Kauno technologijos universitetas

Elektros ir elektronikos fakultetas

Kibernetinių saugos priemonių pramonės įmonėse taikymo tyrimas

Baigiamasis magistro projektas

Andrius Petkus

Projekto autorius

Doc. Gintaras Dervinis

Vadovas

Kaunas, 2020

Kauno technologijos universitetas

Elektros ir elektronikos fakultetas

Kibernetinių saugos priemonių pramonės įmonėse taikymo tyrimas

Baigiamasis magistro projektas

Valdymo technologijos (6211EX014)

Andrius Petkus

Projekto autorius

Doc. Gintaras Dervinis

Vadovas

Doc. Kastytis Ratkevičius

Recenzentas

Kaunas, 2020

Kauno technologijos universitetas

Elektros ir elektronikos fakultetas

Andrius Petkus

Kibernetinių saugos priemonių pramonės įmonėse taikymo tyrimas

Akademinio sąžiningumo deklaracija

Patvirtinu, kad mano, Andriaus Petkaus, baigiamasis projektas tema „Kibernetinių saugos priemonių pramonės įmonėse taikymo tyrimas“ yra parašytas visiškai savarankiškai ir visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

_____	_____
(vardą ir pavardę įrašyti ranka)	(parašas)

Petkus Andrius. Kibernetinių saugos priemonių pramonės įmonėse taikymo tyrimas. Magistro baigiamasis projektas / vadovas doc. Gintaras Dervinis; Kauno technologijos universitetas, Elektros ir elektronikos fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): elektronikos inžinerija, krypčių grupė – inžinerijos mokslai.

Reikšminiai žodžiai: kibernetinis saugumas, pramonė, IEC-62443, Kali Linux, mGuard.

Kaunas, 2020. 45 p.

Santrauka

Baigiamojo magistrinio projekto tikslas – išanalizuoti, kokios kibernetinės grėsmės kyla pramonės įmonėms, kokios yra kibernetinės atakos ir kaip jos kinta, ištirti skirtingų gamintojų tinklo saugos įrangos efektyvumą, taikant skirtingas kibernetines atakas. Darbe analizuojama, kaip prasidėjus Pramonės 4.0 etapui kinta kibernetinio saugumo samprata. Taip pat analizuojama, kaip kito kibernetinių atakų tendencijos per paskutinius tris dešimtmečius ir kokių priemonių reikia imtis pramonės įmonėms, kad padidintų tinklų saugą. Analizuojamas IEC-62443 kibernetinio saugumo standartas, jo esmė ir kaip reikia tinkamai jo laikytis. Šiame darbe aprašyta, kokių paprasčiausių priemonių reikia imtis norint padidinti savo tinklo saugumą. Naudojant „Kali Linux“ operacinę sistemą tiriamas tinklo komunikacijos greitis, duomenų perdavimo ir nuskaitymo laikas, kai naudojama skirtingų gamintojų tinklų įranga ir tinkle yra imituojamos apkrovos naudojant skirtingas kibernetines atakas. Gauti rezultatai parodo skirtumus tarp skirtingų gamintojų įrangos, bei tai, kuri įranga geriausiai apsaugo nuo imituojamų kibernetinių atakų.

Petkus Andrius. Investigation of Application of Cyber Security Instrumentality in Industry. Master's Final Degree Project / supervisor doc. Gintaras Dervinis; Faculty of Electrical and Electronics Engineering, Kaunas University of Technology.

Study field and area (study field group): Electronical engineering, study field group – engineering science.

Keywords: cyber security, industry, IEC-62443, Kali Linux, mguard.

Kaunas, 2020. 45.

Summary

The main goal of this final project of master degree is analyze the cyber threats posed to industrial enterprises, what are cyber attacks and how they changed, to investigate the effectiveness of network security equipment from different manufactures using different cyber attacks. The paper analyzes how the concept of cyber security changes with the beginning of the Industrial 4.0 stage. It also analyzes how trends in cyber attacks over the last three decades have changed. What measures need to be taken by industry to increase network security. The IEC-62443 cyber security standart is analyzed, what is its essence and how to follow it correctly. This paper describes the simplest steps you need to take to increase the security of your network. By using „Kali Linux“ operating system I will investigate network communication speed, date transfer, scan time when using network equipment from different manufactures and simulating different loads on a network using different cyber attacks. The obtained results show the differences between used equipment and which equipment best protects against simulated cyber attacks.

Turinys

Lentelių sąrašas

Paveikslų sąrašas

Santrumpų ir terminų sąrašas

WSN (angl. *Wireless Sensor Network*) – bevielis jutiklių tinklas.

M2M (angl. *Machine to Machine*) – dviejų įrenginių tiesioginė komunikacija.

RFID (angl. *Radio Frequency identification*) – radijo dažnio atpažinimas.

IoT (angl. *Internet of Things*) – daiktų internetas.

IT (angl. *Information Technology*) – informacinės technologijos.

OT (angl. *Operational Technology*) – operacinės technologijos.

DDoS (angl. *Distributed Denial of Service*) – paskirstyta paslaugų trikdymo ataka.

IP (angl. *Internet Protocol*) – interneto protokolas.

TCP (angl. *Transmission Control Protocol*) – perdavimo valdymo protokolas.

ICMP (angl. *Internet Control Message Protocol*) – interneto kontrolės žinučių protokolas.

ICS (angl. *Industrial Control Systems*) – pramoninės valdymo sistemos.

SQL (angl. *Structured Quarry Language*) – struktūrizuota užklausų kalba.

MITM (angl. *Man in the Middle*) – kibernetinė ataka.

SCADA (angl. *Supervisory Control And Data Acquisition*) – priežiūros kontrolė ir duomenų rinkimas.

PLC (angl. *Programmable Logic Controller*) – programuojamas loginis valdiklis.

C&C (angl. *Command & Control*).

NAC (angl. *Network Access Control*) – tinklo prieigos valdymas.

IEC (angl. *International Electrotechnical Commission*) – tarptautinė elektrotechnikos komisija.

IACS (angl. *Industrial Automation Control systems*) – pramoninės automatinio valdymo sistemos.

WAN (angl. *Wide Area Network*) – globalusis įrenginių tinklas.

LAN (angl *Local Area Network*) – vietinis įrenginių tinklas.

DMZ (angl. *Demilitarized Zone*) – demilitarizuota zona.

LTE (angl. *Long-Term Evolution*) – 4 kartos bevielės komunikacijos standartas.

VLAN (angl. *Virtual Local Area Network*) – virtualus vietinis įrenginių tinklas.

MAC (angl. *Media Acess Control Address*) – MAC adresas.

VPN (angl. *Virtual Private Network*) – virtualus privatus tinklas.

SYN (angl. *Synchrony*) – sinchronizuotas.

ACK (angl. *Acknowledgment*) – patvirtinimas.

Įvadas

Dėl sparčios technologijos plėtros vis daugiau pramonės įmonių modernizuoja savo procesus. Ekspertai spėja, kad per ateinančius kelis metus prie interneto prijungtų įrenginių skaičius gali išaugti keletą kartų. Informacinių ir veiklos technologijų integravimas kelia naujus iššūkius, ypač kibernetinio saugumo srityje. Plečiantis pramonės automatizavimui, atsirandant naujoms duomenų apdorojimo ir valdymo galimybėms atsiranda poreikis stebėti visus sistemos procesus centralizuotai, iš vienos vietos. Tam turi būti panaudotas interneto ryšys. Šiais laikais, prijungiant sistemas prie vietinio tinklo reikia būti pasiruošus viskam, nes tobulėjant technologijoms, didėja ir kibernetinių atakų grėsmė. Dėl šios priežasties labai svarbu būti tinkamai pasiruošus tam, kad būtų užkirstos ar apribotos kibernetinių grėsmių galimybės. Šiame darbe bus nagrinėjamos kibernetinio saugumo problemos pramonės srityse ir kokių priemonių reikia imtis, kad būtų išvengta problemų, kurios gali kilti dėl kibernetinio saugumo stokos.

Darbo tikslas – ištirti, kaip palaikomos komunikacijos tarp bendraujančių įrenginių, naudojant skirtingų gamintojų kibernetinės apsaugos priemones, esant skirtingoms imituojamoms kibernetinėms atakoms.

Darbo uždaviniai:

1. apžvelgti, kas tai yra „Pramonė 4.0“ ir kokias kibernetines problemas sukelia pramonės plėtra;
2. išanalizuoti dažniausiai pasitaikančias kibernetines atakas;
3. išanalizuoti IEC-62443 standartą ir jo panaudojimo galimybes;
4. ištirti komunikacijos greitį tarp įrenginių, naudojant tinklo saugos įrangą, esant skirtingoms apkrovos sąlygoms;
5. ištirti duomenų nuskaitymo greitį, naudojant tinklo saugos įrangą, esant skirtingoms apkrovos sąlygoms;
6. palyginti skirtinga įranga gautus tyrimo rezultatus.

1. „Pramonė 4.0”

Pramonės revoliucijos pokyčiai yra svarbiausi etapai, kurie keitė žmonijos istorijos eigą. Pasak daugelio mokslininkų, pramonės revoliucija labiau paveikia žmonių gyvenimo būdą, nei įvairios mokslo revoliucijos.

Pramonės revoliucija prasidėjo atradus garo galią. Nuo to laiko pramonė tobulėja ir keičiasi lygiagrečiai su visuomenės poreikiais. Kitos pramonės revoliucijos metu, dvidešimto amžiaus pradžioje, atsirado elektros energija varoma masinė gamyba. Vėliau, aštuntajame dvidešimto amžiaus dešimtmetyje, buvo pradėtos taikyti labai efektyvios elektroninės industrinės automatikos sistemos.

Nuo 2012 metų buvo pripažintas ketvirtasis pramonės sistemų etapas, kuris vadinamas *„Industry 4.0“*. Jam būdingos duomenų valdomos gamybos sistemos, konkrečiau – kibernetinės / fizinės sistemos arba sistemos, kurios susijusios su internetu [1].

Dabartiniu laikotarpiu pasaulis yra ketvirtosios pramoninės revoliucijos pradžioje, kuri yra grindžiama interneto pagrindu. *„IoT“* (angl. *Internet of things*) remiasi įvairiomis technologijomis, tokiomis kaip bevieliai jutiklių tinklai *(WSN)*, mašinų mašinoms *(M2M)* sistemomis, dideliu duomenų kiekiu, debesų paslaugomis ir išmaniosiomis programomis bei radijo dažnių atpažinimo sistemomis *(RFID)*.

Naujas pramonės šakų pokytis, taip pat žinomas kaip *„Industry 4.0“*, sulaukia daug dėmesio iš gamybos įmonių. Tai labai svarbu gamybos įmonėms iš viso pasaulio, nes ši revoliucija didina pramonės efektyvumą, našumą ir pritaikymą.

„Pramonė 4.0“ sprendžia tokias problemas kaip darbą su didelės apimties duomenimis, tobulina žmogus – mašina interaktyvias sistemas bei tobulina komunikaciją tarp skaitmeninio bei fizinio lygio sistemų [2].

„Pramonėje 4.0“ yra trys esminiai etapai: pirmas – gauti skaitmeninius įrašus iš jutiklių, kurie yra prijungti prie įrenginių, renkančių duomenis ir glaudžiai imituojančių žmonių jausmus ir mintis. Ši technologija yra žinoma kaip jutiklio sintezė. Antras – analizavimo ir vizualizavimo žingsnis – apima analizuotų gebėjimų įgyvendinimą iš jutiklių užfiksuotų duomenų. Nuo signalo apdorojimo iki optimizavimo, vizualizavimo, pažinimo ir didelio našumo skaičiavimų, gali būti atliekama daug skirtingų operacijų, kartu su kitomis foninėmis operacijomis. Besivystanti debesų technologija padeda aptarnauti ir suvaldyti didžiulį duomenų kiekį. Trečias etapas – tai įžvalgų ir skaičiavimų pavertimas veiksmais, norint panaudoti sukauptus duomenis tam, kad būtų pasiekti reikšmingi rezultatai. Pramonės debesyje neapdoroti duomenys apdorojami naudojant duomenų analizės taikomąsias programas ir yra panaudojami žinių bazių sudarymui.

Su *„Industry 4.0“* pradžia, prasidėjo ir bendrų sujungtų sistemų era. Sistemų sujungimas suteikia ryšį tarp partnerių, klientų, darbuotojų ir sistemų, siekiant pagreitinti verslo efektyvumą ir kurti naujas galimybes bendradarbiaujant bendroje platformoje. Bendro tinklo privalumas yra tas, kad galima greitai pasiekti tarpusavio priklausomybę ir realiu laiku dalinti duomenimis tarp pramonės šakų iš skirtingų geografinių vietovių. Pramoninis debesis suteikia bendrą platformą duomenims saugoti ir bendradarbiauti su vartotojais iš įvairių pasaulio vietų.

Didesnis duomenų kiekis *„Industry 4.0“* eroje ir informacinių technologijų bei veiklos technologijų sintezė suteikia naujų iššūkių, ypač kibernetinio saugumo srityje [3]. Kibernetinis saugumas yra pagrindinis klausimas, kurį visų valstybių vyriausybės pripažįsta kaip aukščiausio lygio svarbos. Tai verslo ir įmonių vertingos informacijos apie klientų sandorius apsauga skaitmeniniame pavidale prieš piktnaudžiavimą, neleistiną prieigą ir vagystes. Dėl pastovios tinklo plėtros, kibernetinių atakų skaičius yra ženkliai padidėjęs. Kibernetinių atakų rengėjai, perėmę svarbią informaciją, piktnaudžiauja duomenimis įvairiais tikslais, pavyzdžiui, dėl finansinės naudos.

Naujų technologijų bumas, didėjanti visuomenės priklausomybė nuo pasauliniu mastu sujungtų technologijų, automatizavimas ir padidėjusi prekyba kibernetinių atakų įrankiais, sudėtingos įsilaužėlių atakos ir labai mažos saugos priemonės prieš kibernetines atakas, lemia ženkliai išaugusį kibernetinių atakų skaičių [4]. Su didėjančiu potencialių užpuolikų skaičiumi ir didėjančiu interneto tinklo dydžiu, priemonės, kurias potencialūs užpuolikai gali naudoti, tampa vis sudėtingesnės, efektyvesnės ir žalingesnės visuomenei. Dėl šios priežasties komunikaciniai tinklai turi būti apsaugoti nuo vidinių ir išorinių grėsmių ir pažeidžiamumų, norint pasiekti didžiausią *„IoT“* potencialą [5].

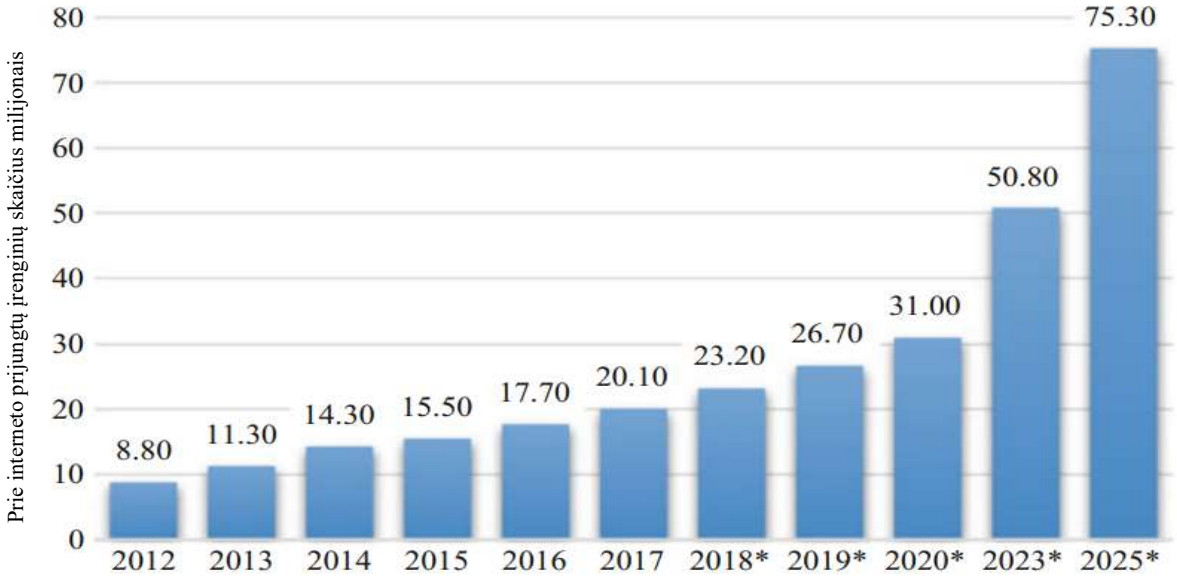
Platus įvairių internetinių prietaisų ir paslaugų naudojimas leido vystyti naujas kibernetinės gynybos formas siekiant užtikrinti patikimą saugumą [5]. Per pastaruosius dešimtmečius, kibernetinių atakų ir grėsmių rizika labai padidėjo. Bet kuri suinteresuotoji šalis, įmonė ar paprastas vartotojas, kuris tiesiogiai ar netiesiogiai naudojasi interneto tiekiamomis paslaugomis, gali bet kuriuo metu susidurti su kibernetinio saugumo rizikomis. Dažniausiai didelės įmonės kenčia nuo kenksmingų išpuolių, dėl kurių atsiranda rimta finansinė našta, ir nepageidaujamų nuostolių, tokių kaip duomenų sugadinimas, sistemos gedimai, privatumo pažeidimas, prestižo kritimas, klientų, patikimumo ir rinkos nuostoliai.

Daugelyje organizacijų kibernetinis saugumas pirmiausia laikomas technologiniu klausimu. Viešųjų ir privačių įmonių vadovai / institucijos žino apie pavojų, ir nenori leisti užpuolikams pasiekti svarbios verslo informacijos ir asmeninių duomenų apie darbuotojus ir klientus. Paprastai organizacijos, kurios patiria kibernetines atakas, to oficialiai dažniausiai nepraneša. Įmonės nėra linkusios atskleisti saugumo spragų, kurias jos turi ir mokėti išpirkų už kibernetinius nusikaltimus. Dauguma didžiųjų įmonių per pastaruosius metus gerokai sustiprino savo kibernetinio saugumo pajėgumą. Buvo išleista milijonai dolerių kuriant naujas strategijas su technologijomis, informacinių technologijų saugumo srityje, siekiant sumažinti kibernetinių atakų riziką.

Interneto pagrindu sukurtos sistemos taps dar patrauklesnės kibernetinėms atakoms, jei per ateinančius metus internete naudojamų prietaisų kiekis ir toliau didės [6]. Keletas bendrovių ir organizacijų prognozavo, kiek bus naujų prietaisų prijungtų prie interneto ateinančiais metais [4] . Pagal „Gartner“ prognozes, iki 2020 metų į bendrą interneto tinklą bus prijungta 20,8 milijardo įrenginių, „Cisco“ teigia, kad iki to paties laiko prisijungs apie 50 milijardų, o „Huawei“ projekcija rodo, kad iki 2025 m. internetinių jungčių skaičius turėtų siekti 100 mlrd. Nepaisant įvertinimų skirtumų, svarbiausias rezultatas – tikėtinas prijungtų įrenginių skaičiaus spartus augimas. Akivaizdžiausia išvada yra ta, kad bus didžiulis interneto įrenginių skaičius, kuriems bus reikalinga visapusiška apsaugos sistema, kuri užkirstų kelią galimoms kibernetinėms atakoms [4]. 1 pav. parodytas prijungtų įrenginių skaičius nuo 2012 iki 2025 m. Jame akivaizdžiai matomas prie interneto prijungtų įrenginių skaičiaus nuolatinis nuoseklus didėjimas.

Per paskutinius metus kibernetinių išpuolių skaičiaus nuolat auga, o nukentėjusieji būna ir fiziniai asmenys, ir vyriausybinio lygio organizacijos visame pasaulyje. 2014 metai buvo paskelbti

„Kibernetinių pažeidimų metais“. Po to sekė 2015 metai, kurie pramonės industrijos specialistų buvo pavadinti „Kibernetinių pažeidimų metai 2.0“ [6]. Kaip matoma iš bendros perspektyvos, akivaizdu, kad kibernetinės atakos padarė didelę žalą visame pasaulyje. Siekiant užkirsti kelią kibernetinėms atakoms, organizacijos turėtų ugdyti vartotojus, šviesti juos apie saugumą užtikrinančias procedūras, kurių reikia laikytis naudojant *„IoT“* sistemas.



1 pav. Prie interneto prijungtų įrenginių skaičius nuo 2012 iki 2025 [6]

1.1. *„IoT“* saugumo grėsmės ir pažeidžiamumas

Nėra bendro universalaus sutarimo dėl interneto architektūros. Skirtingi mokslininkai yra pasiūlę skirtingas architektūras. Apskritai *„IoT“* galima suskirstyti į keturis pagrindinius sluoksnius [7]:

- suvokimo (jutimo) sluoksnis: jį sudaro fiziniai objektai ir jutikliai, pavyzdžiui, įvairių formų jutimo technologijos, *RFID* jutikliai. Šios technologijos leidžia įrenginiams suvokti kitus objektus;
- tinklo sluoksnis: jis yra belaidžio ar laidinio ryšio palaikymo infrastruktūra tarp jutiklių ir informacijos apdorojimo sistemų;
- paslaugų sluoksnis: šis sluoksnis skirtas užtikrinti ir valdyti vartotojams ar programoms reikiamas paslaugas. Jis yra atsakingas už paslaugų valdymą ir turi nuorodas į duomenų bazes;
- taikymo (sąsajos) sluoksnis: jis sudarytas iš sąsajos metodų su naudotojais ar programomis. Šis sluoksnis yra atsakingas už informacijos pristatymą vartotojui.

Naujų prijungtų prietaisų skaičiaus augimas *„IoT“* pastaruoju metu sukūrė didelį poreikį naujoms saugos priemonėms nuo kibernetinių atakų milijonams vartotojų visame pasaulyje. Galimų grėsmių skaičius ir jų sudėtingumas kiekvieną dieną vis labiau didėja, o potencialūs kibernetinių atakų organizatoriai tampa gudresniais ir sunkiau sučiumpamais. Todėl, siekiant, kad *„IoT“* galėtų pasiekti visą savo potencialą, jis turi būti griežtai apsaugotas nuo grėsmių ir pažeidžiamumų [5]. Saugumo grėsmės kiekviename sluoksnyje skiriasi dėl savo savybių. Toliau pateikiami pavojai ir pažeidžiamumai pagal kiekvieną interneto sluoksnį.

Suvokimo sluoksnis. Suvokimo sluoksnyje automatiškai nustatomi pažangieji jutikliai ir *RFID* žymenys, kurie automatiškai atpažįsta aplinką ir keičiasi duomenimis tarp prietaisų. Saugumo problemos yra svarbus klausimas šiame sluoksnyje, nes jame daugelis grėsmių ateina iš išorinių subjektų, daugiausia iš jutiklių ir kitų duomenų rinkimo įrenginių. Dauguma šių įrenginių paprastai yra maži, nebrangūs ir fiziškai neapsaugoti [7]. Bendros grėsmės ir pažeidžiamumai suvokimo sluoksnyje bendruoju atveju gali būti apibrėžti taip:

- neleistina prieiga – pirmajame mazge neleistinos prieigos yra svarbios grėsmės dėl fizinių užpuolimų ar loginių atakų;
- konfidencialumas – užpuolikai gali užkrėsti kenkėjiškus jutiklius ar įrenginius gauti informaciją iš sistemos;
- prieinamumas – sistemos komponentas nustoja veikti, nes jis yra fiziškai užfiksuotas ar logiškai užpultas;
- triukšmingi duomenys (perdavimo pavojai) – jie gali būti neišsami arba neteisinga informacija dėl perdavimo per tinklus, apimančius didelius atstumus;
- kenkėjiškų kodų priepuoliai – užpuolikai gali sukelti programinės įrangos gedimą kenkėjišku būdu – kodu, pavyzdžiui, virusu „Trojos arklys“ ar nepageidaujamais pranešimais.

Tinklo sluoksnis. Tinklo sluoksnis sujungia visus daiktus, susijusius su internetu, ir leidžia jiems žinoti apie juos supančią aplinką. Jis yra gana jautrus atakoms dėl didelio duomenų kiekio, kurį jis turi apdoroti. *„IoT“* jungia įvairių tipų tinklus, kurie gali sukelti tinklo saugumo sunkumų. Todėl saugumo apsaugos lygis yra labai svarbus *„IoT“*. Tinklo sluoksnyje bendros saugumo grėsmės ir pažeidžiamumai yra tokie [8]:

- *„Denial of Services“ („DoS“)* ataka – ji nuolat atakuoja tikslinį tinklą su gedimų pranešimais, padirbtais prašymais ir / ar kitomis komandomis. *„DoS“* išpuoliai yra dažniausia grėsmė tinklui;
- maršruto atakos – tai yra atakos maršruto keliu, pavyzdžiui, maršruto keitimas, kuriant maršruto kilpas arba siunčiant klaidų pranešimus;
- perdavimo grėsmės – tai grėsmės, pavyzdžiui, blokavimas, manipuliavimas duomenimis, nutraukimas;
- duomenų pažeidimas – tai tyčinis arba netyčinis apsaugotos arba konfidencialios informacijos atidavimas nepatikimai aplinkai.

Paslaugų sluoksnis. *„IoT“* paslaugų sluoksnis priklauso nuo tarpinės programinės įrangos technologijos, leidžiančios komunikuoti ir valdyti duomenis taikomosiose programose ir paslaugose. Jis palaiko ir apima paslaugas naudodamas programų programavimo sąsajas. Šiame sluoksnyje duomenų saugumas yra labai svarbus ir sudėtingesnis nei kituose. Toliau išvardintos kelios bendros saugumo grėsmės ir pažeidžiamumai paslaugų lygmenyje [8]:

- manipuliacija – paslaugose esančia informacija manipuliuoja užpuolikas;
- apgavimas – į vartotojo užklausą atsako apsimetęs užpuolikas;
- neteisėta prieiga – piktnaudžiavimas paslaugomis, kurias naudoja nepatvirtinti vartotojai;
- kenkėjiška informacija – privačios ir slaptos informacijos praradimas;
- *„DoS“* atakos – naudingas paslaugų šaltinis tampa nebeprieinamu, kai jį veikia duomenų srautas, viršijantis įrenginio pajėgumus.

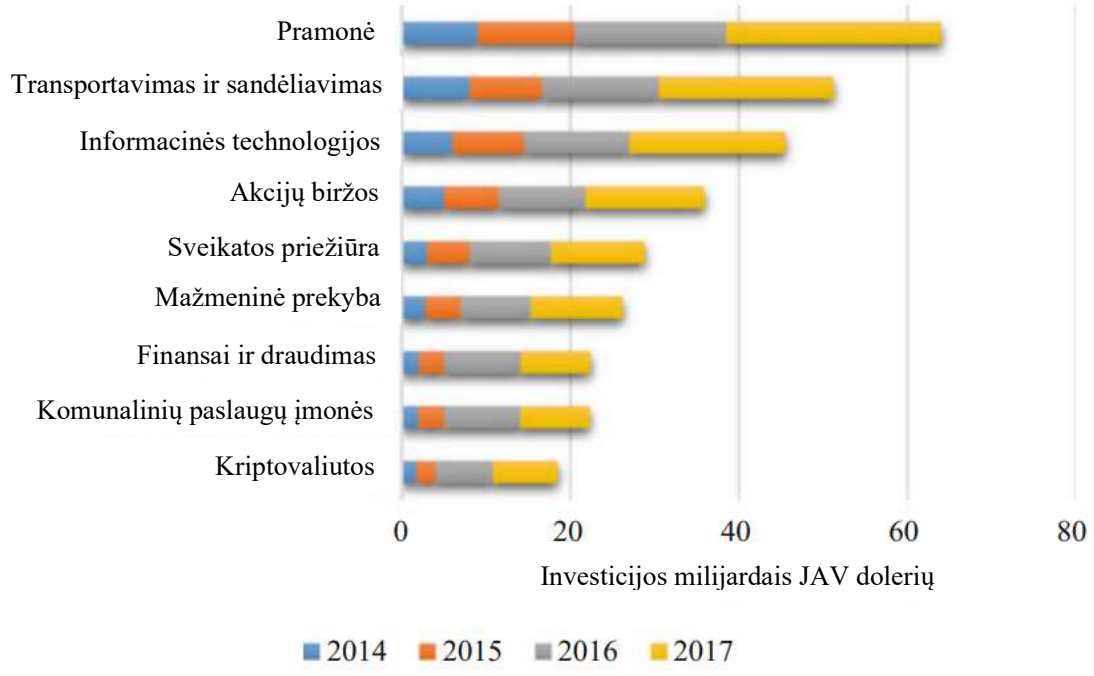
Viršutinis (taikymo) sluoksnis. Tai programos sluoksnis, matomas galutiniam vartotojui. Taikymo sluoksnis apima įvairias sąsajas ir programas, nuo paprastų iki pažangesnių. Taikymo sluoksnio saugumo reikalavimai labai priklauso nuo programų. Šio sluoksnio saugumo grėsmės ir pažeidžiamumai apibendrinami tokiais pavyzdžiais:

- konfigūracijos grėsmės – nesuderinamos sąsajos ir (arba) neteisingas, netinkamas konfigūravimas nuotoliniuose mazguose yra svarbiausi šio sluoksnio pavojai;
- kenkėjiškų programų atakos – šie išpuoliai yra apgalvotai padaromi tiesiogiai į programinės įrangos sistemą įdiegiant specialų virusą, kad būtų galima sąmoningai pakenkti numatomai sistemos funkcijai;
- sukčiavimo išpuoliai – užpuolikai gali bandyti gauti jautrios informacijos, pavyzdžiui, naudotojų vardus, slaptažodžius ir kredito kortelės duomenis.

Pagrindiniai saugumo reikalavimai visuose sluoksniuose yra konfidencialumas, vientisumas, prieinamumas, autentifikavimas ir privatumas.

1.2. Pramonės iššūkiai

Dėl pastaruoju metu vykstančio internetinių sistemų tobulėjimo, pramonei būtų labai nenaudinga neatsižvelgti į vykdomas permainas šioje srityje. Naujos technologijos diegimas, paslaugos ir išaugę pramonės poreikiai yra susiję su interneto technologijos panaudojimo plėtra [9]. Dabartinės taikymo sritys apima išmaniąją gamybą, išmanių namų (angl. *Smart House*) ir išmanių miestų, transporto ir sandėliavimo, sveikatos priežiūros, mažmeninės prekybos, logistikos įmonių ir aplinkos stebėseną, sumanų finansavimą ir draudimus [10]. Todėl gamybos sektorius 2017 metais į internetines inovacijas investavo daugiau kaip 60 milijardų JAV dolerių (2 pav.). Daugiausia, po gamybos įmonių, į internetinių sistemų plėtrą investuojama transporto ir sandėliavimo bei informacinių sistemų sektoriuose.



2 pav. Pramonės šakų investicijos 2014 – 2017 metais į internetines inovacijas

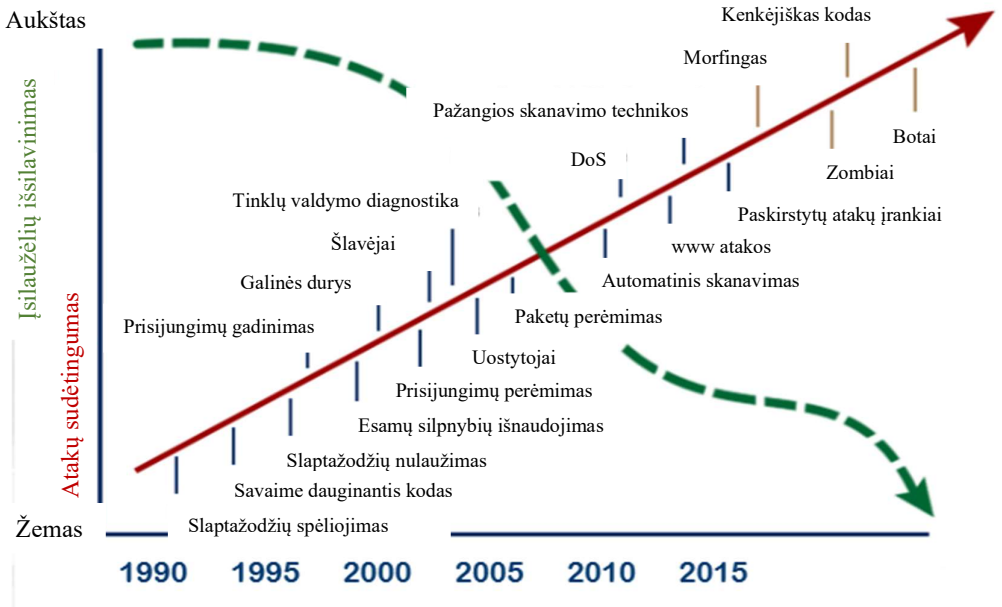
Su šiomis naujomis investicijomis į internetines sistemas ir *„Industry 4.0“* atsiranda labai daug saugumo problemų. Kai kurios iš problemų yra labai akivaizdžios, pavyzdžiui, piktnaudžiavimas asmenine informacija ir finansinės naudos siekis. Kitos iškylančios problemos yra konkretesnės ir priklauso nuo pramonės struktūros. Didžiausią kibernetinio saugumo susirūpinimą kelią finansinių paslaugų sektorius, kuriame pagrindinės problemos yra privatumas ir duomenų apsauga, valdant trečiųjų šalių rizikas.

Per paskutinius metus kibernetinių atakų skaičius prieš pramoninės gamybos sektorių ženkliai padidėjo. Neseniai paskelbtos ataskaitos rodo, kad pagrindiniai kibernetinių atakų taikiniai yra energetikos įmonės. Mažiausiai 75 proc. naftos, dujų ir energetikos sektoriaus įmonių 2016 m. patyrė vieną ar daugiau sėkmingų atakų. Daugiau kaip 15 proc. kibernetinių išpuolių yra tiesioginiai išpuoliai prieš energetikos sektorių [2]. Didžiausią susirūpinimą keliantys iššūkiai energetikos pramonėje yra privatumo apsauga, duomenų saugumas, įgūdžių ir sąmoningumo trūkumas, vis didesnis naudojamų komponentų energetikos sistemose skaičius, prijungiamas prie komunikacinių ryšių ir didėjanti tarpusavio priklausomybė tarp rinkos dalyvių.

1.3. Kibernetinių atakų raida

Viskas, kas susiję su kibernetinėmis atakomis, nuolat keičiasi ir keičiasi dėl sparčių technologijų pokyčių, užpuolikų sumanumo, potencialių tikslų ir vertės, kuriuos gali iššaukti jų išpuoliai. Plačiai naudojant kompiuterinius tinklus, įsilaužėliai gali pasinaudoti tinklo paslaugomis, siekiant gauti asmeninę ir kitą vertingą informaciją. Norint užkirsti grėsmėms kelią, saugumo produktai turi būti nuolat tobulinami arba atnaujinami. Pagrindinis iššūkis yra rasti sprendimą, kuris suteikia ilgaamžišką kibernetinę apsaugą, siekiant užtikrinti ilgalaikį tinklo saugumą.

Kiekviena organizacija dirba ir kaupia informaciją skaitmeniniu būdu. Šiais laikais daugelis įmonių palaiko verslą, įvairius susitarimus ir sandorius per internetines sistemas. Dauguma įmonių yra atviros kibernetinei veiklai, todėl jos yra atviros ir kibernetinėms grėsmėms, kurios kyla iš išorinių ir vidinių ribų. Todėl labai svarbu, kad kibernetinė infrastruktūra būtų apsaugota.



3 pav. Kibernetinių atakų raida [11]

Kibernetinis saugumas iš pradžių buvo vertinamas kaip *IT* sektoriaus problema, tačiau šiandien ji yra susijusi su visais įmonės darbuotojais. Kibernetinių atakų grėsmė gali kilti dėl naujos technologijos panaudojimo, sistemų mobilumo, socialinių žinių ar dėl sparčiai plintančių naujų tendencijų. Tad esant šioms aplinkybėms, protingas, dinamiškas ir evoliucinis požiūris į kibernetinį saugumą yra gyvybiškai svarbus siekiant užkirsti kelią kibernetiniams nusikaltimams. Tam reikalingos kibernetinio saugumo puoselėjimo pastangos norint apsaugoti nuo platesnio masto kibernetinių grėsmių. Dėl naujų mobiliųjų technologijų, naujų informacijos plitimo tendencijų, taip pat dėl to, kad įsilaužėlių organizacijos yra gerai finansuojamos, o atakos gali prasidėti bet kuriuo metu, apsisaugoti nuo visų kibernetinių iššūkių tampa vis sunkiau. Kibernetinės rizikos gali turėti tiesioginį poveikį viskam – nuo vertybinių popierių biržos kainos iki sugadintos prekės ženklo reputacijos ar patirtų finansinių nuostolių.

3 paveiksle vaizduojama kibernetinių atakų raida. Aštuntojo dešimtmečio pradžioje, kibernetinės atakos prasidėjo nuo slaptažodžių nulaužimo ar metodų, kaip atspėti nežinomą slaptažodį. Šiandien vyksta nukreiptos kibernetinės atakos, siunčiami apgaulingi paketai, naudojamas pažangus nuskaitymas ir sistemų užkrovimas duomenimis taip, kad jos nebegalėtų teikti savo pirminių paslaugų. Ateityje tikimasi, kad kibernetinės atakos dar tobulės ir taps labiau komplikuotos. Strateginės kibernetinės atakos sieks pakenkti strateginiams taškams su botais ir kenkėjiškais kodais. Laikui bėgant kibernetinių atakų pobūdis taps žymiai sudėtingesnis ir labiau komplikuotas. Atsekti ir išaiškinti kibernetinius nusikaltimus darysis vis labiau sudėtinga. Todėl prasidedant naujam pramoniniam *„Industry 4.0“* etapui, labai svarbu atkreipti dėmesį į naudojamą įrangą ir visuomenės sąmoningumą, norint užtikrinti kibernetinį saugumą [4].

2. Kibernetinis saugumas

Prieš prasidedant interneto erai, tradicinės pramonės įmonės ir ypatingos svarbos infrastruktūros organizacijos neturėjo prieigos prie interneto. Įmonėse saugumą apibūdindavo fiziniai saugumą užtikrinantys objektai - vartai, tvoros, barjerai ir apsaugos priemonės. Visos kitos sistemos, tokios kaip kontrolės sistemos ir elektroninių įrenginių tinklai, buvo specializuotos ir neturėdavo galimybių būti sujungtos su kitais įrenginiais tame pačiame tinkle. Kadangi nebūdavo galimybės sistemų integruoti tinkle, tai jas apsaugodavo nuo išorinių grėsmių. Komunikacija buvo patentuota ir nebuvo sukurta *IP* (angl. *IP – Internet Protocol*) standartams, pavyzdžiui, *„Ethernet“* ir *TCP / IP* (angl. *TCP – Transmission Control Protocol*). Kadangi visos automatizuotos įmonės automatikos prietaisus laikydavo atskiruose padaliniuose, todėl nebuvo tinklų komunikacijos – nebuvo poreikio naudoti ugniasienės technologijos. Fizinės prieigos ribojimas prie įrenginių būdavo pagrindinė saugos priemonė, nes tik prieigos teisę turintis žmogus galėdavo patekti į įmonių automatikos valdymo korpusus.

Interneto ryšio atsiradimas pakeitė visą saugumo apibrėžimą. Internetinės komunikacijos atsiradimas įgalino išpuolius, kurie nereikalauja tiesioginės fizinės prieigos prie įrenginio. Šiais laikais organizacijos turi galvoti apie kibernetinį saugumą. Pramoninis kibernetinis saugumas yra skirtas tam, kad išlaikytų pramonines valdymo sistemas (angl. *ICS – Industrial Control Systems*) toliau nuo tyčinių ar atsitiktinių kibernetinių grėsmių, kurios sutrikdytų ar kenktų žmonėms, procesams, įrangai ar aplinkai.

Kibernetinės grėsmės pramoninėms sistemoms gali kilti tiek iš vidaus, tiek iš išorės. Šios grėsmės dažnai perduodamos elektroniniu būdu, pavyzdžiui, elektroniniu paštu, per pavogtus ar bendrai naudojamus prisijungimo duomenis, išorines laikmenas. Tokių atakų pasekmės gali būti tiek skaitmeninės, kai pasisavinama ar ištrinama svarbi skaitmeninė informacija, tiek fizinės, kai sugadinami įrenginiai ar atliekami kiti nepageidaujami fiziniai procesai.

Esminiai faktoriai, kurie sudaro kibernetinę saugą [12]:

- taikomųjų programų saugumas – žiniatinklio programų pažeidžiamumas yra bendras kibernetinių nusikaltėlių įsilaužimo aspektas. Kadangi programos vaidina vis svarbesnį vaidmenį versle, organizacijos skubiai turi sutelkti dėmesį į interneto programų saugumą, kad apsaugotų savo klientus, jų interesus ir turtą;
- tinklo saugumas – tai tinklo ir duomenų naudojimo ir vientisumo apsaugos procesas. Tai paprastai pasiekiama atliekant patekimo į tinklą testą, kuriuo siekiama įvertinti tinklo pažeidžiamumo ir saugumo aspektus serveriuose, kompiuteriuose, įrenginiuose ir tinklo paslaugose;
- veiklos saugumas – operacijų saugumas apsaugo organizacijos pagrindines funkcijas stebėdamas kritinę informaciją ir turtą, kuris su juo sąveikauja, kad nustatytų galimą pažeidžiamumą;
- galutinio vartotojo mokymas – žmogaus klaida išlieka pagrindine duomenų pažeidimų priežastimi. Kibernetinio saugumo strategija yra tokia stipri, kaip ir jos silpniausia grandis. Dėl tos priežasties organizacijos turi įsitikinti, kad kiekvienas darbuotojas žino, kaip pastebėti ir spręsti iškylančias grėsmes, su kuriomis jie gali susidurti, nesvarbu, ar jie patys taps sukčiavimo auka;

– lyderystės įsipareigojimai ir dalyvavimas – tai yra raktas į sėkmingą bet kokio kibernetinio saugumo projekto įgyvendinimą. Tačiau tokių įgyvendintų projektų veiksmingumą yra labai sunku nustatyti, kol nesusiduriama su problema. Aukščiausia vadovybė taip pat turi būti pasirengusi investuoti į tinkamus kibernetinio saugumo išteklius, nesvarbu, ar ji samdo kvalifikuotus žmones, ar kelia žmonių kvalifikaciją, ar tobulina turimą technologiją.

2.1. Dažniausios kibernetinės atakos

Dėl kibernetinių grėsmių nuolatinio tobulėjimo, kibernetinis saugumas gali būti labai sudėtingas. Dėl sėkmingų kibernetinių atakų pelningumo, kibernetiniai nusikaltėliai tampa vis išradingesni, todėl jų keliama grėsmė nuolat didėja. Žemiau yra pateikta keletas bendrų kibernetinių atakų ir grėsmių.

Sukčiavimas. Sukčiavimas yra vienas iš seniausių „įsilaužimo“ metodų, kuriuos naudoja elektroniniai nusikaltėliai. Šio būdo esminis faktorius yra įtikinti žmones atskleisti slaptą informaciją, kuri gali pakenkti jų saugumui. Be to, sėkmingi sukčiavimo išpuoliai suteikia didžiulę investicijų grąžą, kuri paskatino nusikaltėlius kurti vis sudėtingesnius ir kūrybiškesnius sukčiavimo metodus.

Socialinė inžinerija. Socialinė inžinerija naudojama apgauti ir manipuliuoti aukomis, kad būtų galima gauti informaciją arba gauti prieigą prie kompiuterio. Dažniausiai tai atliekama apsimetant techniniu asmeniu, kuris teikia paslaugas ar užsiima kompiuterinės įrangos tvarkymu. Tai pasiekiama privertus vartotojus paspausti kenkėjiškas nuorodas arba fiziškai įgyjant prieigą prie kompiuterio apgaulės būdu.

***„DDoS“* ataka.** *„DDoS“* ataka bando sutrikdyti įprastą interneto srautą, tam, kad norima svetainė įgautų neaktyvų statusą. Tai pasiekiama užtvindant sistemą, serverį ar tinklą su daugiau užklausų nei ji gali susitvarkyti.

Kenkėjiškos programos. (angl. *Malware*). Kenkėjiška programa yra platus terminas, naudojamas apibūdinti bet kokį failą ar programą, kuria siekiama pakenkti kompiuteriui. Ši kategorija apima „Trojos arklį“, kirminus, virusus ir įvairias šnipinėjimo programas.

Virusas. Virusas yra kenkėjiško kodo gabalas, kuris įkeliamas į kompiuterį be vartotojo žinios. Jis gali pasikartoti ir išplisti į kitus kompiuterius, prijungdamas jį prie kito kompiuterio failo.

Kirminai. Kirminai yra panašūs į virusus, nes jie yra savaime replikuojami, tačiau jiems nereikia prisijungti prie programos. Jie nuolat ieško pažeidžiamumų ir praneša apie trūkumus, kuriuos jie rado savo kūrėjui.

„Trojos arklys“. Tai – kenkėjiškų programų tipas, kuris užmaskuoja save kaip teisėtą programinę įrangą, pavyzdžiui, virusų šalinimo programą, bet atlieka kenksmingą veiklą.

***„Ransomware“*.** Viena iš sparčiausiai augančių kibernetinių atakų formų - *„Ransomware“* yra kenkėjiškų programų tipas, kuris užšifruoja nukentėjusiųjų asmenines bylas, todėl jų negalima pasiekti. Norint jas pasiekti, būtina sumokėti norimą išpirką. Tačiau išpirkos sumokėjimas negarantuoja užšifruotų duomenų atkūrimo.

***„Spyware / adware“*.** Šnipinėjimo programos gali būti įdiegtos jūsų kompiuteryje be jūsų žinios, kai atidaromi priedai, kenksmingos nuorodos arba atsisiunčiama kenksmingos programinės įrangos. Tada jis stebi jūsų kompiuterio veiklą ir renka asmeninę informaciją.

***SQL* injekcija.** Struktūrizuotos užklausos kalbos injekcija įvyksta, kai užpuolikas į serverį, kuris naudoja *SQL*, įdeda kenkėjišką kodą. *SQL* injekcijos sėkmingos tik tada, kai programos programinėje įrangoje yra pažeidžiamos. Sėkmingi *SQL* išpuoliai priverčia serverį suteikti prieigą prie duomenų ar juos keisti.

***MITM* ataka (**angl. *MITM – Man In The Middle*). *MITM* ataka įvyksta tada, kai įsilaužėlis įterpia save tarp kliento (įrenginio) ir serverio ryšio. *MITM* atakos dažnai pasitaiko, kai vartotojas prisijungia prie nesaugaus viešojo *Wi-Fi* tinklo. Užpuolikai gali įterpti save tarp lankytojo įrenginio ir tinklo. Tuomet vartotojas nežinomai perduos informaciją per užpuoliką.

Interneto programų ir tinklų pažeidžiamumas. Kibernetiniai nusikaltėliai nuolat aptinka naujus sistemų, tinklų ar programų pažeidžiamumus. Ši veikla vykdoma automatizuotais išpuoliais ir gali paveikti bet kur ir bet kada.

Nulinės dienos ataka (angl. *Zero-day attack).* Pasenusios programinės įrangos naudojimas atveria galimybes nusikaltėlių įsilaužėliams pasinaudoti pažeidžiamumu ir galimai išjungti visą sistemą. Nulinės dienos išnaudojimas gali įvykti, kai sistemos pažeidžiamumas paskelbiamas prieš tai, kai kūrėjas paskelbė pataisą ar sprendimą.

2.2. *„Stuxnet“*

„Stuxnet“ yra kompiuterinis virusas, atrastas 2010 metais. Šis virusas yra kirmino tipo (angl. *worm*) – tai atskira, savarankiškai besidauginanti programos infekcija, kuri plinta į kitus kompiuterius per tinklą. *„Stuxnet“* virusas buvo nutaikytas paveikti branduolinius įrenginius Irane. Šis įvykis išprovokavo didžiulį visų valstybių kibernetinės politikos ir strategijos pasikeitimą. Todėl galima teigti, kad *„Stuxnet“* viruso atradimas buvo lūžio taškas, nuo kurio pradėjo kisti visuomenės nuomonė apie kibernetinį saugumą. Taigi, kalbant apie kibernetinio saugumo poreikį, būtų galima išskirti du laikotarpius: *prieš* šio viruso atradimą ir *po* jo [13].

Viruso kūrimas

„Stuxnet“ yra konkretaus viruso pavadinimas, tai kenkėjiška programinė įranga, nukreipta į supervizorinio valdymo ir duomenų atvaizdavimo sistemas (angl. *SCADA – Supervisory Control And Data Acquisition*) pramoniniuose valdikliuose. Tiksliai žinoti, kaip buvo sukurta ši kenkėjiška programa, yra labai sunku (jei išvis įmanoma), tačiau galima teigti, kad tam reikėjo nemažų resursų, darbo jėgos, laiko ir finansų. Specialistų, kurie analizavo šį virusą, vertinimu, tam, kad būtų sukurtas šis virusas reikėjo nuo penkių iki dešimties programuotojų, kurie dirbtų ištisai ir ne mažiau kaip šešis mėnesius [13].

1 lentelėje lyginamas *„Stuxnet“* virusas su įprastais kirmino tipo virusais. *„Stuxnet“* yra daug didesnis už kitus šio tipo virusus. Jis buvo parašytas keliomis skirtingomis programavimo kalbomis, su tam tikrais užšifruotais komponentais. Šis virusas naudojo ne vieną, o keturis nulinės dienos pažeidžiamumus, kad galėtų užkrėsti kompiuterius:

- automatinį procesą iš prijungtų USB atmintinių;
- ryšį su bendrais spausdintuvais;
- dar du pažeidžiamumus, susijusius su privilegijų didinimu.

Toliau virusas galėdavo valdyti kompiuterines programas, net jeigu jos būdavo išjungtos. *„Stuxnet“* siekė užkrėsti kompiuterius, veikiančius su *„Microsoft Windows“* operacine sistema su papildomu užkratu. Tuomet virusas, atsisiuntęs savo pagrindinį rinkinį ir naudodamas papildomas programinės įrangos tvarkykles, galėjo ieškoti *„Siemens“ „Simatic WinCC / Step-7“* programinės įrangos, kuri skirta valdyti pramoninę įrangą. Užkrėsdamas failus, kuriuos naudoja ši programinė įranga, virusas galėjo pasiekti ir valdyti programuojamus loginius valdiklius *(PLC)*, kurie buvo naudojami pramoninių prietaisų galiai reguliuoti. Be to, virusas taip pat galėjo susisiekti su kitomis užkrėstomis mašinomis ir *C&C* (*angl. Command and Control*) serveriais Danijoje ir Malaizijoje, siekdamas atsinaujinti ir siųsti informaciją apie tai, ką rado [12].

Kai visi viruso reikalavimai atitikdavo pradines sąlygas, *„Stuxnet“* pradėdavo savo ataką pakeisdamas centrifugų rotorių greičius, kol jie būdavo nepataisomai sugadinami [14].

1 lentelė. *„Stuxnet“* ir tipinio tos pačios kategorijos viruso skirtumai

Ypatybė	***„Stuxnet“***	**Įprastas kirminas**
Taikinys	Tik *„Siemens Simatic/Step-7“* sistemos	Kompiuterinės sistemos
Dydis	500 kBs	Apie 100 kBs
Užkrato šaltinis	USB laikmenos arba bendri spausdintuvai	Internetu
Išnaudotas pažeidžiamumas užkrėtimui	4 skirtingos nulinių dienų atakos	1 nulinės dienos ataka
Tikslas	Urano sodrinimo centrifugos Irane	Dažniausiai tiesiog plisti arba instaliuoti ,,galinių durų prieigą"

„Stuxnet“ tikslas buvo apkrėsti kompiuterius ir sugadinti įrangą Irano branduolinėje jėgainėje ir urano sodrinimo gamykloje „Natanz“. Tyrėjai mano, jog tai, kad *„Stuxnet“* buvo užprogramuotas taikytis į įrenginius, kurie būtų suskirstyti į grupes iš 164 objektų ir tai, kad „Natanz“ kaskados buvo išdėstytos 164 centrifugose, nėra atsitiktinumas. Iranas naudojo IR-1 tipo centrifugas, kurios buvo gaminamos Europoje nuo septintojo dešimtmečio pabaigos iki aštuntojo dešimtmečio pradžios. Šiuo metu šios centrifugos yra labai neefektyvios ir nebenaudojamos [14]. Jos – labai trapios, dėl to staigus greičio pakeitimas gali jas sugadinti arba net visiškai sulaužyti. *„Stuxnet“* kūrėjai suprasdami šį trūkumą jį išnaudojo. „Natanz“ atominė elektrinė yra fiziškai atjungta nuo interneto (angl. *air gap*) ir turi savo nuosavą uždarą kompiuterių tinklą, o tai reiškia, kad joje nėra jokio ryšio su internetu ar kitais tinklais. Todėl labai tikėtina, kad *„Stuxnet“* užkrėtė tinklą per užkrėstą nešiojamą USB laikmeną. Taigi virusas į sistemą atkeliavo per darbuotojo iš namų atsineštą užkrėstą USB laikmeną.

Poveikis

Vertinant vidaus politiniu lygmeniu galima sakyti, kad kibernetinė ataka diskreditavo Irano vyriausybę. Irano valdžia negalėjo apsaugoti savo branduolinių objektų nuo užsienio kibernetinių atakų. Ji nepareiškė kaltinimų dėl kibernetinių išpuolių, nes nusikaltėlių tapatybės nebuvo žinomos arba buvo neaiškios. Dėl to, kad iki to laiko dar nebuvo tokio precedento, valstybė nežinojo, kaip

turėtų reaguoti į tokį išpuolį. Dėl šio neveiksnumo Irano vyriausybė atrodė silpna ir tapo lengvu taikiniu.

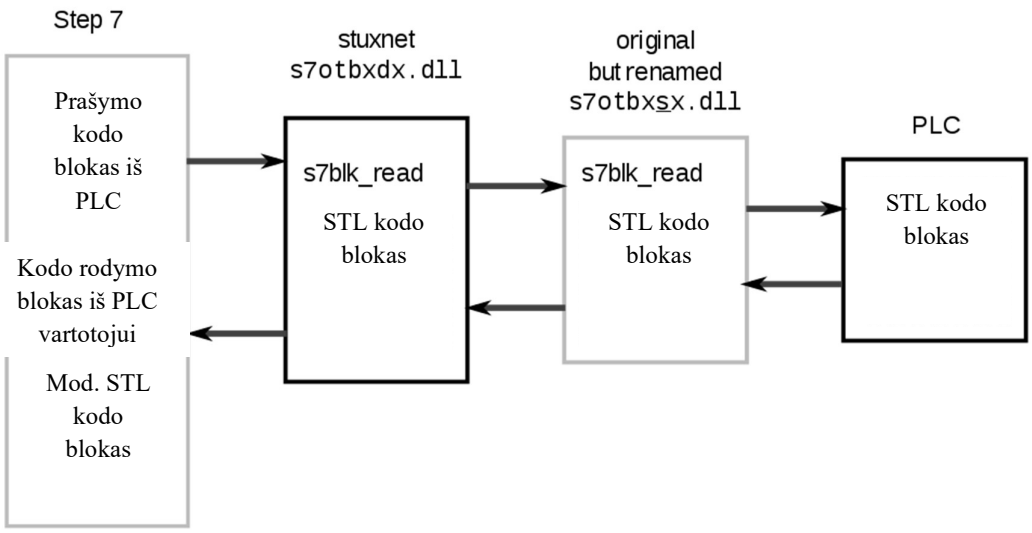
„Stuxnet“ beveik neturėjo tiesioginio poveikio Irano gyventojams. Virusas buvo sukurtas siekiant išvengti papildomos žalos. Jei kibernetinė ataka būtų padariusi papildomos žalos ar stipresnį poveikį, kuris galėtų lemti žmonių gyvybių praradimą, tai galėjo būti suprantama kaip jėgos panaudojimas ir dėl to galėjo išaugti smurto proveržiai tarp Irano ir šalių, kurios, jų manymu, buvo atsakingos už šio viruso paskleidimą.

2 lentelė. Užkrėstų asmeninių kompiuterių *„Stuxnet“* virusu pasiskirstymas [16]

Valstybė	**Užkrėstų kompiuterių skaičius**
Iranas	58,85 %
Indonezija	18,22 %
Indija	8,31 %
Azerbaidžanas	2,57 %
Jungtinės Amerikos Valstijos	1,56 %
Pakistanas	1,28 %
Kitos	9,2 %

Didžiausias *„Stuxnet“* poveikis visuomenei greičiausiai buvo nesaugumo jausmas. Dėl šios priežasties galima manyti, kad iraniečiai jautėsi išduoti dėl neefektyvių šalies kibernetinio saugumo priemonių ir silpnos jos pozicijos dėl šio kibernetinio incidento. Irano tinklų užkrėtimas įrodė, kad tinklai, kurie yra fiziškai neprijungti prie interneto ryšio yra saugesni negu kiti tinklai, tačiau vis tiek jų negalima laikyti pakankamai saugiais. Nors virusas buvo nutaikytas paveikti tik Irano branduolinius įrenginius, mintis, kad kenkėjiška programa pasklido kituose pasaulio kompiuteriuose prisidėjo prie visuotinio nesaugumo jausmo. Šis virusas visame pasaulyje užkrėtė daugiau nei šimtą tūkstančių asmeninių kompiuterių. 2 lentelėje parodytas užkrėstų asmeninių kompiuterių pasiskirstymas pasaulyje.

Tiesioginis ir vienintelis fizinis *„Stuxnet“* viruso efektas buvo gamykloje esančioms urano nusodinimo centrifugoms padaryta žala. Jis buvo aiškiai suprojektuotas taip, kad paveiktų „Natanz“ branduolinį objektą. Buvo manoma, kad kenkėjiška programa daro įtaką centrifugų greičiui, vis sulėtindama jas iki minimalaus greičio ir po to vėl staiga pagreitindama, taip darant įtaką greitesniam centrifugų susidėvėjimui [17]. Šį greičio pokytį virusas užmaskavo atiduodamas į *SCADA* įprastus duomenis, priversdamas operatorius manyti, kad centrifugos sukasi įprastu greičiu. Staigūs greičio pokyčiai lėmė, kad centrifugos greičiau susidėvėjo ir galėjo būti sugadintos nepataisomai. Tai, kaip virusas perimdavo informaciją ir ją pakeitęs atsiduodavo *SCADA* sistemoms, pavaizduota 4 paveiksle.



4 pav. Sistemos, užkrėstos *„Stuxnet“* virusu, duomenų perdavimo schema [15]

2.3. *„Triton“*

Privačią Saudo Arabijos naftos chemijos įmonę 2017 metų rugpjūčio mėnesį ištiko kibernetinė ataka, kuri, tyrėjų teigimu, buvo skirta sugadinti įmonės įrangą ir sukelti visos gamyklos sprogimą. Šis kibernetinis incidentas nebuvo įprasto pobūdžio. Tai buvo vienas iš nedaugelio atvejų, kai kibernetinis ginklas, žinomas kaip *„Triton“*, buvo specialiai sukurtas sugadinti pramoninio valdymo sistemas *(ICS)* [18].

Pramonės kontrolės sistemos yra atsakingos už pramonėje vykdomų procesų stebėjimą bei valdymą, bei nelaimės atveju dirbančių žmonių apsaugą. Saugumo tyrinėtojai atskleidė, kad *„Triton“* kenkėjiška programinė įranga, rasta Saudo Arabijos kompiuteriuose, buvo skirta sunaikinti pačią proceso technologiją - šiuo atveju *„Schneider Electric“* gaminamus *„Triconex“* valdiklius, kurie buvo naudojami viskam, pradedant sistemos stebėjimu ir baigiant avarinių situacijų valdymu. Taigi, naudodamiesi pasirinktinių kodų bibliotekomis, norėdami įgyti nuotolinį šių įrenginių valdymą, įsilaužėliai galėjo išduoti komandas iš bet kurios pasaulio vietos, vykdydami negalimus veiksmus be gamyklos žinios. Nuo manipuliavimo duomenimis iki visiško gamyklos sustabdymo, įvairių galimų baigčių buvo daug [19].

„Triconex“ saugos sistema, kuri yra naudojama naftos chemijos perdirbimo įmonėje, kurią sukūrė *„Schneider Electric“,* yra viena populiariausių saugos sistemų pasaulyje. Šios saugumo sistemos pasaulyje yra sumontuota virš penkiolikos tūkstančių vienetų virš aštuoniasdešimt skirtingų pasaulių valstybių [20]. Ši kibernetinė ataka parodė svarbiausius *„Triconex“* sistemose egzistuojančius saugumo pažeidžiamumus. Kadangi *„Triconex“* dirba plačiame pramonės spektre, pradedant popieriaus gamyklomis ir naftos chemijos pramonės įmonėmis ir baigiant branduolinės energijos jėgainėmis, nė viena pramonės šaka nelieka nepažeidžiama.

5 pav. *„Schneider Triconex“* valdiklis [21]

Kibernetinių ginklų, panaudojamų prieš pramoninės kontrolės sistemas, istorijoje yra nedaug. Todėl bet koks tokio pobūdžio pavyzdys yra svarbus atvejis tyrimams: galime sužinoti apie puolimo būdus, programinės ir aparatinės įrangos pažeidžiamumus, užpuolikų tikslus ir siekius, ir dar daugiau. *„Triton“* esminis dalykas buvo naudoti nuotolinį interneto valdymą. Ankščiau jau nagrinėtame pavyzdyje *„Stuxnet“* valdė Irano centrifugas autonomiškai, kai jau papuolė į sistemos vidų, o tai reiškia, kad kibernetinė ataka turėjo būti iš anksto gerai apgalvota, žinant visas sistemos specifikacijas ir esamą įrangą ir veikimo principus [22].

Tačiau naudodamiesi nuotoliniu interneto valdymu, įsilaužėliai neturi planuoti savo veiksmų, kaip ir kada viskas turi įvykti. Jie gali valdyti procesą realiu laiku ir pakeisti savo ketinimus priklausomai nuo aplinkybių. Šiuo atveju tai yra įrodymas, kad kibernetiniai virusai ilgą laiką gali lengvai pasislėpti sistemose laukdami signalo iš išorės, kad jie turi aktyvuotis.

Retais atvejais kibernetinės atakos yra naudojamos padaryti fizinės žalos pramoninėms valdymo sistemoms *(ICS)*. Bet iki šio įvykio, jos niekada nebuvo naudojamas padaryti žalos, dėl kurios atsirastų rizika žmogaus gyvybei. Todėl ši ataka yra aiškus įspėjimas, kad nors kibernetinės atakos yra skaitmeninės, jų pasekmės vis tiek gali turėtų poveikį žmonių saugumui. Tad kibernetinių atakų prieš svarbius bei galimai pavojingus žmogui objektus ar gamyklas žmonių saugumo klausimas turėtų būti sprendžiamas globaliai.

Pasekmės

„Stuxnet“, *„Triton“* ir kiti panašūs kibernetiniai išpuoliai, nutaikyti į pramonės sektoriaus technologinę dalį, stipriai paveikė visą technologijos sektorių. Tos įmonės, kurių sukurta programinė įranga buvo su pažeidžiamumais, ir kurių kompiuteriai buvo užkrėsti šiais virusais, buvo priverstos reaguoti, kad išvalytų ir apsaugotų savo įrangą nuo kenkėjiškų programų. *„Microsoft“* išleido pataisas, skirtas nulinės dienos išnaudojimams išspręsti, o *„Siemens“* klientams pasiūlė pataisas ir pašalinimo įrankius, kad pašalintų *„Stuxnet“* iš sistemos. Šis virusas buvo pašalintas per kelis mėnesius nuo jo atradimo [14].

Daugumos kibernetinių atakų atveju, žmogaus ar organizacijos sukūrusios kenkėjišką programą tapatybė išlieka neaiški. Minėti pavyzdžiai įrodo, kad įmanoma sukurti labai modernų ir pavojingą kibernetinį virusą, kuris būtų pavojingas pramoninėms sistemoms. Be to, *„Stuxnet“* atvejis parodė, kad oru atskirti (fiziškai atjungti) tinklai nebegali būti laikomi pakankama saugumo priemone.

Pasaulio valstybės suprato, kad jos turi imtis veiksmų, jog jos pačios netaptų tokio išpuolio aukomis. Kelios valstybės, pavyzdžiui, Iranas, investavo į kibernetinį saugumą ir sukūrė karinius kibernetinius vienetus ir centrus tam, kad padidintų savo galimybes artėjančio kibernetinio karo atveju. Kai kurios valstybės taip pat ėmėsi peržiūrėti ir atnaujinti savo kibernetines strategijas, kad apsaugotų valstybinės svarbos objektus ir sustiprintų savo galimybes teisėtai reaguoti į kibernetinius išpuolius [23].

3. Kibernetinių saugos priemonių taikymas

Kalbant apie pramoninio tinklo saugumą, vienas iš svarbiausių ir iš anksto labiausiai apmąstomų dalykų turėtų būti norimo saugumo lygio ir įgyvendinamumo nustatymas. Todėl iš anksto turi būti parengtos strategijos ir priemonės atsižvelgiant į techninius tinklus, kuriuos reikia pasiekti, kad visuomet būtų užtikrintas būtinas saugumas. Tokia sistema turi būti ne tik saugi, bet ir užtikrinti, kad vartotojui bus patogu ja naudotis, ji veiks stabiliai, patikimai ir saugiai. Saugumas tokio lygio sistemose yra ypatingai svarbus. Įsilaužimai į tokią sistemą gali sukelti nemažai žalos – informacijos praradimas, sistemos našumo sumažėjimas, sugadinti fiziniai įrenginiai arba išbalansuotas valdymo procesas gali padaryti nemažai žalos visai įmonės infrastruktūrai. Tad labai svarbu užtikrinti reikiamą apsaugą, kad būtų galima išvengti šios finansinės žalos. Norint užtikrinti tinklo saugumą atsiranda poreikis, kad sistemų integratoriai, integruotų komponentų ir įrangos gamintojai bei sistemos operatoriai bendradarbiautų ir visi atitinkamai laikytųsi saugumo nurodymų.

Norint apsisaugoti nuo kibernetinių atakų pirmiausiai reikėtų pradėti nuo elementariausių veiksmų:

- gamykliškai numatyti vartotojų vardų ir slaptažodžių pakeitimą;
- skirtingiems vartotojoms sukurti individualius prisijungimus ir slaptažodžius;
- apriboti parametrų keitimo teises, nuimti vartotojų teises;
- išjungti nenaudojamus portus;
- naudoti portų apsaugą, stebėjimą ir aliarmų siuntimą dėl pastebėtos įtartinos veiklos;
- apriboti arba visiškai išjungti USB raktų naudojimą;
- išjungti nesaugių protokolų naudojimą, jeigu jie yra nenaudojami;
- įrenginiuose įjungti priverstinį jungimąsi *HTTPS* protokolu;
- naudoti *VLAN* tinklus;
- pašalinti standartinius prisijungimus ir sukurti unikalius, kuriems kiekvienam būtų priskiriamos atitinkamos teisės;
- visados stebėti tinklą, žinoti, kas yra prisijungę ir kas naudojasi šiuo tinklu. Pastebėjus įtartinus vartotojus iškarto imtis priemonių.

Kuo daugiau įvairiausių veiksmų atliekama tinklo apsaugai sustiprinti, tuo sunkiau rasti atvirų spragų tinkle. Reikia uždrausti bet kokį neleistiną fizinį prisijungimą prie tinklo. Dar vienas įrankis, skirtas saugiam prisijungimui prie tinklo - tinklo prieigos kontrolė *(NAC)*. Tai komunikacinių tinklų įrankis, kuris pagal iš anksto nustatytus protokolus nurodo, kaip saugiau prisijungti prie tinklo. Šis įrankis patikrina, ar naujai prisijungiantis įrenginys atitinka nustatytus saugumo kriterijus – ar turi ugniasienę, ar naudoja antivirusinę programą.

Norint apsaugoti savo tinklą nuo *„DoS“* tipo atakų būtina tinklo įrangoje aktyvuoti apsaugą nuo šio tipo kibernetinių atakų. Šį parametrą visados rekomenduojama laikyti įjungtą.

Kita ganėtinai dažna problema, su kuria daugiausiai susiduria pramonės įmonės, tai, kad komunikaciniai tinklai yra labai dideli ir dažniausiai tik su minimaliu arba visiškai jokiu segmentavimu. Apribojimų taikymas tarp *IT* ir *OT* tinklų labai silpnas. *OT* tinkluose nėra jokio tinklų valdymo tarp skirtingų gamybos skyrių. Dažniausiai visi automatikos įrenginiai būna patalpinti viename potinklyje. Vienas iš labai efektyvių būdų kaip apsaugoti savo tinklus, yra juos suskirstyti į atskiras zonas. Visi įrenginiai, kuriems būtina tarpusavio komunikacija, yra paliekami toje pačioje zonoje, o kiti įrenginiai iškeliami į atskiras zonas. Duomenų keitimasis tarp zonų vyksta per specialius

komunikacinius kanalus. Saugumui užtikrinti, informacija, kuri būna per leidžiama per šiuos kanalus, būna griežtai stebima ir filtruojama.

Dar viena iš galimybių, leidžiančių užtikrinti tinklo saugumą – giliųjų paketų tikrinimo naudojimas. Nors šis saugos metodas sumažina tinklų komunikacijos greitį, tačiau jis apsaugo tinklą nuo pavojingų paketų.

Svarbu yra tai, kad kibernetinį saugumą reikia palaikyti pastoviai, todėl ir visų priemonių apsaugoti savo tinklą turi būti imamasi profilaktiškai. Visuomet galima išsibandyti savo tinklus darant periodinius tinklo saugumo / prasiskverbimo testus.

3.1. IEC-62443 standartas

Globalizacijos ir labai konkurencingų rinkų laikais pasaulis reikalauja viską atlikti greičiau ir paprasčiau, todėl visur aplink atsiranda vis daugiau automatizavimo. Tai savo ruožtu padidina kibernetinių grėsmių riziką. Taigi kibernetinio saugumo reikalavimų ir IEC-62443 standarto nurodomų priemonių įdiegimas šiuo metu yra pagrindiniai prioritetai. IEC-62443 – tai kibernetinio saugumo valdymo standartų serija, kurioje pasitelkiamos techninės ataskaitos, susijusi informacija ir apibūdinamas saugių pramoninės automatizavimo ir valdymo sistemų *(IACS)* diegimo procesas.

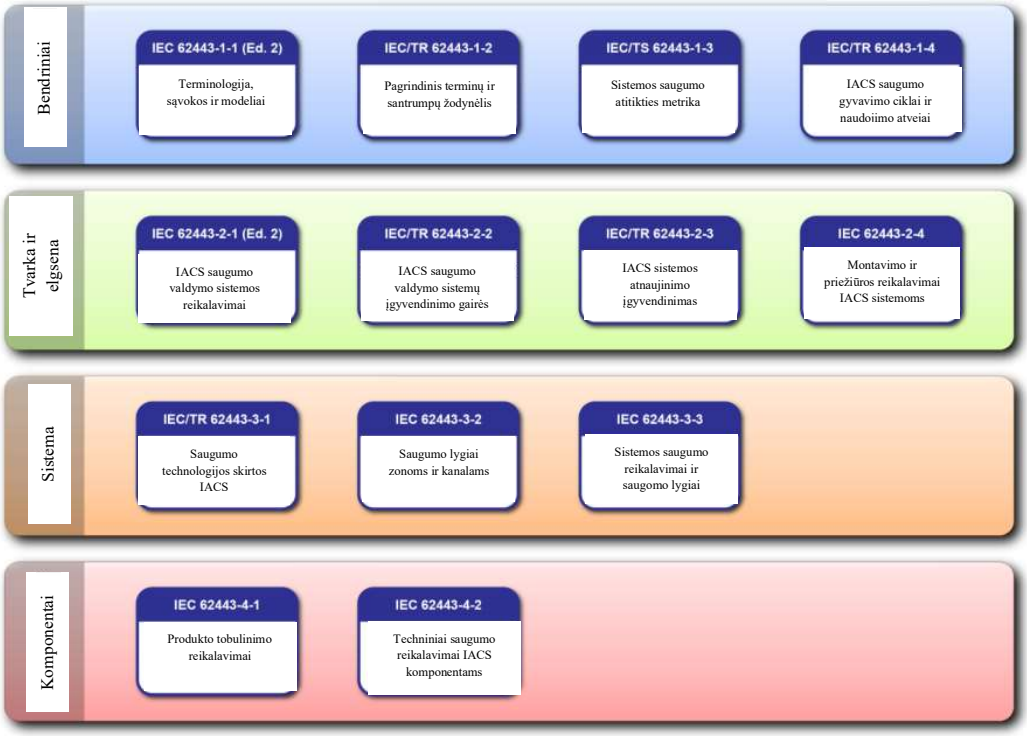
IEC-62443 standartai yra skirti išsamiai *IACS* sistemai ir apibūdina, kaip apsaugos specialistai, sistemos integratoriai ir valdymo sistemų gamintojai turėtų sąveikauti ir užtikrinti jų įrenginių ir komponentų saugą bei saugumą.

Didėjant *IT* ir *OT* konvergencijai, pramoninė interneto sritis plečiasi. Vis daugiau internetinių bei valdymo tinklų yra sujungiami tarpusavyje. Be to, uždaruose tinkluose nebėra oro tarpo ir jie greitai virsta tinklais, sujungtais su biurų ir debesų tinklais. Tai kelia daug rizikos įmonėms ir daro įtaką visai *IACS* sistemai, įskaitant turto savininkus, operatorius ir tiekėjus.

Keletas pagrindinių iššūkių, su kuriais susiduria pramonės atstovai:

- daugeliui kontrolės sistemų trūksta pagrindinių apsaugos mechanizmų (autorizacijos, audito, įvesties patvirtinimo ir kt.), nes jos nebuvo kuriamos atsižvelgiant į saugumą;
- pramoniniai protokolai yra sukurti patikimiems tinklams, o prioritetai yra patikimumas ir prieinamumas;
- atsirandančios technologijos, tokios kaip išmanusis matavimas, mobilusis kompiuteris ir belaidis kompiuteris, pramoniniams įrenginiams kelia vis didesnę kibernetinės atakos riziką.

IEC-62443 standarto įdiegimas yra naudingas organizacijai siekiant pašalinti jų pramoninio kibernetinio saugumo pavojus. Paprasčiau tariant, šis standartas suskirsto tinklus į zonas ir išskiria įvairius duomenų kanalų patikrinimus, kad būtų galima geriau kontroliuoti prieigą ir saugumą valdymo sistemų tinkluose, naudojant tiksliai apibrėžtas sąsajas (kanalus). Jame pateikiama bendra *IACS* saugumo terminologija, pramonės valdymo automatizavimo saugumo valdymo sistema, pateikiamos nuorodos apie pramoninio tinklo saugumo architektūrą ir yra apibrėžti saugos reikalavimai visoje sistemoje ir per visus komponentus. Todėl turto savininkai visame pasaulyje pasirenka šią galimybę apsaugoti savo pramoninį turtą [24].



6 pav. IEC-62443 standarto struktūra [25]

6 paveiksle pavaizduota IEC-62443 standarto struktūra. Jo serija ir techninės ataskaitos skirstomos į šias keturias kategorijas:

- informacija apie sąvokas, terminologiją, modelius, darbo produktus, apibūdinančius saugos metriką;
- kategorija, skirta įvairiems veiksmingos *IACS* saugumo programos generavimo ir palaikymo aspektams, nukreipiantiems į turto savininką;
- pagrindinio sistemos valdymo aprašymas apie sistemos projektavimo gaires ir reikalavimus, kad būtų galima saugiai sujungti valdymo sistemas;
- ketvirtoji kategorija apibūdina valdymo sistemos atnaujinimų techninius reikalavimus ir specifinį produkto vystymą.

4. Tinklo įrangos, skirtos saugumui užtikrinti, tyrimas

Idealiu atveju, kai du įrenginiai komunikuoja tarpusavyje per tinklą, o tinkle nėra daugiau jokių įrenginių, jų komunikacijai daugiau niekas įtakos nedaro. Komunikacijos greitis priklauso vien nuo pačių įrenginių greitaveikos. Tačiau tinkle atsiradus daugiau įrenginių gali kilti įvairių problemų, kurios blogina komunikacijos greitį. Keli iš daugelio komunikacijos suprastėjimo pavyzdžių, gali būti tyčinis ar netyčinis tinklo užteršimas bloga ar sugadinta informacija. Taip gali nutikti dėl sugedusios įrangos, prijungtos prie tinklo, kuri į tinklą transliuoja sugadintą informaciją. Komunikacijos trikdžiai taip pat gali atsirasti dėl orientuotų kibernetinių atakų, nukreiptų prieš įrenginius. Tokiu būdu norima išvesti juos iš rikiuotės. Tyrimo tikslas buvo patikrinti, kaip skirtingų gamintojų ir skirtingų tipų įrenginiai, esant skirtingoms tinklo apkrovos sąlygoms, palaiko komunikaciją tarp bendraujančių įrenginių. Tinklo apkrova buvo sudaryta kuriant *„DoS“* tipo atakas prieš komunikuojančius įrenginius. Tyrimo metu buvo vertinamas komunikuojančių įrenginių atsakas į užklausas esant skirtingiems *„DoS“* tipo atakų parametrams. Buvo palyginta, kaip naudojama skirtinga tinklo įranga apsaugo įrenginių komunikaciją nuo *„DoS“* tipo atakų.

4.1. Tyrimo metu naudota tinklo ir programinė įranga

„Pheonix Contact mGuard rs4004“ maršrutizatorius

„Pheonix Contact mGuard“ šeimos įrenginiai yra skirti užtikrinti pramonės tinklų saugumą. Šie įrenginiai palaiko ugniasienės, tinklų maršrutizavimą ir papildomas *VPN* funkcijas pramoniniuose tinkluose. Šios aukšto lygio trečio sluoksnio funkcijos yra būtinos norint apsaugoti pramoninį tinklą nuo kenkėjiškų išpuolių ir atsitiktinio darbo bei informacijos trikdymo, taip pat apsaugo norint prisijungti prie biurų ar įmonės tinklų. Įvairios aparatinės įrangos parinktys suteikia daug naudojimo galimybių ir lankstumo, tuo pačiu užtikrindamos visišką *„mGuard“* apsaugą ir jungiamumą, pagal unikalius sistemų poreikius. Pramoninio tinklo įranga skiriasi nuo darbastalio ar nešiojamojo kompiuterio tinklų biuro aplinkoje dėl pramoniniams tinklams keliamų skirtingų tinklo prioritetų. *IT* tinkluose prioritetinis tinklo įrangos aspektas yra konfidencialumas, o pramoniniuose tinkluose, dėl labai greitų vidinių procesų, prioritetas yra skiriamas įrenginių prieinamumui. Todėl labai svarbu, kad pramoninio tinklo įranga būtų naudojama atskirai nuo visos įmonės ir biurų.

7 pav. *„Pheonix Contact mGuard rs4004“* tinklo įrenginys [26]

„Pheonix Contact“ gamintojo gaminys *„mGuard rs4004“* (7pav.) veikia *„Linux“* sistemos pagrindu. Šiame įrenginyje yra integruoti keturi pagrindiniai saugos komponentai – dvikryptė ugniasienė,

lankstus *NAT* maršrutizatorius, saugi *VPN* tinklų sąsaja ir pasirinktinai gali būti įdiegta pramonei skirta apsauga nuo kenkėjiškų programų [27].

„mGuard rs4004“ įrenginys gali dirbti kaip *„wan / lan“* maršrutizatorius, jis turi keturias valdomas *„LAN“* jungtis ir vieną specialią *DMZ* (demilitarizuota zona) jungtį su savo individualiomis ugniasienės taisyklėmis. *DMZ* prievadas leidžia labiau suskaidyti segmentus ir atlikti sudėtingesnius saugumo nustatymus atskiriems segmentams. Šio gaminio linija siūlo aukščiausios klasės pramoninį saugumą, kuris idealiai tinka esant dideliems prieinamumo scenarijams ir sudėtingoms saugos architektūroms.

„mGuard rs4004“ puikiai tinka decentralizuotai apsaugai atskiruose gamybos taškuose ar apsaugoti pavienius įrenginius nuo manipuliacijų ir įvairių kibernetinių grėsmių. Centralizuota visos įmonės ugniasienė paprastai nesugeba efektyviai apsaugoti gamybos tinklo sistemų nuo išpuolių tiek iš vidaus, tiek iš išorės. Taigi, gamybos įrenginius galima patikimai apsaugoti nuo sabotažo ir dėl to atsirandančių gamybos prastovų, naudojant decentralizuotą galutinio taško apsaugą.

„*Teltonika RUT240*“ maršrutizatorius

Kitas tiriamas įrenginys – *„Teltonika RUT240“* maršrutizatorius. Tai kompaktiškas, ekonomiškas ir galingas pramoninis *LTE* maršrutizatorius. Jis skirtas saugiam duomenų perdavimui, tinklo ryšio užtikrinimui, tinklo segmentų atskyrimui. Šis maršrutizatorius užtikrina aukštą našumą, kai yra reikalingas mobilus ryšys. Taip gali būti sukuriamas atsarginis išorinis ryšio šaltinis, jeigu dingtų pirminis interneto ryšio tinklas, tokiu būdu užtikrinant atsarginį būdą, kaip saugiai prisijungti prie tinklo.

Šis įrenginys veikia naudojant *„RutOS“* operacinę sistemą, kuri veikia *„Linux“* sistemos pagrindu. Jis sukomplektuotas su *„Atheros Hornet*“ 400 Mhz procesoriumi, 16MB vidinės ir 64MB DDR2 tipo atminties. *„RUT240“* palaiko visas reikalingas saugumo funkcijas, skirtas tinklų saugumui užtikrinti [28].

Ugniasienės pagalba galimas atitinkamų užklausų blokavimas, duomenų paketų filtravimas pagal iš anksto nustatytas taisykles, galima nustatyti sąlygas padedančias apsisaugoti nuo *„DDoS“* kibernetinių atakų. Pasinaudojant *VLAN* ir *VPN* funkcijomis galimas atskirų tinklo segmentų atskyrimas ir papildomų saugos priemonių taikymas norint pasiekti šiuos potinklius.

8 pav. *„Teltonika RUT 240“* tinklo maršrutizatorius [29]

„Huawei B2368-66“ maršrutizatorius

Trečias tiriamasis įrenginys – *„Huawei B2368-66“* maršrutizatorius. Tai *„Huawei“* gamintojo buitinis *LTE* tipo maršrutizatorius dažniausiai naudojamas vietose, kur sudėtingiau atvesti fizinį interneto ryšį. Nors šis įrenginys ir nėra skirtas pramoniniam naudojimui, jis palaiko nemažai saugumą užtikrinančių funkcijų. Užtikrinant ryšio saugumą, galima filtruoti įrenginius pagal *MAC* adresus, aprašyti komunikacijos taisykles, naudoti *„DoS“* atakų blokavimą. Įrenginys taip pat palaiko *L2PT* ir *GRE* tipo *VPN* funkcijas.

9 pav. *„Huawei B2368-66“* maršrutizatorius [30]

„Schneider Electric AS-P“ valdiklis

„Schneider Electric SmartX Controller AS-P“ buvo parinktas, kaip bandomasis įrenginys, prieš kurį bus nukreiptos kibernetinės atakos. Tai galingas įrenginys, kuris gali veikti kaip pavienis serveris, skirtas sistemos apjungimui ir integravimui arba prijungus išorinius praplėtimo modulius gali pats valdyti procesus. Valdiklis veikia *„Linux“* sistemos pagrindu. Jis pagamintas su dviejų branduolių 500Mhz procesoriumi, 512MB DDR3 SDRAM tipo atmintimi ir iki 4 GB vidinės atminties. Valdiklis palaiko daug skirtingų komunikacijų tiek RS-485, tiek *TCP/IP* protokolais. Kadangi komunikacijai tinkle reikia patikimo ryšio, valdiklis buvo pasirinktas, kaip įrenginys, su kuriuo bus atliktas bandymas. Valdiklis bus suprogramuotas, kaip *Modbus TCP/IP* vergas (angl. *slave*) įrenginys ir nuo jo bus nuskaitoma informacija.

10 pav. *„Schneider Electric AS-P“* valdiklis [31]

„Kali Linux“ operacinė sistema

„Kali Linux“ yra galingiausia ir populiariausia pasaulyje komunikacinių tinklų prasiskverbimų testavimo platforma. Ji yra naudojama įvairiausių specialistų tiek *IT*, tiek *OT* sistemose. Sistemos

duomenų bazėje yra sukaupta daugiau nei šeši šimtai įrankių, skirtų įvairioms informacijos saugumo užduotims, tokioms kaip įsiskverbimo testavimas, saugumo tyrimai, kompiuterinė kriminalistika ir atvirkštinė inžinerija. *„Kali Linux“* buvo sukurta kaip laksti sistema, kurią profesionalūs tinklų tikrintojai, saugumo entuziastai, studentai ir mėgėjai gali pritaikyti pagal savo specifinius poreikius. *„Kali Linux“* sistemos sukūrimą ir atnaujinimą finansuoja ir prižiūri pagrindinė informacijos saugumo mokymo įmonė *„Offensive Security“* [32]. Kelios iš pagrindinių *„Kali Linux“* panaudojimo galimybių:

- informacijos rinkimas – duomenų apie tinklą ir jo struktūrą rinkimas, kompiuterių, jų operacinių sistemų ir jų naudojamų paslaugų identifikavimas. Identifikuojamos potencialiai jautrios informacinės sistemos dalys. Visų rūšių įrašai gaunami iš veikiančių servisų;
- pažeidžiamumo analizė – greitai patikrinama, ar vietinei, ar nuotolinei sistemai įtakos neturi daugybė žinomų pažeidžiamumų, ar tinkle nėra palikta nesaugių tinklo konfigūracijų. Pažeidžiamumo paieškos programos naudoja duomenų bazes su jau žinomomis tinklo spragomis, kad nustatytų galimus pažeidžiamumus;
- *web* servisų analizė – netinkamų konfigūracijų ir žiniatinklio programų saugos trūkumų nustatymas. Labai svarbu nustatyti ir sušvelninti šias problemas, atsižvelgiant į tai, kad jos yra viešai prieinamos. Dėl to jos yra idealūs užpuolikų taikiniai;
- išnaudojimo įrankiai – jie skirti išnaudoti ankščiau nustatytą pažeidžiamumą arba juo pasinaudoti, kad įgytų nuotolinio įrenginio valdymą. Tuomet šis įrenginys gali būti naudojamas paskleisti kibernetinėms atakoms vietiniame tinkle;
- uostinėjimo ir šnipinėjimo įrankiai suteikia prieigą prie duomenų, keliaujančių tinklu. Šie duomenys dažnai būna labai naudingi užpuolikams. Su *„Kali Linux“* įdiegtomis sukčiavimo programomis galima apsimesti neteisėtu vartotoju, o su šnipinėjimo programomis galima fiksuoti ir analizuoti tinkle keliaujančius duomenis. Šių dviejų įrankių naudojimas kartu gal būti labai veiksmingas.

4.2. Atsako laiko tyrimas

Tyrimo metu pirmiausia buvo vertinama kompiuterio ir valdiklio komunikacija norint nustatyti komunikacijos greitį, kai nėra jokių išorinių poveikių. Nešiojamas kompiuteris su *„Kali Linux“* operacine sistema buvo sujungtas su *„Schneider Electric AS-P“* valdikliu per *RJ-45* jungtį su 5 kategorijos *FTP* kabeliu. Komunikacijos greičiui įvertinti buvo naudojama *„ping“* komanda. *„Ping“* – tai kompiuterinio tinklo administravimo komanda, kuri interneto valdymo pranešimų protokolu siunčia užklausas kitiems įrenginiams ir tuomet laukia iš jų atsakymų. Ši komanda naudojama tam, kad patikrintų ar kitas įrenginys yra prieinamas, įgalintų komunikaciją tarp įrenginių ir įvertintų, kiek laiko trunka nuo užklausos išsiuntimo iki atsakymo. *„Ping“* užklausos laikas matuojamas milisekundėmis, jis matuojamas nuo paketo išsiuntimo iki atsakymo į išsiųstą paketą gavimo. Pagrindiniai faktoriai, kurie daro įtaką *„ping“* atsako greičiui, yra komunikacijos greitis, tinklo ir įrenginių užimtumas ir fizinis atstumas tarp įrenginių. Atsako laiko vertinimas yra skirstomas į penkias grupes:

- mažiau nei trisdešimt milisekundžių – puikus;
- tarp trisdešimt ir penkiasdešimt milisekundžių – vidutinis;
- tarp penkiasdešimt ir šimto milisekundžių – truputį lėtokas;
- tarp šimto ir penkių šimtų milisekundžių – lėtas;

– daugiau nei penki šimtai milisekundžių – blogas.

Pirmiausia tyrimo metu buvo įvertinta komunikacija tarp kompiuterio ir valdiklio siunčiant šias skirtingas *„ping“* užklausas iš *„Kali Linux“* operacinės sistemos komandinės eilutės:

– root@kali:~# ping 192.168.1.99 (siunčiama 100, 32 baitų, *„ping“* užklausų 1 sekundės intervalu);
– root@kali:~# ping 192.168.1.99 -s 4096 (siunčiama 100, 4096 baitų, *„ping“* užklausų 1 sekundės intervalu);
– root@kali:~# ping 192.168.1.99 -s 16834 (siunčiama 100, 16834 baitų, *„ping“* užklausų 1 sekundės intervalu);
– root@kali:~# ping 192.168.1.99 -s 4096 -i 0.01 (siunčiama 1000, 4096 baitų, *„ping“* užklausų 0,01 sekundės intervalu);
– root@kali:~# ping 192.168.1.99 -s 16834 -i 0.01 (siunčiama 1000, 16384 baitų, *„ping“* užklausų 0,01 sekundės intervalu);
– root@kali:~# ping 192.168.1.99 -s 4096 -i 0.001 (siunčiama 1000, 4096 baitų, *„ping“* užklausų 1 milisekundės intervalu);
– root@kali:~# ping 192.168.1.99 -s 16834 -i 0.001 (siunčiama 1000, 16384 baitų, *„ping“* užklausų 1 milisekundės intervalu);

Šie duomenys buvo gauti idealiu atveju, kai tinkle nėra jokių kitų įrenginių ir kibernetinėmis atakomis neformuojamos tinklo apkrovos sąlygos.

Tyrimo metu tinklo apkrova buvo kuriama prisijungus antrą kompiuterį su *„Kali Linux“* operacine sistema prie to paties tinklo. Naudojant *„Pentmenu“* buvo kuriamos *„ICMP flood“* tipo atakos. *„Ping“* potvynio (angl. *flood*) tipo ataka yra viena iš *„DoS“* atakos rūšių. Jos tikslas – per kuo trumpesnį laiką išsiųsti kuo daugiau užklausų *ICMP* protokolu, kad atakuojamas įrenginys nesuspėtų į jas atsakinėti ir tuo metu įrenginys taptų nebeprieinamas normaliam duomenų srautui, jis neatsakytų į kitų įrenginių jam siųstas užklausas, tad kitiems įrenginiams jis taptų neaktyvus. Nors *ICMP* siunčiamos komandos neužima daug vietos, didelis jų kiekis vis tiek sukuria tinklo apkrovos imitaciją. Tyrimo metu pasitelkus *„pentmenu“* programą, su *„hping3“* buvo siunčiamos tokios komandos *ICMP* potvynio tipo atakai sukurti:

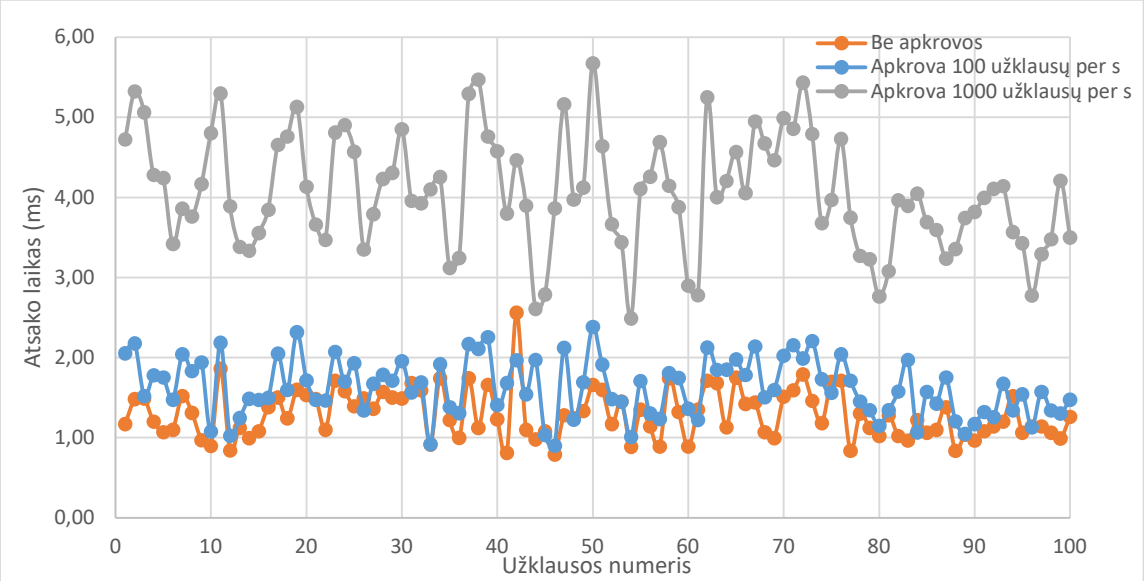
– root@kali:~# hping3 -1 -i u10000 192.168.1.99 (*„ping“* užklausos siunčiamos kas 0,01 sekundės)
– root@kali:~# hping3 -1 -i u1000 192.168.1.99 (*„ping“* užklausos siunčiamos kas 1 milisekundę)
– root@kali:~# hping3 -1 --flood 192.168.1.99 (*„ping“* užklausos siunčiamos maksimaliu greičiu, vidutiniškai tarp dvidešimt – dvidešimt penkių tūkstančių užklausimų per sekundę)

Paleidus „*ICMP flood“* tipo atakas imituojant atakas prieš *„Schneider Electric AS-P“* valdiklį, vėl pakartotos *„ping“* komandos, komunikacijai įvertinti.

3 lentelė. Komunikacijos greičio be tinklo įrangos palyginimas

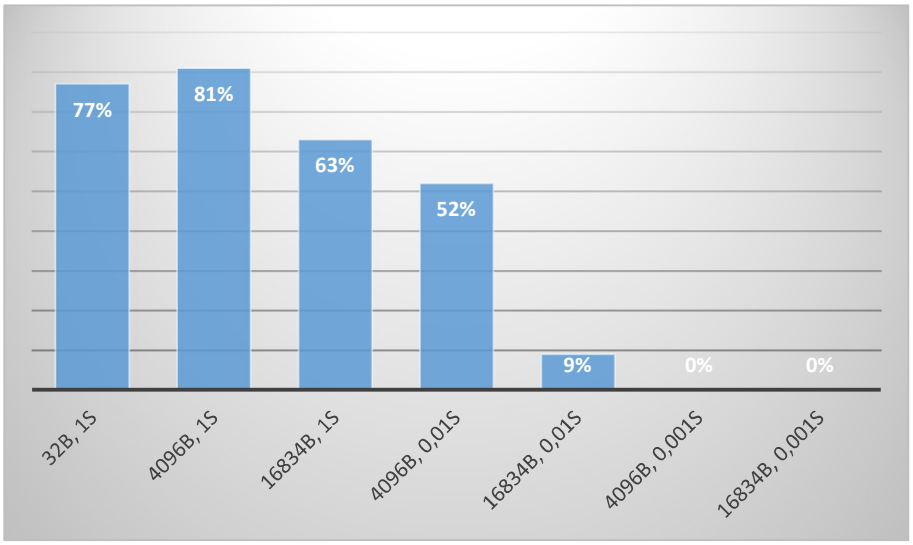
	Be apkrovos		Apkrova - 100		Apkrova - 1000		Apkrova - flood
	Vid.	**Dispersija**	**Vid.**	**Dispersija**	**Vid.**	**Dispersija**	**Vid.**
32B „ping“ 1s	1,29 ms	0,09	1,63 ms	0,13	4,06 ms	0,5	358 ms
4096B „ping“ 1 s	3,04 ms	0,14	3,62 ms	0,18	11 ms	0,93	782 ms
16384B „ping“ 1 s	6,56 ms	0,59	7,74 ms	1,07	23,7 ms	10,8	1724 ms
4096B „ping“ 0,01 s	2,12 ms	0,18	2,94 ms	0,29	13,8 ms	5,45	1744 ms
16834B „ping“ 0,01 s	4,73 ms	0,29	6,25 ms	0,76	29,5 ms	6,8	1931 ms
4096B „ping“ 0,001 s	1,87 ms	0,54	3,52 ms	1,31	22 ms	22,1	-
16834B „ping“ 0,001 s	4,63 ms	0,61	8,89 ms	1,68	67,1 ms	60,1	-

Iš 3 lentelėje pateiktų duomenų matyti, kad imituojant pirmąją apkrovą, vidutinis atsako greitis padidėjo 29 proc. nuo idealaus atvejo. Esant 100 *„ping“* užklausų, apkrovos dispersija padidėjo 2,21 karto. Vidutinis atsako laikas esant šiai apkrovai - 4,94 ms, tai atitinka puikų atsako laiką. Todėl galima teigti, kad tokia pavienė ataka prieš įrenginį jo darbui įtakos neturės. Vertinant rezultatus esant 1000 *„ping“* užklausimų apkrovai matome, kad vidutinis atsako laikas padidėja iki 24,45 ms – padidėja 63,9 proc., o išsibarstymas išauga 43,7 karto. 11 paveiksle matoma, kad reikšmių išsibarstymas esant didesnei apkrovai yra ženkliai didesnis.



11 pav. 32 baitų, 1 sekundės intervalu *„ping“* atsakai esant skirtingoms apkrovos sąlygoms

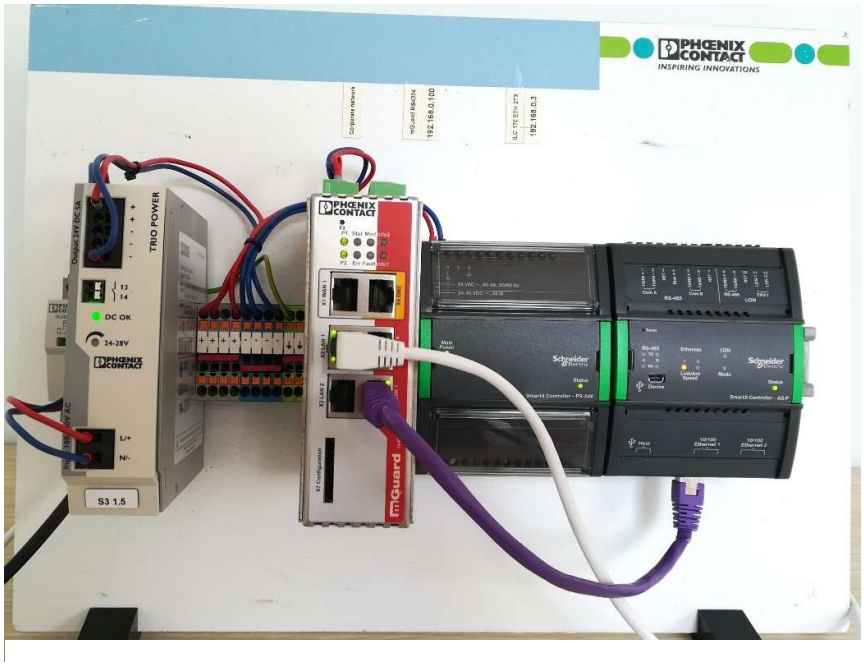
Esant maksimaliam *„ICMP flood“* tipo *„DoS“* atakos greičiui matome, kad įrenginys spėja atsakyti į lėtesnes *„ping“* užklausas. 12 paveiksle matoma, kad esant vienos sekundės intervalui, atsakymas buvo gautas tik iš 74 proc. išsiųstų užklausų. Siunčiant užklausas 0,01 sekundės intervalu, atsakymas gautas tik į 31,5proc. užklausų. Prie greitesnių užklausimų, nebuvo gauta jokio atsakymo iš įrenginio. Pagal rezultatus galima daryti prielaidą, kad esant greitam komunikacijos greičiui, vieno įrenginio, kuriančio *„DoS“* atakas, maksimalių resursų pakanka, kad atakuojamas įrenginys taptų neprieinamas iš tinklo.



12 pav. Gautų paketų skaičius (proc.) esant *„flood“* tipo apkrovai

Apsaugai nuo tokių kibernetinių atakų būtina taikyti vieną ar kelias skirtingas kibernetinės saugos priemones. Šio tyrimo metu naudota tinklo įrangos funkcija – *„DoS“* atakų apsauga. Paprasčiausias būdas apsisaugoti nuo *„DoS“* atakų – tinklo įrangoje nustatyti, kad blokuotų visas *„ping“* tipo komandas. Tačiau to padaryti negalima, nes taip gali sutrikti komunikacija tarp įrenginių, kurie siunčia *„ping“* komandas komunikacijai užmegzti. Todėl įrangoje, prie apsaugos nuo *„DoS“* atakų parametrų, buvo nustatytas maksimalus 500 *„ping“* tipo užklausų pralaidumas per sekundę. Tyrimo metu išbandyta, kaip skirtingų gamintojų ir skirtingų klasių įranga funkcionuoja tomis pačiomis darbo sąlygomis. Tyrimo metu buvo lyginama ši įranga:

- *„Pheonix contact Fl mGuard rs4004“;*
- *„Teltonika RUT240“;*
- *„Huawei B2368-66“.*

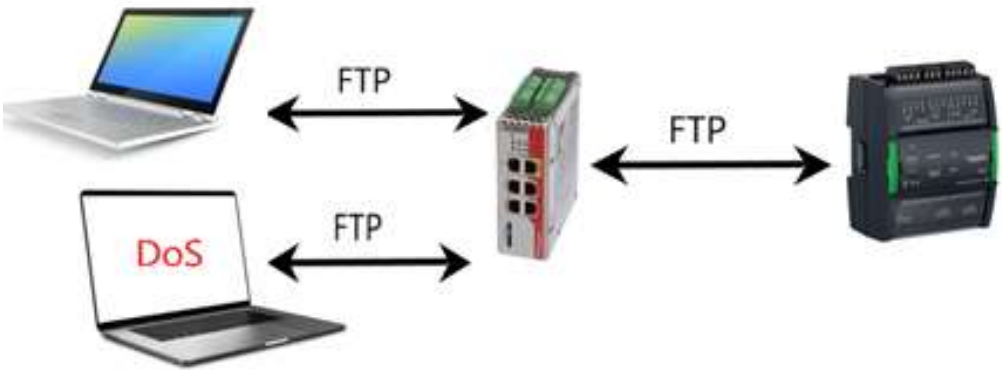


13 pav. Stendas komunikacijos greičio nustatymui naudojant *„mGuard“*

4 lentelė. Komunikacijos greičio su *„mGuard rs4004“* tinklo įranga palyginimas

	Be apkrovos		**Apkrova - 100**		**Apkrova - 1000**		**Apkrova - flood**	
	Vid.	**Dispersija**	**Vid.**	**Dispersija**	**Vid.**	**Dispersija**	**Vid.**	**Dispersija**
32B „ping“ 1s	1,33 ms	0,01	1,52 ms	0,13	2,32 ms	0,28	12,6 ms	8,29
4096B „ping“ 1 s	3,33 ms	0,18	3,95 ms	0,34	6,5 ms	1,14	38,5 ms	51,7
16384 „ping“ 1 s	7,5 ms	1,01	8,84 ms	1,46	14,1 ms	3,99	73,3 ms	139,6
4096B „ping“ 0,01 s	2,53 ms	0,32	3,9 ms	0,88	9,08 ms	5,63	70 ms	203
16834B „ping“ 0,01 s	5,68 ms	0,83	8,92 ms	2,45	18,7 ms	16,6	115,9 ms	553,6
4096B „ping“ 1 ms	2,12 ms	1,01	3,49 ms	4,33	13,4 ms	46,3	163,3 ms	7490
16834B „ping“ 1 ms	5,73 ms	6,7	9,02 ms	18,02	26,5 ms	171,6	198,7 ms	10689

Tyrimo metu, komunikacijos jungimas parodytas 14 paveiksle. Atlikus bandymą su *„Pheonix contact Fl mGuard rs 4004“* įranga, tyrimo metu naudotas stendas pateiktas 13 paveiksle, gauti rezultatai pateikti 4 lentelėje. Lyginant šiuos rezultatus su gautais idealiu atveju, kai du įrenginiai komunikuoja tarpusavyje, matoma, kad dėl atsiradusios papildomos įrangos vidutinis atsako laikas pailgėjo 16,4 proc., o dispersija padidėjo 4,1 karto. Nors įrangos naudojimas padidina atsako laiką, lyginant su normaliomis sąlygomis, tačiau komunikacija vis tiek atitinka puikiai klasei keliamus reikalavimus. Pagrindinė tinklo įrangos nauda matoma prie didesnių apkrovų, kai gaunama 1000 *„ping“* per sekundę ar *„ICMP flood“* tipo užklausų. Prie 1000 užklausų per minutę, naudojant šią tinklo įrangą valdiklio atsako laikas sutrumpėja 89 proc., o prie maksimalios apkrovos atsako laikas



14 pav. Komunikacijos pajungimo schema, atsako greičio tyrimo metu

sumažėja 21 kartą. Tačiau dėl įjungtos *„DoS“* apsaugos, kuri praleidžia tik 500 vieno įrenginio *„ping“* komandų per sekundę, yra nufiltruojama ir dalis komunikacinių *„ping“* signalų. Todėl, kai siunčiamos užklausos 0,001 sekundės intervalu, prarandama dalis signalų. Kai sistema dirba be išorinės apkrovos, sistema gavo 72 proc. paketų, prie 100 *„ping“* apkrovos užklausų, iš valdiklio

buvo gauti 66 proc. paketų, prie 1000 *„ping“* apkrovos užklausų – 69 proc. paketų, prie *„flood“* tipo atakos – 52 proc.

Toks pat bandymas buvo pakartotas su *„Teltonika RUT240“* pramoniniu maršrutizatoriumi, komunikacijos pajungimas analogiškas 14 paveikslui. Gauti rezultatai pateikti 5 lentelėje. Kaip ir su ankščiau lyginta įranga, taip ir su *„RUT240“* gaunami valdiklių užklausų laikai yra lėtesni, lyginant su rezultatais, kur nenaudojama jokia papildoma įranga. Vykstant komunikacijai be apkrovos, naudojant *„RUT240“* gaunamas 26 proc. lėtesnis atsakas. Tačiau ženkliai geresni rezultatai gaunami esant didesnėms apkrovoms.

5 lentelė. Komunikacijos greičio su *„RUT240“* tinklo įranga palyginimas

	Be apkrovos		**Apkrova - 100**		**Apkrova - 1000**		**Apkrova - flood**	
	Vid.	**Dispersija**	**Vid.**	**Dispersija**	**Vid.**	**Dispersija**	**Vid.**	**Dispersija**
32B „ping“ 1 s	1,38 ms	0,11	1,60 ms	0,15	2,46 ms	0,41	17,12 ms	21,46
4096B „ping“ 1 s	3,47 ms	0,25	4,23 ms	0,27	7,26 ms	1,31	50,75 ms	82,23
16384 „ping“ 1 s	7,6 ms	1,09	9,07 ms	1,75	16,42 ms	6,72	82,4 ms	432,7
4096B „ping“ 0,01 s	2,67 ms	1,32	3,96 ms	0,9	10,25 ms	8,42	103 ms	2329
16834B „ping“ 0,01 s	6,64 ms	3,08	8,89 ms	1,68	21,37 ms	18,45	150,1 ms	5441
4096B „ping“ 1 ms	2,38 ms	2,01	4,4 ms	1,97	19,83 ms	121,55	197,5 ms	11534
16834B „ping“ 1 ms	6,39 ms	3,38	10,64 ms	2,64	37,43 ms	386	293,7 ms	19871

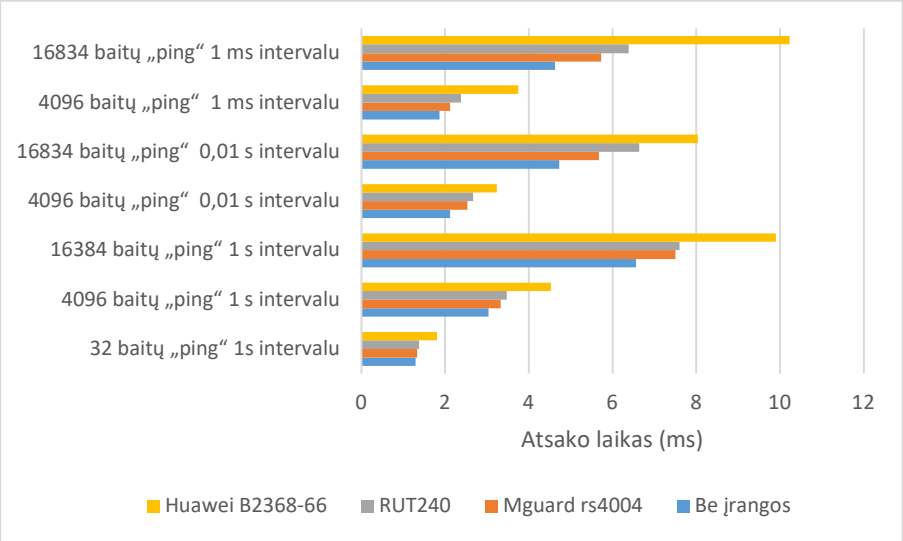
Analogiškas bandymas buvo pakartotas su buitiniu *„Huawei B2368-66“* maršrutizatoriumi. Gauti rezultatai pateikti 6 lentelėje.

6 lentelė. Komunikacijos greičio su *„Huawei B2368-66“* tinklo įranga palyginimas

	Be apkrovos		**Apkrova - 100**		**Apkrova - 1000**		**Apkrova - flood**	
	Vid.	**Dispersija**	**Vid.**	**Dispersija**	**Vid.**	**Dispersija**	**Vid.**	**Dispersija**
32B „ping“ 1s	1,8 ms	0,2	2,21 ms	0,28	2,9 ms	0,64	22,21 ms	37,37
4096B „ping“ 1 s	4,53 ms	0,39	5,86 ms	0,61	8,54 ms	2,63	66,95 ms	170,2
16384 „ping“ 1 s	9,9 ms	2,07	13,99 ms	4,7	20,75 ms	13,97	122,66 ms	1098
4096B „ping“ 0,01 s	3,23 ms	1,19	4,05 ms	0,87	13,59 ms	17,87	111,67 ms	4116

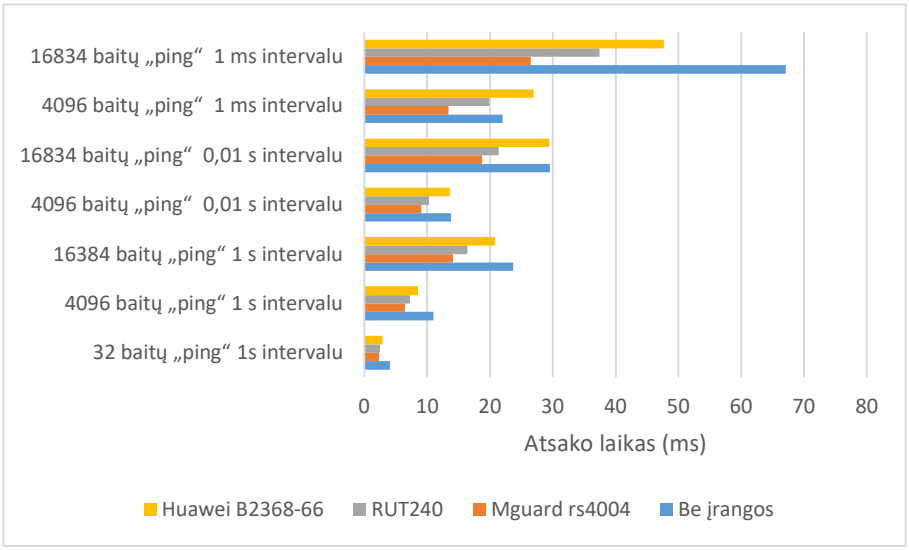
16834B „ping“ 0,01 s	8,03 ms	1,84	9,1 ms	1,69	29,42 ms	42,34	180,21 ms	8408
4096B „ping“ 1 ms	3,75 ms	1,53	4,87 ms	6,73	26,93 ms	161,2	240,53 ms	16181
16834B „ping“ 1 ms	10,23 ms	13,53	12,82 ms	31,52	47,7 ms	699,3	349,02 ms	34630

Iš gautų rezultatų matyti, kad esant tokioms darbo sąlygoms, kai nėra jokios kenksmingos tinklo apkrovos (15 paveikslas) ir žemesniems komunikacijų greičiams, naudojant skirtingą įrangą, atsako laikai yra labai panašūs. Jei svyruoja nuo 1,33 ms iki 1,8 ms, kai atsako laiko vidurkis be tinklo įrangos yra 1,29 ms. Esant intensyvesnei komunikacijai, dėl tinklo įrangos naudojimo, papildomai gali atsirasti iki 6,6 ms vėlavimas. Bandymo metu, be apkrovos *„Pheonix contact“* ir *„Teltonika“* gamintojų įrenginių gauti rezultatai yra labai panašūs – jie skiriasi nuo 1 proc. iki 17 proc.. Tuo tarpu rezultatai gauti su *„Huawei“* įrenginiu, nuo *„mGuard“* skiriasi nuo 25 proc. iki 80 proc.



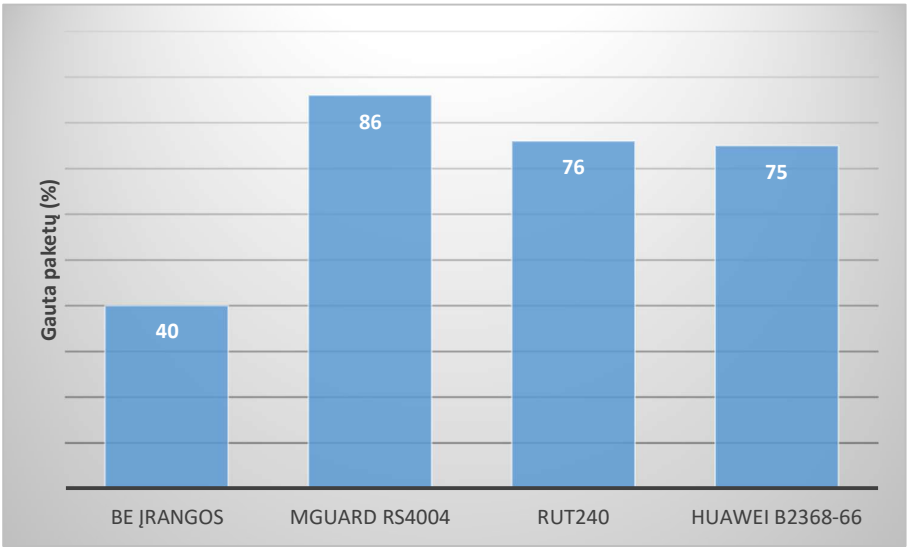
15 pav. Atsako laikas naudojant skirtingą įrangą, kai nėra apkrovos

Svarbiausia, tinklo įrangos naudojimo svarba pasirodo, kai reikia apriboti ir sustabdyti neleistinas tinklo komunikacijas, kibernetines atakas ar kitaip stabilizuoti ir išlaikyti teisingai veikiantį tinklą. 16 paveiksle parodyta, kokie atsakymo laikai į išsiųstas užklausas gaunami iš valdiklio, kai valdiklis yra veikiamas *„DoS“* tipo ataka. Šio bandymo metu buvo tiriamas atsako laikas esant 1000 *„ping“* užklausų per sekundę. Diagramoje matoma, kad tinklo įranga sutrumpina atsako laiką iki 81 proc. Geriausias rezultatas buvo gautas naudojant *„mGuard rs 4004“* įrangą, kurios atsako vidurkis per 7 skirtingus užklausimus buvo 12,94 ms, *„RUT240“* vidurkis – 16,43 ms (27 proc. didesnis), o *„Huawei“* – 21,4 ms (66 proc. didesnis).



16 pav. Valdiklio atsako laikas, esant 1000 *„ping“* komandų per sekundę apkrovai

17 paveiksle pavaizduotas sėkmingai gautų paketų skaičius, kai valdiklis buvo atakuojamas maksimaliu resursu, su *„ICMP flood“* tipo *„DoS“* kibernetine ataka, kuomet siunčiama nuo 20 iki 25 tūkstančių užklausų per sekundę. Diagramoje matoma, kad atliktuose bandymuose, esant tokiai apkrovai, apsaugai naudojant tinklo įrangą, buvo gauta nuo 87,5 proc. iki 115 proc. daugiau paketų.



17 pav. Iš valdiklio gaunamas paketų vidurkis, esant maksimaliai apkrovai

4.3. Modbus TCP/IP nuskaitymo tyrimas

Modbus – tai 1979 metais *„Modicon“* firmos išleistas nuoseklusis komunikacinis protokolas. Modbus leidžia valdančiajam įrenginiui nusiskaitinėti informaciją iš linijoje sujungtų įrenginių. Dėl savo paprasto ir pigaus panaudojimo plačiai paplitęs tarp laisvai programuojamų valdiklių ir *SCADA* sistemų. Modbus TCP/IP tai standartinio Modbus RTU modifikacija su TCP sąsaja ir prijungta prie eterneto. Tyrimo metu, naudota *„Schneider Electric EcoStructure“* programinė įranga, *AS-P* valdiklyje sukonfigūruota Modbus TCP/IP vergo sąsaja. Joje patalpintas analoginis kintamasis, kurio registro numeris yra 101. Šis registras buvo susietas su programa, kuri kiekvieną sekundę padidina registro reikšmę vienetu. Tad valdiklyje, kurio *IP* adresas buvo 192.168.1.99, Modbus įrenginio

adresas - 1, 101 registre buvo analoginis kintamasis, kuris kiekvieną sekundę padidina savo reikšmę vienetu. Kitam kompiuteryje, iš kurio buvo daromas duomenų nuskaitymas, naudojant tapačią programinę įrangą, buvo sukurtas *„Enterprise“* serveris, kuris turi galimybę nuskaityti Modbus TCP/IP protokolą. Sukonfigūravus Modbus sąsają, struktūrizuoto teksto kalba buvo parašytas programos kodas (18 paveikslas), kuris kas 0,1 sekundės nuskaitinėja valdiklyje kintančią reikšmę, ir tuo pačiu skaičiuoja, kiek laiko trunka, kol ši reikšmė pasikeičia. Nuskaičius šias reikšmes, jos įrašomos į atmintį.

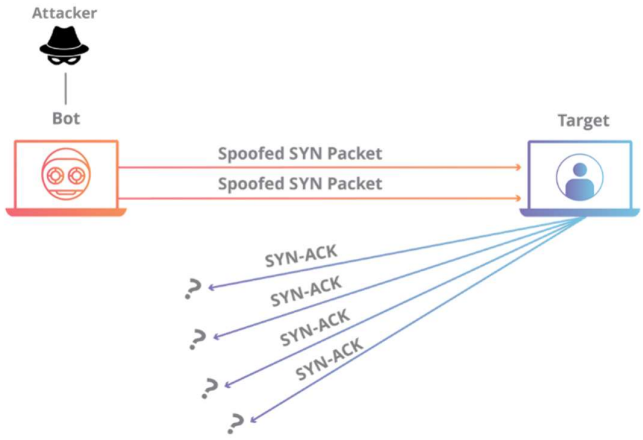
```
Numeric Input Reiksme
Numeric Output Pokytis
Numeric Public Atmintis
Numeric Output Atmintis_Pokytis
Numeric Output Skirtumas

Init:
  Atmintis_Pokytis=0
  Pokytis = 0
  Atmintis = Reiksme
  goto LineA

LineA:
Pokytis = Pokytis + 0.1
if Atmintis <> Reiksme Then
Atmintis_Pokytis = Pokytis
Pokytis = 0
Skirtumas = Reiksme - Atmintis
Atmintis = Reiksme
Goto LineA
Endif
```

18 pav. *„Enterprise“* serveryje parašytas kodas reikšmės nuskaitymui ir įrašymui į atmintį

Bandymo metu prieš valdiklį naudota *„TCP SYN flood“* tipo *„DoS“* ataką. Kaip ir *„ICMP flood“* atakos, jos tikslas yra padaryti įrenginį neprieinamą normaliai duomenų srautui. Siunčiant didelius kiekius paketų pasirinktam įrenginiui, galima padaryti, kad įrenginys atsakinėtų į užklausas labai lėtai arba iš vis į jas neatsakytų.



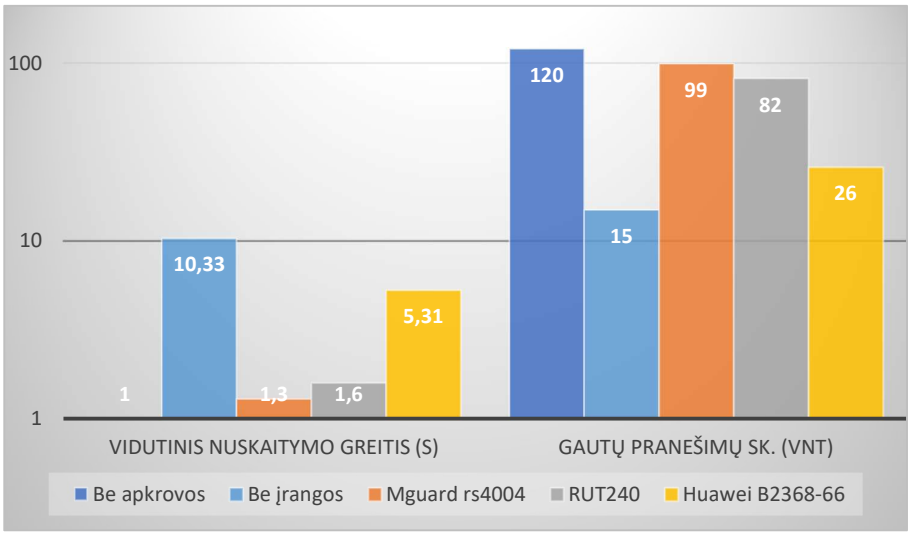
19 pav. *„DoS SYN Flood“* kibernetinės atakos schema [33]

Ši ataka veikia rankų paspaudimo autentifikacijos per *TCP* komunikaciją pagrindu. Tai trijų žingsnių veiksmas (19 pav.). Pirmiausia atakuojantis įrenginys išsiunčia *SYN* užklausą taikiniui, tada taikinys į šią užklausą atsako savo *SYN/ACK* užklausa ir klausosi tinklo, laukdamas, kol gaus *ACK* užklausą atgal. Kol įrenginys klausosi ir laukia, kol gaus *ACK* užklausą, kibernetinė ataka toliau tęsiama, siunčiama dar daugiau *SYN* užklausų, kas priverčia įrenginį atidarinėti naujas jungtis, laukiant sugrįžtančio *ACK* paketo. Naudojant *„Kali Linux“* operacinę sistemą su *„Pentmenu“* programa buvo sukonfigūruota *„TCP SYN Flood“* ataka prieš 192.168.1.99 adresu esantį valdiklį (20 pav.). Ataka buvo nukreipta prieš 502 portą, kurį valdiklis naudoja Modbus komunikacijai.

```
Pentmenu>3
TCP SYN Flood uses hping3 ... checking for hping3 ...
hping3 found, continuing!
Enter target:
192.168.1.99
Enter target port (defaults to 80):
502
Using Port 502
Enter Source IP, or [r]andom or [i]nterface IP (default):
r
Send data with SYN packet? [y]es or [n]o (default)
y
Enter number of data bytes to send (default 3000):
3000
Starting TCP SYN Flood. Use 'Ctrl c' to end and return to menu
HPING 192.168.1.99 (eth0 192.168.1.99): S set, 40 headers + 3000 data bytes
hping in flood mode, no replies will be shown
```

20 pav. *„DoS SYN Flood“* atakos nustatymai *„Kali Linux"* operacinėje sistemoje

Bandymas buvo atliktas 5 būdais. Kiekvienas bandymas truko 120 sekundžių. Pirmiausia buvo išbandytas nuskaitymas be papildomos įrangos ir be apkrovos, tada nuskaitymas darytas paleidus kibernetinę ataką į valdiklį. Po to paeiliui buvo išbandyta *„mGuard“*, *„RUT240“* ir *„Huawei“* tinklo įranga. Bandymo rezultatai pateikti 21 paveiksle.



21 pav. . Taškų nuskaitymo per Modbus bandymo rezultatai

Iš grafiko matyti, kad idealiam atvejui artimiausi rezultatai buvo gauti naudojant *„Pheonix contact mGuard rs4004“* ir *„Teltonika RUT240“* įrangą. Vidutinis nuskaitymo greitis atitinkamai skyrėsi 0,3 ir 0,6 sekundės, o praleista buvo atitinkamai 21 ir 38 pranešimai. Bandymo, kai nuskaitoma buvo be tinklo įrangos, vidutinis nuskaitymo greitis daugiau nei 10 kartų didesnis už bandymą idealiu atveju. Šio bandymo metu buvo gauti tik 15 pranešimų iš 120, tai mažiau nei kas dešimtas pranešimas. Tad tinklo įrangos naudojimas garantuoja patikimesnį ir greitesnį duomenų perdavimą, kai komunikaciją norima paveikti kibernetinėmis atakomis.

Išvados

1. Atlikus literatūros analizę nustatyta, kad dėl sparčiai didėjančio prie tinklo jungiamų įrenginių skaičiaus atsiranda vis daugiau galimų saugumo spragų.
2. Išanalizavus įmonių investicijų prioritetus, pastebėta, kad vis daugiau investicijų skiriama kibernetinio saugumo klausimams.
3. Atlikus literatūros analizę pastebėta, kad nuo 2010 metų pastebima vis daugiau kibernetinių atakų / virusų, kurie būtų nukreipti prieš programuojamus loginius valdikius ir *SCADA* sistemas, o didėjant informacijos ir programinės įrangos prieinamumui, kibernetinių atakų skaičius ir sudėtingumas didėja, o tam reikalingas žinių kiekis mažėja.
4. Išanalizavus IEC-62443 standartą, nustatyta, kad jis ne tik apibrėžia, ko reikia imtis, kad būtų užtikrintas kibernetinis saugumas, bet ir prabrėžia, kad būtina naujinti ir tobulinti saugos mechanizmus.
5. Bandymų metu nustatyta, kad esant 1000 užklausimų per sekundę, *„Pheonix contact mGuard“* maršrutizatorius komunikacijos greitį pagerina 81 proc. Su *„Teltonika RUT240“* ir „*Huawei B2368-66“* gauti rezultatai atitinkamai yra 27 proc. ir 66 proc. prastesni.
6. Modbus TCP / IP nuskaitymo bandymo metu atrasta, kad *„Pheonix contact mGuard“* ir *„Teltonika RUT240“* gauti rezultatai, kai nuskaitomas įrenginys buvo veikiamas kibernetinėmis atakomis, nuo rezultatų gautų idealiuoju atveju skiriasi atitinkamai tik 17 proc. ir 32 proc., o vidutinis nuskaitymo laikas skiriasi atitinkamai 0,3 ir 0,6 sekundės. Rezultatas gautas su *„Huawei B2368-66“* maršrutizatoriumi buvo 82 proc. prastesnis ir buvo tik 6 proc. geresnis lyginant su rezultatais, gautais nenaudojant tinklo saugos įrangos.
7. Apibendrinant rezultatus, geriausi rezultatai gauti naudojant *„Pheonix contact mGuard rs4004“* maršrutizatorių, dirbant be apkrovos šie rezultatai nuo idealių skyrėsi mažiau nei 5 proc., esant didesniam apkrovimui komunikacijos greitį padidina 13 kartų, o patikimumą 2 kartus. Duomenų nuskaitymo bandymo metu, su šiuo įrenginiu gautas 6,7 karto geresnis nuskaitymo patikimumas ir 8 kartus greitesnis nuskaitymas. Su *„Teltonika RUT240“* maršrutizatoriumi gauti rezultatai lyginant su *„mGuard“* yra 15 proc. prastesni. Prasčiausi rezultatai gauti su *„Huawei B2368-66“* maršrutizatoriumi.

Literatūros sąrašas

1. Rüßmann M, Lorenz M, Gerbert P. (2015) Industry 4.0: the future of productivity and growth in manufacturing industries. [Interaktyvus] [žiūrėta 2020 m. vasario 15 d.] Prieiga per internetu: <https://www.zvw.de/media.media.72e472fb-1698-4a15-8858-344351c8902f.original.pdf>
2. [Frost A, Sullivan P. (2017) Cyber Security in the Era of Industrial IoT. [Interaktyvus] [žiūrėta 2020 m. kovo 15 d.] Prieiga per internetą: <https://ww3.frost.com/files/5314/8941/8579/CYBER_SECURITY_IN_THE_ERA_OF_INDUSTRIAL_IOT.pdf>
3. Chen, T M, and S. Abu-Nimeh. "Lessons from Stuxnet." Computer 44.4 (2011): 91-93. Web. [žiūrėta 2020 m. kovo 15 d.] Prieiga internetu: <https://vb.ktu.edu/permalink/f/1746fh5/TN_ieee_s5742014>
4. Weber R H, Studer E (2016). Cybersecurity in the Internet of Things: Legal Aspects. [Interaktyvus] [žiūrėta 2020 m. kovo 18 d.] Prieiga per internetą: <https://vb.ktu.edu/permalink/f/1746fh5/TN_sciversesciencedirect_elsevierS0267-3649(16)30116-9>
5. Abomhara M, Kien GM (2015) Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. [Interaktyvus] [žiūrėta 2020 m. kovo 20 d.] Prieiga per internetą: <https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_414.pdf>
6. Capgemini (2015) Securing the internet of things opportunity: putting cybersecurity at the heart of the IoT. [Interaktyvus] [žiūrėta 2020 m. kovo 30 d.] Prieiga per internetą: <https://www.capgemini.com/wp-content/uploads/2017/07/securing_the_internet_of_things_opportunity_putting_cyber_security_at_the_heart_of_the_iot.pdf>
7. Sethi P, Sarangi SR (2017) Internet of things: architectures, protocols, and applications. [Interaktyvus] [žiūrėta 2020 m. kovo 28 d.] Prieiga per internetą: <https://www.researchgate.net/publication/312957467_Internet_of_Things_Architectures_Protocols_and_Applications>
8. Li S (2017) Security requirements in IoT architecture. ISBN: 0128045051, 9780128045053
9. Tweneboah-Koduah S, Skouby KE, Tadayoni R (2017) Cyber security threats to IoT applications and service domains. doi:10.1007/s11277-017-4434-6
10. BI Intelligence (2015) The enterprise internet of things market—business insider. [Interaktyvus] [žiūrėta 2020 m. kovo 30 d.] Prieiga per internetu: <http://www. businessinsider.com/the-enterprise-internet-of-things-market-2015-7.>
11. Kibernetinių atakų raidos paveikslas [žiūrėta 2020 balandžio 17 d.] Prieiga per internetą: <https://projectswiki.eleceng.adelaide.edu.au/projects/index.php/Projects:2016s1-160a_Cyber_Security_-_IoT_and_CAN_Bus_Security>
12. Solms R., Niekker J. From informacion security to cyber security. (2013). Web. [žiūrėta 2020 m. balandžio 3 d.] Prieiga per internetą: <https://ldc.usb.ve/~torrealba/sti-242/4ta_Clase/solms-2013.pdf>
13. Baezner, Marie, and Patrice Robin. *CSS Cyber Defense Hotspot Analysis (4)* (2017): CSS Cyber Defense Hotspot Analysis (4). Web. [žiūrėta 2020 m. balandžio 6 d.] Prieiga per internetą: <https://vb.ktu.edu/permalink/f/1746fh5/TN_ethz_soai_www_research_collection_ethz_ch_20_500_11850_200661>

14. Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon." IEEE Security & Privacy 9.3 (2011): 49-51. Web. [žiūrėta 2020 m. kovo 30 d.] Prieiga per internetą: <https://vb.ktu.edu/permalink/f/1746fh5/TN_ieee_s5772960 >
15. Sistemos veikimo schema. [žiūrėta 2020 m. kovo 30 d.] Prieiga per internetą: <https://upload.wikimedia.org/wikipedia/commons/thumb/9/9b/Step7_communicating_with_plc.svg/1024px-Step7_communicating_with_plc.svg.png)>
16. W32.Stuxnet [žiūrėta 2020 m. kovo 30 d.] Prieiga per internetą: <https://www.symantec.com/security-center/writeup/2010-071400-3123-99>
17. Farwell, James P, and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." Survival 53.1 (2011): 23-40. Web. [žiūrėta 2020 m. balandžio 6 d.] Prieiga per internetą: <https://vb.ktu.edu/permalink/f/1746fh5/TN_informaworld_s10_1080_00396338_2011_555586 >
18. Bing, C. *Trisis Has the Security World Spooked, Stumped and Searching for Answers*. (2018). Web. [žiūrėta 2020 m. balandžio 6 d.] Prieiga per internetą: <https://www.cyberscoop.com/trisis-ics-malware-saudi-arabia/>
19. Johnson, B. *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure*. (2017). Web. [žiūrėta 2020 m. balandžio 8 d.] Prieiga per internetą: < https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html>
20. Schneider Electric. *Triconex History*. Web. [žiūrėta 2020 m. balandžio 6 d.] Prieiga per internetą: <https://www.schneider-electric.com/en/brands/triconex/triconex-history.jsp>
21. Schneider Truconex valdiklis. [žiūrėta 2020 m. balandžio 6 d Prieiga per internetą: <https://www.se.com/uk/en/work/products/industrial-automation-control/triconex-safety-systems/>
22. Franceschi-Bicchierai, L. *The History of Stuxnet: The World's First True Cyberweapon*. (2016). Web. [žiūrėta 2020 m. kovo 26 d Prieiga per internetą: <https://www.vice.com/en_au/article/ex95m4/the-history-of-stuxnet-the-worlds-first-true-cyberweapon>.
23. Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." Security Studies 22.3 (2013): 365-404. Web. [žiūrėta 2020 m. kovo 26 d.] Prieiga per internetą: <https://vb.ktu.edu/permalink/f/1746fh5/TN_informaworld_s10_1080_09636412_2013_816122 >
24. Bouhdada J. „Things you need to know about IEC 62443 standarts" (2007). Web. [žiūrėta 2020 m. kovo 30 d.] Prieiga per internetą: <https://applied-risk.com/resources/things-you-need-to-know-about-iec-62443-standards>
25. IEC 62443 Struktūra. [žiūrėta 2020 m. kovo 30 d.] Prieiga per internetą: <https://webstore.iec.ch/preview/info_iec62443-3-3%7Bed1.0%7Den.pdf>
26. Pheonix Contact „mGuard rs4004" įrenginys. [žiūrėta 2020 m. kovo 30 d.] Prieiga per internetą: <https://www.alliedelec.com/product/phoenix-contact/2701877/70665667/>
27. mGuard hardware (2020). Web. [žiūrėta 2020 m. balandžio 6 d.] Prieiga per internetą: <https://www.phoenixcontact.com/online/portal/us?1dmy&urile=wcm:path:/usen/web/main/products/subcategory_pages/Cyber_security_P-08-10-08/092edcd8-53eb-4a1e-8113-358e8c20d104/092edcd8-53eb-4a1e-8113-358e8c20d104>

28. Teltonika RUT240 datasheet. Web. [žiūrėta 2020 m. balandžio 16 d.]. Prieiga per internetą: <https://teltonika-networks.com/downloads/en/rut240/Datasheet-RUT240-v1.4.pdf>
29. Teltonika RUT240 paveikslas [žiūrėta 2020 balandžio 17 d.] Prieiga per internetą: <https://teltonika-networks.com/lt/product/rut240/>
30. Huawei B2368-66 paveikslas [žiūrėta 2020 balandžio 17 d.] Prieiga per internetą: <https://e.huawei.com/se/products/wireless/elte-access/terminal/b2368>
31. Schneider Electric AS-P paveikslas [žiūrėta 2020 balandžio 17 d.] Prieiga per internetą: <https://www.se.com/id/en/product/SXWASPXXX10001/smartx-controller-as-p/>
32. Ofensive security. Kali (2019). Web. . [žiūrėta 2020 m. balandžio 7 d.] Prieiga per internetą: <https://www.kali.org/docs/introduction/should-i-use-kali-linux/>
33. DoS SYN Flood atakos schema paveikslas [žiūrėta 2020 balandžio 17 d.] Prieiga per internetą: <https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/>