitu tarjonta, tulisi nämä vaihtoehtoiset menetelmät sulkea pois. Tämä johtaa tilanteeseen, jossa käyttäjälle joko asennetaan tarvittavat sovellukset ennen laitteen luovuttamista, pakotetaan keskitetyn etähallinnan kautta uudet sovellukset tai tarjotaan suljettu sovelluskauppapaikka. Tärkeintä on, että kokonaishallinta järjestelmässä sallituille sovelluksille säilyy viranomaisella.

Osana etähallintaa on laitteen tietojen poistaminen tilanteissa, joissa sen epäillään joutuneen kolmannen osapuolen käsiin. Tapahtuma voi olla myös tahaton, mutta silti varotoimenpide on sama kuin tilanteessa, jossa laite on varastettu. Etähallinnan avulla järjestelmän ylläpitäjä pystyy ohittamaan käyttäjän ja pakottamaan päätelaitteen tilaan, jossa siitä ei ole enää hyötyä kolmannelle osapuolelle. Kaikki käyttäjän tiedot voidaan poistaa hallitusti laitteen muistista ja myös laite itsessään voidaan merkitä ei-sallituksi järjestelmän kannalta ja siten estää sen mahdollinen väärinkäyttö. Etähallinnan heikkouksia on sen toiminnallisuuden riippuvuus saatavilla olevasta verkkoyhteydestä. On mahdollista, että laitteen pääsy verkkoon on estetty, jolloin myöskään etähallinta ei ole käytössä. Näissä tapauksissa laitteeseen voidaan määritellä erityisiä turvaominaisuuksia, kuten tietojen tuhoaminen ja laitteen lukitseminen usean peräkkäisen väärän salasanan jälkeen. Tämä toiminnallisuus nojaa aiemmin esitettyyn mekanismiin, jolla käyttäjä tunnistetaan.

Nykyisiin päätelaitteisiin on mahdollista pyrkiä murtautumaan myös laitteen fyysisten rajapintojen kautta. Tämä tarkoittaa tyypillisesti laitteen avaamista ja sen osien tai komponenttien poistamista tai muuttamista. Joissain tapauksissa voidaan keskeisiä komponentteja vaihtaa uusiin ja siten saada yhteys laitteen keskeisiin tietoihin. Fyysiseen

uhkaan kohdistuvia menetelmiä vastaan pyritään suojautumaan joko ohjelmistopohjaisesti siten, että esimerkiksi käynnistyksen yhteydessä laitteen komponentit tarkistetaan ja tulosta verrataan sallittuun laitekonfiguraatioon. Tämän tyyppistä mallia on käytetty esimerkiksi Applen IOS 9-käyttöjärjestelmässä, jossa laitteesta tuli käyttökelvoton mikäli siihen vaihdettiin tiettyjä komponentteja, kuten kolmannen osapuolen sormenjälkitunnistin (Bell 2016). Toinen vaihtoehto fyysistä murtautumista vastaan on suunnitella laite siten, että se havaitsee laitteen avaamisen ja tuhoaa käyttäjän tiedot (Wilson 2016).

5.2 Viranomaiskentän taustajärjestelmät

Viranomaiskäyttäjä eroaa suuresti tavallisesta kuluttajasta, erityisesti päätelaitteen käyttötarkoituksen suhteen. Kuluttajan voidaan olettaa hyödyntävän päätelaitetta monenkirjavaan kommunikaatioon, erilaisiin sovelluksiin ja mahdollisesti henkilökohtaisen tiedon tallentamiseen. Käyttötavat ja tottumukset määräytyvät kuluttajan omien toimintatapojen ja ymmärryksen mukaan. Viranomaiselle päätelaite on puolestaan pääasiallisesti työväline, jonka käyttöä ohjaa järjestelmän puolelta määritelty ohjeistus ja toimintamalli.

Kuluttajien on mahdollista omalla toiminnallaan vaarantaa päätelaitteen tietoturva ja siten aiheuttaa merkittäviäkin vahinkoja, lähinnä itselleen. Mahdollista hyökkääjää saattaa kiinnostaa käyttäjän päätelaitteessaan säilyttämä tieto, esimerkiksi salasanat, kuvat tai yhteystiedot. Näiden avulla on mahdollista päästä käsiksi käyttäjän pilvipalveluihin tai yhteystietojen kautta esimerkiksi kohdistettuun tietojen kalasteluun. Verkon kautta tapahtuva tietojen kalastelu onkin nousemassa yhdeksi merkittävistä tietoturvauhista. Käyttäjää manipuloimalla pystytään kohdentamaan tietojenkalastelukampanjoita ja mitä enemmän tietoa kohteesta on saatavilla, sen helpompaa manipulointi on. Käyttäjän manipulointi on hyvin tehokas keino ja sitä vastaan suojautuminen on erittäin haasteellista.

Erinomaisena esimerkkinä käyttäjän manipuloinnista voidaan pitää koetta, jossa yhdysvaltalainen journalisti Kevin Roose haastoi kaksi asiantuntijaa selvittämään kaiken mahdollisen hänestä ja, mikäli mahdollista, murtautumaan hänen järjestelmiinsä. Ehtona oli, etteivät he tekisi vahinkoa eivätkä varastaisi rahaa häneltä. Roose itse oli siis täysin

tietoinen häneen kohdistuvasta uhasta ja osasi varoa kaikkea normaalista poikkeavaa. Vain kahta viikkoa myöhemmin asiantuntijat olivat saaneet haltuunsa koko Roosen järjestelmän, hänen pankkitilinsä sekä yksityiskohtaiset tiedot hänen työstään. He myös pystyivät valvomaan Roosea hänen kotonaan olleen verkkokameran kautta. Roose julkaisi aiheesta artikkelin hänen työnantajansa sivustolla (Roose 2016).

Artikkeli osoittaa, kuinka helppoa on päästä käsiksi yksittäisen käyttäjän järjestelmään pelkän verkossa olevan tiedon välityksellä. Mikäli hyökkääjällä olisi jo valmiiksi käytössään yksityiskohtaisempaa tietoa, hänen tehtävänsä helpottuisi entisestään. Roosen tapaus on esimerkki kuluttujaan kohdistuvasta uhasta ja siitä, mistä mahdollinen hyökkääjä on kiinnostunut. Tyypillisesti motiivi on raha. Myös viranomaisjärjestelmään kohdistuvassa uhkakuvassa raha on varmasti tärkeä tekijä, mutta sen lisäksi hyökkääjillä voi olla muitakin motiiveja. Mahdollisten hyökkääjien tavoitteena voi olla pääsy viranomaisjärjestelmässä oleviin tietokantoihin. Nämä tietokannat ovat tyypillisesti taustajärjestelmässä ja niihin pääseminen on toistaiseksi rajoittunut esimerkiksi tietokoneen kautta tapahtuvaan tiedusteluun. On hyvin todennäköistä, että tämä tulee muuttumaan merkittävästi liikkuvan viranomaislaajakaistan yleistyessä.

Uusi teknologia mahdollistaa riittävän nopeat datayhteydet myös kannettavasta päätelaitteesta ja se tuleekin muokkaamaan viranomaisten toimintaa merkittävästi. Siinä missä aiemmin taustajärjestelmiin pääsy oli mahdollista esimerkiksi ajoneuvossa olevan kiinteän päätelaitteen kautta, on hyvinkin mahdollista, että tulevaisuudessa sama toiminto on mahdollista suorittaa älypuhelimesta. Käytännössä tämä tarkoittaa sitä, että mahdollisten hyökkäysrajapintojen määrä tulee kasvamaan merkittävästi nykyisestä. Tämä muutos pakottaa käyttäjäorganisaatiot arvioimaan heidän nykyisiä toimintamallejaan ja jo opittuja käytäntöjä uudesta perspektiivistä.

Viranomaistoimijoilla yksi keskeisimpiä toimintaa ohjaavia tekijöitä on käyttöpolitiikka. Se määrittelee toimintaympäristön ja ohjesäännön, miten käyttäjän tulee toimia ja myös mahdollisesti millaisia päätelaitteita järjestelmässä on sallittua käyttää. Käyttöpolitiikka voi määräytyä joko virallisesta kriteeristöstä, kuten KATAKRI:sta tai se voi olla erikseen määriteltynä käyttäjäorganisaation toimesta. Yhtä kaikki, on hyvin tärkeää, että käyttäjäorganisaatiolla on määritelty ohjeistus käyttöpolitiikalle.

5.3 Kuluttajatuotteet ja viranomaiskenttä

Kuten aiemmin olemme havainneet sekä kuluttajapuolella että viranomaiskentässä löytyy yhteneviä uhkakuvia sekä mahdollisia riskejä. Samalla olemme havainneet, että toimintaympäristöt eroavat toisistaan merkittävästi. Onkin syytä pohtia, voidaanko näiden kahden kentän sisällä oleviin uhkakuviin suhtautua yhdenvertaisina. Välttämättä näin ei ole, ja mikäli oletamme, että viranomaiskäyttäjä pystyy hyödyntämään taustajärjestelmän palveluita suoraan kannettavasta päätelaitteesta, on myös turvallista olettaa, että mahdollista hyökkääjää kiinnostaa juuri taustajärjestelmiin pääsy. Kuluttajakentässä vaarassa on lähinnä yksittäinen käyttäjä ja hänen henkilökohtaiset tietonsa ja usein miten hyökkääjän motiivina on nopea raha. Viranomaiskentässä vaarassa on mahdollisesti useamman henkilön tiedot ja profiilit ja motiivina voi olla myös muu kuin nopea rahastaminen. Viranomaisjärjestelmät, kuten muutkin valtionhallinnon järjestelmät pitävät sisällään myös luokiteltua tietoa ja siihen pääsemisen motiivina voi olla kenties vakoilu tai pahimmillaan jopa sabotaasi.

Myös eri maiden lähestymistavat luovat eroavaisuuksia uhkakuville. Nämä eroavaisuudet eivät pelkästään näy toimintakenttien välillä, vaan myös viranomaiskentän sisällä. Mikäli tavoitteena on käyttää jo olemassa olevaa kaupallista verkkoa täysimääräisesti, avaa se potentiaalisille hyökkääjille väylän haluttuun tietoon jo verkon itsensä kautta. Jotta uhkakuvaan pystyttäisiin varautumaan luotettavasti, vaatii se huomattavan yhteistyön kaupallisen operaattorin ja viranomaistoimijan välille. Kuten aiemmin todettiin, viranomaistoimijoiden käyttöpolitiikka saattaa olla merkittävästi tiukempi kuin kuluttajilla ja jo pelkästään tämä eroavaisuus saattaa johtaa tilanteeseen, missä kaupallisen verkon ratkaisut eivät vastaa viranomaisten vaatimuksia. Mikäli kaupallista järjestelmää pyritään muokkaamaan viranomaisten ehdoilla, voi se puolestaan johtaa tilanteeseen, missä muiden käyttäjien oikeuksia joudutaan rajoittamaan. Tyypillisesti kuluttajapuolen teknologiavaihtuvuus on huomattavasti nopeampaa kuin viranomaiskentässä ja myös tämä muutosnopeus voi aiheuttaa sopeutumisvaikeuksia mahdolliselle yhteiskäytölle.

Siinä missä kuluttajateknologia ja kaupallinen internet ovat vaikeasti käsiteltävä kokonaisuus, joka muodostuu lukemattomista solmukohdista, on viranomaisverkko mahdollista rakentaa hallitusti ja myös joissakin tapauksissa se pystytään kokonaan eristämään kaupallisesta internetistä. Tämä on hyvin merkittävä ero kahden toimialueen välillä ja se

on syytä pitää mielessä myös uhkakuvia verrattaessa. Lisäksi, kun otetaan huomioon viranomaiskentän eroavaisuudet verrattuna tyypilliseen kuluttajaratkaisuun, ja erityisesti, kun nostetaan esiin taustajärjestelmän merkitys kokonaistietoturvaratkaisussa, on dedikoidulla viranomaisverkolla parhaat edellytykset luoda turvallinen pohja tiedon hallintaan ja sen suojaamiseen. Vaihtoehto on kuitenkin kaikkein kallein aloituskustannuksiltaan, eikä ole oletettavaa, että jokainen maa pystyisi erillisen verkon perustamaan.

Riippumatta valitusta verkkoratkaisusta viranomaislaajakaistan turvalliselle käytölle voidaan nostaa esiin kolme pääkohtaa:

I. Käyttöpolitiikka

   Viranomaistoimijalla täytyy olla ajan tasalla oleva käyttöpolitiikka, joka määrittelee järjestelmän turvallisen käytön. Käyttöpolitiikka voi pohjautua viralliseen auditointikriteeristöön, sertifikaatteihin tai muihin dokumentoituihin käyttötapauksiin. Tärkeintä on, että käyttöpolitiikka on määritelty ja sen noudattamista vaaditaan. On huomioitavaa, että käyttöpolitiikan tulee tukea käyttötarkoitusta, eikä sen tule olla sille esteenä.

II. Luotettava käyttäjän tunnistaminen

   Osana käyttöpolitiikkaa tulisi olla määritelmä luotettavalle käyttäjän tunnistamiselle. Tunnistamismenetelmän tulisi puolestaan olla helppokäyttöinen ja nopea, jotta se ei estä viranomaista suorittamasta hänelle tärkeää tehtävää. On suositeltavaa, että viranomaistoimijoiden tulisi käyttää kaksivaiheista tunnistamismenetelmää ja pyrkiä löytämään luotettava ja helppokäyttöinen menetelmä yhdessä toimittajien kanssa.

III. Riittävä päätelaitteen tietoturva

   Määritelmä riittävälle tietoturvalle ei ole yksiselitteinen ja se riippuu käytetystä toimintaympäristöstä. Laitteeseen voidaan rakentaa tarvittaessa hyvinkin järeä suojaus, mutta vähintään laitteen tulisi tarjota:

   a. Luotettava avainten luominen ja niiden tallentaminen
   b. Laitteen integriteetin varmistaminen
   c. Salattu muisti käyttäjän datan suojaamiselle
   d. Mahdollisuus etähallintaan

Näiden lisäksi olisi suositeltavaa, että päätelaite pystyisi havaitsemaan fyysisen tunkeutumisen. Tämä toiminto antaa merkittävän lisäturvan tapauksissa, joissa laite on päätynyt vääriin käsiin.

Yksi tärkeimpiä asioita, joka viranomaistoimijoiden tulisi huomioida, on päätelaitteen merkityksen muutos. Päätelaite tulee olemaan olennainen osa kokonaisjärjestelmää ja se avaa mahdollisuuden päästä käsiksi taustajärjestelmiin. Tästä syystä päätelaitteen, samoin kuin järjestelmänkin, tietoturvaratkaisun tulee olla sisäänrakennettuna eikä sitä tule ajatella mahdollisena lisäoptiona, joka voidaan lisätä tarvittaessa. On mielenkiintoista huomata, että tätä opinnäytetyötä tehdessä tämä sisäänrakennetun tietoturvan lähestyminen on nostettu esiin myös kansallisella tasolla Yhdysvalloissa. Heinäkuussa 2016 Yhdysvaltojen viestintäviranomainen FCC (federal communications committee) julkaisi tiedotteen, jossa se kertoi ottavansa käyttöön ”security by design” vaatimuksen kaikille toimijoille, jotka pyrkivät tuomaan uutta teknologiaa uusille, korkeammille taajuusalueille (FCC 2016).

5.4 Yhteenveto

Opinnäytetyö kuvaa muuttuvaa viranomaiskenttää yleisesti ja se pyrkii tuomaan lukijalle ymmärryksen kokonaiskuvasta ja suhteesta kuluttajakentän haasteisiin. Tärkeänä havaintona on uhkakuvien näennäinen samankaltaisuus. Vaikka julkisuudessa, ehkä tietoisestikin, tuodaan kuluttajakentästä löytyviä uhkakuvia sellaisenaan viranomaiskenttään, on syytä ymmärtää, että uhkakuvat ovat yhteneviä kenties ainoastaan nimensä puolesta. Toimintaympäristöt ovat hyvin todennäköisesti erilaisia, samoin hyökkääjien motiivit. Ehkä keskeisimpänä huomiona opinnäytetyössä on tarve muuttaa viranomaiskäyttäjien katsontakantaa ja ajattelumallia kokonaisvaltaisemmaksi. Tätä huomiota tukee myös aiemmin mainittu, FCC:n vaatimus ”security by design” lähestymiselle.

Opinnäytetyössä on tunnistettu keskeiset pääkohdat, jotka mahdollistavat päätelaitteen tietoturvallisen käytön viranomaislaajakaistajärjestelmässä. Nämä kaikki pääkohdat pitävät sisällään alueita, joita tulisi tarkastella tarkemmin. Esimerkiksi kaksivaiheisen tunnistamisen menetelmiä tulisi kehittää edelleen, samoin käyttöpolitiikan merkitystä tulisi nostaa entisestään esille, unohtamatta tietoisuuden lisäämistä loppukäyttäjien kes-

kuudessa. Myös kaupallisen puolen perusteita olisi hyvä arvioida tarkemmin. Vaikka dedikoitu verkkoratkaisu onkin perustamiskustannuksiltaan todennäköisesti kaikkein kallein, se takaa kuitenkin parhaat mahdollisuudet viranomaistoimijoille määrätä itse palveluistaan. Sama mahdollisuus ei välttämättä toteudu yhteiskäytössä kaupallisessa verkossa, vaan siellä toimintaa ohjaa voimakkaasti tuottavuus.

LÄHTEET

3GPP 2013. Public Safety. Viitattu 14.10.2016.
http://www.3gpp.org/news-events/3gpp-news/1455-Public-Safety

3GPP 2016. LTE ue-Category. Viitattu 14.10.2016.
http://www.3gpp.org/keywords-acronyms/1612-ue-category

3GPP 2016. LTE. Viitattu 4.10.2016,
http://www.3gpp.org/technologies/keywords-acronyms/98-lte

Abdrabou, M., Elbayoumy, A. & El-Wanis, E., 2015. LTE Authentication Protocol (EPS-AKA) weaknesses solution, 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS).
Viitattu 25.10.2016. http://ieeexplore.ieee.org/document/7397256/

Android 2016. Authentication. Viitattu 14.10.2016.
https://source.android.com/security/authentication/

Bell, K. 2016. Apple hit with class action lawsuit for 'Error 53' issue in iOS 9. Viitattu 14.11.2016.
http://www.technobuffalo.com/2016/02/12/apple-hit-with-class-action-lawsuit-for-error-53-issue-in-ios-9/

Belmonte, A., Marinos, L. & Rekleitis, E. 2016. ENISA Threat Landscape 2015. Viitattu 22.3.2016.
https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

Blumbergs, B., Braccini, C., Diez. E., E.Farar, A., Pissanidis, N. &Väisänen, T., 2015. Defending mobile devices for high level officials and decision-makers. Julkaisu. Viitattu 14.10.2016.

https://ccdcoe.org/sites/default/files/multimedia/pdf/Defending%20mobile%20devices%20for%20high%20level%20officials%20and%20decision-makers.pdf

Cichonski, J., Franklin, J. 2015. LTE Security – How Good Is It?. RSA Conference 2015. Viitattu 14.10.2016. https://www.rsaconference.com/writable/presentations/file_upload/tech-r03_lte-security-how-good-is-it.pdf

Duan, S. 2013. Security Analysis of TETRA. Norwegian University of Science and Technology. Master's thesis. Viitattu 14.10.2016. http://www.diva-portal.org/smash/get/diva2:656471/FULLTEXT01.pdf

Euroopan komissio 2005. Rules on Security. Viitattu 14.10.2016. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02001D0844-20050202&qid=1395937087333&from=EN

Federal communications commission 2016. Use of Spectrum Bands Above 24 GHz For Mobile Radio Services. Viitattu 14.10.2016. https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-89A1_Rcd.pdf

Forsythe, M. & Sanger, D. 2015. China Calls Hacking of U.S. Workers' Data a Crime, Not a State Act. Artikkeli. Viitattu 14.10.2016. http://www.nytimes.com/2015/12/03/world/asia/china-hacking-us-opm.html?_r=2

F-Secure 2014. BLACKENERGY & QUEDAGH The convergence of crimeware and APT attacks. White paper. Viitattu 14.10.2016. https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

Fumiyuki, A 2001. Wireless past and Future: Evolving Mobile Communication Systems. IEICE Trans. Findamental, Vol. E84-A, No.1, January 2001. Viitattu 25.10.2016. http://www.mobile.ecei.tohoku.ac.jp/paper/pdf/publish_2001/01_pu_2001_adachi.pdf

Home Office 2015. Emergency services network. Viitattu 14.10.2016.

https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network

Hytera 2016, TETRA Enhanced Data Services, White Paper. Viitattu 14.10.2016. http://www.hyteramobilfunk.com/uploads/tx_wwdownloads/hytera_tetra_90acn-t_teds_wp02_eng_2013-05-16_web.pdf

Mohit, A. 2012. How secure is AES against brute force attacks? Viitattu 14.10.2016. http://www.eetimes.com/document.asp?doc_id=1279619

Newcombe, T. 2014. Firstnet explained. Viitattu 14.10.2016. http://www.govtech.com/public-safety/FirstNet-Explained.html.

Ofcom, Federal Office of Communications 2016. TETRAPOL. Viitattu 14.10.2016. https://www.bakom.admin.ch/bakom/en/homepage/telecommunication/technology/tetrapol.html

O'Harrow, R. 2016. How Clinton's email scandal took root. Artikkeli. Viitattu 14.10.2016. https://www.washingtonpost.com/investigations/how-clintons-email-scandal-took-root/2016/03/27/ee301168-e162-11e5-846c-10191d1fc4ec_story.html

OWASP 2015. Guide to Cryptography. Viitattu 14.10.2016. https://www.owasp.org/index.php/Guide_to_Cryptography

Peltola, M. 2011. Evolution of Public Safety and Security Mobile Networks. Aalto yliopisto. Licentiate's Thesis submitted in partial fulfilment of the requirements for the degree of Licentiate of Science in Technology.

Puolustusministeriö 2015. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 14.10.2015. http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

Purkhiabani, M. & Salahi, A. 2012. Enhanced Authentication and Key Agreement Procedure of next Generation 3GPP Mobile Networks. International Journal of Information and Electronics Engineering, Vol. 2, No. 1, January 2012 Viitattu 14.10.2016. http://www.ijiee.org/papers/57-C099.pdf

Roose, K. 2016. I dared two expert hackers to destroy my life. Here's what happened. Viitattu 14.10.2016. http://fusion.net/story/281543/real-future-episode-8-hack-attack/

Statista. 2016a. Number of apps available in leading app stores as of June 2016. Viitattu 14.10.2016. https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

Statista. 2016b. Number of available applications in the Google Play Store from December 2009 to September 2016. Viitattu 14.10.2016. https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

Symantec 2016. Intern Security Threat Report. Viitattu 14.10.2016. https://www.symantec.com/security-center/threat-report

Tait Radio Communications 2010. Technologies and Standards for Mobile Radio Communications Networks, White Paper. Viitattu 14.10.2016. http://utilities.taitradio.com/__data/assets/pdf_file/0005/39461/tait_technologycomparison_whitepaper_eng.pdf

TandCCA 2016. TETRA. Viitattu 18.10.2016. http://www.tandcca.com/tetra/tetra/

Tetratoday 2012. TCCA signs LTE agreement. Viitattu 14.10.2016. http://www.tetratoday.com/news/tcca-signs-lte-agreement

Tynan, D. 2015. Report: 1 in 5 Android Apps Is Malware. Viitattu 14.10.2015.

https://www.yahoo.com/tech/report-one-in-five-android-apps-is-malware-117202610899.html

Valtiovarainministeriö 2012. Teknisen ICT-ympäristöntietoturvataso-ohje. Viitattu 14.10.2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=5a273c6e-2935-4bbf-a4c6-f00e0f878db5&groupId=10229

Vehkalahti, V. 2008. Study of Video Transmission on TETRA Enhanced Data Service Platform. Viitattu 14.10.2016. https://www.netlab.tkk.fi/opetus/s38310/0708/Vehkalahti_25032008.pdf

Vinkvist J., Peltola, M. & Pesonen T. 2014. Finland Announces Hybrid Plan for Public-Safety Broadband. Artikkeli. Viitattu 14.10.2016. http://www.rrmediagroup.com/Features/FeaturesDetails/FID/494

Wendelken, S. 2013. Public Safety Makes Big Strides in LTE Standards Process Viitattu 14.10.2016. http://www.rrmediagroup.com/Features/FeaturesDetails/FID/362

Wendelken, S. 2016. South Korea Begins Public-Safety LTE Pilot in 3 Cities. http://www.rrmediagroup.com/News/NewsDetails/NewsID/11912

Wikipedia 2016. Pokémon Go. Viitattu 25.10.2016. https://en.wikipedia.org/wiki/Pok%C3%A9mon_Go

Wikipedia 2016. Public-key cryptography. Viitattu 14.10.2016. https://en.wikipedia.org/wiki/Public-key_cryptography

Wilson, M. 2016. Bittium Tough Mobile is ready to take on Blackphone for the most secure phone crown. Viitattu 14.10.2016. http://betanews.com/2016/01/27/bittium-tough-mobile-is-ready-to-take-on-blackphone-for-the-most-secure-phone-crown/

Zilis, M, 2014. South Korea Plans for Dedicated LTE Public-Safety Network by 2017. http://www.rrmediagroup.com/Features/FeaturesDetails/FID/482,

LIITE

ANDROID 6.0 AUTHTOKEN FORMAATTI

Authentication token format

The AuthToken format described in the hw_auth_token.h file is necessary for token sharing and compatibility across languages and components. See the following file:
hardware/libhardware/include/hardware/hw_auth_token.h
A simple serialization protocol with the required fields is defined in the table below. The fields are fixed size.
Field descriptions are below the table.

Field	**Type**	**Required or Optional**
AuthToken Version	1 byte	Required
Challenge	64-bit unsigned integer	Optional
User SID	64-bit unsigned integer	Required
Authenticator ID	64-bit unsigned integer in network order	Optional
Authenticator type	32-bit unsigned integer in network order	Required
Timestamp	64-bit unsigned integer in network order	Required
AuthToken HMAC key (SHA-256)	256-bit blob	Required

Field descriptions

This section describes the fields of the AuthToken table above.

AuthToken Version: Group tag for all fields below.

Challenge: A random integer to prevent replay attacks. Usually the ID of a requested crypto operation. Currently used by transactional fingerprint authorizations. If present, the AuthToken is valid only for crypto operations containing the same challenge.

User SID: Non-repeating user identifier tied cryptographically to all keys associated with device authentication. For more information, see the Gatekeeper page.

Authenticator ID (ASID): Identifier used to bind to a specific authenticator policy. All authenticators have their own value of ASID that they can change according to their own requirements.

Authenticator Type: Either Gatekeeper or Fingerprint, as follows:

Authenticator Type	Authenticator Name
0x00	Gatekeeper
0x01	Fingerprint

Timestamp: Time (in milliseconds) since the most recent system boot.

AuthToken HMAC key: Keyed SHA-256 MAC of all fields except the HMAC field.