Tatu Laakso
Akseli Tyvelä

Modernin IoT-laitteen tietoturvaongelmat ja -ratkaisut

Kandidaatintyö
Tietotekniikan tutkinto-ohjelma
Helmikuu 2019
Tässä kandidaatintyössä perehdytään IoT-laitteissa piileviin tietoturvaongelmiin ja niiden ratkaisuihin. Työssä käydään läpi yleisimmät IoT-laitteita kohtaavat haavoittuvuudet, niihin johtaneet syyt sekä niiden aiheuttamat seuraukset. Lisäksi työssä esitellään jo markkinoilla olevia älykkäillä ominaisuuksilla varustettuja tietoturvalaitteita, joiden on tarkoitus vastata juuri IoT-laitteiden tietoturvaongelmiin.


Avainsanat: tietoturva, palomuuri, esineiden internet
ABSTRACT

This bachelor’s thesis takes a closer look on the security problems and solutions of a modern IoT device. Thesis covers most common vulnerabilities in IoT design, reasons behind, and consequences that follow. In addition, thesis showcases some of the devices intended specially for IoT security that have already reached the markets.

This thesis also includes design process for a Raspberry Pi based embedded system, that includes same functionality as commercial security devices and a mobile application to monitor the embedded system. System consists of packet-filtering type firewall, written in python, to capture and block unwanted packets and of REST-server to transfer information between firewall and mobile application.

Key words: network security, firewall, internet of things
SISÄLLYSLUETTELO

TIIVISTELMÄ
ABSTRACT
SISÄLLYSLUETTELO
ALKULAUSE
LYHENTEIDEN JA MERKKIEN SELITYKSET
1. JOHDANTO.......................................................................................... 7
2. TAUSTA ................................................................................................ 10
   2.1. Uhat ............................................................................................... 10
      2.1.1. Bottiverkot.............................................................................. 10
      2.1.2. Vakoilu.................................................................................. 13
      2.1.3. Kryptovaluutat................................................................. 13
      2.1.4. DoS/DDoS............................................................................. 14
      2.1.5. Saastuminen ................................................................. 16
   2.2. Markkinoilla olevat ratkaisut.................................................. 17
      2.2.1. Norton Core............................................................................ 17
      2.2.2. F-secure Sense ..................................................................... 17
      2.2.3. Bitdefender Box 2 .............................................................. 18
      2.2.4. Suorituskyky................................................................. 18
      2.2.5. Tietoturva .......................................................................... 19
3. ALUSTA .................................................................................................. 21
   3.1. Rasberry Pi ............................................................ 21
   3.2. Rasberry Pi 2 Vs. 3 .............................................................. 21
   3.3. Konfiguraatio ............................................................................. 22
4. PALOMUURI ............................................................................................. 24
   4.1. Pakettien kaappaus ............................................................ 24
   4.2. Pakettien suodatus ............................................................. 24
   4.3. Pakettien estäminen ............................................................ 26
5. MOBIILISOVELLUS .............................................................................. 27
6. REST-PALVELIN ................................................................................. 28
7. JATKOKEHITYS .................................................................................... 29
8. AJANKÄYTTÖ ......................................................................................... 31
9. YHTEEVETO .......................................................................................... 32
10. LÄHTEET .............................................................................................. 33
ALKULAUSE

Tämä työ on tehty osana sulautettujen ohjelmistojen projektia, ja haluamme kiittää Teemu Tokolaa ohjauksesta kurssin aikana.

Akseli Tyvelä
Tatu Laakso
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ARM</td>
<td>Advanced RISC Machine</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed-Denial-of-Service</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DNSBL</td>
<td>Domain Name System Black List</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial-of-service</td>
</tr>
<tr>
<td>GPU</td>
<td>Graphics Processing Unit</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation</td>
</tr>
<tr>
<td>LXDE</td>
<td>Lightweight X11 Desktop Environment</td>
</tr>
<tr>
<td>RAM</td>
<td>Random-Access Memory</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Protocol</td>
</tr>
<tr>
<td>TOR</td>
<td>Anonymity Network</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>XMR</td>
<td>Monero cryptocurrency</td>
</tr>
</tbody>
</table>
1. JOHDANTO

Teknologian kehittyessä ja komponenttien hintojen laskiessa ovat laitevalmistajat alkanneet lisätä älykkää ominaisuuksia yhä useampiin tavallisina pidettyihin kodin laitteisiin. Tietokoneiden ja älypuhelinten lisäksi jääkaapit, itkuhälyttimet ja jopa leivänpaahdintot ovat yhteydessä internettiin. Yhdessä nämä laitteet muodostavat niin sanotun esineiden internetin. Tarkoituksena on tarjota käyttäjille hyödyllisiä sovelluksia, joilla helpottaa kuluttajien elämää. Laitteita voi monitoroida ja ohjata etänä älypuhelimella, jolloin kuluttaja voi esimerkiksi tarkastaa jääkaappinsa sisällön tai ajastaa kahvinkeittimen. Kuvassa 1 on esitetynä yksi näkemys älykkäästä kodista [33].

Kuva 1. Esimerkkä älykodista.

Näillä arkielämää helpottavilla ominaisuuksilla on kuitenkin varjopuolensa, IoT-laitteiden puutteellinen tietoturva tarjoaa internetissä toimiville rikolliselle ja mahdollisille valtiolliselle takaportin, jonka kautta laitteet voidaan saada käyttöön omistajansa tietämättä. IoT-laitteista, kuten itkuhälyttimistä, muodostettuja tuhansien laitteiden bottiverkkoja on jo käytetty palvelunestohyökkäyksiin.


Kuva 2. IoT laitteiden määrän ennustettu kasvu.

IoT-laitteiden tietoturvan parantamiseksi on markkinoille tuotu useita tähän tarkoitukseen suunniteltuja laitteita, mm. Nortonin Core, F-securen Sense ja Cujo AI. Kaikkia laitteita yhdistää korkeahko hinta sekä kuukausimaksullisuus. Kaikkien laitteiden mukana toimitetaan myös mobiilisovellus laitteen ohjaamiseen ja
verkkoliikenteen seurantaan. Tässä työssä esitellään jo markkinoilla olevia
tietoturvaratkaisuja. Ja toteutettu vastaavia toiminnallisuksia sisältävä sulautettu
järjestelmä.
2. TAUSTA


2.1. Uhat

Suurimman uhan IoT-laitteille muodostaa niiden puutteellinen tietoturva. Laitteiden sisältämät sulautetut piirit ovat yleensä halpoja ja tietoturvan taso on usein puutteellista. On arvioitu, että jopa 70 prosenttia IoT-laitteista sisältävät vakavia aukkoja tietoturvassa [27], jotka eivät ole paikattavissa ohjelmistolla. Näitä aukkoja mahdollistavat laitteiden kaappauksen ja käyttöönoton erinäisten rikollisten tahojen toimesta. Esimerkiksi eräs Arizona yliopistossa tehty tutkimus havaitsi, että tutkimuksessa löydyistä noin 50 000 tulostimesta jopa 20 000 olivat haavoittuvaisia [3].

2.1.1. Bottiverkot

Bottiverkot ovat useista internetiin yhteydessä olevista laitteista koostuvia verkkkoja, joiden avulla on mahdollista tuottaa erilaisia verkkohyökkäyksiä. Bottiverkkoihin kuuluvat laitteet ovat useimmiten juuri IoT-laitteita, jotka bottiverkon hallitsija on ottanut käyttöönsä IoT-laitteiden haavoittuvuuksien avulla. Kuvassa 3 kuvataan bottiverkon rakennetta ja toimintaa.

Bottiverkon elämänkaari voidaan jakaa viiteen eri vaiheeseen, jotka ovat esitetty kuvassa 4. Ensimmäistä vaihetta sanotaan tarttuvavaiheeksi, jonka aikana laite altistuu virukselle. Viruksen yleisimpää levystä tapaa ovat tiedostojen lataaminen kyseenalaisilta sivuilta, haitallisen sähköpostin liitteen avaaminen, tai verkkosivuilta löytyvien mainosten klikkaaminen. Laite voi myöskin saastuttaa hyödyntämällä laitteesta löytyviä haavoittuvaisuuksia. Asiantuntijat ovat epäillleen, että jopa 25% kaikista internettiin kytkeytyviä laitteista ovat osana jotakin bottiverkkoa [1]. Tarttunnan jälkeen toisessa vaiheessa saastunut laite pakotetaan lataamaan
bottiverkkoa varten suunnitellun ohjelmiston, joka muunuttaa laitteen botiksi osana bottiverkkoa. [1][2]

Seuraavassa kokoontumisvaiheessa botti ottaa yhteyden bottiverkon hallitsijan määrittämään johtamis- ja ohjaamiskanavaan (eng. Command & Control channel), joka antaa bottiverkkoon kuuluville boteille käskyjä, jotka ohjaavat sen toimintaa. Tämän jälkeen siirrytään hyökkäämisvaiheeseen, jonka aikana voidaan toteuttaa erilaisia hyökkäyksiä uhreja vastaan. Hyökkäyksen pääteeksi bottiverkko siirtyy ylläpitovaiheeseen, jonka aikana bottiverkon hallitsija kokoaa botit jälleen yhteen bottiverkoksien bottiverkko siirtyy takaisin kokoontumisvaiheeseen. Ylläpitovaiheen aikana bottiverkkoa voidaan huoltaa ja päivittää, esimerkiksi tekemällä siitä vaikeammin havaittava viranomaisille. [1][2]


Bottiverkossa olevien laitteiden määrä voi vaihdella tuhansista jopa satoihin tuhansiin laitteisiin. Esimerkiksi avoimen lähdekoodin Mirai-bottiverkko, jota käytettiin useiden suosittujen nettipalvelujen kaatamiseen, kattoi vuonna 2017 noin 380 000 laitetta [36]. IoT-laitteiden määrän kasvaessa, ilman tietoturvan parantamista, voidaan bottiverkkojenkin koon odottaa kasvavan, jolloin rikolliset toimijat saavat käyttöönsä entistäkin suuremmat resurssit. 

Bottiverkkoja on myös käytetty kiiristämistarkoituksessa. Verkkojen hallitsijat voivat uhata verkkopalveluja tai yrityksiä esimerkiksi palvelunestohyökkäyksillä ja vaatia maksua hyökkäyksen lopettamiseksi tai estämiseksi. Lunnaat vaaditaan useimmiten virtuaalivaluuttana sen tarjoaman anonymiteetin vuoksi.
Bottiverkot eivät ole enää ainoastaan niiden perustajien käsissä, vaan kuka tahansa voi vuokrata bottiverkon käyttöönsä tietyksi ajaksi haluamaansa tarkoitukseen. Bottiverkkojen kauppa käydyään anonyymissa Tor-verkossa erilaisilla foorumeilla ja kauppapaikoilla. Tämä muodostaa yhä suuremman uhan, kun kuka tahansa, teknisesti osaamatonkin, henkilö tai taho voi valjastaa bottiverkon haluamaansa tarkoitukseen.

2.1.2. Vakoilu


2.1.3. Kryptovaluutat

Kryptografiasta perustuvien virtuaalisten kryptovaluuttojen syntyminen on herättänyt myös rikollisten toimijoiden kiinnostuksen ja virtuaalisia valuuttoja käytetäänkin laajasti rikolliseen toimintaan niiden anonymitetin takia. Virtuaalisilla valuutoilla on mahdollista käydä kauppa anonyymissa Tor-verkossa ja hankkia laitteita ja palveluja, kuten huumausaineita. Kryptovaluutat ovat herättäneet kiinnostusta myös kyberrikollisten keskuudessa ja bottiverkkoja onkin jo valjastettu louhimaan näitä valuuttoja. Kryptovaluuttojen louhinta tarkoittaa käytännössä tietokoneen, yleensä näytönohjaimen, laskentatehon ohjaamista kryptovaluuttojen siirtojen varmistamiseen matemaattisilla yhtälöillä, josta laitteiden omistajat saavat palkkion kryptovaluuttana. Yleensä louhinta vaatii käyttäjältä suurta rahallista panostusta laitteistoon mutta bottiverkkoa hyödyntämällä ei omaa laitteistoa tarvita. Esimerkiksi Smominru-bottiverkkoa, joka on
parhaimmillaan kattanut yli 500 000 laitetta ja tuottanut omistajilleen arviolta kolmen miljoonan dollarin edestä kryptovaluuttaa [28] on käytetty XMR-kryptovaluutan louhimiseen kaapautuilla Windows-palvelimilla. Smominr käytti hyväkseen NSA:n kehitteen ja sittemmin ShadowBrokersin vuotamaa EternalBlue-haavoittuvuutta [29].


Suora louhinta ei ole ainoaa tapaa hyödyntää böttiverkkoja kryptovaluuttojen hankinnassa. Satori-böttiverkkoa on käytetty Claymore-louhintahjelmiston suojauksen murtamiseen, jolloin böttiverkon omistajat pystyivät vaihtamaan kryptovaluutan siirroissa tarvittavat lompakko-osoitteet omiinsa ja ohjaamaan louhinnan tuottoja omaan lompakkoon [32]. Satori on muokattu versio tuhoisasta Mirai-böttiverkosta, mutta potentialistaan huolimatta on Satorilla hankittujen tuottojen määrä jäänyt verrattain pieneksi. [7]

2.1.4. DoS/DDoS

Denial of Service Attack, (DoS), eli palvelunestohyökkäys on yleinen ja erittäin haitallinen nettitirkollisuuden muoto, jolla pyritään häiritsemään tai kaatamaan internetissä toimivia palveluja, yleensä nettisivuja. Palvelunestohyökkäyksessä hyökkääjä pyrkii internetyhteyden avulla ylikuormittamaan palvelimen resurssuja väärillä palvelin kutsuilla. Myös ohjelmistoissa piileviä haavoittuvaisuuksia voidaan pyrkiä hyödystämään palvelunestohyökkäyksissä.

Distributed Denial of Service, (DDoS), eli hajautettu palvelunestohyökkäys on nimessä mukaan useista lähteistä koostettuja DoS- hyökkäyksiä. DDoS toteutetaan

2.1.5. Saastuminen

2.2. Markkinoilla olevat ratkaisut

IoT-laitteiden mukana tuomat ongelmat on tunnistettu laitevalmistajien toimesta ja markkinoille on tuotu useita tietoturvalaitteita, joiden tarkoitus on verkkoliikenteen suojauksen lisäksi tunnistaa IoT-laitteisiin kohdistuvia uhkia, sekä torjua ne. Seuraavaksi selvitetään kolmen parhaiten tunnetun tunnetun laitteet ominaisuuksia.

2.2.1. Norton Core

Valmistajan sivut tarjoavat laitteesta hyvin vähän tietoa. Valmistajan mukaan Core kuitenkin hyödyntää tekoälyä ja laitteiden yhdessä muodostamaa tietoverkkoa uhkien tunnistamiseen sekä torjumiseen. Lisäksi Core skannaa jokaisen bitin verkkoon tulevaa dataa mahdollisten uhkien varalta.

Coren 280 dollarin hintaan sisältyy itse laite, mobiilisovellus ja vuoden ohjelmistolisenssi, jonka jälkeen ohjelmiston käyttö maksaa 10 dollaria kuukaudessa. Valmistajan mainostamat kehityneet ominaisuudet eivät välttämättä ole kuitenkaan korkean hintansa arvoisia. Vaikka Norton Core on kolmesta esitellystä laitteesta kallein, on se jäänyt hienoisesti jälkeen kilpailevista, sekä edullisemmistä laitteista kuten F-Secure Sensestä [19]. Saman testin mukaan Core tunnisti 99.4% uhista, kun taas Sense pääsi täyteen 100 prosenttiin [20].

2.2.2. F-secure Sense

Valmistajan mukaan Sense yhdistää perinteisen WiFi – reitittimen sekä tietoturvaohjelmiston ja tarjoaa näin suojaa myös bottiverkkojen ja IoT-laitteiden kaappausten varalta. Uhkien estämiseksi Sense turvaa paikallisen liikenteen skannaukseen ja pilvivalvontaan.

Senseen 199 dollarin hintaan sisältyy itse laite, vuoden lisenssi ohjelmistoon sekä mobiilisovellus, vuoden lisessin jälkeen ohjelmisto jatkuu samalla 10 dollarin kuukausimaksulla kuin Nortonin Core.

Vaikka Sense käyttää uhkien torjunnassa ainoastaan paikallista liikenteen skannausta, pääsee se samassa Tom’s guiden puolueetmassa testissä [37] parempiin tuloksiin kuin Nortonin Core joka hyödyntää kehittyneempää teknologioita. Itseasiassa Sense ylsi täyteen 100 prosenttiin. [20]
2.2.3. **Bitdefender Box 2**

Bitdefender Box eroaa kilpailevista laitteista toimimalla rinnakkain jo olemassa olevan reitittimen kanssa ja pyrkimättä korvaamaan sitä kokonaan kuten Sense Tai Core. Bitdefenderiä voi käyttää myös reitittimenä, mutta valmistajan mukaan se ei kilpaile erillisten reitittimen kanssa.


Tom´s guident puolueetoman [37] testin mukaan Bitdefender suoriutui testistä 100 prosentisesti siinä missä F-Securen Sensekin [21].

2.2.4. **Suorituskyky**


Vaikka Bitdefenderiä ei myydä varsinaisena reitittimenä ei se jää juurikaan jälkeen Sensen suorituskyvyystä.

Esteitä sisältävää ympäristössä Bitdefender kuitenkin voittaa noin 30 metrin kantavuudellaan, Coreen yltää noin 26 metriin ja Sensen jäädessä vain n. 20 metriin. [20] [19] [24]
2.2.5. **Tietoturva**

Laitteista on vaikea löytää kattavia testejä, varsinkaan tietoturvan osalta. Ainoastaan tomsguide.com on testannut kaikki kolme laitetta. Tietoturvan testaamisen tosin tekee hankalaksi se, että verkko pitää ensin saattaa jollain tapaa hyökkäyksen kohteeksi, jotta tietoturva voidaan mitata.


Testeissä käytettiin hyväksi myös AV-Test -nimistä tietoturvaohjelmistotestia. Tom’s guiden mukaan Norton Core suoriutui testistä 99,4 prosenttisesti, Sensen ja bitdefenderin saadessa jälleen 100 prosenttia. Huomioitavaa on myös väärien hälytysten määrä AV-test tietoturvatestin aikana, joita Norton Core antoi 4 kappaletta, Bitdefender vain yhden ja Sense huimat 42 kappaletta. [19]

On myös hyvä huomioida, että esimerkiksi Avira ja Kaspersky Lab-tietoturvaohjelmistot saivat samasta testistä täydet pisteet [23], ilman että tarvitsevat tukeen kalliin tietoturvareitittimen, ja esimerkiksi Aviran Prime-tietoturvaohjelmiston lisenssi maksaa noin 10 euroa kuukaudessa. Tämä on saman hintainen kuin Coren, Sensen tai Bitdefenderin lisenssit mukana toimitettavan ilmaisen vuoden jälkeen. Käytännössä laitteiden ainoa etu on juuri IoT-laitteiden turvaamisessa. Tämän testaaminen onkin hankalaa, tai jopa mahdotonta, niihin kohdistuvien hyökkäysten muodon vuoksi, koska yhtä tiettyä kaavaa hyökkäyksille ei ole.

Core luottaa kykyyn tarkistaa verkkoon tulevat paketit mahdollisesti vaarallisena koodin varalta sekä pyrkii tarkastamaan mahdollisesti vaarallisia käyttäytymismalleja [22].

Sense pyrkii tunnistamaan IoT-laitteisiin liittyviä uhkia tarkistamalla pakettien SNI kentän ja suodattamaan yhteyksiä käyttäen tietoja verkko-osoitteiden aiemmasta toiminnasta. [20].

Parhaimman turvan IoT-laitteille, ainakin paperilla, näyttäisi antavan Bitdefender Box, joka kytketään reitittimen ja internet yhteyden väliin antamaan lisäsuojaa koko verkolle ja kaikille sen laitteille. Box antaa suojaa esimerkiksi SQL-injektiointiin, ja tunnistaa poikkeavia käyttäytyymismalleja verkkoliikenteestä, jolloin sekatkaisee...
liikenteen. Bitdefender Box estää myös ns. brute-force-tunkeutumisen, joka on yleinen tapa murtaa IoT laitteita, sekä sisältää suodattimen lähtevälle liikenteelle, jolloin se voi estää esimerkiksi luottokorttitietoja sisältävän liikenteen. [24]

Kaikki kolme laitetta ovat myös suojattuja WPA2-protokollalla, kuten muutkin yleiset nykyaikaiset langattomat reitittimet.


On siis syytä miettiä, onko kallis tietoturvareititin hienolla designilla rahallisen panostuksen arvoinen, vai onko viisaampaa hankkia vain sellaisia IoT-laitteita, joiden tietoturva on kunnossa jo laitteistotasolla, jolloin kolmannen osapuolen ratkaisuja ei välttämättä tarvita.
3. ALUSTA

Työn tarkoituksena on ollut perehtyä markkinoilla jo tarjolla oleviin IoT- tietoturva ratkaisuihin ja tuottaa samoja toiminnallisuksia sisältävää sulautettu järjestelmää. Tämän järjestelmän pohjaksi on valittu yhden piirilevyn Raspberry Pi minitietokone, joka sisältää tarvittavat ominaisuuudet laitteenv toteuttamiseksi.

3.1. Raspberry Pi


3.2. Raspberry Pi 2 Vs. 3

Suurimpana erona Pi 3 tarjoaa huomattavasti tehokkaamman suorittimen sekä grafiikkaohjaimen. Pi 3:een on myös integroitu langaton verkkokortti, joka mahdollistaa Pi:n käytön langattoman verkon tukipisteenä ilman erillistä WiFi-sovitinta toisin kuin Pi 2.

### 3.3. Konfiguraatio

Järjestelmämme varten Pi:hin on asennettu Raspbian-käyttöjärjestelmä, joka on Debian pohjainen, Raspberry Pi:n kevyelle ARM suorittimelle optimoitu Linux jakelu, josta valitsimme graafisen työpöytäympäristön sisältävän version, joka on niin ikään Raspberry Pi:lle optimoitu versio LXDE-työpöytäympäristöstä.
Raspbiania jaellaan myös komenoriviversiona, ilman graafista työpöytää, mutta se ei tarjoa käytännön tehonlisäystä, joten valitsimme testauksen helpottamiseksi graafisen vaihtoehdon.

Työn kannalta oli oleellista, että oma laitteemme, markkinoilla olevien laitteiden tapaan, toimii myös langattoman verkon tukipisteenä. Käytännössä tämä tapahtui siltaamalla Pi:n langallisen ja langattoman verkon sovittimet, wlan0 ja eth0, yhdeksi verkksi, jolloin kaikki wlan sovittimeen liitettyjen laitteiden liikenne ohjautuu ethernet portin läpi. Tämä myös edesauttaa myöhemmässä vaiheessa liikenteen kaappaamisessa ja suodattamisessa, kun tarkastelun kohteena on vain yksi liittymä. Kuvassa 6 on kuvattuna järjestelmän toiminta.

![Kaavio järjestelmän toiminnasta](image)

Kuva 6. Kaavio järjestelmän toiminnasta
4. **PALOMUURI**


4.1. **Pakettien kaappaus**

Pakettien kaappaamiseksi suodatusta varten käytettiin työssä hyväksi TShark-analysaattoriohjelmaa, joka on terminaaliversio suositusta Wireshark-pakettianalysaattorista joka mahdollistaa verkkoliikenteen kaappaamisen, tallentamisen ja analysoinnin. Tshark valittiin sille suunnitellun pyshark wrapper -laajennuksen takia. Kyseisen laajennuksen avulla kaapatut paketit voidaan tuoda python kieliseen ohjelmaan ja niitä voidaan käsitellä ohjelman sisällä lähes reaaliajassa Tsharkin tarjoamien työkalujen sekä itse kirjoitetun ohjelman avulla.

Pyshark mahdollistaa liikenteen kaappauksen halutusta liittymästä halutulla aikajaksolla sekä sen tallentamisen muuttuijin tai tiedostoon. Tässä tapauksessa paketit kaapataan eth0-liittymästä, kaiken liikenteen kulkuessa sen kautta, käyttämällä LiveCapturea Continuously-ominaisuutta, jolla ohjelma kaappaaa kaikki paketit ohjelman käynnistämisestä sen lopettamiseen. Tämän jälkeen paketit tallennetaan muuttujaan suodatusta varten.

4.2. **Pakettien suodatus**

Kuten mainittu, paketit päättettiin suodattaa niiden sisältämän IP-osoitteen perusteella, jolloin pakettien hyvyys on helposti ja konkreettisesti määritettävissä vertaamalla sitä haitallisiin IP-osoitteisiin ja määrittämällä numeerinen kynnysarvo sille, montako haitallista hakutulosta IP-osoitteleella sallitaan ennen paketin hylkäämistä

Toisessa vaiheessa IP-osoitetta verrataan erilaisiin IP-osoite listauksiin, joita on kolmenlaisia:

1. Ohjelman sisäiset listaukset,
2. URL-listaukset ja
3. DNSBL-listaukset.


URL-listaukset sisältävät eri tahojen ylläpitämät HTML muodosi tekstitiedostoja mahdollisesti eri tavalla haitallisista IP-osoitteista, esimerkiksi torstatus.blutmagie.de listaa mahdollisia TOR-verkon poistumiskohtia ja emergingthreats.net puolestaan listaa muun muassa eri tahoilta saamiaan osoitteita spamboteista, Zeus-bottiverkosta sekä pitää ”top-listaa” verkkohyökkääjistä.

URL-listauksia tarkistettaessa ohjelma yksinkertaisesti avaa URL-soitteen tekstitiedoston ja vertaa onko tarkastelun kohteena oleva IP-osoite listalla ja palauttaa totuusarvon TRUE/FALSE.

DNSBL on lyhenne sanoista ”Domain Name System Blacklists”, joka perustuu internetin nimipalvelujärjestelmään (DNS). Nimipalvelujärjestelmän avulla voidaan suorittaa kysely nimipalvelimelle (eng. Resolver) siitä, tunteeko se kysytävän IP-osoitteen. DNSBL:n tapauksessa nimipalvelin vastaa, onko kysytty IP-osoite haitallinen vai ei. Useimmat DNSBL-palvelut listaavat lähinnä sähköpostille haitallisia spambotteja, mutta joukosta löytyy myös esimerkiksi bottiverkkoja seuraavia DNSBL-listauksia.
Oleellista on suorittaa IP-osoitteen vertailu listoihin edellä mainitussa järjestyksessä resurssien säästämiseksi. Nopeinta on tarkastaa IP-osoitteita ohjelman sisäisiin listoihin verrattuna, DNSBL-palvelun ollessa hitain ja yhteydeltään epävarmin.


### 4.3. Pakettien estäminen

Pakettien estämisessä käytettiin linux-kerneliin sisäänrakennettua iptables-suodatinta, johon voidaan komentoriviltä kirjoittaa erilaisia palomuurisääntöjä liikenteen ohjaamiseksi tai estämiseksi. Käyttäjän käyttävä ohjelma sisältää funktion, jota kutsutaan tietyn BAD-muuttujan raja-arvon ylittäessä, joka avaa taustalle uuden prosessin, jossa komentoriville kirjoitetaan kaavassa 1 esitetty ennalta määritetty komento IP-osoitteen estämiseksi.

```
sudo /sbin/iptables -A INPUT -s "+ packet_ip +" -j DROP" (1)
```
5. MOBIILISOVELLUS

Työssä oli myös oleellista tuottaa mobiilisovellus sillä myös jo markkinoilla olevat tietoturvaratkaisut sisältävät usein mobiilisovelluksen liikenteen tarkkailuun ja laitteensa ohjaamiseen.


Käytännössä sovellus sisältää funktiota, joilla haetaan tietyn ajan välein REST-palvelimelta tiedot haitallisten pakettien sekä pakettien kokonaismäärätä ja ne esitetään käyttäjälle graafisessa muodossa.
6. REST-PALVELIN


Serveriä suoritetaan ns. paikallista osoitteena ”http://0.0.0.5000” käyttäen, johon asiakasohjelmat ottavat yhteyden. Tiettyyn resurssiin voidaan osoittaa URL-osoitteella ”http://0.0.0.5000/resursin nimi/”. Esimerkiksi haitallisten pakettien määrään voidaan osoittaa osoitteella ” http://0.0.0.5000/badpkts/”. Jokaista osoitetta varten määrätään halutut http-kutsut, joilla suoritetaan tietyjä toimenpiteitä. Esimerkiksi /badpkts/-resurssi sisältää kutsut GET ja POST, joka http GET-kutsulla palauttaa mobiilisovellukselle pakettien määrän, ja kutsulla POST taas tallentaa palomuurin lähettämän pakettien määrän.

Näin tiedonsiirto voidaan suorittaa sen vaikuttamatta palomuurin tai mobiilisovelluksen toimintaan ja pääinvaatoin, tällöin esimerkiksi sovelluksen vikatilanteessa palomuuri toimii edelleen normaalisti.

Koska palvelinta suoritetaan paikallisesta osoitteesta, jota ei tietoturvaystävistä ole avattu internetin päin, voi REST-palvelinta kutsua ainoastaan saman verkon sisästä. Tällöin myös http-kutsun onnistumiseksi täytyy puhelimen tai muun laitteen olla samassa verkossa kuin Raspberry PI:n.
7. JATKOKEHITYS

Vaikka tässä työssä tuotettu sulautettu järjestelmä toimii tietoturvalaitteena vähintään konseptitasolla, ja sisältää näennäisesti samoja toiminnallisuksia kuin markkinoilla olevat ratkaisut, sisältää järjestelmä kuitenkin tiettyjä puutteita. Nämä olisi korjattava laitteen jatkokehitystä sekä kaupallistamista silmällä pitäen. Näitä ovat:

1. Laitteen suorituskyky,
2. Ohjelmiston suorituskyky,
3. Mobiilisovelluksen ominaisuuDET ja
4. IP-listausten määrä ja luotettavuus.

Kuten jo aiemmin mainittu, on järjestelmän pohjana käytetyn Raspberry Pi:n suorituskyky suhteellisen rajallinen sekä laskentatehonsa että langattoman verkkokortin nopeuden puolesta. Langattoman verkon nopeus jäi auttamattoman hitaaksi 30Mbpss nopeudellaan, joka on reitittimen nopeudeki liian hidas, jotta Pi:tä voitaisiin käyttää reitittimenä.

Laskentatehon puute ilmenee palomuurin toiminnan hidastumisena IP-osoitteita käsitellessä, yhdentä en IP-osoitteen käsitellyyn voi kulua jopa useita sekunteja, jos ohjelma joutuu käymään läpi useita URL- tai DNSBL-listauksia ja ongelma keskaloittuu entisestään, jos verkossa on samanaikaisesti paljon liikennettä ja REST-serveriä suoritetaan yhtä aikaa.


Mobiilisovellus sellaisenaan ei täytä nykyisiä standardeja toiminnallisuuden eikä käyttöliittymän osalta. Jo markkinoilla olevien tietoturvalaitteiden mukana toimitettavat sovellukset sisältävät enemmän ominaisuuksia laitteen tilan tarkkailuun ja ohjaamiseen. Tätä työtä varten tuotettu mobiilisovellus esittää ainoastaan hyvien sekä hylättyjen pakettien määrit, joten käyttäjälle esitetään virheen määrä tulisi lisätä kattamaan esimerkiksi verkossa oleviin laitteisiin, sekä antamaan
käyttäjälle dataa verkon käytöstä esimerkiksi graafin muodossa. Lisäksi olennaista olisi lisätä käyttäjälle tarpeellisia työkaluja laitteen hallintaan.

Tällä hetkellä järjestelmä tarkastaa IP-osoitteita kahden URL-listan ja kuuden DNSBL-listauksen perusteella, ja vaikka nämä listat kattavat yhteensä tuhansia IP-osoitteita, on määrä silti liian alhainen, jotta palomuuri voisi toimia luotettavasti. Suuremmalla tietokannan mukana myös lähteiden luotettavuus kasvaisi, useita listauksia tarkastellessa kynnysarvoa kaikkien hylkämiseksi voitaisiin nostaa yhdestä ylöspäin ja vaatia että IP-osoite löytyisi esimerkiksi kolmelta listalta ennen sen hylkäämistä. Tällöin mahdollisesti vääristä syistä listalle joutuneet osoitteet voisi välttämättä hylättäisi. Lisäksi eri listauksia voisi arvottaa tietyin perustein niiden luotettavuuden mukaan.

Suuremmalla tietokannan saavuttamiseksi on järjestelmän suorituskyvyn kuitenkin kasvettava huomattavasti, sillä esimerkiksi DNSBL.info listaa 57 kappaletta DNSBL-listoja, joista ohjelma tällä hetkellä käsittelee kuutta, joiden lisäksi URL-listauksia on tarjolla eri tahoilta lähes loputon määrä.
8. AJANKÄYTTÖ


<table>
<thead>
<tr>
<th>Nimi</th>
<th>Tunnit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Akseli Tyvelä</td>
<td>247</td>
</tr>
<tr>
<td>Tatu Laakso</td>
<td>253</td>
</tr>
</tbody>
</table>

Taulukko 2. Työhön käytetyt tunnit.
9. YHTEENVETO


Tässä työssä keskityttiin IoT-laitteiden tietoturvaongelmiin yleisellä tasolla sekä esiteltiin markkinoilla olevia kolmannen osapuolen ratkaisuja. Lisäksi työssä tuotettiin vastaavia ominaisuuksia sisältävää sulaautettu järjestelmää.

Sulaautetun järjestelmän avulla pyrittiin tunnistamaan ja estämään tietoliikenne mahdollisesti haitalliseen IP-osoitteeseen kaappamailla kaikki verkkoon tulevat IP-paketit ja vertamaalla paketin sisältämää IP-osoitetta erilaisiin listoihin haitallisiksi tiedetyistä IP-osoitteista.


10. LÄHTEET


[15] Imperva Incapsula Distributed Denial of Service (DDoS)
URL: https://www.incapsula.com/ddos/denial-of-service.html

URL: https://www.quickanddirtytips.com/tech/computers/what-is-the-raspberry-pi


[18] Paul Miller (17.2.2017) Raspberry Pi sold over 12.5 million boards in five years
URL: https://www.theverge.com/circuitbreaker/2017/3/17/14962170/raspberry-pi-sales-12-5-million-five-years-beats-commodore-64

URL: https://www.tomsguide.com/us/norton-core-router,review-4827.html

URL: https://www.tomsguide.com/us/f-secure-sense,review-4801.html

URL: https://www.tomsguide.com/us/bitdefender,review-3983.html

[22] Brian Nadel (6.11.2017) Norton Core Router Review
URL: https://www.tomsguide.com/us/norton-core-router,review-4827.html


URL: https://www.tomsguide.com/us/bitdefender-box,review-3766.html


[27] HP News (29.7.2014) HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack.

URL: http://www.zdnet.com/article/a-giant-botnet-is-forcing-windows-servers-to-mine-cryptocurrency/


URL: https://www.nicehash.com/profitability-calculator

[31] Arjun Kharpal (1.3.2018) 15,000 internet-connected devices could be hacked to mine $1,000 of cryptocurrency in 4 days.


[34] URL: https://static2.businessinsider.com/image/563d14a69dd7cc18008c818a-700-517/unnamed.png


URL: https://www.tomsguide.com/us/toms-guide-who-we-are,review-4166.html