Kimmo Siljander

Älytelevisioiden tietovuodot

Tietotekniikan
Pro gradu -tutkielma
30. marraskuuta 2020

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Kokkolan yliopistokeskus Chydenius

Tekijä: Kimmo Siljander
Yhteystiedot: ksiljander@hotmail.com
Puhelinnumero: 040-842 5010
Ohjaaja: Risto T. Honkanen
Työn nimi: Älytelevisioiden tietovuodot
in English: Data leakage of Smart TV's
Työ: Tietotekniikan Pro gradu -tutkielma
Sivumäärä: 66
Tiivistelmä: Älytelevisioiden kehitys on ollut todella nopeaa viimeisten vuosien aikana. Tässä Pro gradu -tutkielmassa tarkastellaan älytelevisioiden mahdollisia tietovuotoja että yksityisyyden loukkauksia. Tarkastelun kohteena on saman valmistajan kaksi eri älytelevisiota.

Työn teoriaosassa esitellään älytelevision ominaisuuksia sekä sen kehityspolku tähän päivään asti. Teoriaosassa käydään läpi älytelevision tietoturvariskejä, mahdollisia hyökkäystapoja sekä tietoturvan parantamista. Aiheesta tehtyjä muita tutkimuksia esitellään myös laajasti.

Tutkimuksen empiirisessä osassa esitellään tutkimusympäristö, käytetyt laitteet ja datan keruu- sekä analyysisuunnitelmat. Tutkimusosassa kerätään älytelevisioiden tietoliikennedataa sen keräämiseen tarkoitetulla ohjelmalla. Tutkimusosassa lisäksi analysoidaan kerättyä dataa erilaisin keinoin.

Älytelevision valmistajan laatima tietosuojakäytäntö on hyvin puolueellista luettavaa. Tietosuojakäytäntö on tehty lähinnä suojaamaan valmistajan oikeuksia. Tietosuojakäytäntö on pakotettu hyväksymään, jos haluaa liittää älytelevision internetiin ja käyttää siinä olevia sovelluksia.

Sovellusten sekä toimintojen tietoliikenteendatasta on mahdollista huomata erilaisia tietoturvaongelmia. Älytelevisioon löytyy uusi ohjelmistoversio, mutta päivitystä ei voi tehdä langattomassa verkossa. Älytelevision selainta ei voi päivittää tai poistaa, koska sopimus on loppunut toimittajan ja älytelevision valmistajan välillä. Älytelevisiot myös keräävät käyttäjien tietoja ja jakavat niitä eteenpäin valmistajalleen tai kolmannelle taholle.
Avainsanat: Älytelevisio, tieto
Abstract: The evolution of Smart TV has been very rapid in the past years. In this Master Thesis we examine possible data leaks and privacy concerns of Smart TV's. Two Smart TV's from the same manufacturer has been viewed in this essay.

The theoretical part of the research presents the features of Smart TV and its

development path to this day. The theoretical part reviews the security risks of Smart TV's, possible ways of attack and improving security. Other studies on the subject are also presented widely.

The empirical part of the research presents the research environment, product equipment, data collection and analysis designs. First, in the research part, a number of communication data of Smart TV's is collected. After that, the data is analyzed by a network analysis software.

The Privacy Policy developed by the smart TV manufacturer is very biased to read. This privacy policy is primarily designed to protect the rights of the manufacturer. You are required to accept Privacy Policy if you wish to connect your Smart TV to the Internet and use the applications on it.

It is possible to notice various security problems in the communication data of applications and functions. There is a new software version for Smart TV, but update cannot be done over a wireless network. The Smart TV browser cannot be updated or removed because the agreement between the supplier and the Smart TV manufacturer has expired. Smart TV's also collect user information and pass it on to its manufacturer or a third party.
Keywords: Smart TV, data

Sanasto

Amazon Fire TV	Amazonin valmistama mediatoistin.
Android Studio	Android-käyttöjärjestelmän ohjelmointiympäristö.
Android TV	Älytelevision käyttöjärjestelmä.
API	Application Programming Interface eli ohjelmointirajapinta.
Apple TV	Applen valmistama mediatoistin tai älytelevision käyttöjärjestelmä.
ARP	Address Resolution Protocol on protokolla, jolla selvitetään loogista osoitetta vastaava fyysinen osoite.
Bluetooth	Avoin standardi langattomaan kommunikointiin.
CIA	Central Intelligence Agency on Yhdysvaltain keskustiedustelupalvelu.
Connected TV	Englanninkielinen termi älytelevisiolle.
DOM	Document Object Model eli dokumenttioliomalli, jolla kuvataan dokumentin rakenne puumuodossa.
EPG	Electronic Program Guide eli ohjelmaopas.
Eurosport Player	Palvelu, jolla voi katsoa Eurosportin kanavia internetin välityksellä.
exeDSP	Älytelevision pääprosessi.
FFmpeg	Kokoelma vapaita ohjelmistoja, jotka voivat tallentaa ja suoralähettää digitaalista ääntä ja videota.
Google Chromecast	Palvelu, jolla voidaan siirtää esimerkiksi sisältöä puhelimesta television näytölle .
Google Play	Googlen oma sovelluskauppa.
hakkerointi	Yleismaailmallinen termi, jolla kuvataan kaikenlaista murtautumista tietojärjestelmiin.

HbbTV	Hybrid Broadcast Broadband TV. Standardi, jonka ideana on tuottaa selainpohjaisia palveluita televisioon. Palvelut ovat räätälöity jokaiselle kanavalle erikseen ja palveluiden tarjoajina toimivat ohjelmayhtiöt [23].
HDMI	High Definition Multimedia Interface. Kuvan ja äänen siirtoon tarkoitettu liitäntä.
HTML	Hypertext Markup Language. HTML tunnetaan yleisesti kielenä, jolla voi koodata vaikkapa nettisivuja.
HTML GET	Metodi, jolla voi lähettää HTML koodattuja tietoja.
HTTP	Hypertext Transfer Protocol. Protokolla, jota selaimet käyttävät tiedonsiirtoon.
HTTPS	Hypertext Transfer Protocol Secure. Protokolla, jota selaimet käyttävät suojattuun tiedonsiirtoon.
Hybrid TV	Englanninkielinen termi älytelevisiolle.
IoT	Internet of Things eli esineiden internet.
Java	Ohjelmistoalusta / ohjelmointikieli.
Linux	Käyttöjärjestelmä.
MAC	Media Access Control. MAC-osoite on verkkosovittimen yksilöivä osoite.
MI5	Military Intelligence (osasto 5), on yksi Yhdistyneen kuningaskunnan salaisen palvelun osastoista.
My Home Screen	Panasonicin käyttämä älytelevision käyttöjärjestelmä.
Netflix	Yhdysvaltalainen tilausvideopalvelu.
Nmap	Porttiskannaukseen tarkoitettu ohjelma [29, s. 1].
Protokolla	Yhteyskäytäntö.
Roku TV	Älytelevision käyttöjärjestelmä sekä myös mediatoistin.
root	Käyttöjärjestelmien pääkäyttäjä tai juurihakemisto.
Smart Hub	Samsungin sovelluskauppa.
Smart TV	Englanninkielinen termi älytelevisiolle.

Tizen	Samsungin käyttämä älytelevision käyttöjärjestelmä.
Tizen Studio	Tizen-käyttöjärjestelmän ohjelmointiympäristö.
TLS	Transport Layer Security. Suojataan internet-sovellusten tietoliikennettä IP-verkkojen yli.
UHD	Ultra High Definition. Näyttöresoluutio, jonka koko on 7680 kertaa 4320 pikseliä.
URL	Uniform Resource Locator. URL-osoite, kansanomaisesti kutsutaan myös nettiosoitteeksi.
USB	Universal Serial Bus. Datan siirton käytettävä portti tai johto.
Vevo	Musiikkivideoiden katsomiseen tarkoitettu sovellus.
Viewster	Suoratoistoon tarkoitettu sovellus.
Visual Studio	Ohjelmointiympäristö.
VPN	Virtual Private Network eli virtuaalinen erillisverkko.
Watchever	Median toistoon tarkoitettu sovellus.
Weeping Angel	Tällä nimellä kutsutaan vuoden 2014 hakkerointiskua Samsungin älytelevisioita kohtaan.
webOS	LG:n käyttämä älytelevision käyttöjärjestelmä.
Widget	Älytelevision pienoisohjelmia kutsuttiin tällä nimellä.
Wireshark	Ohjelma, jolla voidaan analysoida verkon liikennettä.
XHR	XMLHttpRequest-oliota käytetään tiedon lähettämiseen selaimen ja palvelimen välillä.
XML	Extensible Markup Language on metakieli (kansankielellä HTML-kielen riisuttu versio).
Yle Areena	Yleisradion verkkopalvelu, josta voi katsoa sisältöä suorina lähetyksinä tai tallenteina.
Youtube	Googlen omistama videopalvelu.

Sisältö

1 Johdanto

Tietoturva sekä yksityisyyden suoja ovat olleet viime vuosina ja varsinkin viime aikoina todella polttava puheenaihe. Esineiden internetiin liittyy jatkuvasti lisää laitteita ja yksi suosituimmista laitteista on ehdottomasti älytelevisio. Älytelevision kautta kirjaudutaan moniin erilaisiin palveluihin ja palveluista suosituimmat liittyvät tilausvideopalveluihin.

Mitä tietoa älytelevisio mahdollisesti kerää käyttäjästään ja mihin näitä tietoja käytetään? Vuotavatko älytelevisiot yksityisiä ja arkaluontoisia tietoja käyttäjän sitä tietämättä tai hyväksymättä? Löytyykö älytelevisioista mahdollisia tietoturvaongelmia? Nämä kysymykset ovat älytelevision käyttäjän yksityisyyden sekä tietoturvan kannalta erittäin mielenkiintoisia kysymyksiä.

Tutkimuksia älytelevisioiden tietovuodoista on maailmalla tehty jonkin verran. Benjamin Michélen ja Andrew Karpowin tutkimuksessa [32] esitellään, kuinka älytelevision voi kaapata käyttämällä hyväksi haitalliseksi tehtyä videotiedostoa. Älytelevisioiden tietovuotoa on testattu myös muun muassa Twenten yliopistolla [46]. Testeissä analysoitiin älytelevisioista lähtevää sekä tulevaa tietoliikennettä. Vastauksena löydettiin päivittämättömiä palvelimia, joissa oli paljon tietoturvaongelmia.

Eri tietokantojen (esimerkiksi Google Scholar sekä IEEE Xplore) hakusanoina on tässä tutkimuksessa käytetty aiheeseen liittyviä termejä, kuten muun muassa smarttv, data leaks, esineiden internet, iot, connected-tv, hacking, malware, Samsung, Sony, Tizen, HTTP, Wireshark, Android, älytelevisio, tietovuoto sekä näiden monia eri yhdistelmiä. Aiheesta löytyy aiemmin tehtyjä tutkimuksia, erilaisia raportteja, tietoturvaan liittyviä kirjoja sekä tietoturvaan erikoistuneita yritysten kattavia internetsivustoja.

Teoriaosassa käydään läpi älytelevision kehityskaarta, yleisimpiä käyttöjärjestelmiä, ominaisuuksia sekä toimintoja ja sovelluksia. Teoriaosassa esitellään lisäksi esineiden internetin tietoturvaa. Siinä tarkastellaan myös tietoturvariskejä, mahdollisia hyökkäystapoja esimerkkien avulla sekä käydään läpi tietoturvaa parantavia asioita. Muita aiheesta kertovia tutkimuksia esitellään varsin kattavasti.

Tutkimuksen empiirisessä osassa käydään läpi tutkimusympäristö, käytetyt laitteet sekä ohjelmat. Siinä esitellään myös datan keruusuunnitelma sekä datan ana-

lyysisuunnitelma. Tutkimuksessa on mukana kaksi saman valmistajan erimallista älytelevisiota ja tutkimus tehdään molemmille älytelevisioille erikseen. Aluksi tutkimuksessa kerätään tietoliikennedataa sen keräämiseen tarkoitetulla ohjelmalla. Kun dataa on saatua kerättyä tarpeeksi, niin se analysoidaan suunnitelman mukaan. Empiirisessä osassa ei testata tai käydä läpi varsinaisia hyökkäysmenetelmiä resurssien puutteen takia.

Tutkimustuloksista tulee esille tietosuojakäytännön puolueellisuus. Se lähinnä turvaa valmistajan oikeuksia, eikä käyttäjän. Tietoliikennedataa analysoimalla löytyy myös selkeitä tietoturvauhkia sekä tietovuotoja. Esimerkkinä toiseen tutkimuksessa käytettyyn älytelevisioon löytyy ohjelmistopäivitys, mutta päivitys ei onnistu, jos älytelevisio on liitetty internetiin langattomasti. Toinen selkeä tietoturvauhka on se, että älytelevision selaimen toimittajan sekä älytelevision valmistajan välinen sopimus on loppunut eikä vanhaa selainta pysty poistamaan. Muutaman sovelluksen tietoliikennedatasta voi helposti poimia sovelluksessa olevia videoita ja tallentaa niitä omaan käyttöön. Tämä tuskin on sisällöntoimittajan tahto.

Luvussa 2 käydään läpi älytelevisioiden kehitystä, käyttöjärjestelmiä sekä niissä olevia toimintoja. Älytelevisioiden tietoturvaa, mahdollisia hyökkäystapoja sekä tiedon keräämistä esitellään luvussa 3. Muita aiheeseen liittyviä ja kiinnostavia tutkimuksia käydään läpi luvussa 4. Luvussa 5 esitellään tutkimus ja sen vaiheet. Luvussa 6 käydään läpi tutkimuksen tulokset. Luku 7 sisältää yhteenvedon ja johtopäätökset.

2 Televisio

Ensimmäiset yleiset televisiolähetykset alkoivat 1930-luvulla ja ensimmäiset väritelevisiot tulivat myyntiin jo 1950-luvulla [1, ss. 68 – 69]. Sen jälkeen television kehitys ei edennyt kovin nopeasti eteenpäin, vaan se tuntui hieman jopa seisahtuneen paikalleen. Vasta internetin yleistyminen sai aikaan sen, että television kehitys sai uuden käänteen ja televisio onnistui säilyttämään jo hieman laskevan suosionsa kodin tärkeimpänä viihdelaitteena. [38]

Vuonna 2018 suomalaisista talouksista noin 95 prosenttia omisti television [49]. Finnpanelin tuottaman tutkimuksen mukaan suomalaiset katsoivat vuonna 2019 lineaarista televisiota (eli televisio-ohjelmien katsomista silloin, kun ne esitetään televisiossa) 2 tuntia ja 42 minuuttia vuorokaudessa. Tämän lisäksi television ruutua käytettiin muuhun tarkoitukseen, eli lähinnä internetin välityksellä tarjottaviin palveluihin, 41 minuuttia vuorokaudessa. Päivittäin televisiota katsoi 66 prosenttia väestöstä ja katsotuin hetki oli yhdeksän aikaan illalla, jolloin noin kolmasosa suomalaisista oli television ääressä. [18]

Noin kolmannes kaikista televisioista on älytelevisioita. Uudet myynnissä olevat televisiot ovat lähes kaikki älytelevisioita, joten niiden prosentuaalinen osuus nousee koko ajan kaikista televisioista. Älytelevision suosion kasvuun vaikuttavat niiden hintojen lasku, sisältöpalveluiden suuri määrä sekä sisällön helppo saatavuus ja katseltavuus. [17]

2.1 Älytelevisio

Älytelevisio on televisio, joka sisältää jonkinlaisen tietokoneen. Siinä on oma käyttöjärjestelmä, prosessori sekä keskusmuisti ja paljon muita tietokoneista löytyviä osia sekä toimintoja. Älytelevisiolla voi tehdä erilaisia toimintoja, käyttää sovelluksia sekä interaktiivisia palveluita internetin välityksellä. Sen voi yhdistää internetiin langallisesti tai langattomasti. Älytelevisiota voi kutsua huoletta myös kodin viihdekeskukseksi, koska sen avulla voi nykypäivänä käyttää todella monia eri palveluita. Älytelevisiosta käytetään myös englanninkielisiä nimiä Smart TV, Connected TV sekä Hybrid TV [3].

Älytelevisiot voidaan ryhmitellä niiden internetiin kytkeytyvien ominaisuuksien mukaan. Ensimmäiseen ryhmään voidaan sijoittaa älytelevisioiden elinkaareen aivan ensimmäiset tuotteet, joihin oli esiasennettu erilaisia pienoisohjelmia. Toiseen ryhmään laitetaan älytelevisiot, joihin on esiasennettu valmiiksi sovelluksia. Kolmanteen ryhmään sijoitetaan älytelevisiot, joihin käyttäjä pystyy itse lataamaan haluamiaan sovelluksia ja toimintoja. Erillisenä ryhmänä voidaan pitää televisioon liitettäviä mediatoistimia, jotka tekevät televisiosta älytelevision.

Television tarkoitus on aina ollut näyttää käyttäjälle sisältöä. Nykyisillä älytelevisioilla voi sisällöstä nauttia monella muullakin tavalla kuin vanhaan tapaan vain katsomalla lineaarista lähetystä. Ensimmäiset älytelevision toiminnot olivat erilaiset pienoisohjelmat, joilla pystyi vaikka lukemaan uutisia tai katsomaan pörssitiedotteita. Kehitys on tuosta hetkestä mennyt huimasti eteenpäin. [31, s. 2]

2.2 Älytelevision kehitys

Älytelevision historia alkaa periaatteessa vasta vuodesta 2007. Paljon aiemminkin on ollut televisioita, joita on pystynyt yhdistämään internetiin, mutta niiden toiminnallisuus sekä käytettävyys on ollut hyvin rajattua. Vasta ainoastaan älytelevisioille tarkoitetut käyttöjärjestelmät sekä niihin sopivat sovellukset laajemmin mahdollistivat älytelevisioiden helpon käytettävyyden sekä toimivuuden. Älytelevisioita löytyy nykyään monista eri paikoista; kodeista, hotelleista, työpaikoilta, sairaaloista sekä kirjastoista. [38]

Eri valmistajat etenivät eri tahdissa älytelevisioiden kehityksessä ja sen takia onkin hieman hankalaa yleistää älytelevisioiden historiaa. Alla olevasta listauksesta saa historian kulusta paremman käsityksen. Listassa on tuotu esille Samsungin älytelevisioiden historian kehittyminen vuoteen 2015 asti [42]:

- 2008 Valmistui sisältöön keskittynyt älytelevisiomalli, joka oli helppo yhdistää internetiin.
- 2009 Samsung otti käyttöön pienoisohjelmat (englanniksi widget).
- 2010 Markkinoille tulivat ensimmäiset sovellukset, jotka toimivat samalla tavalla monessa eri laitteessa.
- 2011 Sisältöä oli saatavissa jo huomattavasti aikaisempaa enemmän. Uusi käyttöliittymä nimeltä SmartHub lanseerattiin markkinoille.

- 2012 Interaktiivisuus lisääntyy.
- 2013 Sovellukset paranevat. Yle Areena tuli Samsungin älytelevisioihin vuonna 2014 [28].
- 2014 Käyttäjäystävällisyys paranee uuden käyttöliittymän päivityksen myötä.
- 2015 Samsung lanseerasi kokonaan uuden käyttöjärjestelmän nimeltä Tizen.

Älytelevisiot haastavat jo nyt pöytätietokoneet toiminnoillaan sekä käytettävyydellään. Älytelevisioista löytyy jo oma käyttöjärjestelmä, prosessori, erilaisia muisteja, USB- ja HDMI-portit, langaton ja langallinen internetyhteys, Bluetooth-yhteys sekä sisäänrakennettu mediatoistin. Pöytätietokoneet ovat edelleen tehokkaampia, mutta älytelevisiot kirivät etumatkaa umpeen koko ajan. Bluetooth-yhteydellä toimivat näppäimistö sekä hiiri helpottavat älytelevisioiden sisältöjen käyttöä huomattavasti. Älytelevision kaukosäädintä voi käyttää osoittimena ja sitä kautta ohjata eri toimintoja ja valita palveluja. Erilaisten pelien pelaamisen suosio älytelevision kautta kasvaa koko ajan. Syiksi voidaan mainita pelaamisen helppous, selvästi suurempi ja tarkempi näyttö sekä älytelevisioiden koko ajan parantuva tehokkuus. Varsinkin Ultra High Definition (UHD) tarkkuus älytelevisioissa tekee pelaamisesta miellyttävän kokemuksen. [5]

Vanhoista ei älyllisistä televisioista voi tehdä älytelevisioita liittämällä niihin suora- tai mediatoistolaitteen. Vanhalta televisiolta vaaditaan lähinnä vain HDMI-portti ja matka älytelevision ihmeelliseen maailmaan voi alkaa. Suora- ja mediatoistolaitteita sekä niihin liittyviä palveluita on markkinoilla useita. Google Chromecast on yksi markkinoiden tunnetuimmista suoratoistolaitteista. Kun Google Chromecastin on yhdistänyt sekä televisioon että kotiverkkoon, niin sillä voi peilata vaikkapa Yle Areenan omasta samaan kotiverkkoon liitetystä älypuhelimesta tai taulutietokoneesta suoraan television näytölle. [33, ss. 51 – 55]

Apple, Roku sekä Amazon ovat vieneet omia palveluitaan vielä hieman pidemmälle; heidän omiin mediatoistolaitteisiin on ladattu jo valmiiksi erilaisia sovelluksia käytettäväksi. Sovelluksia voi ladata näihin laitteisiin myös lisää, mutta myös sovellusten peilaaminen omasta älypuhelimesta television näytölle onnistuu helposti. Kotimaisille markkinoille suunnatut palvelut kuten Elisa Viihde, DNA TV sekä Telia TV tuovat omien sovellusten sekä mediatoistolaitteidensa kautta asiakkailleen pääsyn älytelevision kiehtovaan maailmaan. Sovellusten sekä mediatoistolaitteiden kautta avautuvaa televisiopalvelua kutsutaan yleensä internet-pohjaiseksi televisioksi (Internet Protocol Television) eli IPTV:ksi.

2.3 Älytelevisioiden käyttöjärjestelmät

Älytelevisioiden käyttöjärjestelmiä löytyy tällä hetkellä markkinoilta useita. Tunnetuimpia niistä ovat Samsungin käyttämä Tizen, LG:n käyttämä webOS, monilla eri valmistajilla käytössä oleva Android TV sekä Panasonicin My Home Screen kuten taulukossa 2.1 on tiivistetysti esitetty. Hajanainen käyttöjärjestelmien joukko hidastaa erilaisten sovellusten saamista kaikkiin järjestelmiin. Yksinkertaisesti saman palvelun tekeminen uudestaan monelle eri järjestelmälle ei ole mitenkään kaupallisesti järkevää. Älytelevisioiden käyttöjärjestelmät kehittyvät kuitenkin koko ajan ja niihin onkin saatavilla tasaisin väliajoin versiopäivityksiä. Suosituin päivitystapa on ehdottomasti internetin kautta tehtävä päivitys, mutta päivitys onnistuu myös USB-portin tai televisiosignaalin avulla.

Taulukko 2.1: Tunnetuimmat älytelevisioiden käyttöjärjestelmät.

Käyttöjärjestelmä	**Valmistaja**	**Pohja**	**Tyyppi**	**Käyttäjät**
Tizen	Samsung	Linux	Avoin lähdekoodi	Samsung
webOS	LG	Linux	Avoin lähdekoodi	LG
Android TV	Google	Linux	Avoin lähdekoodi	Sony, Philips, Sharp
My Home Screen	Panasonic	Linux	Avoin lähdekoodi	Panasonic

Tietyn käyttöjärjestelmän käytön helppous, sen vakaa toimivuus, loogisesti toimiva navigointi sekä valmiina tai mahdolliset ladattavissa olevat sovellukset vaikuttavat huomattavasti ostopäätökseen [5]. Esimerkiksi kaikki sovellukset eivät välttämättä toimi kaikissa älytelevisioissa johtuen juuri eri käyttöjärjestelmistä. Onkin mielenkiintoista seurata, tuleeko myös älytelevisioiden käyttöjärjestelmistä yhtä paljon niiden käyttäjiä jakava ominaisuus kuin se älypuhelimissa tällä hetkellä on. Älytelevisioiden elinkaari on pidempi kuin älypuhelimien tai taulutietokoneiden, mutta älytelevisioiden hintojen halpeneminen on tehnyt niistä myös selkeästi kulutustavaraa [5]. Seuraavissa luvuissa tarkastelemme hieman enemmän muutamaa suosittua älytelevision käyttöjärjestelmää.

2.3.1 Samsung ja Tizen

Eteläkorealainen Samsung Electronics oli maailman ensimmäinen yritys, joka toi markkinoille digitaalisen television vuonna 1998. Vuonna 2011 markkinoille esitel-

tiin Samsungin oma Smart Hub niminen käyttöliittymä, joka helpotti huomattavasti eri toimintojen etsimistä sekä käyttöä. Tätä hetkeä voidaankin kutsua nykyaikaisen älytelevision syntymähetkeksi.

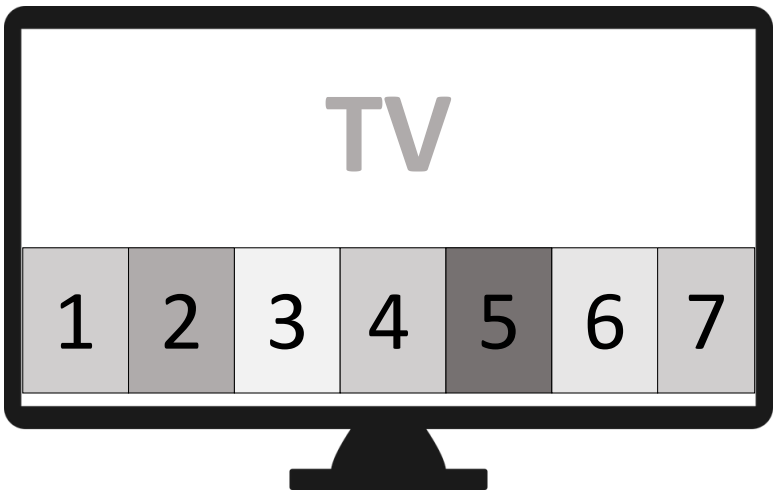
Vuonna 2015 Samsung lanseerasi Tizen-nimisen käyttöjärjestelmän omiin älytelevisioihinsa. Tizen on Linux-pohjainen avoimeen lähdekoodiin perustuva käyttöjärjestelmä. Kyseistä käyttöjärjestelmää voidaan käyttää monissa muissakin eri laitteissa kuten kameroissa, älypuhelimissa sekä taulutietokoneissa. Tizen olikin alun perin tarkoitettu älypuhelimia varten, mutta sen suosio älypuhelimien käyttöjärjestelmänä on ollut minimaalista. Uusia palveluita ja sovelluksia voi käyttöjärjestelmään hankkia edellä mainitun Smart Hub -käyttöliittymän avulla. Tizen käyttöjärjestelmään voi tehdä sovelluksia Tizen Studio - tai Visual Studio -ohjelmien avulla [13].

Tizen on tällä hetkellä yksi maailman suosituimmista älytelevisioiden käyttöjärjestelmistä. Sen suosio perustuu pitkälti jouhevaan käyttöön, helposti ymmärrettäviin toimintoihin sekä hyvään yhdistettävyyteen muihin laitteisiin. Tizenin toimintaperiaate on hyvin yksinkertainen; kun painetaan kaukosäätimestä Smart Hub -nappia, niin älytelevision ruudun alaosan päälle ilmestyy Smart Hub -käyttöliittymä. Havainnekuvassa 2.1 numeroidut laatikot kuvaavat eri toimintoja ja sovelluksia. Laatikkoa klikkaamalla saa kyseisen toiminnon tai sovelluksen päälle. Käyttöliittymässä on helppo liikkua joko nuolinäppäimillä tai käyttämällä kaukosäätimen osoitinta.

2.3.2 LG ja webOS

LG Electronics on eteläkorealainen monikansallinen elektroniikkayritys. LG hankki käyttöoikeudet webOS-käyttöjärjestelmään vuonna 2013 tietokoneita valmistavalta yhtiöltä nimeltä Hewlett-Packard. WebOS-käyttöjärjestelmän alkuperäinen kehittäjä oli teknologiayritys Palm ja se on Linux-pohjainen avoimeen lähdekoodiin perustuva käyttöjärjestelmä. Kyseisellä käyttöjärjestelmällä on nykyään vahva kanta-asiakas verkko ja tämän takia käytettävyyttä on muutettu vain vähän verrattuna vanhempiin versioihin.

Navigointi itse järjestelmässä on hyvin samanlaista, kuin muissakin käyttöjärjestelmissä. Käyttöjärjestelmän ja älytelevision asetuksia pystyy säätämään television katselun ohessa. Sovelluksia voi hankkia lisää LG:n oman kauppapaikan kautta. WebOS-käyttöjärjestelmässä on tällä hetkellä menossa versionumero 4. WebOS-käyttöjärjestelmän toimintaperiaate on hyvin samanlainen kuin Samsungin Tize-



Kuva 2.1: Havainnekuva Samsung Tizen älytelevision käyttöliittymästä.

nin. Käyttöliittymä avautuu ruudun alaosan päälle. Siinä on helppo navigoida ja sitä pystyy muokkaamaan helposti oman näköiseksi. WebOS-käyttöjärjestelmään on upotettu monia hienoja toimintoja; voit esimerkiksi kesken elokuvan kysyä käyttöjärjestelmältä kyseisen elokuva ohjaajan tai näyttelijän nimeä.

2.3.3 Google ja Android TV

Google on yksi maailman tunnetuimmista yrityksistä. Android on taas yksi suurimmista käyttöjärjestelmistä maailmassa, jollei jopa suurin. Android TV on Googlen kehittämä ja omistama älytelevisioille tarkoitettu käyttöjärjestelmä. Se kilpailee tällä hetkellä Samsung Tizenin kanssa suosituimman älytelevisioille tarkoitetun käyttöjärjestelmän tittelistä. Android TV on Linux-pohjainen ja perustuu avoimeen lähdekoodiin. Suosituin ohjelmointikieli on Java ja sovelluksia voi tehdä Android Studion avulla.

Android TV -käyttöjärjestelmä on jatkumoa epäonnistuneelle Google TV -projektille ja se lanseerattiin kesällä 2014. Kyseinen käyttöjärjestelmä on looginen käytettävä ja navigointi tapahtuu riveittäin vasemmalta oikealla. Lisää toimintoja ja sovelluksia voi hankkia Googlen omasta Google Play -sovelluskaupasta. Android TV -käyttöjärjestelmässä on sisäänrakennettu mediatoistin nimeltä Chromecast ja järjestelmä tukee myös äänikomentoja. Android TV ei ole kuitenkaan unohtanut iOS-

käyttöjärjestelmän käyttäjiä, koska Android TV tukee myös AirScreen-sovellusta. Android TV -käyttöjärjestelmää käyttävät älytelevisioissaan muun muassa Sony, Philips, Sharp, TCL sekä Grundig. Jokainen edellä mainituista televisiovalmistajista tuo oman mausteensa Android TV -käyttöjärjestelmään, joten ulkoasu ja toiminnot hieman vaihtelevat riippuen televisiovalmistajasta.

2.3.4 Panasonic ja My Home Screen

My Home Screen -käyttöjärjestelmä on Panasonicin kehittämä älytelevisioille tarkoitettu avoimeen lähdekoodiin perustuva Linux-pohjainen käyttöjärjestelmä. Se perustuu jo lopetettuun Mozilla Firefox OS -käyttöjärjestelmään. Käyttöjärjestelmän valikoissa on helppo navigoida toiminnosta toiseen. Lisää sovelluksia voi ladata Firefoxin omasta kauppapaikasta, mutta niitä on valitettavasti tarjolla verrattain vähän. Tällä hetkellä My Home Screen -käyttöjärjestelmästä on menossa kehitysversio 3.0. Panasonic on kuitenkin ottanut uusissa älytelevisioissaan käyttöjärjestelmäksi Android TV:n.

2.3.5 Muut valmistajat

Muita älytelevisioille käyttöjärjestelmiä valmistavia tahoja on todella vähän Suomen markkinoilla. Yhdysvaltalaiset Roku ja Amazon ovat kehittäneet omat älytelevisioille tarkoitetut käyttöjärjestelmät nimeltään Roku TV ja Amazon Fire TV. Näiden kahden käyttöjärjestelmän vahvuus on niiden rikas sisältö, joka on suurimmaksi osaksi suunnattu Yhdysvaltojen markkinoille.

Roku TV on älytelevisioille sekä erilaisille mediasoittimille tarkoitettu käyttöjärjestelmä. Roku TV -käyttöjärjestelmää löytyy esimerkiksi Hitachin sekä Hisensen älytelevisioista ja se on Linux-pohjainen käyttöjärjestelmä. Itse käyttöjärjestelmä on hyvin samantapainen käytettävyydeltään kuin kilpailijoidenkin, mutta Roku TV on ehkä eniten muunneltavissa käyttäjän itsensä näköiseksi.

Fire TV on taas Amazonin omistama ja kehittämä älytelevisioille tarkoitettu käyttöjärjestelmä. Fire TV -käyttöjärjestelmää käytetään Roku TV -käyttöjärjestelmän tapaan monissa eri mediasoittimissa. Amazon onkin keskittynyt enemmän juuri mediasoittimien kuin älytelevisioiden myyntiin. Japanilainen Toshiba tarjoaa kuitenkin ainakin joissain uusimmissa malleissaan Amazon Fire TV -käyttöjärjestelmällä varustettuja älytelevisioita.

2.4 Älytelevisioiden ominaisuudet

Ensimmäisten älytelevisioiden internetiin liitettyjä toimintoja kutsuttiin pienoisohjelmiksi (englanniksi widget). Kyseisten pienoisohjelmien alustana toimi Yahoo TV ja niillä oli mahdollista vaikkapa tarkistaa päivän sää tai katsoa jotain nettiin ladattuja videoita. Kyseisten pienoisohjelmien käyttö oli todella kömpelöä ja toiminta hitaanpuoleista. Kaikki suurimmat televisiovalmistajat tukivat Yahoo TV -alustaa, mutta se ei koskaan lyönyt kunnolla markkinoilla läpi. [6]

Älytelevisioista löytyy nykyään todella monia erilaisia toimintoja sekä sovelluksia. Älytelevision ohjaamiseen ei tarvita enää edes kaukosäädintä, vaan älytelevisiota voi ohjata vaikkapa omalla älypuhelimella tai ääniohjauksella eli esimerkiksi puhumalla. Sovelluksien avulla voi katsoa eri televisiokanavia (maksullisia tai maksuttomia), lukea sähköpostia, päivittää Facebook-tiliä tai vuokrata vaikka videoita. Ensimmäinen sovellus, joka löi suuresti läpi älytelevisioissa, oli Yhdysvaltalainen tilausvideopalvelu Netflix [6].

2.4.1 Toiminnot ja sovellukset

Verkkoselain on toiminto, joka löytyy monesta älytelevisiosta. Sen käytettävyys älytelevision kautta tosin jakaa mielipiteitä eikä verkkoselain usein edes tue kaikkea sisältöä. Jos kuitenkin haluaa käyttää verkkoselainta älytelevision kautta, niin kannattaa hankkia erillinen näppäimistö sekä hiiri, jotka helpottavat huomattavasti selaimen käyttöä. Älytelevisiota käytetään myös paljon pelkkänä näyttönä. Kuva siirretään pienemmästä laitteesta, kuten puhelimesta, langattomasti tai langallisesti isompaan näyttöön eli älytelevisioon.

Myös monia erilaisia pelejä pystyy pelaamaan älytelevision avulla eli enää ei välttämättä tarvita erillistä pelikonsolia lainkaan. Toki pelikonsolit toimivat vielä tällä hetkellä jouhevammin, mutta älytelevisioiden tekniikka kehittyy koko ajan. Pelejä ohjataan älytelevision kaukosäätimellä, pelikonsoleista tutuilla peliohjaimilla tai vaikka omalla älypuhelimella. Osa peleistä on ilmaisia, mutta osan joutuu ostamaan älytelevision oman kauppapaikan kautta. Älytelevision kuvaruudun suuri koko sekä kuvan hyvä tarkkuus ovat ne suurimmat edut, kun verrataan pelaamista vaikkapa kannettavaan tietokoneeseen.

Älytelevision avulla voi soittaa myös niin sanottuja kuvallisia puheluita, jos on hankkinut älytelevisioon kameran ja mikrofonin. Joistakin älytelevisioista kamera sekä mikrofoni löytyy jo valmiiksi asennettuna. Älytelevisioilla voi myös kuunnel-

la musiikkia, katsella valokuvia tai vaikka päivittää omia sosiaaliseen mediaan liittyviä palveluita. Kun liittää älytelevisioon USB-portin kautta kiintolevyn, niin voi älytelevisiota käyttää tallentavan digiboksin tavoin.

Älytelevision sisältämät toiminnot ja siinä toimivat sovellukset ovat hyvin paljon riippuvaisia älytelevision merkistä, mallista sekä valmistusvuodesta. Myös älytelevision käyttöjärjestelmä sekä käyttöjärjestelmän versio vaikuttavat toimintoihin sekä varsinkin sovelluksiin. Sovelluksia kehittävät yritykset tekevät sopimuksia suoraan älytelevisiovalmistajien kanssa ja melkein jokaiselle saman merkin televisiomallille joudutaan räätälöimään pahimmassa tapauksessa oma sovellus [35]. Tästä ollaan pyrkimässä eroon yhtenäistämällä älytelevisioiden käyttöjärjestelmiä ainakin valmistaja tasolla.

Suosituimmat ja käytetyimmät palvelut Suomessa ovat erilaiset tilausvideopalvelut sekä urheilusisältöä tarjoavat palvelut. Jokaisen tuntema tilausvideopalvelu Netflix löytyy valmiiksi asennettuna jo melkein kaikista älytelevisiomalleista. Tilausvideopalvelun suosion takaa periaatteessa kolme kohtaa: hinta pitää olla kohdallaan, palvelun pitää olla helppo ja joustava käyttää sekä sisällön pitää vastata kuluttajien vaatimuksia. Tällä hetkellä noissa kolmessa kohdassa on ehkä parhaiten onnistunut juuri Netflix. Viaplay, HBO Nordic, C More, Yle Areena, Ruutu, Youtube, Spotify sekä MTV Katsomo ovat Netflixin ohella suosituimpia ja käytetyimpiä sovelluksia.

Erikseen täytyy mainita maailman markkinoille loppuvuodesta 2019 lanseerattu suoratoistopalvelu Disney+. Tämä palvelu lanseerattiin Suomessa syyskuussa 2020 ja tilausmäärä maailmanlaajuisesti on ylittänyt jo sadan miljoonan tilaajan rajapyykin. Suoratoistopalvelun mahtava suosio varmasti lisää myös Disneyn kiinnostusta panostaa kyseiseen palveluun vielä enemmän tulevaisuudessa [24].

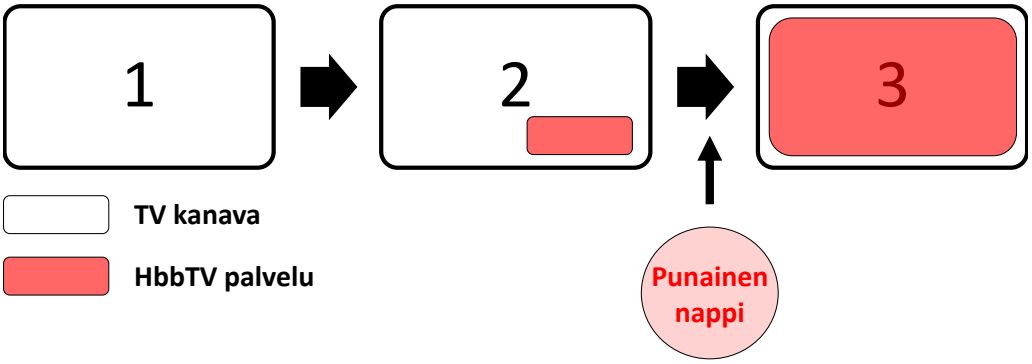
Taulukko 2.2: Älytelevisioiden tunnettuja sovelluksia.

Netflix	Viaplay	HBO Nordic
YLE Areena	Ruutu	MTV Katsomo
Youtube	Facebook	C More
Skype	Disney+	Spotify

2.4.2 HbbTV-palvelu älytelevisioissa

Yksi jo Euroopassa huomiota saanut ja menestynyt palvelu on HbbTV (Hybrid broadcast broadband TV). Se on standardi, jonka ideana on tuottaa selainpohjaisia palveluita älytelevisioon. Nykyään HbbTV-palvelun kautta tarjottavia toimintoja ovat esimerkiksi laajennettu ohjelmaopas, mahdollisten mediakirjastojen käyttö (uutiset) tai sisällön katsominen jälkikäteen[21]. HbbTV-palvelulla voi myös äänestää tv-ohjelmissa tai ohjata käyttäjä kyseisen televisiokanavan maksullisen sisällön tilaamiseen. Palvelut ovat räätälöity jokaiselle kanavalle erikseen ja palveluiden tarjoajina toimivat eri ohjelmayhtiöt. Suomessa HbbTV-palvelu on käytössä ainakin Digitan antenniverkossa sekä Telian kaapeliverkossa. HbbTV-palvelu vaatii toimiakseen sen, että televisiosignaalin tarjoava taho (esimerkiksi Telia) laittaa televisiosignaaliin mukaan tiedon HbbTV-palvelusta, käyttäjän älytelevisio tukee HbbTV-palvelua sekä älytelevisio on yhteydessä internetiin [23]. HbbTV-palvelun toimivuus on havainnollistettu kuvassa 2.2 ja se menee yksinkertaistettuna seuraavalla tavalla [20]:

- Ohjelmayhtiö laittaa oman kanavansa signaalin mukana URL-tiedon (esimerkiksi MTV3).
- Kun käyttäjä vaihtaa kyseiselle HbbTV-palvelun sisältävälle kanavalle, niin älytelevision ruudulle tulee yleensä ilmoitus, että tällä kanavalla on HbbTV-palvelu käytössä.
- Käyttäjä aktivoi kanavalla ollessaan HbbTV-palvelun päälle painamalla kaukosäätimen punaista nappia.
- Itse HbbTV-palvelu on eräänlainen pieni kyseisen kanavan oma käyttöliittymä, joka näkyy kanavan päällä. Käyttöliittymän kautta voi käyttäjä valita haluamiaan palveluita.



Kuva 2.2: HbbTV-palvelun aktivointi

Nelonen median kanavilla HbbTV-palvelusta löytyy samoja palveluita kuin heidän omasta Ruutu-palvelustaan. Käyttäjä voi aloittaa ohjelman katsomisen alusta tai katsoa esimerkiksi kyseisen sarjan muita jaksoja. Näitä kyseisiä toimintoja on yleensä mahdollista käyttää vain suoraan Ruutu-palvelun avulla. [14]

Laajennetun ohjelmaoppaan avulla käyttäjä näkee ohjelmista enemmän tietoja kuin perinteisen EPG:n avulla. HbbTV-palvelun avulla käyttäjä pystyy myös katsomaan elokuvien esittelyfilmejä [14]. Palveluntarjoaja pystyy helposti myös mainostamaan omia maksullisia palvelujaan käyttäjille sekä ohjaamaan heitä suoraan omille tilauskanavilleen. Tällä tavoin palveluntarjoajan ei tarvitse maksaa myyntipalkkioita lisäpalveluiden myynnistä. Tämä syy (eli televisiosignaalin tarjoavan tahon ohittaminen myynnissä) taitaa olla suurin syy siihen, miksi HbbTV-palvelu ei ole yleistynyt Suomessa kaapelitelevisioverkoissa sen enempää.

3 Esineiden internetin tietoturva

Älytelevision yhdistäminen internetiin tuo sille paljon uusia ominaisuuksia sekä lisäarvoa. Verkkoon kytkettyä laitetta voidaan ohjailla olematta itse paikan päällä, verkon kautta saadaan laitteesta lisätietoa tai siihen voidaan lisätä eri toimintoja. Internetiin kytkettyjä erilaisia laitteita kutsutaankin esineiden internetiksi [44, ss. 17 – 19]. Esineiden internetin laitteiden kasvava joukko houkuttelee myös paljon sellaisia tahoja, jotka haluavat hyötyä käyttäjien tiedoista jollain tavalla tai sitten kaapata vaikkapa koko kotiverkon omaan käyttöönsä [38].

Älytelevisio on tuonut maailmaan yhden uuden tietoturvaongelman lisää. Älytelevisio on kytketty internetiin eikä yleensä sisällä lainkaan minkäänlaista palomuuri- tai tietoturvaohjelmistoa [13]. Älytelevisioihin on valitettavasti saatavilla vähemmän tietoturvapäivityksiä kuin tietokoneisiin, joka tekee niistä enemmän haavoittuvimpia. Älytelevisioiden käyttöjärjestelmät ovat hyvinkin suljettuja, joten käyttäjän on liki mahdotonta tietää, että onko oma älytelevisio haavoittuvainen esimerkiksi erilaisille tietoturvahyökkäyksille [32].

Helpoin ja paras tapa suojautua tietoturvaongelmilta on kytkeä älytelevisio kokonaan irti internetistä. Tämä luonnollisesti aiheuttaa sen, että suurinta osaa älytelevision sovelluksista ei voi käyttää lainkaan. Samsungin älytelevisioihin on ollut mahdollista hankkia oma virustorjuntaohjelma tietoturvayritys McAfeen kautta, mutta tuki tuotteelle on valitettavasti jo loppunut [30]. Älytelevision käyttäjän yksityisyyttä sekä turvallisuutta on parannettu ja sitä parannetaan koko ajan.

3.1 Tietoturvariskit

Esineiden internetin suurimpia tietoturvariskejä ovat siihen liitetyt huonosti suunnitellut sekä toteutetut laitteet ja ohjelmat. Esineiden internetin kasvuvauhti on ollut viime vuosina todella hurja ja se tulee vain kasvamaan tulevaisuudessa [50]. Tietoturva ja yksityisyyden suoja ei millään pysy kehityksessä mukana [4]. Tämä aiheuttaa sen, että esineiden internetissä on paljon erilaisia tietoturvariskejä.

Yksi kiinnostavista kohteista hakkeroinnille on älytelevisio. Mahdolliset hakkerit pystyvät tunkeutumaan älytelevisioon esimerkiksi mediatoistimen, kameran, in-

ternetin tai haittaohjelman avulla [26]. Tosin älytelevisioon suunnatun hakkeroinnin pitää olla kohdistettu juuri oikein, jotta siitä saadaan irti haettu hyöty. Esimerkiksi vuonna 2013 havaittiin Philips-älytelevisioissa vakava tietoturvariski. Hakkeri pystyi halutessaan ottamaan koko älytelevision haltuunsa ja muun muassa tallentamaan käyttäjän käyttämiä tunnuksia ja salasanoja. [27]

Todennäköisesti älytelevision yleisin tietoturvariski on itse älytelevision käyttäjä. Harvempi käyttäjä lukee älytelevision käyttöohjeita tai käyttöehtoja missään vaiheessa. Käyttäjä ei tee ohjelmistopäivityksiä eikä käytä palveluissaan tarpeeksi vahvoja salasanoja. Hän ei välttämättä kirjaudu ulos sovelluksista tai lataa sovelluksia epämääräisiltä tahoilta. Käyttäjä ei ota käyttöön mahdollisia palomuureja eikä virustorjuntaohjelmistoja. [38]

Suuri käyttäjän yksityisyyttä loukkaava asia on se, että käyttäjä on pakotettu hyväksymään palvelun tarjoajan ehdot ja edellytykset (käyttöehdot) ennen kuin käyttäjä pääsee edes asentamaan kyseistä laitetta. Tällainen käyttöehtojen pakotettu hyväksyminen on käytössä esimerkiksi Sonyn älytelevisioissa, joiden käyttöjärjestelmänä on Googlen ylläpitämä Android TV. Ottaakseen käyttöön ostamansa älytelevision, on käyttäjän siis pakko hyväksyä käyttöehdot, halusi hän sitä tai ei [13].

3.2 Yleisiä hyökkäystapoja

Hyökkääjä voi halutessaan aiheuttaa paljon haittaa ja ongelmia älytelevision omistajalle. Älytelevision haavoittuvimpiin osiin lukeutuvat sisäänrakennettu mediasoitin, HbbTV-palvelun standardin puutteellisuus, laiteohjelmisto (firmware), älytelevisiossa oleva selain sekä älytelevisiossa olevat tai siihen ladattavat sovellukset. Myös laitteen avoimet portit (esimerkiksi USB-portti) sekä älytelevision huono konfigurointi ovat hyökkääjälle mahdollisuuksia murtautua sisään älytelevisioon [31, s. 3] [45]. Hyökkääjä voi päästä hyväksikäyttämään edellä mainittuja haavoittuvuuksia erilaisilla haittaohjelmilla sekä hyödyntämällä mahdollisia tietoturva-aukkoja. Monet hyökkäystavoista ovat erilaisten hyökkäystapojen yhdistelmiä.

3.2.1 Troijan hevonen

Troijan hevonen on yleisnimitys naamioiduille haittaohjelman avulla tehdyille hyökkäyksille. Haittaohjelma naamioidaan tavalliseksi ohjelmaksi ja tällä tavoin se pääsee sisään tietokoneeseen. Haittaohjelma kerää tietoa salasanoista, pankkitiedoista

ja muista arkaluontoisista tiedoista käyttäjän siitä mitään tietämättä [55].

Haittaohjelma voidaan syöttää älytelevisioon monella eri tavalla. Haittaohjelman sisältämä sovellus voidaan ladata käyttäjän toimesta yleisestä sovelluskaupasta ja sovelluksen asentamisen tai käynnistämisen aikana haittaohjelma pääsee älytelevisioon [34]. Yleisissä sovelluskaupoissa kuitenkin pyritään karsimaan tällaiset haittaohjelmia sisältävät sovellukset pois valikoimasta, jos se vain on mahdollista.

Toinen tapa on asentaa haittaohjelma suoraan USB-portin kautta. Tämä tapa tietysti vaatii fyysisen pääsyn älytelevisioon. Kolmas tapa on lähettää älytelevision käyttäjälle sähköpostia tai viestiä sosiaalisen median kautta. Kun käyttäjä sitten avaa viestissä olevan latauslinkin älytelevisiollaan, niin haittaohjelma pääsee murtautumaan sisään [2].

Neljäs tapa on syöttää haittaohjelma väärennetyn antenniverkon sekä HbbTV-palvelun avulla. Väärennettyä antenniverkon signaalia voidaan lähettää vaikka pienoislennokin avulla ja väärennetyn signaalin mukana tuleva ilkeämielinen HbbTV-palvelu syöttää älytelevisioon haittaohjelman käyttäjän huomaamatta. Tällä tavoin on mahdollista kaapata isokin joukko älytelevisioita yhdellä kerralla. [43]

3.2.2 ARP-myrkytys

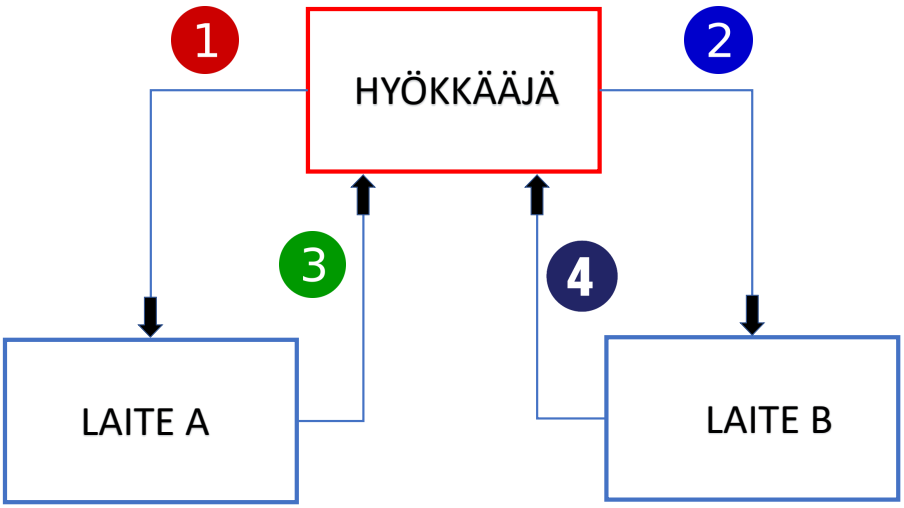
ARP eli Address Resolution Protocol on protokolla, joka muuntaa loogiset osoitteet fyysisiksi osoitteiksi [37]. Loogisella osoitteella tarkoitetaan IP-osoitetta ja fyysisellä osoitteella tarkoitetaan MAC-osoitetta (Media Access Control). ARP-kyselyllä laitteet saavat tietoonsa toistensa MAC-osoitteet. Ne tarvitaan, jotta laitteet voivat keskustella keskenään. ARP-kysely menee seuraavasti [19]:

1. Laite A kysyy: Kenellä on IP-osoite XXX? Minun MAC-osoite on AAA.
2. Laite B vastaa: Minulla on IP-osoite XXX. Minun MAC-osoite on BBB.
3. Laitteet päivittävät ARP-taulunsa ja yhteys on muodostettu.

ARP-protokolla on tehokas tapa suorittaa laitteiden välinen tunnistus. Se on samalla myös hyvin haavoittuvainen, koska se ei sisällä minkäänlaista todennusta ja täten siihen on mahdollista hyökätä väliin [39]. ARP-myrkytyksellä hyökkääjä haluaa päästä kahden eri laitteen väliin ja se voidaan tehdä vain lähiverkossa. ARP-myrkytys etenee kuvassa 3.1 osoitetulla tavalla [10]:

1. Hyökkääjä lähettää ARP-vastauksen laitteelle A omalla MAC-osoitteellaan.

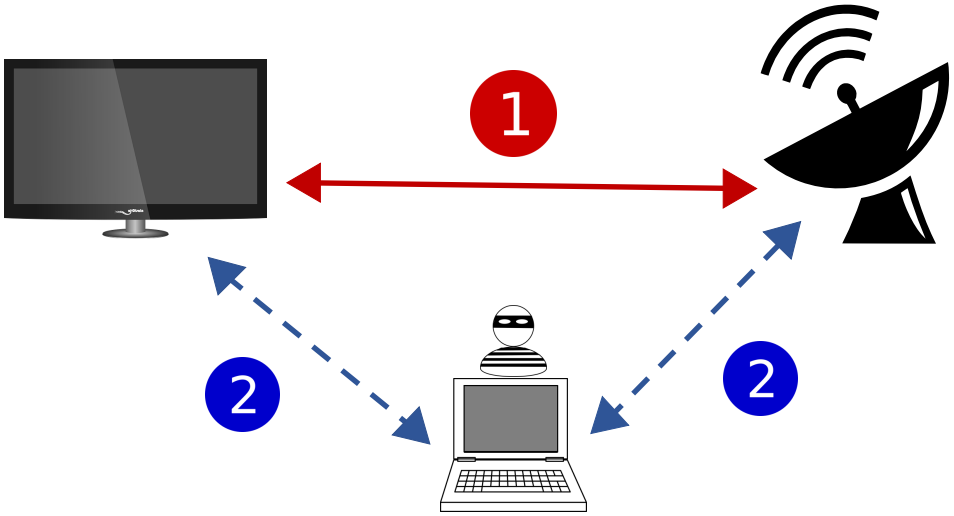
2. Hyökkääjä lähettää ARP-vastauksen laitteelle B omalla MAC-osoitteellaan.
3. Kun laite A haluaa lähettää viestin laitteelle B, niin viesti kulkeekin Hyökkääjän kautta.
4. Kun laite B haluaa lähettää viestin laitteelle B, niin viesti kulkeekin Hyökkääjän kautta.



Kuva 3.1: Havainnekuva ARP-myrkytyksestä

3.2.3 Man In The Middle

Mies välissä -hyökkäys on englanniksi ”Man In The Middle -attack” (myöhemmin tekstissä MITM). Se on yksi kaikkien tunnetuimmista hakkerointitavoista sekä se aiheuttaa eniten huolta tietoturva-asiantuntijoille. MITM-hyökkäystapoja on useita erilaisia, mutta periaate on kuitenkin kaikissa sama. MITM-hyökkäyksessä hyökkääjä asettaa itsensä kahden tai useamman viestijän väliin, kuten kuvassa 3.2 on esitetty. Tätä hyökkäystapaa voidaan käyttää periaatteessa missä vain, kuten esimerkiksi sisällön- tai palveluntarjoajan sekä älytelevision välillä. Kuvassa 3.2 kohta 1 on alkuperäinen yhteys ja kohta 2 on uusi yhteys, joka kulkee siis hyökkääjän kautta [10].



Kuva 3.2: Havainnekuva MITM-hyökkäyksestä

3.2.4 Hyökkäys selaimen kautta

Selaimen kautta voidaan hyökätä monella eri tavalla. Virus tai haittaohjelma pääsee uhrin koneelle, kun uhri käy ilkeämielisellä sivustolla. Uhrin ei tarvitse edes klikata sivustolla mitään, pelkkä käynti riittää.

Man In The Browser -hyökkäys käyttää Troijalaista hevosta saastuttaaksen uhrin selaimen. Kun uhri käyttää selainta, niin hyökkääjä saa selville kaikki uhrin tekemät toiminnot, kuten esimerkiksi tunnukset ja salasanat yksityisiin tietoihin. Suosituin tapa hyökätä uhrin koneelle on laajennusten kautta, kuten esimerkiksi käyttämällä JavaScriptiä hyödyksi. Koska nykyaikaiset selaimet on rakennettu käyttöjärjestelmien mukaan kerroksittain, niin niihin voidaan hyökätä myös eri kerroksien kautta [40].

3.2.5 Kiristyshaittaohjelma

Kiristyshaittaohjelmalla hyökkääjä yrittää tavoitella taloudellista hyötyä. Haittaohjelma tekee käyttäjän elämästä vaikeaa ja maksamalla tietyn korvauksen hyökkääjä palauttaa tilanteen alkuperäiseen muotoonsa. Kiristyshaittaohjelmalla tehty hyökkäys etenee seuraavalla tavalla:

1. Haittaohjelma laitetaan liikkeelle.
2. Kun haittaohjelma on tunkeutunut uhrin koneeseen, niin se käynnistää hyökkäyksen ja ilmoittaa kiristyksestä uhrille.
3. Kun taloudellinen korvaus on maksettu, hyökkääjä lähettää haittaohjelman purkukoodin uhrille.

Kiristyshaittaohjelmia voidaan käyttää moneen eri tarkoitukseen. Sillä voidaan vaikka sulkea uhrin puhelin, varastaa arkaluonteisia tietoja tai jopa ohjata liikennevaloja. Kryptovaluuttojen yleistyminen ja anonyymisyys on myös lisännyt kiristyshaittaohjelmien käyttöä. [56]

3.3 Älytelevisioon tehtyjä hyökkäyksiä

3.3.1 Troijan hevonen

Haittaohjelma on hyökkääjän ehkä potentiaalisin tapa päästä älytelevisioon sisään ja aiheuttaa käyttäjälle ongelmia. Kyseistä hyökkäystä kutsutaan Troijan hevoseksi. Itse haittaohjelma voi sitten suorittaa älytelevisiossa monenlaisia eri toimintoja. Se voi kerätä käyttäjän käyttäjätunnuksia sekä salasanoja eri sovelluksista ja lähettää ne takaisin hyökkääjälle. Haittaohjelma voi määrätä älytelevisiossa olevan kameran ja mikrofonin kuvaamaan ja äänittämään huoneen tapahtumia. Haittaohjelmalla voidaan saada selville käyttäjän langattoman verkon tietoja, kuten tunnuksen sekä salasanan. Haittaohjelmalla hyökkääjä voi vaikka sulkea tai lukita koko älytelevision ja pyytää sen uudelleen avaamisesta taloudellista hyötyä.

Kuuluisin haittaohjelmalla tehty hyökkäys on varmaankin CIA:n sekä MI5:n harjoittama Samsungin älytelevision kaukosäätimen mikrofonin kautta tehty vakoilu. Kyseistä hyökkäystä kutsuttiin nimellä Weeping Angel. Kyseisessä hyökkäyksessä älytelevisio näytti ulospäin siltä, että se olisi kokonaan pois päältä, mutta se pystyi kuitenkin kaukosäätimessä olevan mikrofonin avulla tallentamaan sen lähellä tapahtuvat keskustelut [25]. Ironisinta koko Weeping Angel -vakoilu tapauksessa on se, että kyseinen hyökkäys tuli julkiseen tietoon CIA:han tehdyn tietomurron jälkeen paljastetuista salaisista dokumenteista [11].

Toinen esimerkki Troijan hevosesta on Symantecin tutkija Candid Wueestin omalle älytelevisiolle tekemä hyökkäys [53]. Kyseisessä hyökkäyksessä Wueest käytti hyväkseen älytelevisioon etukäteen ladattua pelikauppaa, jonka kautta pystyi lataamaan pelejä. Pelikauppa ei käyttänyt salattuja viestejä kommunikoidessaan palvelimensa kanssa ja näin viestejä pystyi muokkaamaan haluamallaan tavalla. Wueest muutti yhden autopelin sovelluksen sijaintietoja niin, että pelin lataamisen sijasta hän latasikin haittaohjelman älytelevisioonsa. Kun haittaohjelma oli latautunut, niin se lukitsi koko älytelevision eikä sitä voinut enää käyttää ollenkaan.

3.3.2 Man In The Middle sekä HbbTV-palvelu

Symantecin tutkija Candid Wueest käytti yhdistettyä MITM-hyökkäystä sekä Troijan hevosta, kun hän hyökkäsi omaa älytelevisiota vastaan [53]. Ensin hän salakuuntelemalla löysi salaamattomat viestit, tämän jälkeen laittoi itsensä viestien väliin jotta pystyi muuttamaan niiden sisältöä ja kolmanneksi latasi vielä haittaohjelman eli

troijalaisen hevosen älytelevisioon.

Columbian yliopiston tutkijat Yossef Oren sekä Angelos Keromytis löysivät väliintulohyökkäyksen mahdollistavan aukon HbbTV-palvelussa vuonna 2014. Kyseisen aukon kautta hyökkääjä pystyi muokkaamaan sisältöä haluamallaan tavalla. Tällä tavoin hyökkääjästä tulee itse sisällön hallitsija ja lähettäjä [36].

3.3.3 Selaimen avulla

Selaimen kautta hyökkääjällä on myös mahdollisuus tunkeutua älytelevision järjestelmään sisään ja saada hankittua arkaluontoisia tietoja. Yleensä älytelevision selaimet ovat vanhoja, päivityksiä vailla eikä niiden turvallisuuteen panosteta samalla lailla kuin esimerkiksi tietokoneissa oleviin selaimiin. Sveitsiläisen Oneconsult yrityksen työntekijä Rafael Scheel löysi kaksi haavoittuvuutta älytelevision selaimesta. Toinen liittyi Flash Player -sovellukseen ja toinen liittyi JavaScriptissä olevaan toiminnallisuuteen. Näiden haavoittuvuuksien kautta hyökkääjällä oli mahdollisuus murtautua järjestelmään [11].

3.3.4 Kiristyshaittaohjelma

Älytelevisiota voidaan käyttää myös täysin rikolliseenkin toimintaa. Jos rikollinen on saanut kaapattua älytelevisioon integroidun kameran tai älytelevisioon kytketyn kameran haltuunsa, niin hän pystyy helposti havaitsemaan milloin asunto on tyhjä mahdollista ryöstöä varten. Jos taas älytelevision käyttäjä on syöttänyt älytelevisioon esimerkiksi luottokorttinsa tiedot tai ladannut johonkin kauppaan valmiiksi rahaa, niin kaapattuaan älytelevision on rikollisella mahdollisuus käyttää noita tietoja omaksi hyväkseen. Älytelevision käyttäjää voidaan myös kiristää lukitsemalla toiminnot ja pyytämällä avaamisesta taloudellinen korvaus. [31, s. 82]

Vuonna 2015 älytelevisioita kiusasi kiristyshaittaohjelma nimeltä FLocker, joka päästyään sisään laitteeseen lukitsi uhrin näytön. Uhrin älytelevision näytölle tuli huijausviesti poliisilta tai muulta viranomaiselta. Tällä tavoin hyökkääjä yritti olla uskottavampi uhrin silmissä. Hyökkääjä vaati uhrilta 200 dollarin lahjakorttia iTunesiin, jotta hyökkääjä avaisi älytelevision näytön uudestaan. [8]

3.4 Älytelevision tiedon keräys ja hyötykäyttö

Tiedon kerääminen älytelevisioista ei näyttäisi olevan mikään vaikea asia. Monet älytelevisiovalmistajat niin sanotusti turvaavat selustansa sillä, että käyttäjän pitää uutta televisiota hankkiessa tai päivitystä tehdessään hyväksyä palvelun ja laitteen käyttöehdot. Noissa käyttöehdoissa sitten mainitaan pienellä tekstillä, että älytelevision kautta saatetaan lähettää tietoa joko älytelevisiovalmistajan omaan tai jonkun kolmannen tahon käyttöön [41]. Yhdysvaltalainen älytelevisiovalmistaja Vizio kuitenkin joutui maksamaan miljoonien sakot, koska he olivat piilottaneet informaation tiedon keräämisestä liian vaikeaselkoisten valikoiden taakse [15].

Mihin kerättyä tietoa voi sitten käyttää? Mainostajat ovat varmasti erittäin kiinnostuneita siitä, että millä kanavavilla ja mitä ohjelmaa eri käyttäjät katsovat. Myös katselun ajankohta on erittäin tärkeä tieto suunniteltaessa esimerkiksi televisiomainontaa [51]. Kaikenlainen täsmämainonta onnistuu sitä paremmin, mitä enemmän on tietoa palvelun käyttäjistä saatavilla. Tämän tiedon mainostajille pystyy tarjoamaan älytelevisiovalmistaja itse ja kenties saamaan siitä jonkinlaisen korvauksenkin. [46]

Osa LG:n älytelevisioista lähettää koko ajan tietoa käyttäjän tekemistä valinnoista salaamattomana eteenpäin. Tietoa esimerkiksi käyttäjän katsomista kanavista, kanavien ohjelmatiedoista sekä katseluajoista siirtyy älytelevisiovalmistajan omille palvelimille [46]. Syyskuussa 2019 Washington Postin kolumnisti Geoffrey Fowler sai selville, että ainakin Samsung on älytelevisioissaan käyttänyt toimintoa nimeltä ACR (Automatic Content Recognition). Kyseinen toiminto kerää joka sekunti käyttäjän älytelevision näytöltä pikseleitä eli kuvapisteitä, joita se sitten lähettää valmistajan palvelimille. Kuvapisteitä verrataan tiedossa oleviin sisältöihin ja tällä tavalla saadaan selville käyttäjän katsoma sisältö [52]. Näistä tapahtumista voidaan käyttää termiä tietovuoto.

Ohjelmayhtiöt hyötyvät myös itse tiedoista esimerkiksi HbbTV-palvelun kautta. He pystyvät suoraan mainostamaan älytelevisioiden käyttäjille omia maksullisia lisäpalveluitaan ja näin maksimoimaan oman katteensa. Tällä tavoin toimimalla ohjelmayhtiöt pystyvät jättämään myyjänä toimivan paikallisen operaattorin kokonaan välistä pois. Myös lisätiedot ohjelmista ja tulevista uusista palveluista pystytään nopeasti välittämään älytelevisioiden käyttäjille.

Älytelevisiovalmistajat voivat käyttää tietoja tuotteensa kehittelyyn ja parantamiseen. Käyttäjien tekemät valinnat eri toiminnoissa antavat arvokasta tietoa siitä,

kuinka hyvin tuote oikeasti toimii. Älytelevisiovalmistajat pystyvät haravoimaan mahdolliset ongelmakohdat pelkästään käyttäjien tiedoista ja puuttumaan niihin nopealla aikataululla. Käyttäjien tietoja voidaan käyttää hyväksi myös tieteellisessä tutkimuksessa. Tiedoista saadaan selville suosituimmat ohjelmat, kanavat ja sovellukset sekä pystytään tekemään vertailuja katseluajoittain ja jopa maittain.

3.5 Älytelevision tietoturvan parantaminen

Kuten aikaisemmin jo mainittiin, niin älytelevisioissa ei yleensä ole lainkaan palomuuri- tai tietoturvaohjelmistoa [13]. Älytelevisioiden tietoturvaa parannetaan valmistajien toimesta koko ajan päivittämällä älytelevisioita sekä niiden ohjelmistoja. Älytelevision käyttäjä pystyy kuitenkin jo nyt parantamaan tietoturvaa sekä suojelemaan yksityisyyttään tekemällä oikeita valintoja esimerkiksi kotiverkon suhteen.

Turvallisin ja yksinkertaisesti paras keino on tietysti kytkeä älytelevisio kokonaan irti internetistä, mutta silloin koko älytelevision idea sekä toimivuus katoavat. Jos kuitenkin haluaa pitää älytelevision kiinni internetissä, niin silloin on hyvä käyttää langallista yhteyttä älytelevision sekä reitittimen välillä. Jos päätyy käyttämään langatonta yhteyttä, niin silloin on ehdottomasti suojattava yhteys hyvin [7]. Langattoman yhteyden turvallisuus varmistetaan vaihtamalla oletuksena olevat reitittimen käyttäjätunnus sekä salasana omiin uusiin tunnuksiin. Käyttäjän kannattaa myös huolehtia siitä, että uudet omat tunnukset ovat tarpeeksi vahvoja eli pitkiä ja monimutkaisia. Reitittimiin on saatavilla myös päivityksiä, joten reititin on hyvä pitää päivitettynä ja ajan tasalla. Toinen hyvä keino on luoda älytelevisiolle kokonaan oma verkko reitittimeen, jota mikään muu kotiverkon laite ei käytä. On myös mahdollista piilottaa tai vaihtaa verkon nimi, mutta nämä teot eivät estä kuitenkaan mahdollisia hyökkäyksiä, korkeintaan hieman hidastavat. Kolmas keino turvalliseen langattomaan viestintään on käyttää VPN-palvelua, jos se vain suinkin on mahdollista.

Älytelevisioihin tulee erilaisia päivityksiä aika ajoin ja älytelevisio onkin hyvä pitää päivitettynä. Jos käyttäjällä on mahdollisuus konfiguroida älytelevisiota, niin se kannattaa tehdä. Asennuksen tai uudelleen asennuksen yhteydessä kannattaa käyttäjän hyväksyä vain ne käyttöehdot, jotka on valmiina hyväksymään sekä joiden sisällön ymmärtää. Jos käyttöehdoissa mainitaan tiedon siirtämisestä jollekin kolmannelle osapuolelle, niin tällaista käyttöehtoa ei kannata hyväksyä missään nimessä, jollei se ole aivan pakollista.

Sellaiset sovellukset tai älytelevisioon liittyvät laitteet, joita ei käytä juuri sillä hetkellä, kannattaa kytkeä pois päältä. Sisäänrakennetut kamerat ja mikrofonit voi aivan hyvin vaikka peittää, koska yleisimmässä malleissa niitä ei kuitenkaan saa kokonaan pois päältä lainkaan. Nykyään löytyy jo älytelevisioille suunniteltuja tietoturvasovelluksia, kuten Android TV:lle saatavilla oleva maksullinen ESET Smart TV Security -sovellus.

Erilaisten sovellusten ja pelien lataamisessa sekä käyttöönotossa kannattaa olla varovainen ja käyttää vain yleisesti hyväksyttyjä kauppapaikkoja. Kannattaa myös hieman ottaa asioista selvää etukäteen, tarkistaa kyseisen sovelluksen latausmääriä ja lukea arvosteluja. Näistä asioista saa jo aika hyvän käsityksen siitä, että onko kyseinen sovellus validi vai ei. Erilaisten suoratoistovideoiden kanssa pitää olla myös tarkkana mahdollisten videoon sisään laitettujen haittaohjelmien takia. [12]

4 Muut tutkimukset

Tutkimuksia älytelevisioiden tietoturvallisuuden heikkouksista tai yksityisyyden suojan loukkaamisista löytyy yllättävän vähän. Paljon löytyy erilaisia artikkeleita, nettikirjoituksia tai blogeja, joissa on löydetty puutteita älytelevisioiden yksityisyyden suojasta tai tietoturvallisuudesta. Monet kotihakkerit kertovat innokkaasti omista löydöistään, mutta hirveän montaa niin sanottua virallista tutkimusta ei löydy. Seuraavissa luvuissa tarkastelemme neljää erilaista tutkimusta sekä niiden tuloksia.

4.1 Tutkimusasetelma Twenten yliopiston tutkimuksessa

Älytelevisioiden tietovuotoa on testattu muun muassa Twenten yliopistolla [46]. Testeissä analysoitiin älytelevisioista lähtevää sekä tulevaa tietoliikennettä. Tärkeimpänä kohteena oli etsiä salaamatonta tietoa katsotuista ohjelmista ja kanavista. Testit tehtiin kahdessa erilaisessa ympäristössä; monella älytelevisiolla yliopistoalueen omassa verkossa sekä yhdellä älytelevisiolla suljetussa verkossa. Testit tehtiin Samsungin ja Philipsin älytelevisioilla.

Yliopistoalueen oman verkon testissä käytettiin mittausvälineenä laitetta, joka pystyi lukemaan tietoliikennettä alueen verkosta. Laite oli määritelty niin, että se tallensi tietoa vain parhaaseen katseluaikaan, jotta saataisiin mahdollisimman paljon tietoa analysoitavaksi. Tallennetusta tiedosta etsittiin lähinnä HbbTV-palvelun liikennettä, koska sitä on kohtuullisen helppo analysoida myöhemmin.

Suljetun ympäristön testi taas suoritettiin yhdistämällä älytelevisio tietokoneeseen ja tietokone internetiin kuvassa 4.1 esitetyllä tavalla. Älytelevision tietoliikennettä analysoitiin Wireshark nimisellä verkon liikennettä analysoivalla ohjelmalla. Tarkoitus oli etsiä ja analysoida HbbTV-palvelun liikennettä tiettyinä kellonaikoina.

Yliopistoalueen oman verkon testi suoritettiin niin, että tietoliikennettä mittaavan laitteen tuloksia analysoitiin eri avainsanojen avulla. Yksi haetuista avainsanoista oli ”hbbtv” ja sen avulla saatiin myös tuloksia aikaan. Esimerkiksi Philipsin älytelevisio lähetti HTML GET -kutsuja kolmannelle osapuolella ja tuo kolmas osapuoli paljastui testissä Philipsin elektronisen ohjelmaoppaan tuottajaksi. Tämä kyseinen toiminta oli sinänsä ihan harmitonta, koska HTML GET -kutsun kohteena oli

Kuva 4.1: Suljetun ympäristön testi suoritettiin yhdistämällä älytelevisio tietokoneeseen ja tietokone internetiin.

vain yksittäinen kuva. Asia on kuitenkin hyvä ottaa huomioon, koska tuon viestin sisältö lähetettiin yleisen verkon kautta ja täysin ilman minkäänlaista salausta. Jos sisältönä olisikin ollut älytelevision käyttäjän tallentamat ohjelmat tai eniten katsotut kanavat, niin silloin puhuttaisiin jo selvästä tietovuodosta.

Toinen tapa analysoida verkon tietoliikennettä oli etsiä älytelevisiovalmistajien kotisivujen osoitteita hakusanoilla kuten ”samsung.com” sekä ”philips.com”. Kyseiset osoitteet löytyivät analysoidusta tiedosta, mutta ne eivät olleet missään yhteydessä älytelevisioihin.

Paras keino analysoida tietoliikennettä isossa verkossa on tehdä analysointia eri avainsanojen avulla. Joillain tavalla käyttäjien toimintaan liittyvät avainsanat ovat erittäin toimivia. Esimerkiksi avainsanat kuten ”channelname, updateviewingstats” ja jo aikaisemmin mainittu ”hbbtv” ovat osoittautuneet hyviksi avainsanoiksi. MAC-osoitteiden perusteella voi myös analysoida liikennettä, mutta silloin pitäisi osata ottaa huomioon kaikki mahdolliset MAC-osoitteet.

Suljetun verkon testissä oli kaksi eri älytelevisiovalmistajan tekemää televisiota. Samsung ei kuitenkaan lähettänyt valitettavasti minkäänlaista HbbTV-palveluun liittyvää tietoa, joten testi keskittyi ainoastaan Philipsin laitteeseen. Kun Philipsin älytelevisio laitettiin päälle, niin laite tarkasti aluksi, että löytyykö laitteeseen uutta ohjelmistopäivitystä. Tämän viestin mukana lähetettiin tieto nykyisestä ohjelmistoversiosta sekä älytelevision sarjanumero. Tämän jälkeen useat eri älytelevisiosovel-

lukset alkoivat keskustelemaan omien palvelimiensa kanssa. Testissä paljastui myös se asia, että Philipsin tietoja keräävän palvelimen ohjelmistona oli jo vanhentunut ja haavoittuva ohjelmisto.

4.2 Berliinin teknisen instituutin tutkimus älytelevision kaappaamisesta

Benjamin Michélen ja Andrew Karpowin Berliinin tekniselle instituutille tekemässä tutkimuksessa [32] esitellään, kuinka älytelevision voi kaapata käyttämällä hyväksi haitalliseksi tehtyä videotiedostoa. Kaappaaja saa älytelevision täysin haltuunsa käyttämällä älytelevision mediasoitinta hyväksi ja kaappaus tapahtuu vielä niin, että käyttäjä ei sitä huomaa millään tavalla. Tutkimuksen loppupuolella esitellään vielä, kuinka älytelevision mikrofonia sekä kameraa voidaan salakuunnella. Testaus ja tutkimus suoritettiin kahdella eri Samsungin älytelevisiolla. Taulukosta 4.1 löytyvät molempien älytelevisioiden tekniset tiedot.

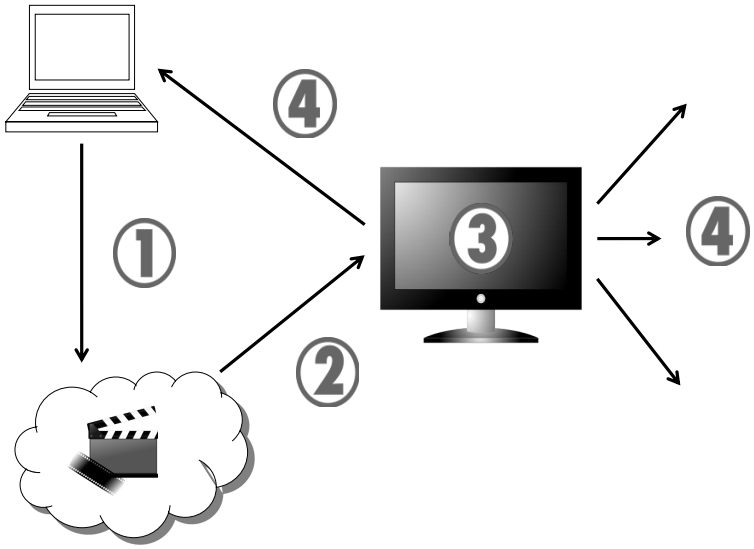
Taulukko 4.1: Tutkimuksessa käytettyjen älytelevisioiden tekniset tiedot.

Merkki:	Samsung	-	**Merkki:**	Samsung
Malli:	LE40B650	-	**Malli:**	UE40ES7000
Vuosi:	2009	-	**Vuosi:**	2012
Ohjelmisto:	T-CHLCIPDEUC-002007	-	**Ohjelmisto:**	T-ECPDEUC-1021.1
Suoritin:	600MHz ARMv6	-	**Suoritin:**	1GHz ARMv7 Cortex-A9
RAM:	292	-	**RAM:**	584
Muisti:	1GB flash	-	**Muisti:**	2GB flash
Järjestelmä:	Linux 2.6.18	-	**Järjestelmä:**	Linux 2.6.35
FFmpeg:	2008	-	**FFmpeg:**	2011-03
libavformat:	v 52.23.1	-	**libavformat:**	v 52.104.0

Melkein kaikissa markkinoilla olevissa älytelevisioissa on sisäänrakennettu mediasoitin. Näissä mediasoittimissa on yleensä erilaisia haavoittuvuuksia. Samsung käyttää median hallinnointiin avoimeen lähdekoodiin perustuvaa ohjelmistokokoelmaa nimeltä FFmpeg. Tässä tutkimuksessa juuri tuon FFmpegin haavoittuvuuksia käytetään kaappauksessa hyväksi.

Tutkimuksessa tehdyn älytelevision kaappauksen ensimmäisessä vaiheessa hyökkääjä lataa käyttäjää kiinnostavan, mutta haitalliseksi muutetun videon ensin internetiin tai vaihtoehtoisesti siirtää sen suoraan käyttäjän älytelevisioon vaikkapa USB-

liittymän kautta. Toisessa vaiheessa käyttäjä lataa haitallisen videon omaan älytelevisioonsa. Hyökkääjä pääsee tunkeutumaan älytelevisioon ja sen järjestelmään hyökkäyksen kolmannessa vaiheessa, kun älytelevision käyttäjä käynnistää haitallisen videon. Neljännessä vaiheessa hyökkääjä on kaapannut älytelevision haltuunsa ja sitä kautta pystyy hyökkäämään myös muihin laitteisiin samassa verkossa tai hankkimaan tietoja mikrofonin tai kameran kautta. Kuvassa 4.2 on kuvaus kaappauksen etenemisestä.



Kuva 4.2: Älytelevision kaappaus haitallista videotiedostoa hyväksikäyttäen.

Ennen kaappausta hyökkääjän pitää saada selville älytelevision käyttämän FFmpegin käyttöversio. Tämän jälkeen hyökkääjään pitää etsiä haavoittuvuuksia liittyen kyseiseen FFmpegin käyttöversioon. Haavoittuvuuksia voi etsiä internetistä erilaisilta vikafoorumeilta. Seuraavaksi pitää liittää itse haittaohjelma videoon ja tärkeintä on se, että se näyttää ja kuulostaa oikealta videolta. Kun video laitetaan pyörimään, niin haittaohjelma pääsee sisään järjestelmään huomaamattomasti. Pääprosessi nimeltään exeDSP toimii älytelevision järjestelmässä täysillä käyttöoikeuksilla (root). Koska FFmpeg on ladattu samaan prosessitilaan kuin exeDSP, niin sillä on myös täydet käyttöoikeudet. Tuloksena on se, että haittaohjelma pystyy täysillä käyttöoikeuksilla hallitsemaan tämän jälkeen koko järjestelmää.

Kun hyökkääjä on saanut kaapattua älytelevision hallintaansa, niin hyökkääjällä on mahdollisuus aiheuttaa paljon harmia älytelevision käyttäjälle. Hyökkääjä pystyy pienillä lisäyksillä ottamaan haltuunsa videopuheluita varten älytelevisioon lii-

tetyn kameran sekä älytelevisiossa olevat mikrofonit. Hyökkääjä pystyy halutessaan pitämään älytelevision koko ajan päällä, vaikka se näyttäisi käyttäjälle päin olevankin sammutettu. Hyökkääjä pystyy myös halutessaan hallitsemaan muita samassa verkossa olevia laitteita.

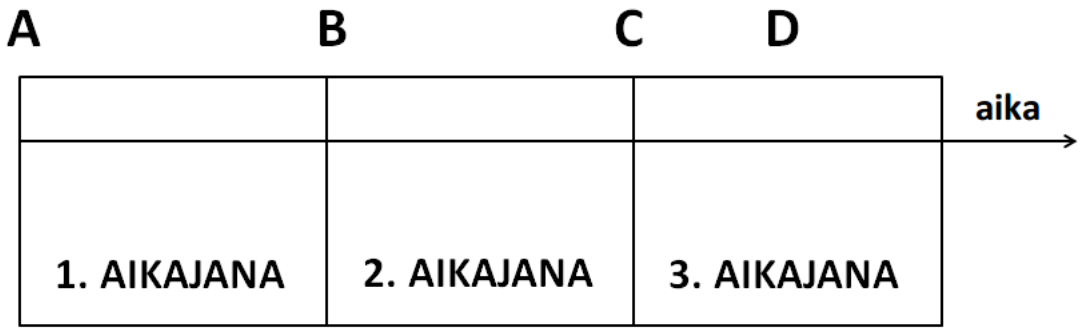
4.3 Darmstadin teknisen yliopiston tutkimus HbbTV-palvelun tietovuodoista

HbbTV on palvelu, jonka ideana on tuottaa selainpohjaisia palveluita älytelevisioon. HbbTV-palvelu vaatii toimiakseen internet-yhteyden, HbbTV-palvelua tukevan älytelevision sekä HbbTV-palvelua tarjoavan televisiokanavan. HbbTV-palvelu on räätälöity jokaiselle televisiokanavalle erikseen ja siitä vastaa ohjelmayhtiö. Älytelevisio saa viestin mahdollisesta HbbTV-palvelusta televisiosignaalin mukana tulevasta viestistä (URL-osoite), jonka ohjelmayhtiö laittaa signaaliin mukaan. HbbTV-palvelu aktivoidaan painamalla älytelevision kaukosäätimen punaista nappia.

Darmstadin teknillisessä yliopistossa tehty tutkimus [21] HbbTV-palvelun tietovuodoista on Marco Ghiglierin ja Erik Tewsin käsialaa. Tutkimuksessa tuodaan esille, kuinka helppoa kolmannen tahon on saada tietoja älytelevision käytöstä HbbTV-palvelun kautta. Tutkimuksessa käytetään kahta erilaista Samsungin valmistamaa älytelevisiota ja HbbTV-palvelun tarkasteluun käytetään saksalaisia sekä itävaltalaisia televisiokanavia.

HbbTV-palvelun liikennettä tarkastellaan tutkimuksessa signaaleista, jotka tulevat satelliitin, ilmateiden (terrestial) tai kaapelin kautta. Näiden kolmen eri signaalin välillä ei havaittu juuri mitään eroja. Jotta tutkimuksessa saataisiin eroja liikkuvien tietopakettien välillä, niin pakettien liikkuminen jaetaan kolmeen eri ajalliseen vaiheeseen.

- 1. AIKAJANA
  - Aikajana alkaa, kun älytelevisioon laitetaan HbbTV-palvelun sisältävä televisiokanava päälle (A).
  - Aikajana loppuu, kun HbbTV-palvelun viesti näkyy (B).
- 2. AIKAJANA
  - Aikajana alkaa, kun HbbTV-palvelun viesti näkyy (B).
  - Aikajana loppuu, kun käyttäjä painaa kaukosäätimen punaista nappia aktivoidakseen HbbTV-palvelun (C).
- 3. AIKAJANA
  - Aikajana alkaa, kun Käyttäjä painaa kaukosäätimen punaista nappia aktivoidakseen HbbTV-palvelun (C).
  - Aikajana loppuu, kun HbbTV-palvelu käynnistyy (D).



Kuva 4.3: Tutkimuksen aikajanat.

Tässä tutkimuksessa keskitytään lähinnä ensimmäiseen ja toiseen aikajanaan, missä käyttäjä ei ole tarkoituksella käynnistänyt HbbTV-palvelua eli painanut kaukosäätimen punaista nappia. Eri televisiokanavat (ohjelmayhtiöt) käyttävät kahta erilaista pyyntötyyppiä, aloituspyyntöä sekä jaksottaista pyyntöä. Alla on selitetty pyynnöt sekä niiden erot.

- Aloituspyynnöt (Start-up)
  Kun älytelevisiosta valitaan kanava, joka käyttää HbbTV-palvelua, niin viesti

HbbTV-palvelusta tulee näkyville (paina punaista nappia aktivoidaksesi HbbTV-palvelun). Jos viestiä ei tule, niin silloin HbbTV-palvelu ei ole käytössä.

- Jaksottaiset pyynnöt (Periodic)
  HbbTV-palvelun aktivoinnista ilmoittavan viestin sekä punaisen napin painalluksen väliset pyynnöt. Eri televisiokanavilla pyyntöjen väliset aikaerot ovat yhdestä sekunnista jopa 15:een minuuttiin.

Nämä molemmat pyyntötyypit tapahtuvat ennen kuin HbbTV-palvelu edes aktivoidaan ja voisi hyvin olettaa, että mitään tietoliikennettä ei tapahtuisi ennen aktivointia, mutta näin ei siis kuitenkaan ole. Tästä tulee hyvin myös esille se, että HbbTV-palvelun sisältö on hyvin erilainen eri televisiokanavilla.

Ensimmäisen aikajanan sisällä tapahtuu aloituspyynnöt. Niissä ohjelmayhtiö välittää viestin HbbTV-palvelun löytymisestä kyseisellä televisiokanavalla. Tämän jälkeen älytelevisio lataa mahdollisen logon sekä tekstit ohjelmayhtiön palvelimelta. Toisen aikajanan aikana tapahtuu jaksottaiset pyynnöt. Nämä pyynnöt sisältävät jo huomattavasti enemmän informaatiota. Jaksottaisilla pyynnöillä esiladataan sisältöä tai seurataan älytelevision käyttäjän liikkeitä hyvinkin tarkasti. Kyseisen televisiokanavan omistama ohjelmayhtiö pystyy tarkistamaan, että onko älytelevision käyttäjä vielä kyseisellä televisiokanavalla. Tutkimuksessa havaittiin tietoliikenteessä seuraavia tahoja; Google Analytics, Chartbeat.com ja Webtrekk. Kaikki nämä kolme edellä mainittua tahoa keräävät, analysoivat ja myyvät kaikenlaista keräämäänsä tietoa. Tässä tapauksessa kerätty tietoa voi olla esimerkiksi televisiokanavalla vietetty aika tai mitä televisiokanavia älytelevision käyttäjä on katsonut tietyllä aikavälillä.

Mitä sitten voidaan tehdä, jotta tällaisia tietovuotoja ja yksityisyyden loukkauksia ei pääsisi tapahtumaan? Yksi tapa on kirjata selkeästi HbbTV-standardiin ne ehdot, joiden mukaan HbbTV-palveluita saa tuoda markkinoille. Luodaan niin sanottu uusi normi, jossa otetaan huomioon myös käyttäjän yksityisyyden suoja nykyistä paremmin. Voidaan vaatia, että mitään tietoliikennettä ei tapahdu, ennen kuin käyttäjä on painanut punaista nappia. Toinen tapa on antaa käyttäjälle mahdollisuus päättää, mikä televisiokanava voi käyttää HbbTV-palvelua ja mikä taas ei. Tällä tavalla käyttäjä saa itse päättää, haluaako käyttää kyseisen ohjelmayhtiön lisäpalveluja HbbTV-palvelun muodossa.

4.4 Tutkimus älytelevision sovellusten tietovuodoista

Ruhrin yliopistossa tehdyssä tutkimuksessa [34] tutkittiin älytelevision sovellusten tietovuotoja sekä tietoturvaan liittyviä puutteita. Monet tunnetut sovellukset, mukaan lukien Facebook sekä Ebay, lähettävät käyttäjän tietoja eteenpäin salaamattomana. Mahdollisia hyökkäysmetodeja on monia erilaisia. Yksi metodi on se, että hyökkääjä itse tekee ja asentaa sovelluksen älytelevisioon usb-portin kautta ja pystyy sitä kautta tunkeutumaan älytelevisioon luotuun tiliin ja käyttämään kaikkia käyttäjän kyseiseen tiliin liittämiä laitteita. Samsung Tizen-käyttöjärjestelmään sovelluksia voi tehdä Tizen Studio - tai Visual Studio -ohjelmien avulla. Toinen metodi on käyttää hyväksi TLS-suojauksen (Transport Layer Security) puuttumista sovelluksesta siinä vaiheessa, kun sovellukseen kirjaudutaan sisään. TLS-suojauksella suojataan internet-sovellusten tietoliikennettä IP-verkkojen yli. Näitä samoja sovelluksiin kohdistuvia hyökkäysmetodeja voi käyttää muihinkin sovelluksia sisältäviin laitteisiin, kuten autoihin sekä älykelloihin.

Testaus ja tutkimus suoritettiin kahdella eri älytelevisiolla sekä kolmella eri televisioon liitettävällä mediatoistimella. Samsungin älytelevisio valittiin markkinajohtajuuden takia ja Grundigin älytelevisio valittiin taas siitä syystä, että se ei ole viiden myydyimmän älytelevision joukossa. Mediatoistimet Apple TV, Google Chromecast sekä Amazon Fire valittiin sen takia, että ne ovat markkinoiden suosituimmat tuotteet omassa kategoriassaan. Taulukosta 4.2 löytyvät laitteiden tarkemmat tiedot.

Taulukko 4.2: Tutkimuksessa käytettyjen laitteiden tarkemmat tiedot.

VALMISTAJA	**LAITE**	**VERSIO**
Samsung	UE22H5670	2606
Grundig	42VLE922BL	J5GRMR
Apple	TV	7.0.3
Google	Chromecast	27946
Amazon	Fire TV	53.1.1.0

Testauksen aikana käytettiin kolmea eri hyökkäystapaa. Hyökkäystavat on nimetty tutkimuksessa nimillä A, B ja C. Hyökkäystapa A tehtiin molemmille älytelevisioille ja hyökkäystavat B ja C vain Samsungin älytelevisiolle. Hyökkäystavat on esitelty alla olevassa taulukossa 4.3.

Salakuuntelemista hyökkäystapana käytettiin kaikissa tutkimuksessa mukana olevissa laitteissa. Ensin selvitettiin, että kuinka monessa sovelluksessa käytetään

Taulukko 4.3: Tutkimuksessa käytetyt hyökkäystavat.

NIMI	HYÖKKÄYSTAPA
A	Salakuuntelemalla analysoidaan HTTP-liikennettä. Tässä tutkimuksessa laitteet oli liitetty salaamattomaan langattomaan verkkoon.
B	Älytelevisioon liitetyn laitteen (esimerkiksi USB-muisti) kautta asennettu haittaohjelma.
C	Sovelluskaupan tai sähköpostin kautta asennettu haittaohjelma.

jonkinlaista kirjautumista tai tunnistautumista, kuten taulukosta 4.4 tulee esille. Tätä tutkittiin analysoimalla sovelluksen HTTP-liikennettä. Tämän jälkeen selvitettiin, että tallennetaanko tunnistetiedot salattuna vai salaamattomana. Jos hyökkääjä salakuuntelee käyttäjän HTTP-liikennettä samaan aikaan kuin käyttäjä kirjautuu sellaiseen sovellukseen, joka ei salaa tunnistetietoja lainkaan, niin silloin hyökkääjän on mahdollista saada käyttäjän tunnistetiedot itselleen.

Taulukko 4.4: Salakuuntelulla löydettyjen salaamattomana tunnistetietoja tallentavien sovellusten määrät laitteittain.

VALMISTAJA	Sovellukset	Tunnistetiedot	Salaamaton
Samsung	56	16	4
Grundig	34	7	3
Apple	28	17	1
Google	10	-	0
Amazon	20	4	0

Samsungin älytelevisiolla testattiin valmiiksi esiasennettuja sekä käyttäjän itse älytelevisioon asentamia sovelluksia. Näistä sovelluksista neljä ei salannut tunnistetietoja millään tavalla. Yksi näistä on median toistoon tarkoitettu sovellus nimeltä Watchever ja sen versio 2.200. Grundigin älytelevisioon käyttäjä taas ei voi itse asentaa sovelluksia lainkaan. Seitsemän Grundigissa testattua sovellusta käyttää tunnistetietoja, joista kolme sovellusta ei salaa tunnistetietoja lainkaan. Suoratoistoon tehty sovellus nimeltä Viewster on yksi niistä.

Tutkimuksen salakuuntelu-hyökkäystavassa tarkastellaan lähemmin Samsungin älytelevisiosta löytyvää musiikkivideoiden katsomiseen tarkoitettua sovellusta ni-

meltä Vevo ja sen versiota 3.701. Salakuuntelemalla kyseisen sovelluksen HTTP-liikennettä löytyi sovelluksesta kaksi tietoturvaan liittyvää puutetta. Ensinnäkin sovellus lähettää tietoja käyttäjän tekemistä valinnoista kolmannelle osapuolelle, tässä tapauksessa netin käyttöä tutkivalle yritykselle nimeltä ScorecardResearch. Toiseksi kyseinen sovellus ei salaa tunnistetietoja millään tavalla, vaan ne on poimittavissa tietoliikenteestä selkokielisenä. Kyseiseen sovellukseen kirjaudutaan käyttäjän Samsung tilin avulla. Jos hyökkääjä (salakuuntelija tai mainittu kolmas osapuoli) saa käyttäjän Samsungin tunnistetiedot käyttöönsä, niin silloin hyökkääjällä on mahdollisuus ohjata kaikkia käyttäjän Samsung tiliin liitettyjä sovelluksia tai laitteita.

Älytelevisioon liitetyn laitteen, sovelluskaupasta ladatun tai sähköpostin mukana tulleen haittaohjelman kautta pystyy hyökkääjä myös saamaan selville tunnistetietoja. Käyttäjän pitää kuitenkin yleensä näissä tapauksissa itse tehdä jotain käynnistääkseen haittaohjelman; käynnistää haittaohjelma USB-muistista, ladata haittaohjelma sovelluskaupasta tai klikata latauslinkkiä sähköpostiviestissä. Tunnistetietojen kalastelu haittaohjelman avulla eroaa salakuuntelusta juurikin hyökkäysmetodin kautta.

Yksi tapa hyökätä haittaohjelman avulla älytelevisioon on tehdä haittaohjelmaan sellainen toiminto, että hyökkääjää pääsee käsiksi Samsungin älytelevisiossa kohtaan Document Object Model (DOM) esimerkiksi JavaScriptiä hyväksi käyttäen. Jos käyttäjä on kirjautunut älytelevisioon sekä samalla käynnistää haittaohjelman, niin hyökkääjällä on DOM:in kautta mahdollista saada selville muun muassa käyttäjän tunnistetiedot, television mallin sekä maakoodin.

Toinen tapa päästä kiinni älytelevision tietoihin on murtautua sen tiedostojärjestelmään. Koska kyseinen resurssienhallintaan tarkoitettu sovellus puuttuu, niin sellainen täytyy rakentaa itse. Älytelevision juurihakemistoon (root) pääsee suoraan käyttämällä sovelluksessa file-protokollaa kolmella vinoviivalla (file:///) http-protokollan sijaan. Kun juurihakemistoon on pääsy, niin tiedot voidaan lähettää hyökkääjän omalla palvelimelle käyttäen hyväksi XHR (XMLHttpRequest) ohjelmointirajapintaa. Resurssienhallintaan tarkoitetulla sovelluksella on hyökkääjällä mahdollisuus päästä kiinni seuraaviin tietoihin:

- Langattomaan verkkoon ja sen tietoihin (käyttäjätunnus ja salasana)
- Selaimen evästeisiin
- Selaimen historiatietoihin

- Samsung tilin tietoihin

Analysoimalla tiedostoa nimeltä UDBCOMMON, löytyi todella kriittinen turvallisuusriski. Kyseiseen tiedostoon tallentuu usein syötettyjä käyttäjätunnuksia sekä salasanoja. Käyttäjätietoja hyväksi käyttäen on mahdollista esimerkiksi kirjautua sisään käyttäjän Facebook-tilille.

5 Tutkimus kahden älytelevision mahdollisista tietovuodoista

Tässä tutkimuksessa tutkitaan kahden eri aikakaudelta olevan saman valmistajan älytelevision mahdollisia tietovuotoja, yksityisyyden loukkauksia tai selkeitä tietoturvauhkia. Tutkimuksessa käytettävät älytelevisiot ovat omiani, päivittäisessä käytössä olevia älytelevisioita. Tällä tavoin tutkimuksista sekä niiden tuloksista saa mahdollisimman autenttisen kuvan.

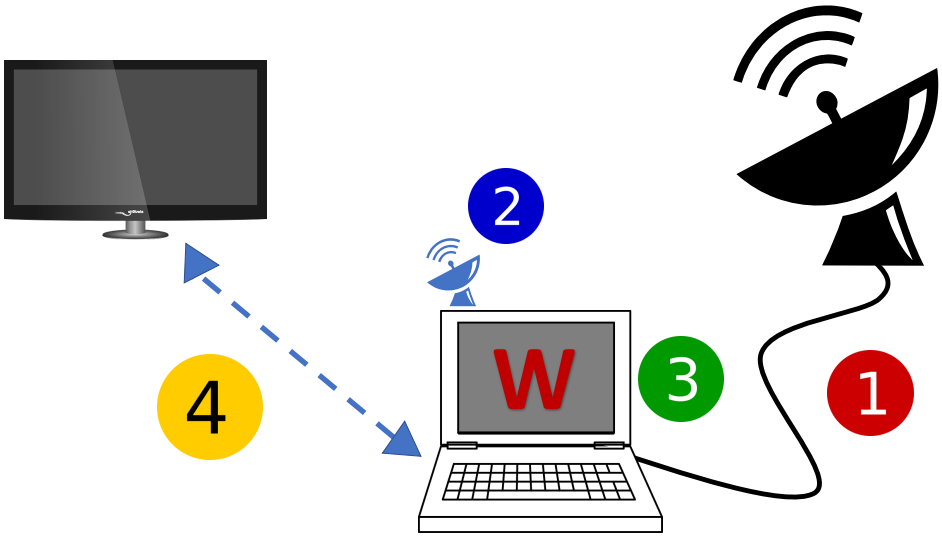
Tutkimus suoritetaan analysoimalla älytelevision sekä internetin välillä liikkuvaa dataa normaalissa käytössä. Wireshark-ohjelmalla kerätään ja tallennetaan dataa samalla, kun älytelevisiolla suoritetaan tutkimuksen kannalta mielenkiintoisia toimintoja [9, s. 20]. Tällaisia toimintoja ovat esimerkiksi älytelevision liittäminen internetiin sekä erilaisten sovelluksien käynnistäminen ja niiden sisällön katseleminen. Kun tietoliikennedataa on saatu kerättyä tarpeeksi, se analysoidaan. Analysointia tehdään hakemalla tiettyjä avainsanoja tai toimintoja (kuten "HTTP") ja avaamalla näiden toimintojen tietoja tarkemmin.

Ensimmäisessä alaluvussa esitellään tutkimusympäristö ja tutkimuksessa käytetyt laitteet sekä ohjelmat. Toisessa sekä kolmannessa alaluvussa esitellään datan keruu- ja analyysisuunnitelmat. Neljännessä alaluvussa esitellään ensimmäinen älytelevisio ja siihen kohdistuvat tutkimukset sekä viidennessä alaluvussa esitellään toinen älytelevisio ja siihen kohdistuvat tutkimukset.

5.1 Tutkimusympäristö sekä käytetyt laitteet ja ohjelmat

Tutkimusympäristönä on suljettu kotiverkko. Molemmat älytelevisiot testataan ja tutkitaan erikseen, jotta olisi helpompi eritellä ja vertailla tuloksia. Kannettava tietokone toimii MITM:n (man in the middle) tapaan tutkimuksen keskiössä kuvassa 5.1 esitetyllä tavalla. Kannettava tietokone yhdistetään internetiin langallisesti eli ethernet-kaapelin avulla. Älytelevisio on taas kytketty internetiin langattomasti kannettavaan tietokoneeseen perustetun tukiaseman kautta. Tällä tavoin kaikki tietoliikenne älytelevisiosta tai älytelevisioon kulkee kannettavan tietokoneen kautta.

Tutkimus alkaa laitteiden kytkemisellä, yhteyksien tarkistuksella sekä Wireshark-



Kuva 5.1: Tietoliikenteen seurantakaavio

ohjelmiston käynnistyksellä. Alkuasennukset etenevät seuraavasti (tähän viitataan myöhemmin tekstissä termillä alkuasennukset):

1. Kytketään kannettava tietokone ethernet-kaapelilla reitittimeen kiinni ja käynnistetään tietokone.
2. Perustetaan kannettavalle tietokoneelle tukiasema.
3. Avataan Wireshark-ohjelma ja aloitetaan tietoliikenteen seuranta.
4. Avataan älytelevisio, palautetaan sen tehdasasetukset, viritetään kanavat sekä liitetään älytelevisio internetiin kannettavan tietokoneen tukiaseman avulla.

Kannettavana tietokoneena tutkimuksessa on HP EliteBook, jossa on Linux Mint 18.1 Cinnamon käyttöjärjestelmä. Kannettavaan tietokoneeseen perustetun tukiaseman verkkoon ei ole kytketty mitään muita laitteita tutkimuksen aikana, jotta tietoliikennettä olisi helpompi seurata. Komentokehotteen ip-komennolla tarkistetaan kannettavan tietokoneen verkkoasetukset. Nmap (network mapper) porttiskannausohjelmaa käytetään tarkistamaan, että yhteydet toimivat kannettavan tietokoneen sekä älytelevision välillä [29, s. 1]. Kannettavaan tietokoneeseen on asennettu tietoliikenteen analysointiin sekä keräämiseen tarkoitettu ohjelma nimeltä Wireshark ja sitä käytetään hyväksi tässä tutkimuksessa. Taulukosta 5.1 löytyy ohjelmien tarkemmat tiedot.

Taulukko 5.1: Tutkimuksessa käytetyt ohjelmat sekä niiden tiedot

OHJELMA	VERSIO	KEHITTÄJÄ
Nmap	7.01	Gordon Lyon
Wireshark	3.2.7	Gerald Combs

5.2 Datan keruusuunnitelma

Älytelevision sekä internetin välillä liikkuvaa dataa kerätään tässä tutkimuksessa käyttäen hyväksi Wireshark-ohjelmistoa. Kun Wireshark-ohjelma on käynnistynyt, niin valitaan alkuvalikosta oikea verkko, jonka tietoliikennettä aletaan seuraamaan. Tämän jälkeen liitetään älytelevisio internetiin ja älytelevisiolla tehdään erilaisia valintoja ja toimintoja, kuten esimerkiksi vaihdetaan kanavaa, käynnistetään sovelluksia, luetaan käyttöohjeita ja selaillaan valikkoja. Kun dataa on saatu kerättyä tarpeeksi, lopetetaan tietoliikenteen seuraaminen, tallennetaan saatu tulos sekä aloitetaan sen analysointi.

Tietoliikenne tallennetaan sellaisenaan kuin Wireshark-ohjelma sitä huomaa ja esittää. Tietoliikennettä ei suodateta millään lailla seuraamisen aikana, vaan kerätään kaikki mahdollinen tietoliikenne talteen. Kun haluttu tietoliikenteen osa on tallennettu, niin kerättyä dataa aletaan analysoimaan tarkemmin. Sanahaut ovat parhaita keinoja mielenkiintoisen tiedon etsintään [46].

5.3 Datan analyysisuunnitelma

Kun älytelevision sekä internetin välillä liikkunutta dataa on kerätty tarvittava määrä, niin sitä voidaan alkaa analysoimaan. Kun jollain avainsanalla on löydetty mielenkiintoista tietoa tallennetusta datasta, niin aloitetaan kyseisen datan tarkempi tarkastelu ja analysointi. Wireshark-ohjelmasta löytyy valmiina suodatintoiminto, jolla voi suodattaa helposti näkyville vain ne rivit, joissa on esimerkiksi käytetty HTTP-protokollaa. Kun on löydetty mielenkiintoista tietoa, niin sitä aletaan tarkastelemaan sitten tarkemmin. Tarkemman analysoinnin tarkoituksena on löytää vastauksia datan liikehdintään ja sitä kautta löytää myös mahdollisia tietoturvauhkia tai tietovuotoja.

Wiresharkilla kerättyä tietoliikennedataa kertyy valtavia määriä nopealla aikataululla. Jotta dataa pystyisi analysoimaan jollain järkevällä tavalla, niin datan ke-

rääminen on pilkottava pienempiin osiin, kuten esimerkiksi sovelluksen käynnistäminen, sovellukseen kirjautuminen sekä sovelluksessa toimiminen. Avainsanoja on helpointa hakea juuri suodatintoiminnon avulla suoraan Wireshark-ohjelmasta. Toinen käytännöllinen tapa on siirtää kerätty data käyttäjän valitsemaan tiedostomuotoon (esimerkiksi .txt) ja erilaisten hakutoimintojen avulla hakea haluamaansa tietoa tai hakusanaa suoraan tiedostosta. Molemmat tavat ovat erittäin käyttökelpoisia. Taulukossa 5.2 on esitetty tässä tutkimuksessa käytetyt avainsanat, sekä syyt, miksi juuri niitä on käytetty.

Taulukko 5.2: Tutkimuksessa käytettyjä avainsanoja

AVAINSANA	**Syy avainsanan käyttöön**
sony	Tutkimuksessa käytettyjen älytelevisioiden valmistaja.
HTTP	Protokolla, jota esimerkiksi palvelimet käyttävät tiedonsiirtoon [16]. HTTP-protokolla on salaamaton, joten siksi se on altis mahdollisille tietoturvauhkille.
HTTP GET	HTTP-pyynnön GET-metodilla pyydetään lähettämään tietoa, mikä on osoitettu kutsussa.
HTTP HEAD	HTTP-pyynnön HEAD-metodi on kuin GET-metodi, mutta ilman sisältöä.
HTTP POST	HTTP-pyynnön POST-metodi, jolla voidaan lähettää tietoja.
EAPOL	Paketointitekniikka, jolla EAP-viestit eli autentikointiviestit välitetään esimerkiksi älytelevision sekä langattoman verkon tukiaseman / reitittimen välillä [54].
collector	Etsitään mahdollisia tiedon kerääjiä
analytics	Etsitään mahdollisia tiedon kerääjiä
viewing	Etsitään mahdollisia tiedon kerääjiä
cloudfront	Tunnettu sisällön jakelija sekä pilvipalvelu
akamai	Tunnettu sisällön jakelija sekä pilvipalvelu
google	Hakukone
finnpanel	Television katselua mittaava yritys
login	Mahdollinen kirjautuminen

5.4 Sony Bravian tietoliikenteen tutkimus

Tutkimuksen ensimmäinen kohde on maaliskuussa vuonna 2010 valmistettu Sony Bravia KDL-40NX700 (käytän myöhemmin tästä älytelevisiosta nimeä Bravia). Tämä malli kuuluu niin sanottuun ensimmäiseen älytelevisioiden ryhmään. Sony Braviaan on asennettu erilaisia internetin välityksellä toimivia pienoissovelluksia sekä pienoisohjelmia. Pienoissovelluksissa on yleensä takana jonkinlainen videokirjasto, josta sitten käyttäjä voi valita haluamansa videon, jota katsella. Pienoisohjelmien alustana taas toimii jo haudattu Yahoo TV. Taulukossa 5.3 on listattu Sony Braviasta löytyvät pienoissovellukset, pienoisohjelmat sekä laitteen tekniset tiedot. Sony Bravian pystyy liittämään internetiin sekä langallisesti että langattomasti. Sony Bravian viimeinen ohjelmistopäivitys on asennettu 12.1.2015.

Taulukko 5.3: Sony Bravian tekniset tiedot sekä toiminnot.

Merkki	Sony	
Malli	Bravia KDL-40NX700	
Valmistusvuosi	2010	
Ohjelmisto	PKG4.131EUH-0108	
Sarjanumero	9312314	
Pienoissovellukset	Search Internet Video	Tämän toiminnon avulla voi käyttäjä itse etsiä internetistä videoita. Palvelu ei enää vastaa.
	iFood.tv	Erilaisia ruuan valmistusvideoita.
	uStudio	Erilaisia lyhyitä videoita.
	Tagesschau	Palvelu ei enää vastaa.
	DW (Deutsche Welle)	Erilaisia lyhyitä videoita.
Pienoisohjelmat	Yahoo Widget Gallery	Palvelu ei enää vastaa.
	Weather Widget	Palvelu ei enää vastaa.
	Yahoo News	Palvelu ei enää vastaa.
	Yahoo Finance	Näyttää pörssin tietoja.

5.4.1 Bravian käynnistysvaihe

Kun alkuasennukset on tehty, niin tarkistetaan vielä, että yhteydet toimivat älytelevision sekä kannettavan tietokoneen tukiaseman välillä. Avataan komentokehote kannettavan tietokoneen Linux Mint -käyttöjärjestelmässä klikkaamalla kuvaketta ”Pääte” ja kirjoitetaan komento *ip addr show*. Kuten kuvasta 5.2 nähdään, niin kannettavan tietokoneen tukiaseman langattoman liittymän nimi on wlo1 sekä ip-osoite on 10.42.0.1.

```
kimmo@kimmo-HP-EliteBook-2570p ~ $ ip addr show
4: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state
    link/ether 84:3a:4b:5b:f6:7c brd ff:ff:ff:ff:ff:ff
    inet 10.42.0.1/24 brd 10.42.0.255 scope global wlo1
```

Kuva 5.2: Komentokehotteen komento: ip addr show

Seuraavaksi tarkistetaan, että älytelevisio on liitetty kannettavan tietokoneen tukiasemaan. Komentokehotteeseen kirjoitetaan komento *nmap -sn 10.42.0.1/24*. Nmap on porttiskannaukseen tarkoitettu ohjelma, joka käynnistetään kirjoittamalla komento *nmap*. Parametri *-sn* tarkoittaa Ping Scan -toimintoa, jota voisi suomeksi kutsua verkkoyhteyden testaamiseksi tai yhteyskokeiluksi. Komennon loppuun liitettävä *1/24* parametri tarkoittaa sitä, että skannaus suoritetaan koko alueella 10.42.0.1 - 10.42.0.255. Kuvasta 5.3 nähdään, että kannettavan tietokoneen tukiaseman verkkoon on liitetty laite, jonka ip-osoite on 10.42.0.32. Tämän jälkeen tarkistetaan, että sama ip-osoite löytyy myös Bravian asetuksista.

```
kimmo@kimmo-HP-EliteBook-2570p ~ $ nmap -sn 10.42.0.1/24

Starting Nmap 7.01 ( https://nmap.org ) at 2020-11-08 09:00 EET
Nmap scan report for 10.42.0.1
Host is up (0.00037s latency).
Nmap scan report for 10.42.0.32
Host is up (0.038s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.05 seconds
```

Kuva 5.3: Komentokehotteen kehote: nmap -sn 10.42.0.1/24

Kun Braviassa valitaan internetyhteydeksi langaton vaihtoehto, valitaan oikea langaton verkko (kannettavan tietokoneen tukiasema) sekä kirjoitetaan langattoman verkon salasana, niin alkaa dataliikennettä näkyä välittömästi. Autentikoin-

tiviestit (todentamisviestit) välitetään Bravian sekä kannettavan tietokoneen tukiaseman välillä käyttäen EAP-protokollaa ja ne löytyvät datasta avainsanalla *EAPOL*, kuten kuvasta 5.4 voi hyvin havaita. *IntelCor* tarkoittaa kannettavaa tietokonetta ja *MitsumiE* tarkoittaa Braviaa.

Source	Destination	Protocol	Lengtl	Info
IntelCor_5b:f6:7c	MitsumiE_55:fb:af	EAPOL	113	Key (Message 1 of 4)
MitsumiE_55:fb:af	IntelCor_5b:f6:7c	EAPOL	135	Key (Message 2 of 4)
IntelCor_5b:f6:7c	MitsumiE_55:fb:af	EAPOL	169	Key (Message 3 of 4)
MitsumiE_55:fb:af	IntelCor_5b:f6:7c	EAPOL	113	Key (Message 4 of 4)

Kuva 5.4: Autentikointiviestit Bravian sekä kannettavan tietokoneen välillä

Bravia ottaa yhteyden osoitteeseen sony.net internetin kautta käyttämällä HTTP HEAD -metodia, kuten alla olevasta kuvasta 5.5 näkyy. HTTP HEAD -metodin onnistumisesta kertoo vastauksen info-sarakkeessa oleva statuskoodi 200 [16]. Kun kyseistä HTTP HEAD -metodia tarkastelee tarkemmin, niin sen tiedoista löytyy juuri edellä mainittu internetosoite.

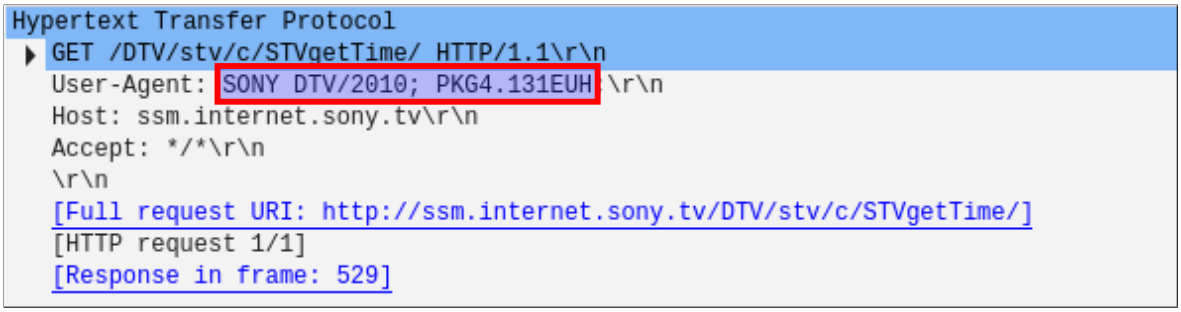
Source	Destination	Protocol	Lengtl	Info
10.42.0.32	23.37.97.210	HTTP	180	HEAD / HTTP/1.1
23.37.97.210	10.42.0.32	HTTP	316	HTTP/1.1 200 OK

Kuva 5.5: HTTP HEAD -metodi

Bravia suorittaa aika ajoin onnistuneesti HTTP GET-metodilla STVgetTime -toiminnon. Kyseisessä kutsussa on aikamääreen lisäksi myös Bravian vuosimalli sekä ohjelmistoversio. Kuvassa 5.6 näkyy STVgetTime -toiminto sekä kuvassa 5.7 on osa sen sisällöstä.

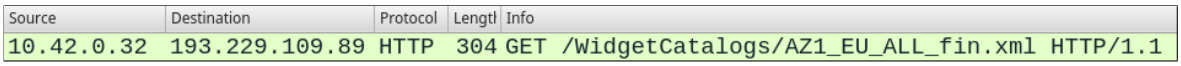
Source	Destination	Protocol	Lengtl	Info
10.42.0.32	52.24.252.10	HTTP	187	GET /DTV/stv/c/STVgetTime/ HTTP/1.1
52.24.252.10	10.42.0.32	HTTP/XML	616	HTTP/1.1 200 OK

Kuva 5.6: HTTP GET -metodi STVgetTime -toiminnossa



Kuva 5.7: HTTP GET -metodin sisältö STVgetTime -toiminnossa

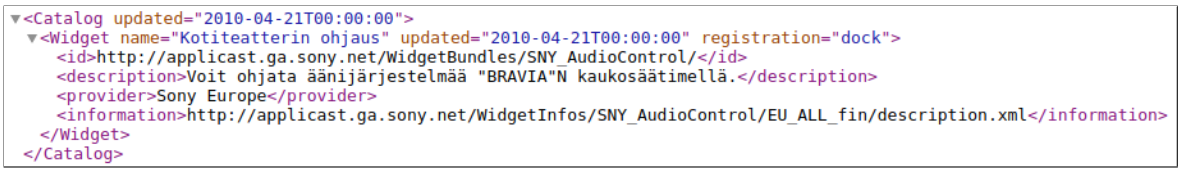
Bravia hakee Kotiteatterin ohjaus -toiminnon tiedot päävalikon Verkko-kohtaan internetin kautta käyttämällä HTTP GET -metodia, kuten alla olevasta kuvasta 5.8 näkyy. Kun kyseistä HTTP GET -metodia tarkastelee tarkemmin, niin sen tiedoista löytyy internetosoite, jonka voi nähdä kuvan 5.9 viimeisellä rivillä. HTTP GET -metodin tarkemmista tiedoista löytyy myös Bravian mallinumero, asiakastunniste, maakoodi sekä Bravian asennuksessa valittu kielikoodi.



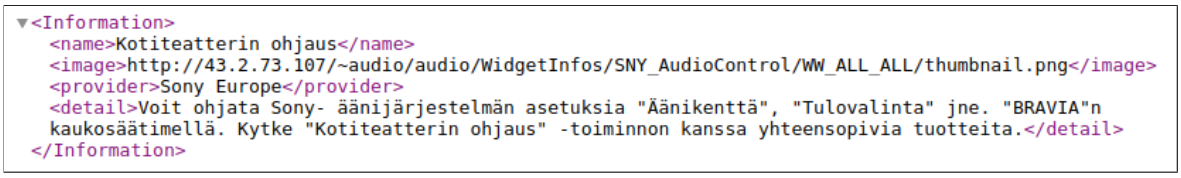
Kuva 5.8: HTTP GET -metodi Kotiteatterin ohjaus -toiminnossa

Kuva 5.9: HTTP GET -metodin sisältö Kotiteatterin ohjaus -toiminnossa

Kun avaa kuvassa 5.9 olevan fin.xml -loppuisen internetosoitteen, saa esille kuvassa 5.10 olevan Kotiteatterin ohjaus -näkymän. Kun vielä avaa kuvassa 5.10 olevan description.xml -loppuisen internetosoitteen, niin saa näkyviin kuvassa 5.11 olevan Kotiteatterin ohjaus -infosivun. Kuvissa 5.10 sekä 5.11 olevat tiedot määrittelevät sisällön tekstit Bravian päävalikossa olevaan Kotiteatterin ohjaus -kohtaan.



Kuva 5.10: Kuva Kotiteatterin ohjaus -sivusta



Kuva 5.11: Kuva Kotiteatterin ohjaus -infosivusta

Bravia hakee älytelevision valikossa olevat kuvakkeet ja logot käyttäen hyväksi HTTP GET -metodia kuvassa 5.12 olevalla tavalla. Logon internetosoite löytyy, kun kyseisen metodin tulosta tarkastellaan tarkemmin, kuten alemmasta kuvasta 5.13 tulee esille.

Kuva 5.12: Esimerkki HTTP GET -metodista valikon kuvakkeiden ja logojen hakuun

Kuva 5.13: Aktivoi toiminnon logon internetosoite

5.4.2 Pienoissovellukset

Braviasta löytyy muutama erilainen pienoissovellus. Näiden sovellusten toiminta-periaate on hyvin samanlainen kaikilla eli haetaan erilaisia videosisältöjä palvelimelta. Kun käynnistää iFood.tv nimisen pienoissovelluksen, niin ensin tapahtuu niin sanottu kättely Bravian ja palvelun tarjoajan (palvelimen) välillä. Kättely mahdollistaa turvallisen tiedonsiirron. Kyseinen kättely tapahtuu käyttäen TLS-protokollaa ja etenee seuraavalla tavalla [48]:

1. Bravia lähettää Client Hello -viestin palvelun tarjoajalle.
2. Palvelun tarjoaja vastaa Bravialle Server Hello -viestillä, joka sisältää muun muassa sertifikaatin.
3. Bravia todentaa saadun viestin ja näin saadaan varmuus siitä, että palvelun tarjoaja on se, kuka se väittää olevansa.
4. Tämän jälkeen yhteys salataan käyttämällä julkista avainta ja avataan käyttämällä yksityistä avainta.

Kuvasta 5.14 voi nähdä datasta kaapatun kättely-keskustelun Bravian sekä palvelun tarjoajan välillä.

Source	Destination	Protocol	Lengtl	Info
10.42.0.32	35.166.22.196	TLSv1	152	Client Hello
35.166.22.196	10.42.0.32	TLSv1	1514	Server Hello
35.166.22.196	10.42.0.32	TLSv1	959	Certificate, Server Hello Done
10.42.0.32	35.166.22.196	TLSv1	392	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
35.166.22.196	10.42.0.32	TLSv1	125	Change Cipher Spec, Encrypted Handshake Message

Kuva 5.14: Kättely Bravian ja palvelun tarjoajan välillä

Tämän jälkeen valitaan sovelluksesta haluttu video ja käynnistetään se. Kyseinen toiminto tehdään käyttämällä HTTP GET -metodia kuvassa 5.15 nähdyllä tavalla. Kun mennään syvemmälle kyseiseen HTTP GET -metodiin, niin päästään kiinni itse videon internetosoitteeseen kuvan 5.16 osoittamalla tavalla. Videon voi sitten katsoa kopioimalla internetosoite selaimeen.

Source	Destination	Protocol	Lengtl	Info
10.42.0.32	69.16.175.10	HTTP	219	GET /files/8wn4hw/vi/converted/f5/cf/311667.mp4 HTTP/1.1

Kuva 5.15: Esimerkki HTTP GET -metodin käytöstä videon hakemisessa

```
Hypertext Transfer Protocol
▸ GET /files/8wn4hw/vi/converted/f5/cf/311667.mp4 HTTP/1.1\r\n
  Range: bytes=0-\r\n
  Host: static.ifood.tv\r\n
  Accept: */*\r\n
  User-Agent: SONY DTV/2010; PKG4.131EUH\r\n
  \r\n
  [Full request URI: http://static.ifood.tv/files/8wn4hw/vi/converted/f5/cf/311667.mp4]
  [HTTP request 1/1]
```

Kuva 5.16: Esimerkki HTTP GET -metodin sisällöstä videon hakemisessa

5.4.3 Pienoisohjelmat sekä muut asiat

Kun valitsee Bravian kaukosäätimellä asetukset-valikosta kohdan "Päivitä Internet-sisältö", niin silloin käyttäjä saa esille pienoisohjelmat. Pienoisohjelmia on Braviassa kolme kappaletta; Yahoo Finance, Yahoo News sekä Weather Widget. Yahoo Finance käynnistyy, mutta sitä ei pysty käyttämään millään tavalla. Yahoo News tai Weather Widget eivät vastaa ollenkaan. Näyttäisi vahvasti siltä, että tuki näille pienoisohjelmille on jo loppunut palvelun tarjoajan taholta.

Kun liikkuu Bravian käyttövalikossa, vaihtaa televisiossa kanavia, säätää äänenvoimakkuutta tai selaa ohjelmaopasta, niin dataa ei liiku lainkaan. Tämä tarkoittaa sitä, että nuo edellä mainitut toiminnot eivät ole Braviassa yhteydessä internetiin.

5.5 Sony Cecilian tietoliikenteen tutkimus

Tutkimuksen toinen kohde on helmikuussa vuonna 2019 valmistunut Sony KDL-50WF665 (käytän myöhemmin tästä älytelevisiosta nimeä Cecilia). Tämä malli kuuluu niin sanottuun toiseen älytelevisioiden ryhmään. Ceciliaan on siis esiasennettu erilaisia sovelluksia jo valmiiksi, mutta lisää sovelluksia ei valitettavasti käyttäjä voi itse asentaa ollenkaan. Jos Cecilian käyttäjälle esimerkiksi riittää vain Netflixin ja Yle Areenan käyttö, niin kyseiset sovellukset toimivat erittäin jouhevasti. Taulukossa 5.4 on listattu Cecilian tekniset tiedot sekä siitä löytyvät sovellukset. Cecilian pystyy liittämään internetiin sekä langallisesti että langattomasti.

Taulukko 5.4: Sony Cecilian tekniset tiedot sekä toiminnot.

Merkki	Sony	
Malli	Sony KDL-50WF665	
Valmistusvuosi	2019	
Ohjelmisto	v8.464-1000-1.700	Uusi päivitys löytyy internetistä. v8.585
Sarjanumero	6024899	
Käyttöjärjestelmä	Linux	
Sovellukset	Netflix	Yhdysvaltalainen tilausvideopalvelu.
	SF Anytime	Bonnierin omistama tilausvideopalvelu.
	MeteoNews	Sveitsiläinen sääpalvelu.
	prime video	Amazonin omistuksessa oleva tilausvideopalvelu.
	DW (Deutsche Welle)	Saksan radion ulkomaanpalvelu.
	Berliner Philharmoniker	Berliinin filharmonikoiden esityksiä tarjoava tilausvideopalvelu.
	Yle Areena	Yleisradion verkkopalvelu, josta voi katsoa sisältöä suorina lähetyksinä tai tallenteina.
	Youtube	Googlen omistama videopalvelu.
	Browser	Verkkoselain nimeltä Vewd Browser.

5.5.1 Cecilian käynnistysvaihe

Cecilia kysyy ensimmäisen käynnistyksen yhteydessä (eli kun älytelevisioon palautetaan tehdasasetukset), että hyväksyykö käyttäjä tietosuojakäytännön vai ei. Jos tietosuojakäytäntöä ei hyväksytä, niin Ceciliaa ei voi liittää internetiin. Tämä tarkoittaa käytännössä sitä, että mitään älytelevision toimintoja ei voi käyttää. Tietosuojakäytännön pystyy hyväksymään myös myöhemmin niin halutessaan.

Kun tietosuojakäytännöt on hyväksytty, yhdistetään Cecilia internetiin. Käyttäjä voi valita joko langallisen tai langattoman yhteyden. Yhteydet voidaan tarkistaa samalla tavalla kuin Bravian tutkimuksessa on tehty. Ainoana ero on muuttunut

ip-osoite, joka Cecilialla on 10.42.0.99. Tämän jälkeen yhteys vielä tarkistetaan Cecilian asetuksista. Langattoman verkon autentikointi tapahtuu samalla lailla Ceciliassa kuin Braviassakin.

Cecilia hakee valikossa näkyvät sovellusten logot samalla tavalla kuin Braviakin eli käyttämällä HTTP GET -metodia. Logot haetaan internetosoitteesta http://static.-internet.sony.tv/bivl-ww/static/service/icons/. Cecilia myös suorittaa Bravian tavoin aika ajoin onnistuneesti HTTP GET-metodilla STVgetTime -toiminnon. Kyseisessä kutsussa on aikamääreen lisäksi myös Cecilian vuosimalli sekä ohjelmistoversio. Tällä kertaa Wireshark-ohjelmaan on laitettu päälle toiminto Resolve Network Addresses ja sen avulla Wireshark kääntää ip-osoitteen luettavaan muotoon, kuten kuvasta 5.17 tulee hyvin esille.

Cecilialle löytyy internetistä uusi ohjelmistopäivitys. Automaattinen ohjelmiston lataus on otettu tarkoituksella pois päältä, jotta voidaan seurata tietoliikennettä latauksen aikana. Ohjelmistopäivitys käynnistetään manuaalisesti Cecilian asetuksista, mutta päivitys päättyy virhekoodiin. Sonyn tukisivustolta ehdotetaan, että Cecilia pitäisi yhdistää internetiin käyttäen langallista yhteyttä.

Source	Destination	Protocol	Lengtl	Info
10.42.0.99	ssm1.internet.sony.tv	HTTP	188	GET /DTV/stv/c/STVgetTime/ HTTP/1.1
ssm1.internet.sony.tv	10.42.0.99	HTTP/XML	616	HTTP/1.1 200 OK

Kuva 5.17: HTTP HEAD -metodin sisältö

5.5.2 Ceciliassa olevat sovellukset

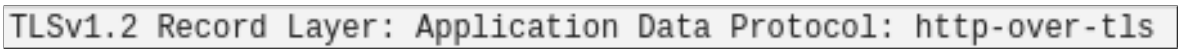
Ceciliassa on jo valmiiksi ladattuja sovelluksia, eikä käyttäjä pysty valitettavasti itse lataamaan sovelluksia lisää käyttöönsä. Cecilian sovelluksista löytyy neljä sovellusta, joissa on pakko kirjautua palveluun, jotta käyttäjällä on mahdollisuus katsoa sisältöä. Nämä sovellukset ovat yhdysvaltalaiset tilausvideopalvelut Netflix ja Amazonin Prime Video, ruotsalaisen mediakonsernin omistama SF Anytime sekä klassista musiikkia tarjoava Berliner Philharmoniker.

Sovelluksista löytyy myös kaksi sellaista sovellusta, joihin on vapaaehtoinen kirjautuminen; Yleisradion oma sisältöpalvelu Yle Areena sekä Googlen omistama videopalvelu Youtube. Sveitsiläinen sääpalvelu MeteoNews sekä Saksan radion ulkomaanpalvelu Deutsche Welle eivät vaadi kirjautumista lainkaan, vaan ne ovat käyttäjän vapaasti katsottavissa. Viimeisenä sovelluksena löytyy verkkoselain nimeltä Vewd Browser.

Yhteydet ja sovellukset ovat hyvin salattuja, joten Wiresharkin avulla napattua tietoliikennettä ei ole hirveän helppo analysoida. Seuraavassa kuitenkin muutamia mielenkiintoisia huomioita eri sovellusten tietoliikenteestä.

Netflix ja Youtube

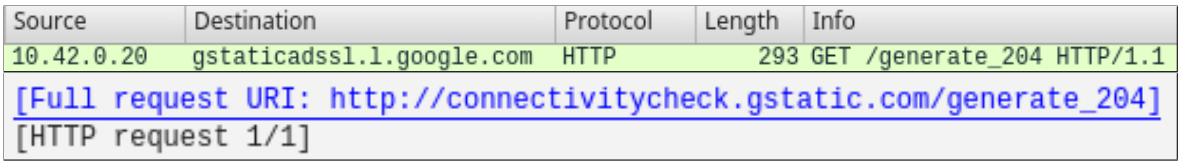
Kun käynnistää yhdysvaltalaisen tilausvideopalvelu Netflixin sovelluksen, niin tietoliikenne paketit suorastaan vilisevät silmissä. Tieto ja huomiot siitä, että kaikki liikenne on salattua, ei tule yllätyksenä. Data on suojattu käyttäen TLS-salausprotokollaa, kuten kuvasta 5.18 tulee esille. Netflixin ja Cecilian välillä liikkuvaa dataa ja paketteja pystyy katsomaan ja selaamaan, mutta datan tarkempi analyysi ei onnistu. Olisikin hieman outoa, jos maailman tunnetuin ja suurin tilausvideopalvelujen välittäjä jakaisi tietonsa helposti kaikkien nähtäville.



Kuva 5.18: TLSv1.2 suojaus

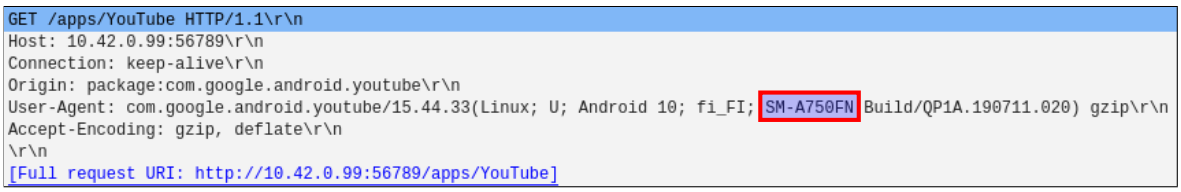
Datan määrä kasvaa huimasti Wireshark-ohjelmassa Netflixin tapaan, kun käynnistää toisen videon välitykseen erikoistuneen sovelluksen eli Youtube-sovelluksen. Paketteja liikkuu nopeaan tahtiin ja datassa vilahtelee tasaisin väliajoin sana Youtube. Kun käyttäjä kirjautuu Youtube-sovellukseen sisään, on hänellä pääsy omiin tallennettuihin videoihin sekä hakuihin. Youtube-sovellukseen pystyy helposti kirjautumaan esimerkiksi käyttäjän omalla älypuhelimella. Tässä tapauksessa käyttäjän älypuhelin liitetään samaan langattomaan verkkoon kuin Ceciliakin on ja avataan Youtube-sovellus älypuhelimella. Tämän jälkeen annetaan älypuhelimen Youtube-sovelluksessa lupa Ceciliankin käyttää samaa tunnistautumista hyväkseen ja kirjautuminen Cecilian Youtube-sovellukseen onnistuu tällä tavalla. Seuraavassa kappaleessa kerrotaan kyseinen kirjautumisprosessi Wireshark-ohjelmalla kaapatun tietoliikennedatan avulla.

Käyttäjällä on Samsungin Galaxy A7 2018 SM-A750FN älypuhelin käytössä. Kun käyttäjän älypuhelin liittyy samaan verkkoon kuin missä Ceciliakin on, niin se tarkistaa langattoman verkon yhteyden kuvassa 5.19 olevalla metodilla ja ottamalla yhteyttä connectivitycheck.gstatic.com -osoitteeseen.



Kuva 5.19: HTTP GET -metodi yhteyden varmistamiseen

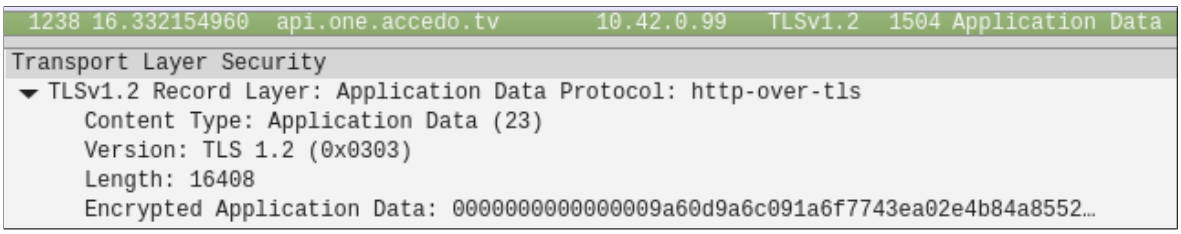
Kun käyttäjän älypuhelin on saatu liitettyä samaan langattomaan verkkoon Cecilian kanssa, niin avataan älypuhelimesta Yuotube-sovellus ja kirjaudutaan sisään. Tämän jälkeen hyväksytään kirjautuminen älypuhelimen kautta Ceciliaan. Tämä toiminto näkyy tietoliikenteessä kuvassa 5.20 esitetyllä tavalla. Kuvassa punaisella ympyröity teksti näyttää käyttäjän älypuhelimen mallin SM-A750FN.



Kuva 5.20: Youtube-sovellukseen kirjautuminen

Yle Areena

Käynnistettäessä Yle Areena -sovelluksen tietoliikenteen sekä erilaisten pakettien määrän kasvun huomaa helposti Wireshark-ohjelmassa. Laittamalla päälle toiminnon Resolve Network Addresses ja seuraamalla pelkästään pakettien lähdeosoitteita löytää mielenkiintoisen osoitteen; api.one.accedo.tv. Kaikki liikenne Cecilian ja kyseisen osoitteen välillä on salattua, kuten kuvasta 5.21 tulee hyvin esille. Kun nimeä Accedo tutkii tarkemmin, niin löytää Ylen omilta sivuilta tiedon, että Yle Areena sovelluksen on toteuttanut ruotsalainen yritys nimeltä Accedo [22].



Kuva 5.21: api.one.accedo.tv sekä TLSv1.2 suojaus

Kun kirjautuu Yle Areena -sovellukseen sisään, niin tietoliikenteessä tulee esille seuraavia osoitteita; akamaiedge.net, yleisradio, analytics-collector-production, login-api-prod-c8.yle.fi, areena-api-production sekä endpoint.finnpanel.fi. Kyseisten tahojen ja Cecilian välinen tietoliikenne on salattu TLSv1.2-protokollaa hyväksikäyttäen. Osoitteiden sisällöistä ja omistajasta lisää tutkimuksen tulokset -osiossa.

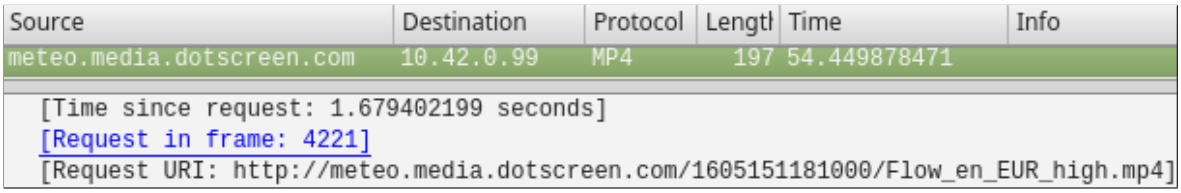
SF Anytime

SF Anytime on Bonnierin omistama tilausvideopalvelu. Kun sovelluksen avaa Cecilian kautta, niin saman tien alkaa tietoliikennedataa liikkua kasvavaan tahtiin. Nimet kuten cloudfront.net sekä akamaitechnologies.com toistuvat monta kertaa datassa. Nämä kyseiset tahot ovat erittäin tunnettuja sisällön jakelijoita sekä pilvipalveluita tarjoavia yrityksiä. Tietoliikenne näiden tahojen sekä Cecilian välillä on luonnollisesti salattua eikä tietoliikenteeseen pääse kiinni. Kun laittaa SF Anytimen sovelluksen kautta pyörimään elokuvan The Professor trailerin, niin tämän tiedon pystyy poimimaan datasta, kuten kuvasta 5.22 voi nähdä. Tietoliikennedatasta löytyy myös nimi google analytics moneen kertaan.

Kuva 5.22: Kuvakaappaus SF Anytimen tietoliikenteestä

MeteoNews

Sveitsiläinen sääpalvelu MeteoNews ei vaadi kirjautumista sovellukseen lainkaan, vaan palvelu on ilmainen kaikille käyttäjille. Kun sovelluksen käynnistää ja selailee sen sisältöä, niin tietoliikennedatasta löytyy esimerkiksi MP4-protokollalla varustettuja paketteja. MP4-protokollan nimi antaa jo vahvan vinkin sisällöstä ja kun pakettia tutkitaan tarkemmin, paljastuu sieltä videoleikkeen internetosoite, kuten kuvasta 5.23 tulee esille. Kun internetosoitteen laittaa selaimeen, voi videon katsella tai vaikka tallentaa omaa käyttöön.



Kuva 5.23: Videoleikkeen internetosoite

Yksi erittäin mielenkiintoinen löytö MeteoNews-sovelluksen tietoliikennedatasta on osoite nimeltä visitanalytics.userreport.com/hit.gif, kuvassa 5.24 on yksi esimerkki. Kyseinen sivu tuo mihin tahansa palveluun tai internetsivustolle html-koodilla yhden läpinäkyvän pikselin, jota ei voi ihmissilmällä havaita eikä se häiritse sivuston käyttöä. Kun käyttäjä sitten käy läpinäkyvän pikselin sisältämällä sivustolla, niin html-koodi lähettää omalle palvelimelleen tiedon, että sivustolla on käyty.

```
[Full request URI: http://visitanalytics.userreport.com/hit.gif?t=SMCDIR_34486&RND=392209]
```

Kuva 5.24: visitanalytics.userreport.com

Kun html-koodi lähettää tiedon sivustolla käymisestä, niin samassa viestissä lähtee tieto älytelevisio merkistä, mallista sekä ohjelmistoversiosta, kuten kuvasta 5.25 näkyy.

```
Model/Sony-KDL-50WF665 SonyCEBrowser/1.0 (KDL-50WF665; v8.464-100
```

Kuva 5.25: Älytelevision merkki, malli ja ohjelmistoversio

DW (Deutsche Welle)

Käyttäjän käynnistettyä ilmaisen DW (Deutsche Welle) -sovelluksen, nousee tietoliikenteestä heti esille HTTP GET -pyyntö. Kyseinen pyyntö (näkyy alla kuvassa 5.26) sisältää ehkä jopa hieman yllättäen suoran internetosoitteen internetin päälle rakennettuun palveluun. Eli sovellus ei olekaan oikea sovellus, vaan vain linkki internetosoitteeseen, joka näyttää aivan sovellukselta. Kun menee kyseiseen internetosoitteeseen, niin osoitteessa pystyy käyttämään palvelua aivan kuin käyttäisi normaalia sovellusta.

```
Cookie: xtvrn=$506921$; SERVERID=s2\r\n
\r\n
[Full request URI: http://smarttv.dw.com/web]
[HTTP request 1/1]
[Response in frame: 66]
```

Kuva 5.26: Deutsche Welle -sovelluksen internetosoite

Browser

Selainsovelluksena Ceciliassa on aikaisemmin Operan valmistama selain nimeltä Vewd Browser. Tietoliikenne on salattua selaimen ja internetin välillä. Selainsovellusta on vaikeahko ja kömpelö käyttää pelkän Cecilian kaukosäätimen avulla ja tämän takia kyseistä sovellusta tuskin hirveästi edes käytetään. Toki selaimeen on mahdollista tallentaa suosikkeja tai selailla historiatietoja, mutta taitaa siltikin löytyy huomattavasti helpommin käytettäviä laitteita internetissä seikkailemiseen.

6 Tutkimustulokset

Ensimmäisessä aliluvussa käydään läpi käyttäjän hyväksyttävät tietosuojakäytännöt. Toisessa aliluvussa käydään läpi sekä Bravian että Cecilian tietoliikennedatasta löydetyt mahdolliset tietovuodot sekä tietoturvaongelmat.

6.1 Tietosuojakäytännöt

Kun Cecilian käynnistää ensimmäisen kerran, on käyttäjän hyväksyttävä Sonyn laatima tietosuojakäytäntö. Jos käyttäjä ei hyväksy käytäntöä, ei Ceciliaa voi liittää internetiin lainkaan eikä mitään sovelluksia voi käyttää. Vastaavaa tietosuojakäytännön pakotettua hyväksymistä ei ole Braviassa. Toki tämä johtuu varmasti siitä, että Braviassa ei ole samanlaisia sovelluksiakaan tarjolla.

Kuulostaa erittäin oudolta, että käyttäjän itse ja omaan käyttöön hankkimaa laitetta ei suurimmaksi osaksi voi käyttää lainkaan ilman, että käyttäjä hyväksyy valmistajan laatiman tietosuojakäytännön. Tämä tapa on yleisesti käytössä monilla eri valmistajilla sekä monissa eri laitteissa. Olisi todella hyvä, jos käyttäjä voisi poimia tietosuojakäytännöstä itse ne kohdat, mitä olisi valmis hyväksymään. Tällä hetkellä valmistaja käyttää ota tai jätä -taktiikkaa ja pakottaa käyttäjät hyväksymään kaikki laatimansa ehdot.

Sana tietosuojakäytäntö kuulostaa nopeasti luettuna siltä, että se olisi laadittu suojaamaan käyttäjän tietoja sekä oikeuksia. Näin ei kuitenkaan valitettavasti ole, vaan tietosuojakäytäntö on lähinnä laadittu suojaamaan valmistajan oikeuksia hankkia tietoja käyttäjästä sekä käyttäjän tekemistä valinnoista.

Mitä käyttäjän sitten pitää hyväksyä, kun hän hyväksyy Cecilian tietosuojakäytännön? Tietosuojakäytännön ensimmäisellä sivulla sanotaan, että käyttäjän on annettava yritykselle Sony tietoja itsestään, ostamastaan älytelevisiosta, sen käytöstä ja katseluhistoriasta. Tämä kuulostaa jo aika pahalta yksityisten tietojen kalastelulta. Seuraavaksi tarkastellaan, mitä kaikkea Cecilia kerää käyttäjästään; älytelevision asetukset, tietoja palveluiden sisällöstä, bittinopeudesta, laitetunnuksesta, ohjelmistoversiosta sekä kielestä, alueesta ja mallin nimestä. Nämä tiedot ovat kuulemma välttämättömiä, jotta käyttäjällä olisi pääsy internetiin. Pelkkä ohjelmistoversion tar-

kistus olisi kyllä aivan riittävä tieto käyttäjästä valmistajan suuntaan. Tällä tiedolla voidaan myös aidosti parantaa tietoturvaa, koska laite voidaan päivittää uuteen ohjelmistoversioon sellaisen ollessa tarjolla.

Tietosuojakäytännössä mainitaan myös se, että Sony voi jakaa keräämiään tietoja kolmansien osapuolten palveluntarjoajien kanssa. Tämä kohta on erittäin epäilyttävä, koska tämä antaa periaatteessa Sonylle oikeuden jakaa tietoja käyttäjistään kenelle tahansa. Sonyn palvelimet sijaitsevat ympäri maailmaa, mutta jos käyttäjä asuu esimerkiksi Suomessa, niin tietoja suojataan Euroopan komission mallisopimuslausekkeiden mukaisesti. Tämä tieto on positiivinen, koska tietosuojakäytännöt saattavat olla huomattavasti heikompia Euroopan ulkopuolellla.

Sony säilyttää keräämiään tietoja noin 6 kuukautta, jonka jälkeen tiedot poistetaan. Tosin missään ei mainita sitä, että lähteekö tuo 6 kuukauden aika aina uudestaan alusta, kun tekee laitteelle tehdasasetusten palautuksen. Käyttäjä voi myös halutessaan muuttaa kantaansa tietosuojakäytännön hyväksymisen suhteen, mutta jos käyttäjä ei hyväksy ehtoja, niin ei myöskään mikään internetiä käyttävä sovellus tai toimintokaan toimi. Tietosuojakäytännöllä on positiivinen kaiku, mutta todellisuus ei kuitenkaan kuulosta siltä, valitettavasti. Taulukkoo 6.1 on kerätty Cecilian tietosuojakäytännön tärkeimmät havainnot.

Taulukko 6.1: Cecilian tietosuojakäytännön tärkeimmät havainnot

Havainto
Käyttäjän on pakko hyväksyä tietosuojakäytäntö kokonaisuudessaan, jos aikoo käyttää kaikkia älytelevision toimintoja.
Olisi hyvä, jos käyttäjä voisi itse valita, minkälaiset tietosuojakäytännöt hän hyväksyy. Nyt vaihtoehtoina on vain hyväksy tai hylkää.
Tietosuojakäytäntö on tehty lähinnä suojaamaan valmistajan oikeuksia, ei niinkään käyttäjän.
Tietosuojakäytännön hyväksynnällä käyttäjä antaa luvan omien tietojensa käyttöön tai luovuttamiseen kolmannelle osapuolelle.
Sony säilyttää keräämiään tietoja 6 kuukautta. Tosin missään ei lue, että alkaako tietojen keräys aina alusta, kun palauttaa tehdasasetukset älytelevisioon.
Positiivinen asia on se, että suomalaisen käyttäjän tietoja suojataan Euroopan komission mallisopimuslausekkeiden mukaisesti (vaikka tiedot olisikin tallennettu johonkin muualle).

6.2 Toiminnot sekä sovellukset

Bravia

Sekä Bravian että Cecilia tarkistavat aika ajoin ohjelmistoversiot omalta palvelimeltaan käyttäen STVgetTime-toimintoa. Tämä toiminto tarkistaa palvelimelta, jos löytyy uusi ohjelmistoversio ja ilmoittaa siitä käyttäjälle. Ceciliassa tämä toiminto ei tosin toimi, mutta Braviassa tämä toiminto toimi hyvin muutama vuosi sitten. Käynnistyksen jälkeen tuli ruutuun ilmoitus uudesta ohjelmistoversiosta ja sen lataus onnistui internetin välityksellä vaivatta. Tällainen toiminta parantaa tietoturvaa huomattavasti.

Bravian iFood.tv nimisestä pienoissovelluksesta pystyy tallentamaan videoita omaan käyttöön todella helposti. Kun sovelluksesta käynnistää haluamansa videon ja hakee sen jälkeen tietoliikennedatasta hakusanalla HTTP GET tietoja, niin kyseinen video löytyy nopeasti. Tämän jälkeen käyttäjä poimii videon internetosoitteen talteen ja lataa videon omaan käyttöönsä. Kun käyttäjä käyttää Kotiteatterin ohjaus -toimintoa Bravialla, niin tietoliikenteestä löytyy widget-hakusanalla xml-loppuinen internetosoite. Tämän osoitteen avaamalla selaimessa pääsee xml-kieliselle sivustolle, jossa näkyy kaikki Kotiteatterin ohjaus -toiminnossa olevat kirjoitetut ohjeet. Jos hyökkääjä pääsee murtautumaan kyseiselle sivustolle, niin hyökkääjällä on ainakin teoriassa mahdollista muuttaa koko sisältö haluamakseen sisällöksi.

Cecilia

Cecilialle on tarjolla uusi ohjelmistoversio 8.585. Ohjelmistoversion päivitys ei kuitenkaan toimi, jos Cecilia on yhdistetty internetiin käyttämällä langatonta yhteyttä. Ceciliaan on laitettu automaattinen ohjelmiston lataus -toiminto päälle, mutta Cecilia ei edes ilmoita käyttäjälle, että uusi ohjelmistoversio olisi saatavilla. Tämä on selkeä tietoturvaongelma, varsinkin silloin, jos ohjelmistoversio korjaisi jonkun selkeän olemassa olevan tietoturva-aukon. Langaton yhteys on kuitenkin erittäin suosittu tapa yhdistää älytelevisio internetiin (ja suosio vain kasvaa), joten tämä puute pitää saada ehdottomasti korjattua.

Ohje Sonyn tukipalveluista kertoo, että päivitys uuteen ohjelmistoversioon kannattaa tehdä niin, että lataa uuden ohjelmistoversion usb-muistitikulle ja asentaa uuden version sitä kautta. Tämäkin tapa on aivan toimiva, mutta tietysti työläämpi. Myös tietoturva kärsii huomattavasti, kun koko vastuu uuden ohjelmistoversion päivityksestä jää käyttäjän harteille. Ohjelmistopäivityksiä on aikaisemmin myös jaettu televisiosignaalin kautta, mutta ne ovat loppuneet melkein kokonaan niiden

maksullisuuden sekä kömpelön jakoprosessin takia.

Kun Yle Areena -sovelluksen laittaa päälle Ceciliassa, alkaa tietoliikennettä virrata moneen eri suuntaan. Pakettien osoitteista voi päätellä jo hyvinkin paljon. Akamai on hyvin tunnettu sisältöjen toimittaja, kun taas analytics collector viittaa vahvasti tiedon keräämiseen. Finnpanel on suomalainen toimija, joka mittaa television katselua. Login-api sekä areena-api -osoitteet viittaavat Yle Areenan sovelluksen kirjautumiseen sekä Yle Areena -sovelluksen toimintaan.

Ceciliasta löytyvää SF-Anytimen sovellusta käyttäessä vilahtaa tietoliikenteessä hakusanapari google analytics. Nimi kertoo jo paljon eli on kyse tiedon keräämisestä. Tietoliikenne on salattua, joten syvällisempää analyysiä ei tästä voi tehdä. Deutsche Wellen sovelluksen tietoliikenteestä on taas mahdollista löytää internetosoite, jonka kautta pääsee käyttämään kyseistä sovellusta suoraan esimerkiksi tietokoneen kautta. MeteoNews-sovelluksen tietoliikenteestä löytyy suoraan videoiden osoitteet, joten niitä pystyy lataamaan omaan käyttöön helposti. MeteoNews sovellus myös lähettää käyttäjätietoja omalle palvelimelleen käyttäen hyväkseen läpinäkyvää pikseliä sekä html-koodia. Tämä on selvää käyttäjätiedon keräämistä.

Cecilian Youtube-sovellukseen pystyy käyttäjä kirjautumaan älypuhelimen avulla, jos älypuhelin on vain samassa langattomassa verkossa. Teoriassa tätä keinoa pystyy käyttämään mahdollinen hyökkääjä hyväkseen niin, että hyökkääjä huijaa käyttäjää kirjautumaan hyökkääjän omalle Youtube-tililleen. Tämän jälkeen käyttäjä selailee hyökkääjän hänelle valitsemaa videosisältöä hyökkääjän omalta tililtä. Käyttäjän valitessa jonkun hyökkääjän määrittelemän videon, voi hyökkääjä esimerkiksi laittaa haittaohjelman latauslinkin videosta kertovaan kuvaukseen. Kun käyttäjä sitten klikkaa kuvausta, niin haittaohjelma latautuu käyttäjän laitteeseen.

Cecilian selainsovellusta Vewd Browser ei löydy enää Sonyn uusimmista malleista, koska sopimus Vewd-kauppapaikan ja Sonyn välillä on purettu kesäkuussa 2019 [47]. Vewd Browser toimii kyllä nykyäänkin, mutta mitään päivityksiä siihen ei enään saa. Tämä tekee kyseisestä sovelluksesta selkeän tietoturvauhkan. Selain on ollut nyt jo noin puolitoista vuotta ilman päivityksiä ja se on todella pitkä aika tietoturvallisesti erittäin herkässä sovellustyypissä kuten selain. Tässä vaiheessa turvallisin keino olisi poistaa sovellus kokonaan, mutta sitäpä ei pysty käyttäjä itse tekemään. Tämä on toinen selkeä tietoturvauhka, koska jos selaimeen tulee tietoturvaongelma, niin silloin tämä tietoturvaongelma on pysyvä sellainen eikä korjaavaa päivitystäkään enää tule. Alla olevaan taulukkoon 6.2 on vielä kerätty yhteenvetona tutkimuksessa esiin tulleita havaintoja.

Taulukko 6.2: Bravian ja Cecilian tutkimusten havaintoja

Havainto	**Bravia**	**Cecilia**
Tietosuojakäytäntö	Ei pakotettua tietosuojakäytännön hyväksymistä.	Pakotettu tietosuojakäytännön hyväksyminen.
Langattoman verkon autentikointi	Ok	Ok
Ohjelmistoversion tarkistus	Ok	Ok
Ohjelmistopäivitys	Ei saatavilla uutta päivitystä.	Uusi saatavilla, mutta päivitys ei onnistu langattoman verkon kautta.
Videoiden lataus	IFood.tv -sovelluksen videoita voi ladata omaan käyttöön.	MeteoNews-sovelluksen videoita vai ladata omaan käyttöön.
Sisällö muokkaus	Teoriassa mahdollista Kotiteatterin ohjaus -infosivun kautta	-
Tietojen keräys	-	Finnpanel kerää käyttäjästä tietoja Yle Areena sovelluksen ollessa päällä.
Tietojen keräys	-	Google analytics kerää käyttäjästä tietoja SF Anytime -sovelluksen ollessa päällä.
Tietojen keräys	-	Visitanalytics kerää tietoja käyttäjästä MeteoNews-sovelluksen ollessa päällä.
Suora linkki	-	Tietoliikennedatasta löytyy internetosoite, jonka kautta pystyy käyttämään sovellusta suoraan selaimen kautta.
Kirjautuminen	-	Sovellukseen pystyy periaatteessa kirjautumaan väärällä Youtube -tilillä.
Selain	-	Vewd Browser -sovellukseen ei ole mahdollista saada päivityksiä eikä sovellusta voi poistaa.
Netflix	-	Netflix-sovelluksen tietoliikenne on erittäin hyvin salattua.

7 Yhteenveto

Älytelevisioiden kehitys on ollut erittäin nopeaa viimeisten vuosien aikana. Älytelevisoista on tullut kodin viihdekeskuksia ja niistä löytyy paljon eri toimintoja sekä sovelluksia. Yksityisyyden suoja sekä tietoturvakysymykset ovat ehkä jääneet kehityksen jalkoihin.

Tutkimuksessa etsitään vastauksia mahdollisiin älytelevisioiden tietovuotoihin sekä tietoturvariskeihin. Työn teoriaosassa tarkastellaan älytelevision historiaa sekä sen sovelluksia ja toimintoja. Tietoturvaan liittyviä asioita esitellään teoriassa, mutta myös esimerkkien avulla. Lisäksi käydään läpi muita samaan aiheeseen liittyviä tutkimuksia.

Työn empiirisessä osassa esiteltiin sekä tutkimusympäristö että datan keräämiseen ja analysointiin liittyviä asioita. Molemmat tutkimuksessa mukana olevat älytelevisiot käytiin läpi erilaisine toimintoineen sekä sovelluksineen. Tutkimus suoritettiin keräämällä älytelevisioiden tietoliikennedataa. Tarkempi datan analysointi suoritettiin, kun dataa oli saatu kerättyä tarpeeksi.

Tutkimuksen tuloksista tulee hyvin esille, että tietosuojakäytännöissä olisi vielä paljon parannettavaa, ainakin käyttäjän näkökulmasta katsottuna. Sovelluksista ja toiminnoista löytyy myös tietoturvaongelmia. Esimerkkinä Ceciliassa esille tullut ohjelmistoversion päivitysongelma sekä selaimen toimittajan sopimuksen loppuminen. Useimmat ongelmat olisivat kohtuullisen helposti ratkaistavissa, jos niin vain halutaan tehdä.

Keinot käyttäjän yksityisyyden suojaamiseen sekä tietoturvan parantamiseen ovat periaatteessa hyvinkin yksinkertaisia. Ei tarvita suuria määriä rahaa tai kalliita laitteita vaan järkevää ja ennen kaikkea rauhallista ja ennakoivaa mieltä. Seuraavilla toimenpiteillä pääsee oikein hyvin alkuun: 1) huolehtii tarpeeksi vahvoista salasanoista eri palveluissa, 2) päivittää laitteita aina kun se vain on mahdollista, 3) käyttää virustorjuntaohjelmia (jos vain niitä on saatavilla). Kun lataa sovelluksia vain tunnetuilta kauppapaikoilta, niin todennäköisesti sovellukset ovat toimivia eivätkä sisällä haittaohjelmia.

Jatkotutkimuksena olisi luontaista sukeltaa syvemmälle älytelevisioiden maailmaan käyttäjän yksityisyyden sekä tietoturvan parantamisen näkökulmasta katsot-

tuna. Löytyisikö kenties keinoja tehdä laitteista turvallisempia käyttää? Kuinka vanhojen laitteiden tietoturvaa voisi parantaa? Onko ainoa vaihtoehto aina uuden hankinta vai löytyisikö kenties joku kiertotie? Jatkaako älytelevisiot valitsemallaan linjalla eli älytelevisiovalmistajat rakentavat laitteisiin aina vaan lisää sovelluksia vai tuleeko älytelevisioista vain näyttöpäätteitä?

Älytelevisiot ovat tulleet jäädäkseen. Vielä muutama vuosi sitten monet ajattelivat, että televisio laitteena tulee kuolemaan pois samalla tavalla kuin on käynyt digibokseille. Näin ei kuitenkaan käynyt, vaan älytelevisiot nostivat television uudestaan kodin johtavaksi viihdekeskukseksi. Älytelevision nykyinen helppokäyttöisyys, loistava kuvanlaatu ja monipuoliset palvelut sekä sovellukset ovat taanneet sen suosion.

Toivottavasti tulevaisuuden älytelevisiot ottavat myös käyttäjien yksityisyyden ja tietoturvan paremmin huomioon. Niin kuin aiemmin jo mainitsinkin, niin älytelevisiot ovat tulleet jäädäkseen. Toivoa sopii, että myös niiden tietoturva kehittyy samaan tahtiin kuin itse tuote.

Lähteet

[1] ABRAMSON, A. *The History of Television, 1942 to 2000*. McFarland, 2003.

[2] ABUZAID, A. M., SAUDI, M. M., TAIB, B. M., JA ABDULLAH, Z. H. An Efficient Trojan Horse Classification (ETC). *International Journal of Computer Science Issues (IJCSI) 10*, 2 (2013), 96.

[3] AHMED, B. S., JA BURES, M. Testing of Smart TV Applications: Key Ingredients, Challenges and Proposed Solutions. Julkaisusarjassa *Proceedings of the Future Technologies Conference* (2018), Springer, 241–256.

[4] ALABA, F. A., OTHMAN, M., HASHEM, I. A. T., JA ALOTAIBI, F. Internet of Things Security: A Survey. *Journal of Network and Computer Applications 88* (2017), 10–28.

[5] ALAM, I., KHUSRO, S., JA NAEEM, M. A Review of Smart TV: Past, Present, and Future. Julkaisusarjassa *2017 International Conference on Open Source Systems & Technologies (ICOSST)* (2017), IEEE, 35–41.

[6] ALGAZE, B. Smart TVs in 2015 - The Next OS Battleground. URL `https://www.extremetech.com/electronics/197582-smart-tvs-in-2015-the-next-os-battleground`, viitattu 16.1.2019.

[7] ALI, B., JA AWAD, A. I. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors 18*, 3 (2018), 817.

[8] BUDD, C. Ransomware Makes its Debut on the Small Screen: FLocker Infects Smart TVs. URL `https://blog.trendmicro.com/ransomware-makes-its-debut-on-the-small-screen-flocker-infects-smart-tvs/`, viitattu 29.11.2018.

[9] BULLOCK, J., JA PARKER, J. T. *Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework*. Wiley Online Library, 2017.

[10] CONTI, M., DRAGONI, N., JA LESYK, V. A Survey of Man in the Middle Attacks. *IEEE Communications Surveys & Tutorials 18*, 3 (2016), 2027–2051.

[11] CYBERYOZH SECURITY GROUP. Cyber Espionage Through Smart TVs. URL https://book.cyberyozh.com/cyber-espionage-through-smart-tvs/, viitattu 28.10.2020.

[12] DESPINS, G. L. Top Tips for Protecting Your Smart TV. URL https://www.welivesecurity.com/2018/10/01/protecting-your-smart-tv/, viitattu 20.2.2019.

[13] DICKSON, B. Millions of Smart TVs Are Vulnerable to Hackers. URL https://www.dailydot.com/debug/protect-smart-tv/, viitattu 4.10.2018.

[14] DIGITA. HybridiTV. URL https://www.digita.fi/antennitv/hybriditv/, viitattu 29.10.2020.

[15] FEDERAL TRADE COMMISSION. VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users Consent. URL https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it, viitattu 1.11.2020.

[16] FIELDING, R., GETTYS, J., MOGUL, J., FRYSTYK, H., MASINTER, L., LEACH, P., JA BERNERS-LEE, T. Hypertext Transfer Protocol – HTTP/1.1. URL https://www.hjp.at/doc/rfc/rfc2616.html, viitattu 9.11.2020.

[17] FINNPANEL. Television katselu kasvoi alkuvuonna. URL https://www.finnpanel.fi/tulokset/tiedote.php?id=202, viitattu 6.3.2020.

[18] FINNPANEL. TV-vuosi 2020: Finnpanelin esitys. URL https://www.finnpanel.fi/lataukset/tv_vuosi_2020.pdf, viitattu 16.9.2020.

[19] GAO, W., SUN, Y., FU, Q., WU, Z., MA, X., ZHENG, K., JA HUANG, X. ARP Poisoning Prevention in Internet of Things. Julkaisusarjassa *2018 9th International Conference on Information Technology in Medicine and Education (ITME)* (2018), IEEE, 733–736.

[20] GHIGLIERI, M. I Know What You Watched Last Sunday A New Survey Of Privacy In HbbTV. Julkaisusarjassa *Workshop Web* (2014), vol. 2.

[21] GHIGLIERI, M., JA TEWS, E. A Privacy Protection System for HbbTV in Smart TVs. Julkaisusarjassa *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)* (2014), IEEE, 357–362.

[22] HAAKANA, K. Areenan ensimmäinen äly-tv-sovellus käytössä. URL https://yle.fi/aihe/artikkeli/2014/09/16/areenan-ensimmainen-aly-tv-sovellus-kaytossa, viitattu 17.11.2020.

[23] HBBTV. HbbTV Overview. URL https://www.hbbtv.org/, viitattu 6.10.2015.

[24] HEINVUO, T. Disney+ on ollut niin iso menestys, että viihdejätti keskittyy nyt suoratoistoimperiumin rakentamiseen. URL https://tekniikanmaailma.fi/disney-on-ollut-niin-iso-menestys-etta-viihdejatti-keskittyy-jatkossa-suoratoistoimperiumin-rakentamiseen/, viitattu 13.10.2020.

[25] HOLLISTER, S. Weeping Angel: Did the CIA Really Hack into TVs? URL https://www.cnet.com/news/weeping-angel-hack-samsung-smart-tv-cia-wikileaks/, viitattu 4.2.2019.

[26] KANG, S., JA KIM, S. How to Obtain Common Criteria Certification of Smart TV for Home IoT Security and Reliability. *Symmetry 9*, 10 (2017), 233.

[27] KYBERTURVALLISUUSKESKUS. Philips–älytelevisioissa tietoturvaongelma. URL https://yle.fi/uutiset/3-7162795, viitattu 11.10.2015.

[28] LEHTO, T. Yle Areena tuli Samsungin televisioihin. URL https://www.tekniikkatalous.fi/tekniikka/ict/2014-09-16/Yle-Areena-tuli-Samsungin-televisioihin-%E2%80%93-%C3%A4ly-tv-standardin-puute-hiert%C3%A4%C3%A4-Yle%C3%A4-3255665.html, viitattu 16.1.2019.

[29] LYON, G. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Nmap Project, namp.org, 2009.

[30] MCAFEE. McAfee Software End of Life Announcement for Customers Using Samsung Tizen TV. URL https://service.mcafee.com, viitattu 24.6.2020.

[31] MICHÉLE, B. *Smart TV Security: Media Playback and Digital Video Broadcast*. Springer, 2015.

[32] MICHÉLE, B., JA KARPOW, A. Watch and be Watched: Compromising All Smart TV Generations. Julkaisusarjassa *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)* (2014), 351–356.

[33] MILLER, M. *The Internet of Things*. QUE Publishing, 2015.

[34] NIEMIETZ, M., SOMOROVSKY, J., MAINKA, C., JA SCHWENK, J. Not so Smart: On Smart TV Apps. Julkaisusarjassa *2015 International Workshop on Secure Internet of Things (SIoT)* (2015), IEEE, 72–81.

[35] NYKÄNEN, J. Television uudet vaatteet –kaikki älytelevisiosta. *Tekniikan Maailma*, 18E (2015), 26–27.

[36] OREN, Y., JA KEROMYTIS, A. D. From the Aether to the Ethernet - Attacking the Internet Using Broadcast Digital Television. Julkaisusarjassa *23rd {USENIX} Security Symposium ({USENIX} Security 14)* (2014), 353–368.

[37] PLUMMER, D. C. *An Ethernet Address Resolution Protocol*, Marraskuu 1982.

[38] POPESCUL, D. Smart TVs: What Do They Know (and Tell) about Us?

[39] RAHMAN, M. F. A., JA KAMAL, P. Holistic Approach to ARP Poisoning and Countermeasures by Using Practical Examples and Paradigm. *International Journal of Advancements in Technology 5*, 2 (2014), 82–95.

[40] RAUTI, S., JA LEPPÄNEN, V. Man-in-the-browser Attacks in Modern Web Browsers. Kirjassa *Emerging Trends in ICT Security*. Elsevier, 2014, ss. 469–480.

[41] RUTLEDGE, R. L., MASSEY, A. K., JA ANTÓN, A. I. Privacy Impacts of IoT Devices: a SmartTV Case Study. Julkaisusarjassa *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)* (2016), IEEE, 261–270.

[42] SAMSUNG. History of Samsung Smart TV. URL `http://news.samsung.com/global/infographic-history-of-samsung-smart-tv`, viitattu 12.10.2015.

[43] SCHEEL, R. Hacking a Smart TV. URL `https://www.youtube.com/watch?v=bOJ_8QHX6OA`, viitattu 1.11.2020.

[44] SHACKELFORD, S. J. *The Internet of Things: What Everyone Needs to Know®*. Oxford University Press, 2020.

[45] SIDIROPOULOS, N., JA STEFOPOULOS, P. Smart TV Hacking, 2013.

[46] SMIT, L. What Does Your Television Know About You, 2015.

[47] SONY.FI. VEWD TV Store poistuu Sonyn vuosien 2012-2018 televisioista. URL https://www.sony.fi/electronics/support/articles/00226633, viitattu 19.11.2020.

[48] T. DIERKS, E. R. The Transport Layer Security (TLS) Protocol Version 1.2. URL https://www.hjp.at/doc/rfc/rfc5246.html, viitattu 9.11.2020.

[49] TILASTOKESKUS. Suomen virallinen tilasto (SVT): Kuluttajien luottamus [verkkojulkaisu]. ISSN=2669-8862. Joulukuu 2018, Liitekuvio 13. Televisiolaitteet kotitalouksissa 2/2000-11/2018 (15-74 -vuotiaiden kohdehenkilöiden taloudet) . Helsinki: Tilastokeskus. URL http://www.stat.fi/til/kbar/2018/12/kbar_2018_12_2018-12-27_kuv_013_fi.html, viitattu 16.10.2020.

[50] TWENEBOAH-KODUAH, S., SKOUBY, K. E., JA TADAYONI, R. Cyber Security Threats to IoT Applications and Service Domains. *Wireless Personal Communications 95*, 1 (2017), 169–185.

[51] VARMARKEN, J., LE, H., SHUBA, A., MARKOPOULOU, A., JA SHAFIQ, Z. The TV Is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking. *Proceedings on Privacy Enhancing Technologies 2020*, 2 (2020), 129–154.

[52] WAGENSEIL, P. New Studies Reveal How Smart TVs Spy on You. URL https://www.tomsguide.com/news/new-studies-reveal-how-smart-tvs-spy-on-you, viitattu 31.10.2020.

[53] WUEEST, C. Can Smart TVs Be Hacked? URL https://www.forbes.com/sites/quora/2015/12/10/can-smart-tvs-be-hacked/?sh=13eb4d834683, viitattu 22.11.2020.

[54] WWW.VOCAL.COM. EAPoL - Extensible Authentication Protocol over LAN. URL https://www.vocal.com/secure-communication/eapol-extensible-authentication-protocol-over-lan/, viitattu 9.11.2020.

[55] YU, W., YALIN, Y., JA HAODAN, R. Research on the Technology of Trojan Horse Detection. Julkaisusarjassa *2019 12th International Conference on Intelligent Computation Technology and Automation (ICICTA)* (2019), IEEE, 117–119.

[56] ZAHRA, S. R., JA CHISHTI, M. A. Ransomware and Internet of Things: A new security Nightmare. Julkaisusarjassa *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (2019), IEEE, 551–555.