Hannu Peltonen

Kodin IoT-laitteiden suojauksen esittely- ja koulutusympäristö

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

5.5.2019

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Hannu Peltonen Kodin IoT-laitteiden suojauksen esittely- ja koulutusympäristö 44 sivua 5.5.2019
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	IoT and Cloud computing
Ohjaaja(t)	Lehtori Marko Uusitalo

Insinöörityön päätavoite oli pyrkiä rakentamaan esittely-ympäristö kodin IoT-laitteiden ja muiden päätelaitteiden suojauksen esittelylle ja koulutuksille. Ympäristö rakennettiin ja testattiin Zyxel-reitittimen VMG3927-50-mallilla ja siihen integroidulla F-Secure Sensen IoT-suojan yhdistelmällä. Haittaliikennettä simuloitiin turvallisilla mutta haitalliseksi luokitelluilla www-osoitteilla.

Työn toinen tavoite oli tutkia myös muita verkkoliikenteen suojaukseen liittyviä haasteita sekä mahdollisuuksia tietoliikenneverkon eri tasoilla. Työssä tutkittiin yksityiskohtaisesti salatun HTTPS-liikenteen luonnetta ja merkitystä tietoliikenneverkon monitoroinnin näkökulmasta. Salatun liikenteen osuus kaikesta internetliikenteestä on noussut merkittävästi aivan muutamina viime vuosina. HTTPS-liikenteen teknisten toteutusten kehitys on ollut nopeaa viime vuosina, samoin erilaisten HTTPS-liikenteen hyökkäysten kehittyminen.

Työtä tehdessä opittiin uusimman TLS 1.3 -protokollan tärkeitä yksityiskohtia sekä miten ne eroavat kaikista vanhemmista TLS- ja etenkin SSL-versioista. Yllättävän pienellä yksityiskohdalla eli SNI:lla tulee olemaan palomuurien parissa erittäin suuri rooli, koska TLS 1.3 -protokollassa mahdollisuus luvalliseenkin TIA-toimintaan on merkittävästi vaikeutunut uuden Diffie-Hellman-salausavaimen kättelymekanismin muodossa.

Avainsanat	IoT, HTTPS, TLS, salaus, internetsuojaus

Author(s) Title Number of Pages Date	Hannu Peltonen Training and demo environment of home IoT-devices protection system. 44 pages 5th May 2019
Degree	Bachelor of Engineering
Degree Programme	Computer engineering
Specialisation option	IoT and Cloud protection
Instructor(s)	Principal Lecturer Marko Uusitalo

The main target for this engineering theses was to build protection and demo environment of home IoT-devices. It will include Zyxel router model VMG3927-50 that has embedded into F-Secure Sense SDK software. Demo environment is full system with host computers and actual router itself. Harmful www pages and anomaly http traffic were simulated by harmful demo pages provided by F-Secure.

Secondary target for this work was to study challenges and possibilities of network traffic protection. Thesis work studied in detail HTTPS traffic and its nature on network monitoring perspective. Share of encrypted HTTPS traffic out of all www traffic is increasing on enormous speed. Development of HTTPS protocol stack has been rapid on last years, and as well as there has been rapid development on different attacks against different TLS protocols.

Writer gained new information regarding TLS 1.3 implementation and usage. Also differences of older TLS 1.2 compared to the newest version TLS 1.3 were identified detailly. There is surprisingly small detail called SNI that is playing major role on network monitoring on future. It will create new way of monitoring as traditional DPI approach is difficult with TLS 1.3. Classical DPI enabled firewalls and other network devices will need to work differently as Diffie-Hellman TLS handshake implementation on TLS 1.3 will make also legal TIA process very difficult for DPI purposes.

Keywords	IoT, HTTPS, TLS, encryption, internet protection

Sisällys

Lyhenteet

1 Johdanto 1

2 Verkkolaitteiden tietoturvauhat ja niiltä suojautuminen 2

2.1 Tietoturva ja älykäs laite 3
2.2 Klassiset PC-haittaohjelmat ja niiltä suojautuminen 3
2.3 Puhelinten ja tablettien tietoturva 6
2.4 WiFi-verkon IoT-laitteet 7
2.5 4G- & LTE-verkon IoT-laitteet 8
2.6 Intregroidun SIM-kortin eli nk. eSIM-kortin omaavat IoT-laitteet 8
2.7 Uudentyyppiset IoT-haittaohjelmat 9
2.8 Verkkotason suojaus operaattorin toimesta 10
2.8.1 Broadband forum 11
2.8.2 Tulevaisuuden modeemien hallintatarpeet kodeissa 12
2.8.3 USP-protokolla – usean verkkokontrollerin hallintaprotokolla 13
2.8.4 Teleoperaattorin rooli uudessa IoT-maailmassa 14
2.8.5 Internetin reititys 15
2.9 Verkkoselaus ja sen salaaminen 16
2.9.1 HTTP eli selkokielinen www-liikenne 16
2.9.2 Verkkoselauksen salaamisen kehitys 16
2.9.3 HTTPS ja SSL 17
2.9.4 Moderni TLS-salaus www-selainliikenteessä 17
2.9.5 SNI-parametri TLS-protokollassa 18
2.9.6 TLS-kättely selaimen ja palvelimen välillä 20
2.9.7 DoH eli DNS HTTPS:n ylitse 22
2.9.8 DoT eli DNS TLS:n ylitse 23
2.9.9 DPI ja TLS-kättely 23
2.9.10 IPv4- ja IPv6 -protokollat ja TLS 25

3 Tekninen IoT-suojauksen esittely-ympäristö 25

3.1 Esittely-ympäristön demonstraatiolaitteet 26
3.2 Testiosoitteet 27
3.3 Esittelyprosessi 27

4 Esittely-ympäristön konfigurointi loppukäyttäjän päätelaitteella 28

4.1 Tuotteen hallinta matkapuhelimesta 28
4.2 F-Secure Sensen profiilien konfigurointi 32
4.3 Ajallinen internetin käytön eston konfigurointi 33
4.4 Internetselauksen sisällön suodatuksen konfigurointi 34

5 Loppukäyttäjän käyttökokemus 35

5.1 Käyttökokemus normaalissa internetkäytössä 35
5.2 Käyttökokemus estetyssä internetkäytössä 35
5.3 Käyttökokemus haitallisen sivuston käyttötapauksessa 36
5.4 Haitallisen aikuisviihdesivuston selaaminen 36
5.5 Aikarajoituksen kohtaaminen www-selauksessa 37
5.6 HTTPS-sivun suojaus 38
5.7 Saastuneen laitteen liikenteen detektointi 38

6 Yhteenveto 40

6.1 Haasteet kodin tietoturvassa 40
6.2 Haasteet tietoturvasuojauksessa TLS-protokollan kanssa 41
6.3 Mahdollisuudet kodin tietoturvassa 42

Lähteet 44

Lyhenteet

CPE	Customer-premises equipment. CPE-laitteella tarkoitetaan yleisesti teleoperaattorin toimittamaa kodin reititintä, joka kytketään kotiverkon ja teleoperaattorin toimittaman liittymän väliin. CPE-laite voi olla 4G-mobiiliverkon tai kiinteän verkon reititinlaite.
DNS	Domain Name Server. Internetin nimipalveluprotokolla, yleiskielessä lyhenne tarkoittaa myös itse DNS-palvelinta.
DoH	DNS over HTTPS. DNS-protokolla salattuna HTTPS:n ylitse, nopeasti yleistävä tapa DNS:n käytössä. DoH käyttää porttia 443.
DoT	DNS over TLS. DNS-protokolla salattuna HTTPS:n ylitse, nopeasti yleistävä tapa DNS:n käytössä. Tämä on äärimmäisen läheistä sukua yllä olevalle DoH:lle mutta toimii eri portissa. DoT toimii portissa 853.
ETH	Ethernet. Kiinteän paikallisverkon tämän päivän tyypillisin pakettipohjainen liikenteeseen perustuva lähiverkkoratkaisu.
EPP	End Point Protection. Klassinen lähestyminen päätelaitteiden suojaukseen, itse päätelaitteeseen asennettava suojausohjelmisto.
HTTP	Hyper Text Transfer Protocol. Selkokielisen www-liikenteen protokolla.
HTTPS	Hyper Text Transfer Protocol Secure. Muutoin kuten yllä mutta S-kirjain lyhenteessä tarkoittaa TLS-salauksen lisäämistä protokollaan.
IoT	Internet of Things. Esineiden internet, tarkoittaa kaikkia laitteita, joita voidaan yhdistää Internettiin.
IP	Internet Protocol. Internetin kulmakivi eli tietoliikenneprotokolla ja protokollaperhe, jolla kaikki tieto liikkuu internetissä. Tunnetaan myös nimellä TCP/IP-protokolla.
LAN	Local area network. LAN on rajattu kiinteän tekniikan paikallisverkkoalue, kotona tai työpaikalla.

LTE	Long Term Evolution. Mobiilin laajakaistaverkon eli internetin käyttöön suunniteltu tiedonsiirtotekniikka, jota käytetään 4G-yhteyksissä.
MItM	Man in the Middle. Hyökkäys jossa nk. välimies ottaa paikan lähettäjän ja vastaanottajan välissä, ja näkee kaiken kommunikaation. Tämä on lainvastainen toiminne, siinä missä TIA on laillinen.
NAT	Network Address Translation. Osoitteenmuutosmenetelmä julkisesta yksityiseen IP-osoiteavaruuteen esimerkiksi kodin CPE-laitteessa.
SDK	Software development kit. Ohjelmisto, jonka avulla voidaan edelleen kehittää jotain ohjelmistoa käytettäväksi johonkin tarkoitukseen.
SNI	Server Name Indication. Kertoo TLS-kättelyssä kohdepalvelimen www-domainin.
SSL	Secure Socket Layer. Vanha mutta yleisesti käytössä oleva termi www-selauksen salaukselle.
TCP	Transmission Control Protocol. IP-protokollan päällä toimiva yhteydellinen tiedonsiirtoprotokolla.
TIA	TLS Intercept Application. TIA-lyhenne tarkoittaa laillista TLS-salauksen purkua ja salausta palomuurissa tai muussa yhdyskäytävälaitteessa.
ToR	Term of Reference. ToR selain on työkalu päästä kiinni nk. dark nettiin.
TLS	Transport Layer Security. Uusi termi www-selauksen salaukselle. Tarkoittaa samaa kuin SSL.
WAN	Wide area network. Tiedonsiirtoverkon osa, joka muodostaa nk. suuralueverkon. Tämä on teleoperaattorien ylläpitämää kokonaisuutta, missä tieto liikkuu ja muodosta siis kaikkien tunteman Internetin.
WLAN	Wireless Local Area Network. Langaton verkko, niin työpaikalla kuin kotona. Tunnetaan myös WiFi-nimellä. IoT-laitteet hyvin tyypillisesti kytkeytyvät WLAN-verkon kautta WAN-verkkoon.

1 Johdanto

Insinöörityö tehdään F-Secure Oyj:n toimeksiannosta. Tehtävänä on rakentaa esittely- ja koulutusjärjestelmä älykodin reitittimen ja älykodin nk. Internet of Things -laitteiden (IoT) ja klassisten tietokone- ja puhelinlaitteiden muodostamaan ympäristöön, joka suojataan F-Securen kotireitittimeen tarkoitetulla tietoturvaohjelmistolla. Kotireititin on paikallisen teleoperaattorin toimittama laite, joka yhdistää kodin WiFi- ja LAN-verkon internetiin.

Toisaalta tämä insinöörityö tarkastelee internetin tietoliikenteen kehittymistä HTTP-liikenteen Transport Layer Security -salauksen (TLS) näkökulmasta. Salatun liikenteen näkökulmasta tutkitaan myös useamman tason tietoturvan mahdollisuuksia ja haasteita IoT-laitteiden, puhelinten ja tietokoneiden kokonaissuojaukselle.

Insinöörityön tavoitteena on rakentaa siirrettävä ympäristö, jossa on edustettuna tyypilliset älykodin laitteet. Tällä ympäristöllä voidaan esitellä kodin tietoturvasuojauksen kokonaisratkaisun toimintaa eli hyödyntää järjestelmää koulutuksessa sekä myös esitellä kodin tietoturvan uhkakuvia tietoturvahyökkäysesimerkeillä.

F-Secure on suomalainen tietoturvaohjelmistoja suunnitteleva, valmistava ja myyvä yritys. F-Secure valmistaa tuotteita niin yritys- kuin kuluttajamarkkinalle. Yrityksen pääkonttori on Helsingissä, Suomessa. Kuluttajaliiketoiminnan kivijalka on kansainvälisessä teleoperaattoriyhteistyössä. Kansainvälisiä operaattoripartnereita on yli 200 yritystä viidellä mantereella. F-Securen uusimpia kuluttajatuotteita on F-Secure Sense Software Development Kit -ohjelmisto (SDK), jolla voidaan integroida IoT-laitteiden tietoturva kiinteäksi osaksi kodin reititintä, jonka paikallinen teleoperaattori toimittaa.

Zyxel on maailman johtavia reititin- ja tietoliikennelaitteiden valmistaja. Sen pääkonttori on Taiwanissa. Zyxel valmistaa laajasti erilaisia koteihin ja yrityksille soveltuvia reitittimiä ja muita tietoliikenteen laitteita.

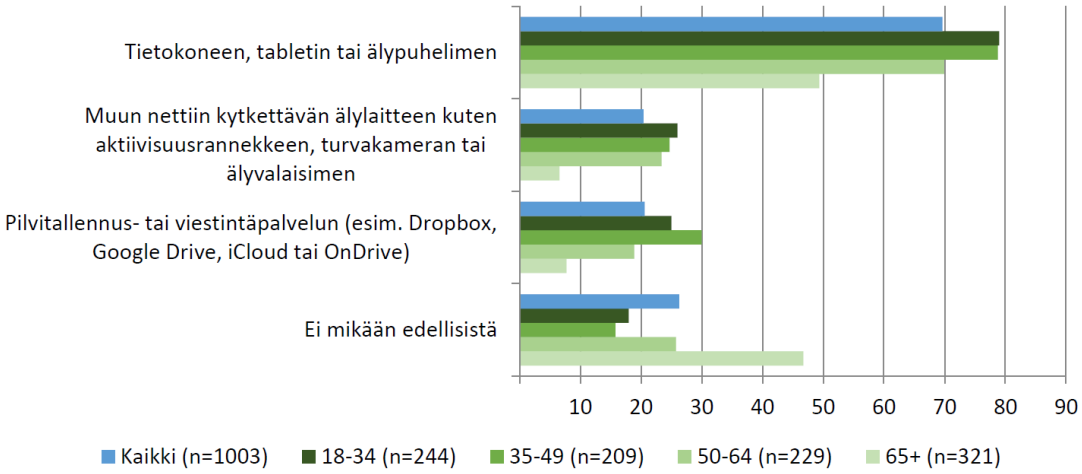
Elisa Oyj on Suomen markkinajohtaja sekä kiinteän että mobiilin tietoliikenneverkon palveluiden tarjoajana. F-Secure tekee yhteistyöprojektia [1] Elisan ja Zyxelin kanssa,

minkä tavoitteena on integroida Zyxel-reitittimeen F-Secure Sensen SDK-toiminnallisuus. Laite on tulossa kuluttajamarkkinan reititintuotteeksi älykoteihin turvaamaan nk. IoT-laitteiden käyttöä.

2 Verkkolaitteiden tietoturvauhat ja niiltä suojautuminen

Internetiin liitettävien laitteiden määrä lisääntyy voimakkaasti. Määrää ovat lisänneet huomattavasti nk. IoT-laitteet eli kotona esimerkiksi jääkaapit, kamerat, pesukoneet ja muut laitteet, joita voi ohjata ja/tai monitoroida internetin ylitse. Tämä laitteiden lisääntymisen vauhti kiihtyy jatkuvasti. Kaikki internetiin liittyvät älykkäät laitteet ovat tietoturvamurtojen ja muiden uhkien kohteena – aivan kaikki laitteet.

Kuvassa 1 esitetään Traficomin (entisen Viestintäviraston) tuore tutkimus [2], kuinka moni suomalainen harkitsee puhelimen tai älylaitteen hankintaa.



Kuva 1. Kuinka suuri osuus suomalaisista suunnittelee hankkivansa tai on hankkinut viimeisen kolmen vuoden aikana älylaitteen tai pilvipalvelun.

Kuva 1. Traficomin tutkimus suomalaisten halukkuudesta ostaa IoT-laitteita [2]

Jotta saadaan kokonaiskuvaa kodin tietoturvan todellisesta tarpeesta, seuraavaksi käsitellään lyhyesti tietoturvan ilmentymät ja toisaalta suojaustarpeet kodin klassisesta pöytätietokoneesta aina IoT-laitteeseen saakka. Jos kokonaisuus ei toimi, eivät toimi

myöskään osakokonaisuudet tietoturvan näkökulmasta - siksi kokonaiskuvan näkeminen ja ymmärtäminen on tärkeää.

2.1 Tietoturva ja älykäs laite

Olisi varmasti liiketoimintapuolen oman tutkimuksen aihe, miksi älykkäät laitteet eivät toteuta sellaista tietoturvaa, että niitä voisi käyttää sellaisenaan ilman kolmannen osapuolen tietoturvaa IoT-laitteen näkökulmasta. Näin on kuitenkin ollut siitä lähtien, kun PC-tietokoneiden massamarkkinat alkoivat 1980-luvulla. Mitä enemmän erilaisia laitteita on tullut tarjolle, sitä enemmän verkkorikollisuus on ottanut jalansijaa. Nykyään verkkorikollisuudesta käytetään nimeä kyberrikollisuus. Näistä ilmiöistä saa nykyään lukea ihan tavallisista sanomalehdistä päivittäin.

Tavallisen, valveutuneenkin kuluttajan on mahdotonta estää kyberhyökkäyksiä tapahtumasta, jos laitteissa ei ole tarvittavaa lisäsuojausta. Tietoturva on kuluttajien kannalta äärimmäisen vaikea ongelma, joten he tarvitsevat siinä apua. Yrityksen tai valtion tilanne on tietoturvan kannalta luonnollisestikin vielä haastavampi.

Älykkäät laitteet ovat haavoittuvia. Mitä enemmän markkinalla on älykkäitä laitteita kuluttajien käytössä, sitä enemmän kyberrikollisilla on massamarkkinaa, mihin kohdistaa hyökkäyksiä ja siten ansaita erilaisilla rikollisilla tavoilla rahaa tai muuta etua.

Tämä insinöörityö ei pyri ratkaisemaan tätä yllä mainittua valitettavaa tosiasiaa tietoturvan tarpeesta. Tietokoneiden ja IoT-laitteiden haavoittuvuudet otetaan annettuna faktana tässä työssä.

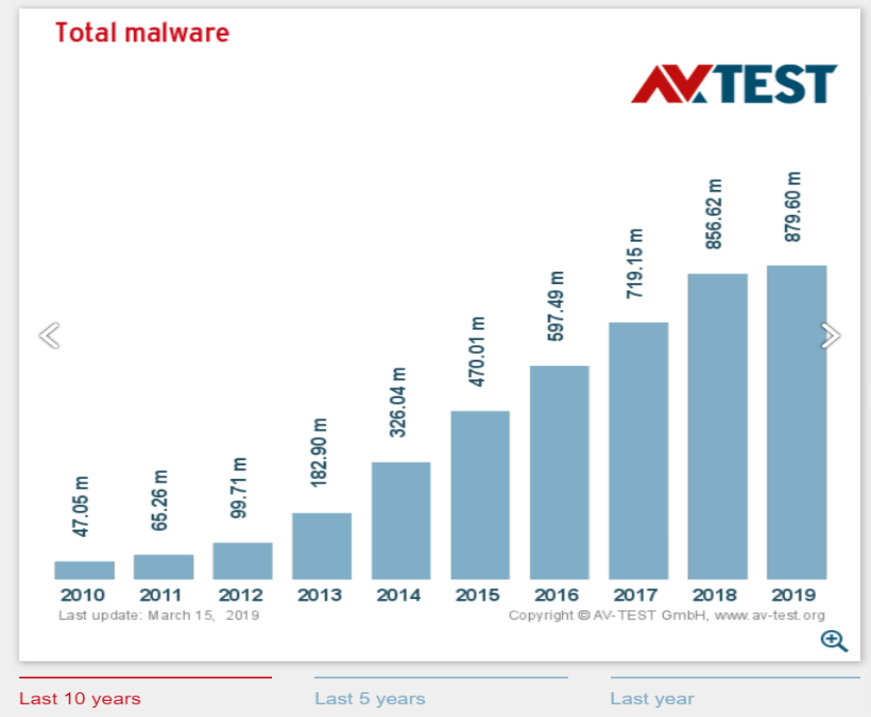
2.2 Klassiset PC-haittaohjelmat ja niiltä suojautuminen

PC-tietokoneille on ollut haittaohjelmia aina vuodesta 1986 lähtien. Ensimmäinen tunnettu haittaohjelma oli nimeltään Brain [3]. Muita haittaohjelmia oli jo huomattavasti aiemmin, mutta tässä yhteydessä käsitellään vain PC-tietokoneille suunnattuja haittaohjelmia.

PC-tietokoneiden haittaohjelmia on nykyään hyvinkin erilaisia. Yhteistä niille on se, että ne toimivat ja leviävät PC-tietokoneissa ja niiden kautta. Yleisin tarttumisvektori lienee verkon kautta tarttuva haittaohjelma. Haittaohjelmia tarttuu silti edelleen myös USB-tikuilta ja jopa CD- ja DVD-levyiltä.

Eräs merkittävä taitekohta klassisten PC-tietokoneiden haittaohjelmissa koettiin 2000-luvun alussa. Muutamassa aallossa verkkomadot toisensa jälkeen kulkivat kirjaimellisesti maapallon ympäri parhaimmillaan alle vuorokaudessa. Esimerkkejä näistä ovat Sasser [4], Melissa [5] ja Conficker [6]. Ne levisivät erittäin nopeasti tartuttaen ennätysmääriä tietokoneita ja kuormittivat samalla internetin runkoverkkoa. Nämä tapahtumat muuttivat maailmaa ja haittaohjelmamarkkinaa monella tapaa. Haittaohjelmat levisivät ensimmäistä kertaa maailmanlaajuisesti aiheuttaen haittaa kaikkialla. Tästä oli enää pieni hyppäys siihen, että haittaohjelmilla pystyttiin ansaitsemaan rahaa ja muuta etua rikollisessa mielessä.

Kuvassa 2 on esitetty PC-tietokoneiden haittaohjelmien kehityskulkua [7]. Haittaohjelmien määrä kehittyy nousujohteisesti, ja on kehittynyt jo useita vuosia.



Kuva 2. AV-Test Institute -testilaboratorio [7]

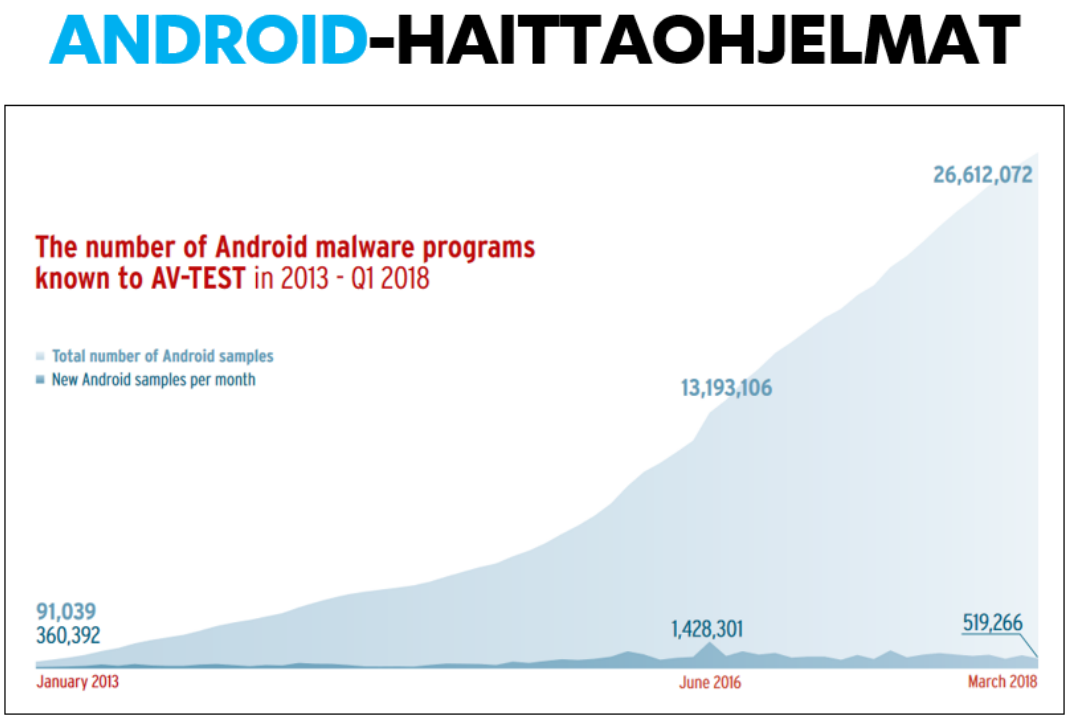
Jo 90-luvun alkupuolelta saakka on ollut saatavilla PC-tietokoneeseen paikallisesti asennettava virustutka, joka nykynimeltään tunnetaan paremmin internetsuojana. Ohjelmistotuotteiden valmistajia on useita niin Euroopassa kuin Pohjois-Amerikassakin. Ohjelmistot ovat kehittyneet voimakkaasti, ja ne sisältävät nykyään tekoälyominaisuuksia, mikä onkin välttämätöntä, koska nk. nollapäivähaavoittuvuudet ovat arkipäivää. Niin sanotulla allekirjoituspohjaisella eli nk. hash-tunnisteisiin perustuvalla antivirusohjelmalla ei ole nykyään sijaa hyvälaatuisessa suojauksessa, koska nollapäivähaavoittuvuudet ovat yleisiä. Jo pelkästään nollapäivähaavoittuvuuden luonteen takia hash-perusteisen tunnistuksen on mahdotonta toimia laadukkaasti nykypäivän ympäristöissä. Haittaohjelmia ja nollapäivähaavoittuvuuksia on yllättävän helppo ostaa nk. dark netin markkinapaikoilta. ToR tulee lyhenteestä Term of Reference (ToR). ToR-selainta voidaan käyttää moneen laittomaan ja lailliseen asiaan internetin nk. dark netin puolella. Haittaohjelmien etsiminen ja ostaminen tapahtuu ToR-selaimella anonyymisti, etenkin jos maksut suorittaa bitcoinilla. Haittaohjelmat löytyvät valitettavan helposti aivan tavallisilla hakusanoilla, ja jotta tämä insinöörityö ei olisi suora ohje, miten ostaa ja valmistaa haittaohjelmia, varsinaiset linkit on jätetty pois tästä työstä tarkoituksella.

Paikallisesti asennettava haittaohjelmatutka eli antivirusohjelma on tunnistuskyvyn puolesta tiettävästi edelleen paras ratkaisu. Siinä on kuitenkin muita mahdollisia ongelmia - yksinkertaisimpana valitettavasti se, että edes ostettuja ohjelmia ei asenneta koti- eikä työkoneille, jolloin suojaakaan ei luonnollisesti ole olemassa. F-Secure on markkinajohtaja teleoperaattorimarkkinan tietoturvassa ja täten sillä on lähes kahdenkymmenen vuoden tieto tästä asiasta. Päätelaitteeseen asennettava tietoturva jää maailmanlaajuisesti katsottuna hyvin usein asiakkaalta asentamatta – samoin kuin moni muukin ostettu ohjelmisto. Toisin sanoen myydyn EPP-tietoturvan aktivointiaste on parhaimmillaankin noin 80%. Paikallisesti asennetun ohjelman ylivertaisuus perustuu siihen hyvin yksinkertaiseen tosiasiaan, että se voi tunnistaa haittaohjelman, tarttuu se sitten minkä tahansa median kautta. Tämä on tärkeä asia huomata. Tämä asia tulee tärkeäksi etenkin, kun aletaan miettiä mobiililaitteita, jotka on mahdollisesti suojattu WiFi-verkon vaikutusalueella. Suoja saattaakin loppua, kun laite siirtyy esimerkiksi 4G-verkon piiriin. Tätä asiaa käsitellään lisää tuonnempana.

2.3 Puhelinten ja tablettien tietoturva

Älypuhelinten ja tablettien esiasteet nähtiin kuluttajamarkkinalla jo vuosina 2001-2002. Samoin ensimmäiset versiot mobiililaitteiden tietoturvaohjelmistoista nähtiin tällöin. Mobiililaitteiden haittaohjelmien määrät ovat kuitenkin alkaneet nousta vasta vuosien 2015-2016 tuntumassa. On edelleenkin niin, että Android-laitteeseen haittaohjelmat tarttuvat itseasiassa käyttäjän omasta toimesta. Tyypillisin haittavektori on Googlen Play Storesta ladattu ohjelma, johon on injektoitu haittaohjelma. Android-haittaohjelmien määrä tullee kasvamaan merkittävästi silloin, kun jokin taho onnistuu tekemään haittaohjelman, joka tarttuu PC-tietokoneen haittaohjelman tavoin automaattisesti ilman loppukäyttäjän vuorovaikutusta. Kuvassa 3 on kaavio Android-haittaohjelmien määrän kehityksestä [8].

Applen iOS-laitteissa ei käytännössä nähdä haittaohjelmia. Mobiilien laitteiden osalta haittaohjelmia tavataan ainoastaan Android-laitteissa.



Kuva 3. Kaavio Android-haittaohjelmien määrän kehityksestä [8].

2.4 WiFi-verkon IoT-laitteet

IoT-laitteen määritelmästä näkee variaatioita, mutta yleisen ja vallalla olevan määritelmän mukaan laitteet, jotka voivat itsenäisesti aistia, viestiä ja/tai kommunikoida älykkäästi aistimansa perusteella, ovat IoT-laitteita. Esimerkiksi Gartner määrittelee asian tällä tavalla [9].

Kodin WiFi-verkossa voikin olla kytkettynä todella useita ja hyvin erityyppisiä IoT-laitteita: esim. kello ja askelmittari, pesukone, jääkaappi, kamera ja TV. Kodin automaatio, turvallisuus ja lukot on myös mahdollista valita IoT-tuella. Seuraavassa IoT:n aallossa on nähtävissä älykkäät vaatteet ja esimerkiksi älysilmälasit. Tämä voi kuulostaa utopistiseltä mutta on tulevaisuudessa todellisuutta.

IoT-laitteille on tyypillistä, että ne kommunikoivat itsenäisesti, jo ihan IoT:n määritelmän mukaan. On hyvin tyypillisistä, että näillä laitteilla on myös jonkinlainen kytkös johonkin pilvipalveluun, mikä taasen tarkoittaa liikennettä julkisen internetin ylitse.

Tämä edellä mainittu tarkoittaa haittaohjelmien näkökulmasta useitakin eri asioita. Ensinnäkin itse laite on kiinni internetissä, ja se on älykäs. Älykäs tarkoittaa käytännössä samaa asiaa kuin haavoittuva. Tämä tosiasia tunnetaan Mikko Hyppösen lakina, ”smart means vulnerable” eli älykäs tarkoittaa haavoittuvaa [10]. Ihan pienimmillekin ja yksinkertaisimmillekin IoT-laitteille on päivitysohjelmia haavoittuvuuksien takia. Toisekseen se, että IoT-laite liikennöi julkisen verkon ylitse, on riskikohta turvallisuudelle. Kolmantena riskinä on pääsy pilveen, mikä tarkoittaa aina automaattisesti jonkinlaisia käyttäjätunnuksia. Tämäkin on normaalille kuluttajalle vaikea asia. Tyypillisimpiä ongelmia ovat liian lyhyet salasanat, jotka vieläpä toistuvat eri palveluissa, ja sekin on iso erillinen ongelma.

Suojausnäkökulmasta päästäänkin sitten uusien asioiden äärelle. IoT-laite on usein varustettu nk. ”proprietary” eli valmistajan omalla käyttöjärjestelmällä. Vaihtoehtoisesti käyttöjärjestelmänä on jonkinlainen Linux-versio. Kaikkia edellä mainittuja yhdistää se tosiasia, että paikallista antivirustuotetta ei käytännössä ole saatavilla. Laite on niin pienellä mikroprosessorilla tai jopa vain mikrokontrollerilla varustettu, että ei ole mitään mahdollisuutta asentaa paikallista suojausta. Laitteen suorituskyky on niin rajallinen, että tyypillisen IoT-laitteen suorituskyky ei yleensä kestä edes pienen kolmannen osa-

puolen ohjelmiston rasitusta. Lisäksi IoT-käyttöjärjestelmä ei ole tyypillisesti tuettu perinteisten suojausohjelmien näkökulmasta. Kaikki tämä johtaa siihen, että paikallisen suojauksen ratkaisuja ei tänä päivänä ole olemassa IoT-laitteille.

2.5 4G- & LTE-verkon IoT-laitteet

WiFi-verkon tapaan IoT-laitteita löytyy myös 3G/4G-laitteina, ja kohta 5G-laitteina. Näissä on syystä tai toisesta itsenäinen yhteys WiFi-verkon sijasta. Tämä on riskinäkökulmasta sekä etu että haitta.

Kun IoT-laite ei ole kiinni kodin WiFi-verkossa, ei myöskään ole nähtävissä, että murtautuminen kodin muihin laitteisiin helpottuisi ko. IoT-laitteen mahdollisen haavoittuvuuden takia. Tämä johtuu siitä yksinkertaisesta syystä, että 4G-laite on eristetty muualle kodin verkosta. Voidaan sanoa toisin sanoen; laitteen suojaaminen on todella vaikeaa, koska se on kiinni julkisessa verkossa suoraan julkisella IP-osoitteella eikä itse laitteeseen tyypillisesti pysty asentamaan paikallista suojausta, kuten aiemmin todettiin.

Tämä edellä mainittu aidon mobiililaitteen eli esim. 4G-laitteen IoT:n tyyppinen ratkaisu on erittäin ongelmallinen tietoturvan näkökulmasta. Suojausta ei voi oikein mitenkään toteuttaa paikallisesti, ja koska laite on suoraan kiinni julkisessa verkossa, on tietoturva ratkaistava muilla keinoilla. Tähän liittyviä ratkaisuja käsitellään tuonnempana.

2.6 Intregroidun SIM-kortin eli nk. eSIM-kortin omaavat IoT-laitteet

5G-verkon myötä tulemme näkemään vielä kapeampia ja siten edullisempia valvonta- ja kommunikaatiokanavia, joita 5G-protokolla mahdollistaa. Tämä tulee tarkoittamaan IoT-laitteiden määrän runsasta lisääntymistä.

Tämän tyyppisiä laitteita on jo muutamia markkinoilla. Esimerkiksi Garminilla [11] on kello, joka tukee eSIM-ratkaisua. Samoin Telialta tulee saataville eSIM-laitteita [12] ensimmäisenä Suomessa.

Tietoturvan näkökulmasta riskit ovat vahvasti samankaltaisia kuin 4G IoT -laitteissa. 4G/5G -tyyppisten IoT-laitteiden lisääntyminen tulee vain korostamaan tietoturvan merkitystä.

On ilmeistä, että tietoturvan tarve korostuu kuluttajien saataville tulvivien uudentyyppisten laitteiden myötä. Täytyy muistaa, että kyberrikollisuuskin on liiketoimintaa, joskin laitonta. Tästä seuraa se, että kyberrikollisuuteen käytetään resursseja samoin kuin laillisenkin liiketoiminnan kehittämiseen. Tällöin myös tämän rikollisen liiketoiminnan laatu nousee, mikä taas osaltaan nostaa laadukkaan tietoturvan tarvetta.

2.7 Uudentyyppiset IoT-haittaohjelmat

Kuluttajamarkkina on jo saanut tutustua uudenlaisiin haittaohjelmiin. Ensimmäisessä massiivisessa aallossa vuosista 2016-2017 alkaen Mirai-haittaohjelma tarttui verkon modeemeihin ja muihin laitteisiin. Mirai hyödynsi tavallaan niinkin alkeellista tekniikkaa kuin default- eli vakiosalasanoja: eli karuimmillaan esimerkiksi käyttäjätunnus on admin ja salasana on admin. Verkossa on runsaasti tällaisia laitteita, ja siksi Mirai alkeellisesta tekniikastaan huolimatta levisi todella laajalle. Se tarttui muun muassa ilmalämpöpumppuihin, web-kameroihin, kodin modeemeihin ja moniin muihin laitteisiin.

Tämä oli uuden ajan alku siinä mielessä, että haittaohjelman kohteena olivat aivan muut laitteet kuin älypuhelimet ja PC-tietokoneet.

Seuraava Miraita selvästi kehittyneempi haittaohjelma oli VPN-Filter [13], joka on huomattavasti monimutkaisempi. Miraista on useita variaatiota, ja ne osaavat jopa kirjoittaa itsestään osia modeemin flash-muistille. VPN-Filter lataa itsensä erillisissä moduuleissa useista eri syistä kohdelaitteeseen. Tällöin saavutetaan piiloutumiskykyä mutta modulaarisuus tukee myös ajatusta, että haittaohjelmaa voidaan hyödyntää monin eri tavoin myöhemmin.

Tiivistäen olemme saaneet tutustua hyvinkin monimutkaisiin ja erittäin toimiviin haittaohjelmiin, joiden toiminta kohdistuu kaikkiin mahdollisiin älykkäisiin laitteisiin, jotka ovat kiinni julkisessa verkossa. Näitä haittaohjelmia saatetaan käyttää valtiollisiin tarkoituksiin, mutta myös aivan tavallisiin rikollisiin ansaintatarkoituksiin. On valitettavasti myös

niin, että valtiollisen tason työkaluja on varastettu ja niitä on siten päätynyt tavallisten kyberrikollisten käytettäväksi [14]. Tällaiset työkalut ovat usein nk. nollapäivähaavoittuvuushyökkäystietoja, mikä tarkoittaa rikollisten näkökulmasta äärimmäisen tehokkaita haittaohjelmia.

Miten NSA, vakoojat ja hakkerit koskevat tavallista kuluttajaa, joka ehkä vain haluaa soittaa Android-puhelimellaan puheluita ja ehkäpä vain Suomessa? Kenties hän käy vain kotimaan verkkopankissa ja HS.fi-verkkosivuilla lukemassa uutiset. Helposti unohtuu, että kyberrikollisten toiminta on volyymiliiketoimintaa ja se kohdistuu kaikkiin mahdollisiin haavoittuviin laitteisin, jotka ovat kiinni internetissä. Valtioiden rajat eivät kyberrikollisen toimintaa estä, eivät liioin hidasta.

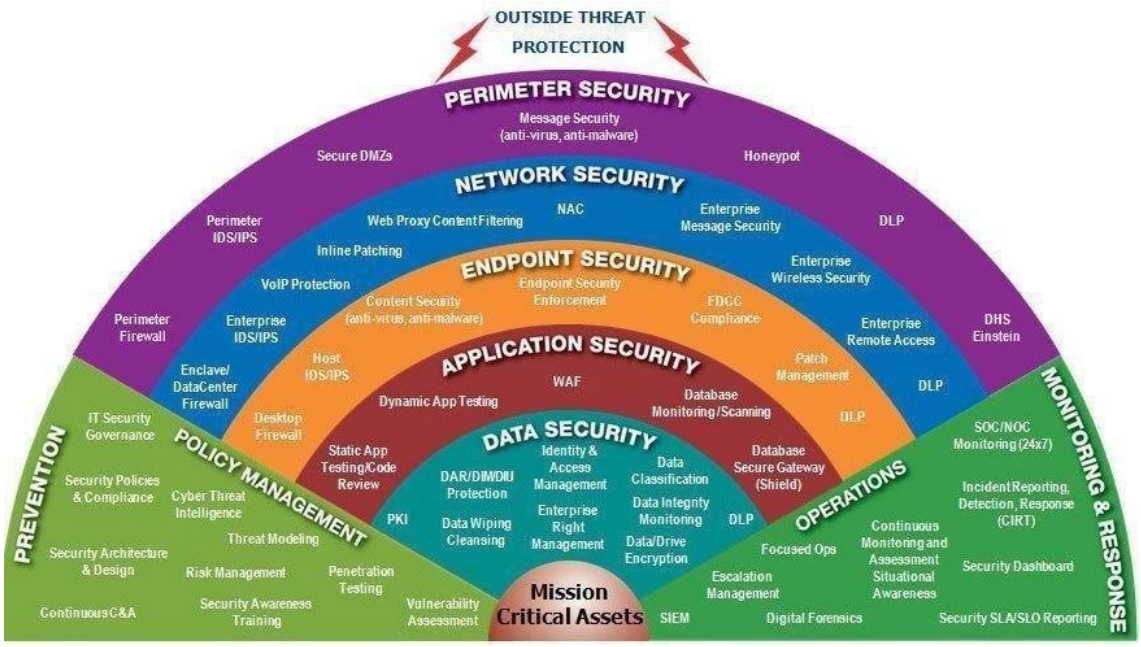
2.8 Verkkotason suojaus operaattorin toimesta

F-Secure Sense on suojausmekanismi, joka toimii kodin ja laajakaistaverkon rajapinnassa. Tarkemmin sanottuna se on F-Securen tuote, joka toimii kodin reitittimessä, osana reitittimen kokonaistoimintaa. F-Secure Senseä käsitellään tarkemmin seuraavassa luvussa. Kuten aiemmin mainittiin, mobiililaite, älypuhelin tai vaikkapa WiFi-tabletti siirtyessään naapurin kahvilaan ei ole enää lähtökohtaisesti kodin reitittimen vaikutuspiirissä.

Kokonaiskuvan kannalta on tärkeä ymmärtää, mitä kaikki yllä kuvatut erilaisiin laitteisiin liittyvät uhat tarkoittavat. Esimerkiksi yksittäistä IoT-laitetta ei tulisi tarkastella omana yksinäisenä saarekkeenaan vaan sitä tulisi tarkastella kokonaisuuden osana. Laadukkaasti toteutettuna tietoturva on toimiva kokonaisuus. Jos se taasen rakennetaan toisistaan erillään olevina osina, kokonaisuus ei hahmotu eikä liioin toimi. Kokonaisrakenteeseen jää tällöin kyberrikollisen toivomia tietoturvareikiä eli haavoittuvuuksia.

Cyber security hub [15] kuvaa tätä verkon kaikkien tasojen suojausta erinomaisesti kuvassa 4. Kuva on ensisijaisesti tarkoitettu yritysmaailman puolelle, mutta se on erittäin käyttökelpoinen myös kodin tietoturvan tarkasteluun. Kodin suojauksen aloitustasona voidaan kuvasta mainita nk. Endpoint Security, johon on aiemmin viitattu End Point Protection -tuotteilla (EPP). Näillä suojataan klassisia PC-tietokoneita, mm. kannettavia tietokoneita sekä älypuhelimia. Sen sijaan kuvassa oleva Network Security on

se osuus kotona, mitä tämä insinöörityö käsittelee eli kodin verkon reunalla tapahtuvaa suojausta. Uutena ajatuksena kodin suojaukseen on sitten kuvassa uloimmassa kehässä näkyvä osuus eli Perimeter Security. Se tapahtuisi nimenomaan teleoperaattorin toimesta heidän omassa verkossaan, joka siis toimii solmupisteenä kuluttajan ja laajakaistaverkon välissä.

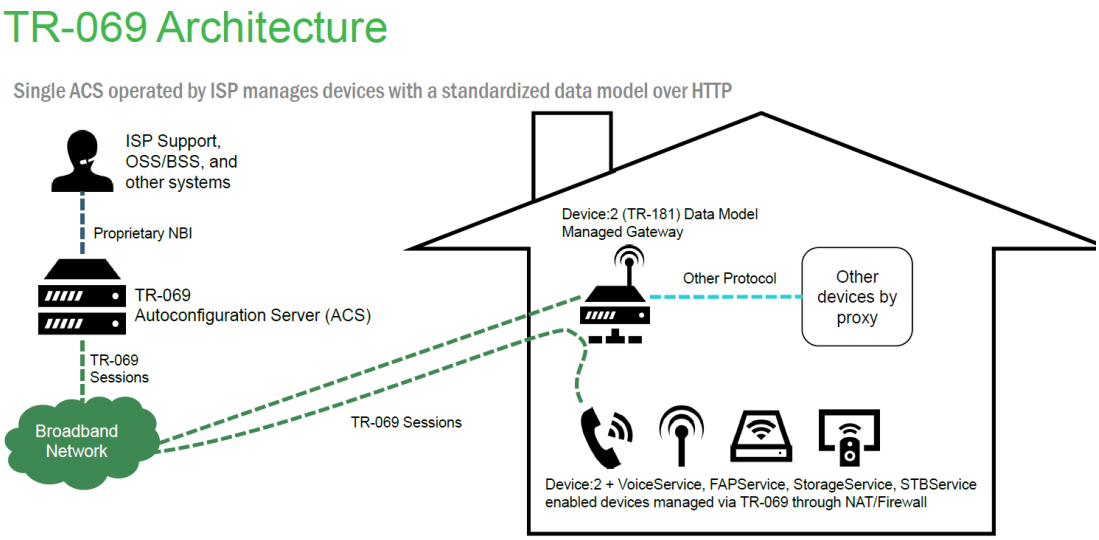


Kuva 4. Verkon eri tasojen suojaus [15]

Mitä me tästä kuvasta opimme? Tässä kuva näyttää erinomaisesti, mikä on suorastaan ilmeistä: laadukasta tietoturvaa ei voi saada aikaan yhdellä tasolla, vaan tietoturva on kokonaisuus, jonka tulee kytkeytyä yhteen toimivana kokonaisuutena niin kotona kuin työpaikalla. Tässä teleoperaattorilla on keskeinen rooli.

2.8.1 Broadband forum

Broadband forum (www.broadband-forum.org) on voittoa tavoittelematon organisaatio, joka työskentelee erilaisten verkkoasioiden parissa. Sen suurin menestystuote on erittäin laajasti käytössä oleva TR-069, joka on Customer Premises Equipment -laitteiden (CPE) hallintaprotokolla. Kuvassa 5 näytetään yleiskuvaus tästä vuonna 2002 julkaistusta protokollasta [16].

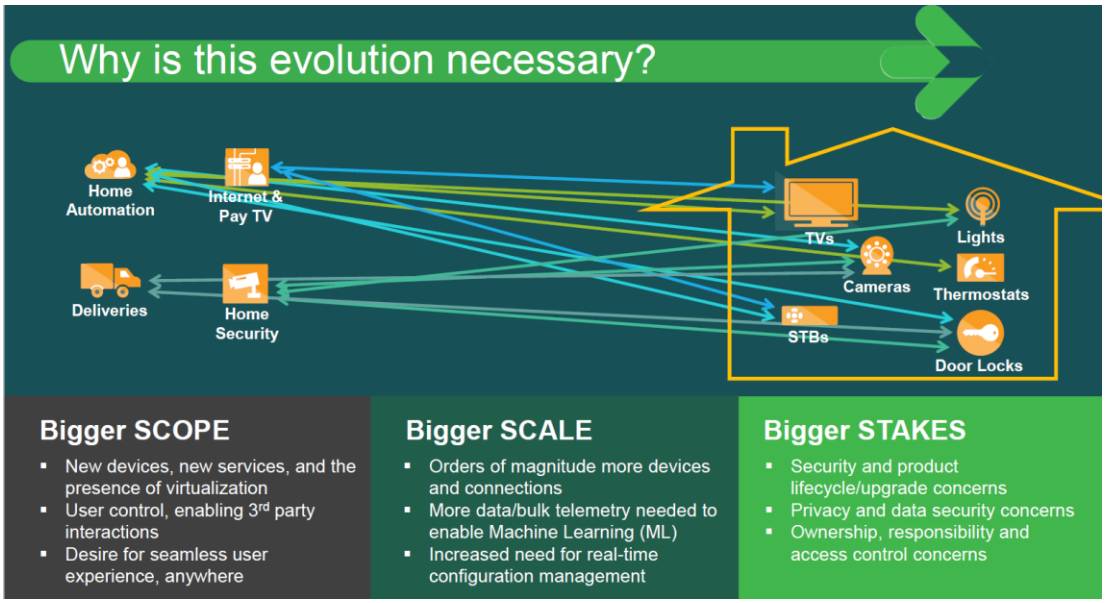


Kuva 5. Yleiskuvaus TR-069 protokollasta [16]

Broadband forum ei siis luo de facto -standardeja, joita kaikki käyttävät. Sen sijaan se luo protokollia yleiseen käyttöön, ja siinä mielessä se toimii samalla mallilla kuin IETF.

2.8.2 Tulevaisuuden modeemien hallintatarpeet kodeissa

Technical Report -069 (TR-069) on laajasti käytössä, mutta se alkaa olla jo vanha protokolla, joskin se toimii mainosti edelleen alkuperäiseen tarkoitukseensa eli CPE-laitteiden hallintaan. Vanha TR-069 ei anna mahdollisuuksia uusimpien palveluiden hallintaan, eli ongelmat TR-069 -protokollan kanssa syntyvät uusien palveluiden hallinnassa CPE-laitteissa. Seuraavana on kuva Broadband forumin näkemyksistä ja haasteista, joita tulisi ratkaista tulevaisuuden versiolla tästä hallintaprotokollasta.



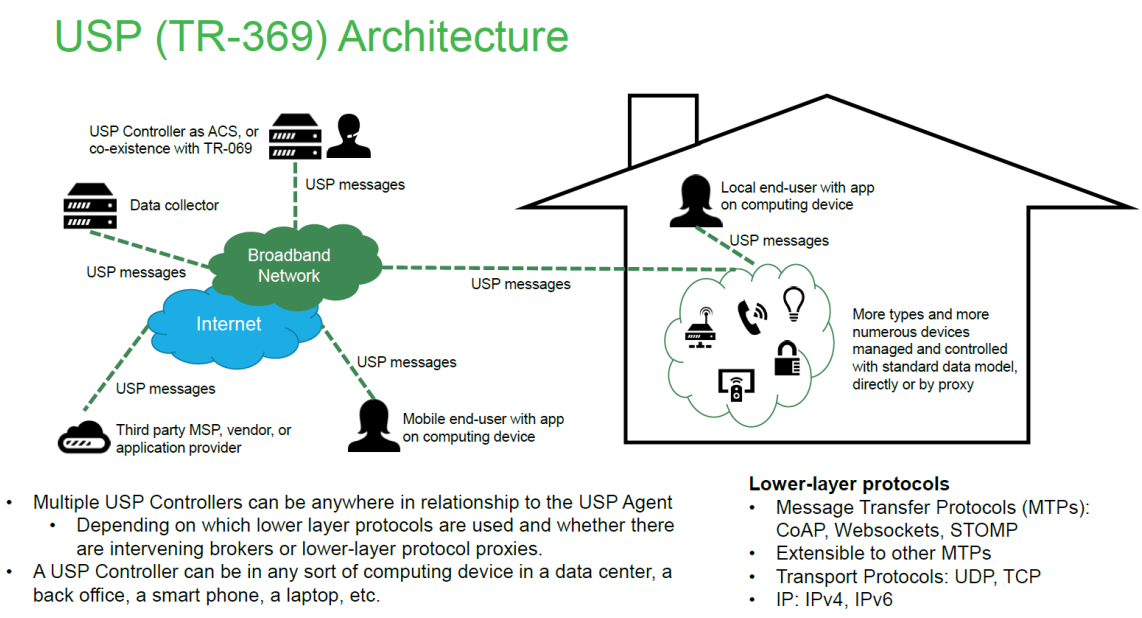
Kuva 6. USP-protokollan yleiskuvaus [17].

Kuvassa 6 esitetään integraatiopisteitä nykymaailman IoT-laitteiden ja kodin välillä [17]. Toiminnalliseen kuvaan on tullut runsaasti erilaisia toimijoita lisää. Teleoperaattorilla on luonnollisestikin keskeinen rooli, mutta uusina toimijoina olisivat esimerkiksi tietoturvaa toimittavat tahot. Verkkokaupat tulevat integroitumaan tavalla tai toisella, ja erilainen älykkääseen kotiin liittyvä toiminnallisuus on myös keskiössä.

Kodissa on nähtävissä jo aiemmin auki kirjoitettu tulevaisuus älykodista: älykkäät valot ja lukot sekä kodin laitteet mukaan lukien TV:t, jääkaapit, pesukoneet ja tietenkin talo-automaatio. Tämä on ennennäkemätön mullistus verkottumiseen mutta myös siihen, että älykkäiden laitteiden tulisi kommunikoida keskenään.

2.8.3 USP-protokolla – usean verkkokontrollerin hallintaprotokolla

Nykyajan haasteet tuovat uusia ongelmia, joita ratkaisemaan on jo tuotettu uusia työkaluja. Broadband forum on julkaissut vuonna 2018 uuden version hallintaprotokollasta, joka tunnetaan nimellä TR-369 - mutta myös nimellä USP eli Universal Services Platform [18]. Kuvassa 7 havainnollistetaan uutta USP-protokollaa yleistasolla.



Kuva 7. USP-protokollan esittely, lähde; Broadband forum [18].

Uusi asia tässä USP- eli TR-369-protokollassa [18] on useiden nk. kontrollerien mahdollisuus. Yksi mahdollinen kontrolleri voisi olla tietoturvayhtiö, joka nykymallin mukaisesti API-teknologiota hyväksikäyttäen tarjoaisi tietoturvan suojaa operaattorin verkon kautta. Muita mahdollisia kontrollereita voisivat olla taloautomaation ohjaus ja esimerkiksi fyysinen turva kodissa, etäältä valvottuna.

2.8.4 Teleoperaattorin rooli uudessa IoT-maailmassa

Teleoperaattori tulee olemaan uudessa yhtälössä monella tapaa keskiössä, aivan ytimessä. Teleoperaattori tarjoaa kaikki yhteydet - niin kiinteät yhteydet kotiin kuin mobiilit yhteydet tien päälle ja osin kotiinkin. Tästä syystä teleoperaattori toimii integraatiopisteenä kodin ja laajakaistaverkon välillä. Näin on tietysti ollut aiemminkin, mutta tämä rooli tulee korostumaan.

Kaikki liikenne kulkee teleoperaattorin kautta, mikä on hyvä pitää mielessä. Samoin monet palvelut provisioidaan luontevasti teleoperaattorin kautta. Toki niitä provisioidaan muuallakin: mm. Apple Storessa, Goole Play Storessa ja erilaisissa pilvipalveluissa – mutta on niinkin, että teleoperaattorilla on tavallaan etulyöntiasema siinä mielessä, että asiakassuhde on jo olemassa. Muut ehkä joutuvat luomaan asiakassuhteen,

mutta aktiivinen teleoperaattori hyödyntää olemassa olevaa asiakassuhdetta ja alkaa tarjota enenevässä määrin lisäarvopalveluita IoT-maailmaan.

2.8.5 Internetin reititys

Yllä todettiin yleisluonteisesti, että kaikki liikenne kulkee teleoperaattorin kautta. Tarkastellaan tätä asiaa teknisesti. Kun kaikki liikenne kulkee jonkin pisteen kautta, tätä kutsutaan solmupisteeksi. Solmupisteessä on luonteva paikka tarjota palvelua kaikille. Lyhyesti todettuna teleoperaattorin runkoverkon puolella pitäisi periaatteessa pystyä suojaamaan älykoti samaan tapaan kuin paikallisella CPE-laitteella. Kaikki liikennehän kulkee niin kodin CPE-laitteen kautta kuin myös teleoperaattorin runkoverkon kautta.

Tässä tulee kuitenkin verkon reitityksen kannalta tärkeä asia. CPE-laite tekee yleensä nk. Netwrok Address Translation -toiminnetta (NAT). NAT-operaatio muuttaa IP-osoitteet CPE-laitteessa WAN-verkon puolella julkiseksi ja taas älykodin LAN-verkon puolella yksityiseksi IP-avaruudeksi. Tästä seuraa, että NAT-laitteen takana olevien laitteiden tunnistaminen runkoverkossa ei ole itsestäänselvyys. Onkin niin, että erinäisistä syistä osa teleoperaattoreista tunnistaa kodin laitteita melko tarkastikin jopa NAT:n takaa. Toiset taas eivät tähän vielä pysty.

Suojaamisen ja tietoturvan näkökulmasta olisi tärkeää tunnistaa älykodin laitteet teleoperaattorin solmupisteessä runkoverkon puolella. Muuten on erittäin vaikea tarjota kuluttajalle palvelua, missä hän voisi teleoperaattorin ylläpitämässä portaalissa tms. palvelussa valita, mitä oman älykodin laitteita tulisi suojata ja millä tavoin. Täten hyvin tyypillinen NAT-ratkaisu kodin CPE-laitteessa tekee teleoperaattorin runkoverkon puolella tietoturvan tarjoamisesta varsin haastavaa.

Tässä teleoperaattorin runkoverkon puolella tarjottavassa tietosuojassa on myös toinen ongelma. Secure Socket Layer (SSL) eli nykyään TLS:n nimellä tunnettu useimmiten www-selaimissa käytettävä suojaus eli tiedon salaaminen omalta osaltaan vaikeuttaa myös tätä tietosuojan toteuttamista. TLS tekee omaa tehtäväänsä erittäin hyvistä syistä, mutta samaan aikaan tietoliikenne menee salattuna niin kodin CPE-laitteen läpi kuin myös teleoperaattorin solmupisteen läpi. Tämä tekee tietoliikenteen laillisestakin tarkastelusta haastavaa, ja näitä asioita tarkastelemme tarkemmin F-Secure Sensen käyttökokemuksien puolella.

Asiat vaikeutuvat tulevaisuudessa vielä lisää, kun myös DNS-liikennettä ollaan salaamassa enenevässä määrin. Tällöin pilvipohjainen mainepalvelu alkaa olla vaikeuksissa verkon puolella tapahtuvassa suojauksessa. Tämän asian vaikutusta arvioidaan lisää insinöörityön yhteenvedossa.

2.9 Verkkoselaus ja sen salaaminen

Tämän työn kannalta on tärkeää ymmärtää selainverkkoliikenteen salaus, sen kehitys ja metodit. Siksi ne käsitelläänkin alla yksityiskohtaisesti verkon liikenteen monitoroinnin näkökulmasta.

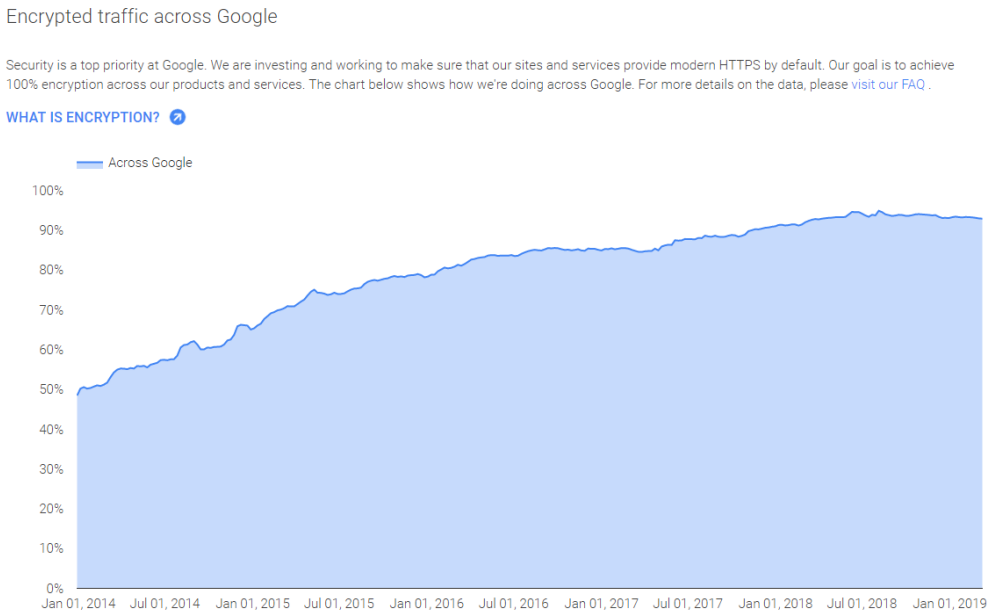
Samoin käsitellään muutamia erilaisia mahdollisia liikenteen analyysikeinoja kuten mm. Deep Packet Inspection (DPI) ja Server Name Indication -analyysi (SNI) IP-liikenteestä.

2.9.1 HTTP eli selkokielinen www-liikenne

HTTP-liikenne ei ole salattua ja tälle liikenteelle kaikki monitorointi on mahdollista. Kuten myöhemmin osoitetaan, että HTTPS-liikenteen osuus on noussut viime vuosina merkittävästi. Tulevaisuuden ratkaisuiden kannalta tuleekin keskittyä HTTPS- eli TLS-liikenteen syvälliseen tulkintaan ja käyttäytymiseen eri tilanteissa.

2.9.2 Verkkoselauksen salaamisen kehitys

Kuva 8 on Googlen grafiikka [19], joka kertoo HTTPS:n käytön lisääntymisen vuodesta 2014 aina tammikuuhun 2019. Käytön määrän nousu on massiivinen ja suunta on edelleen ylöspäin. Tästä metriikasta voidaan nähdä, että se ei ole www-käyttökertojen määrä vaan koko liikenteen määrä tavuina. Tässä yhteydessä tulee huomata, että esim. Netflix- ja Apple TV -liikenne kulkee HTTPS-liikenteenä ja edustaa samalla todella huomattavaa datamäärää. Tavanomaisen www-liikenteen määrästä on edelleen kohtuullinen osuus silti selkokielistä HTTP-liikennettä.



Kuva 8. Googlen metriikka salatun HTTPS-liikenteen määrästä [19]

2.9.3 HTTPS ja SSL

Verkkoselaamisen salaaminen on yleistynyt todella nopeasti. Tähän on myös hyvät syyt; liikenteen salaaminen suojaa erilaisilta verkkohyökkäyksiltä tehokkaasti. SSL oli ensimmäinen verkkoselainten protokolla, jonka Netscape kehitti jo niinkin aikaisin kuin 1993-1994. Alkuun verkkoselauksen SSL-protokollaa käytettiin lähinnä verkkopankeissa ja kauppapaikoilla. HTTPS:n käyttö on kuitenkin yleistynyt viime vuosina voimakkaasti oikeastaan kaikilla mahdollisilla sivustoilla.

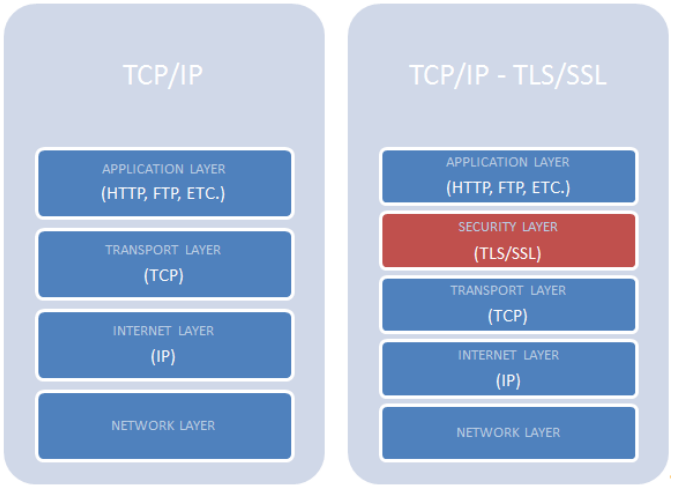
2.9.4 Moderni TLS-salaus www-selainliikenteessä

Aika on ajanut SSL:n ohitse ja TLS-salausprotokolla on syrjäyttänyt SSL:n. TLS kehitettiin vuonna 1999. TLS:n viimeisin versio TLS 1.3 [28] on niinkin tuore, että se on vuodelta 2018.

Vaikka SSL:n nimi on virallisesti vanhentunut, ja sitä käytetään silti TLS-nimen ohella hyvinkin paljon. Tarkasti tulkiten TLS on kuitenkin se uusin selainliikenteen salausprotokolla. Osa vanhemmista selaimista ei välttämättä tue TLS-salausta, ja ne saattavat

täten edelleen kätellä vanhemman ja haavoittuvan SSL-yhteyden selaimen ja palvelimen välille.

Tärkeintä ehkä tässä tietoturvan kontekstissa on ymmärtää, että TLS toimii TCP-protokollan yläpuolella protokollapinossa. Tästä seuraa monia asioita, mutta laillisen verkkomonitoroinnin näkökulmasta siitä seuraa se, että selaimen tarkka kohdesivutieto ei ole selvillä. Tiedossa on vain nk. kohdedomain; itse mahdollinen alidomain ja/tai alasivu ei ole tiedossa, koska se tieto on salattuna TLS-salatuissa HTTP:n otsaketiedoissa. Kuvassa 9 on protokollapino [20], joka kertoo, missä kohtaa salaus tehdään.



Kuva 9. TLS-toimintamalli [20]

2.9.5 SNI-parametri TLS-protokollassa

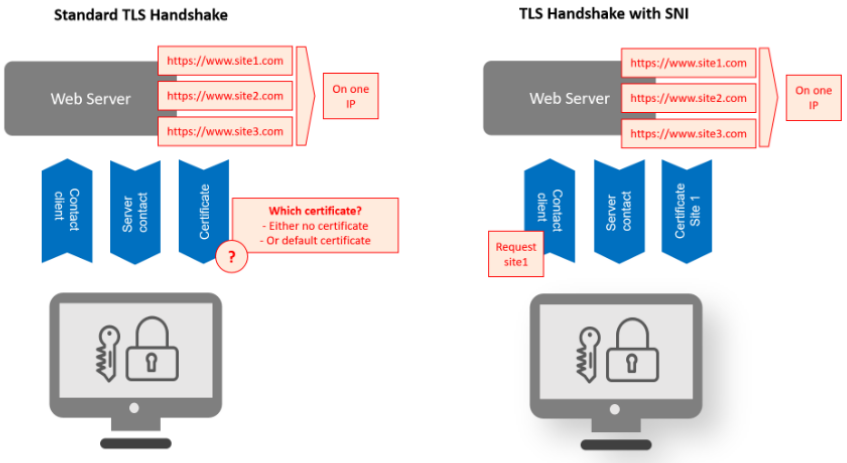
SNI-parametri toimii tärkeänä osana TLS-protokollaa. On tyypillistä, että yhden IP-osoitteen takana on useita www- eli nk. domain-nimiä. Tähän on useita syitä, esim. kustannussyyt. On myös niin, että www-palvelimessa voi olla useampia www-nimiä ylläpidossa, ja täten www-palvelimessa voi olla useita SSL-sertifikaatteja. SNI-tiedon avulla TLS-kättelyssä voidaan välittää domaintieto selaimelta palvelimelle, millä saadaan selaimelle takaisin oikea sertifikaatti loppukäyttäjän näkyville ja arvioitavaksi.

SNI on siis lisäattribuutti TLS-protokollalle, sillä loppukäyttäjän selain voi välittää kohdepalvelimelle tiedon kohdedomainin nimestä TLS-kättelyn ensimmäisessä vaiheessa. SNI-tiedolla voidaan täten identifioida oikea sertifikaatti www-palvelimelta mutta myös

tietoturvan näkökulmasta voidaan identifioida, mitä osoitetta www-selaimella on tarkoitus selata.

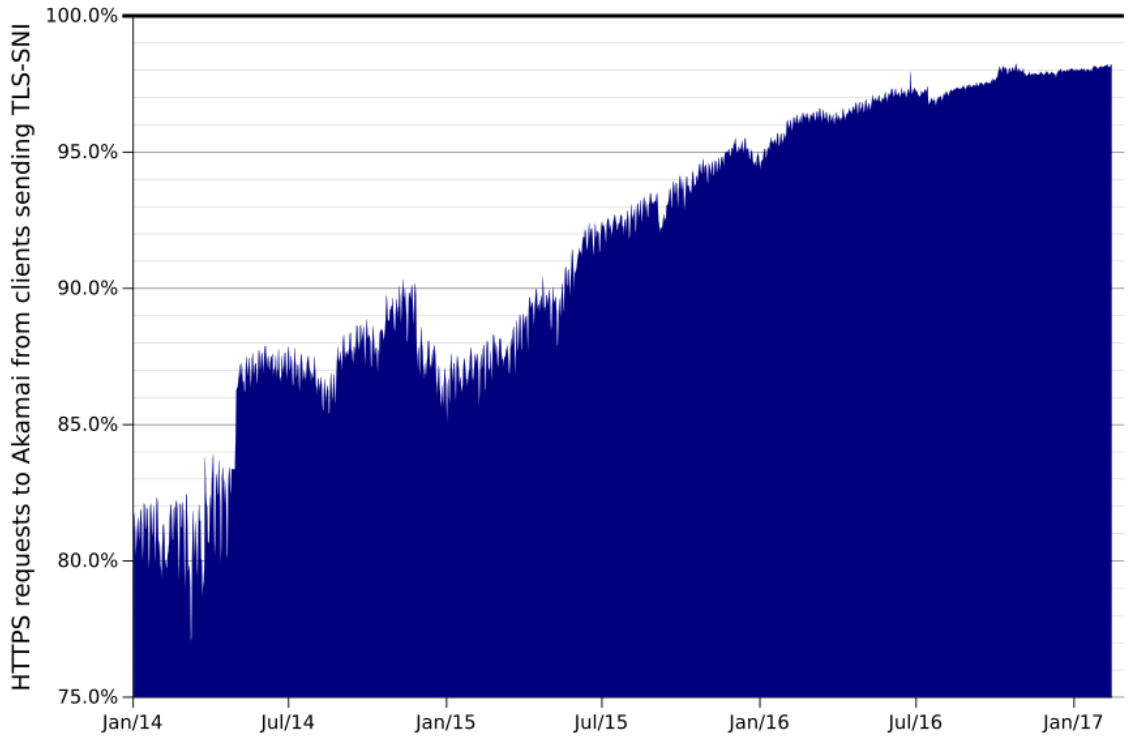
On syytä myös huomata tärkeä yksityiskohta: SNI-tiedossa ei mene mukana koko Uniform recource Locator -tieto (URL), vaan ainoastaan nk. päädomaini. Varsinainen selaustieto, mm. tarkka sivuosoite kulkee salattuna TCP-paketeissa TLS:llä salattuna, TLS-kättelyn jälkeen. Tämä on hankala tilanne, jos esimerkiksi https://www.whatevargood.com-sivuston alla olisi esimerkiksi sivusto https://www.whatevargood.com/normalpages/reallybadstuff.html, jolloin turvallisen pääsivuston alla oleva alasivusto olisi haitallinen jollain tavoin, mutta tämä HTTP-liikenne kulkee salattuna TLS:n takia ja ansiosta.

TLS-kättelyn ero SNI-tiedolla ja ilman on käsitelty kuvassa alla. Selaimen kohteena on yksittäinen web-palvelin, jossa on ylläpidossa useita www-palveluita omalla domainnimellään. Ilman SNI-tietoa on mahdotonta sanoa, mitä kyseisen web-palvelimen domaineista selaimen on tarkoitus käyttää. Liikenne menee salatuksi ensimmäisen TLS-kättelykierroksen jälkeen, joten ei ole mahdollista tehdä verkkotasonsuojauksen päättelyä ilman SNI-tietoa. Oikeanpuoleisessa vaihtoehdossa on SNI-tieto mukana TLS-kättelyssä, ja siitä seuraa useita hyötyjä. Verkkotietoturvan kannalta voidaan päätellä, mille sivustolle selaimella ollaan menossa ja täten estää tai päästää liikenne läpi verkkotason suojauslaitteessa, kuten F-Secure Sensessä.



Kuva 10.TLS-kättelyn kuvaus [21]

Kuten kuvasta 10 havaittiin, SNI-tiedon saaminen mahdollistaa verkkotietoturvan näkökulmasta päättelyn, mihin www-osoitteeseen selainsessiota ollaan avaamassa salatussa TLS-liikenteessä. Onneksi kehitys kulkee siihen suuntaan, että HTTPS-liikenteestä pääosa sisältää SNI-tiedon, joten verkkotietoturva mahdollistuu. Kuvassa 11 on Akamai-yrityksen metriikkaa HTTPS-liikenteen osuudesta SNI-tiedolla [22]. Tästä voidaan havaita, että luku lähentelee 100 prosenttia. Akamai on johtava yritys www-palvelimien hotellipalveluliiketoiminnassa.



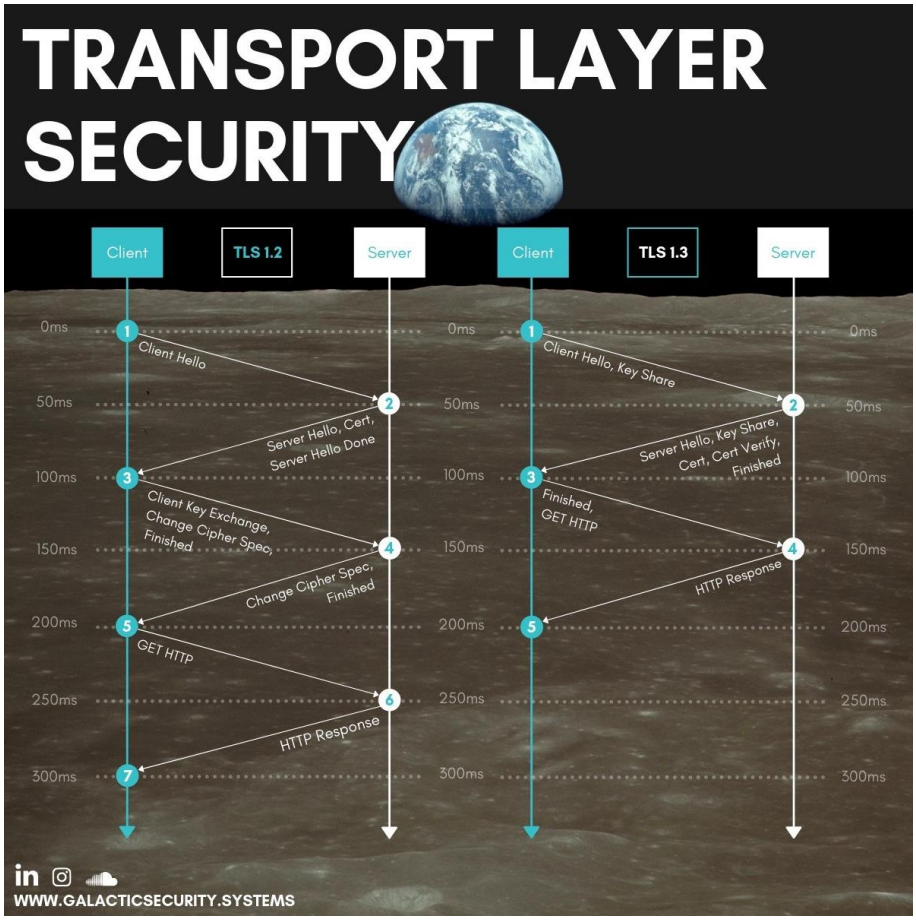
Kuva 11. SNI-parametrin käytön osuus kaikesta HTTPS-liikenteestä [22].

2.9.6 TLS-kättely selaimen ja palvelimen välillä

Kuvasta voidaan havaita useitakin tärkeitä asioita TLS:n toiminnasta. Ensinnäkin TLS-protokollan viimeinen 1.3-versio on parempi loppukäyttäjän käyttökokemukselle, koska se on yksinkertaisesti nopeampi. Tämä on saavutettu lyhennetyllä kättelyprosessilla, mikä ilmenee kuvasta 12.

Kuvasta voidaan myös havaita, että liikenteen salaus käynnistyy hyvin nopeasti selaimen ja palvelimen ensimmäisen kättelykierroksen jälkeen. Tästä seuraa HTTPS-liikenteen tarkan monitoroinnin hankaluus ja jopa mahdottomuus.

Kuvasta 12 pystytään myös havaitsemaan, että kun TLS-salaus on aloitettu [23], yhteys toimii kuten HTTP-liikenne. TLS toimii siis TCP-tason näkökulmasta samaan tapaan kuin selkokielinen HTTP-liikenne.



Kuva 12. TLS 1.2 ja 1.3 kättely ja nk. Client hello -vaihe [23].

Request For Comment 6066 [29] (RFC) määrittele TLS 1.3 -protokollalle (RFC 8446) [28] extensiot eli lisäykset, joita eri kutsuissa pitää olla tai voi olla. Yllä käsitelty tärkeä SNI-arvo voidaan RFC-standardin näkökulmasta vapaaehtoisesti liittää ensimmäisen TLS-kättelyn nk. ”Client hello” -viestin lisäyksiin - siellä tarkemmin sanottuna nk. ServerNameList:iin eli palvelinnimilistaan, jonka selain TLS-kättelyssä voi toimittaa. Alla on

kuva RFC 6066-standardista [24] liittyen rakenteeseen SNI-datasta ServerName-List:ssa.

```
struct {
    NameType name_type;
    select (name_type) {
        case host_name: HostName;
    } name;
} ServerName;

enum {
    host_name(0), (255)
} NameType;

opaque HostName<1..2^16-1>;

struct {
    ServerName server_name_list<1..2^16-1>
} ServerNameList;
```

Kuva 13. SNI-tieto TLS-protokollassa [24].

2.9.7 DoH eli DNS HTTPS:n ylitse

DNS-protokolla HTTPS-liikenteen [30] ylitse kulkee portissa 443 kuten muukin HTTPS-liikenne. Kaikki liikenne TLS-kättelyn jälkeen on salattua ja siten mahdotonta monitoroida mihinkään tarkoitukseen selaimen ja palvelimen ulkopuolella.

Edellä mainituista syistä ne selaimet ja palvelut, jotka käyttävät DNS-palvelua HTTPS:n ylitse, ovat vahvasti suojattuja ja salattuja. Näin ollen DNS-liikenteen monitorointi ei onnistu kolmannen osapuolen toimesta.

Mahdollisesti osin ohi tästä insinöörityöstä mutta yleisen tietoturvan nimissä on hyvä havaita, että DNS over HTTP (DoH) on vaikea protokolla esimerkiksi teleoperaattoreille tai isoille yrityksille. Ne eivät voi suodattaa HTTPS-liikennettä, koska valtaosa selainliikenteestä on nimenomaan HTTPS-liikennettä. Tästä seuraa, että loppukäyttäjän selaimen ja kohdepalvelimen välissä ei kukaan voi tietää, mitä ja minne selain välittää tietoa. Tämä on erinomainen asia ihmisoikeuksien ja tietoturvan näkökulmasta mutta äärimmäisen vaikea tilanne esimerkiksi ison yrityksen tietoliikenteen monitoroinnin näkökulmasta. Sinänsä tällekin työlle tämä on tärkeä havainto yleisestä näkökulmasta.

Tahtoo olla niin, että äärimmäinen tietoturva ei yleensä kohtaa toista ääripäätä eli esimerkiksi laillista liikenteen monitorointia ja/tai verkontason liikenteen suodatusta.

2.9.8 DoT eli DNS TLS:n ylitse

Erotuksena edelliseen DoH-protokollaan DNS over TLS (DoT) [31] käyttää erikoisporttia 853. Tästä seuraa, että on mahdollista havaita DoT:n käyttö, jos tällaista porttia käytetään ja täten se voitaisiin jopa estää. Kaikki liikenne ensimmäisen vasteen jälkeen on toki salattua eli sen monitorointi ei onnistu.

Tiivistetysti voidaan todeta, että jos selain käyttää liikenteeseen DoT-protokollaa, liikenne on salattua ja eikä siitä saa tietoa kolmannelle osapuolelle - ei laillisesti eikä laittomasti – minne IP-liikenne menee. Täten tässä tapauksessa verkkotason suojaus on voimaton DNS-monitoroinnin näkökulmasta.

2.9.9 DPI ja TLS-kättely

DPI-nimikin jo kertoo pitkälti, mitä tämä prosessi tekee. Tarkoituksena on analysoida tietoliikennepaketteja tarkasti TCP-sisältöä myöden - ja tätä on tehtykin vuosikausia. Aiemmin mainittu hyvin tuore TLS 1.3 [28] vaikeuttaa merkittävästi DPI:n toimintamahdollisuuksia. Tässä ei käydä DPI:tä sen tarkemmin läpi. Todetaan vain, että TLS 1.2 ja vanhemmat versiot selkeästi huonommalla salauksen kättelyprotokollalla ovat sallineet esimerkiksi palomuurilaitteiden asettua TLS 1.2 -yhteyden väliin. Tämä on mahdollistanut tietoliikenteen salauksen purun ja uudelleen salauksen lennossa, ja tässä välissä tapahtuvan liikenneanalyysin. Tämä on ollut ilmeinen yksityisyyden tietoturvaongelma.

TLS 1.2 ja sen vanhemmat versiot eroavat tietyiltä osin merkittävästi uusimmasta TLS 1.3 -versiosta. TLS 1.2 ja vanhemmat versiot ovat yleisesti käyttäneet staattisen RSA-avaimen lähestymistä TLS-kättelyssä. Tämä on käytännössä tarkoittanut, että selain on salannut kättelyssä www-palvelimen julkisella avaimella viestin, jonka palvelin on purkanut. Tässä on se ongelma, että esimerkiksi yrityksen palomuuri on tällaisessa kättelyssä kyennyt purkamaan salauksen. Ongelmaksi tulee nk. Man In the Middle -tilanne (MItM) eli palomuuri on välimiehen asemassa purkaen ja salaten liikenteen lennossa ja samalla suorittaen DPI-prosessia. Tämä on ollut jo pitkään tunnistettu tietoturvaongelma, jonka mahdollisuutta on vaikeutettu merkittävästi TLS 1.3 -versiossa. Tohtorintyö

On the design and Implementation Secure Network Protocols [25] kuvaa erinomaisesti ja syvällisesti tätä TLS-protokollien haavoittuvuuksia TLS 1.1- ja TLS 1.2 -versiolla.

TLS 1.3 neuvottelee salatun yhteyden selaimen ja palvelimen välillä asymmetrisiä avaimia sekä Diffie-Hellman-protokollaa käyttäen, ja sen jälkeen tietoliikenne salataan TLS-protokollalla luotua jaettua symmetristä avainta käyttäen. Voidaan sanoa että asymmetrisillä avaimilla luodaan symmetrinen salaus selaimen ja palvelimen välillä. Tähän liittyy vielä sellainen hyvin tärkeä yksityiskohta, että Diffie-Hellman-protokollan asymmetristen avainten minimipituudet on määritelty uudella tavalla. Tästä seuraa, että aiemmin TLS 1.2 -protokollalle yleiset nk. force downgrade -hyökkäykset eivät toimi TLS 1.3 -protokollalle ja täten tietoturva on aivan uudella tasolla.

Voidaan siis sanoa, että sinänsä laillinen DPI-toiminne vaikeutuu merkittävästi TLS 1.3 -protokollaa [26] käyttävissä selainyhteyksissä. Tietoturvayhtiö Symantec on kirjoittanut [32] TLS 1.2 vs. TLS 1.3 käytön DPI-asiasta selonteon ja ohjeistuksen. Siinä todetaan muun muassa, että TIA on erittäin vaikeaa palomuuri- ja yhdyskäytävälaitteissa, jopa niin vaikeaa, että perussääntö uusimpien protokollien noudattamisesta jää toiseksi. Yksi mahdollistava lyhyen aikavälin metodi on nimittäin pakottaa yhdyskäytävälaite käyttämään vanhempaa TLS 1.2 -salausta, jolloin asia – kuten aiemmin todettiin – on selvästi helpompaa. TIA tietyin tapauksin onnistuu TLS 1.3 -yhteyksille, mutta kokonaistietoturvan kannalta sekä yhdyskäytävälaitteen valmistajan että itse laitteen omistavan hallitsevan tahon tulee olla erittäin tarkkana. On aina mahdollista, että syntyy tuntemattomia tietoturvahaavoittuvuuksia, kun kierretään vahvaksi tehtyä protokollaa erikoiskonfiguraatioilla. Tunnistamattomat haavoittuvuudet ovat erittäin vaarallisia kokonaisturvan kannalta.

Väitöskirja *An Analysis of the Transport Layer Security Protocol* [27] tutkii ja kuvaa yksityiskohtaisesti, miten TLS 1.3 saavuttaa uuden TLS-version vaatimukset erilaisten verkkohyökkäysten suhteen. Tohtorintyössä on tutkittu TLS 1.3:n eri luonnosversioiden hyvyyttä erilaisia MItM- ja muitakin hyökkäyksiä vastaan. TLS 1.3:n luonnos-21 on jo toiminut MItM-hyökkäyksiä kohtaan oikeellisesti siinä, missä TLS 1.2 -versiot ja sitä vanhemmat versiot eivät ole toimineet. Kyseisen väitöskirjan valmistumisen jälkeen on tehty vielä 7 uutta luonnosta. Valmis TLS 1.3 -protokolla on löydettävissä nimellä RFC 8446 https://tools.ietf.org/html/rfc8446 [28]. Intrernet Engineering Task Force (IETF) kirjoittaa hyvin tarkasti, miten TLS 1.3 -protokollaa käytetään turvallisesti. Tämä liittyy

esimerkiksi siihen, millaisia nk. salauskittejä tuetaan ja ei tueta, tai esimerkiksi millaisilla parametreillä TLS 1.3 -kättelyä suositellaan käytettäväksi. Näissä yksityiskohdissa piilee ne vaarat jos ja kun jollain tavalla muutetaan ja/tai heikennetään TLS 1.3 -kättelyä yhdyskäytävälaitteessa. Tämä on niin uusi asia, että todellinen lopputulema on vielä näkemättä - jopa niin, että TIA-toiminnetta tukevien yhdyskäytävälaitteiden valmistajat suunnittelevat vasta, miten tämä asia hoidetaan laillisesti ja turvallisesti.

2.9.10 IPv4- ja IPv6 -protokollat ja TLS

IPv6 on tulevaisuuden IP-protokolla tunnetuista syistä ja siksi on tärkeää kommentoida sitä tämänkin työn osalta. IPv6 on tärkeä protokolla, jotta IP-avaruuden käyttämät osoitteet riittävät pitkälle tulevaisuuteen etenkin, kun IoT-laitteet alkavat toimia enenevässä määrin eSIM-korteilla suoraan internetiin julkisilla osoitteilla.

TLS:n näkökulmasta on kuitenkin niin, että IPv4 ja IPv6 toimivat samalla tavalla, joten IP-liikenteen monitoroinnin ja verkon tietoturvan kannalta ei ole merkitystä, onko käytössä IPv4- vai IPv6-protokolla.

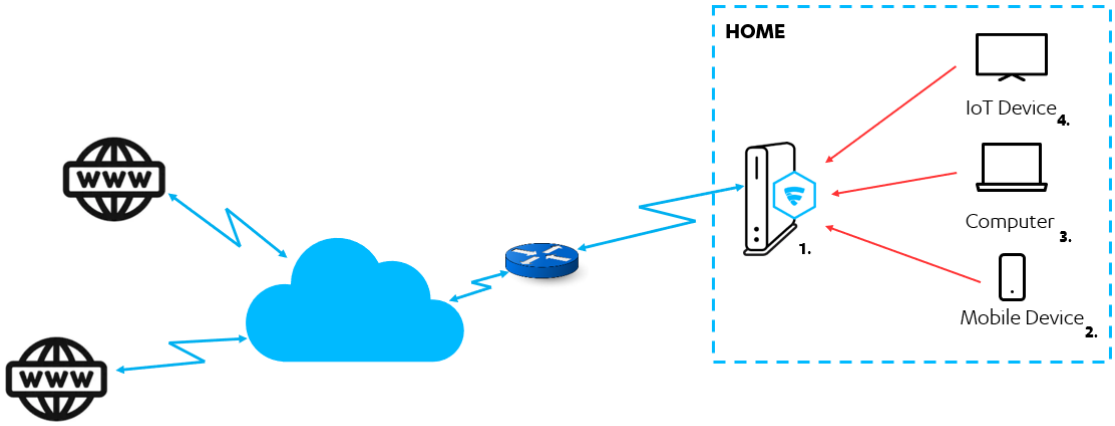
IPv6 muuttaa tilannetta siltä osin että CPE laitteiden takana olevat osoitteet ovat operaattorin niin halutessaan julkisia IP osoitteita. Tämä ei muuta itse TLS salausta, mutta voi muuttaa tapaa miten sertifikaatteja käytetään TLS tuetuissa palvelimissa.

3 Tekninen IoT-suojauksen esittely-ympäristö

Insinöörityön tuloksena rakennettiin esittely-ympäristö IoT-laitteiden suojaukselle ja esittelylle. Kyseessä on täydellinen toiminnallinen ympäristö IoT-laitteilla ja laajakaistaverkkoyhteydellä. Ympäristöön on liitetty kuvassa 14 olevat laitteet.

Keskeisessä roolissa tässä ympäristössä on operaattorin tarjoama kiinteän internetin Zyxel-reititin (malli VMG3927-B50A). Laite on Zyxelin uusinta mallisarjaa, jossa on enemmän muistia sekä suorituskykyä ajaa kolmannen osapuolen sovelluksia, kuten esimerkiksi F-Secure Sense -suojausohjelmistoa.

F-Secure SDK on ohjelmisto, joka on esiasennettu kuluttajan puolesta Zyxel xDSL -laitteeseen. F-Securen ohjelmistosta on saatavilla erilaisia versioita riippuen käytettävissä olevasta reitittimen muistin määrästä. Muistin määrä liittyy suoraan siihen, millaisia palveluita ja missä laajuudessa reitittimessä voidaan ajaa. Yksinkertaisimmillaan se olisi ehkä vain selauksen suojausta, jolloin kuluttajaa suojattaisiin päätymästä verkkosivuille, joille ei ole aiheellista mennä sisällön haitallisuuden takia. Enimmillään F-Secure Sense -suojaus on älykästä IoT-laitteiden suojausta, jolloin voidaan automaattisesti liikenneanalyysillä tunnistaa haitallista liikennettä, jollaista haittaohjelma tuottaa saastuneessa IoT-laitteessa.



Kuva 14. Sense-esittely-ympäristön arkkitehtuuri.

3.1 Esittely-ympäristön demonstraatiolaitteet

Taulukko 1. Taulukossa on kuvattuna kodin käyttölaitteet F-Secure Sense -esittely-ympäristössä.

#	**Laite**	**Malli**	**Tyyppi & tehtävä**
Laite 1.	Zyxel modeemi	VMG3927-B50A	xDSL-modeemi kotiin

Laite 2.	F-Secure Sense	SDK v. 1.1.43.210	Suorittaa verkkotason suojaus-ta kotona
Laite 3.	IoT WiFi -kamera	D-Link Mini HD Wi-Fi Camera	IoT-WiFi -webkamera kotiin
Laite 4.	PC-tietokone	DELL kannettava tietokone,	Kodin tietokone internetverkon selaukseen

3.2 Testiosoitteet

Tässä työssä ei ole aihetta selata haittaohjelmasivuja tai muitakaan aidosti haitallisia sivuja. Täten toiminnan esittelyyn ovat käytössä F-Securen testisivut, jotka simuloivat haitallista sisältöä. Alla on kuvattu testiosoitteet:

http://unsafe.fstestdomain.com-osoite on yleisesti haitallinen sivusto.

http://adult.fstestdomain.com-sivusto simuloi aikuisviihdesivustoa.

3.3 Esittelyprosessi

F-Secure Sense -laitteiston esittely tehdään tietyssä järjestyksessä, jotta saadaan luotua lyhyessä ajassa ymmärrys kokonaisjärjestelmän toiminnasta ja samalla pystytään esittelemään tarvittavassa laajuudessa suojauksen toimintaa.

Esittely tehdään seuraavassa järjestyksessä:

1. Esitellään itse laitteet.
2. Esitellään puhelimen käyttöliittymä Sense-hallintaan.

3. Esitellän Sensen konfigurointia yleisesti.
4. Näytetään, miten selaus toimii sallituilla sivuilla.
5. Näytetään esimerkkisivuna yleisesti haitallisen sivun esto.
6. Esitellään Sense-profiilien käyttö ja vaikutus internetin käyttöön.
7. Esitellään haitallisen liikenteen identifointi Sense-päätelaiteohjelmassa.

Seuraavilla sivuilla esiteltävä konfiguraatiokokonaisuus esittelee ylläkuvatun testi- ja esittelykokonaisuuden.

4 Esittely-ympäristön konfigurointi loppukäyttäjän päätelaitteella

Järjestelmällä kyetään esittämään ja kouluttamaan kaikki tyypilliset käyttö- ja uhkatilanteet kodin WiFi-verkossa.

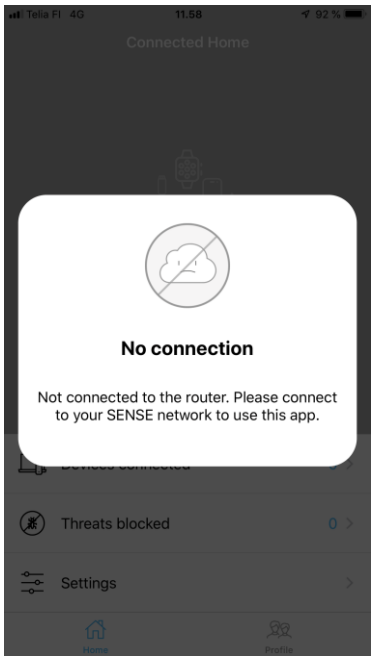
Järjestelmän pääkäyttötarkoitus on esittelytilanteet teleoperaattoriasiakkailla. Tällaisissa tilanteissa ja tilaisuuksissa tulee pystyä aidosti näyttämään, miten järjestelmä toimii, miten laitteita ja järjestelmää voi konfiguroida sekä millainen on asiakaskokemus suojaustilanteissa.

4.1 Tuotteen hallinta matkapuhelimesta

Tuotetta voi hallita monipuolisesti matkapuhelimen Sense-applikaatiosta. Kuvakaappaukset alla ovat iPhone-laitteessa käytetystä Sense-ohjausohjelmistosta. Ohjelmistoa ei ole valitettavasti tällä hetkellä vielä saatavilla suomenkielisenä, joten kuvakaappaukset ovat englanniksi.

Kuvassa 15 esittetään tilannetta, jossa Sense-ohjelmisto ei käynnisty. Puhelin ei ole joko lainkaan WIFI-verkossa tai on kiinni muussa WIFI-verkossa. Tällöin puhelimen käyttöliittymä ja ohjelmisto on harmaa ja se antaa virheilmoituksen ”No connection” eli että se ei ole liitettävissä Zyxel-reitittimeen. Sense siis vaatii WIFI-yhteyden samaan

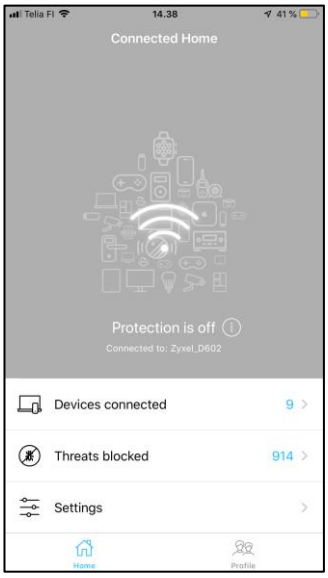
verkkoon Zyxel-reitittimen kanssa, jotta hallintayhteys F-Secure Sense -ohjelmistoon on mahdollinen.



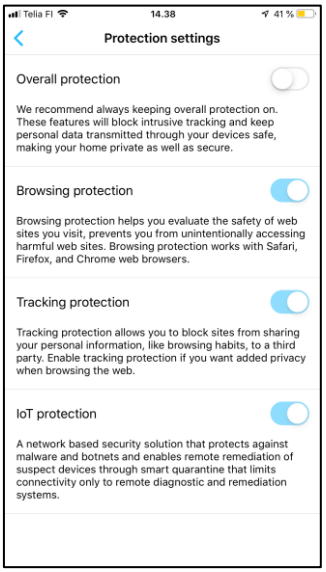
Kuva 15. Sense -ohjelmisto on nk. offline-tilassa.

Kuvassa 16 Sense-ohjelmisto on pois päältä reitittimessä. Käyttöliittymä on tällöin harmaa.

Kuvassa 17 esitetään iOS-käyttöjärjestelmälle tyypilliset liukukytkimet. ”Overall protection” on pois päältä. Se tulee laittaa päälle, jotta Sense-toiminnallisuus aktivoituu.



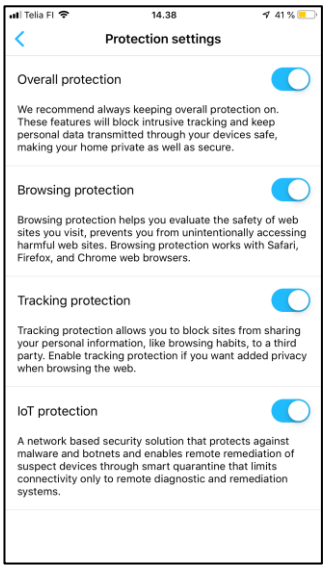
Kuva 16. Päätelaiteohjelmisto on harmaa eli suojausohjelmisto on sammutettu.



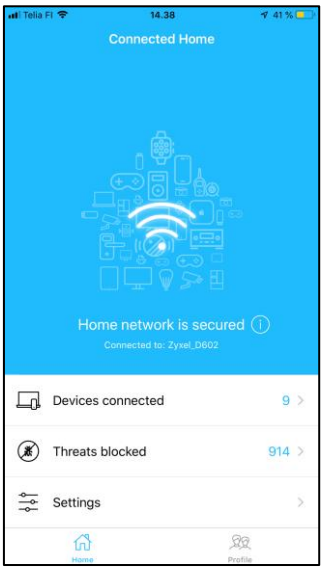
Kuva 17. Päätelaiteohjelmiston pääkytkin on pois päältä.

Ohjausohjelmiston pääkytkin on laitettu päälle kuvassa 18.

Ohjelmisto muuttuu siniseksi kuvassa 19 ja nyt on mahdollisuus konfiguroida asetuksia kyseisen Zyxel-reitittimeen WIFI:iin kytkeytyneille laitteille.



Kuva 18. Päätelaiteohjelmiston pääkytkin laitettu päälle.



Kuva 19. Päätelaiteohjelmisto sinisenä ja aktiivisena.

4.2 F-Secure Sensen profiilien konfigurointi

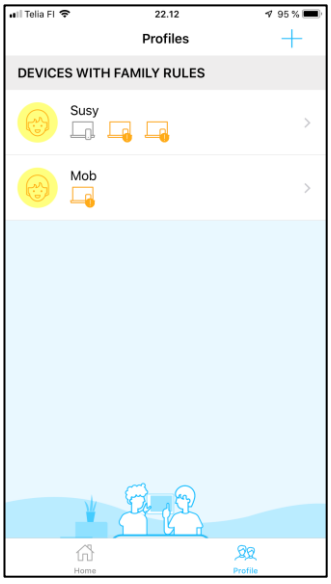
Sense-tuotteessa on käsite profiilit. Näillä voidaan luoda internetin käytön käyttöprofiileja, joilla voidaan rajoittaa tai sallia erinäisiä asioita. Profiileja voidaan sitten assosioida eri laitteille, ja siksi onkin luontevaa tehdä omanlaiset profiilit esimerkiksi jokaiselle lapselle erikseen. Tarpeet ja mahdolliset aikakatkaisut selainliikenteessä ovat isosti ikäriippuvaisia ja siinä kohtaa uniikit profiilit käyttäjäkohtaisesti luovat oikeaa ja hyvää asiakaskokemusta.

Profiileja voidaan luoda ja muuttaa päänäkymän kautta.

Tässä esimerkissä kuvassa 20 on nyt Mob-profiili ja Suzy-profiili. Niissä voi olla omat asetuksensa sisällön ja selauksen aikarajojen suhteen.

Suzy-profiilissa on nyt kiinni kolme päätelaitetta. Näille on omat yhteiset asetukset.

Nämä erilliset asetukset on kuvattu tarkemmin kuvassa 21.

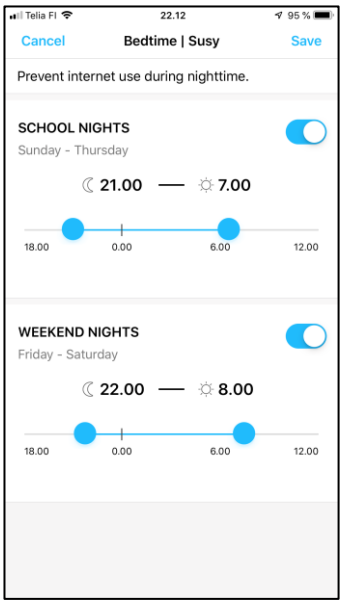


Kuva 20. Perheturvan lapsiprofiilien päävalikko.

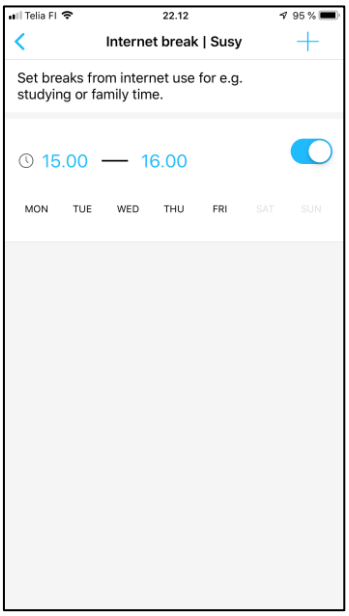
Kuva 21. Perheturvan lapsiprofiilin asetusvalikko.

4.3 Ajallinen internetin käytön eston konfigurointi

Internetselauksen ajallista käyttöä voi kontrolloida eri tavoin. Voidaan asettaa nukkumaanmenoaika erikseen viikolle ja viikonlopulle kuten alla kuvassa 22. Esimerkiksi keskellä koulupäivää voidaan luoda käyttökatkos kuvan 23 tapaan. Tällainen tarve tulee esimerkiksi koulutehtävien lukuhetkestä.



Kuva 22. Perheturvan verkonselauksen aikamäärityksen käyttöliittymä.

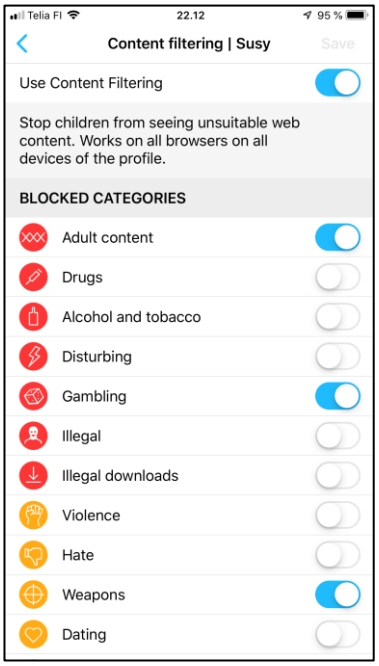


Kuva 23. Perheturvan verkonselauksen aikamäärityksen päiväkohtaisen katkoksen asetus.

4.4 Internetselauksen sisällön suodatuksen konfigurointi

Internetselauksen sisällön kontrollia voidaan konfiguroida eri tavoin.

Internetselauksen sisältöä voidaan hallita kuvan 24 tapaan ja kontrolloida sisältötyyppien perusteella. F-Secure-mainepalvelu on kategorisoinut sivustot. Järjestelmä voi täten estää ja sallia sisältöä riippuen konfiguraatiosta. www-sivuja voidaan kategorisesti estää tai sallia. Alla olevassa kuvassa 25 on esimerkki, jossa www.lego.com on sallittu ja pelisivusto www.veikkaus.fi on estetty.



Kuva 24. Perheturvan erilaisia estettäviä sisältöprofiileja.

Kuva 25. Perheturvan sallittuja ja estettyjä verkko-osoitteita.

5 Loppukäyttäjän käyttökokemus

Koulutuskäyttöä silmälläpitäen erilaiset käyttökokemustilanteet on kuvattu seuraavaksi myös koulutustarkoituksessa hyödynnettäväksi.

5.1 Käyttökokemus normaalissa internetkäytössä

Normaalissa internetkäytössä loppukäyttäjän ei tule huomata mitään eroa internetin käytössä, jos sivut ovat tavallisia ja turvallisia. Niiden tulee latautua yhtä nopeasti kuin ilman tietoturvaa eikä sisältö saa muuttua.

5.2 Käyttökokemus estetyssä internetkäytössä

Normaalissa internetkäytössä eroa normaaliin suojaamattomaan käyttöön ei huomaa. Tämä onkin aivan yleinen tavoite internetsuojaohjelmistojen kanssa - niiden tulisi toimia näin. Yleisesti F-Secure jakaa sivustoja kolmeen pääkategoriaan:

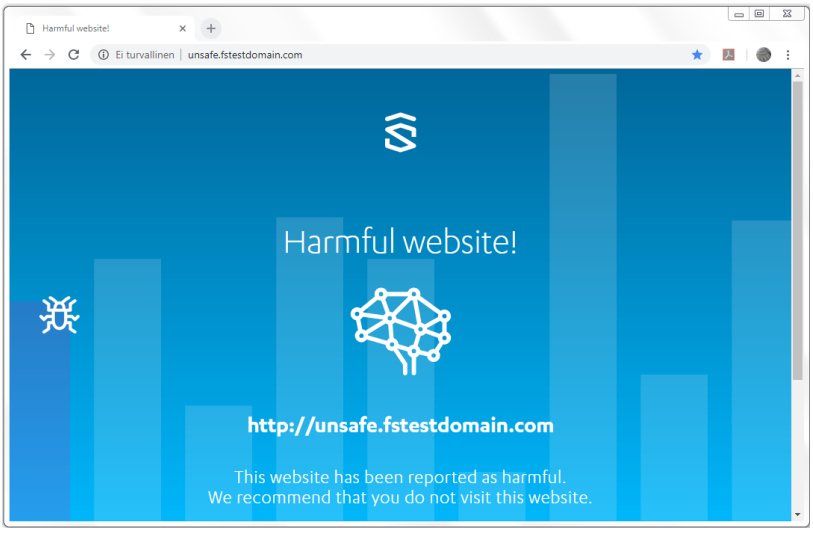
1. tunnettuihin hyviin www-sivuihin tai tiedostoihin
2. tunnettuihin huonoihin www-sivuihin tai tiedostoihin
3. tuntemattomiin www-sivuihin ja tiedostoihin.

Tästä syystä virhetilanteisiin liittyy seuraavia käsitteitä:

- ”False negative”, joka tarkoittaa, että haitallista sivua ei ole tunnistettu ja liikenne on sallittua. Tästä tehdään yleensä virheilmoitus ja sivu nk. blacklistataan eli määritellään tunnetuksi haitalliseksi F-Securen pilvipohjaiseen mainepalveluun.
- ”False positive”, hyväksi määriteltävä sivu on tunnistettu virheellisesti haitalliseksi; tämäkin tulee raportoida ja se määritellään tunnetuksi hyväksi sivuksi F-Securen mainepalveluun.

5.3 Käyttökokemus haitallisen sivuston käyttötapauksessa

Loppukäyttäjä yrittää käyttää sivustoa http://unsafe.fstestdomain.com, joka on Sense-ohjelmiston mielestä haitallinen. Käyttökokemus on loppukäyttäjän selaimessa ao. kuvan kaltainen. Sense-ohjelmisto on estänyt sivuston selaamisen. Estosivu on esitetty kuvassa 26, joka kertoo estetyn www-sivun ja sen, mistä syystä se on estetty.



Kuva 26. Sense-ohjelmiston yleinen estosivu.

5.4 Haitallisen aikuisviihdesivuston selaaminen

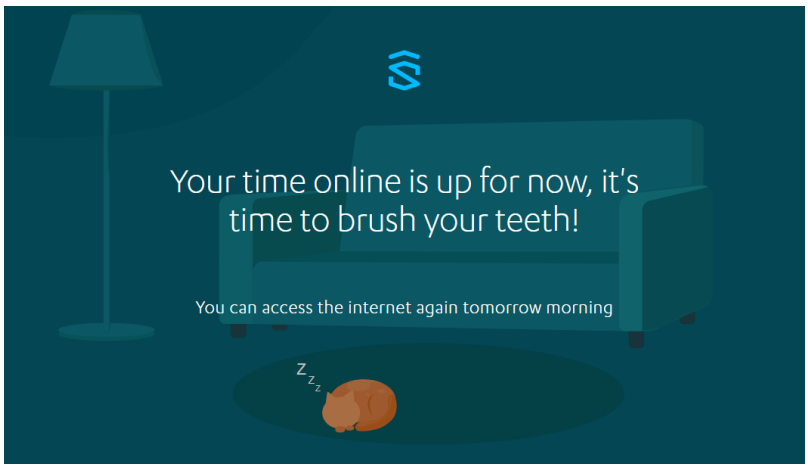
Perheturva on kuvassa 27 estänyt http://adult.fstestdomain.com-sivun näyttämisen. Estosivussa kerrotaan, että esto perustuu Perheturvan asetuksiin, joissa on estettynä sisältö, jossa on jotain jäljempänä mainittua sisältöä: pelaaminen, aikuisviihde tai aseet. Kyseiset määritellyt sisällöt ovat siis profiiliin konfiguroituja estoprofiileja eli sisältöä, jota ei näytetä loppukäyttäjälle.

Kuva 27. Sense-ohjelmiston profiloidun sisällön estosivu.

Kuvan informaatio tulee Zyxel-reittitimestä, F-Secure Sense -tuotteen injektoimana selaimen ja palvelimen väliseen liikenteeseen, kun se on katkaistu profiilissa konfiguroiduista syistä.

5.5 Aikarajoituksen kohtaaminen www-selauksessa

Aikarajoitus on tyypillinen internetin perheturvan käytön tilanne, ja sellainen voidaan kertoa ao. kuvalla Sense-tuotteessa. Aikarajoitus on asetettu Sense-profiilissa. Täten se mahdollistaa käyttäjäkohtaisilla asetuksilla loppukäyttäjän suojauksen kuten kuvassa 28.

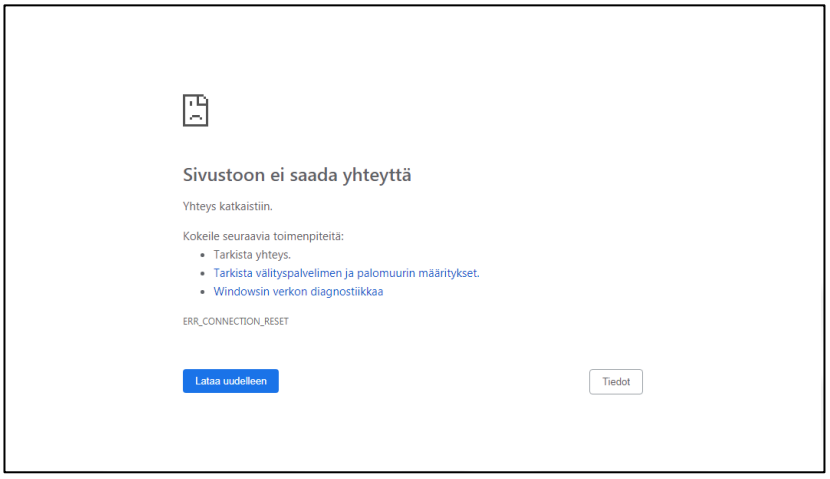


Kuva 28. Sense-ohjelmiston aikaeston informaatiosivu.

Kuten yllä, kuvan informaatio injektoidaan TCP-liikenteeseen automaattisesti estotilanteen triggreroituessa.

5.6 HTTPS-sivun suojaus

HTTPS-selauksen esimerkkinä on https://www.gunsandammo.com/-sivusto. Sivusto sisältää tietoa ja kuvia aseista, mikä on estettyä sisältöä profiilissa Suzy. F-Secure Sense antaa alla olevan estoilmoituksen ja katkaisee liikenteen. Estetty liikenne on salattua HTTPS-liikennettä ja siihen hyvin vaikeaa ja tietyissä tilanteissa osin mahdotontakin injektoida eli sisällyttää väliin ylläolevien käyttötapauksien kaltaisia asiakasystävällistä informaatioita. Tämän HTTPS-liikenteen estosivun sisältöä ja syytä tähän ilmoitukseen käsiteltiin syvemmin luvussa 2. Estoilmoitus on validi, mutta sisältö ei ole käyttäjäystävällinen.

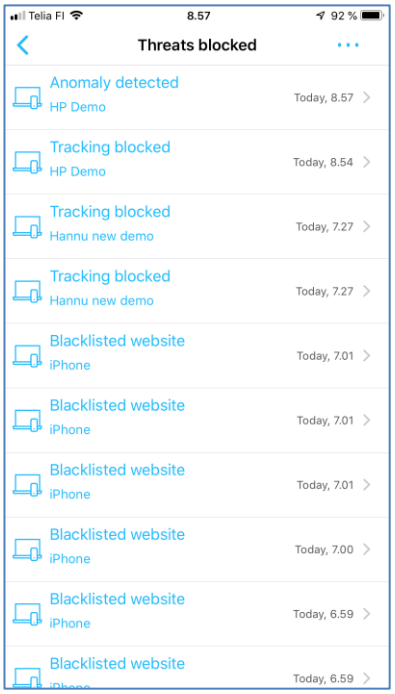


Kuva 29. HTTPS-liikenteen estosivu.

5.7 Saastuneen laitteen liikenteen detektointi

Saastunutta laitetta implikoi esimerkkikokoonpanossa IoT-WIFI-kamera. Mutta kuten aiemmin mainittiin, aidosti saastuneita esimerkkilaitteita ei ole syytä käyttää. Simuloitu

haittaliikenne tuotetaan NMAP-ohjelmistolla verkkoskannausliikenteen muodossa. ”Anomaly detected” alla olevassa kuvassa 30 kertoo haitallisesta liikenteestä.



Kuva 30. Haitallisen IoT-liikenteen ilmitulo Sense-applikaatiossa.

6 Yhteenveto

F-Secure Sense -laitteella voidaan saavuttaa kodin tietokoneiden ja IoT-laitteiden suojaus. Tämä on ensimmäisen sukupolven CPE-laitteeseen integroitu suojausohjelmisto, ja siinä on vielä paljon parantamisen varaa, mutta toisaalta se tekee jo perustyönsä. Selkeät F-Secure Sensen kehitysalueet lienevät ensivaiheessa asiakaskokemassa ja käytettävyydessä. Ensisijaisesti HTTPS liikenteen mahdollisten estojen loppuasiakaskomunikaatio voisi parantua. Yksi mahdollinen polku tälle olisi EPP ohjelmiston yhteistyö Sensen kanssa, jolloin voidaan tietää tarkasti minne loppuasiakas haluaa selaimellaan asioida. Toinen kehitysalue on aina käytettävyys, ja helppo käyttöönotto on aina korkealla listalla teleoperaattoreilla.

Rakennettu F-Secure Sense -esittely-ympäristö pääsee nk. tositoimiin pian, jo huhti-toukokuulla, jopa jo ennen tämän insinöörityön hyväksyntää. Tässä työssä on hyvinkin tarkasti testattu ja kirjattu kaikki mahdolliset esittelytapaukset, ja samalla on tullut tutkittua tarkoin Sensen käytettävyys, josta syntyy F-Securen omia sisäisiä kehityspolkuja.

Nykyinen kodin toimintakenttä hyvin erilaisilla ja eritasoisilla laitteilla on haastava. IoT-laitteissa ei parhaimmillaankaan ole edes käyttöliittymää, ja tietokone edustaa toista ääripäätä. Silti kaikille laitteille tulisi löytää helppo yksittäinen kokonaisuus, miten suojata ne internetin tietoturvauhilta.

Tämä insinöörityö sai kirjoittajan ajattelemaan ja tutkimaan tämän päivän tietoliikenteen uhkia. Vaikka sanotaan, että jokin asia ja tapahtuma on salattu, se ei aina oikeasti sitä tarkoita. Tavallisen kuluttajan ei voi olettaa ymmärtävän näitä kompleksisia kokonaisuuksia, vaan ne tulee pystyä tarjoamaan siistinä, toimivana ja helppona pakettina kuten minkä tahansa kuluttajatuotteen.

6.1 Haasteet kodin tietoturvassa

Toimiakseen kattavasti kodin tietoturva tarvitsee useita eri suojaavia kerroksia. Jokaisella kerroksella on etunsa mutta myös ongelmansa; nk. hopeista luotia ei liene olemassa.

Päätelaitesuojauksessa (EPP) ongelmana on se hyvin yksinkertainen tosiasia, että suojausohjelmat jäävät asentamatta, tai kuten alan sanonta kuuluu: asentamaton päätelaiteturva ei turvaa. Laadukas asennettu päätelaiteturva edustaa nykyään parasta mahdollista tietoturvan tasoa laitteissa, joihin sen voi asentaa.

IoT-laitteet vaativat omat ratkaisunsa päätelaitesuojan ohelle. Kodin CPE-laite eli kotireititin on luonteva ratkaisu IoT-laitteiden suojaamiseksi. Kodin reitittimen turvaratkaisussa on tosin omat ongelmansa tietoliikenteen salauksen muodossa. Osa tilanteista kyetään kommunikoimaan huonommin, jolloin asiakaskokemus kärsii - tämä luonnollisestikin koskee TLS-salattuja yhteyksiä. Puhelinten ja tietokoneiden sekä uusien IoT-laitteiden suojaus on mutkatonta reititinturvalla, koska päätelaiteohjelmia ei tarvitse asentaa. Tästä päästään päätelaitesuojauksen etuihin eli siihen, että ne suojaavat myös muilta uhilta kuten USB-tikkujen ja muiden medioiden uhilta.

Teleoperaattorit ovat suunnattoman kiinnostuneita tietoturvasta CPE-laitteiden kautta. Tämä on tavallaan ilmeistä, sillä operaattorit saavat paljon tukipuheluita liittyen tietoturvaan, ja ajatuksena onkin, että perustason suojaus voidaan toteuttaa helposti kodin verkon reunalla pienemmillä tukikustannuksilla. Teleoperaattoreilla on ainainen ongelma saada CPE-laitteet päivittymään uudempiin versioihin. Tuomalla lisäarvopalveluita itse reitittimeen saadaan uutta kommunikoitavaa loppuasiakkaille. Täten loppukäyttäjä motivoituu vaihtamaan CPE-laitteensa uudempaan versioon.

6.2 Haasteet tietoturvasuojauksessa TLS-protokollan kanssa

Aiemmin tässä dokumentissa on käsitelty TLS-salausta ja muitakin tietoturva-asioita yksityiskohtaisesti, joten niitä ei ole tarvetta toistaa tässä. TLS tekee tietoturvan hankalammaksi kodin tietoverkon reunalla, mutta se ei tee sitä mahdottomaksi. Huonomaineiset www-sivut voidaan tunnistaa hyvällä tasolla. Kehitettävää on enemmänkin käyttäjäkokemuksen puolella.

F-Secure Sensen esittelyjärjestelmän testivaiheessa havaittu harmaa estosivu HTTPS- eli TLS-liikenteen käyttötapauksessa on www-selaimen ilmoitus katkaisusta liikenteestä. Koska F-Secure Sense ei tee MItM-hyökkäystä edes luvallisesti loppukäyttäjän liikenteeseen, on tuloksena yllä havaittu www-selaimen estosivu eli sivu, joka kertoo,

että tietoliikenneyhteydessä on vikaa. Selain ei voi ymmärtää, että kyseessä on tarkoituksellinen tietoliikenteen katkaisu. Tämä on selkeä käyttötapaus, joka vaatii tuotekehitystä F-Secure Sense -tuotteelle.

Kuten aiemmin käsiteltiin, nk. DPI-tuotteet palomuureissa tekevät DPI-toiminnetta jopa TLS-liikenteelle. Palomuurivalmistajat markkinoivat tätä toiminnetta nk. Big Data -analyysinä, jota se yrityksen näkökulmasta ehkä onkin, mutta yksittäisen loppukäyttäjän eettisestä näkökulmassa kyseessä on selkeä MItM-hyökkäys. Tässä on ollut valmistajilla jo jonkin aikaa valintatilanne. Liikenne on salattua mutta tavallaan huonon TLS-protokollan syystä ja ansiosta yhtäaikaa on ollut mahdollista rakentaa yrityksen ja teleoperaattorinkin tasolla järjestelmiä, jotka purkavat salauksen matkalla lennossa loppukäyttäjän sitä ymmärtämättä. Tämä on huomattavasti suurempi eettinen asia kuin nopeasti tulee ajateltua. Eettisestä näkökulmasta TLS 1.3 -protokolla vaikeuttaa jatkossa yhdyskäytävälaitteiden konfigurointia DPI-asiassa vahvempien TLS-liikenteen kättelyprotokollien takia ja ansiosta. F-Secure Sense -testiympäristön rakentamisessa ja testikäytössä on havaittu, että tämä polku ei ole ollut F-Securen valinta vaan valintana on ”vain” tietoliikenteen katkaisu. Käyttökokemus kaikilla verkkotason suojaa toteuttavilla valmistajilla on uusien haasteiden edessä samalla kun TLS 1.3 -version käyttöaste nousee, koska kaikkien valmistajien laitteissa HTTPS-liikenteelle on samat ongelmat.

6.3 Mahdollisuudet kodin tietoturvassa

On muutamia selkeitä mahdollisuuksia, joita tulee tutkia tulevaisuudessa. Kodin CPE-laitteen ja päätelaitesuojauksen parempi integraatio parantaisi käyttäjäkokemusta etenkin salatun liikenteen vaikeissa tilanteissa. Tämä vaatii saumatonta yhteistyötä kahdelta eri tietoturvan osa-alueen tuotteelta. Tällaisen tuotekehityspanostuksen edut ovat selkeästi nähtävissä. Varmasti tulemme näkemään tällä polulla tuotekehitystä tulevina vuosina.

Aivan uusi TR-369-protokolla voi luoda mahdollisuuksia tuottaa tietoturvaa teleoperaattorin oman verkon kautta. TR-369 ei ole vielä käytössä juuri missään eli vie aikaa, että tätä päästään hyödyntämään. Standardointitahot kuten Broadband Forum ovat nähneet tulevaisuuteen selkeästi ja ottaneet huomioon monia uusia hallintaan liittyviä asioita, joita markkinoille on tulossa.

Toivottavasti lukijalle on syntynyt hyvä yleiskuva 2020-luvun kynnyksellä kodin tietoturvan vaikeuksista sekä mahdollisuuksista. Mahdollisuuksia on paljon – mutta myös kehitettävää on edelleen. Töitä on syytä jatkaa, koska kyberuhat eivät tule vähenemään; uhat tulevat lisääntymään joka vuosi.

Lähteet

1. Elisa ja F-Securen IoT laitteiden kehitysprojekti, https://www.kauppalehti.fi/uutiset/elisa-ja-f-secure-kehittavat-esineiden-internetin-tietoturvalaitetta/6706d1fe-abbd-31cb-a57c-e39f759605ab. Luettu 29.10.2018.

2. Traficom, IoT laitteiden kuluttajatutkimus, https://www.traficom.fi/sites/default/files/media/file/Kuluttajatutkimuksen_IoT-tulokset.pdf. Luettu 1.3.2019.

3. F-Secure. Brain haittaohjelma, https://www.f-secure.com/v-descs/brain.shtml. Luettu 5.3.2019.

4. F-Secure. Sasser verkkomato https://www.f-secure.com/v-descs/sasser.shtml. Luettu 5.3.2019.

5. F-Secure. Melissa verkkomato https://www.f-secure.com/v-descs/melissa.shtml. Luettu 5.3.2019.

6. F-Secure. Conficker verkkomato https://www.f-secure.com/v-descs/worm_w32_downadup.shtml. Luettu 5.3.2019.

7. AV-Test Institute testilaboratorio, PC haittaohjelmien määrän kehitys; https://www.av-test.org/en/statistics/malware/. Luettu 16.3.2019.

8. AV-Test Institute testilaboratorio,Android haittaohjelmien määrän kehitys, lähde: AV-TEST GmbH Security Report 2017/2018: The latest Analysis of the IT Threat Scenario. Luettu 15.3.2019.

9. Gartner, IoT määritelmä: https://www.gartner.com/it-glossary/internet-of-things/. Luettu 22.3.2019.

10. Hyppönen Mikko, https://twitter.com/mikko/status/808291670072717312?lang=fi. Luettu 28.3.2019.

11. Telia, eSIM tuettuja laitteita suomessa https://www.telia.fi/kauppa/liittymat/e-sim#tuetut-laitteet. Luettu 12.4.2019.

12. Telia, eSIM tarjonta https://www.telia.fi/kauppa/liittymat/e-sim. Luettu 12.4.2019.

13. Talos Intelligence, VPN-Filter haittaohjelman kuvaus, Ciscon tytäryritys Talos Security: https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html. Luettu 13.4.2019.

14. Wired, NSA työkalujen varastaminen: https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/. Luettu 13.4.2019.

15. Cyber Security Hub kuva verkon suojauksen tasoista, lähde: https://www.cshub.com/. Luettu 15.4.2019.

16. Boadband Forum, TR-069 protokollan arkkitehtuuri. Luettu 26.3.2019.

17. Broadband Forum, näkemys verkon laitteiden tulevaisuudesta. Luettu 27.3.2019.

18. Broadband Forum, TR-369 protokolla yleisarkkitehtuuri. Luettu 27.3.2019.

19. Google, HTTPS salaamisen käytön kehitys, kuva https://transparencyreport.google.com/https/overview. Luettu 28.3.2019.

20. Red-Gate.com, TLS protokollapino kuva https://www.red-gate.com. Luettu 27.3.2019.

21. Globalsign, https://www.globalsign.com/en/blog/what-is-server-name-indication/. Luettu 29.3.2019.

22. Akamai, https://blogs.akamai.com/2017/03/reaching-toward-universal-tls-sni.html. Luettu 2.4.2019.

23. Cyber security hub, Galactic Security Systems. Luettu 4.4.2019.

24. IETF, SNI toimintamalli TLS protokollassa: https://tools.ietf.org/html/rfc6066#section-3, sivu 6. Luettu 23.3.2019.

25. Nadhem J AlFardan, väitöskirja, On the design and Implementation Secure Network Protocols, 2014, http://www.isg.rhul.ac.uk/~kp/theses/NAFthesis.pdf. Luettu 13.4.2019.

26. IETF, DPI toiminne TLS 1.3 protokollassa, lähde: https://tools.ietf.org/html/draft-camwinget-tls-use-cases-00. Luettu 3.3.2019.

27. Thyla van der Merwe. Väitöskirja An Analysis of the Transport Layer Security Protocol. Sivut 4, 199 ja 202. Maaliskuu 2018. http://www.isg.rhul.ac.uk/~kp/theses/TvdMthesis.pdf. Luettu 13.4.2019.

28. TLS 1.3 protokolla RFC 8446 https://tools.ietf.org/html/rfc8446. Luettu 10.3.2019.

29. RFC 6066 määrittää TLS 1.3 protokollan yksityiskohdat. Luettu 15.4.2019.

30. DNS over HTTPS eli DoH protokollan RFC 8484 https://tools.ietf.org/html/rfc8484. Luettu 29.3.2019.

31. DNS over TLS eli DoT protokollan RFC 7858 https://tools.ietf.org/html/rfc7858.html. Luettu 29.3.2019.

32. Symantec tietoturvayhtiön selvitys ja ohjeistus TLS1.3 protokollan käyttöön palomuureisssa ja muissa laitteissa https://www.symantec.com/content/dam/symantec/docs/other-resources/responsibly-intercepting-tls-and-the-impact-of-tls-1.3-en.pdf. Luettu 24.4.2019.