TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

TOMMI TIITINEN

TIETOTURVALLISUUDEN HAASTEET INTERNETIIN KYTKETYSSÄ TEOLLISESSA AUTOMAATIOJÄRJESTELMÄSSÄ

Diplomityö

Tarkastaja: professori Jarmo Harju
Tarkastaja ja aihe hyväksytty
Tieto- ja sähkötekniikan tiedekunta-neuvoston kokouksessa 4. kesäkuuta 2014

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Sähkötekniikan koulutusohjelma
Tiitinen, Tommi: Tietoturvallisuuden haasteet Internetiin kytketyssä teollisessa automaatiojärjestelmässä
Diplomityö, 57 sivua
Joulukuu, 2014
Pääaine: Tietoliikenneverkot ja protokollat
Tarkastaja: professori Jarmo Harju
Avainsanat: Tietoturva, Yrityksen toiminnanohjaus, Automaatiotekniikka

Teollisuustuotantokoneisto tarvitsee menestyäkseen jatkuvuutta ja tehokkuutta. Tavoitteisiin pyritään rakentamalla automaatiojärjestelmiä, jotka voivat parhaimmillaan moninkertaistaa tuotantokapasiteetin samalla, kun käyttökustannukset pienenevät ja tuotannossa tapahtuvat ajonaikaiset inhimilliset virheet harvenevat. Nykyaikainen automaatiojärjestelmä on usein kytketty Internetiin. Tässä työssä tutkitaan automaatiojärjestelmien tietoturvahaavoittuvuustasoa sekä sen mahdollisista puutteista johtuvia riskejä. Työn tarkoituksena on löytää turvallinen tietoturvataso yritykselle, jolla on sekä toimistoverkko että automaatiojärjestelmä sekä tavoite käyttää Internet-yhteyttä ohjausjärjestelmässään.

Työ jakautuu kahteen osaan: kirjallisuustutkimusosassa käsitellään yleisellä tasolla, millaisia ominaisuuksia teollisella automaatiojärjestelmällä on omien ominaisuuksiensa lisäksi Internet-verkkojen ja tietoturvan suhteen. Osassa käsitellään lyhyesti myös järjestelmän tietoturvan tason soveltuvuutta Internetin ja pilviteknologian käyttöön.

Tutkimusosassa tehdään laboratoriossa palvelunestohyökkäys PC-ympäristöön Ruge ja Ostinato -työkaluilla ja verrataan siitä saatuja tuloksia toisessa yliopistossa tehtyyn simuloituun hyökkäykseen, jossa kohteena on ollut automaatiolaitteisto. Lisäksi tarkastellaan tunnetun laitevalmistajan haavoittuvuuden hyödyntämisestä tehtyä tutkimusta, jossa kohteena olivat oikeat, nykyaikaiset automaatiokontrollerit. Tämä diplomityö osoittaa, että jo pelkän palvelunestohyökkäyksen kohteena olevan laitteen kyky vastaanottaa ja lähettää ohjausviestejä vahingoittuu riippuen hyökkäyksen kohteen sijainnista verkossa. Automaatiolaitteiden tietoturvaa päivitetään harvoin. Tarkasteltava tutkimus osoittaa, että päästessään palomuurien ohitse, hyökkääjä saattaa automaatioverkkoon päästessään saada kohdelaitteensa kokonaan komentoonsa. Johtopäätöksenä todetaan, että teollisessa automaatiojärjestelmässä on oltava korkeatasoinen helposti ylläpidettävä tietosuojaus verkon osille ja laitteistoille, joiden oma tietoturva ei riitä. Tällaisen suojauksen suunnittelussa on erityisesti otettava huomioon, että suojattava laitteiston tietoturva toimii lähes täysin lisäsuojalaitteiston varassa.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Programme in Electrical Engineering
Tiitinen, Tommi: Information security challenges in industrial automation systems with Internet connectivity
Master of Science Thesis, 57 pages
December, 2014
Major: Communication Networks and Protocols
Examiner: Professor Jarmo Harju
Keywords: Information security, Enterprise Resource Planning

Industrial Enterprise environment requires contingency and efficiency in order to succeed. Companies aim at these target factors by building automation systems that at best may bring exponential capacity growth while decreasing the level of monetary expenses and probability of run-time human errors. An up-to-date automation system is usually connected to the Internet. This thesis focuses on the level of information security of such systems and the possible risks related to low level cases. The target of this thesis is to find a safe information security level for a company that has both an office network and an automation system and aims at utilizing the Internet.

The work is divided into two parts: literature study part will handle generally which kinds of features of an automation system are related to Internet networks and information security. Additionally the Internet and cloud technology usage ability will be briefly visited.

In the research part of the thesis a service denial attack will be carried out and compared to a synthetized attack. Also a recent study about exploiting a well-known manufacturer's PLC device will be looked into. Its targets were real PLC devices that are still in use by manufacturing technology.
The thesis points out that a correctly positioned DoS attack may seriously harm a target device's ability to send or receive controller messages, the level of harm depending on the location of the victim in an automation network.

Additionally, industrial network devices are not often updated frequently. Should an attacker somehow pass all the firewalls and other IDS systems in front of the automation network the exploitation study shows that he may sometimes acquire the full control of his target automation device. For that reason a high level easy-to-maintain information security system needs to be implemented separately to cover the lack of security in an automation network and its devices.

ALKUSANAT

Tämä diplomityö tehtiin Tampereen Teknillisen Yliopiston Tietoliikennetekniikan laitokselle. Professori Jarmo Harju antoi minulle työn aiheen toukokuussa 2014 ja työtilan laitoksen toimistosta tarvittavaksi aikaa.

Haluan erityisesti kiittää Professori Jarmo Harjua ja DI Markku Vajarantaa pidetyistä seurantapalavereista sekä DI Joona Kannistoa avusta työn etenemiseksi. Kiitos myös diplomityön tekijä Niko Heikuralle, jonka erinomaisesta avusta johtuen sain tehtyä vertailututkimukseni vähemmillä virheillä ja nopeammassa aikataulussa. Haluan kiittää Professori Jarmo Harjua lisäksi myös mahdollisuudesta työskennellä yliopiston tiloissa ja kaikkia laitoksen työntekijöitä erinomaisesta työskentelyilmapiiristä. Suuri kiitos myös TTY:n opiskelijapalveluihmisille ja heidän antamalle ohjaukselle, jonka avulla sain suunniteltua opintoni järkeväksi kokonaisuudeksi. Lopuksi haluan kiittää puolisoani Heli Lukkaria, joka jaksoi tukea minua opintojen loppuunsaattamisessa sekä vihjasi hyvistä tavoista edetä kirjoittamistyössä.

SISÄLLYS

TERMIT JA NIIDEN MÄÄRITELMÄT

ERP-hanke	ERP-järjestelmän koko hankintaprosessi asiakasyrityksen kannalta.
ERP-järjestelmä	Tietojärjestelmä, jonka toiminnallisuus kattaa yrityksen toiminnan kaikki osa-alueet (Enterprise Resource Planning System).
DMZ	Demilitarisoitu alue
HART	Highway Addressable Remote Transducer – teollisuusprotokolla.
HLA	High Level Architecture
Konfigurointi	Järjestelmän parametrointi esimerkiksi valmiiden konfigurointitaulujen mukaan
IED	Intelligent Electronic Device. Mikroprosessorilla varustettu kontrolleri.
ISA-99	Turvallisuusstandardi teollisuusautomaatio- ja ohjausjärjestelmille
ISA-100	Langattoman verkkoliikenteen standardi
ICS	Industrial Control System (Teollinen ohjausjärjestelmä)
IDS	Intrusion Detection System (Hyökkäyksen tunnistava järjestelmä)
ISO-TSAP	International Standards Organization Transport Service Access Point
OMNet++	Laajennettavissa oleva modulaarinen C++ simulointikirjasto
Palomuuri	Järjestelmä, joka suodattaa suojattavan verkon ja sen ulkopuolisen verkon välisiä yhteyksiä. Palomuuri voi olla sekä ohjelmallinen toteutus että erillinen laite.
PLC	Ohjelmoitava logiikka
RTU	Remote Terminal Unit. Etäviestintää tukeva automaatiokontrolleri. Muutoin sama kuin PLC.
SCADA	Supervisory Control and Data Acquisition
Simulink	Graafinen ohjelmointikieli ja työkalu järjestelmien simulointia ja analysointia varten
SNMP	Simple Network Management Protocol
VNC	Virtual Network Computing. Etäkäyttöprotokolla graafisille käyttöliittymille.

1 JOHDANTO

Teollisuudessa käytetään automaatiojärjestelmiä tuotannon tehokkuuden ja suorituskyvyn optimoimiseksi. Teollinen automaatiojärjestelmä koostuu tuotannonohjauksesta, ohjelmoitavista logiikkalaitteista sekä erilaisista koneista. Ohjelmoitavia logiikoita hallinnoidaan SCADA-järjestelmistä, jotka samalla keräävät lokitietoa niiden toiminnasta tiedostoihin ja tietokantoihin. Tämän tiedon avulla SCADA raportoi järjestelmän tilasta ja tapahtumista. Lisäksi se ohjaa järjestelmän toimintaa.

Automaatiojärjestelmä saattaa olla käytössä monessa eri sijainnissa olevassa laitoksessa. On hyödyllistä, jos järjestelmän mittaustiedot voidaan tallentaa ja jakaa mahdollisimman reaaliaikaisesti muiden tuotantolaitosten kanssa. Reaaliaikaisuus saavutetaan parhaiten kytkemällä automaatiojärjestelmä ainakin osittain Internetiin, tai vähintään yrityksen sisäiseen tietoverkkoon. Yhteyden tulee olla nopea ja turvallinen, mutta ennen kaikkea tiedonsiirron tulee olla luotettavaa ja varmatoimista. Varmatoimisuuden saavuttamiseksi yritykset saattavat joskus laiminlyödä tietoturvallisuutta, koska näkevät turvallisuusominaisuuksien aiheuttavan hitautta ja turhia kustannuksia.

Huonosti suunniteltu yritysverkko saattaa altistaa järjestelmän tietoturvahyökkäyksille joko välillisesti tai suoraan. Tässä diplomityössä mallinnetaan toimiva yritysverkko ja haetaan ratkaisut esiintyvien tietoturvaongelmien korjaamiseksi. Koska tietoturvaongelmat ja laaja kokoelma erilaisia hyökkäystapoja voidaan mallintaa turvallisesti kokeellisessa verkossa, tämän työn lopputuloksena on tarkoitus löytää ratkaisu, jonka pitäisi palvella tietoturvallisena automaatiota hyödyntävän yrityksen tuotantolaitoksen verkkomallina.

1.1 Työn tavoitteet

Työssä rakennetaan tietokoneiden avulla informaatioverkko, joka vastaa mahdollisimman paljon pienen teollisyrityksen verkkoa, johon on kytketty SCADA-järjestelmä ja automaatiotekniikkaa. Koska käytännön syistä automaatiolaitteita ei työn aikana ollut saatavilla, toteutetaan työssä tehtävät hyökkäykset tietokoneympäristössä ja vertaillaan tuloksia sekä simuloituun automaatioverkon hyökkäykseen, että olemassa olevan haavoittuvuuden hyödyntämismenetelmän vaikutuksiin.

Automaatioverkossa hyökkäyksestä johtuvana ongelmana voivat olla komentojen hukkuminen, viiveet, laitteiden liikenteen luvaton lukeminen sekä laitteen luvaton hallinnointi tietomurron avulla. Tutkimusta varten rakennettuun verkkoon tehdään hyökkäyk-

siä, jotka saattaisivat olla vahingollisia automaatiolaitteiston avulla ohjatun tuotannon toiminnan kannalta. Hyökkäysten avulla löydetyt haavoittuvuudet pyritään paikkaamaan ehdotuksessa. Työn päätavoitteena on löytää malli, jolla yritykset voisivat rakentaa turvallisen verkon siten, että automaatiota ohjaava SCADA-järjestelmä pystyy ottamaan turvallisesti yhteyden Internetiin, vaikka itse tuotantolaitteiston tietoturvataso ei riittäisikään. Tietoturvallisuuden riittämätön toteutus aiheuttaa suuren taloudellisen uhkan yrityksille, joten toimivan konseptin löytämisestä on varmasti suuri hyöty.

Koska suojaamatonta verkkoa vastaan tehty hyökkäys on nykyisin lähes vaivatonta, se voidaan todeta triviaaliksi. Vastuu pitäisikin oikeastaan jakaa sekä teollisuusverkon ylläpitäjän, että palveluntarjoajien kesken jollakin järkeistetyllä tavalla. Murretut laitteet huonosti suojatuissa verkoissa mahdollistavat myös muiden kuin itse yrityksen vahingoittamisen. Työssä käydään läpi murtautumismalli erään tunnetun automaatiovalmistajan laitteeseen.

1.2 Työn rakenne

Työn eri vaiheet esitellään siten, että työn jokainen vaihe kuvataan omassa luvussaan. Kokonaisuudet pyritään esittämään jatkumona. Luvussa kaksi esitellään, millaisessa ympäristössä SCADA toimii, mitä ohjelmoitavat logiikat ovat ja mitä protokollia ne käyttävät kommunikointiin. Lisäksi kuvataan Internet-yhteyden roolia järjestelmässä.

Luvussa kolme arvioidaan, mitkä tahot ovat kiinnostuneita tietoturvauhkien hyödyntämisestä, millaisia hyökkäyksiä automaatiojärjestelmiin saattaa kohdistua ja mitä haittoja hyökkäyshaavoittuvuuksista mahdollisesti seuraa. Olemassa oleva tutkimus automaatiolaitteistojen näkyvyydestä Suomen alueen Internetissä toimii vertailukohtana luvussa tehdylle lyhyelle tutkimukselle. Luvussa käsitellään, miten laitteiden löytäminen tehdään ja minkä verran niitä näkyi työn tekemisen ajankohtana.

Luvussa neljä käsitellään yleisellä tasolla automaatioverkon etäohjauksesta johtuvaa tietoturvaongelmaa ja sen turvallisia perusratkaisuja. Lisäksi suositellaan suojautumistapoja eräältä yleisimmistä nykyisistä hyökkäystavoista.

Luvussa viisi tutkitaan automaatioverkkoon tehtävää simuloitua hyökkäysmallia sekä automaatiolaitteen murtautumismenetelmää. Lisäksi tehdään erilaisia palvelunesto-hyökkäyksiä laboratorioverkkoon, esitellään työn vaiheet ja työkalut sekä kirjataan niistä saatuja tuloksia.

Luvussa kuusi käydään keskustelua työn kulusta ja pohditaan, mitä on löydetty. Luvussa seitsemän on yhteenveto työn löydösten ja tulosten suhteesta toisiinsa sekä ehdotus siitä, mitä turvallisen automaatioverkon suunnittelussa olisi syytä ottaa huomioon työn löydösten perusteella.

2 AUTOMAATIOVERKKO JA SCADA

Tässä luvussa selitetään, millainen teollinen automaatioverkko rakenteeltaan on ja millaisia komponentteja siihen tavallisesti kuuluu normaaliin tietoverkkoon verrattuna tai lisäksi. Verkon rakenne on sinänsä itse yrityksen tarpeiden määrittelemä, mutta luvussa käydään läpi, mitkä ovat eri automaatioverkolle tyypillisten osien roolit ja mitä erityisesti juuri ohjelmoitavat logiikkakontrollerit sekä SCADA ja ERP tekevät. Lisäksi kerrataan, mihin Internet-yhteyden tarve tällaisessa verkossa perustuu.

2.1 Tietoverkko automaatioyrityksessä

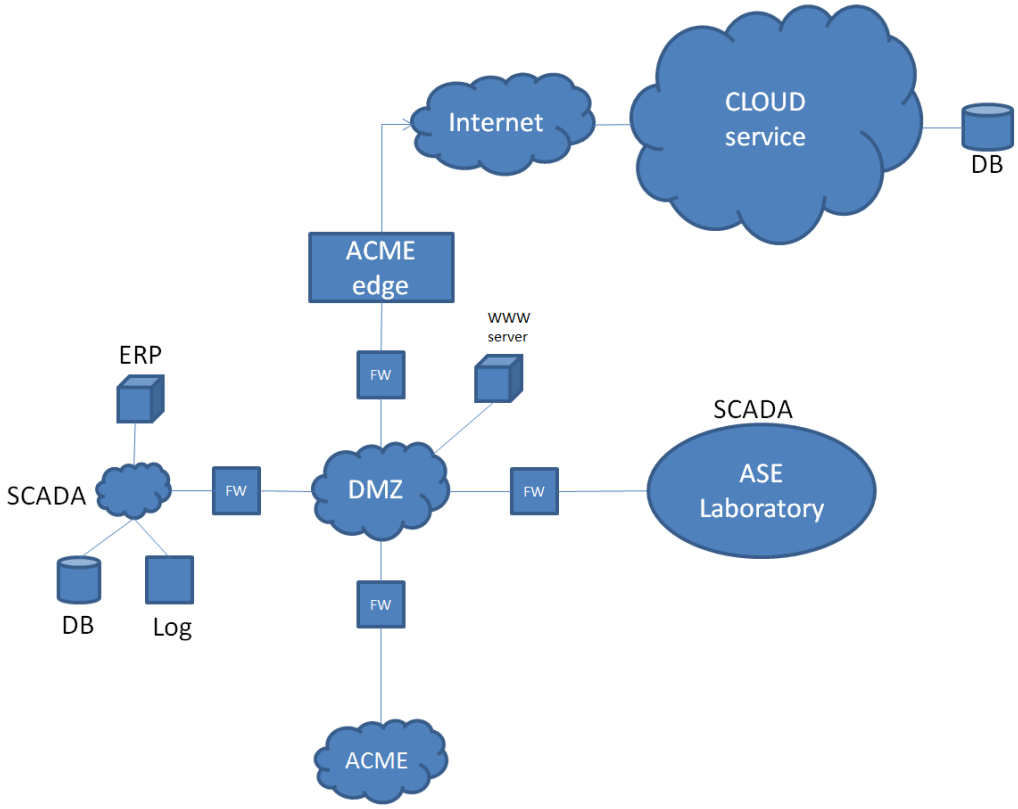
Teollinen automaatioverkko on tietoverkko, joka rakentuu hierarkkisesti muutamasta eri kerroksesta riippuen käytössä olevan tuotantojärjestelmän tarpeista. Kerrosten järjestyksen voi ajatella muodostuvan siten, että ylimpään kerrokseen kuuluu tuotannonohjaus, sen alla on automaatiosta tietoa keräävä ja ohjaava järjestelmä ohjelmoitavine logiikoineen. Lopulta alin kerros on itse tuotantolaitteisto robotteineen, linjastoineen, pumppuineen tai painekattiloineen riippuen yrityksen käyttämästä teknologiasta. Verkon laitteista osa on yhteydessä yrityksen verkkoon tai Internetiin.

Käytettävä ympäristö ja verkon ulkopuolelle Internet-yhteyksiä ottavat sovellukset vaikuttavat siihen, millainen tietoturvan taso tarvitaan suojaamaan järjestelmän toiminta. Myös se on oleellista, että järjestelmän toiminnan seurauksena syntyvä tieto pysyy tarkoituksenmukaisten tahojen tiedossa eikä sitä vuodeta esimerkiksi teollisuusvakoilijalle. Tietovuodot ovat olleet jo pitkään ongelma teollisuudessa, koska perinteisten menetelmien lisäksi nykyaikainen automaatiojärjestelmän toimintaympäristö rakennetaan siten, että tarvittaessa apuvälineiden ja ohjauslaitteistojen käytössä on Internet-yhteys. Huonosti suojattu yhteys tarjoaa mahdollisuuden kerätä ja jakaa reaaliaikaista tietoa tuotannosta ja siten ohjata ja tehostaa tuotantoa sekä löytää virhetilanteita ja korjata niitä. Kääntöpuolena tälle edulle on se, että automaatiojärjestelmä altistuu esimerkiksi palvelunestohyökkäysten kohteeksi.

2.2 Tutkittavan verkon rakenne ja osat

Työn alkutilanteessa tutkittavaksi kaavailtu verkko oli kuvan rakenteen mukainen. Kuvassa ACME tarkoittaa yritystä, jolla on käytössään teollinen automaatio-ohjausjärjestelmä. SCADA, yrityksen toimiston tietokoneet ja laboratorio on eristetty toisistaan palomuurien avulla. Verkkoon on rakennettu mahdollisuus Internet-yhteyden käyttöön. Se saadaan yrityksen reunapalvelimen, ACME edge, kautta. Palomuurien si-

säpuolelle jäävä suojavyöhyke sisältää yrityksen oman Web-palvelimen ja ulkopuolisille käyttäjille pääsyn yrityksen julkisille sivuille, joka tarjoaa yrityksen tietokoneille pääsyn intranetiin. Myöhemmin työn aikana selviää, saadaanko haavoittuvuusongelmaa vastaava tilanne mallinnettua ja kuinka paljon sellainen poikkeaa alla olevasta kuvasta. Jos vastaavaa verkkoa ei saada rakennettua, työn ohessa selvitetään joka tapauksessa oleellisimmat kuvan 1 kaltaisen verkon Internetin käyttöön liittyvät tietoturvahaasteet.



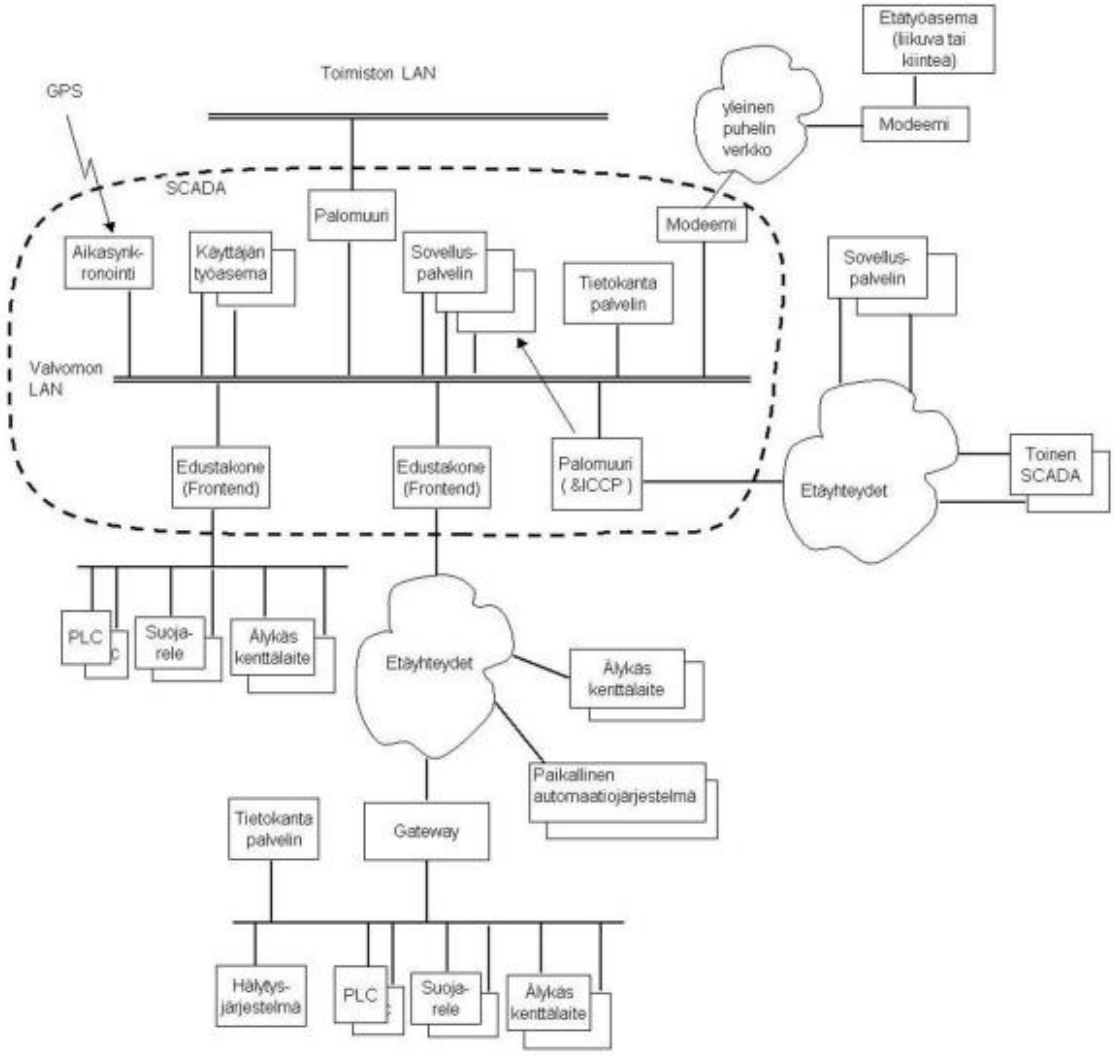
Kuva 1. Lähtökohta tutkittavan verkon rakenteelle. Kuvassa oleellista on SCADA-järjestelmän suojaus palomuurien avulla ja tietokannan pilvipalvelu.

2.3 SCADA

SCADA tarkoittaa valvomosovellusjärjestelmää, jonka avulla hallitaan teollisessa automaatioverkossa olevien ohjelmoitavien laitteiden toimintaa keskitetysti [1]. Laitteet saattavat sijaita maantieteellisesti hajautettuina, mutta tiedon hankinta eri yksiköistä tehdään keskitetysti. Lyhenne tulee sanoista: ”Supervisory Control and Data Acquisition.” SCADA-järjestelmillä on tällä hetkellä useita eri toimittajia ja osa toimittajista tekee myös automaatiolaitteita, kuten Siemens Industry Inc. Automaatiojärjestelmän valvomo-ohjelmiston tärkeimmät ominaisuudet ovat ohjelmoitavien logiikoiden toiminnan ohjaus ja erityisesti valvonta. Valvontaa voidaan tehdä muun muassa PLC-työkaluilla, jotka ovat PC-ympäristöön tehtyjä sovelluksia. Tällaisista sovelluksista kuitenkin puuttuvat tiedon tallennus- ja välitysominaisuudet, jolloin niiden ei katsota olevan valvomosovelluksia, eli SCADA-järjestelmiä, vaan käyttöliittymäsovelluksia.

Valvomosovelluksilla sen sijaan on valmiit rajapinnat PLC-käyttöisiin koneohjauksiin, standardoituja tiedonsiirtotapoja, kuten OPC sekä tuki tietokantajärjestelmään tiedon tallentamista varten. Valvomosovelluksen ja tuotannon välissä voi lisäksi olla ohjelmistosovelluskerros MES (Manufactoring Execution System), jolla muunnetaan tieto paremmin tuotannonohjausjärjestelmiin soveltuvaksi. Tyypillisiä hajautettuja toimintoja, joissa käytetään SCADA-järjestelmiä, ovat infrastruktuurijärjestelmät, kuten energianjakeluverkot, kaasulinjat, vesijärjestelmät, jätevesijärjestelmät sekä muut vastaavat verkot.

Järjestelmä rakentuu siten, että tyypillisesti liiketoimintoja varten yrityksellä voi olla pääsy tehtaan tietojärjestelmiin joko Internetin tai WAN-verkon kautta ja toimintoja ohjataan paikallisverkon palveluiden kautta. Laitoksen ohjausjärjestelmä pidetään kuitenkin erotetussa verkossa. Kuvassa 2 on edelliselle kuvalle vaihtoehtoisen toimintamallin esitys: maantieteellisesti hajautettu SCADA-järjestelmä [1].



Kuva 2. Maantieteellisesti hajautettu SCADA-tyyppinen järjestelmä (Erkki Anttila ABB, Pekka Koponen VTT) [1]. Kuva on vanha, mutta kuvaa hyvin järjestelmän yleistä rakennetta.

Erityisesti sähkönsiirron ja –jakelun järjestelmät ovat kuvassa 2 esitetyn kaltaisia järjestelmiä. Siinä ICCP-tietomalli (Inter Control Center Protocol) on tarkoitettu SCADA-järjestelmän keskinäistä keskustelua varten TCP/IP-verkossa. SCADA-järjestelmän valvomon lähiverkko on palomuurin kautta yhteydessä toimiston paikallisverkkoon ja laajaan lähiverkkoon. Huomioitavaa tällaisessa järjestelmässä on, että itse järjestelmä ja sen ala-asemat on aikasynkronoitava esimerkiksi GPS-ajan perusteella. SCADA-tyyppisiin järjestelmiin kuuluvat keskusvalvontayksikkö sekä yksi tai useampia etäasemia. Keskitetty ohjausjärjestelmä sijaitsee ohjauspalvelimessa ja kommunikaatio reititetään oman suojatun aliverkon kautta. Ohjausjärjestelmä kerää etäasemien tiedot lokeihin ja toimii havaintojen ja mittausten perusteella [1].

2.4 Tuotannonohjausjärjestelmä

Tuotannonohjausjärjestelmää kutsutaan termillä ERP (Enterprice Resource Planning) [2]. Yksinkertaistettuna tuotannonohjaus tarkoittaa menettelyä, jolla ohjataan tuotantoa, mutta tämän työn aihepiirin mukaisesti rajataan merkitys siten, että tuotannonohjausjärjestelmällä viittaan ohjelmistoon, jonka avulla yrityksessä hallitaan sekä kustannuksia ja laatua, että rahan käyttöä ja informaatiota. Valvontaohjelmistolla kerätyn tiedon avulla voi suunnitella tuotannon materiaalitarpeet ja vähentää varastointikustannuksia ja pitää yllä tietoa yrityksen tarvitsemien komponenttien ja materiaalien riippuvuuksista. Se kokoaa alleen materiaalien hallinnan ja ohjauksen sekä tuotantokoneiston kapasiteetin hallinnan. Lisäksi siihen yhdistyy taloushallintaohjelmistot sekä tuotannonohjausjärjestelmät.

Kokonaisuudessaan tuotannonohjausohjelmisto on erittäin laaja mutta myös monimutkainen ja kallis ylläpitää. Laajuuden käsittämiseksi valvontasovellusten lisäksi tuotannonohjauksessa on otettava huomioon CRM (Customer Relationship Management), SRM (Supplier Relationship Management), resurssien hallintastrategiat, toimitusketjun hallinta, PLM (Product Lifecycle Management) sekä teknologian arkkitehtuurivalinnat, jotka ovat jatkuvan muutosprosessin alaisina.

2.5 RTU ja ohjelmoitavat logiikat

Automaatioverkkoon kytketään yleensä RTU-laitteita ja ohjelmoitavia logiikoita. RTU-laitteiden tehtävänä on muuntaa sensoreiden tekemää tietoa digitaaliseen muotoon ja lähettää sitä ohjausjärjestelmälle. Ne tukevat yleensä sekä digitaalisia että analogisia ohjauksia ja toimivat hyvin samalla tavalla kuin PLC-laitteet. Myös RTU-laitteet pystyvät suorittamaan pieniä esiohjelmoituja tehtäviä ilman SCADA-järjestelmän ohjausta ja lisäksi tukevat usein langatonta viestintätekniikkaa, kuten satelliittiyhteyksiä.

Laitteiden toiminta ei poikkea kovin paljoa, koska PLC-laitteetkin tukevat nykyisin tietojen lähettämistä verkon ulkopuolelle. Sen sijaan RTU-laitteiden ohjelmointiominai-

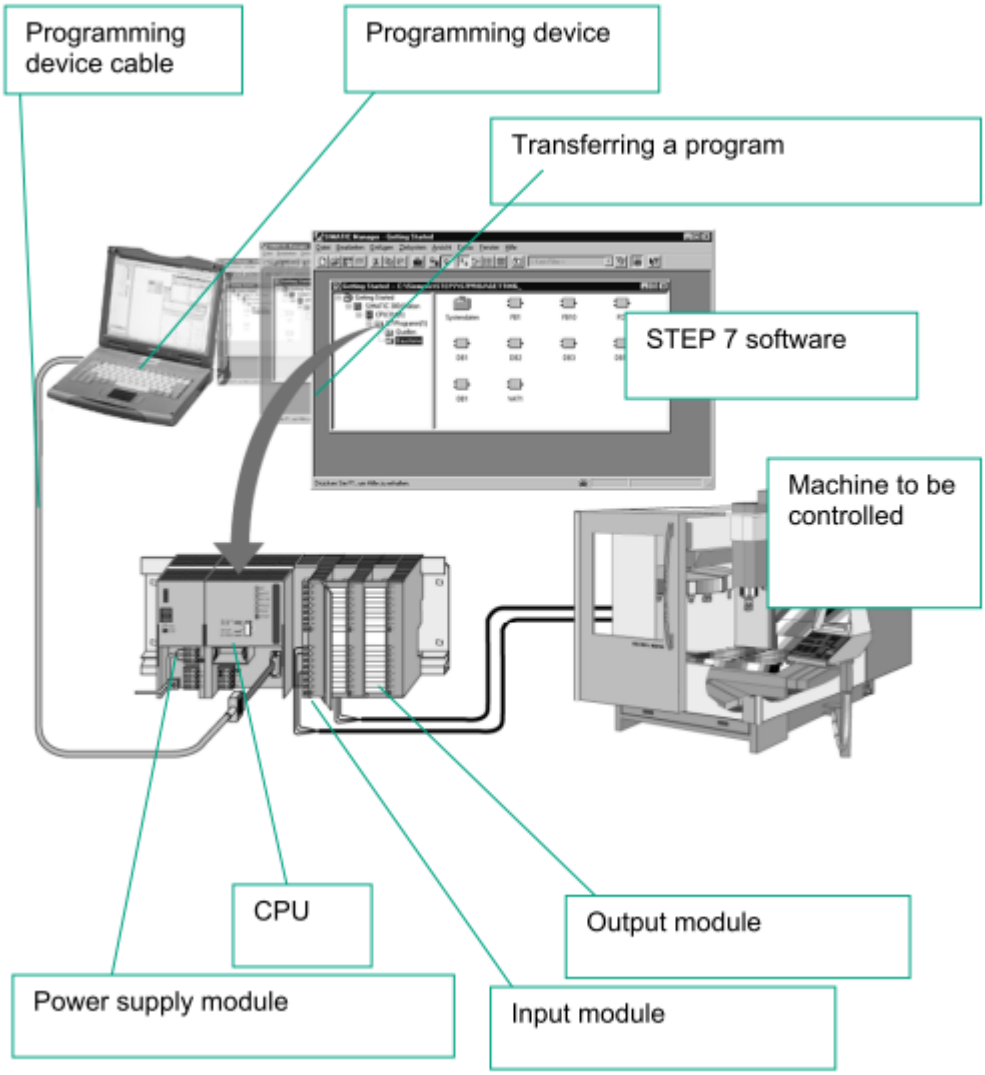
suudet ovat rajallisemmat ja sen vuoksi niiden rinnalle kytketään myös PLC-laitteita. SCADA-järjestelmät hyödyntävät ja tukevat molempia laitekantoja.

PLC-laitteita sanotaan ohjelmoitaviksi logiikoiksi. Tämä johtuu siitä, että tällaiset laitteet ovat ohjaimia, jotka voidaan ohjelmoida ohjaamaan suhteellisen lyhyitä toimintoja, kuten materiaalien ja komponenttien työstämistä tai asentamista ilman jatkuvaa käyttäjän valvontaa ja ne tukevat usein useampaa kuin yhtä ohjelmointitapaa. RTU-laitteilla ohjelmointitapa yleensä rajoittuu yhteen [3]. Ohjelmoitavat logiikat osaavat tehdä niille määritellyn tehtävän itsenäisesti loppuun, mutta ovat rajoittuneita sen suhteen, että ne eivät osaa pääsääntöisesti aloittaa uutta tuotetta tai muuttaa tehtäväänsä. Eräs tunnetuimmista järjestelmätoimittajista on Siemens, joka on tuonut markkinoille oman ohjelmoitavan logiikkaohjaimensa: ”Simatic S5” jo vuonna 1979. Sitä ohjelmointiin Assemblerillä ja ns. ”function block” -kielellä. Nykyisin käytössä on usein S7-sukupolven ohjainyksiköt, (Kuva 3) joiden avulla voidaan hallita prosesseja ja tuotantoa esimerkiksi apteekin lääkehakurobotin ohjauksessa tai suuressakin ympäristössä, esimerkiksi paperi- tai puhelintehtaassa.

Kuva 3. Siemens S7-1200. Logiikkaohjain sekä siihen tarkoitettu käyttöliittymäkomponentti (HMI), jolla voidaan automatisoida ja ohjata tehdasautomaatiota tukevia laitteita. Kuva on otettu Jyväskylän Kyberturvallisuusmessuilta syyskuussa 2014 Siemensin osastolla.

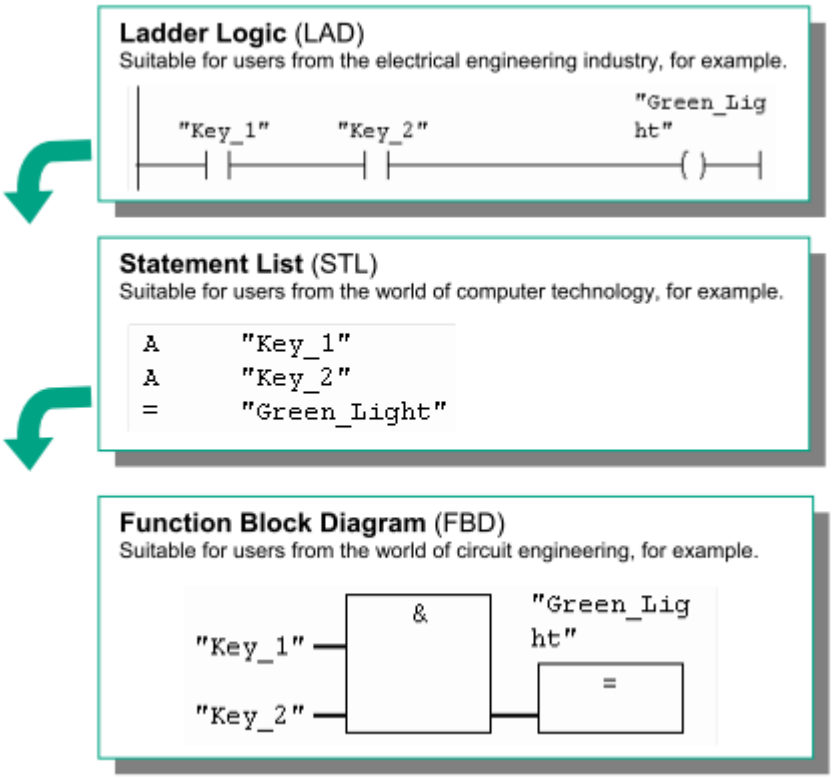
Kun teollinen automaatioverkosto haluaa olla yhteydessä Internetiin, tarvitaan reititin, palomuuri ja erityisesti ympäristöön sopiva kytkin, joka sietää lämpötilavaihteluita, tärinää ja muita häiriöitä paremmin kuin toimistoympäristöön sijoitetut laitteet. Reitittimet ja toimistoverkon puolella olevat laitteet voivat olla lähempänä normaaleja toteutusvaatimuksia.

Automaatiolaitteiden yhteyteen on nykyisin liitetty graafisia käyttöliittymäpaneeleita, joilla laitteiden tilaa voidaan seurata helpommin. Sama tieto voidaan näyttää SCADA-sovellusta pyörittävän tietokoneen näytöillä yhdistettyinä muiden järjestelmässä käytössä olevien ohjainten tietoihin. Laitteiden, esimerkiksi kytkinten, on kestettävä toimistoympäristön laitteita paremmin teollisuusympäristössä esiintyviä rasitteita, kuten likaa ja erilaisia häiriöitä.



Kuva 4 Ohjelmoitavien logiikkakontrollereiden työskentely-ympäristö [3].

Logiikkakontrollerit ohjelmoidaan yllä olevan kuvan 4 mukaisella ympäristöllä laitetoimituksen mukana toimitettavalla ohjelmistopaketilla ja sarjaliitynnällä. Ohjelmointitapoja on laitteistotoimittajasta riippuen useita ja esimerkiksi Siemens-laitteita ohjelmoidaan Step7-kielellä, jonka käyttäminen on yhdistelmä erilaisia ohjelmointimalleja. Kontrolleria ohjelmoiva henkilö voi itse valita oman taustansa mukaisen ohjelmointitavan, esimerkiksi: ”ladder”-tavan, jossa tapahtumat kuvataan tikapuumaisessa järjestyksessä (ajateltu sopivan perinteisemmille sähköinsinööreille), ”statement list”-tavan, jossa sovellus ajetaan määrittelytiedostomaisella kuvauksella (ajateltu sopivan ohjelmistotekniikkataustaisille ohjelmoijille) tai toiminnallisen ”block diagram”-tavan, jossa ohjelmointi tehdään loogisten komponenttien avulla (ajateltu sopivan piirisuunnittelutaitoisille ohjelmoijille). Kuvassa 4 on havainnollistettu yllä mainittuja ohjelmointimalleja.



Kuva 5. Ohjelmointimalleja on kolme. Työkalu luo projektin valitun ohjelmointimallin mukaisena. Ohjelmointitapaa voi vaihtaa kesken projektin [3].

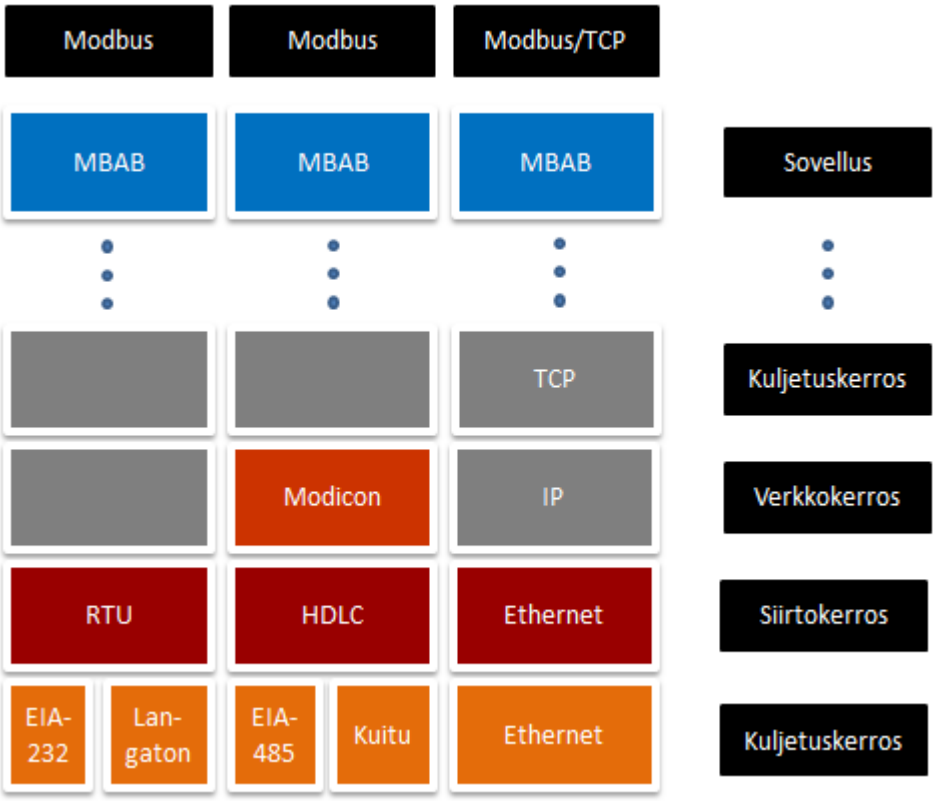
2.6 SCADA-protokollat

SCADA on tietojen keräys- ja ohjausjärjestelmä (Supervisory Control and Data Acquisition). Se on tietokoneavusteinen ohjaustiedon hallintajärjestelmä, joka voisi olla hitaasti kehittymässä kohti Internet of Things -tyyppistä toimintaa. Nykyisin paljon keskusteluissa esiintyvät pilvipalvelujärjestelmät eivät kuitenkaan suoraan sovi niille suorituskyvyn kohdalla olevan epävarmuuden vuoksi.

SCADA-järjestelmät tarvitsevat mieluiten viiveetöntä tiedonsiirtoa, jossa jokainen paketti kulkee lähettäjältä perille ja siksi esimerkiksi UDP ei oikein sovellu järjestelmään. SCADA käyttää sille määriteltyjä protokollia ohjausviestien siirtämiseen laitteiden välillä. Automaatioverkoissa on käytössä useita eri protokollia, mutta yleisemmät niistä Internet-hakujen mukaan ovat: Modbus, DNP3, Ethernet, PROFIBUS ja Foundation Fieldbus.
Protokollan valinta riippuu paljon sekä käyttäjän vaatimuksista, että teollisuuden asettamista määritelmistä. Teollisuuden asettama määritelmä voi olla esimerkiksi laitteistotoimittaja. PROFIBUS [4] on automaatiosovelluksille tehty kenttäväylä, josta on tarjolla erilaisia toteutuksia eri tuotantoympäristöihin, esimerkiksi: prosessiautomaatio (Profibus PA), tehdasautomaatio (Profibus DP), liikkeenohjaus ja turvallisuussovellukset. Sähkölaitoksen järjestelmässä saatetaan kuitenkin valita käytettäväksi protokollaksi

DNP3, koska sen avulla keskuskoneella järjestelmää valvova käyttäjä voi seurata esimerkiksi sensoreiden, jännitemittareiden ja muuntajien tiloja [4].

Mainituista protokollista yleisesti on käytössä myös Modbus-protokolla tai jokin sen variaatioista, jolla on hyvä hallita master-slave-suhteessa olevia ohjelmoitavia PLC-laitteita. Tällaisesta suhteesta voidaan mainita esimerkkinä HMI ja PLC. Siemens PLC:t ja RTU:t ovat teollisuudessa tunnettuja tuotteita ja ainakin osa niistä käyttää keskinäiseen kommunikointiin PROFIBUS-protokollaa. PROFIBUS-protokollan kehittänyt Modicon (nykyisin Schneider Electric) kehitti sen yksinkertaiseksi ja julkisti määrittelydokumentit. Sen sijaan osa laitteistosta käyttää PROFINET:ia, joka on teollisuuteen tarkoitettu Ethernet-protokolla. Joissakin Siemensin automaatiolaitteista on myös etähallintatuki, joten niiden tietoturvaa on mielenkiintoista käsitellä.



Kuva 6. MODBUS prokokollaperheen OSI-kerrosmalli. Muokattu viitteestä [4].

Alkuperäinen protokolla oli vain kahden kerroksen sarjaliikennepino. Kun uudempia kuljetuskerroksia tuli saataville, protokollasta julkaistiin niitä tukevia versioita. MODBUS ja sen muunnelmat, kuten MODBUS/TCP on suosittu, koska tässä protokollassa ei ole lisenssimaksua, vaan sen saa käyttöönsä helposti ja se siirtää tietoa rajoituksetta. Yhteinen tekijä protokollaversioille on seitsemännen OSI-tason asiakas/palvelimen komentorakenne: MBAB (Modbus Application Protocol). Tiedon pyytämistä ja siirtoa varten käydään varsin yksinkertainen keskustelu. Siinä asiakas, esimerkiksi käyttöliit-

tymälaite lähettää request-viestin PLC-laitteelle pyytääkseen jonkin asian arvoa ja aloittaakseen tiedon siirron. PLC vastaa reply-viestillä ja pyydetyllä tiedolla.

MODBUS ja ainakin sen vanhemmat versiot ovat alttiita tietoturvahyökkäykselle, koska se esimerkiksi kuljettaa tiedon selväkielisenä eikä se tue autentikointia. Järjestelmien tietoturvan tason alhaisuudesta johtuen ne ovat alttiina lukuisille hyökkääjätahoille, kuten haittaohjelmien levittäjille, haavoittuvuuksien etsijöille ja vakoilijoille. Oikein kohdennettu hyökkäys voi lisäksi aiheuttaa sen, että joku ulkopuolinen taho saa jonkin järjestelmän laitteista hallintaansa ja muutettua sen toimintatapoja haitallisesti tai jopa pysäytettyä koko tuotannon. Hyökkäysten vaikutuksia käsitellään tarkemmin luvussa ”Hyökkäysten vakavuudet”.

MODBUS ei ole ainoa tietoturvaongelmallinen protokolla, jota käytetään automaatiolaitteiden kommunikoinnissa. Siemens S7 laitteet ovat nykyaikaisia logiikkakontrollereita, jotka käyttävät PROFINET-protokollaa. PROFINETin etuja on, että sen avulla voidaan käyttää tuhansia PLC-laitteita yhtäaikaisesti keskitetysti yhdeltä tai muutamalta tietokoneelta käsin, mutta siitäkin on löydetty tietoturva-aukkoja, joiden avulla laitteen toimintaan saatetaan päästä käsiksi. Yksi tällainen tapaus käsitellään luvussa 5.3 Hyökkäys Siemens Simatic S7 PLC-laitteeseen. Tällä on suuri kustannusvaikutus teollisuudessa. Protokolla tukee Ethernetiä, HART, ISA 100 ja 820.11-protokollia sekä vanhempia väyliä.

2.7 Ethernet ja TCP/IP työkaluina

Ethernet tarjoaa mahdollisuuden suuriin kaistanopeuksiin, pitkiin etäisyyksiin laitteiden välillä sekä yhteensopivamman tiedonsiirron ja arkkitehtuurin. Vaihtoehtona se on kuitenkin haasteellinen, koska sen mukana tulee muun muassa tarve toimittaa tietoa luotettavasti laitteelta toiselle, valvontaohjelmistoille sekä tuotannonohjaukseen. Ongelman muodostaa tarve pitää mahdollisimman pienet viiveet tiedon kulussa samalla, kun sen tulee olla erityisen virheetöntä. TCP-protokolla tukee kyllä vikasietoisena vaihtoehtona toista näistä vaatimuksista, muttei ole kovin nopea eikä takaa tasaista tiedonsiirtonopeutta. Sen sijaan esimerkiksi virtauttamisessa käytetty UDP-protokolla palvelee nopeammin, mutta ei estä tiedonsiirrossa tapahtuvia virheitä.

On siis valittava tarkkaan, mihin käyttöön Ethernet-yhteyttä teollisessa automaatiokokoonpanossa voidaan käyttää. Teollisuustilojen ympäristöluonne eroaa toimistotiloista usein merkittävästi siinä, että laitteiden ympärillä on enemmän erilaisia häiriöitä. Yleisimmät verkon häiriöt teollisessa ympäristössä ovat: jatkuva altistus lialle, suuret lämpötilavaihtelut ja voimakas tärinä. Ethernet-verkkoa rakennettaessa siihen tulee liittää kaikki edellä mainitut häiriöt sietävä kytkin. Ethernet tarjoaa perinteisiin automaatioväyliin verrattuna muun muassa nopeamman tiedonsiirron, mutta vastaavasti satunnaiset viiveet ja virheet muodostavat haasteen, joka pitää osata voittaa ennen verkon

integroimista liian syvään automaatioverkkoon. Lisäksi Internetiin kytketyt laitteet tulee suojata tietoturvan kannalta riittävän hyvin, kuten toimistoympäristössä. Koska täydellistä eristämistä Internetistä ei kuitenkaan haluta tehdä, suojauksen tulee sijaita verkon muissa osissa, esimerkiksi haittaohjelmia skannaavissa laitteistoissa tai sovelluksissa sekä huolellisessa verkkosuunnittelussa.

3 YLEISIMMÄT UHKAT JA HAITAT

Luvussa käydään läpi, millaisia tietohyökkäyksiä verkkoihin usein kohdistuu ja millä motiivilla. Lisäksi käsitellään, mitä haittoja hyökkäyshaavoittuvuuksista mahdollisesti seuraa. Ethernetiin kytketty automaatioverkko on avoin suuressa määrin samanlaisille hyökkäyksille, kuin mikä tahansa tietoverkko. Suurin altistaja uhkan muodostumiselle on yrityksen oman sisäverkon kytkeminen automaatioverkon kanssa yhteen, koska myös yrityksen toimistopäätelaitteet ja tabletit saattavat sen jälkeen tuoda haittaohjelmia verkon automaatiolaitteiden yhteyteen. Riski on todellinen, koska teollista automaatiota varten rakennetut ohjelmistot sekä laitteistot saattavat sisältää vanhentuneita osia sekä huonoa tietoturvatasoa, kuten telnet-yhteyden ilman salasanaa. Niihin usein sisältyy paljon tietoturva-aukkoja, ellei vähintään ole pidetty huolta tietoturvapäivityksistä. Usealla yrityksellä on käytössään MS Windows-käyttöjärjestelmä. Windows XP on ollut yksi suosituimmista, mutta pitkään myös eräs haavoittuvimmista käyttöjärjestelmistä. Vaikka Windows-järjestelmistä silloin tällöin löytyykin uusia haavoittuvuuksia, jotka korjaantuisivat päivityksellä, yritykset eivät mielellään keskeytä toimintaansa, ellei päivityksen laiminlyönnistä seuraa välitöntä haittaa.

Mikäli tietoverkon kytkemistä yrityksen verkkoon sekä Internetiin ei toteuteta tietoturvasta huolehtien, siihen saatetaan vaikuttaa esimerkiksi palvelunestohyökkäyksillä, etähallintaohjelmilla, tehdä hiljaista näkymätöntä teollisuusvakoilua tai aiheuttaa vahinkoa suoraan tuotantojärjestelmään tai tehtyihin tuotteisiin. Aina sekään ei riitä, sillä kuka tahansa laitetoimittaja saattaa julkaista valvontaohjelmiston sisällä haittaohjelman. Tällaisesta uhasta on esimerkkinä muun muassa Stuxnet sekä vuonna 2012 löydetty automaatiojärjestelmiin asennettu takaportti, jolla mahdollistettiin pääsy jopa huoltovarmuuskriittisiin järjestelmiin. Teollisuusautomaatiojärjestelmää ei siis voi suojata pelkästään valvomalla ja rajoittamalla sen Internet-yhteyksiä, vaan suojauksissa tulisi olla vieläkin tarkempi ja ottaa huomioon myös laitetoimittajien ohjelmistojen riskit sekä perinteisemmät hakkerointitavat, kuten social engineering, jossa tietoja hankitaan tekeytymällä joksikin asianmukaiseksi henkilöksi.

3.1 Tietoturvaheikkouksien laittomia käyttökohteita

Tietoturvauhkien suurimmat hyödyntäjät suunnittelevat tekemisensä ammattimaisesti ja ovat verkostoituneita muiden hyödyntäjien kanssa. Liikkeellä on varmasti myös ideologisista syistä toimivia tahoja, mutta pääosin toiminnan motiivi tuntuu kytkeytyvän erilaisiin ansaintalogiikoihin. Monenlaisten osaajien verkostossa toimivat tahot tarjoavat toisilleen palveluita saaden vastineeksi joko palveluita tai rahaa. Kuvan mustat nuolet

kuvaavat palveluita, punaiset kuvaavat rahaa. Muulien kohdalla on erikoistilanne, jossa katkoviivalla on kuvattu tilannetta, jossa muuli ei saa rahaa. On järkevää olettaa, että myös näiden nuolien lisäksi kulkee rahavirtoja, mutta kuvaa on yksinkertaistettu niiltä osin selkeyden vuoksi. Alla olevan kuvan lisäksi erilaisia tietoturva-aukkojen hyödyntäjiä ovat olla myös laittomien, muun muassa varastettujen tavaroiden kauppaajat, rikollisjärjestöt sekä vakoilu- ja terroristiorganisaatiot.

Kuva 7. Rikollisten toimijoiden palveluiden ja rahavirtojen vuorovaikutus. Mustat nuolet kuvaavat palveluita, punaiset nuolet rahavirtojen suuntaa [5].

3.1.1 Rikollisesti hankitun tiedon myyntikanavat

Rikollisin keinoin hankitun tiedon myynti vaatii omat markkinansa ja markkinointikanavansa [5]. Markkinointipaikan suhteen rikollisen tahon ongelmana on turvallisen markkinapaikan löytyminen, jossa omaa henkilöllisyyttään voi varjella. Lisäksi ongelmana on se, että myös kauppakumppanina on rikollinen toimija, joten oikein mihinkään ei voi luottaa. Koska myyjä ei voi luottaa ostajaan eikä ostaja voi luottaa myyjään, julkinen laillinen kauppapaikka ei ole tarpeeksi riskitön käyttää. Laillisten palveluntarjoajien käyttöä voi harkita, jos tarkoituksenomaisen sivuston sijainti on esimerkiksi ulkomailla. Lisäksi rikollisilla voi olla käytössään virtuaalipalvelimia tai muita suojattuja ympäristöjä, joiden käyttöehdot eivät ole rajoitteena laittomalle toiminnalle.

Vaihtoehtoinen rikollisesti hankitun tiedon myyntikanava on suojattu ympäristö, jossa tiedon jakaminen tehdään esimerkiksi Freenetin [6] tai vastaavalla sovelluksella. Sovellus mahdollistaa tiedostojen jakamisen ja sivujen julkaisun omassa erillisenä pysyttelevässä verkossaan. Toinen suosittu ja paljon julkista keskustelua herättänyt ympäristö on TOR-verkot [7], joiden suojausominaisuus perustuu reititystekniikkaan. Siinä paketit kuljetetaan satunnaisten reittien ja solmujen kautta kohteeseen, jolloin viranomaisten on vaikea selvittää tiedon lähettäjiä ja vastaanottajia. TOR-verkkoihin perustuvia toteutuksia on myös Suomessa, esimerkiksi Thorlauta ja Sipulilauta.

3.1.2 Bottiverkko

Internetiin kytketyt automaatiolaitteet ovat alttiita tietohyökkäyksille ja rikolliselle verkostolle yhtä paljon kuin muutkin Internetin käyttäjät, jos verkko on suojattu huonosti tai jos laitteiden ohjelmisto on vanhentunutta. Laitteiden ohjelmiston ja tietoturvatason vanhentuminen on todellinen riski toimistoverkkoon verrattuna, koska niitä ei aina voida päivittää kuin pääasiassa suurempien kunnossapito- tai muutostöiden yhteydessä. Eräs rikollinen toimintamalli on bottiverkko, jota voidaan hyödyntää muun muassa palvelunestohyökkäystä toteutettaessa [8]. Palvelunestohyökkäyksen vaikutuksen suurin saavutettava tehokkuus perustuu ominaisuuteen, jossa toimintaa voidaan nimenomaan hajauttaa. Mallissa hyökkääjien saastuttamia koneita yritetään saada hyökkäystä varten yhtäaikaisesti saman tahon hallintaan mahdollisimman monia [5]. Hyökkääjät voivat ensin ottaa koneen haltuunsa esimerkiksi näppäimistön toimintoja tallentavalla troijalaisella (keylogger), joka on levinnyt murretulta web-sivulta tai sähköpostiohjelman liitteestä levinneellä sovelluksella.

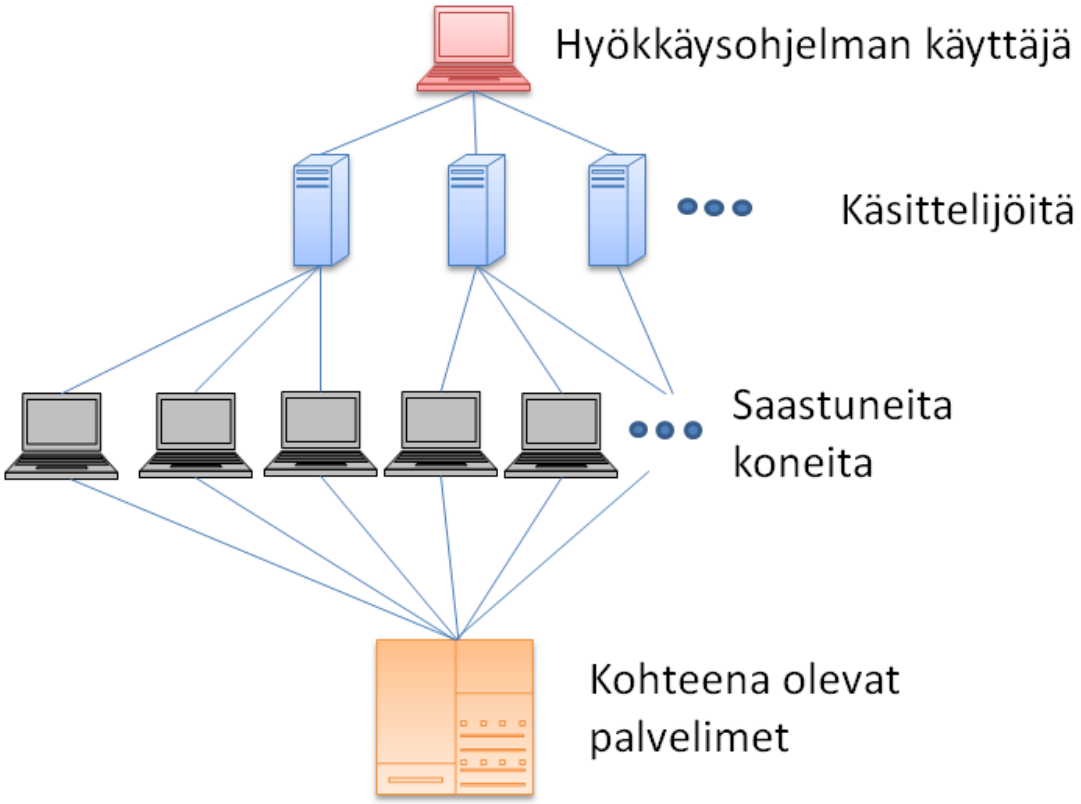
Kun saastutettuja koneita on tarpeeksi, niistä voidaan muodostaa verkko hajautettuja palvelunestohyökkäyksiä varten. Rikollisen toimijan ansaintalogiikka perustuu mahdollisuuteen kiristää yrityksiltä rahaa, koska hyökkäyksellä voidaan lamauttaa yrityksen oman verkon laitteiden toiminta tai tietoliikenne hyvin tehokkaasti. Bottiverkolla on mahdollista myös vaikuttaa hakukoneiden tuloksiin ja tehdä petoksia sekä identiteettivarkauksia. Jos palvelunestohyökkäys esimerkiksi kohdennetaan reitittimeen, sillä voidaan myös muuttaa reititystä tai haitata muuten tietoliikennettä.

3.1.3 Palvelunestohyökkäys

Palvelunestohyökkäyksellä tarkoitetaan sellaista hyökkäystä, jolla pyritään tukkimaan kohteen Internet-yhteys ja estetään siten verkon välityksellä tapahtuva tiedon kulku [1]. Jos esimerkiksi SCADA-ympäristön loki tai tietokanta sijaitsee pilvessä, yhteyden käyttökatkoksen vaikutukset voivat olla vakavia. Jos sen sijaan jopa SCADA:n käyttämien automaatioreseptien saatavuus tai etäohjausyhteys katoaa sopivasti, saattaa yritys joutua pysäyttämään tuotantonsa hetkeksi, tai se ei muutoin saa korjattua tilannetta. Kustannusvaikutukset alkavat siitä, että yrityksen täytyy tilata korjaaja menemään paikanpäälle. Korjaajan veloituksesta suoraan aiheutuvien kustannusten lisäksi hyökkäyksestä aiheutuu tällaisessa tapauksessa myös viivettä suhteessa etähallintaan ja menetettyä tuotantoaikaa.

Alla oleva kuva havainnollistaa bottiverkon avulla tehtyä palvelunestohyökkäystä perinteisellä tietokone-esimerkillä. Kuvaus on hyvin yleistävä, koska hyökkäysmalleja on useita erilaisia, esimerkiksi: verkko-/kuljetuskerroksen flooding-hyökkäykset, joita tehdään pääosin TCP-, UDP- tai ICMP-protokollalla. Toiseksi on olemassa protokollan hyödyntämiseen perustuvat flooding-hyökkäykset, jotka perustuvat siihen, että hyökkääjä hyväksikäyttää protokollan erityisominaisuutta tai toteutukseen jäänyttä viallista

toiminnallisuutta, esimerkiksi: SYN-, TCP SYN-ACK-, ACK ja PUSH ACK-, RST/FIN-flood-hyökkäystä ja niin edelleen. Lisäksi voidaan tehdä vastausviesteihin perustuvia hajautettuja palvelunestohyökkäyksiä, jolla kohteen liikenne tukitaan pakottamalla se vastaamaan useasta lähteistä tuleviin muokattuihin ICMP echo request –viesteihin. [9].



Kuva 8. Hajautettu bottiverkon avulla tehty palvelunestohyökkäys DDoS. Tällaisessa hyökkäyksessä lähteitä on useita, jolloin useat bottiverkon muodostavat saastutetut koneet tuottavat niin paljon liikennettä kohteessa, että se ei enää kykene käyttämään yhteyksiään oman tarkoituksensa mukaisesti [1] [9].

Kuvassa 8 on hyökkäävän tahon lisäksi käsittelijöitä, joiden avulla hyökkääjätaho voi ohjata epäsuorasti bottiverkkonsa saastuneita koneita. Käsittelijöitä voivat olla esimerkiksi palvelimilla pyörivät haittasovellukset. Niissä on se ongelma, että sovellukset voidaan löytää haittaohjelmia paljastavilla ohjelmilla. Siitä syystä hyökkääjät usein käyttävätkin muita keinoja ohjatakseen bottiverkkoaan.

Yksi tällainen tapa on käyttää esimerkiksi IRC-palvelua [10]. IRC on tekstipohjainen keskusteluohjelma, jolla on asiakas-palvelin-arkkitehtuuri ja oletuksena kanavia, joiden avulla voidaan kommunikoida palvelinten välillä. IRC voi yhdistää satoja käyttäjiä muutamiin palvelimiin. Hyökkäystavan etuna on lisäksi se, että hyökkääjällä on mahdollisuus lähettää komentojaan IRC-portteihin, jolloin sen komentoviestejä on vaikeaa havaita muiden IRC-palvelinten runsaan viestiliikenteen seasta. Hyökkäystavassa on kuitenkin se vika, että hyökkäykseen käytettävä IRC-palvelin on myös niin sanottu sing-

le-point-of-failure. Jos kohteena ollut osapuoli saa palvelimen alas, koko hyökkäys saadaan lopetettua. [9].

Palvelunestohyökkäys voidaan siis toteuttaa myös hajautettuna eri tavoin, jolloin liikennettä saadaan aikaiseksi enemmän. Pakettien lähteen väärentäminen on tavallinen tapa hyökätä hajautetusti, mutta siihen voidaan yhdistää myös liikenteen määrää nopeasti kasvattavia ominaisuuksia. Suuren ongelman muodostavat myös sovellustason hyökkäykset, koska niiden jäljittäminen on vaikeampaa. Lyhyesti selitettynä, sovellustasolla toimittaessa pyritään vähentämään palvelinten resursseja.

Hyökkäystä suunnittelevalla taholla on käytössään lisäksi erilaisia HTTP-hyökkäyksiä, esimerkiksi: HTTP request-viestien hyödyntäminen siten, että uhrina olevalle Web-palvelimelle lähetetään bottiverkon avulla get/post-viestejä. Toisaalta hyökkäyksen voi tehdä myös asymmetrisesti lähettämällä kohteelle useita pyyntöviestejä asetettuna yhden paketin sisään, joissa pyydetään suuria määriä tietoa. Matala lähetettävien pakettien määrä auttaa hyökkääjää pysymään itse piilossa.

Näiden tapojen lisäksi voidaan edelleen laittaa kohteena oleva palvelin itse työskentelemään oman tietokantansa kanssa esimerkiksi SQL-injektiohyökkäyksellä. Palvelimen voi saada alas myös lähettämällä osittaisia HTTP-pyyntöjä, jotka kasvattavat yhteyksien määrää nopeasti, mutta päivittyvät hitaasti eivätkä sulkeudu ollenkaan. Hyökkäys jatkuu, kunnes palvelimen kaikki vapaat yhteydet ovat käytössä. [9].

Koska teollisuudessa tilanne on usein sellainen, että siedettävät toimintakatkoksen aikarajat tulevat hyvin nopeasti vastaan, käytännössä millään automaatioverkolla ei ole varaa joutua tämänkaltaisen hyökkäyksen kohteeksi. Ei, vaikka automaatioverkon laitteet liikennöivätkin keskenään usein eri protokollilla kuin PC-tietokoneet. Verkkoa suunnitellessa on harkittava hyvin tarkkaan, mitä laitteita teollisesta verkosta voi olla yhteydessä Internetiin ja millaisin tarkoituksin.

3.1.4 Roskapostit ja tiedon kalastus

Tiedonhankintamenetelmää, jossa käyttäjä saadaan itse luovuttamaan hyödynnettävää tietoa rikolliselle taholle joko tietäen tai tietämättään sanotaan usein verkkourkinnaksi tai tietojen kalastukseksi. Yleinen tapa tehdä verkkourkintaa on lähettää kohdetaholle sähköposti, joka näyttää viralliselta palveluntarjoajan postilta. Postissa oleva toiminnallisuus ohjaa sähköpostin lukijan antamaan käyttäjätietoja, salasanoja tai muuta tärkeää tietoa postin lähettäjätaholle samalla kun postin lukija luulee asioivansa verkkopankissa tai muussa tutussa verkkopalvelussa [5].

Tietojen kalastusta tehdään paljon sovelluksilla, jotka tallentavat tietoa käyttäjän tekemisistä. Virallisten huijauspostien lisäksi rikolliset tahot keräävät tietoja myös roskaposteilla, jotka levittävät erilaisia haittaohjelmia. Koska sähköpostiliitteenä kulkevat sovel-

lukset ovat nykyisin aika huomiota herättäviä, ihmiset pyritään mieluummin ohjaamaan haitallista koodia sisältävälle sivustolle. Sivustolla oleva sovellus saattaa asentaa huonosti suojattuun koneeseen esimerkiksi sovelluksen, joka tekee vierailevasta koneesta roskapostipalvelimen.

Tämä tietoturvauhka ei liity ainoastaan perinteisillä tietokoneilla hyödynnettävään yrityksen tietoverkkoon, vaan huonosti ylläpidetyt ja suojatut tietokoneet saattavat aiheuttaa uhkan myös automaatiolaitteiden tietoturvalle. Vaikka automaatiolaitteistot olisivat kohtuullisesti suojattuja, niin niihin yhteydessä olevat tietokoneet saattavat muodostua riskiksi. On olemassa uhka, että yrityksen tietokoneiden kautta rikollisen tahon tietoon kulkeutuu dokumentaatiota, jonka avulla päästään vaikuttamaan yrityksen automaatiokontrollereiden toimintaan.

3.1.5 Epärehelliset palveluntarjoajat

Mistä kaikki haittaohjelmien käyttäjät sitten saavat sovelluksensa? Missä näitä sivustoja ylläpidetään ja miksi niitä ei ajeta alas viranomaisten toimesta? Sivuston ylläpitäjäksi voi ryhtyä kuka tahansa, koska sivuston ylläpitoon tarvitaan ainoastaan verkkotunnukset (domain). Tunnukset voidaan rekisteröidä miltä tahansa nimipalvelua tarjoavalta taholta rikkomatta lakia.

Epärehelliset rekisteröijät sekä palveluntarjoajat ovat suljettavissa, mutta ei kovin tehokkaasti. Vastaavasti ICANN voi purkaa rekisteröijän oikeuden myydä verkkotunnuksia tarvittaessa, mutta siihen ei yleensä ryhdytä, vaan useammin pyydetään Internet-palveluntarjoajaa sulkemaan laiton sivusto oikeuden päätöksellä. Joskus palveluntarjoaja ei suostu sulkemaan sivustoa ja joudutaan sulkemaan itse palveluntarjoaja. Palveluntarjoajan sulkeminen tapahtuu lopettamalla yhteistyö ja sopimukset rikollisen palveluntarjoajan kanssa. Esimerkkinä voidaan mainita Russian Business Network, joka tarjosi hyökkääjille tilan hyökätä ulkomaisia yrityksiä vastaan [5].

3.1.6 Maksunvälittäjät

Rikollisin keinoin hankitun rahan alkuperä piilotetaan yleensä käyttämällä rahan pesemistarkoitukseen hankittuja toimijoita, eli maksunvälittäjiä. Maksunvälittäjä, eli muuli on siis henkilö, jonka tehtävänä on vastaanottaa rikoksella hankittua omaisuutta ja toimittaa se ketjussa eteenpäin, esim. toiseen valtioon [11]. Muulit eivät kuitenkaan välttämättä tiedä toimivansa rahan pesijöinä, vaan saattavat olla tietämättään mukana rikollisessa kaupankäynnissä. Ansaintatarkoituksessa toimivat ihmiset voivat siksi kiinni jäädessään vedota siihen, etteivät tienneet kaupankäynnin toisen osapuolen rikollisista tarkoitusperistä, vaan toimivat niin sanotusti hyvässä uskossa.

3.2 Viranomaiset laillistettuina tiedonkerääjinä

Tietoa kerätään ja tietoliikennettä valvotaan myös laillisesti esimerkiksi eri maiden viranomaisten toimesta. Viranomaisten tarkoituksena on tutkia rikoksia, ennaltaehkäistä erilaisia tietoturva-aukoista johtuvia uhkia sekä käyttää kerättyä tietoa yleiseen hyötyyn sekä kansallisen turvallisuuden vuoksi. Koska valvontaa varten tehdään yhteistyötä laitevalmistajien ja ylläpitäjien kanssa, tietoverkkojen käyttöä valvovalla taholla on vastuu siitä, ettei se samalla tee hallaa yleiselle tietoturvalle muun muassa avatessaan käyttöönsä uusia rajapintoja [12].

Viranomaiset valvovat yksityishenkilöiden lisäksi sekä oman, että muiden maiden yrityksien tietoliikennettä myös eri maiden välillä. Laajaa standardoitua valvontaa perustellaan maan turvallisuusnäkökohdilla, mutta lisäksi muun muassa tiedustelupalveluiden toimesta tehdään tahallisesti haittaakin ja on selvää, että osalla tahoista motiivina on myös teollisuusvakoilu. Yhdysvalloilla sekä muutamalla Euroopan maalla epäillään yleisesti olevan hankkeita, joilla kerätään automaattisesti tietoa kaupallisista järjestelmistä, mutta ei ole mitään syytä epäillä, ettei muillakin mailla olisi samanlaisia hankkeita.

Suomessa laillistettuna tiedon valvojana toimii Viestintävirasto, jonka tehtävänä on oman määritelmänsä mukaan valvoa yksityisyyden suojaa televiestinnässä sekä teletoiminnan tietoturvaa ja varautumista, selvittää ja kerätä tietoa verkkopalveluihin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä tiedottaa tietoturva-asioista. Viranomaisten käyttämät seurantalaitteiden sijainnit on suunnattu oletettavasti suurempien palveluntarjoajien ja maiden välisen liikenteen rajapinnoille, koska pienempien verkkojen seuraaminen olisi kalliimpaa ja tehottomampaa.

Liikenteen seuraamista varten viranomaiset käyttävät erikseen tarkoitusta varten määriteltyjä laitevalmistajien jättämiä rajapintoja. Rajapinnan tarjoaja tai palveluntarjoaja ei välttämättä tiedä tästä ominaisuudesta. Salassapitoa perustellaan viranomaisten tarpeella säilyttää toimintansa näkymättömyys. Vaikka toteutuksesta ei välttämättä kerrota, ainakin viralliset rajapinnat noudattavat ETSI, IETF tai 3GPP standardeja, joihin ne on julkisesti määritelty. Viranomaisrajapintoja pyritään saamaan osaksi standardeja valtioiden välisellä lainsäädännöllä, esimerkiksi Euroopassa [12] [13]. ETSI ja 3GPP määrittelydokumenttiin on määritelty muun muassa toimintamalli liikenteen kuuntelemista, uudelleenohjausta ja signalointiviestien lähettämistä varten viranomaisrajapinnan kautta [14].

Viranomaisten tarkkailun toimintamallista ainakin osa on standardoitu ja siitä on olemassa määritellyt vaiheet. Suomennetut vaiheet ovat seuraavat:

- Vaihe 1: Tarkkailtavan yhteyden aikana siirretty tieto kerätään
- Vaihe 2: Kerätty tieto muunnetaan standardiin muotoon
- Vaihe 3: Muunnettu tieto välitetään viranomaiselle

Standardoidussa muodossa tieto on tehokkaampaa käsiteltävää, koska se siten mahdollistaa tiedonkäsittelyn automatisoinnin, jolloin saatua dataa voidaan kattaa suurempia määriä. Tästä on suurta hyötyä, koska maailmalla kulkee yhä enemmän dataa, jota viranomaisten pitäisi pystyä kuuntelemaan.

Viranomaisrajapintojen standardointi siis tehostaa viranomaisten valvontaa, mutta samalla mahdollistaa myös sen, että jokainen laite, joka on toteutettu standardien mukaan, sisältää rajapinnat. Tästä seuraa, että myös kuka tahansa aiemmin määritelty verkkorikollinen voi hyödyntää näitä rajapintoja eikä rajapintoja voida poistaa laitteista standardointimääräyksiä rikkomatta. Turvallisuudestaan huolehtiva yritys voi kuitenkin suojautua aika pitkälle rajaamalla verkkoyhteydet pois laitteidensa ulottuvilta, ellei niihin ole piilotettu suoraan omia verkkopalveluita. Jos viranomaiset saavat ulotettua rajapintansa laillisesti verkkopalveluihin, käytännössä siitä muodostuu tilanne, jossa viranomaiset antavat myös verkkorikollisille parannetun mahdollisuuden hyödyntää viranomaisrajapintoja. Vaihtoehtoisesti, koska yritykset parantavat jatkuvasti tietoturvaansa sulkemalla verkkoyhteyksiään ja käyttämällä yhä paranevia salauksia, sekä viranomaisten, että muiden tiedonkulkua seuraavien tahojen on muutettava toimintamalliaan tiedon saamiseksi.

3.3 Automaatiolaitteiden näkyvyys Internetissä

Teolliseen verkkoon kytketyt automaatiolaitteet on usein suojattu hieman heikosti eikä niiden käyttämiä yhteyksiä välttämättä salata. Tälle saattaa olla useita erilaisia syitä, kuten muun muassa se, että sekä yhteydet että ylipäänsä kaikki toiminta halutaan pitää mahdollisimman vikavapaana ja viiveettömänä. Lisäksi ei tiedosteta salaamattomuuden ja piilottamisen uhkia. Laitteiden suojauksiin tehdään jatkuvasti parannuksia, mutta parannukset aiheuttavat joskus uusia virheitä. Havaitsematta jääneet virheet saattavat kuitenkin tulla löydetyiksi hyökkääjien keskuudessa jo ennen laillisen tahon havaintoa. Tällöin puhutaan rikollisten tahojen kannalta erittäin arvokkaasta nollapäivähaavoittuvuudesta. Siinä vian korjaus ei ole vielä alkanut, mutta haavoittuvuus on jo hyödynnettävissä.

Aalto-yliopiston tutkijat Seppo Tiilikainen ja Jukka Manner löysivät vuoden 2013 tammikuussa 2915 Suomessa sijaitsevaa automaatiolaitetta, joihin he olisivat pystyneet ottamaan yhteyden yleisen Internetin avulla [15]. Tutkimuksen tarkoitus oli kartoittaa, kuinka paljon kriittisiä SCADA-, kontrolli- ja tehdasautomaatiojärjestelmiä on löydettävissä ja kuinka monesta laitteesta löytyy tunnettu haavoittuvuus. Maaliskuussa tutkijat tekivät seurantaa tilanteesta ja havaitsivat, että osa laitteista oli poistettu Internetistä.

Laitteiden löytäminen siihen tarkoitetun palvelun avulla on helppoa, mutta siihen toimii myös perinteisemmät haittaohjelmat. Aikaisemmin hyökkääjien käytössä olivat muun

muassa Neosploit, Gumblar ja Luckysploit. Mutta koska ne ovat poistuneet jo käytöstä, yksi tapa tehdä hyökkäys on hakkeroida esimerkiksi myöhemmin käsiteltävällä Shodanilla löydetty haavoittuvuuden sisältävällä web-palvelimella sijaitseva sivusto. Hyökkääjätaholla on mahdollisuus piilottaa haavoittuvaan sivustoon esimerkiksi linkki omalle sivulle iFrame:n avulla tai levittää haittaohjelmaa esimerkiksi tekemällä haavoittuneesta tahosta roskapostipalvelimen. Perimmäisenä tarkoituksena on saada mahdollisimman monta päätelaitetta haavoitettua ja sitten myydä tietoa sitä tarvitseville rikollisille tai valtiollisille tiedon ostajatahoille, vaikkei hyökkäystä olisikaan itse tarkoitus viedä pidemmälle. Markkinoilla ei varsinaisesti toimita avoimesti eikä luottamusperiaatteella, joten on selvää, että hankitut tiedot myydään monelle taholle ja niitä saatetaan silti hyödyntää itse ensin.

Hyökättyjä koneita voi hyödyntää esimerkiksi tekemällä niistä bottiverkko tai tutkimalla niiden avulla, mitä mahdollisuuksia haavoittuvuudet tuovat rikolliseen käyttöön. Rahavirrat kulkevat Shodanin lisäksi myös muissa haavoittuvuuksia etsivissä sovelluksissa, joista esimerkkinä Neosploit, joka tarjosi maksullisena palveluna käyttäjätukea sovellukseensa ja Shodanin mahdollisuus ostaa kattavampi käyttölisenssi.

3.3.1 Automaatiolaitteiden löytäminen

Automaatiolaitteiden näkyvyyttä voidaan tutkia tällä hetkellä tehokkaasti esimerkiksi Shodan-työkalulla [16], joka toimii ikään kuin se olisi Intrusion as a Service. Shodan on Internetissä toimiva web-käyttöliittymällä tai ohjelmointirajapinnalla käytettävä palvelu, joka itsenäisesti suorittaa satunnaista koko Internetin laajuista porttiskannausta lähettämällä kyselyitä eri IP-osoitteisiin. Tietoja kerätään eri maissa sijaitsevien palvelimien avulla, jotka tallentavat saamansa tiedon tietokantaan. Kyselyistä saadut vastaukset, eli tervehdysviestit tulkitaan ja tiedot tallennetaan julkiseen tietokantaan. Koska tietokantaa saa muokata vain Shodan ja koska kanta on julkinen, sitä voidaan pitää melko luotettavana.

Skannauksen kohteina on yleensä tunnettujen palveluiden portteja, kuten SSH (22) ja HTTP (80). Palveluita voidaan siis yleensä tunnistaa suoraan avoinna olevien porttien numerosta, kuten myös Telnet:n, FTP:n ja SNMP:n-tapauksissa.

Työkalussa voidaan asettaa hakusanoja sekä maa- ja IP-osoiterajoja. IP-osoiterajauksia käytetään esimerkiksi siihen, että voidaan rajata yhden yrityksen osoiteavaruus tutkittavaksi kerralla. Siten hakukoneen käyttäjälle paljastuu, millaisia laitteita yritys on kytkenyt tietoverkkoon ja samalla rajoitus auttaa selvittämään, millaisia hakutermejä voidaan hyödyntää. IP -osoitteita voidaan selvittää esimerkiksi hyödyntämällä RIPE tietokantaa. Hakujen tuloksista näkee suoraan myös arvioidun maantieteellisen sijainnin. Tietoja on saatavissa riippuen kohteista, mutta hakuja voi tehdä myös palveluperustaisesti.

Alla olevassa kuvassa on kuvakaappaus Shodanin Web-käyttöliittymästä, jossa esitellään erään automaatiolaitteen etähallintatoiminnallisuuden toiminnallisuuksien näkyvyyttä. Shodanin saama vastaus vahvisti laitteen olevan Siemensin valmistama Simatic ja siinä olevan myös VNC-palvelun portissa 5900. Palvelu on käytännössä etähallintaohjelma, joka mahdollistaa verkossa olevien palvelua tukevien laitteiden hallinnan toiselta tietokoneelta tai mobiililaitteelta. Laitteiden löytäminen ei siis vaadi kovin suurta työmäärää.

Kuva 9. Shodan kertoo, mitä palveluita laitteella on näkyvissä. Porttinumeroiden perusteella voidaan päätellä, että laitteella on todennäköisesti tunnettuja palveluita avoinna. Esimerkiksi VNC portissa 5900.

Shodan ei toki ole ainoa työkalu, jolla voidaan löytää Internetissä suojaamattomana olevia laitteita. Internetin laitteistoa voidaan skannata myös toisenlaisilla automatisoiduilla sovelluksilla, joita kutsutaan boteiksi [17]. Etsintään ja tiedon käsittelyyn tarvitaan tiedustelua, tiedon louhintaa ja prosessointia varten omat bottinsa, joiden toiminta voidaan hajauttaa lisää myös käyttämällä useampia palvelimia. Erilaisten bottien avulla voidaan löytää ja paljastaa haittaohjelmia käyttävien yhteisöjen piilotettuja verkkoja, joita ei löydä tavallisesti esimerkiksi Googlen hakukoneella. Botit käsittelevät tietoa hyödyllisempään muotoon ja toimivat lisäksi huomaamatta. Siksi myös botit ovat varteenotettava tapa etsiä piilossa olevia laitteita ja käyttäjiä. Tässä työssä keskitytään kuitenkin Shodan-palveluun sen saatavuuden ja käytettävyyden vuoksi.

3.3.2 Aiemmin tehty Shodan-tutkimus

Aalto-yliopiston tekemässä tutkimuksessa vuonna 2012 käytettiin hakupalveluna Shodania [16]. Se hakee Internetissä olevia laitteita ja tallentaa niistä saamansa tiedot julkiseen tietokantaansa. Oikeilla hakusanoilla ja rajoituksilla tietokannasta voidaan löytää muun muassa automaatiolaitteita, joihin on rajoittamaton pääsy eri tavoilla, vaikka varmasti näin ei pitäisi olla. Tammikuun tutkimuksessa löydettiin laitteita, jotka kuuluivat muun muassa sähkönhallinta-, rakennus- ja etäkäyttöautomaatiojärjestelmiin. Kokonaisuudessaan Suomesta löydettiin tuolloin 185000 HTTP-vastauksen antanutta laitetta. Tutkijoiden näkemyksen mukaan määrä oli tuolloin kasvussa eikä Shodan ollut vielä

skannannut kaikkia Suomen osoitteita. Löydetyistä laitteista noin 60%:iin liittyi yleisesti tiedossa oleva haavoittuvuus [15].

Tutkimuksessa löydettiin useita Siemens Simatic-laitteita, joihin pääsi kiinni Telnet-yhteydellä. Työn kirjoittamisen hetkellä määrä ei ollut nopeasti katselmoituna Suomessa juuri vähentynyt.

Taulukko 1. Tutkimuksen raportista löytyy useita erilaisia palveluita [15]:

Siemens Simatic laitteita: S7, HMI, NET: PLC-laitteita, valvontajärjestelmiä, automaatiojärjestelmän osien liityntä Internetiin etävalvonnalla.	Yhteensä: 8 kpl
Schneider TSX: Automaatioverkkojen kommunikaatiomoduleita.	Yhteensä: 12 kpl
Schneider Modicon Quantum, web-käyttöliittymä: PLC-laitteiden kontrolleri raskaan tason vaativaan automaatiokäyttöön.	Yhteensä: 6 kpl
clearScada: Scheiderin SCADA-palvelinalusta web-etäkäyttöliittymällä.	Yhteensä: 3 kpl
Pocket CMD-komentorivikäyttöliittymä telnet-yhteyden yli Windows CE käyttöjärjestelmälle. Käytetään mm. automaation hallinnassa.	Yhteensä: 8 kpl

Vertailun vuoksi Shodanin tietokannasta yhdistelemällä hakusanoja: ”HMI, XP277 country:"FI", saatiin tämän työn tekemisen aikoihin:

- 27 valvontalaitetta Suomessa, joista 7 kpl tuki Telnet-yhteyttä ilman salasanaa: Siemens, SIMATIC HMI, XP277

Alkuperäisen raportin hakusanat on sen tekijöiden mukaan luovutettu viranomaisille, joten täydellistä vertailua ei voida toteuttaa. Kokonaismäärä Internetissä näkyvistä suojaamattomista automaatiolaitteista oli vähentynyt havaittavasti jo saman vuoden aikana, sillä aiemmin tehdyn raportin mukaan laitteita oli näkyvillä 2915, mutta parin kuukauden jälkeen enää 1979. Tällä hetkellä näkyvillä olevia laitteita löytyi vain muutama sata kappaletta riippuen hakusanasta. Maailmanlaajuisesti automaatiojärjestelmien laitteistoja oli näkyvillä merkittävästi enemmän.

3.4 Uhka ilman Internetiä

Eräs vaarallisimmista uhkista on, että tuotantotiloissa oleva ihminen pystyy asentamaan matotyyppisen ohjelmiston, joka tekee haittaa tuotantolaitteiston automaatiolaitteiden toiminnalle, tai lähettää kerättyä dataa ulkopuoliselle taholle, esimerkiksi NSA:lle. Tällaisia hakkerointeja on tehty aiemminkin, kuten: STUXNET, Flame sekä viimeisimpänä löydetty sovellus, jota kutsutaan nimellä Energetic Bear tai Crouching Yeti. Siitä Kapersky kirjoitti raportin, jossa se selvittää hyökkääjien toiminnan tapahtumaketjua [18]. Sovellus aiheutti haittaa energia-alan toimijoille sekä puolustushallinnon alihankkijoille. Sovellus asennettiin suoraan laiteohjelmiston mukana. Haittaohjelman löysi Crowdstrike-yritys vuonna 2012. Ohjelma löydettiin ja korjattiin, mutta tämän kaltaisten sovellusten käytön estämisestä pitäisi huolehtia jo laitevalmistajien tehdessä komponenttejaan ja valitessaan alihankkijoitaan.

Nykyisellään teollisuusautomaatiossa on niin paljon eri valmistajien komponentteja, että täydellinen suojautuminen on lähes mahdoton ajatus. Jos vaikkapa logiikkaohjaimen muistikomponentin valmistaja on yhteistyössä esimerkiksi NSA:n kanssa, ohjaimen valmistaja ei tiedä siitä mitään eikä voi tehdä muuta kuin yrittää valvoa, testata ja rajoittaa laitteensa toimintaa ja liikennöintiä.

3.4.1 USB tietoturvariskinä

Nykyaikaiset käyttöjärjestelmät eivät käynnistä automaattisesti USB-tikulta löytyvää ohjelmatiedostoa oletusarvoisesti ja uusimmat järjestelmät eivät tue koko toiminnallisuutta. USB-tikku muodostaa kuitenkin tietoturvaongelman, sillä sen voi naamioida optiseksi asemaksi, joille automaattista käynnistystoiminnallisuutta vielä tuetaan. Koska tämän lisäksi tikku on mahdollista ohjelmoida esiintymään myös komentoja antavana näppäimistönä ja hiirenä, hyökkääjällä on aika vapaat kädet saadessaan tikkunsa kohteen USB-porttiin [19].

Tällaisella tavalla ohjelmoitu USB-tikku voi porttiin liityttyään esimerkiksi ajaa tikulta löytyvän haittaohjelmakoodin. Vaikka ylläpitäjä olisi poistanut käytöstä USB-median toiminnallisuuden asentamistoiminnallisuuden, esimerkiksi Windowsin omat työkalut auttavat sen palauttamisessa. Lisäksi näppäimistönä ja hiirenä esiintyminen USB-tikun toiminnallisuutena on saatavissa jokaisella tunnetulla käyttöjärjestelmällä, joten ongelma ei rajoitu pelkästään yleisimpiin tai vanhimpiin käyttöjärjestelmiin. USB-tikkujen toimintaa voidaan rajoittaa ainoastaan siten, että järjestelmät hyväksyvät vain erikseen sallitut 16-bittiset usb-id:t omaavat tikut. Tällainen rajoitus on työläs toteuttaa, ellei kyseinen luettelo ole kohtuullisen kokoinen. Suojaus on siis harvinainen, mutta vaikka se olisi toteutettukin, USB-tikun ohjelmoija voi silti muuttaa tikun ID:n haluamakseen ja siten ohittaa tällaisenkin suojauksen. Riittää siis, että tikun saa järjestelmään huijaamalla käyttäjän laittamaan sen siihen tai tekeytymällä itse luvalliseksi käyttäjäksi, kuten tapauksessa Stuxnet [20].

3.4.2 Stuxnet

USB:n hyödyntämisestä hyökkäyksenä on olemassa erinomainen ennakkotapaus: Stuxnet [21]. Se on tunnetuin teollisuusautomaation haittaohjelmasovellus viime vuosilta. Sovellus tunnetaan siitä, että se onnistuttiin asentamaan Iranissa ydinvoimalan ohjausjärjestelmään tavallisen muistitikun avulla. Hyökkäyksen kohteena olevat järjestelmät olivat hyvin samanlaisia laitteita, joita Shodan-tutkimuksessa löydettiin (Siemens Simatic S7 PCL). Vaikka laitteistoa ei ollut turvallisuussyistä kytketty Internetiin, riitti, että niihin päästiin käsiksi paikanpäällä. Paikallisesti asennettu sovellus muutti laitoksen taajuusmuuttajien toimintaa siten, että uraaninrikastukseen käytettävien sentrifugien moottoreihin syötettävän sähkön taajuus saatiin sen avulla muutettua erittäin korkeataajuiseksi. Seurauksena oli sentrifugien pyöriminen ylikierroksilla, mikä rikkoi ne lopulta.

Hyökkäysohjelmiston rakenteesta ja varsinaisesta toteutustavasta johtuen suojautuminen Stuxnetin kaltaisilta tietohyökkäyksiltä on monimuotoista, koska vaikka tietoverkko suojattaisiinkin hyvin, useissa laitoksissa urakoitsijoilla ja toimittajilla on pääsy tietojärjestelmiin ja mahdollisuus itse asentaa sovelluksia. Ulkopuolisten henkilöiden toiminnalle on asetettava selkeät turvallisuusrajoitukset [1]. Lisäksi yrityksellä on oltava tarkasti määritellyt ja mahdollisuuksien mukaan standardoidut säännöt siitä, mitä tuotantoverkkoon saa tuoda ja miten sitä saa käyttää. Esimerkiksi yrityksen ulkopuoliset tietokoneet, puhelimet ja muistitikut tai muutkaan tallennuslaitteet eivät saa olla yhteydessä ohjausjärjestelmään.

Kaikkien tietojärjestelmien ei tarvitse olla tietoverkossa, kuten ei vakoilusovellustenkaan. Johtopäätöksenä on sanottava, että pidättäytymällä tarpeettomista tietoverkkoyhteyksistä suojaus tietohyökkäyksiä vastaan on yleensä parempi. Stuxnetin kaltaisella haittaohjelmalla voitaisiin saada paljon aikaan myös ydinvoimalan kaltaisen järjestelmän ulkopuolella. Suojauksen kasvattamiseen tähtäävä ajattelumalli on tärkeä myös muissa tuotantolaitoksissa, koska Stuxnet ei ole jäänyt viimeiseksi kaltaisekseen haittaohjelmaksi. Stuxnet lisäksi tehtiin siten, että sen osia voidaan kopioida uusien haittaohjelmavarianttien tekemistä varten. Tästä uhkasta esimerkkinä on Flame, joka on myöhemmin löydetty haittaohjelma ja siinä on havaittu olevan Stuxnetissa käytettyä ohjelmakoodia.

4 TURVATON AUTOMAATIOVERKKO

Tässä luvussa käsitellään automaatioverkon laitteiden Internet-yhteyksiin liittyviä tietoturvan perusvaatimuksia. Verkkohyökkäyksiltä suojautumiseen tarvitaan ympäristöstä ja suojautumisen perusteellisuudesta riippuen joko eristäytymistä palomuurein tai muilla keinoin. Teollisessa automaatioverkossa merkittävintä on tunnistaa verkon laitteet ja osat, jotka eivät saa olla suorassa yhteydessä Internetiin ja ne, jotka voivat olla hyvin suojatulla tavalla yhteydessä esimerkiksi yrityksen omaan palvelimeen. Yrityksen on järkevää tehdä palveluntarjoajan kanssa sopimus siitä, miten menetellään esimerkiksi palvelunestohyökkäyksen sattuessa ja sopia liikenteen vaihtoehtoisesta järjestelystä valmiiksi. Tärkeää on siis huolehtia tietoturvasta kahdessa eri vaiheessa: sekä ennakoivasta tietoturvasta, että käytännöistä hyökkäyksen kohteeksi jouduttaessa.

Nykyisin on tarjolla myös koulutuksia, joiden avulla yrityksen tietoturvasta vastaava voi paremmin pysyä mukana muuttuvissa tietoturvauhkissa, ellei yrityksellä ole varaa palkata konsulttia tai muuta ulkopuolista tahoa pitämään tietoturvatasoa vaatimusten mukaisella tasolla. Lisäksi on tarjolla erilaisia tapoja suojautua mm. USB-hyökkäyksiltä käyttämällä esimerkiksi mobiililaitteiden USB-lataamista varten tehtyjä liitäntäadaptereita, jotka antavat liitynnän vain tuoda sähköä, mutta estää tiedon siirtämisen.

Vaikka automaatioverkon suojaaminen on sinänsä uutta ja haasteellista, palomuuritkin voidaan murtaa eikä aina ole varaa sijoittaa uusimpaan IDS-tekniikkaan, siihen kannattaa panostaa. Teollisuusyritys välttää monet ongelmat, jos se edes eristää automaatiojärjestelmänsä toimistojärjestelmistään palomuuri- ja reititinratkaisuilla. Siten esimerkiksi palveluvyöhykkeeseen (DMZ) voidaan sijoittaa palvelin, jolla hoidetaan virustietokanta- ja muut tietoturvapäivitykset. Jos päivitykset lisäksi ajetaan vain erikseen hyväksymällä, laitteiden Internet-yhteyksien määrää saadaan huomattavasti vähennettyä ja hyökkäysriskiä pienennettyä.

4.1 Verkon suojauksen vaatimuksia

Yleisesti tiedetään, että automaatioverkot eroavat tavallisista toimistoverkoista. Yksimerkittävimmistä eroista on siinä, että automaatiolaitteita käytetään vanhentuneilla ohjelmistoilla, joissa on matala tietoturvataso, joten on erittäin tärkeää huomioida muutamia perusvaatimuksia. Esimerkiksi on oleellista, että automaatiolaitteissa on määritelty ja ennen kaikkea vaadittu käyttäjiltään riittävän usein vaihtuvat ja laadukkaat salasanat. Asianmukainen käyttäjien autentikointiprosessi sekä haittaohjelmien tunnistus tulee olla kunnossa. Kokonaiselle yrityksen verkkoarkkitehtuurille tulee olla määriteltyinä myös

tiedon kulkureitit sekä palomuurit ja kytkimet. Tiedon kulkua varten on asetettava oleelliset vaatimukset ja rajoitukset, jotta vain asianmukainen tieto liikkuu verkossa vain sallittuja reittejä pitkin. Sallittujen osoitteiden dokumentointi ja jopa aivan yksinkertainen porttien muutos auttaa tietoturvan tason parantamisessa.

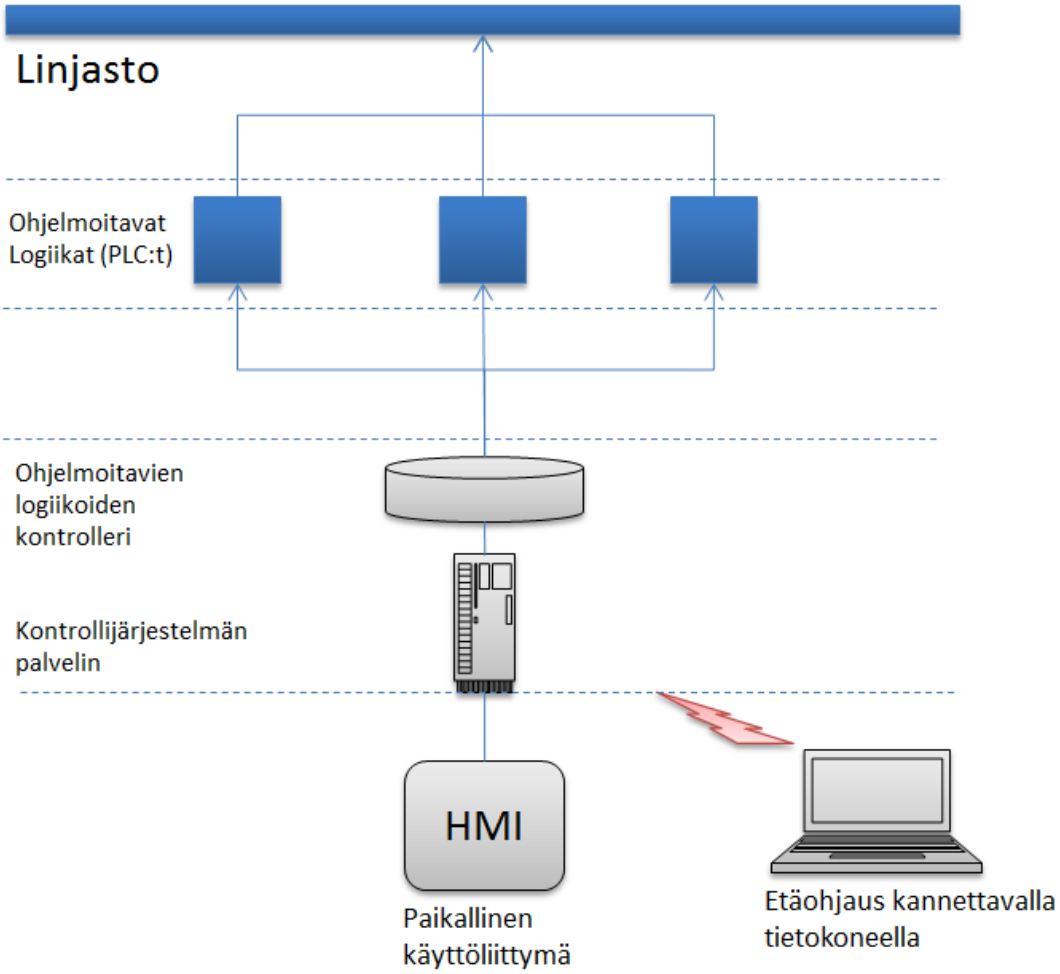
Tietoturvan takaamiseksi on onneksi nykyisin olemassa standardeja [1]. Työturvallisuuteen ja esimerkiksi terveyteen liittyviä säädöksiä ja direktiivejä on ollut jo hyvän aikaa olemassa, mutta vasta viime vuosina on saatu aikaan sekä suoria vaatimuksia, että epäsuorasti tietoturvan parantamiseen tähtääviä standardeja. Teollisuusautomaatioon kuuluvat eurooppalaiset standardit (CEN ja CENLEC) sekä kansainväliset (ISO ja IEC) sisältävät vaatimuksia riskien hallintaan. Erityisesti ohjausjärjestelmiä koskevat standardit, jotka parantavat turvallisuutta ja suunnittelua, ovat epäsuorasti kytkettävissä tietoturvaan. On tärkeää, että automaatioverkkoon kytketyt laitteistot toimivat odotetulla tavalla eivätkä esimerkiksi ylikuumene haittaohjelman vuoksi.

Varsinaisesti valmistusteollisuuden tietoturvaan liittyviä vaatimuksia on katettu IEC:n standardissa. Siinä on vaatimuksia muun muassa teknisten järjestelmien väliselle tietoliikenteelle, esimerkiksi kenttä- ja turvaväylille [1]. Standardia on valmistellut sen Digital Communications -alakomitean Cyber Security –työryhmä ja sen uusin versio on 65/412/RVN [22].

4.2 Automaatioverkon etäohjauksen ongelma

Automaatioverkkovaihtoehtoja käsiteltiin aiemmin luvussa 2, mutta tietoturvaongelmia kuvattaessa voidaan keskittyä verkon osaan, jossa automaatiolaite on kytketty alla olevan kuvan mukaisesti. Siinä ohjelmoitavia logiikoita käytetään palvelimelta ajettavalta valvontajärjestelmältä ja järjestelmään on rakennettu sisään etäohjausmahdollisuus VNC-palvelun avulla. Palvelu löytyy Shodanin julkiselta palvelimelta, ellei sitä ole piilotettu asianmukaisesti, kuten luvussa 3.3. mainitaan.

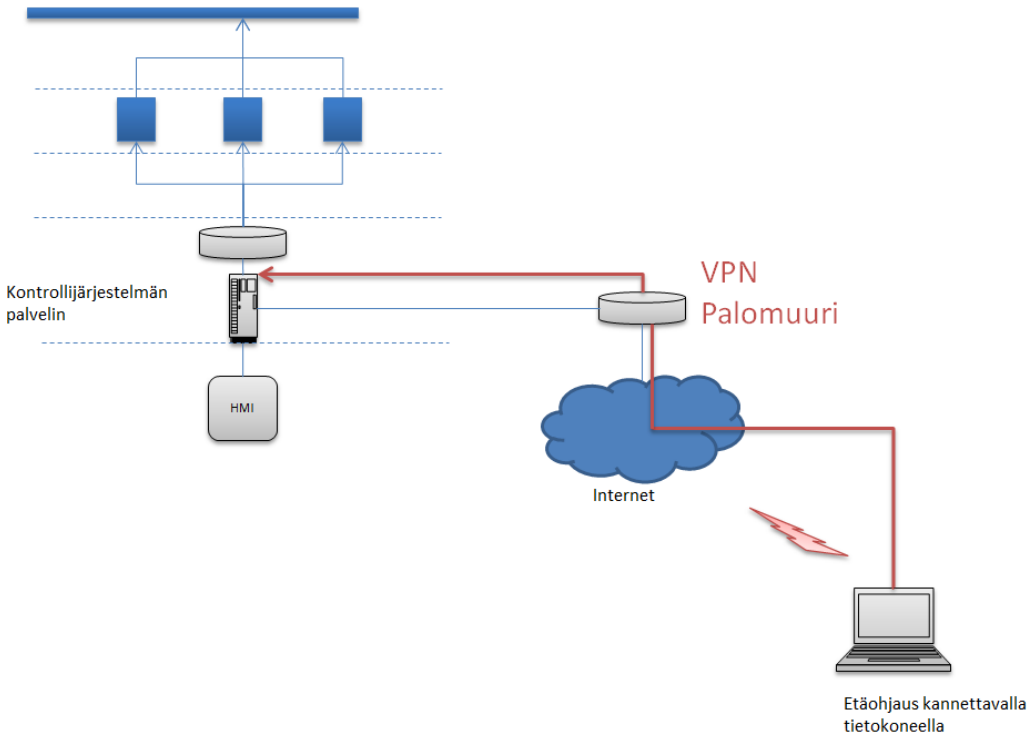
Koska kontrollijärjestelmän palvelimeen halutaan ottaa etäyhteys, se joudutaan kytkemään tietoverkkoon. Jos etähallintayhteyden sallivaa palvelua ei ole piilotettu asianmukaisesti julkiselta verkolta, esimerkiksi Shodan voi havaita sen ja julkistaa laitteen osoitteen sekä haavoittuvuudet. Yrityksen kannalta on tärkeää, että asiattomat käyttäjät eivät pääse käsiksi palvelimeen, joten sen Internet-yhteys tulee eristää palomuurilla ja sallia vain VPN:n avulla. Kyseessä on erittäin tunnettu tietoturvatekniikka ja siten perusvaatimus tällaisen järjestelmän käyttäjälle.



Kuva 10. Esimerkki automaatiolaitteiden keskinäisistä kytkennöistä korkealla tasolla.

4.3 VPN etäohjauksen turvallisuuden perusratkaisuna

Etäohjausta varten luodun yhteyden voi suojata monella tavalla, esimerkiksi kryptaamalla lähetetyn tiedon ja käyttämällä salausavaimia. Tällöin ei ole kovin tarkkaa, millaista yhteyttä muuten käytetään, ellei yhteyden suhteen ole muita vaatimuksia, esimerkiksi nopeuden ja käyttövarmuuden suhteen. Vaikka liikennöinti olisikin tehokkaasti salattua, käytännössä yrityksen verkko on liitettävä Internetiin kuitenkin palomuurin kautta, kuten aiemmissa kuvissa esitetään, ettei siinä oleva normaali liikennöinti vaarantaisi verkon muita koneita ja päinvastoin. Palomuuri toimii siten, että siihen määritellään säännöt, joiden avulla palomuuri suodattaa asiaankuulumattomat paketit pois liikenteestä ja sallii kauttaan vain luvallisen tietoliikenteen. Lisäksi, vaikka mikään ratkaisu ei lopullisesti poista rikolliselta taholta hyökkäysmahdollisuutta, palomuurien lisäksi tietoturvaa voidaan parantaa myös toisiaan täydentävillä ratkaisuilla, esimerkiksi kerrostamalla tietoturvatekniikoita.



Kuva 11. VPN ja palomuuri mahdollistaa turvallisemman yhteyden etäohjaukselle.

Palomuureja on perustoiminnallisuuksiltaan kahta eri mallia: tilallinen ja tilaton. Perusperiaatteeltaan konseptissa on kuitenkin kyse pakettisuodattimesta, joka tarkastaa vastaanottamiensa pakettien osoitteet ja portit sekä tekee päätöksen paketin jatkamisesta. Tilaton ja tilallinen palomuuri eroavat siten, että tilaton palomuuri tarkastaa jokaisen paketin luvallisuuden palomuuriin tehtyjen asetusten perusteella. Tilallinen palomuuri sen sijaan vertaa paketteja muodostettuihin TCP- ja UDP-yhteyksiin ja estää paketit, jotka eivät kuulu johonkin muistissa olevista yhteyksistä. Tarkemmin sanottuna, se tarkkailee sekä molempiin suuntiin meneviä paketteja, että yhteyksien tiloja ja tallentaa niistä tietoa, jonka avulla edellisiä ja aktiivisia yhteyksiin liittyviä paketteja voidaan hyväksyä tai hylätä. Päätöstä hylkäämisestä tai hyväksymisestä ei siis tehdä pelkästään ylläpitäjän tekemien asetusten perusteella.

Toimintamallista johtuen, TCP-liikenne on turvallisempaa kuin UDP-liikenne, koska sen kohdalla ei tehdä kaksisuuntaista yhteydenmuodostusta, vaan palomuurin täytyy merkitä UDP-yhteys hyväksytyksi ensimmäisten toimivien pakettien kohdalla. Yhteyden lopettamiseksi ei ole muuta keinoa kuin aikakatkaisu, mikä saattaa altistaa palomuurin UDP hole punching-hyökkäykselle. TCP sen sijaan tekee tutun kättelyn (SYN, SYN-ACK, ACK) ja merkitsee yhteyden ESTABLISHED-tilaan vasta, kun tervehdys on tehty. Lisäksi yhteyden sulkemiseen on olemassa oma viestinsä (FIN/ACK) kuittauksineen. Tilallinen palomuuri toimii nopeammin kuin tilaton palomuuri, koska sen ei tarvitse tarkastaa jokaista pakettia kokonaan. Paketin hyväksymiseen riittää, että palo-

muuri tarkastaa tilataulukon, johon se on tallentanut käynnissä olevien yhteyksien tiedot. Pelkkä yhteyksien ja lähdeosoitteiden tarkastaminen ei kuitenkaan riitä turvaamaan esimerkiksi vertaisverkkojen välityksellä tapahtuvaa liikennettä. Paremman tietoturvan tarjoaa sovellustason palomuuri, joka valvoo, mitkä palvelut ovat sallittuja. Sovellustason suodatusta käytetään yleensä tilallisen suodatuksen lisänä tarkastamaan, mihin liikennöintiin käytettyä protokollaa käytetään. Vaikka sovellustason suodatusta tekevä palomuuri on jonkin verran hitaampi kuin tavallinen tilallinen tai tilaton palomuuri, se toisaalta pystyy erottamaan saman protokollan alla kulkevan liikenteen, jota käytetään Web sivujen lataamiseen liikenteestä, joka kuuluu tiedostojen jakamiseen.

Jos lisäksi käytetään IPSec–salattua yhteyttä, pitää yhteyden kanssa käyttää VPN-ratkaisua. Kyseessä on tekniikka, jolla voidaan muodostaa kahden eri toimipisteen välille yhteys ja käyttää siihen liitettyjä laitteita, kuten ne olisivat samassa lähiverkossa siihen kuuluvin palveluin. VPN rakennetaan käyttämällä VPN:ää tukevaa palvelinta, siirtymäverkkoa, tunneloitua yhteyttä ja tunnelointiprotokollaa. VPN-yhteys itsestään on yhteyden osa, jossa lähetetty data tunneloidaan, eli kapsuloidaan ja salataan esimerkiksi Point-to-point tunnelointi- tai IPSec-protokollalla. Tunneloitu tieto kulkee kapseloituna, eli paketoituna, siirtymäverkon kautta. Siirtymäverkoksi kelpaa mikä tahansa julkinen Internet-verkkoyhteys.

VPN-yhteys voidaan tehdä sekä etäyhteytenä, että reitittimien välisenä VPN-yhteytenä. Etäyhteystoteutuksessa liikennettä valvotaan erilliseltä koneelta ja tieto salataan ennen reitintä. Vaihtoehtoisesti salaus ja kryptauksen avaaminen voidaan tehdä suoraan reitittimillä. Eri valmistajien reitittimet eivät välttämättä ole yhteensopivia, mutta toisaalta tässä ratkaisussa ei tarvita erillistä tietokonetta.

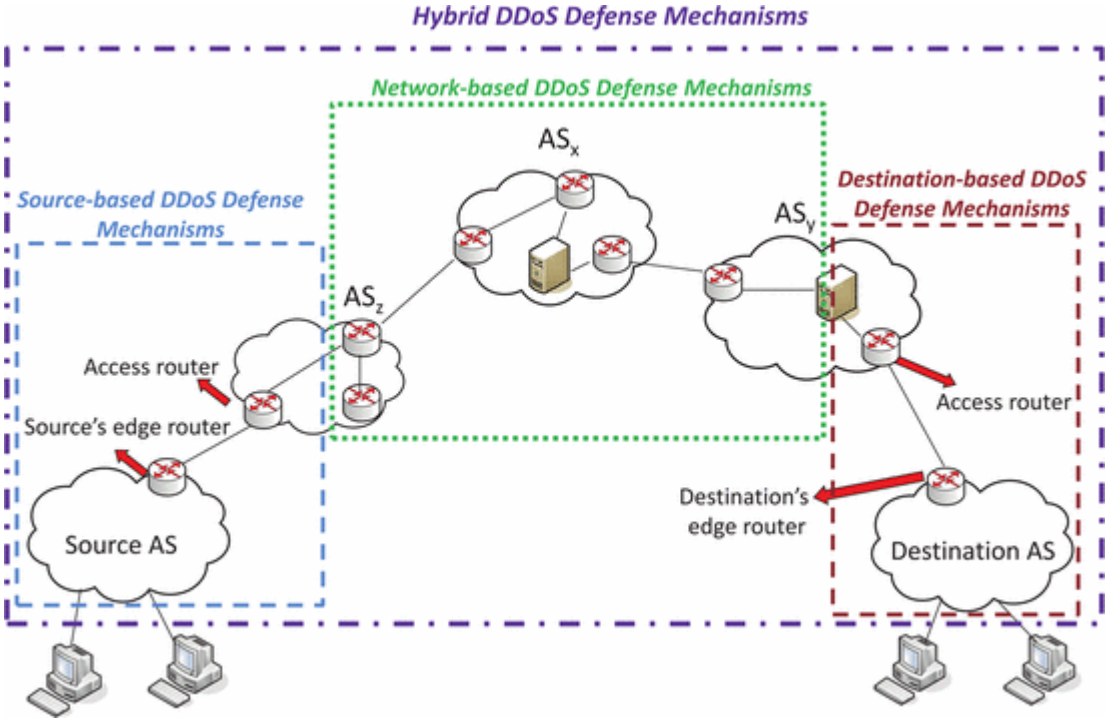
Toimintaa ja yhteyden muodostusta varten VPN varmistaa, että tieto on tullut perille, ja että tieto on tullut perille muuttumattomana. Lisäksi VPN autentikoi lähettäjän, eli varmistaa, että lähettäjä on todellinen lähettäjä. Se myös varmistaa, että tieto on saapunut perille ja että vastaanottajakin on se, joka väittää olevansa. Itse autentikointi tehdään salaisella avaimella ja tiedonsiirrossa käytetään neuvoteltua symmetristä avainta. Käytetyn avaimen pituus ja käyttöikä vaikuttaa siihen, voidaanko avain päätellä laskemalla. Jos käytetty avain on pitkä ja se vaihdetaan tarpeeksi usein, suojaus on todella murtovarma. VPN sisältää myös suojauksen toistoa vastaan, jossa pyritään hyödyntämään olemassa olevaa datavirtaa yhteyden huomaamatonta hyväksikäyttöä varten.

4.4 Palvelunestohyökkäykseltä suojautumisen perusteita

Vaikka palvelunestohyökkäys [9] [23] on erittäin tehokas tapa sulkea esimerkiksi automaatioverkossa toimivan kontrollerin tai palvelimen toiminta, siltä voidaan kuitenkin suojautua jossakin määrin. Se voidaan myös havaita tehokkaammin esimerkiksi asettamalla rajoja, jolla tunnistetaan normaalista poikkeava hyökkäykselle tunnuksenomainen

liikennemäärä. Lisäksi tärkeimpiä toimintoja voi hajauttaa, jolloin hyökkäyksen kohteeksi joutuminen yhdessä paikassa ei tarkoita palvelun tukkeutumista kokonaan. On tärkeää, että yrityksen Internet-palveluntarjoaja pystyy tarjoamaan esimerkiksi SCADA-verkon etäohjaustoiminnallisuuden takaamiseksi nopeasti lisäresursseja ja että yrityksen oma verkon osuus on rakennettu laitteista, jotka täyttävät oleelliset laatukriteerit ja ovat vikasietoisia.

Suojautumismekanismien voidaan ajatella riippuvan paljon siitä, mihin ne on sijoitettu ja onko kyseessä suojautuminen etukäteen, vai reagointi meneillään olevaan hyökkäykseen. Verkko- ja kuljetuskerroksen hyökkäyksiltä suojautuminen voidaan ainakin ajatella jakautuvan sen mukaan, onko kyseessä lähde-, kohde-, vai verkkoperusteinen hyökkäysmalli.



Kuva 12. Suojausmekanismin luokittelu verkko- ja kuljetuskerroksen palvelunestohyökkäykselle. Perusteena sijainti AS-verkoissa [9].

Suojausmekanismi siis valitaan sen mukaan, minkä tyyppiseltä hyökkäykseltä halutaan suojautua, esimerkiksi lähdeperusteisesti asettamalla rajoitukset mahdollisimman lähelle hyökkäyksen lähdettä, eli sen verkon reunareitittimen kohdalle. Koska lähdeosoitteet ovat kuitenkin usein väärennettyjä ja hyökkäykseen käytetään bottiverkkoja, tämä suojausmalli on riittämätön. IPSec-protokollalla voidaan tarkistaa lähteen oikeellisuus, mutta palvelu ei ole useinkaan käytössä sen tuoman overheadin vuoksi. Lisäksi hyökkääjä voi silti onnistua valitsemalla IP-osoitteen oikeasta avaruudesta. Puolustava taho voi myös vertailla verkkonsa liikennettä lähdeverkosta tulevaan liikenteeseen ja seurata, ettei lähetettävien pakettien määrä ole liian suuri. Puolustusmekanismi syö laskentatehoa ja suojaa lähinnä toisten verkkoja ja on lisäksi ohitettavissa pysymällä riittävän pienissä lähetysmäärissä.

5 VERKKOHYÖKKÄYKSEN TEKO

Tässä luvussa arvioidaan yhden tunnetun verkkohyökkäystavan vaikutuksia automaatiolaitteiden muodostaman verkon ja siihen kuuluvien laitteiden toimintaan. Koska testausta varten ei ollut saatavilla oikeaa SCADA-verkkoa, luvussa vertaillaan tämän työn ohella tehdyn testauksen johtopäätöksiä erääseen automaatioverkkoon tehdyn simuloidun palvelunestohyökkäyksen johtopäätöksiin. Tarkoitus on saada aikaiseksi aiempia tutkimustuloksia tukevaa tai vastustavaa näyttöä. Sekä simuloidussa, että tässä työssä tehtävässä hyökkäyksessä toteutetaan toimintamalli, jossa verkkoon tuotetaan ylimääräistä liikennettä sen verran, että voidaan puhua palvelunestohyökkäyksestä. Perusteluna hyökkäysmallivalinnalle on, että palvelunestohyökkäys on helppo ja yleinen sekä hajautettuna vaikutuksiltaan tehokas. Siinä tapa toteuttaa hyökkäys on hyödyntää joko verkosta suoraan löytyviä maksullisia rikollispalveluita tai suorittaa koe suljetussa laboratoriossa. Koska työn toteutus on tehtävä Suomen lainsäädännön puitteissa, koe suoritetaan laboratoriossa.

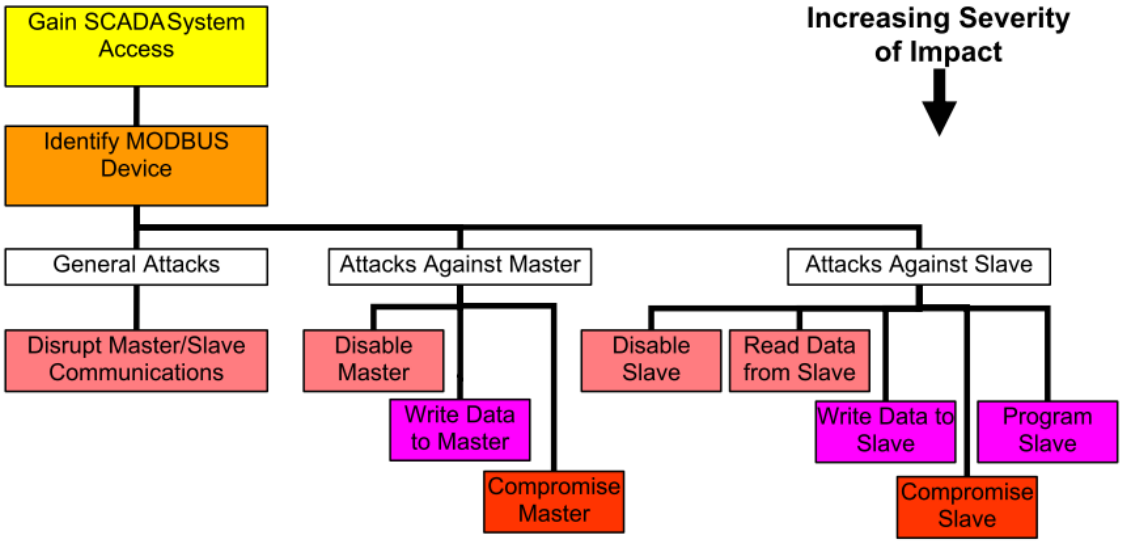
Koska tietojen vakoileminen eri haittaohjelmien avulla ja niiden vuotaminen on oma lähes rajoittamattoman laaja alueensa ja lisäksi koska suurinta välitöntä haittaa yritykselle seuraa nimenomaan laitteiden toimintakykyyn vaikuttamalla, tämän työn kohdalla valinta on käyttää Tampereen teknilliselle yliopistolle (TTY) tällaisia kokeita varten erikseen hankittua Rugged Tooling Oy:n valmistamaa Ruge-työkalua, tutkia millaista haittaa sillä voisi saada aikaan tietoverkossa sekä tutkia myös jotakin ilmaiseksi saatavilla olevaa ohjelmistotyökalua. Rugelle tehdyn Linux-ohjelmiston avulla laite luo hallitusti ylimääräistä IP liikennettä valittuun tietoverkkoon. Työkalun asetukset voidaan esimerkiksi määritellä siten, että sen tekemä tiedonsiirto luo palvelunestohyökkäystä vastaavan tilanteen. Siinä tietoverkon sisäisen liikenteen määrä kasvaa niin suureksi, että se haittaa muiden laitteiden liikennöintiä merkittävästi. Työkalu hyödyntää etukäteen tallennettuja tietovirtoja, ohjausviestejä sekä aikaleimoja. Ethernet-, IP- ja UPD-protokollaviestejä voidaan muokata ja populoida uudelleen. Lisäksi viestitulvaan voidaan sisällyttää esimerkiksi tunnelointiprotokollia.

Tutkittavaksi verkoksi valikoitui TTY:n tietoturvalaboratorion verkko. Ruge kytkettiin verkkoon ja sitä ohjattiin Kali Linux-käyttöjärjestelmällä terminaaliportin kautta sarjakaapelin avulla lähettämään halutunlaisia paketteja kohdekoneelle. Ensimmäiseksi hyökkäystyökalu päästetään generoimaan liikennettä ilman rajoituksia ja tutkitaan, miten paljon verkkoon jää tilaa muulle liikenteelle. Sen jälkeen kokeillaan, miten ylimääräistä liikennettä voidaan rajoittaa ja miten tehokkaasti esimerkiksi palomuuraus vaikut-

taa tilanteeseen. Lopuksi mietitään, miten saadaan riittävän tehokas palomuurausrakenne, jollainen turvallisessa verkossa tulisi olla palvelunestohyökkäykseltä suojautumisen kannalta ajateltuna.

5.1 Hyökkäyksen vakavuus

Jos hyökkääjä saa yrityksen järjestelmän automaatiolaitteen hallintaansa, siitä seuraava haittavaikutus on vakavuudeltaan erilainen, kuin jos laitteen toiminta vain keskeytyy hetkeksi [24]. Lisäksi kohteeksi joutuneen laitteen asema järjestelmässä vaikuttaa paljon. Mitä verkottuneempaan osaan tuotantoverkkoa hyökkääjä pääsee käsiksi, sitä vahingollisemmaksi hyökkääjän mahdollisuudet kasvavat. Toisaalta jopa yksittäisen kontrollerin haavoittuvuuden hyödyntäminen saattaa tuoda mahdollisuuden käyttää tietoja jossakin toisessa samaan tuotantoverkkoon kytketyssä laitteessa.



Kuva 13. Hyökkäyksen haitat vaikuttavat eri tavoin eri rooleissa olevissa laitteissa. [24]

Laitteiston suojausta voidaan kuitenkin parantaa systemaattisesti, esimerkiksi asettamalla tarkkaan mietittyjä rajoituksia käyttäjien toiminnalle. [25] Triviaaleja rajoituksia ovat esimerkiksi sellaiset, jotka estävät vierailijatunnukset kokonaan tai ainakin vierailijoita muuttamasta laitteiden asetuksia tai tuotannon toimintamallia.

5.2 Hyökkäys simuloituun automaatioverkkoon

Automaatioverkot ovat usein sellaisia, että niiden sammuttaminen päivitysten tai verkkotestien pystyttämistä varten vähäksikin aikaa on merkittävän suuri kustannus tuotantolaitokselle. Sen vuoksi tuotantoa ei voida kovin usein pysäyttää edes tietoturvan tason testaamista varten. Laitteistojen elinkaari on usein todella pitkä, jopa vuosikymmeniä. Carnegie Mellon, Vanderbilt ja California Berkeleyn Yliopistoissa tehty tutkimus pal-

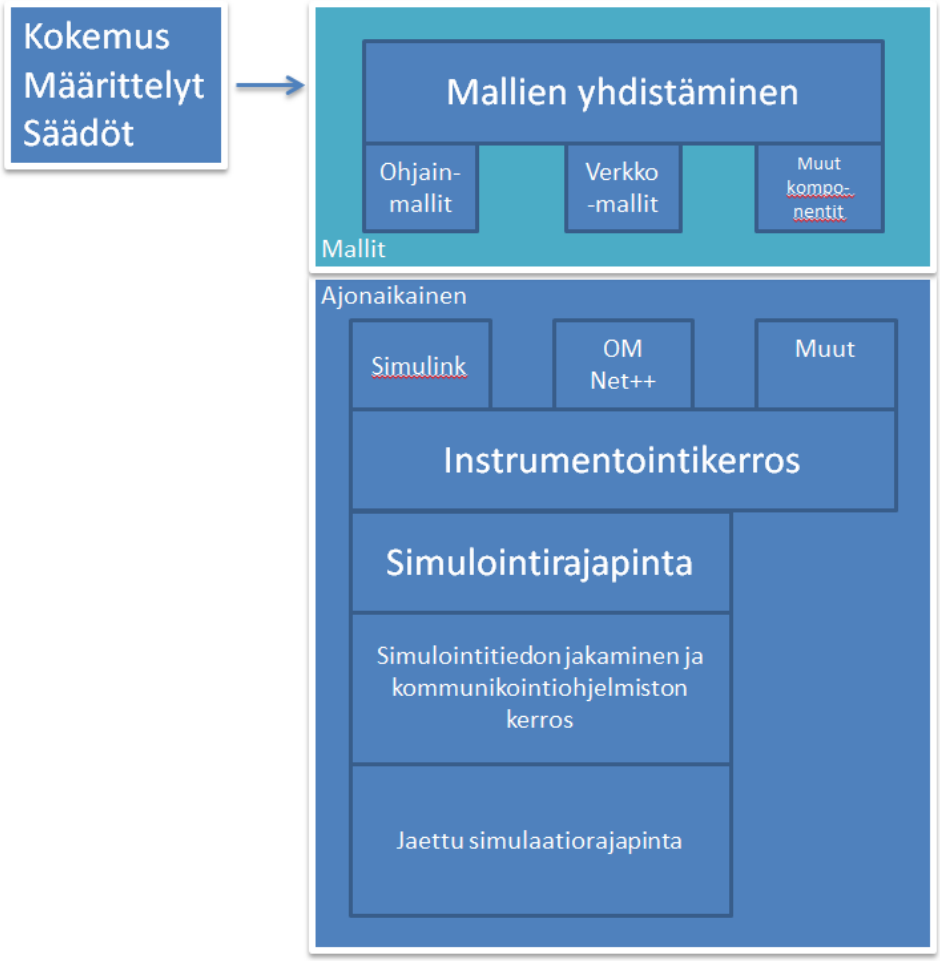
jastaa, että verkkohyökkäys ja tyypillinen teollinen automaatiojärjestelmä voidaan onneksi myös simuloida pystyttämättä jonnekin kallista SCADA-järjestelmää.

Simuloidussakin järjestelmässä olisi vähintään oltava ohjausyksikkö ja tuotantolaitoksen dynamiikkaemulointi esimerkiksi Matlab:ssa tai verkkosimulointityökalussa, kuten OMNeT++:ssa [26]. Riittävän lähellä todellista toimintamallia oleva simulaatio vaatii myös ohjelmiston, jolla voidaan yhdistää simulaation osat loogiseksi ja koherentiksi kokonaisuudeksi [27]. Eräs tällainen simulointiohjelmisto on Command and Control Wind Tunnel [26] [28]. Sovellus on rakennettu erityisesti teollisten ohjausjärjestelmien ohjaustoimintojen simulointia varten.

Ohjelmisto yhdistää erilaisten teollisissa ohjausympäristöissä olevien vuorovaikutusten mallinnuksen ja kokeelliset tulokset toisiinsa. Vuorovaikutuksista ohjelmisto hyödyntää mallinnettavana olevan kokonaisuuden oleellisimmat parametrit sekä kokoonpanon ominaisuuksia, jotka ovat mallintamisen kannalta tärkeitä. UML:n ja DSML:n avulla sillä voidaan simuloida tilanteita. DSML on räätälöity kuvauskieli, jonka avulla C2WindTunnelia varten voidaan määritellä integrointimalleja ja yksityiskohtia simuloitavaa järjestelmää ajatellen. Alla olevassa kuvassa näkyy C2WindTunnelin simulaation ohjelmien hierarkia.

Viitteessä [26] kuvatussa simulointitutkimuksessa hyökättiin C2WindTunnel – sovelluksen avulla simuloituun SCADA-järjestelmään. Kohteena olevassa järjestelmässä on reaktori, jossa on yhdistetty separointijärjestelmä. Järjestelmän toiminnan mallintaminen tehtiin muuntamalla mallista saatavilla oleva FORTRAN ohjelma C-koodiksi ja lopulta Simulink-malliksi. Mallin toimintojen viiveet säädettiin siten, että vasteajat muuttuivat tunneista sekunneiksi ja ohjelman diskreetiksi tarkkuudeksi säädettiin sadasosasekunti.

Kontrollerin ja simuloitavan tuotantojärjestelmän välille asennettiin verkko. Verkossa yhden reitittimen tehtävänä on kerätä tietoa järjestelmän reitittimen ja fyysisesti lähellä toisiaan olevilta sensoreilta. Samalla reitittimen tehtävänä on lähettää ohjaustietoa sitä lähellä oleville venttiileille. Verkossa on yhteensä neljä reititintä, jotka lähettävät tietoa sensoreilta ohjausyksiköille.



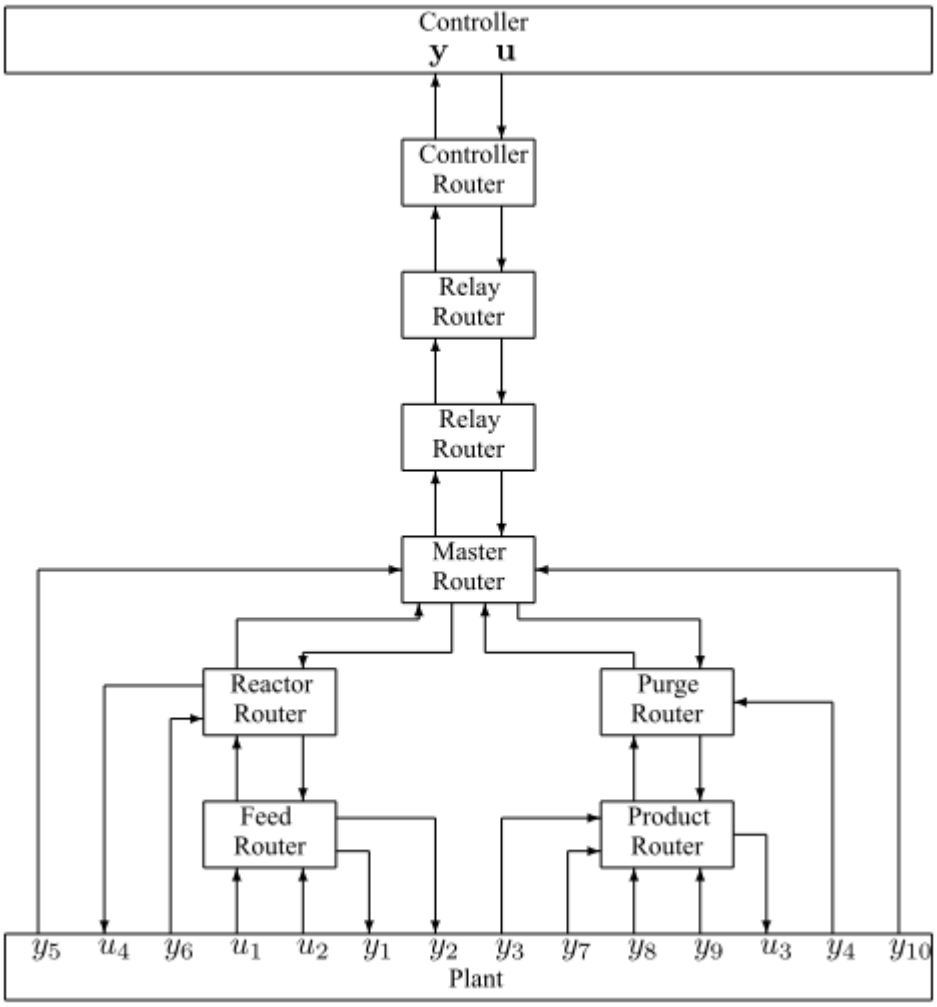
Kuva 14. C2WindTunnelin simulointimalli [26].

Simuloidun järjestelmän tietoverkkoa kuvaa parhaiten malli, jossa niin sanottu pääkontrolleri jakaa ja kerää tietoa kolmitasoisessa hierarkiassa. Muut reitittimet sijaitsevat pääkontrollerin ja simuloitavan laitteiston välillä. Verkko simuloitiin hyödyntämällä OMNeT++:n INET-protokollia tukevaa pakettia. OMNeT++ erottelee simuloidun verkkoliikenteen ajonaikaisesta liikenteestä. Verkon rakenne selviää yllä olevassa kuvasta.

Tutkijaryhmä teki verkkoa vastaan palvelunestohyökkäyksiä kohdentaen hyökkäykset jokaiselle reitittimelle erikseen. Tavoitteena oli lähettää hajautetuilta lähteiltä käsin hyökkäyksen kohteelle niin paljon yhtäaikaisesti käsiteltävää tietoa, että sen toiminta joko pysähtyi kokonaan, tai hidastui niin paljon, ettei se enää pystynyt toimittamaan asianmukaista tietoa tarkoituksenmukaisesti eteenpäin. Simulaatio toimi 150 sekunnin ajan, hyökkäys tehtiin kohdassa 30 sekuntia ja kesti kohtaan 60 sekuntia.

Hyökkäyksen seurauksena kohteena oleva verkon piste meni käytännössä toimimattomaksi. Verkon rakenteesta kertovassa kuvassa ylimmäisenä osana näkyvä kontrolleri lakkasi näkemästä sensorit, joilta hyökkäyksen alaisena oleva reititin keräsi tietoa. On selvää, että tällainen tilanne aiheuttaa kontrollerin toiminnassa sen, että laite ei kykene

tekemään toimintojaan säännöllisesti eivätkä laitteet vastaa kontrollerilta tuleviin komentoihin. Käyttökustannukset, laitevahinkojen todennäköisyydet sekä laitteiden rikkoontumisriskit kasvavat. Jos hyökkääjä pääsee tukkimaan minkä tahansa reitittimen laitteiston ja kontrollerin välinen kommunikaatio katkeaa tai kärsii vakavista ongelmista. Järjestelmät tosin saattavat selviytyä tällaisesta tilanteesta automaattisesti, mutta riippuen hyökkäyksen kestosta, vahingot voivat olla suuria johtuen myös pelkästään järjestelmän toimimattomuuden vuoksi tehdystä tuotannon alasajosta [26].



Kuva 15. Simuloidun verkon rakenne [26].

Tutkimuksessa kontrollerireititintä vastaan tehty hyökkäys aiheutti näkyviä ongelmia kontrollerin kommunikoinnissa. Toisaalta lähellä laitteistoa sijaitseva Feed Router ei hyökkäyksen kohteeksi joutuessaan vaikuttanut millään tavalla järjestelmän paineen, tuotantonopeuden eikä käyttökustannusten arvoihin. Tästä voi päätellä, että kontrollerin toimintavarmuus on tärkeä turvata ja että etäohjaus on varmasti suuri riskikohta. Lisäksi vähänkään monimutkaisempien järjestelmien reagointia on vaikeaa ennustaa. Simulointi toisaalta osoittautui yhdeksi tehokkaaksi tavaksi mallintaa tuotantoverkon toiminnan heikkoja kohtia.

5.3 Hyökkäys Siemens Simatic S7 PLC-laitteeseen

NSS Labs teetti heinäkuussa 2011 tutkimuksen siitä, miten helppoa on murtautua suosittuun Siemens S7 Simatic logiikkakontrolleriin [29] ja miten vakavasta haavoittuvuudesta on kyse. Tutkimus lähti liikkeelle oletuksesta, että Simatic S7 PLC-tuoteperhe on paljon teollisuudessa käytetty ohjainjärjestelmä (ICS) ja että sen käyttämät protokollat on suunniteltu lähes kokonaan ilman tietoturvaa olettaen, että teollisuusautomaatioverkko on toteutettu irrallaan Internetistä. Niiden lisäksi tuotteeseen on nykyisin kuitenkin lisätty Internet-yhteys, joten on triviaalia olettaa, että tietoturva ei kokonaisuudessaan ole riittävällä tasolla. NSS Labs:n teettämässä tutkimuksessa selvitettiin S7 logiikan haavoittuvuuksien lisäksi tavat, jolla hyökkäys voidaan toteuttaa esimerkiksi S7-1200 ja S7-300 -laitteisiin.

Siemens käyttää automaatioverkossa laitteiden väliseen kommunikointiin PROFINET-protokollaa ja laitteiden manageroinnin varten TCP/IP-yhteyttä portin 102 kautta (ISO-TSAP). S7 kontrolleriperhe on valittu tutkimuksen kohteeksi, sillä sen käyttämää protokollaa käyttää tämän vuoden tilastojen mukaan miljoonat teollisuuslaitteet ja määrä näyttäisi olevan kasvussa [30].

Wireshark tukee PROFINET-protokollaa, joten Ethernet-viestikehykset ovat tutkittavissa. Hyökkäystä ei kuitenkaan toteutettu itse PROFINET-protokollalla, vaan se toimii PLC-laitteiden yhteytenä verkossa. Sen sijaan ISO-TSAP on protokolla, jolla ohjelmoidaan muun muassa Siemensin valmistamien kontrollereiden toimintaa. Protokollaa purkamalla voi päätellä, millaisia paketteja S7 PLC-laitteiden välillä automaatioverkossa liikennöi. Hyökkääjälle riittää, että käytössä on Wireshark sekä Step7 Totally Integrated Portal (TIA) ohjelmointityökalu. Tutkimuksessa siitä oli käytössä versio 11. Kirjoittamisen hetkellä uusin versio on 13 ja se tukee vanhempien versioiden yhtäaikaista asennusta (versio 11 mainittu yhteensopivuusluettelossa). S7-laitteista tutkimus käsitteli seuraavia malleja ohjelmistoversiolla V02.00.02:
PLC1 6ES7 212-1BD30-0XB0 AC/DC => S7-1200
PLC2 6ES7 212-1BD30-0XB0 AC/DC => S7-1200
PLC1 6ES7 321-1BH02-0AA0 AC/DC => S7-300
PLC2 6ES7 321-1BH02-0AA0 AC/DC => S7-300

ISO-TSAP-paketteja seuratessa Wiresharkilla, havaittiin, että ne ovat selkokielisiä. Niistä on siis mahdollista saada tarvittava tieto pakettien replikointia ja muokattujen pakettien uudelleenlähettämistä varten. Siten hyökkääjä voi esiintyä kontrollerina ja esimerkiksi sulkea laitteen keskusyksikön virran, poistaa muistinsuojauksen käytöstä ja ladata itse luomiaan ohjelmia kontrolleriin. Paketeista löytyi selkokielisinä esimerkiksi käyttäjänimiä, salasanoja ja tiedonsiirtosessioita. S7 kontrollereista nimittäin löytyy telnet-palvelu sekä web-palvelin (SimaticHTTP). Hyökkääjän on lisäksi mahdollista luoda laitteeseen takaportti esimerkiksi muokkaamalla laitteen ladder-logiikkaa.

S7-laitteet tukevat salasanojen asettamista, joten yhteyttä luotaessa PLC saattaa kysyä salasanaa. Jos liikenteestä saadaan luettua paketti, jossa on tiiviste- eli hajautusarvo (engl. hash), voidaan sen avulla luoda omia autentikointipaketteja, koska PLC antaa kirjoitus-, luku- ja ajamisoikeudet muistiinsa saadessaan sellaisen paketin. Hyökkääjä voi siis halutessaan uudelleen lähettää valitsemansa paketin ja autentikoida itsensä [29]. Hyökkääjä voi selvittää monia asioita laitteesta ennen hyökkäyksen tekemistä seuraamalla TCP-liikenteestä esimerkiksi Wiresharkissa, mikä PLC-laiteen sarjanumero ja malli on kyseessä. Pääasiallisesti tutkimuksessa havaittiin, että hyökkäys S7-laitteeseen tehdään seuraavanlaisessa järjestyksessä:

1. Tallennetaan ohjaimen määrittelytyöaseman ISO-TSAP –liikennettä.
2. Seurataan TCP-liikennettä protokolla-analysaattorissa
3. Avataan ja hylätään asiaankuulumattomat paketit
4. Liitetään löydetty hyödyllinen viesti Metasploit-työkalun moduuliin
5. Hyökätään.

Alla olevissa kuvissa ja ohjelmointikoodissa ovat PLC-laitteelle kulkeva kaapattu viesti, jossa on laitteen vastaus työasemalle. Viestistä saadaan tarpeellista tietoa Metasploitin käyttämistä varten. Alla olevassa kuvassa on merkittynä tervehdysviestin sijainti.

```
char peer0_0[] = {
0x03, 0x00, 0x00, 0x16, 0x11, 0xe0, 0x00, 0x00,
0x00, 0x7e, 0x00, 0xc1, 0x02, 0x06, 0x00, 0xc2,
0x02, 0x06, 0x00, 0xc0, 0x01, 0x0a };
```

Kuva 16. ISO-TSAP S7 Probe Client Request –viesti [29].

Laitteen tervehdysviestin voi kopioida suoraan hyökkäyssovelluksen koodiin. Vaikka testi on tehty jo aiemmin, tutkimuksessa käytetyt laitesukupolvet ovat suhteellisen uusia ja voidaan olettaa, että niitä löytyy vielä teollisuuden käytössä. Ainakin Wireshark tukee edelleen PROFIBUS-protokollan lukemista. Lisäksi Wireshark on kirjoittamisen hetkellä mainittuna ja saatavissa PROFIBUS-ryhmän web-sivuilta. Vaikka diplomityön aikana vastaavat laitehankinnat eivät olleet työn tekemistä varten sovittuja hankintoja, on selvää, että työkalut olemassa olevilla saatavuuksilla sopivat vastaavanlaisen hyökkäyksen tekemiseen. Tehty tutkimus sekä diplomityöt ovat julkisia, joten tarkat ohjeet hyökkäyksen tekemiseen on saatavilla kenelle tahansa kiinnostuneelle taholle. Ainoaksi vaihtoehdoksi jää jälleen laitteistojen ulkopuolisen tietoturvatason nostaminen riittäväksi.

Kuva 17. S7 Metasploit-moduulin autentikointipaketti S7-1200:lle [29].

Metasploitin moduulin malli hyökkäyksen tekemistä varten. Alla olevasta ohjelmakoodissa [29] on **lihavoituna** se kohta, johon logiikkakontrollerilta tullut vastausviesti on voitu kopioida suoraan.

```
require 'msf/core'
class Metasploit3 < Msf::Auxiliary

 include Msf::Exploit::Remote::Tcp
 include Msf::Auxiliary::Scanner
 include Msf::Auxiliary::Report
 def initialize
 super(
 'Name' => 'Siemens Simatic S7-1200 PLC Scanner',
 'Version' => '$Revision: 1 $',
 'Description' => 'Locates Simatic S7-1200 PLC device info.',
 'Author' => 'Dillon Beresford <dberesford@nsslabs.com>',
 'License' => MSF_LICENSE
 )
 register_options([ Opt::RPORT(102)], self.class)
 end
def run_host(ip)
begin
pkt = [ "\x03\x00\x00\x16\x11\xe0\x00\x00"+
```

```
 "\x00\x2c\x00\xc1\x02\x06\x00\xc2"+
 "\x02\x06\x00\xc0\x01\x0a",
"\x03\x00\x00\x07\x02\xf0\x00"
 ]

 connect()
 pkt.each do |i|
 sock.put("#{i}")
 sleep(1)
 end
data = sock.get_once().lstrip.gsub(/[ÐÀÁÂ#ðÊ!ðü&ðü_r^ð*ü<\"Ô,\r\n\/]/,").chomp
 print_good("#{ip} is up, iso-tsap is open.")
 print_status("Packet scraping PLC device configuration.")
 print_status("Identification: #{data}".chomp)
 report_note(
 :host => "#{ip}",
 :port => "102",
 :proto => 'tcp',
 :type => "Siemens Simatic S7-1200 PLC",
 :data => Rex::Text.encode_base64("#{data}")
 )
 disconnect()
 rescue ::EOFError
 end
 end
end
```

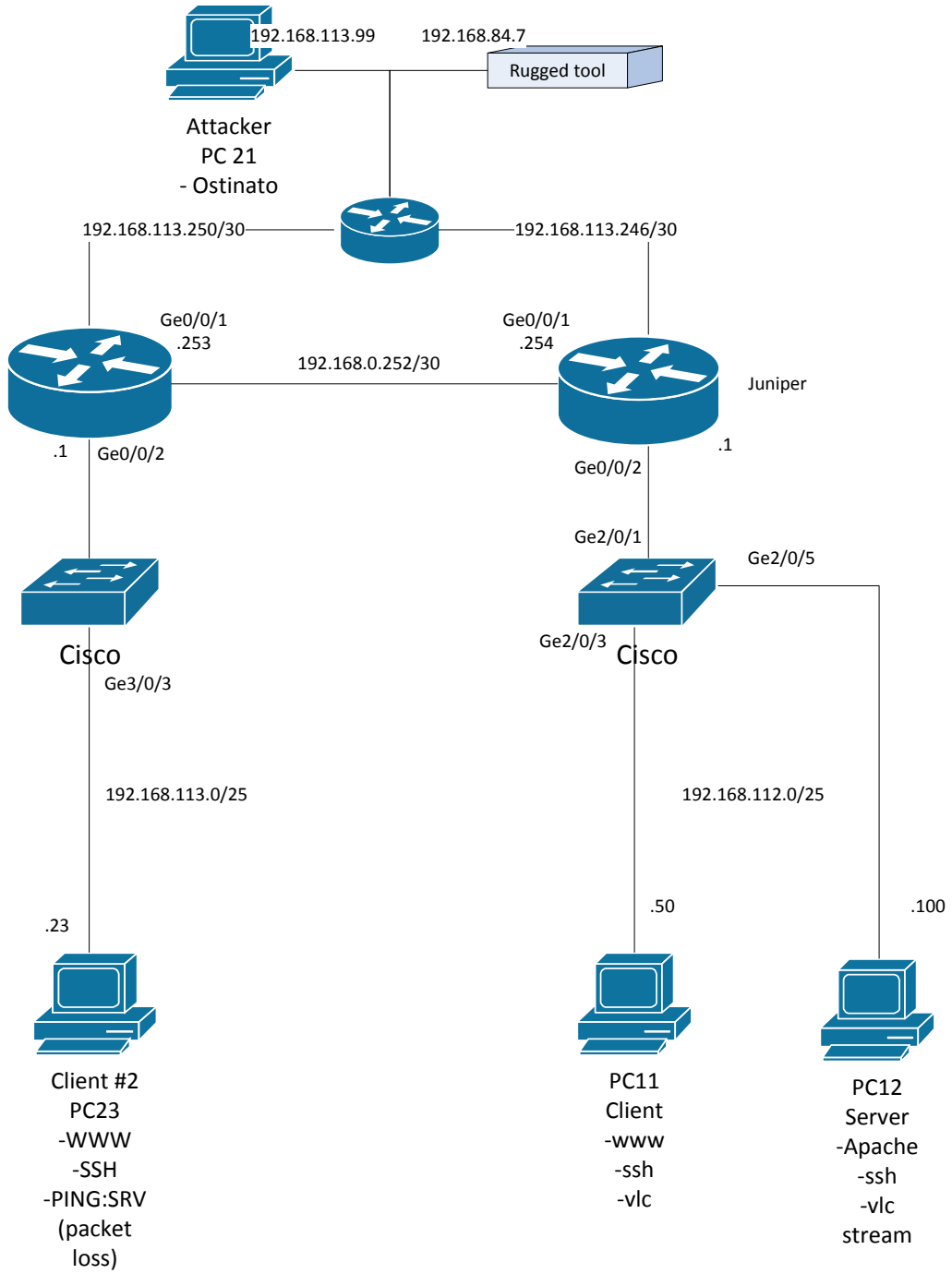
Ohjelma 1. Tervehdysviestin voi liittää hyökkäysohjelmakoodiin.

Kontrolleriin voi siis hyökätä lopulta kohtuullisen yksinkertaisella tavalla. Hyökkäykseen riittää, että käytössä on jokin protokolla-analysaattori ja laitteen oma hallintalaitteisto. Vaihtoehtoisesti tarvittava koodi voi olla mahdollisesti ostettavissakin, jolloin hyökkäyksen tekijän ei tarvitse olla fyysisesti kiinni laitteissa.

5.4 Palvelunestohyökkäys tietoverkkoon

Tässä luvussa käsitellään TTY:n kyberlaboratoriossa tehdyn tietohyökkäyksen tulokset ja niiden analyysi. Hyökkäyksessä käytettiin olemassa olevia Linux-koneita, jotka oli juuri hankittu TTY:n tietoturvallisuuden kursseja varten. Ensimmäisen kokeen ympäristöksi järjestettiin yksinkertainen verkko, jossa oli sekä hyökkäyksen suorittava Linux-PC (Kali). Siemensin automaatiolaitteita ei ollut hankittu erikseen, koska niiden hankkimiseen ei ollut budjettia.

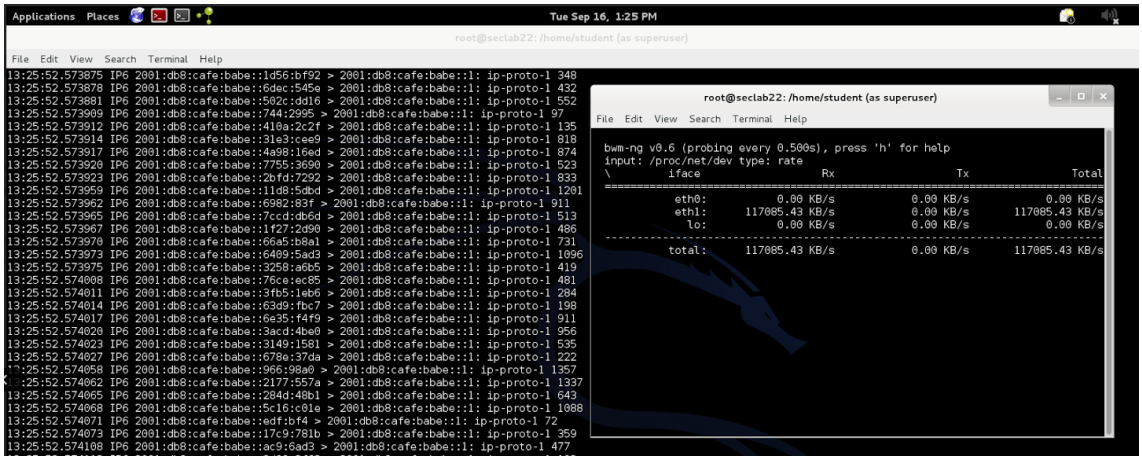
Testaus tehtiin kuvan 18 mukaisessa verkossa, johon oli asennettu sekä Attacker PC, että erillislaite Ruge. Laitteilla lähetettiin paketteja hyökkäyksen kohteena olevalle tietokoneelle. Käytössä olevat laitteet olivat puhtaita asennuksia ja oikeat verkko-osoitteet on kuvassa 18 muunnettu yleisiksi osoitteiksi. Siirrettyä tietoliikenteen määrää seurattiin bwm-ng –sovelluksella, joka näkyy kuvassa 19. Sen avulla voitiin seurata sekä vastaanotettua että lähtevää liikennettä lyhyen ajan keskiarvona joko bitti- tai pakettilukumäärin ilmaistuina kerrallaan.



Kuva 18. Käytössä ollut verkkorakenne.

5.5 Työkalut

Kuvan 19 kaappaus on tilanteesta, jossa vasta kokeillaan bwm-ng -työkalua, joten siinä olevat lukuarvot eivät suoranaisesti liity lopulliseen testiin ja siksi niitä ei käsitellä. Työkaluista kuitenkin juuri Bwm-ng:n käyttäminen ja asentaminen olivat verrattain helppoja tehtäviä. Työkalusta riitti, että sen käynnisti ja muisti seurata, mitä tietoa sen käyttöliittymä tarjosi. Sen sijaan esimerkiksi Ostinaton käyttämistä varten piti ottaa epästabiilien sovellusten asennuskirjastot käyttöön. Lisäksi Ruge piti olla asennettuna erikseen. Liikennöinti lähdekoneesta toteutettiin aina vain yhtä fyysistä tietoliikenneporttia kerrallaan käyttäen. Koska testattavassa ympäristössä kohdekone oli tavallista automaatiokontrolleria tehokkaampi nykyaikainen PC, jolla oli 1Gbps tietoliikenneyhteys, sitä vastaan tehty hyökkäyspakettien lähettäminen tehtiin lisäksi siten, että portin tehoa rajoitettiin 100Mbps:ksi.

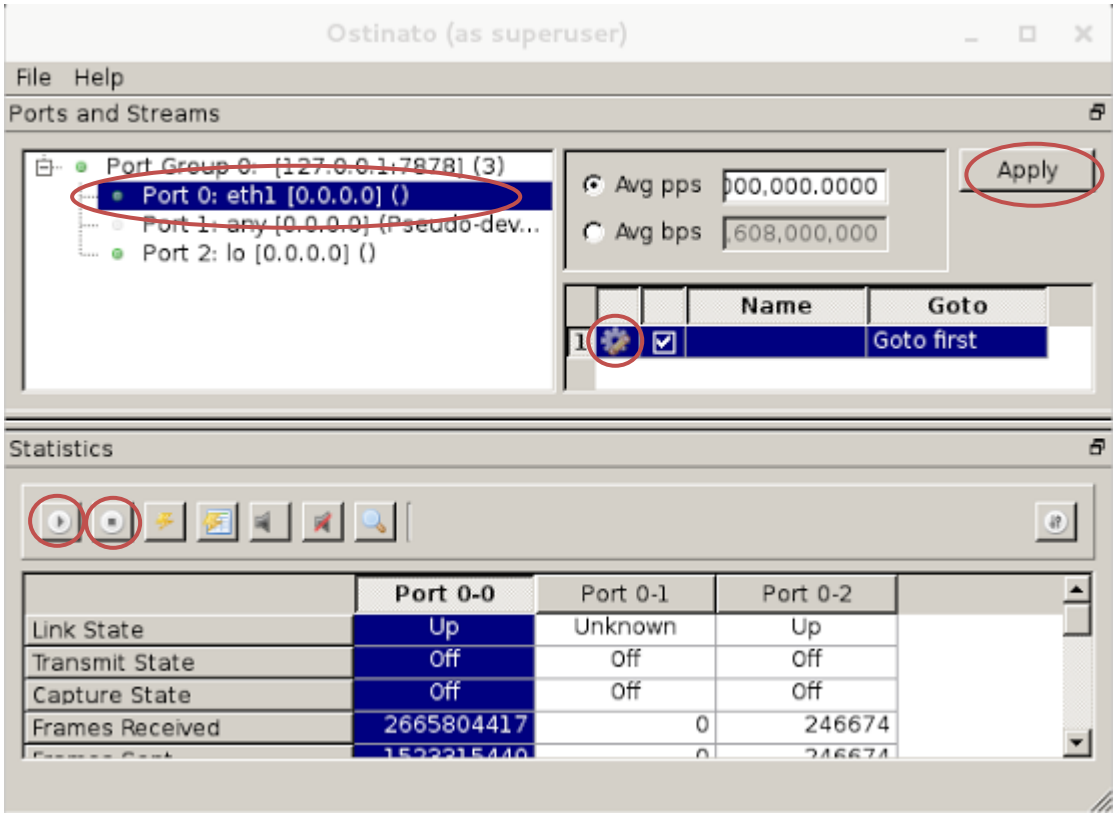


Kuva 19. BWM-ng on sovellus, jolla tarkkailtiin hyökkäyksen kohteeksi joutuneen koneen vastaanottaman ja lähettämän liikenteen nopeutta.

Ostinato on avoimen lähdekoodin tietoliikennegeneraattori. Sen asetuksissa voitiin säätää erikseen, millaisia paketteja kohdekoneelle lähetettäisiin. Työkalun asetuksissa pystyttiin valitsemaan, mitä protokollia paketti käyttäisi ja kuinka paljon ja minkä suuruisia paketteja lähetettäisiin sekunnissa. Myös tämän työkalun käyttöliittymä oli kuitenkin melko selkeä, kuten kuvissa 20 ja 21 näkyy.

Testien toimivuus varmistettiin siten, että lähetettiin ICMP echo request -paketteja (komennolla: ping –i 0.1 –c 100 192.168.x.x) ja mitattiin pakettien hävikkiä kohdekoneella sen omassa lähiverkossa PC11:n ja PC12:n välillä sekä hyökkääjän omasta lähiverkosta kolme kertaa ja laskemalla niiden keskiarvot. Komennon lisäasetuksilla saatiin lähetettyä ping-testipaketti 100 kertaa 0.1 sekunnin intervallein, jolloin testaaminen nopeutui huomattavasti. Selvisi, että kohdekone harvoin kärsi omassa verkossaan, mutta ulkoa päin tulevan liikenteen paketteja sen sijaan hukkui paljon useammin.

Pakettien koon säätäminen oli työlästä Rugessa, mutta ne onnistuttiin kuitenkin saamaan vastaamaan Ostinatolla lähetettyjen pakettien kokoa syöttämällä jokainen pakettimääritys manuaalisesti.



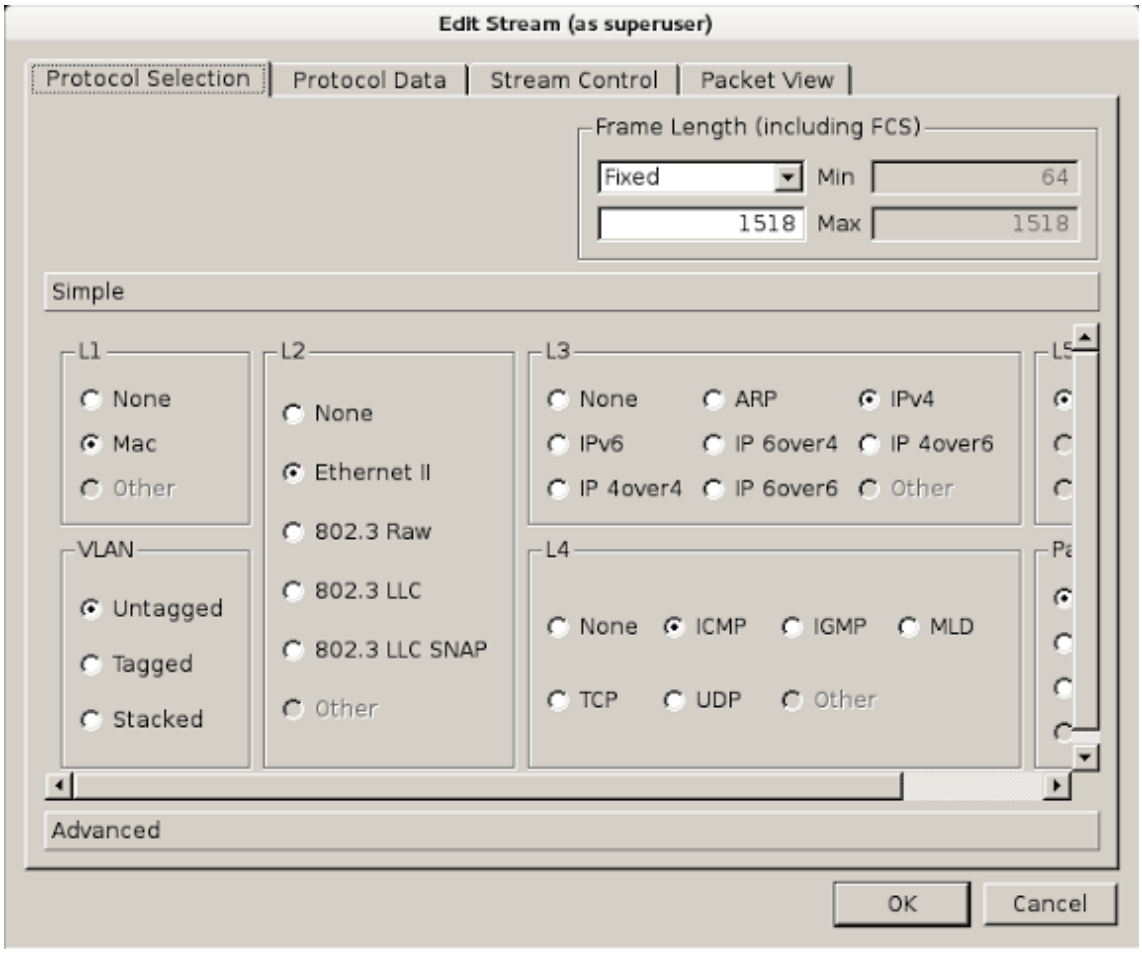
Kuva 20. Ostinato-työkalun päänäkymä.

Pakettien koko aloitettiin molemmilla työkaluilla 64 tavusta ja lopetettiin 1518:aan. Työkalun käyttö ei asettanut muita rajoituksia pakettien laillisen lähetyskoon säätämisessä, mutta Ostinatossa paketin koko piti aina erikseen säätää 4 tavua suuremmaksi kuin mitä oli tarkoitus lähettää, Rugessa sen sijaan yhtä tavua pienemmäksi. Ostinatolla ainoastaan maksimikokoa lähettäessä paketin kooksi pystyttiin laittamaan tasan 1518.

Ostinaton päänäkymässä oli tieto pakettien lähettämiseen käytettävästä tietoliikennerajapinnasta. Päänäkymä tarjosi toiminnallisuudet käynnistää ja sammuttaa tietoliikenteen lähetys sekä päivittää ja ottaa käyttöön asetuksissa viimeksi tehdyt muutokset. Pakettien koon säätäminen oli helppoa. Paketteihin liittyvät asetukset piti käydä ensin tekemässä ympyröidyn rataskuvakkeen kautta toisessa näkymässä. Sen jälkeen juuri tehdyt asetukset voitiin päivittää työkaluun tässä näkymässä, kunhan tietoliikenne oli ensin varmasti pysäytetty.

Ostinatolla asetukset olivat:
Payload size: 64-1518
Number of packets: 100

Packets per second: 2,000,000
After this stream: Goto first



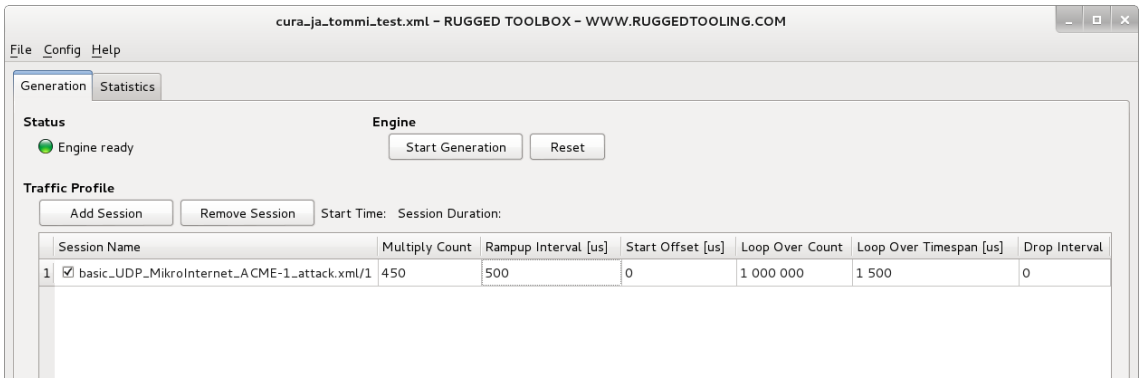
Kuva 21. Ostinaton oleelliset asetukset säädettiin tässä näkymässä.

Työkalun kaikkiin asetuksiin ei siis tarvinnut edes koskea, vaan riitti, että Ostinaton lähettämän liikenteen yksityiskohtiin määriteltiin sopiva pakettikoko, paljonko paketteja piti lähteä sekunnissa, käytettiinkö IPv4- vai jotakin muuta L3 protokollaa ja tietysti, oliko kyseessä TCP, vai UDP. TCP-liikennettä määritellessä täytyi kuitenkin määritellä SYN-viestin lähetys, jotta liikennettä saatiin ylipäänsä aikaiseksi. Työn määrä ennen liikenteen aloittamista oli siis hyötyyn nähden vähäinen.

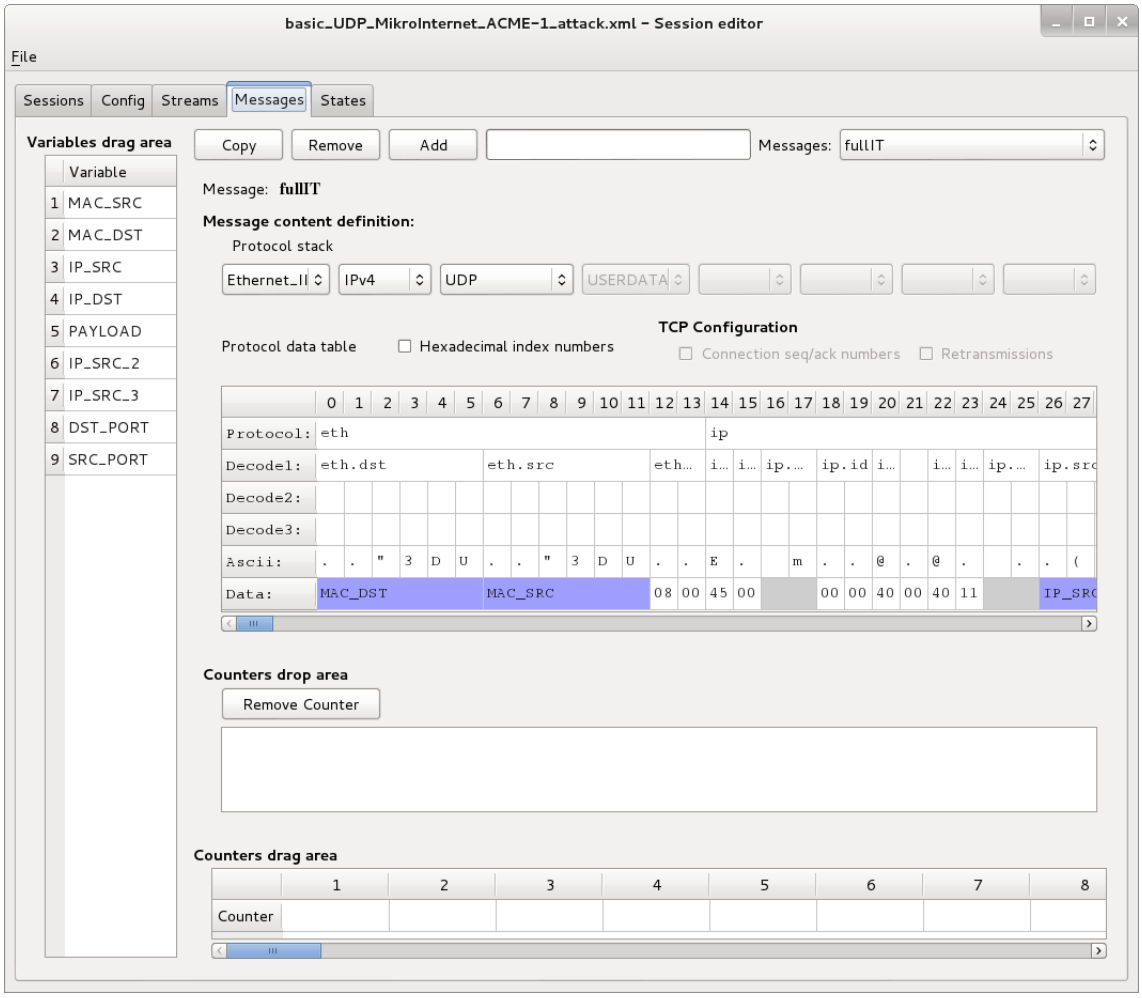
Ostinaton lisäksi käytettiin työkalua Ruge. Koska työkalua ei oltu juuri käytetty aiemmin, oikeat asetukset suurimman tietoliikennemäärän aikaansaamiseksi jouduttiin hakemaan iteroimalla. Työkalulle oli olemassa onneksi manuaali, josta sen asetusten merkitykset avautuivat hieman paremmin.

Kuvissa 22-25 näkyy, miten Rugella piti tehdä asetukset, jotta tarvittavat vastaavanlaiset paketit saatiin lähetettyä. Työkalu oli siinä mielessä paljon monipuolisempi kuin Ostinato, mutta toisaalta käytettävyydeltään aika alkutekijöissään. Syy kahden työkalun käyttämiseen tätä yksinkertaista hyökkäystä tehdessä nähtiin välttämättömäksi, koska ei

voitu taata, että avoimen lähdekoodin epävakaaksi luokiteltu sovellus (Ostinato) lähettäisi varmuudella sellaista määrää tietovirtaa, kuin oli tarkoitus, vaikka tietovirran kulkua valvottiinkin bwm-ng -työkalulla erikseen. Työn luonteen vuoksi ei kuitenkaan voitu käyttää laittomia Internetistä löytyviä sovelluksia, joiden avulla olisi voitu tehdä oikea hajautettu palvelunestohyökkäys, mutta Ruge lisäksi tarjosi mahdollisuuden siihen, että lähetettyjen pakettien lähdeosoitteet olivat satunnaisia, joka vastaa vähän paremmin hajautettua tietohyökkäystä.



Kuva 22. Ruge-työkalun päänäkymä.



Kuva 23. Paketin protokollapino ja sisältö määriteltiin erikseen.

Kuvassa 22 on Ruge-työkalun päänäkymä. Siinä määriteltiin, mitä esimääriteltyä liikennevirtaa lähetettiin ja lähinnä näkymä palveli siinä, että sen avulla pystyi aloittamaan ja lopettamaan lähetyksen.

Tässä työssä valittiin lähetettäväksi UDP-liikennettä ja lähetettävien pakettien sisältö määriteltiin erikseen toisessa näkymässä. Erilaisia pakettikokoja tarkasteltiin sen vuoksi, että saataisiin selville, millainen pakettikoko tukkisi eniten esimerkiksi automaatiolaitteiden verkon reunareitittimen.

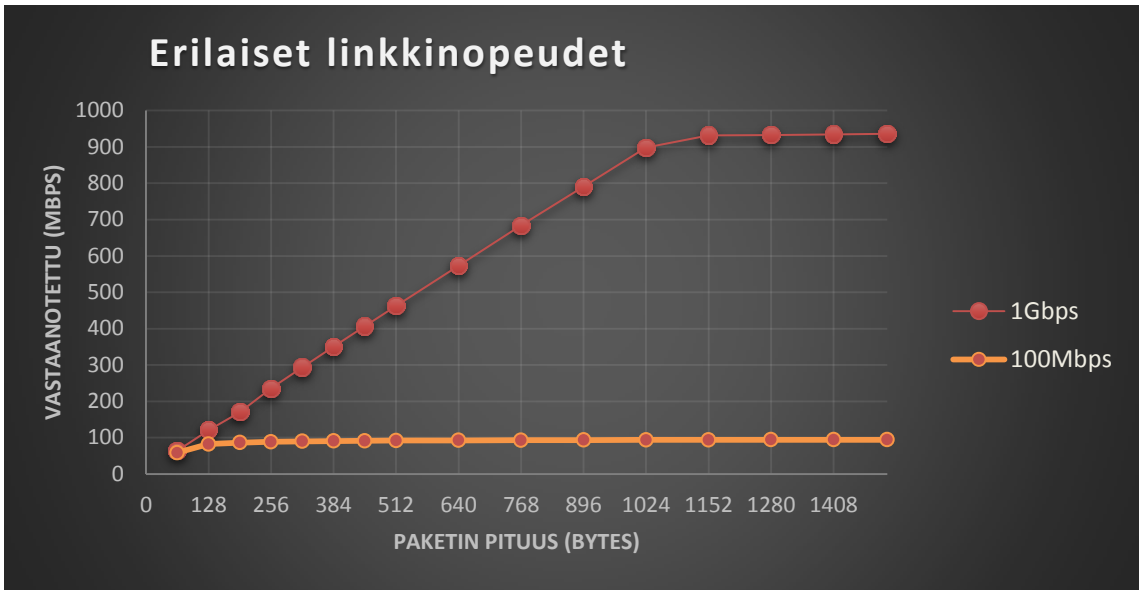
Työkalun ohjekirjasta piti ensin selvittää, mitä rivillä näkyvät asetukset tarkoittivat. Sessio oli määritelty erikseen xml-tiedostossa, mutta myös näkyvissä olevat asetukset vaikuttivat silti hyvin paljon siihen, miten suuri tietoliikennemäärä lopulta lähti liikkeelle kohti hyökkäyksen kohdekonetta. Kuvassa 23 vasemmalla näkyvät muuttujat voitiin lisäillä lähetettävään pakettiin kätevästi hiirellä, mutta ne piti ensin määritellä Config-välilehdellä.

5.6 Tulokset

Teollisessa automaatioverkossa kulkee kerrallaan kohtuullisen pieniä tietomääriä, mutta on erityisen tärkeää, että viestit menevät perille. On siis käytännöllistä tietää, miten liikennettä kannattaa säätää, jos halutaan varautua verkon satunnaiskuormituksiin. ICMP echo requestit ovat kohtuullisen pieniä paketteja eivätkä juuri vaadi käsittelyresursseja eivätkä kaistaa. Siksi niiden katsottiinkin olevan sopivia tietoliikenteen hävikin mittaamiseen.

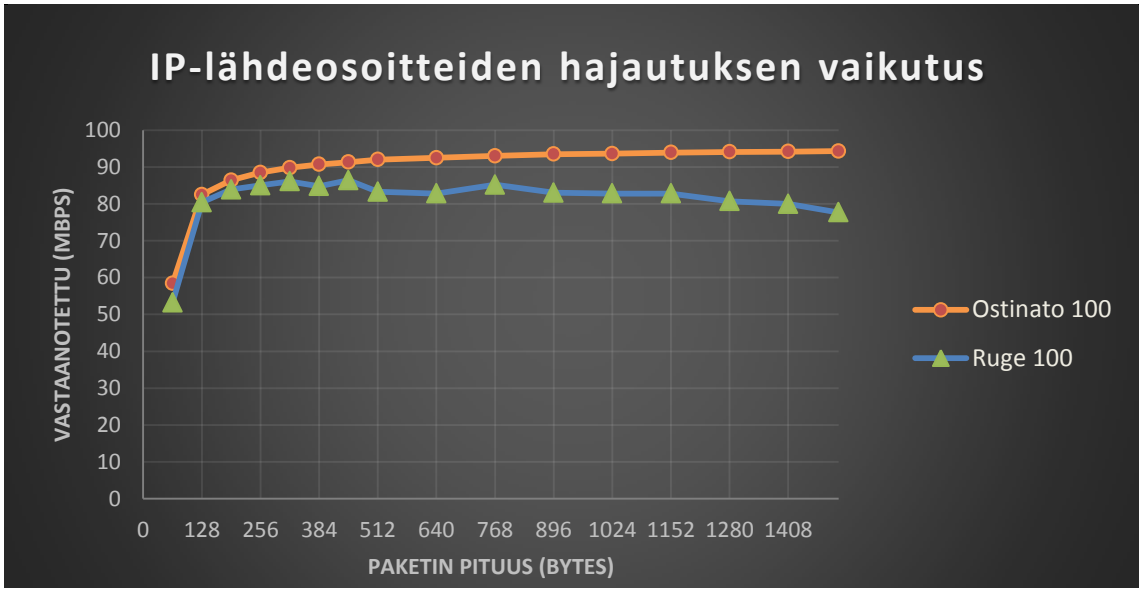
Testin tarkoitus oli simuloida palvelunestohyökkäystä ja haitata kohdekoneen vastaanottokykyä muun kuin haittaliikenteen suhteen. Haittaliikenne tehtiin siten, että kohdekoneelle lähetettiin tietoliikennegeneraattorilla muodostettuja keskenään samankokoisia UDP-paketteja mahdollisimman paljon. Lähetykset tulivat kerrallaan joko yhdestä tai useasta lähdeosoitteesta. Samaan aikaan mitattiin, minkä verran ICMP echo request -paketteja häviää sekä sisäverkosta että ulkoverkossa sijaitsevassa tietokoneessa mitattuina. Tässä luvussa sisäverkko viittaa samassa aliverkossa keskenään oleviin kahteen tietokoneeseen PC11 ja PC12, joista PC12 oli liikennegeneraattorien kohdekone. Ulkoverkolla tarkoitetaan Ostinaton ja Rugen verkkoa. Ulkoverkoksi lasketaan myös PC23:n verkko, josta mitattiin ulkoverkosta lähetettävien ICMP-pakettien häviö.

Ostinato ja Ruge sijaitsivat keskenään samassa verkossa. Molempien kohdekoneena oli PC12, jonka vastaanottokykyä testattiin sekä 100Mbps:n että 1Gbps:n linkeillä sen mukaan, miten tuloksissa oli odotettavissa eroavaisuuksia. Samalla, kun kohdekoneen linkkiä kuormitettiin joko Ostinaton tai Rugen generoimalla UDP-liikenteellä, mitattiin ICMP echo request -pakettien prosentuaalinen hukkumismäärä kolmen mittauksen keskiarvona sen omassa verkossa sekä ulkoverkosta käsin.



Kuva 24. Oranssi kuvaaja kertoo 1Gbps -linkin ja punainen kuvaaja 100Mbps -linkin vastaanottaman UDP-liikenteen PC11:ssä. Liikenteen lähteenä Ostinato.

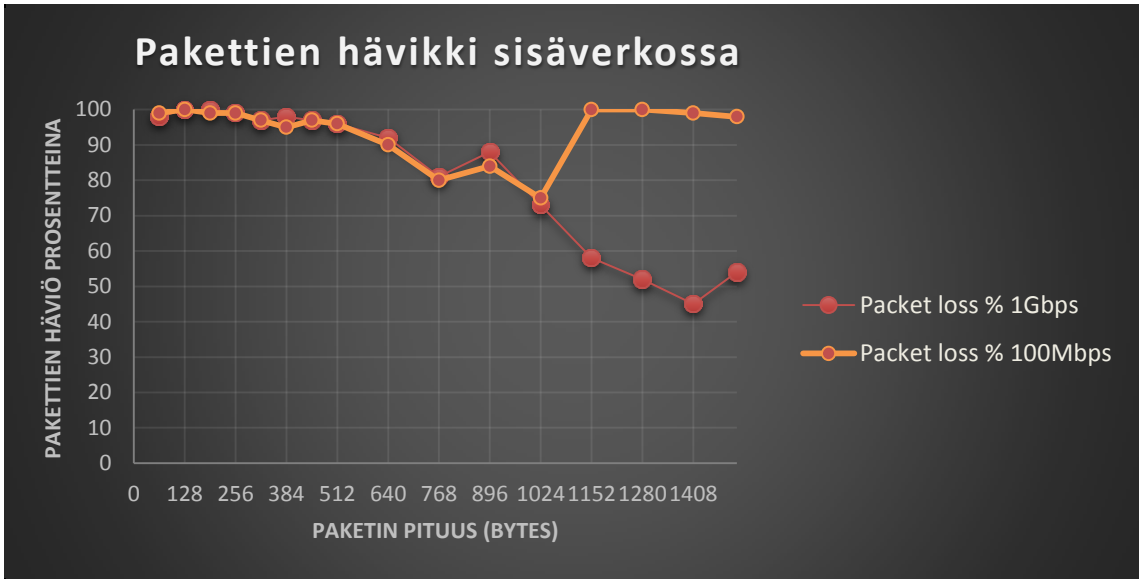
Automaatiolaitteistossa on todennäköisesti pienempi tiedonkäsittelykapasiteetti kuin nykyaikaisessa PC-tietokoneessa. Sellaisessa ympäristössä vastaanotto reagoi todennäköisesti samalla tavalla kuin kuvan 24 alempi kuvaaja. Joka tapauksessa kuvaajasta näkee, että vastaanotetun liikenteen määrä kasvaa suurimpaan vasta suuremmilla pakettikokoluokilla.



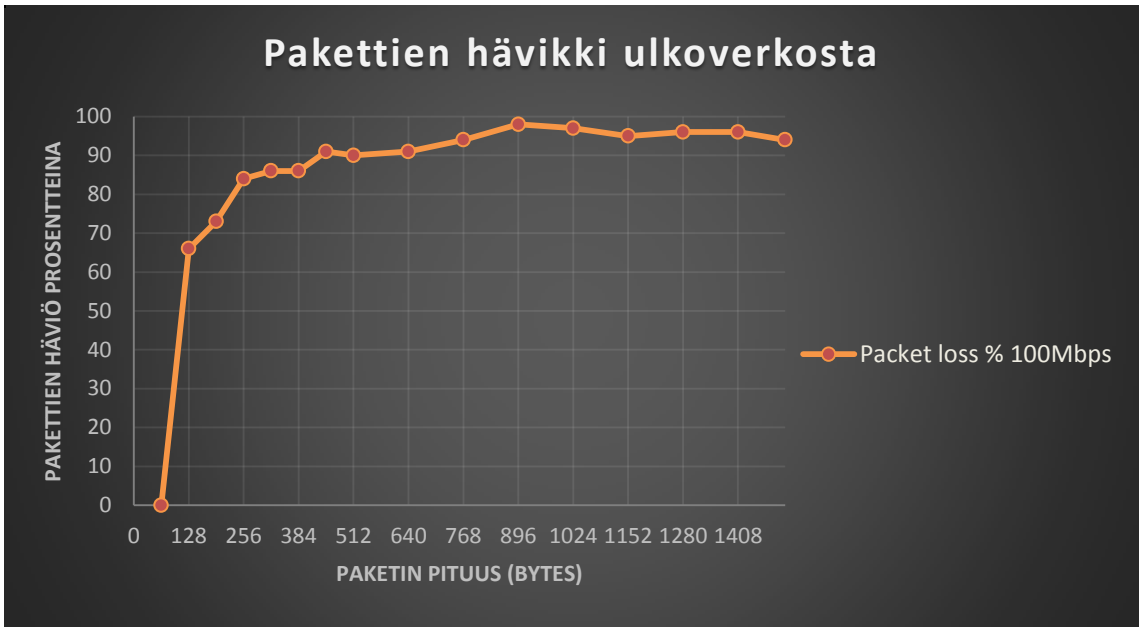
Kuva 25. IP-lähdeosoitteet hajautettiin Rugessa. Kuvaajana hajautuksen vaikutus suhteessa pakettikokoon. UDP-liikenteen lähteenä Ostinato ja Ruge, kohteena PC11 100Mbps:n linkillä.

Kun sama testi tehdään Ruge-työkalulla, joka hajautti lähdeosoitteet saavuttamattomiksi satunnaisosoitteiksi, kuvassa 25 näkyy sen vaikutus uutena kuvaajana. Ero ei näyttäisi olevan kovin merkittävä, mutta vastaanottaja käyttää silti noin 10% vastaanottamasta liikenteestään ICMP Destination unreachable -viesteihin. Vastaanotetun datan määrä tietenkin parani, kun Ruge säädettiin lähettämään liikennettä vain yhdestä osoitteesta. Silloin liikennemäärissä ei enää näkynyt eroa.

Laboratoriokokeessa testattiin myös, miten pakettien häviöt muuttuvat suhteessa lähetettyjen pakettien kokoon. Tulokset olivat samat myös TCP-likenteellä. Kokeen tästä vaiheesta voidaan päätellä, ettei ostetuilla pakettigeneraattoreilla ole kovin yksinkertaista tukkia liikennettä, jos käytössä on vain yksi lähde. Jos lähteet hajautetaan väärentämällä lähdeosoitteet, tilanne paranee hieman hyökkääjän kannalta, muttei merkittävästi.



Kuva 26. ICMP Echo request -pakettien hävikki vastaanottavan laitteen (PC12) sisäverkossa 1Gps ja 100Mbps –linkeissä Ostinatolta tulevan UDP-kuormituksen aikoina. Pakettihävikki laskettiin ICMP-liikenteestä, jota PC11 generoi P12:lle ping-ohjelmalla.



Kuva 27. ICMP Echo request -pakettien hävikki ulkoverkosta tulevalle liikenteelle vastaanottavan koneen 100Mbps linkillä. Lähteenä Ostinato. DoS-liikenteen lähteenä on Ostinato ja pakettihävikki laskettiin ICMP-liikenteestä, jota PC23 generoi P11:lle ping-ohjelmalla.

Ongelmaksi palvelunestohyökkäystä suunnittelevalle rikollisille muodostuu se, että kohteena olevan laitteen sisäverkon liikenne ei kovin helposti häiriinny, ellei esimerkiksi sama reititin ole vastuussa sekä yrityksen laitteiden sisäverkosta, että ulkoverkosta. Kuvassa 25 näkyy, miten pakettien hävikki laski hieman, kun lähteenä toimi työkalu,

joka hajautti IP-lähdeosoitteet. Syy hävikin muuttumiseen tähän jäi epäselväksi, mutta huomioitavaa oli, että suuremmilla paketeilla on ainakin periaatteessa paremmat mahdollisuudet tehdä resurssienkulutukseen kohdistuva palvelunestohyökkäys. Tehokas palvelunestohyökkäys on siis toteutettava mahdollisimman suurella määrällä hajautettuja lähteitä esimerkiksi bottiverkon avulla. Bottiverkon käyttäminen olisi ollut tämän työn aihealueen sisällä, mutta lainvastainen ja jäi sen vuoksi toteuttamatta.

6 KESKUSTELU

Tämä työ tutki pääasiassa teoriapainotteisesti Internetiin kytketyn teollisuusautomaatioverkon tietoturvaongelmia. Työn tarkoitus oli löytää järkeviä tapoja suojata tällainen ympäristö nykyaikaiselta verkkorikollisuudelta sekä kiteyttää asiasta olevaa tutkimustietoa. Työn kokeellinen osuus suoritettiin saatavilla olevilla laitteistoilla, eli pääosin Linux-käyttöjärjestelmää käyttävillä PC–tietokoneilla ja sekä ostetuilla lisenssityökaluilla että ilmaisilla avoimen lähdekoodin sovelluksilla. Työssä käsiteltiin tietokoneiden lisäksi erilaisia teollisen verkon laitteita ja niiden rooleja. Lisäksi avattiin aiheesta tehtyjen tutkimusten tuloksia ja vertailtiin niitä laboratoriossa tehtyjen hyökkäysten tuloksiin. Suurena haasteena työssä oli, että sen puitteissa ei ollut mahdollista hankkia ja rakentaa omaa automaatioverkkoa automaatiolaitteineen eikä siten varsinaisesti suoraan testata teollista automaatioverkkoa. Internetistä löytyvien työkalujen ja tutkimusten avulla työtä varten saatiin kuitenkin aikaan aineistoa hyvin runsaasti ja lopulta tulosten ja aineistojen avulla saatiin kasvatettua ymmärrystä valmistusteollisuuden tietoturvahaasteista.

Teoriaa kirjoittaessa oli huomioitavaa, että suuri osa teollisuudessa olevista laitteistoista on varustettu Internet-yhteydellä, mutta valitettavan monen laitteen pystyi näkemään ja lisäksi niiden palvelut pystyi havaitsemaan lähes vaivatta. Lisäksi selvisi, että laitteiden käyttöikä on jopa vuosikymmeniä ja tietoturvan päivittäminen on sekä kallista, että usein lähes pidetty kannattamattomana suhteessa tuotannon keskeytymisestä aiheutuviin kuluihin. Lisäksi automaatioverkkojen laitteiden välinen keskustelu oli suoraan luettavissa protokolla-analysaattorilla ja oli selkokielistä.

Työn yhtenä kokeellisena osana oli tehdä yksinkertainen palvelunestohyökkäys PC-ympäristössä, jotta voitaisiin nähdä, miten paljon liikennettä pitää tehdä, että se haittaisi mahdollisesti myös automaatiolaitteita. Testien tuloksena saatiin, että pienet paketit kulkevat suurestakin kuormasta huolimatta lähiverkossa aika pitkään, vaikka häiriöliikennettä olisi ollut paljon. Vastaavasti suurempia paketteja käyttävä liikenne sekä verkkorajapintaa kuormittavat ongelmat näyttäisivät saavan jalansijaa ongelmien luomisessa. Automaatioverkkojen toimintaa simuloineessa tutkimuksessa selvisi, että aiheutetun palvelunestohyökkäyksen kohteen etäisyys tuotantolinjasta on kääntäen verrannollinen hyökkäyksen aiheuttamaan haittaan. Eli, mitä suurempi kohteen etäisyys oli tuotannosta, sen paremmin järjestelmä siitä selvisi. Sen sijaan, jos käytettyyn laitteistoon tai automaatioverkon reitittimeen pääsi murtautumaan, hyökkäävällä taholla olisi helposti mahdollisuuksia tehdä jopa suoranaista haittaa tuotannolle. Tästä johtopäätöksenä on, että yksin automaatioverkon ulkopuolisen laitteiston turvaaminen ei riitä takaamaan

edes alkeellista tietoturvaa valmistusteollisuuden tarpeisiin. Koska uhkina on sekä tuotannon haittaaminen että muun muassa teollisuusvakoilu jopa valtiotaholla, automaatioverkon ulkopuolisen turvaamisen lisäksi tarvitaan ehdottomasti myös ratkaisuja, jotka kohdistuvat myös suoraan sisäisen automaatioverkon toiminnallisuuksiin ja esimerkiksi käyttäjien valvontaan. Nykyaikaisia automaatiolaitteistoja ja -verkkoja käyttävien yritysten tietoturvahaasteet ovat siis vielä pitkään ongelma, koska tietoturvan ylläpitäminen on niissä toimistoverkkoja monipuolisempaa ja vaativampaa samalla, kun osaajia on suhteessa paljon vähemmän.

Osa toimistoverkon tietoturvaosaamisesta on kuitenkin suoraan sovellettavissa teollisuusverkkoihin. Tietoturvaa rakennetaan tällä hetkellä jo standardoimalla sekä EU:ssa, että sen ulkopuolella. Silti työ tuntuisi olevan vielä aika alussa ja tarvitaan paljon yhdenmukaisia ratkaisuja, jolla esimerkiksi käytettävät tietoliikenneprotokollat saataisiin turvallisemmiksi ja esimerkiksi VPN- ja sovelletut IDS-ratkaisut vakiokäytännöiksi.

On selvää, että kannattavuustarkastelua on tehtävä jokaisen automaatioverkon rakentamisen yhteydessä sekä kustannusten että käytön tehokkuuden suhteen. Jos ylläpito on tehnyt palveluntarjoajan kanssa sopimuksen ja laitteiden käyttörajoitukset ja päivitykset toteutetaan tietoturvallisuutta silmälläpitäen, ainakin suurimman määrän uhkia voidaan katsoa väistetyn. Automaatiojärjestelmässä kaikkein tärkeintä on yleensä se, että laitteille tarkoitetut ohjausviestit kulkevat nopeasti eivätkä ne katoa matkalla. Turvalliselle ratkaisulle teollisessa järjestelmässä onkin vähimmäisvaatimus, että SCADA-järjestelmän toiminnallisuutta hajautettaisiin mahdollisimman vähän, eikä esimerkiksi lokitoimintoja ja etäohjausmahdollisuuksia asennettaisi pilvipalveluympäristöön, ellei se olisi välttämätöntä. Ylläpitäjän täytyy nykyisillä vaatimuksilla eriyttää automaatioverkon laitteet reitityksen ja palomuurien avulla suojavyöhykkeellä sekä yrityksen toimistoverkosta. Lisäksi muun muassa viranomaisten vaatimien tietoturva-aukkojen olemassaolo pitäisi voida ottaa huomioon ja määritellä tarkemmin, ettei rikollisille tahoille jäisi liian suuria mahdollisuuksia. Teollisuusautomaatioverkkojen tietoturvan parantaminen ja sen tutkiminen vaatii tulevaisuudessa lisää avoimuutta ja erityisesti yhteistyötä. Yhteistyön on oltava sekä maiden että eri teknologia-alojen välistä.

7 YHTEENVETO

Automaatiojärjestelmän verkolla on paljon erityispiirteitä yleiseen toimistoverkkoon nähden. Ihmisten terveyden ja turvallisuuden varmistaminen sekä laitteistojen suojaaminen vahingoilta ovat tavoitteita, joita toimistoverkoissa yleensä kohdataan hieman toisenlaisessa mittakaavassa. Lisäksi on tärkeää, että laitteistoilla valmistettavat tuotteet ovat laadukkaita ja, että tuotantotoiminta jatkuu häiriöittä.

Tietoturvatavoite toimistoverkossa keskittyy suojelemaan palvelimeen tallennettuja tietoja, mutta hajautetussa tuotantojärjestelmässä yksiköiden toiminta on tärkeämpää kuin keskuksen toiminta. Lisäksi automaatiojärjestelmän jatkuvuusvaatimuksesta johtuen, odottamattomat pysäytykset tuotannon toiminnassa eivät ole yhtä hyväksyttyjä kuin toimistoverkoissa. Esimerkiksi toistuvat uudelleenkäynnistykset eivät siis ole käytännön syistä mahdollisia. Siksi on tärkeää estää esimerkiksi henkilövalvonnalla asiattomien käyttäjien pääsy ohjelmointirajapintoihin sekä verkossa, mutta myös tuotantolaitteiston läheisyydessä. Joidenkin automaatiolaitteiden liikennöintiä pystyy lukemaan suoraan, joten työn aikana ilmenneiden tietojen valossa on välttämätöntä pyrkiä eristämään kaikkein kriittisimmät toimialueet sekä lähi-, että etäkäytöltä.

Tämä työ osoitti, että siinä, missä toimistojärjestelmät eivätkä sen käyttäjät aina kärsi kohtuuttomasti satunnaisen vikatilanteen, laitteistosta johtuvan muun viiveen tai lyhyehkön palvelunestohyökkäyksen sattuessa, automaatiojärjestelmät ovat erilaisia. Jos automaatiojärjestelmä pysähtyy odottamatta, koska järjestelmän jokin vaihe ei saa uutta toimintoa ajoissa, niin sanottu ei-toivottu seuraus on vakavuudeltaan paljon haitallisempi kuin toimistossa. Siksi esimerkiksi hätäpysäytystä ei voida ohjelmoida verkkoyhteyden tai tekstiviestin taakse. Tehdasympäristön olosuhteissa tällaista vikaa ei kuitenkaan välttämättä ymmärretä liittää tietohyökkäykseen, vaan ajatellaan helposti, että kyseessä on vain satunnainen tekninen häiriö. Ongelma saattaa jäädä korjaamatta ja hyökkääjä saa jatkaa toimintojaan rauhassa.

Samanlaisen ongelman luovat myös laitteistojen sovellusten päivitykset. Järjestelmien tulee saada toimia häiriöittä ja keskeytyksittä. Vaikka päivitys sujuisikin nopeasti, päivityksen tekijän täytyy tuntea muuttuneen ohjelmiston aiheuttamat vaikutukset tarkkaan. Muutosten testaaminen vaatii joskus toiminnan simulointia tai erityisolosuhteita ja aiheuttaa siten sen, että vaikka äkillisesti löytyneeseen tietoturvaongelmaan olisikin ratkaisu, sitä ei voida välttämättä toteuttaa heti, tai ollenkaan. Sen vuoksi ratkaisua suunnitellessa tulee ottaa huomioon esimerkiksi mahdollisuus käyttää vain hetkellisesti verkko-

yhteyttä hyödyntävää päivityspalvelinta, pakettisuotimia, virus-skannereita, heuristisia tunnistusmenetelmiä vääränlaisen liikenteen havaitsemiseen sekä kaikkia turvallisuusnormeiksi havaittuja toimintamalleja, laitteita ja sovelluksia tuotantojärjestelmän kriittisyyden ja verkkokytkentäisyyden mukaan.

Toimistosovelluksilla on yleensä saatavilla asiantuntijoita, mutta automaatiosovellusten toimintaan ja ylläpitoon tarvitaan myös erityisosaajia. Lisäksi monissa järjestelmissä ei ole mahdollisuuksia salauksiin, salasanasuojauksiin tai oikeastaan muihinkaan tietoturvateknologioihin. Sen vuoksi tietoturva olisi tällöin toteutettava teollisuuslaitteiston ulkopuolisilla laitteilla, esimerkiksi eristämällä järjestelmä yrityksen toimiston tietoverkosta.

Arvio siitä, millaisen tietoturvallisen teollisen automaatioverkon rakenteen sitten tulisi olla, kun se on liitetty Internetiin, on monisyinen. Työn aikana tehdyt kokeet ja muiden tutkimusten analysointi osoittivat, että on triviaalia löytää automaatiolaitteita palveluineen Internetistä. Lisäksi niihin on monia erilaisia mahdollisuuksia hyökätä ja ottaa niiden toiminta haltuun. Reitittimiä vastaan voidaan tehdä useita erilaisia hajautettuja palvelunestohyökkäyksiä, mutta eivät palomuuritkaan aukottomia ole. Hajauttamalla reitittimien vastuita, eli jakamalla yrityksen verkko palomuurien ja reitittimien avulla, voidaan päästä jo kohtuulliseen suojauksen tasoon. Verkossa tulee tietysti olla tarkat määrittelyt siitä, mitä liikennettä siinä saa liikkua ja yrityksen toimistoverkon käytetyissä laitteissa tulee olla ajantasainen virustorjuntaohjelmisto. Tasoon vaikuttaa lisäksi henkilökunnan tietoturvatietoisuus sekä laitteiston muunkin ohjelmiston ylläpito, esimerkiksi selainohjelmien lisäosien kohdalla.

Kun varmistutaan myös, että kaikki automaatiolaitteisiin muodostetut yhteydet tehdään VPN-, tai muulla salatulla yhteydellä, laitteiden käyttöä valvotaan, mahdollisen toimistoverkon laitteiden ja myös reititinlaitteiston ohjelmisto pidetään päivitettyinä, päästään jo hieman edemmäs kohti turvattua automaatioverkkoa. Lisäksi olisi hyvä sopia palveluntarjoajan kanssa varasuunnitelmasta esimerkiksi juuri palvelunestohyökkäyksen varalta sekä ylläpitäjän varautua omassa verkossaan siihen, että ohjauskomennot eivät ole täysin riippuvaisia yhdestäkään yksittäisestä reitistä tai reitittimestä.

Työn lähtökohta, Kuva 1, oli lopulta oikeastaan aika hyvä turvallista verkkoa toteutettaessa sillä erotuksella, että SCADA-järjestelmässä on kuitenkin selkeästi turvallisempaa pitää lokitiedostot ja tietokannat mieluummin lähellä käyttäjän verkkoa kuin etäyhteyden päässä. Mutta koska SCADA pääosin toimii hajautettuna järjestelmänä, tällainen toimintamalli varmasti täytyy suunnitella joihinkin järjestelmiin. Jos toiminnallisuutta halutaan siten käyttää ja valvoa etäyhteyden välityksellä, sen saavutettavuuden varmentaminen kannattaa sopia palveluntarjoajan kanssa.

LÄHDELUETTELO

[1] Viestintävirasto, ”Automaation Tietoturva. Verkottumisen riskit ja niiden hallinta,” 2010. [Verkossa]. Saatavissa: https://www.viestintavirasto.fi/attachments/cip/5na1SblCp/SAS29_TeollisuusautomaationTietoturva.pdf. [Haettu 14.10.2014].

[2] C. A. Ptak, ERP: Tools, Techniques and Applications for Integrating Supply Chain, CRC Press, 2004.

[3] Siemens, ”Working with Step 7,” 2010. [Verkossa]. Saatavissa: http://www.automation.siemens.com/doconweb/pdf/SINUMERIK_SINAMICS_03_2013_E/S7_GS.pdf?p=1. [Haettu 10.10.2014].

[4] Profibus, ”www.profibus.com,” Profibus, 10 October 2014. [Verkossa]. Saatavissa: http://www.profibus.com/technology/profinet/overview/. [Haettu 10.10.2014].

[5] Jukka Koskinen et. al, ”Yhteisöt tietoturvan uhkana ja suojana,” 30.5.2012. [Verkossa]. Saatavissa: http://www.cs.tut.fi/kurssit/TLT-3700/socsec-sem.pdf. [Haettu 14.10.2014].

[6] O. source, ”Freenet,” Open source, 2014. [Verkossa]. Saatavissa: https://freenetproject.org/. [Haettu 10.10.2014].

[7] The Tor Project Inc., ”Tor project, Anonymity Online,” The Tor Project Inc., 2014. [Verkossa]. Saatavissa: https://www.torproject.org/index.html.en. [Haettu 10.10.2014].

[8] Symantec, ”Botit ja bottiverkot - kasvava uhka,” Symantec, 2014. [Verkossa]. Saatavissa: http://fi.norton.com/botnet. [Haettu 19.10.2014].

[9] Saman Taghavi Zargar et al., ”A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,” IEEE Communications surveys & Tutorials, vol 15. NO. 4, Fourth quarter 2013.

[10] Irchelp.org, ”An IRC tutorial,” [Verkossa]. Saatavissa: http://www.irchelp.org/irchelp/irctutorial.html#part1. [Haettu 21.10.2014].

[11] J. Kangaspunta, ”Sähköisen maksamisen sääntelyyn liittyvät erityiskysymykset ja vastuunjako,” Pro-Gradu, 2011. Aalto-yliopisto, Laskentatoimen laitos. 95s.

[12] European Telecommunications Standards Institute, ”Lawful interception architecture and functions,” 2011.

[13] THE COUNCIL OF THE EUROPEAN UNION, ”Council Resolution of 17

January 1995 on the lawful interception of telecommunications," 11 4 1996.

[14] Generation Partnership Project (3GPP), "3GPP TS 33.107 V10.4.0 (2011-06)," 2011.

[15] J. M. Seppo Tiilikainen, "Aalto.fi (Suomen automaatioverkkojen haavoittuvuus)," 21.3.2013. [Verkossa]. Saatavissa: https://research.comnet.aalto.fi/public/Aalto-Shodan-Raportti-julkinen.pdf. [Haettu 14.10.2014].

[16] Shodan, "Shodan," Shodan, 2014. [Verkossa]. Saatavissa: www.shodanhq.com. [Haettu 19.10.2014].

[17] Symantec, "Internet-tietoturvan sanasto," Symantec, 2014. [Verkossa]. Saatavissa: http://fi.norton.com/security-glossary/article. [Haettu 19.10.2014].

[18] P. Paganini, "Security Affairs," Security Affairs, 2014. [Verkossa]. Saatavissa: http://securityaffairs.co/wordpress/27224/cyber-crime/kaspersky-report-energetic-bear.html. [Haettu 19.10.2014].

[19] Tietoviikko, "USB tietoturvariskinä," *Tietoviikko,* Kesä-Heinäkuu, 2014.

[20] M. Särelä, "Turvallisuus&Riskienhallinta," s. 14-15, 4/2014.

[21] STUK, "Artikkeli: Stuxnet loi kyberturvallisuudelle uudet vaatimukset," Säteilyturvakeskus, 4.2.2013. [Verkossa]. Saatavissa: http://www.stuk.fi/ajankohtaista/artikkelit/fi_FI/artikkeli-stuxnet-loi-kyberturvallisuudelle-uudet-vaatimukset/. [Haettu 14.10.2014].

[22] IEC, T. Phinney, "Security for Industrial Process Measurement and Control – Network and System Security," 8.6.2007. [Verkossa]. Saatavissa: http://www.iec.ch/dyn/www/f?p=103:38:0::::FSP_LANG_ID,FSP_APEX_PAGE,FSP_ORG_ID,FSP_PROJECT:25,20,1250,IEC/PAS%2062443-3%20Ed.%201.0#. [Haettu 20.10.2014].

[23] J. M. a. P. Reiher, "A taxonomy of DDoS attack and DDoS," *ACM SIGCOMM Computer Communications,* osa/vuosik. 34, nro 2, s. 39-53, 2004.

[24] Byres, Eric J., Matthew Franz, and Darrin Miller. "The use of attack trees in assessing vulnerabilities in SCADA systems." *Proceedings of the International Infrastructure Survivability Workshop*. 2004.

[25] IEEE: Chee-Wooi Ten, et al, "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees," 2007. [Verkossa]. Saatavissa: http://powercyber.ece.iastate.edu/publications/gm-cs.pdf. [Haettu 14.10.2014].

[26] Rohan Chabukswar, et al, "Simulation of Network attacks on SCADA systems," 2011. [Verkossa]. Saatavissa: http://users.ece.cmu.edu/~rchabuks/scspaper.pdf. [Haettu 14.10.2014].

[27] Nan, Cen, and Irene Eusgeld. "Adopting HLA standard for interdependency study." *Reliability Engineering & System Safety* 96.1 (2011): 149-159.

[28] G. Hemingway et al, "Rapid Synthesis of HLA-Based Heterogenous Simulation:

A Model-Based Integration Approach," 10.1.2012. [Verkossa]. Saatavissa: http://129.59.129.55/sites/default/files/0037549711401950.full_.pdf. [Haettu 14.10.2014].

[29] D. Beresford, "Exploiting Siemens Simatic S7 PLCs," 8 7 2011. [Verkossa]. Saatavissa: http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/beresford.pdf. [Haettu 14.10.2014].

[30] Profibus, "PROFINET - the leading Industrial Ethernet Standard," 2014. [Verkossa]. Saatavissa: http://www.profibus.com/technology/profinet/overview/. [Haettu 19.10.2014].