KAUNO TECHNOLOGIJOS UNIVERSITETAS

ELEKTROS IR ELEKTRONIKOS FAKULTETAS

Vytenis Gumauskas

PRAMONINIŲ KOMPIUTERINIŲ TINKLŲ SAUGUMO SISTEMŲ TYRIMAS

Baigiamasis magistro projektas

Vadovas
Doc. dr. Romas Rutkauskas

KAUNAS, 2015

KAUNO TECHNOLOGIJOS UNIVERSITETAS
ELEKTROS IR ELEKTRONIKOS FAKULTETAS
AUTOMATIKOS KATEDRA

PRAMONINIŲ KOMPIUTERINIŲ TINKLŲ SAUGUMO SISTEMŲ TYRIMAS

Baigiamasis magistro projektas
Valdymo Technologijos (kodas 621H66001)

Vadovas
Doc. dr. Romas Rutkauskas

Recenzentas

Projektą atliko
Vytenis Gumauskas

KAUNAS, 2015

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Elektros ir Elektronikos fakultetas

(Fakultetas)

Vytenis Gumauskas

(Studento vardas, pavardė)

Valdymo technologijos, kodas 621H66001

(Studijų programos pavadinimas, kodas)

Baigiamojo projekto „Pramoninių kompiuterinių tinklų saugumo sistemų tyrimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 15 m. gegužės 25 d.

Kaunas

Patvirtinu, kad mano **Vytenio Gumausko** baigiamasis projektas tema „Pramoninių kompiuterinių tinklų saugumo sistemų tyrimas“ yra parašytas visiškai savarankiškai, o 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)*

Santrauka

Autorius: Vytenis Gumauskas
Pavadinimas: „Pramoninių kompiuterinių tinklų saugumo sistemų tyrimas“
Kalba: lietuvių
Puslapių skaičius: 53
Iliustracijų skaičius: 51
Lentelių skaičius: 4

Raktiniai žodžiai: Saugumo sistemos, ugniasienė, tinklo saugumas, šifravimas, VPN, Jungtinė apsaugos sistema.

Sparčiai tobulėjant skaitmeninėms technologijoms, vis didesnę įtaką pramonėje daro tinklų saugumas. Tobulėjant protokolams, spartėjant perdavimo greičiams, sukuriant naujas duomenų perdavimo technologijas, sudaromos sąlygos neautorizuotų svečių vizitams tinkle, kas gali sukelti neplanuotus nuostolius kompanijai. Dėl šios priežasties siekiama užkirsti kelią įsilaužimui prieš jam įvykstant. Tobulėjant įsilaužimų metodams, esame priversti tobulinti ir apsaugos priemones. Šiame darbe bus tiriamos apsaugos sistemos, jų panaudojimo sritys, pasinaudojant surinkta medžiaga, sukurta universali įmonės tinklo apsaugos sistema, atskirianti LAN (angl. *Local Access Network*) – įmonės tinklą nuo nesaugaus interneto tinklo, kas yra pagrindinis atakų šaltinis. Apžvelgtos vidinės LAN tinklo apsaugos sistemos, saugančios nuo vidinės kilmės įsibrovimų. Jungtinę tinklo apsaugos sistemą sudaro įprastos įsilaužimo aptikimo, įsilaužimo prevencijos ir ugniasienės apsaugos sistemos. Atlikta tinklo pranešimų analizė pagal DoS (angl. Denial of Service) atakos kriterijus, taip pat aptiktas pps (pranešimai per sekundę) duomenų srauto padidėjimas iki 1879% arba 3729% (skirtingais vertinimo metodais) tiriant interneto duomenų srautą, lankantis galimai kenksmingo turinio svetainėse. Remiantis šiuo bandymu, Matlab Simulink aplinkoje atliktas įprastos ugniasienės ir Jungtinės apsaugos sistemos, kurią sudaro ugniasienė, įsilaužimo aptikimo ir prevencijos sistemos, kurios pagrindinis privalumas yra galimybė realiu laiku papildyti įsilaužimo duomenų bazę, tyrimas. Pastaroji sistema nepraleidžia prieš tai aptiktų atakų šaltinių, tikrindama pranešimo antraštę.

Summary

Author: Vytenis Gumauskas
Name: „Investigation of security systems in industrial computer networks“
Speech: lithuanian
Number of pages: 53
Number of figures: 51
Number of tables: 4

Key words: Security systems, firewall, network security, encryption, VPN, Joint network security system.

When rapidly increases advantages of digital technology, also increases impact of network security in the industry. With the development of protocols, increase trensfer throughput, creating a new data transmittion technology, allowing unauthorized visitors online visits, which may cause unexpected losses for the company. For this reason, we need to prevent burglary before it takes place. With the development of methods of attack, we are forced to improve safeguard tools. This paper will examine the security systems and their application areas, using sourses collected, also created a versatile industry network security system that separates the LAN (Local Access Network) – the company network from the unsafe network, which is the main source of the attacks. Universal network security system consists of conventional intrusion detection, intrusion prevention and firewall security system. In addition, an overview of the internal LAN security systems designed to prevent the intrusion of internal origin. Joint network security system consists of conventional intrusion detection, intrusion prevention and firewall security system. Made network analysis reports by DoS (Denial of Service) attacks criteria also detected pps (packets per second) bandwidth increase by 1879% and 3729% (in different assessment methods) investigation of Internet data traffic, while visiting potentially harmful content sites. Based on this test, Matlab Simulink environment carried out in the usual firewall and security system, which includes a firewall, intrusion detection and prevention system, whose main advantage is the possibility of real-time supplement hacking database research. This system is suitably against the attacks of sources detected by examining the message header.

Turinys

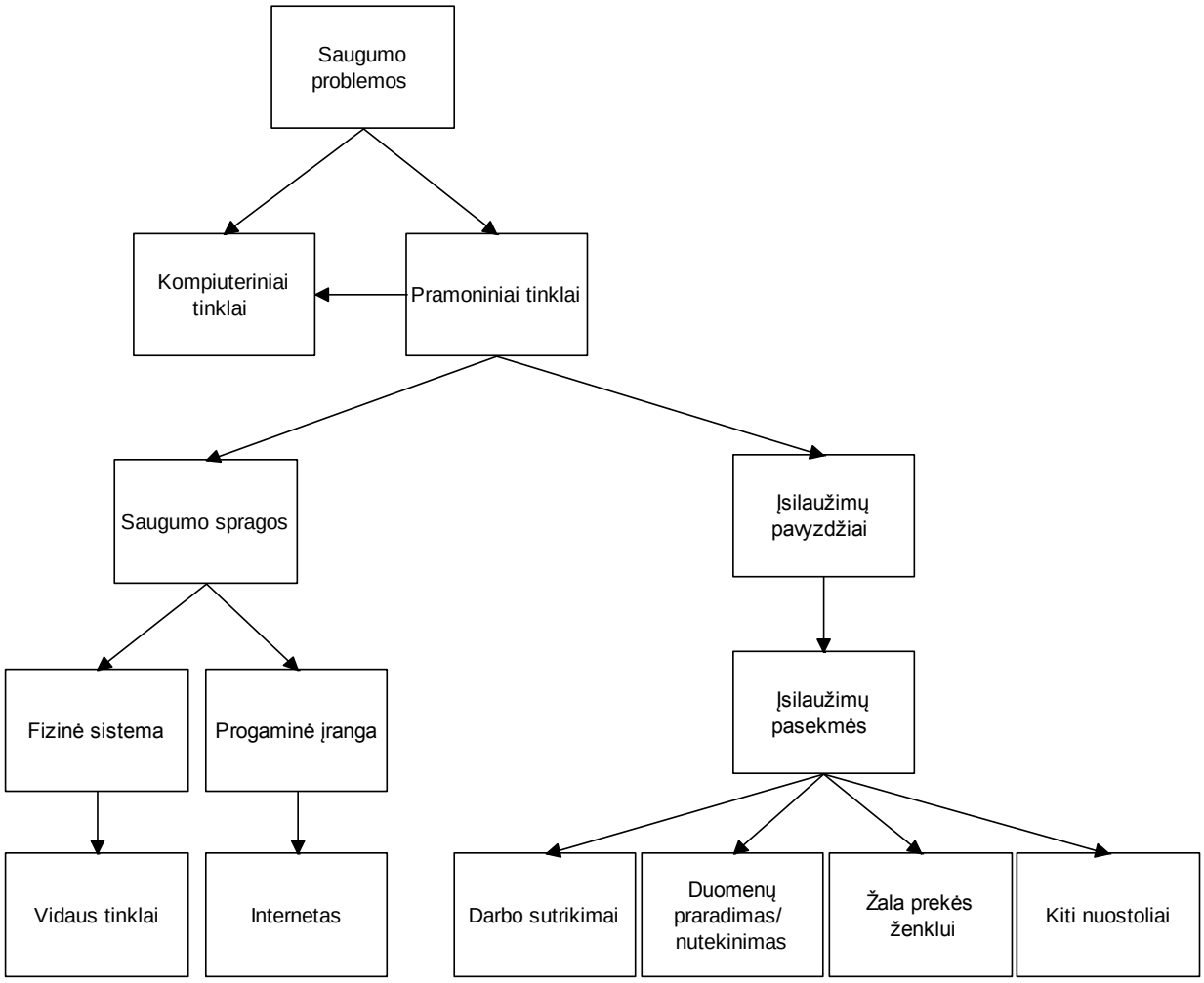
Įvadas

Šiame darbe nagrinėjamos pramoninių kompiuterinių tinklų saugumo problemos ir jų sprendimo būdai. Pagrindinis darbo tikslas – ištirti pramoninių komunikacijų tinklo saugumo užtikrinimo metodus. Tikslui pasiekti iškelti uždaviniai: išanalizuoti ir suklasifikuoti įsilaužimų tipus. Priskirti tipiniams įmonės tinklo mazgams konkrečias saugumo priemones apsaugai nuo įsilaužimo. Pasiūlyti pramoninio tinklo saugumo sistemų pagerinimo rekomendacijas ir sprendimus. Sistemos veiksmingumas vertintas pagal literatūroje pateikiamus duomenis. Ištirti realaus mazgo gaunamų duomenų srautą ir atakų bei apsaugos galimybes. Sumodeliuoti ir patobulinti ugniasienės sistemą. Tinklo saugumo sistemų tyrimui naudota Wireshark programa ir Matlab Simulink programinis paketas. Pirmąja programa analizuota DoS atakų duomenų bazė, taip pat sukaupti ir analizuoti įprasti ir galimai kenksmingi interneto pranešimai. Matlab Simulink paketu sukurtas ugniasienės ir Jungtinės apsaugos sistemos palyginimo metodas (modelis). Patvirtintas pastarojo metodo pranašumas prieš įprastą ugniasienės apsaugą.

1. Pramoninių tinklų saugumo problemos ir pažeidimai

1.1 Komunikacijų tinklų saugumo problemos

Visas tinklo saugumo spragas ir grėsmes galima suskirstyti į kompiuterinį tinklą, šiuo atveju tai įprastos darbo vietos, turinčios tiesioginę prieigą prie interneto ir pramoninį tinklą, dirbantį vietiniame įmonės tinkle. Šiame darbe bus aptarta antroji grėsmių grupė. Struktūra pavaizduota 1 pav. Tai yra išskiriama pramoninių tinklų saugumo spragos, jų tipai, bei bus pateikiama keletas įsilaužimų pavyzdžių. Dažnai kompiuteriniai tinklai tampa pramoninio tinklo dalimi ir sudaro vienas pagrindinių saugumo spragų.



1 pav. Komunikacijų tinklų saugumo problemų skirstymas

1.2 Įsilaužimo į pramonės tinklus pavyzdžiai ir pasekmės

Tinklo saugumo pažeidimas – tai bet kokia veikla tinkle, turinti neigiamas pasekmes saugumui. Tai dažniausiai reiškia, kad veikla pažeidžia aiškią arba numanomą saugaus darbo tvarką. Pažeidimai gali būti vykdomi iš bet kurios tinklo vietos, nors kai kurių tipų pažeidimams būtinas priėjimas prie tam tikrų rūšių sistemų ar specialių vartotojų teisių. Tinklų saugumo pažeidėjai gali būti labai įvairūs asmenys: tai gali būti vaikai, norintys išsiaiškinti, ką jie gali daryti tinkle, jauni programuotojai, sukūrę naują programinę priemonę, asmenys, siekiantys asmeninės naudos, ar net šnipai, ieškantys ekonomiškai naudingos arba kitoms valstybėms reikalingos informacijos. Pažeidėjai taip elgtis gali norėdami pasilinksminti, įrodyti savo sugebėjimus, dėl valdžios jausmo, dėmesio arba finansinės naudos.

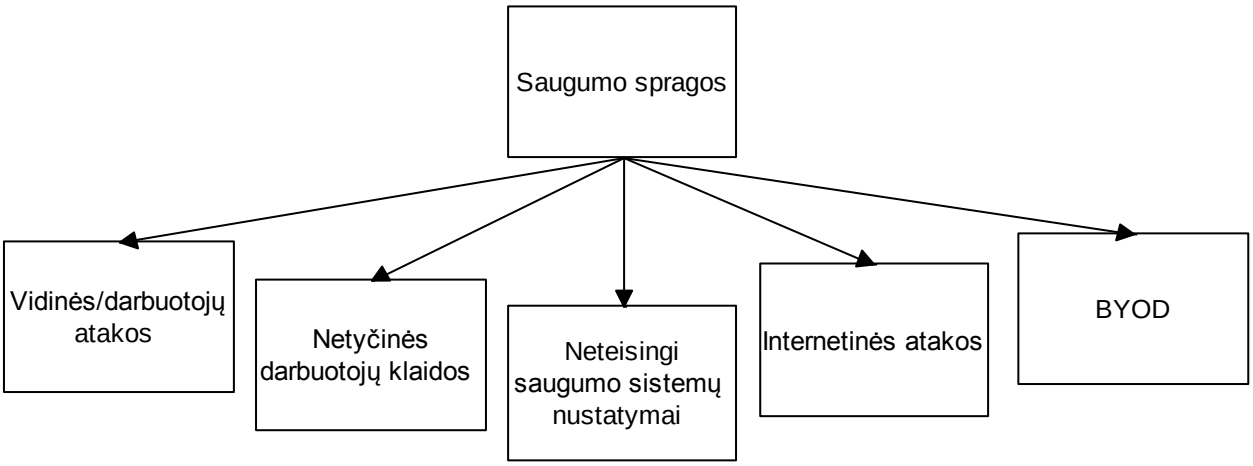
Žemiau pateikta keletas įvairių tipų tokių įsilaužimų į pramonės sistemas.

- 2014 metais buvo kibernetiškai įsilaužta į vieną Vokietijos plieno liejyklą. Užpuolikai perėmė krosnies valdymą, sukeldami incidentus tose vietose, kuriose krosnis negali būti išjungta įprastiniu būdu. Įsilaužėliai turėjo pažangių techninių įgūdžių ne tik IT srityje, bet ir puikiai išmanė pramonės kontrolės sistemas [1].
- 2010 metais Irane, Natanz branduoliniame komplekse urano sodrinimo centrifugos netikėtai sustojo ir ėmė pakartotinai persikrauti. Atlikus patikrą buvo rasta kenksminga programinė įranga, tačiau nepanaši į įprastines kirminų ar virusų formas. Užuot vogusi informaciją ar užgrobusi kompiuterius, ši programinė įranga fiziškai sugadino kompiuterių valdomą įrangą. Ši ataka laikoma pirmuoju pasaulyje skaitmeniniu ginklu. Pažymėtina, kad pats branduolinis kompleksas neturi jokio ryšio su internetu, visgi, buvo užkrėsta penkių, kaip tikėtina, prie šio projekto dirbusių kompanijų flash atmintinės, taip kenksminga programa galėjo patekti į sistemą [2].
- 2014 metų vasario ir gegužės mėnesiais buvo įsilaužta į eBay internetinės parduotuvės sistemą. Buvo paviešinti 233 tūkstančių vartotojų slaptažodžiai. eBay, reaguodama į tai, paskelbė pranešimą, prašydama visus vartotojus pakeisti savo slaptažodžius [3].
- 2014 metų birželio mėnesį dėl komunikacijų kompanijos Feedly užpuolimo DoS ataka, buvo paveikti apie 15 milijonų vartotojų [3].

Dėl įsilaužimo į kompanijos tinklą nuostoliai gali būti intelektinės nuosavybės ir duomenų praradimas, alternatyviosios sąnaudos, įskaitant paslaugų ir darbo sutrikimus, žala prekės ženklui ir reputacijai, baudos ir kompensacijos klientams, atsakomųjų priemonių išlaidos ar draudimas, išlaidos atsigavimui po atakos, konkurencingumo praradimo bei prekybos sutrikimų išlaidos. Kompiuterinės apsaugos kompanijos McAfee duomenimis, kasmet žala, patiriama dėl kibernetinių atakų, siekia iki 300 milijardų JAV dolerių [4].

1.3 Saugumo spragos kompiuteriniuose pramonės tinkluose

Norint sukurti idealią saugumo sistemą, reikia įvertinti kiekvieną galimą individualų saugumo pažeidimą. Kadangi daugeliu atvejų to padaryti fiziškai neįmanoma, nes kenksmingos programos kuriamos ir tobulinamos nuolat, saugumo spragos suskirstomos į tam tikras grupes, kaip pavaizduota 2 pav.



2 pav. Saugumo spragų skirstymas

Norint sukurti patikimą saugumo sistemą, reikia įvertinti kiekvieną galimą individualų saugumo pažeidimą. Kadangi daugeliu atvejų to padaryti fiziškai neįmanoma, nes kenksmingos programos kuriamos ir tobulinamos nuolat, saugumo spragos suskirstomos į tam tikras grupes, kaip pavaizduota 2 pav.. Techniškai paprasčiausias įsilaužimo būdas – tiesiogiai per vidinį tinklą – gali būti atliktas darbuotojo ar kito neteisėtai gavusio prieigą žmogaus. Tačiau nuo to ir apsauga yra gana paprasta, tai yra nereikalingos sudėtingos programos ar algoritmai, tiesiog griežta prieigos kontrolė. Netyčinės darbuotojų klaidos – tai per internetą ar išorinius įrenginius, pavyzdžiui USB raktą plintantys virusai ar kita kenksminga programinė įranga. Neteisingi saugumo sistemų nustatymai gali reikšti neteisingai naudojamą ar (dalinai) atjungtą antivirusinę įrangą ir/ar ugniasienę. Taip pat šiai grupei galima priskirti neteisingą VPN ar kitų saugumo sistemų naudojimą. Kaip ir kiekviena sistema, saugumos sistemos yra veiksmingos tik tinkamai jas pritaikant konkrečiam saugomam tinklui. Sąlygos, leidžiančios vykdyti internetines atakas yra silpnos saugumo sistemos ar jų nebuvimas, kitas atvejis, kai naudojamos saugumo sistemos, tačiau įsilaužimams naudojama galinga įranga, gebanti „nulaužti“ net sudėtingus saugumo sistemų algoritmus.

Penktąją grupę – BYOD (angl. *Bring Your Own Device*), galima priskirti netyčinėms darbuotojų klaidoms, tačiau tai yra santykinai naujas terminas dėl vis kompaktiškesnių ir galingesnių mobilių įrenginių naudojimo tiek darbe, tiek asmeninėms reikmėms. BYOD

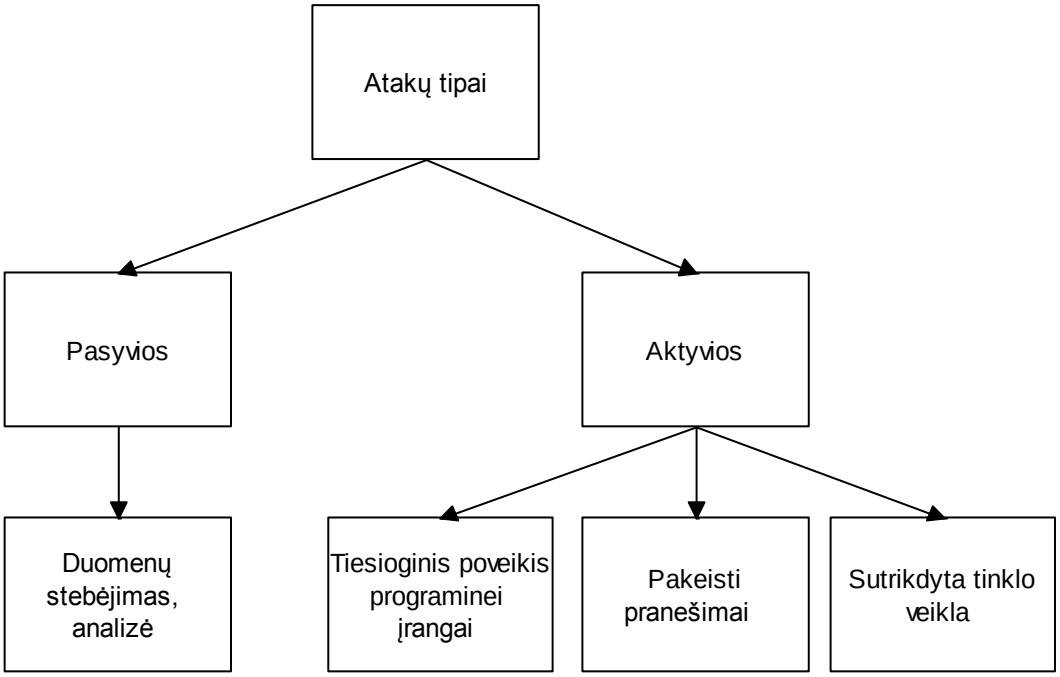
naudojimas suteikia patogumo, palengvina darbo iš namų galimybes, suteikia darbuotojams lankstumo. Tačiau naudojant BYOD, įmonės tinkle atsiranda papildomos saugumo spragos [5].

Identifikacijos ir prieigos kontrolės esmė yra apsaugoti įrenginį, taigi, ir visą sistemą nuo neautorizuoto prisijungimo. Tam naudojami slaptažodžiai, jie turi būti tam tikro, ne mažesnio nei numatyta ilgio, naudojami įvairių tipų simboliai, siekiant apsunkinti atspėjimo galimybę, maksimalus klaidų skaičius vedant slaptažodį. Taip pat slaptažodis turi būti periodiškai keičiamas ir nesikartoti. Be slaptažodžių dar naudojami automatinio užsirakinimo metodai Jei įrenginys tam tikrą laiką nenaudojamas, jis turi būti užrakinamas. Tinklo atskyrimas naudojamas neleisti BYOD įrenginiui vienu metu prisijungti prie keleto tinklų [5].

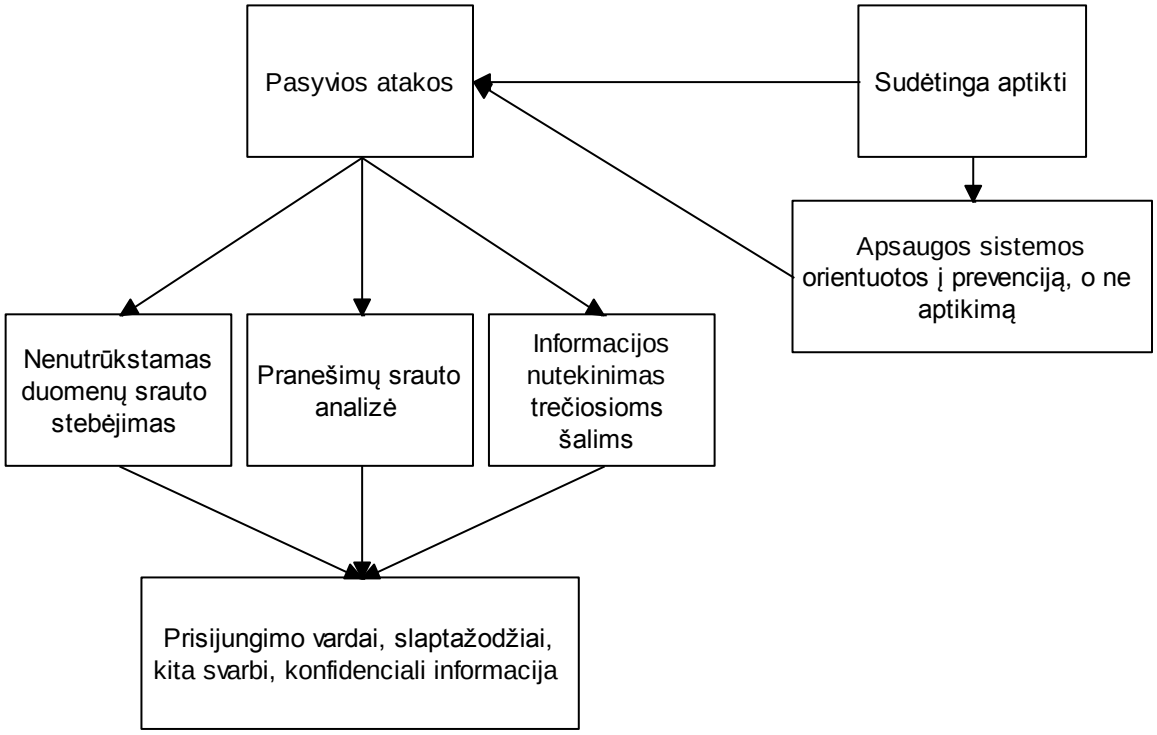
Naudojami saugomų duomenų šifravimo metodai, kad apsaugoti privačius įmonės duomenis, prieinamus per mobilius įrenginius. Labiau kraštutinė priemonė yra automatinis duomenų ištrynimas po tam tikro nesėkmingų prisijungimo bandymų skaičiaus. Žinoma duomenys turi būti saugomi atsarginėje laikmenoje ir reguliariai atnaujinami. Aplikacijų saugumas naudojamas išvengti nepatikimų programų veiklos, siuntimosi, identifikuoti kenksmingas programas.

1.4 Pramoninių tinklų atakų klasifikavimas

Visos kompiuterinių tinklų atakos gali būti suskirstytos į dvi grupes, tai yra į pasyvias ir aktyvias. Pasyviomis atakomis vadinamos tokios atakos, kurios nedaro poveikio vartotojo sistemai, tiktai stebi duomenis, juos kaupia ar siunčia užpuolikui, atlieka duomenų dešifravimą bei analizę. Aktyvia ataka vadinamas tiesioginis įsilaužimo poveikis aukos sistemai. Tai gali būti įdiegta žalinga programinė įranga, pakeičiami siunčiami paketai ar sutrikdomas tinklo darbas. Jei pasyvios atakos metu tinklas gali dirbti įprastu režimu, net nejausdamas atakos reiškinio, tai pasireiškus aktyviai atakai, anksčiau ar vėliau sistema bus išvesta iš rikiuotės. Atstatyti sistemos darbą prireikia tam tikrų investicijų, dėl to aktyvios atakos dažnaiusiai pridaro kur kas didesnių nuostolių, nei pasyvios. Tačiau aktyvias atakas lengviau pastebėti ir užkirsti kelią nuostoliams dėl įsilaužimo. 3 pav. pateiktas detalesnis atakų tipų skirstymas. Toliau šiame skyriuje aprašomi pateiktų atakų požymiai ir savybės.



3 pav. Atakų tipai



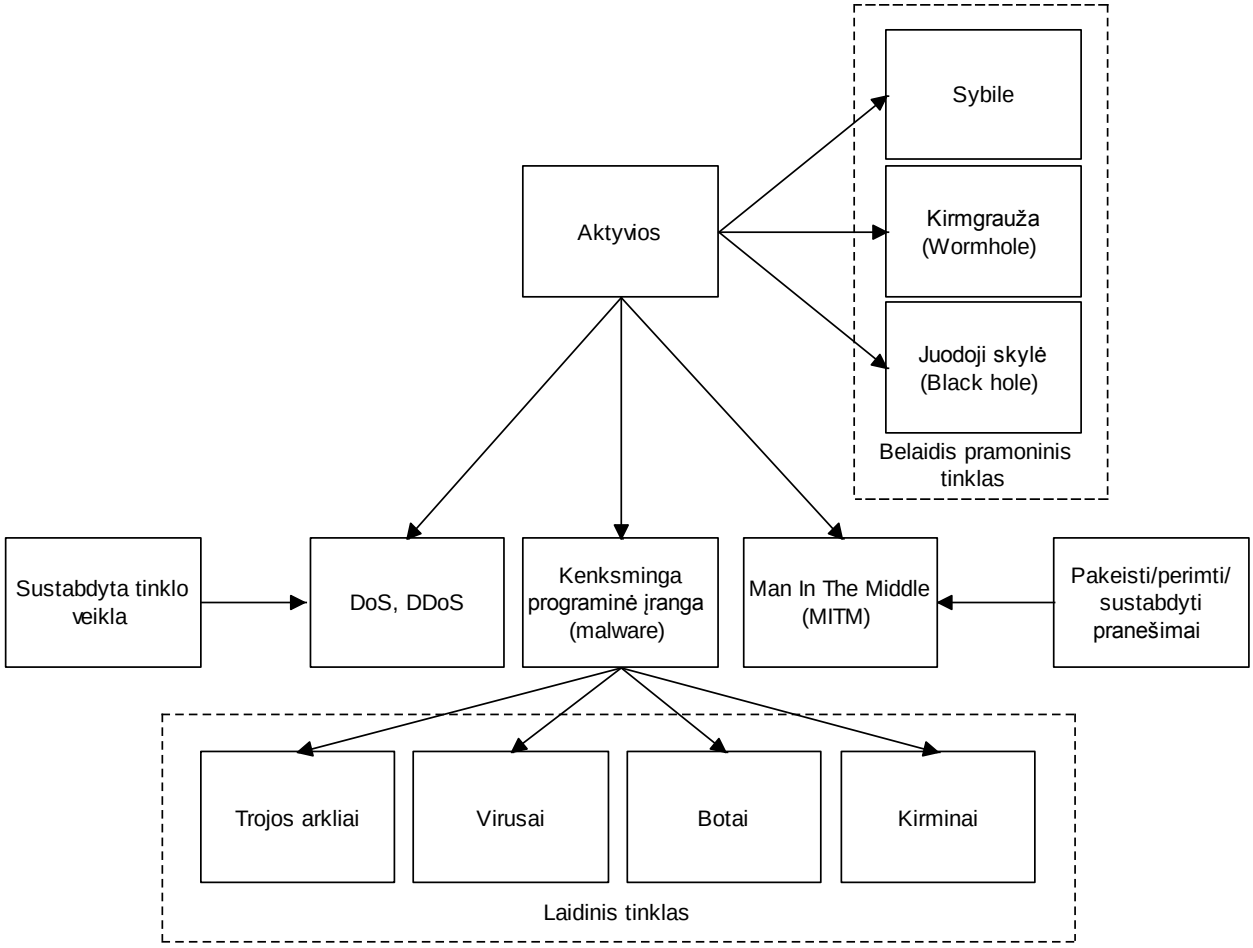
4 pav. Pasyvių atakų savybės

Dažniausiai, kaip parodyta 4 pav. schemoje, pasyvių atakų taikiniai būna prisijungimo vardai ir slaptažodžiai, taip pat svarbi informacija, kuri vėliau gali būti panaudota kito tipo atakose, aktyviose atakose, 5 pav. Jų tipai plačiau aprašyti kitame skyrelyje. Kitas šio tipo atakų pavojus – atskleista konfidenciali įmonės informacija, kaip cheminės formulės, kompiuterinės programos,

valdymo algoritmai, kalbant apie techninę pramonės pusę, bei svarbūs dokumentai, patentai, kalbant apie įmonės valdymą.

Duomenų srauto skenavimui naudojama keletas mechanizmų, besiskiriančių duomenų priėjimo galimybės kokybe ir sudėtingumu [6]:

- Nepriklausomi užpuoliko kontroliuojami mazgai, priimantys siunčiamus duomenis.
- Tam tikrais atvejais srauto stebėjimo įranga gali būti įrengta tame pačiame domene, kaip ir mazgas. Dėl to bus nuskaitomi visi IP paketai iš kitų mazgų su tiksliu laiko žymėjimu. Šie duomenys gali būti siunčiami tiesiai analizės įrangai.
- Įdiegiant neįterptinę skenavimo įrangą tarp mazgų, taip pat skenuojami duomeys, tačiau šiuo atveju prarandamas tikslus laiko žymėjimas dėl nedidelio maršrutizatorių vėlavimo svyravimų.
- Kitas duomenų perėmimo būdas – perkonfigūruojant maršrutizatorių, kad jame būtų atliekamas skenavimas, tačiau čia, labai tikėtina, bus prarastas paketų laiko tikslumas. Tiksliausiai laikas fiksuojamas perimant paketą arčiausiai mazgo.



5 pav. Aktyvių atakų tipai ir savybės

DoS (angl. *Denial of Service*) ir DDoS (angl. *Distributed Denial of Service*) – atakų tipas, kai tinklas užpildomas beverčiais pranešimais. Tokiu atveju, tikrieji pranešimai neišsiunčiami ir negaunami, sustoja visa tinklo, taigi ir sistemos veikla. Tarp minėtų atakų skirtumas tame, kad DoS atveju puolama iš vieno kompiuterio ir naudojamas vienas prisijungimo taškas serverio užpildymui paketais, taip apkraunant pralaidumo juostą ir kitus resursus. DDoS atakos metu, naudojama keletas interneto prieigos taškų, dažnai paplitusių plačiai pasaulyje, tai vadinama botų tinklu (angl. *botnet*). Nuo DDoS atakos daug sunkiau apsiginti, nes nėra vieno užpuoliko, o tinklo užtvindymas paketais gali vykti iš šimtų ara tūkstančių įvairių šaltinių. Norint apsisaugoti suo šio tipo atakos, būtinas greitas aptikimas ir reagavimas. Taigi, pirmasis iššūkis yra identifikuoti įeinantį srautą kaip kenksmingą. Po to įeinantys pranešimai turi būti sugerti lanksčios struktūros gavėjo, kol identifikuojamas ir užblokuojamas atakos šaltinis. Apsaugai nuo DDoS atakų derėtų riboti bandymų prisijungti iš to paties IP skaičių [7].

MITM (angl. *Man In The Middle*) atakos yra atakų tipas, kai tarp dviejų sąveikaujančių šalių įsiterpia trečias asmuo – užpuolikas. Tokiu atveju užpuolikas turi galimybę ne tik perimti siunčiamus pranešimus, bet ir juos keisti, blokuoti ar siųsti naujus, žalingus pranešimus realiu laiku. MITM tipo atakos dažniausiai naudojamos, kai vyksta apsikeitimas viešais raktais (2.3 skyrius), užpuolikas pateikia savo viešą raktą, taip apgaudamas sistemą ir prieidamas prie užšifruotų duomenų. Apsaugai nuo šios atakos naudojami sudėtingi šifro algoritmai tarp serverio ir vartotojo, naudojami skaitmeniniai parašai. Visgi, ši ataka pramonėje nėra plačiai paplitusi, nes čia dažniausiai naudojama ta pati, patikrinta ir saugi interneto prieiga.

Virusai, kirminai, trojos arkliai, arba trojanai, botai, šnipinėjimo programos – visi šie atakų tipai priklauso kenksmingai programinei įrangai (angl. *malware*). Tai yra kodas ar programa, specialiai sukurta siekiant pakenkti, sutrikdyti, vogti ar daryti kitokią žalą tinklui, duomenims ar įrangos veiksmams. Patiriama žala gali svyruoti nuo nedidelių sistemos sudirginimų, kaip iššokantys skelbimi, iki konfidencialios informacijos ar pinigų vagystės, duomenų sunaikinimo ar visiško sistemos ar tinklo išjungimo. Dvi dažniausiai sutinkamos kenksmingos programinės įrangos klasės – virusai ir kirminai. Jie turi savybę skleisti savo kopijas tinkle, netgi šiek tiek modifikuotis, prisitaikyti. Skirtumas tarp jų – kirminai veikia daugiau ar mažiau nepriklausomai nuo kitų failų, o virusai yra priklausomi nuo priimančios programos. Plačiau kenksmingos programinės įrangos klasės aprašytos toliau [8].

Kompiuterinis virusas yra kenkėjiškų programų tipas, kuris sklinda įterpiant savo kopiją ir tampa sistemos dalimi. Jis plinta iš vieno kompiuterio į kitą, palikdamas savo kopiją. Virusai gali skirtis sunkumo lygiu, pagal tai, kokiu padarinius jie sukelia. Beveik visi virusai turi vykdomąjį (.exe) failą, tai reiškia, kad virusas gali egzistuoti sistemoje, bet būti neaktyviu ir neplisti, kol vartotojas neatidarys to kenksmingo failo ar programos. Kai kodas paleidžiamas, kenksmingas

kodas taip pat vykdomas. Paprastai priimančioji programa veikia toliau, net kai virusas paskleistas. Tačiau yra tokių virusų, kurie perrašo programos kodą, taip naikindami pačią programą. Virusai plinta kai užkrėsta programinė įranga ar dokumentai perkeliami iš vieno kompiuterio į kitą.

Kompiuteriniai kirminai yra panašūs į virusus tuo, kad jie skleidžia savo kopijas ir gali sukelti tą pačią žalą. Tačiau, skirtingai nuo virusų, jie veikia kaip atskira programa ir jiems nereikia kitos programos ar vartotojo pagalbos plitimui. Kirminai naudojasi sistemos silpnomis vietomis duomenų mainų sistemoje, tai leidžia jiems plisti be išorinės pagalbos.

Trojanai yra teisėtos programos kenksminga dalis. Paprastai vartotojai apgaule verčiami įsirašyti šią kenksmingą programą į savo sistemą. Kai trojanas aktyvuojamas, jis gali rengti neribotą skaičių atakų iš vidaus. Taip pat žinoma atvejų, kai sukuriamas priėjimas neuatorizuotiems vartotojams prie sistemos. Skirtingai nuo virusų ir kirminų, trojanai nesidaugina sistemoje. Jie plinta per vartotoją – jam atidarius elektronį laišką ar gavus failą.

Botai yra automatizuotas procesas, kuris sąveikauja su kitais tinklais. Botai atlieka užduotis, kurias kitu atveju atliktų žmogus. Tipiškas naudojimas yra rinkti informaciją ar automatiškai bendrauti su klientais. Kenkėjiški botai savarankiškai dauginasi užkrėsdami kompiuterį, prisijungdami prie infekuotų įrenginių tinklo, kuris veikia kaip vienas valdymo centras, taip pat vykdo kito tipo atakas. Kaip ir kirminai, botai, botų tinklai geba daugintis, taip pat prisijungti prie sistemos, vesti slaptažodžius, rinkti ir analizuoti informaciją, vykdyti DoS atakas, sukurti prieigą prie infekuoto kompiuterio.

Sybil (angl.) ataka būdinga belaidžiam jutiklių tinklui pramonėje. Sybil ataka vadinamas saugumo pažeidimas, kai mazgas neleistinai įgyja dvi tapatybes. Tai sukelia maršrutizavimo, resursų paskirstymo problemų, neteisingai nustatoma būsena. Tiesioginio ryšio atveju, mazgas siunčia duomenis Sybil užkrėstam mazgui, taigi, duomenys perimami. Taip pat įsilaužėlis gali siųsti duomenis iš Sybil mazgo. Netiesioginio ryšio atveju, joks sveikas mazgas tiesiogiai nekomunikuoja su Sybil mazgu, tačiau pranešimai siunčiami per tarpinius sveikus mazgus, kurie leidžia keistis duomenimis Sybil mazgui ir kitiems sveikiems mazgams. Sybil mazgai tapatybę gali gauti dviem atvejais: sufabrikuoti naują arba pavogti tapatybę iš sveiko mazgo. Pavyzdžiui, jei kiekvienas mazgas identifikuojamas 32 bitų integer kodu, įsilaužėlis gali suteikti atsitiktinę 32 bitų vertės kodo reikšmę sufabrikuotam mazgui. Jei į tinklą negalima įtraukti naujų mazgų, įsilaužėlis turi atjungti legalų mazgą tam, kad jo kodu galėtų pats prisijungti. Susijęs atvejis yra, kai tas pats mazgo kodas naudojamas daug kartų daugelyje tinklo vietų. Apsaugai nuo to naudojama mazgų vietos paieška ir registracija. Apsisaugoti nuo Sybil atakų naudojami metodai susiejant konkretų mazgo kodą su konkrečiu fiziniu mazgu. Yra du būdai patvirtinti tapatybę. Pirmasis, kai mazgas tiesiogiai tikrina kito mazgo tapatybę. Antrasis, netiesioginis, kuriame jau patvirtinti mazgai gali patvirtinti ar paneigti kitus mazgus. [12]

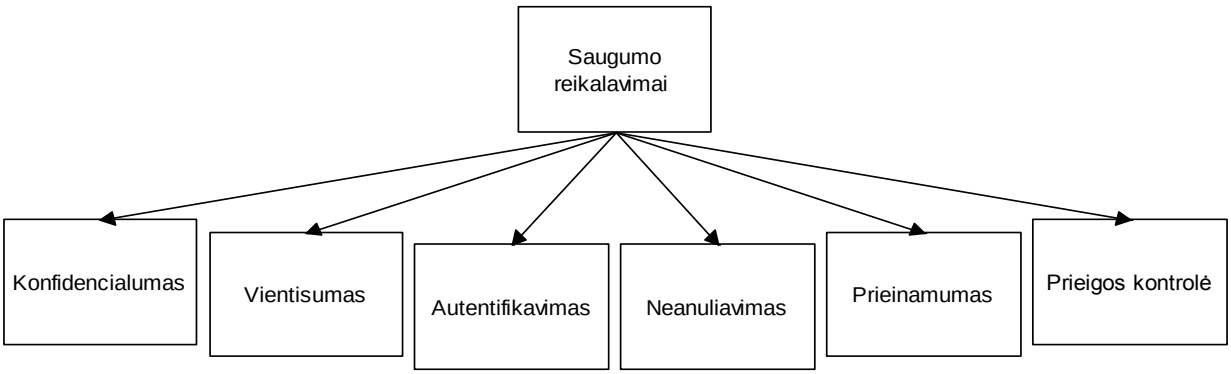
Dar viena ataka būdinga belaidžiam pramonės tinklui – kirmgrauža (angl. *wormhole*). Šio tipo ataka yra sukurtas netikras ryšio tunelis, prie kurio turi priėjimą įsilaužėlis. Aptikti tokį tunelį yra sudėtinga, nes kenksmingi mazgai geba apsimesti įprastais. Prevencijai naudojami įvairūs metodai. Vienas jų, siunčiant pranešimą, nurodoma tiksli siuntėjo pozicija ar laikas, siekiant apriboti maksimalų galimą perdavimo atstumą. Taip pat galima nustatyti tikslias mazgų pozicijas, taip užkertant kelią informacijos perdavimui kitais tuneliais. Kryptinės antenos taip pat gali sumažinti kirmgraužos atakos tikimybę. Visiems minėtiems metodams reikalinga papildoma įranga. Tačiau šie metodai neaptinka kirmgraužos tunelio, tik apsunkina galimybę jį realizuoti. [13]

Taip pat belaidžiams pramonės tinklams būdinga ataka – juodoji skylė (angl. *blackhole*). Juodosios skylės atakos metu užkrėstas mazgas traukia visus tinkle esančius duomenis į save. Šio tipo mazgas gali įsiterpti net tarp toli nuo jo esančių kitų mazgų ir stebėti transliuojamus duomenis. Šiam pažeidimui aptikti ir nuo jo apsisaugoti naudojami įvairūs metodai. Duomenų nuoseklumo ir tinklo srauto metodas įtraukia centrinę stotį į aptikimo procesą. Iš centrinės stoties išsiunčiami užklausos pranešimai, reikalaujantys atsakymo su mazgo ID. Gavus atgalinius signalus, centrinė stotis sudaro tinklo srauto grafą, iš kurio galima identifikuoti juodąją skylę. Kitas metodas – priimto signalo stiprumo matavimas (RSSI). Šiuo atveju reikalingi papildoma monitoringo įranga. Pagal gautus signalus nustatoma mazgų pozicija, kai centrinės stoties koordinatės laikomos atskaitos pradžia. Ši informacija naudojama kaip svoriai aptikti juodosios skylės ataką. Pažeidimą aptikti taip pat galima matuojant CPU apkrovą. Matuojant kiekvieno mazgo CPU apkrovą fiksuotais laiko intervalais, centrinė stotis skaičiuoja skirtumą tarp apkrovų. Apskaičiavus skirtumą, centrinė stotis gali nustatyti ar mazgas yra užkrėstas. Taip pat juodųjų skylių aptikimui naudojamas mobilių agentų metodas. Šiuo atveju, tinkle paleidžiama programa, tinkle ne tik pernešanti informaciją, bet ir atliekanti skaičiavimus. Ryšio algoritmas paremtas mobiliais agentais. Jie naudojami surinkti informacijai iš visų mazgų ir užkerta kelią žalingų mazgų perduodamai informacijai. Šiuo atveju nereikalingas šifravimo-dešifravimo mechanizmas juodųjų skylių aptikimui. [14]

2. Pramoninių tinklų saugumo sistemos

2.1 Reikalavimai pramoninių tinklų saugumo sistemoms

Ankstesniuose skyriuse aprašytos pramonėje naudojamų tinklų saugumo problemos, įsilaužimo galimybės ir įsilaužimų tipai. Šiame skyriuje pateikiami reikalavimai saugiam tinklo darbui ir užduotys, skirtos tinklų saugumo sistemoms.



6 pav. Saugumo reikalavimai, keliami pramonės tinklų sistemoms

Saugumo reikalavimai, keliami pramonės sistemoms [9], 6 pav.:

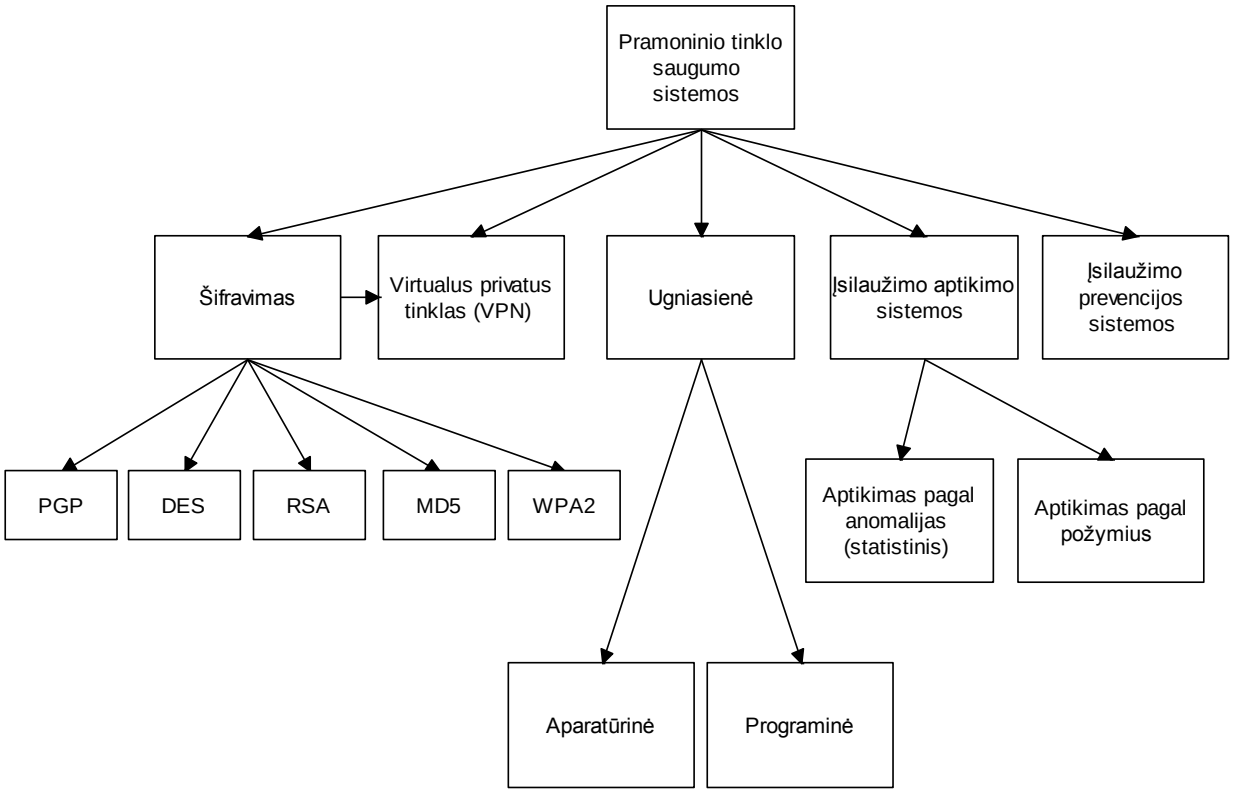
- Konfidencialumas – apsauga nuo duomenų atskleidimo pašaliniams asmenims;
- Vientisumas – duomenų nuoseklumo palaikymas;
- Autentifikavimas – autorizuotų vartotojų atpažinimas ir sklandaus darbo užtikrinimas;
- Neanuliavimas – originalių ryšių (komunikacijų) išlaikymas
- Prieinamumas – tesėti vartotojai turi turėti prieigą, kai ji reikalinga
- Prieigos kontrolė – neautorizuoti vartotojai neprijungiami

Informacijos apsaugai yra naudojama ISO 27000 standartų grupė. Ji pateikia informacijos saugumo valdymo sistemų apžvalgą ir apibrėžia susijusius terminus.

ISO/IEC 27001 – Standartas, aprašantis reikalavimus informacijos technologijoms, Saugumo technikai, informacijos saugumo valdymo sistemoms. Šis tarptautinis standartas nurodo nustatymo, įgyvendinimo, veikimo, stebėjimo, peržiūros, palaikymo ir formalaus informacijos saugumo valdymo sistemų gerinimo, reikalavimus. ISO/IEC 27006 Informacijos technologijos – Saugumo technika – Reikalavimai keliami įstaigoms atliekančioms auditą ir informacijos saugumo valdymo sistemų sertifikavimą.

2.2 Duomenų apsaugos technologijos ir prevencijos priemonės

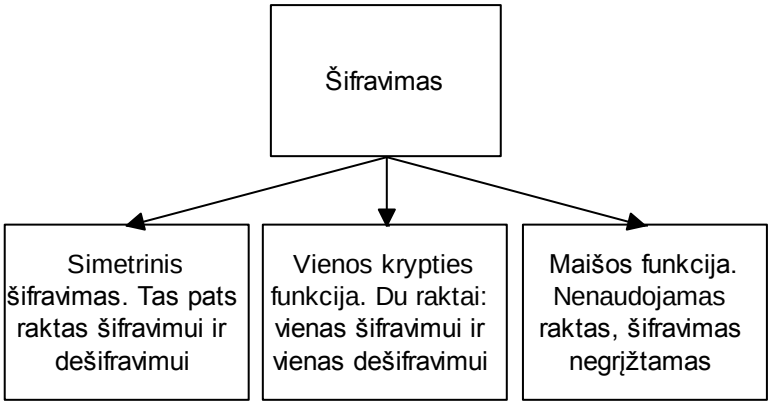
7 pav. pavaizduota pramoninio tinklo saugumo sistemų suskirstymo schema. Kiekviena sistema plačiau aprašyta tolesniuose skyriuose.



7 pav. Pramoninių tinklų saugumo sistemų klasifikacija

2.3 Pranešimų šifravimo metodai

Kadangi informacija siunčiama nesaugiais kanalais, pavyzdžiui, internetu, reikia užtikrinti, kad siuntėjui išsiuntus informaciją, jos negalėtų perskaityti niekas kitas, tiktai gavėjas, kuriam informacija yra skirta. Tai pasiekiama informaciją šifruojant. Reikia užtikrinti, kad siunčiamų duomenų nebūtų įmanoma suklastoti ar pakeisti. Dažniausiai tam pasitelkiamos specialios santraukos funkcijos, kurios iš turimų duomenų sugeneruoja duomenis atitinkančią santraukos reikšmę. Siuntėjas kartu su pranešimu išsiunčia ir santrauką. Jei gavėjas, panaudojęs tą patį santraukos algoritmą, gauna skirtingą reikšmę, galima tvirtinti, kad duomenys pakeliui buvo pakeisti. Gavėjui, priėmusiam informaciją, būtina įsitikinti siuntėjo autentiškumu. Vienas autentifikavimo metodų – elektroninis parašas. Šifravimo tipai pateikti 8 pav.



8 pav. Šifravimo tipai

SSL (angl. *Secure Sockets Layer*) ir TLS (angl. *Transport Layer Security*)

PGP (angl. *Pretty Good Privacy*) – vienas populiariausių ir stipriausių šifravimo algoritmų. Šifravimo algoritmas, tai matematinė funkcija naudojama šifravimo ir dešifravimo procese. Algoritmo veikimui reikalingas slaptažodis. Slaptažodis gali buti žodis, numeris, frazė, įvairūs simboliai. Tas pats tekstas užšifruotas skirtingais slaptažodžiais skirsis vienas nuo kito. Taigi viso užšifruoto teksto saugumas priklausys nuo pasirinkto algoritmo ir slaptažodžio slaptumo. Viešojo rakto šifravimas paremtas tuo, kad yra sudaromi du raktai – viešas (naudojamas duomenims užšifruoti) ir privatus (naudojamas duomenims dešifruoti). Taigi, viešas raktas duodamas siuntėjui, bet kam, o privatus laikomas saugiai padėtas (pvz.: diske, CD-ROM ir t.t.). Siuntėjas, pasinaudojęs viešuoju raktu užšifruos duomenis, kuriuos dešifruoti galės tik konkretus gavėjas (pasinaudodamas savo privačiu raktu). Prieš šifruodama duomenis PGP programa suspaudžia (suarchivuoja) tekstą. Tai duoda nemažą pliusą saugumui: dauguma šifroanalizių panaudoja iškarpų sutapimą duomenų dešifravimui. Archivuojant tekstą jis šiek tiek iškraipomas, taip sumažinant galimybę sėkmingai panaudoti tokią ataką. Rakto stiprumas dar priklauso nuo jo dydžio. Dydis matuojamas bitais. Pvz.: 1028 bitų dydžio raktas laikomas labai dideliu. Viešojo rakto šifravime kuo ilgesnis raktas, tuo saugesni duomenys. Viešasis ir privatus raktai yra matematiškai susije. Nustatyti privatų raktą turint tik viešąjį yra sudėtinga, tačiau, tai įmanoma skyrus pakankamai laiko ir skaičiavimo resursų. Taip pat reikia numatyti kas norės perskaityti siunčiamus duomenis, ar labai jie tam pasiryžę, kiek laiko jie turi ir maždaug kokius resursus jie gali panaudoti. Raktai yra užšifruoti ir saugomi dvejuose failuose. Šie failai vadinami viešas žiedas raktams (angl. *public keyring*) ir privatus žiedas raktams (angl. *private keyring*). Į viešą žiedą raktams galima dėti įvairių įmonių/žmonių viešuosius raktus. O į privatų žiedą - tik savo paties privačius raktus. Praradus savo privatų žiedą, nebegalima dešifruoti net autorizuotam vartotojui skirto pranešimo.

DES (angl. *Data Encryption Standart*) duomenų kodavimo standartas sukurtas JAV vyriausybės 1977 metais. Tai blokinio tipo šifravimas, kuriame 64 bitų duomenų blokai užšifruojami naudojant 56 bitų privatų raktą. DES algoritmas naudojamas daugumoje programų. Naudojamas vyriausybiniuose bei privačiuose sektoriuose. Šifruojant daugiau nei 64 bitus yra naudojami keturi oficialūs metodai:

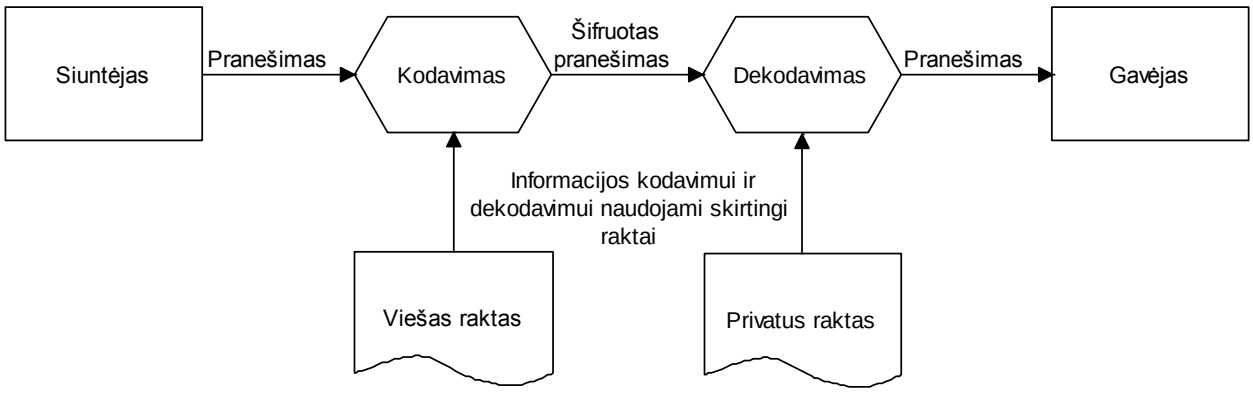
- Elektroninė kodų knyga (angl. *Electronic Codebook*) – ECB
- Šifro blokų grandinės (anlg. *Cipher Block Chaining*) – CBC
- Išvesties atsakomoji reakcija (angl. *Output Feedback*) – OFB
- Šifro atsakomoji reakcija (angl. *Cipher Feedback*) – CFB

DES algortimas taip pat gali būti naudojamas iki 64 bitų kontrolės sumoms sudaryti [16].

RSA yra viešojo rakto tipo kriptosistema, kuri palaiko duomenų šifravimą ir skaitmeninius parašus [16].

MD5 ima fiksuoto dydžio žinutę ir išveda 128 bitų "pirštų antspaudą". Naudojamas viešojo rakto kriptosistemose skaitmeniniams parašams daryti [16].

Viešojo rakto kodavimo (dar vadimama asimetrine kriptografija) schema pavaizduota 9 pav. Pranešimas, užkoduotas viešuoju raktu, gali būti atkoduotas tik turint privatų raktą. Taip pat ir pranešimas, užkoduotas privačiu raktu, atkoduojamas viešuoju raktu.



9 pav. Viešojo rakto šifravimas

Steganografija paslepia ne pranešimo turinį, o patį siunčiamą pranešimą. Tai yra menas paslėpti pranešimą, įliejant jį į multimedijos duomenis (paveikslus, garsą, vaizdą, ir t.t.). Steganografijos pagrindas yra pakeisti nešiklį į nepastebimus duomenis, dėl to, kad atrodo įprastai. Tai paslepia egzistuojantį kanalą, ar patį siuntimo faktą. Tačiau pramonėje jutiklių tinklai nėra tiesiogiai susiję su multimedijos duomenimis, tad sudėtinga pranešimus įkomponuoti į labiau įprastus informacijos nešiklius. [17]

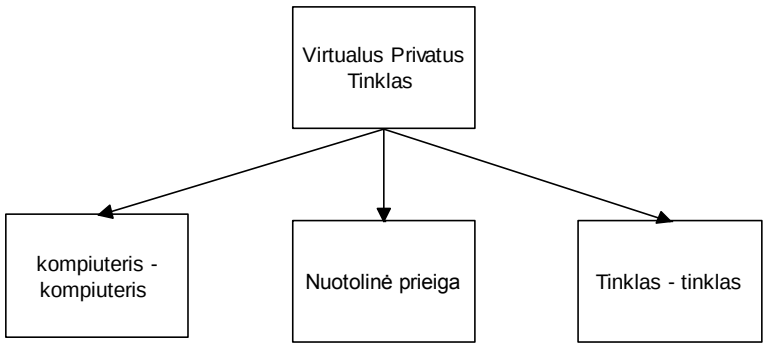
WPA2 (angl. *Wi-Fi Protected Access II*) yra saugumo protokolas, pakeitęs senesnį WPA, kuris pakeitė prieš tai buvusį WEP. WPA2 standartą sudaro dvi dedamosios, kodavimas ir

autentifikacija. WPA2 naudoja AES (angl. *Advanced Encryption Standart*), 128 bit, tačiau palaiko ir TKIP (angl. *Temporal Key Integrity Protocol*), 128 bit. Autentifikacijos dalis turi du režimus, asmeninį ir įmonės. Asmeninis režimas reikalauja PSK (angl. *Pre-Shared Key*), tačiau nereikalauja atskiro vartotojų autentifikavimo. Įmonės režimas, kuris reikalauja atskiro vartotojų autentifikavimo, pagrįstas IEEE 802.1X standartu [21]

2.4 Virtualaus privataus tinklo sistemos

Virtualus privatus tinklas (VPN – angl. *Virtual Private Network*) padeda saugiai pasiekti įmonės tinklą per internetą. To gali prireikti valdymo tiklsais, prieiti prie duomenų ar kitais sumetimais. Iš esmės VPN yra duomenų šifravimo algoritmas, kai šifro raktą turi tik siuntėjas ir gavėjas. Neturint rakto, net ir perėmus duomenis jie bus nesuprantami, beverčiai. Taip pat ir su gautais duomenimis, jei jie bus neužšifruoti būtent tuo raktu, kokį naudoja siuntėjas, gavėjas pranešimą tiesiog ignoruos. Yra keletas VPN tipų, 10 pav. [18]:

- Kompiuteris – kompiuteris (angl. *PC-to-PC*) VPN – paprasčiausias VPN tinklas kai sujungiami du kompiuteriai. Naudojamas kai tinkle tik keli kompiuteriai, jungiami per VPN. Šiuo atveju VPN įrašomas visuose kompiuteriuose, kuriuos reikia sujungti.
- Nuotolinės prieigos (angl. *Remote Access*) VPN – pramonėje dažniau sutinkamas reiškinys, kai nutolęs įrenginys jungiamas prie tinklo fizinio sluoksnio, t.y. prisijungiama iškart prie keleto įrenginių, kurie sujungti į bendrą LAN (*Local Area Network*) tinklą. Šiuo atveju, per VPN prijungta įrenginys veikia lyg būtų tiesiai pajungtas į LAN tinklą.
- Tinklas – tinklas (angl. *LAN-to-LAN*) VPN. Kap pavadinimas pasako, šiuo atveju sujungiami du nutolę LAN tinklai į bendrą tinklą. Naudojant papildomą programinę įrangą galima sujungti daugiau nei 2 tinklus.



10 pav. Virtualaus privataus tinklo tipai

VPN naudoja vieną šių šifravimo protokolų [8]:

- IPsec – *Internet Protocol Security* (angl.) naudoja du šifro modelius: tunelio, kuris šifruoja antraštę ir paketo turinį, ir transportinį, kuris šifruoja tik turinį. Šis metodas palaiko 56 bitų ir 168 bitų šifravimą.
- PPTP/MPPE – palaiko 40 bitų ir 128 bitų šifravimą, naudojamas *Microsoft Point-to-Ponit* (angl.) šifravimas.
- L2TP/IPsec – naudoja antro lygmens IPsec tunelio šifravimą.

2.5 Ugniasienės tinklo apsaugai

Ugniasienės paskirtis filtruoti praeinančius duomenis ir leisti arba riboti vartotojų prisijungimą. Būtina pasirinkti tinkamą ugniasienę turimai sistemai, atsižvelgiant į įmonės dydį, interneto galimybes bei reikalaujamą saugumo lygį. Taip pat ugniasienė neturi trukdyti įprastai įmonės veiklai. Didelėms sistemoms apsaugoti galima naudoti hierarchinius lygmenis, šablonus, sistemą padalinti į keletą mažesnių, taip padidinant tiek ugniasienės, tiek viso tinklo efektyvumą.

Ugniasienės priemonės yra mechanizmas, naudojamas apsaugoti patikimą tinklą nuo nepatikimo. Paprastai, yra nagrinėjami du tinklai: organizacijos vidinis tinklas (patikimas) ir internetas (nepatikimas). Ugniasienės priemonės yra skirtos internetui, kuris komunikacijoms naudoja TCP/IP protokolą.

Programinio lygio saugumas gali būti naudojamas apsaugoti slaptiems duomenims globaliame tinkle, kuris leidžia nuo kiekvieno tinklo jame prisijunti prie kito (tinklų izoliavimas ugniasienės priemonių pagalba labai žymiai sumažina atsiradusį rizikos faktorių), ugniasienės priemonės gali pastebimai sumažinti vidinio pralaužimo grėsmę, t.y. autorizuotų vartotojų neautorizuotą prisijungimą. Tai problema, kuri visada aukščiau išorinio įsilaužimo visose informacijos slaptumo apžvalgose [11].

Pramoniniuose tinkluose apsaugai nuo nepageidaujamų neautorizuotų prisijungimų bei įvairių tipų virusų naudojama ugniasienių įranga. Pagrindiniai skirtumai tarp programinės ir aparatūrinės ugniasienių įrangos pateikti 1 lentelėje. Programinės ugniasienės rekomenduojamos daugiausia namų vartotojams ar nedidelėms įmonėms dėl paprasto naudojimo ir nedidelė kainos. Aparatūrinės įrangos ugniasienės dideliems tinklams pasirenkamos, nes gali saugoti didesnį įrangos kiekį, taip pat dėl didesnio duomenų pralaidumo ir geresnio saugumo užtikrinimo.

Lentelė 1 Programinės ir aparatūrinės ugniasienių skirtumai

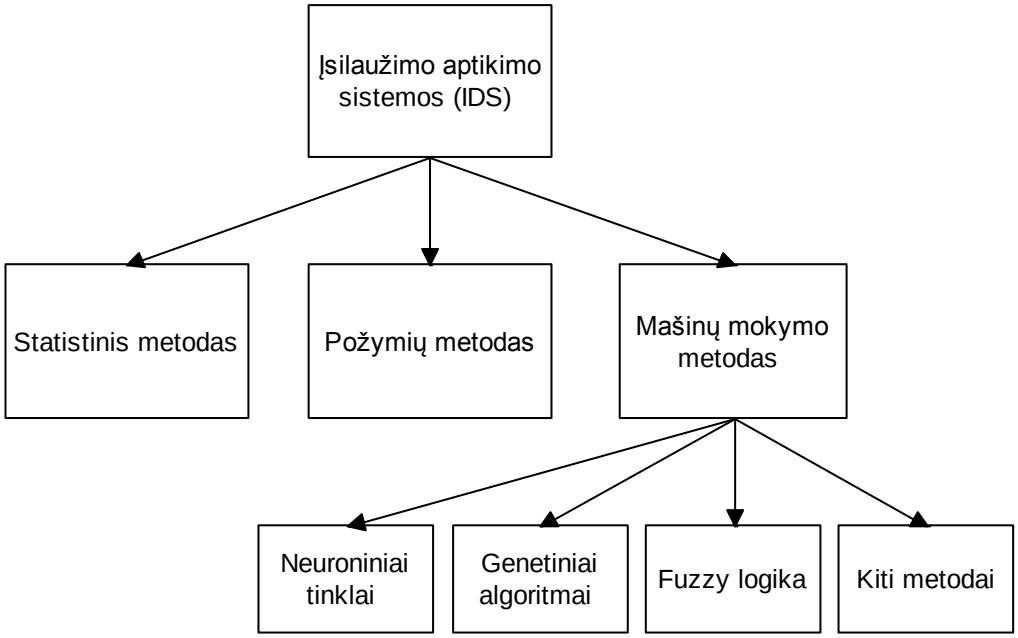
Programinė ugniasienė	Aparatūrinė ugniasienė
Pigesnė ir lankstesnė įranga	Brangesnė įranga
Lengviau įrašyti ir konfigūruoti	Sudėtingesnis konfigūravimas, tačiau ne visada būtinas
Dažnai ribojamas duomenų pralaidumas	Didelis duomenų pralaidumas
Būtina pasirinkti tokią ugniasienę, kurią palaiko naudojama programinė įranga	Mažiau pažeidžiama, nes tai atskiras įrenginys, konfigūruojamas išoriškai
Yra atviro kodo programinė ugniasienių įranga	Neapkrauna saugomos įrangos procesoriaus

2.6 Įsilaužimo aptikimo sistemos tinklo apsaugai

Įsilaužimo aptikimo sistemos (IDS – angl. *Intrusion Detection System*) naudojamos aptikti priešiškiems veiksmams tinklo atžvilgiu. Tipai pavaizduoti 11 paveiksle. Naudojamos dvi pagrindinės technologijos. Pirmoji tiria saugumo klausimus, susijusius su nukrypimais nuo įprastos vartotojų elgsenos (statistinis metodas). Antroji atpažįsta įsilaužimams būdingus požymius. Rečiau sutinkamas metodas – mašinų mokymo. Visų trijų metodų pagrindiniai privalumai ir trūkumai pateikti 2 lentelėje [22].

Statistiniame metode analizuojami tinklu siunčiami pranešimai, tinklo aktyvumas, prisijungimų skaičius, IP adresai, įvykus ženkliasniam nuokrypiui (jis gali būti nustatomas), detektuojama neįprasta veikla, kas gali reikšti įsilaužimą į tinklą. Naudojant požymių metodą ieškoma iš anksto nustatytų specifikacijų. Mašinų mokymo metodas apjungia prieš tai minėtus metodus, analizuoja žinomus atakų požymius ir kuria taisykles kitoms atakoms aptikti.

IDS privalumai yra galimybė atsekti vartotojo veiklą iki galimo įsilaužimo, taip tiksliai nustatnt aliarmo priežastį ir parenkant kovos būdą. Taip pat IDS atpažįsta ir praneša apie duomenų pakitimus, toliau seka priežasties aiškinimasis. Internete ieškomos naujausios atakos, taip apsisaugant nuo jų. IDS gali aptikti sistemos konfigūracijos klaidas ir, žinoma, aptikti, kad sistema yra puolama.

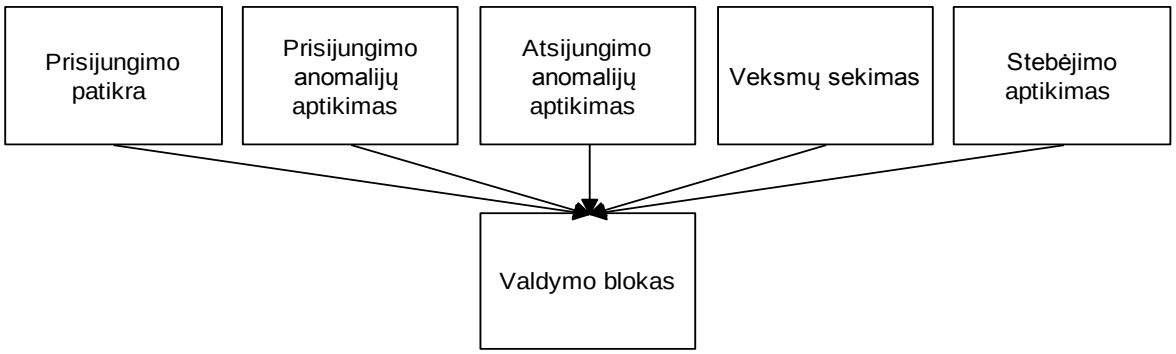


11 pav. IDS tipai

Lentelė 2 Skirtingų įsilaužimo aptikimo sistemų privalumai ir trūkumai

Metodas	Privalumai	Trūkumai
Statistinis	Tikslus kenksmingos atakos aptikimas	Sudėtingas parametrų nustatymas, nerealistinė pusiau stacionaraus proceso prielaida
Požymių	Atsparumas, lankstumas	Sudėtingas, reikalauja daug laiko, aukštos kokybės duomenų
Mašinų mokymo	Lankstumas, pritaikomumas	Priklausomybė nuo sistemos elgsenos, reikalauja daug išteklių

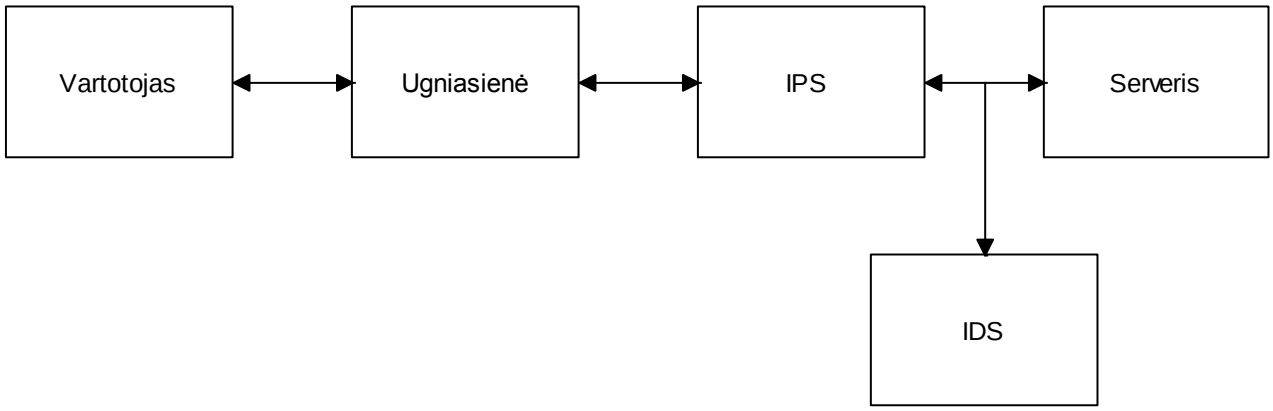
12 pav. pateikiama IDS sistemų veikimo schema. Prisijungimo patikros, prisijungimo anomalijų aptikimo, atsijungimo anomalijų aptikimo, veiksmų sekimo, stebėjimo aptikimo blokai siunčia informaciją centriniam valdymo blokui, kuris reaguoja į galimus įsilaužimo atvejus ir priima tolesnius sprendimus. [19]



12 pav. Tipinės IDS sistemos schema

2.7 Įsilaužimo prevencijos sistemos tinklo apsaugai

Įsilaužimo prevencijos sistema (IPS – angl. *Intrusion Prevention System*) skirta aptikti įsilaužimo į tinklą ar sistemą požymius ir atlikti reikiamus veiksmus. Tai gali būti įspėjimai ir/ar aktyvus įsilaužimų blokavimas. Skirtingai nei ugniasienė, IPS pranešimų neskenuoja, tik blokuoja galimai įsilaužimo pranešimus. Skirtumas tarp IDS ir IPS yra tas, kad pastaroji sistema yra tiesioginiame pranešimų kelyje (kaip ir ugniasienė), kai tuo tarpu IDS atlieka pranešimų stebėjimą iš šalies. Struktūrinė šių sistemų schema pavaizduota 13 pav.



13 pav. Ugniasienės, IPS ir IDS sistemų vieta tinkle

IPS sistema turi būti nuolat atnaujinama, į duomenų bazę įtraukiant naujas grėsmes (įsilaužimo būdus, rizikas), dėl to būtinas pastovus apsaugos sistemosgamintojo palaikymas. Apie įrangą plačiau 2.8 skyriuje.

Skirtingų IPS/IDS sistemų tipų privalumai/trūkumai pateikti 3 lentelėje.

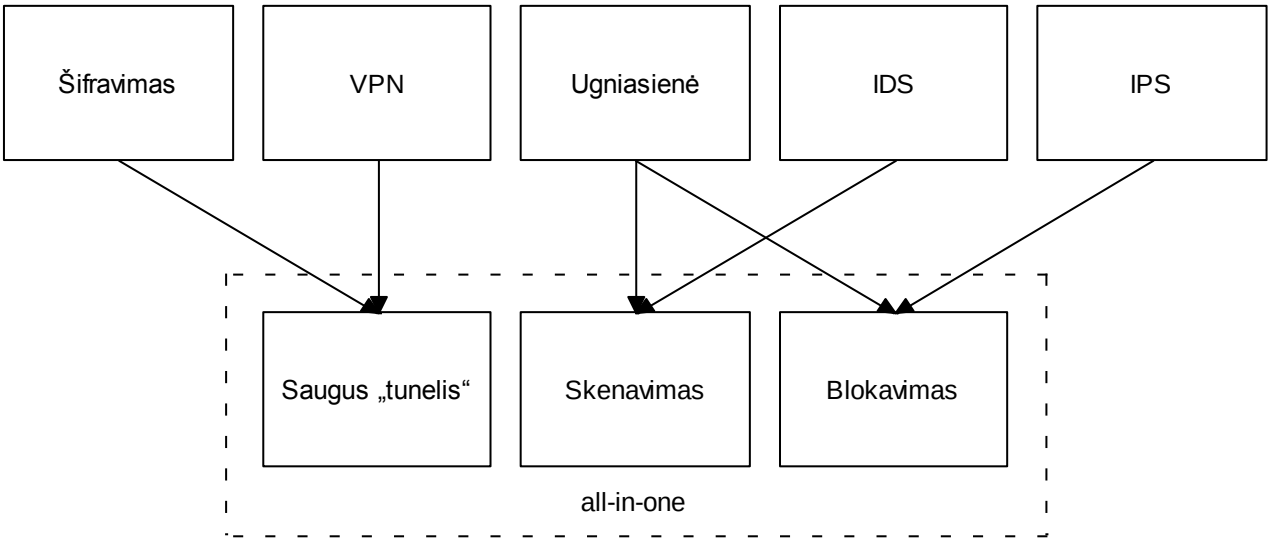
Lentelė 3 Skirtingų IPS/IDS sistemų tipų privalumai ir trūkumai

IPS/IDS metodas	Charakteristikos/privalumai	Apribojimai/trūkumai
Požymiais grįsta detekcija	• Aptinka įsibrovimą pagal iš anksto žinomus modelius • Aukštas aptikimo tikslumas • Maži skaičiavimo resursai	• Neaptinka naujų žinomų atakų variantų • Didelis aptikimo netikslumas nežinomoms atakoms
Anomalijų detekcija	• Naudoja statistiką įsilaužimo aptikimui • Mažesnis aptikimo netikslumas nežinomoms atakoms	• Reikalauja daugiau laiko atakai aptikti • Aptikimo tikslumas pagrįstas surinkta elgsenos duomenų baze
Dirbtiniai neuroniniai tinklai	• Efektyviai klasifikuoja nestruktūrizuotus paketus • Keletas paslėptų sluoksnių didina efektyvumą	• Reikalauja daugiau laiko ir apmokymo • Mažesnis lankstumas
Fuzzy logika	• Naudojama kiekybinėms savybėms • Didesnis lanksumas neapibrėžtoms problemoms	• Mažesnis tikslumas nei dirbtinių neuroninių tinklų
Ryšių taisyklės	• Naudojama aptikti žinomą ataką ar panašias atakas	• Neaptinka visiškai nežinomų atakų • Reikalauja didesnės duomenų bazės taisyklėms sukurti • Naudojama tik neatitikimų detekcijai
Vektorinė detekcija	• Gali teisingai klasifikuoti įsilaužimus jei pateikiamas ribotas pavyzdžių kiekis • Gali dirbti su daug savybių	• Klasifikuoja tik diskretines savybes. Reikalauja daug pasiruošimo
Genetiniai algoritmai	• Naudojami geriausi pavyzdžiai detekcijai • Didelis efektyvumas	• Kompleksinis metodas • Naudojama specifinėms užduotims
Hibridinės technikos	• Efektyvus metodas tiksliam taisyklių klasifikavimui	• Didelės skaičiavimų sąnaudos

2.8 Pramoninių tinklų apsaugos įranga

Kompiuterinių tinklų apsaugai naudojama aparatūrinė arba programinė apsaugos įranga. Dažniausiai programinė įranga yra pigesnė, naudojama mažesniems tinklams, ji yra lankstesnė, lengvai perkonfigūruojama netgi nuotoliniu būdu. Aparatūrinė įranga – priešingai – dažniausiai yra brangesnė, ilgesnis ir sudėtingesnis diegimas, tačiau neapkrauna pagrindinės įrangos papildomais skaičiavimais, todėl naudojama didesnėse kompanijose, galinčiose daugiau investuoti į tinklų saugumą.

Ankstesniuose skyriuose aprašytos atskiros saugumo sistemos. Kiekviena jų atlieka savo funkciją. Kuriant stiprią tinklo apsaugos sistemą, reikalinga naudoti jas visas ar daugumą jų. Dauguma kompiuterinių pramonės tinklo įrenginių gamintojų siūlo savo saugumo įrangą. Visgi, didžiausi tinklų saugumo įrangos gamintojai yra Cisco ir Hawlett-Packard. Dažniausiai pigesnis, paprasčiau diegiamas variantas naudoti *all-in-one* tipo įranga, turinti visas ar dalį ankstesniuose skyriuose minėtų apsaugos sistemų. Jų suskirtymas pagal atliekamas funkcijas pavaizduotas 14 pav. Punktyrine linija apvesta *all-in-one* tipo įrangos atliekamos funkcijos.

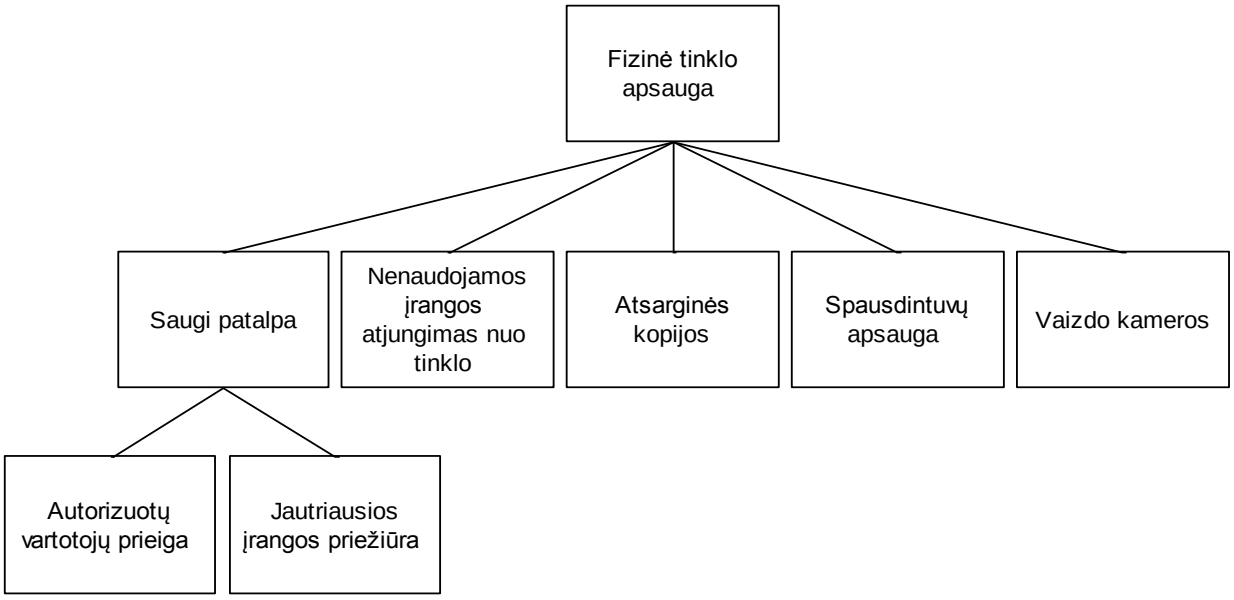


14 pav. Tinklų apsaugos sistemų funkcinis suskirstymas

3. Rekomendacijos pramoninio tinklo saugumo sistemoms

3.1 Fizinė tinklo apsauga

Fizinė tinklo apsauga yra pirmas žingsnis į įmonės saugumą. Tai užkerta kelią žemiausio lygio, paprasčiausiai realizuojamoms grėsmėms. Pagrindinės fizinės tinklo (įmonės) apsaugos sistemos pateiktos 15 pav. Prieiga prie pagrindinių tinklo sistemų turi būti prieinama tik autorizuotiems vartotojams, taipa pat leidimai naudotis darbo stotimis turi būti išduodami tik jų darbuotojams, tinklo administratoriui, atsakingam už tinklo saugumą. Svarbiausia informacija apsaugoma nuo negrįžtamo pradingimo skiriant atskirą serverį atsarginėms kopijoms. Šiandieniniai spausdintuvai saugo vidiniame diske spausdintų dokumentų įrašus, dėl to prieiga prie jų (programinė ir fizinė) taip pat turi būti tvirtai apsaugota.



15 pav. Fizinės tinklo apsaugos sistemos

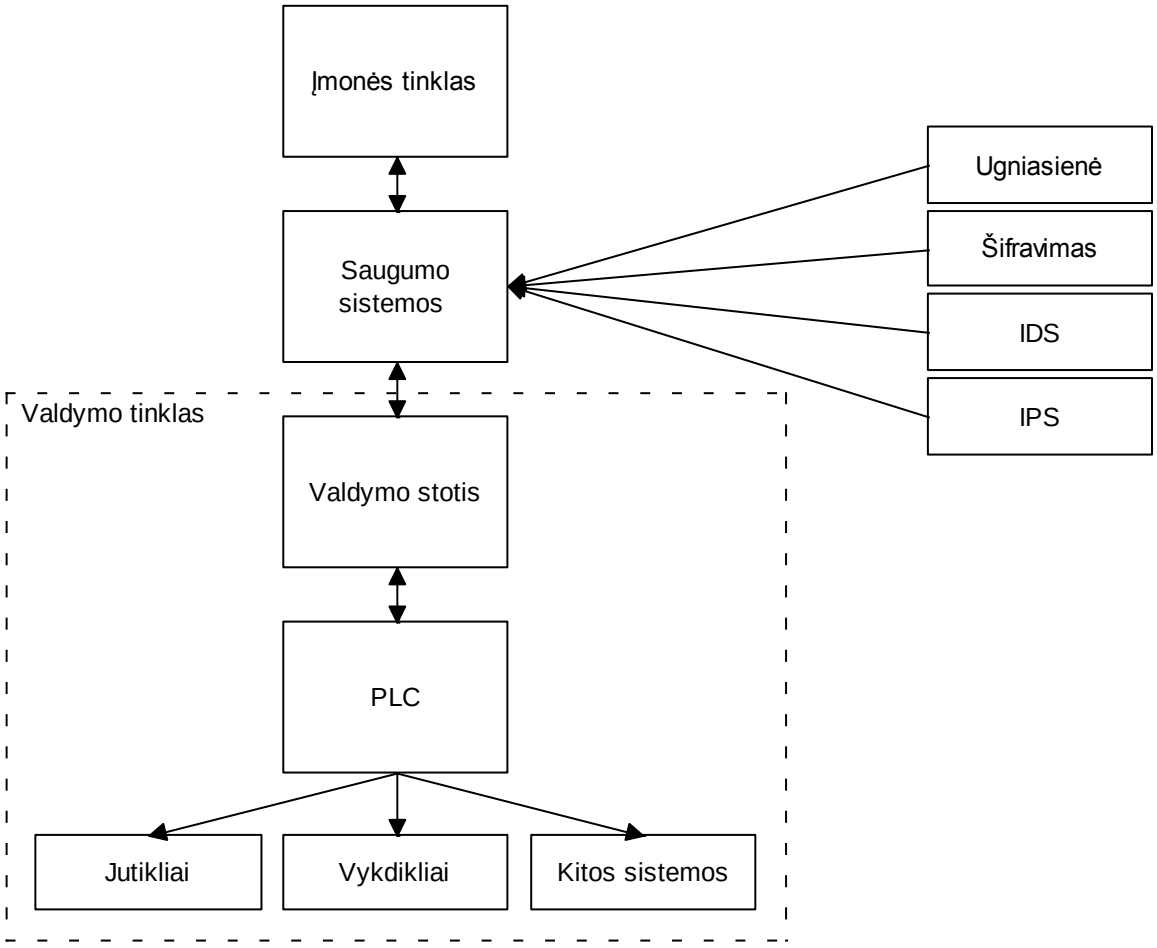
Visa programinė apsauga bus bevertė, jei nebus skiriamas dėmesys kas vyksta įmonės viduje. Saugumu besirūpinančioje įmonėje kiekvienas vartotojas turi unikalų prisijungimo kodą, slaptažodį, taip galima atsekti kas ir kada prisijungė, tai gali užkirsti kelią neleistinai veiklai įmonės viduje. Kaip ir bet kuriai saugumo įrangai, geriausia apsauga yra prevencija.

3.2 Programuojamų loginių valdiklių apsauga

Programuojami Loginiai Valdikliai (angl. *Programable Logical Controller* – PLC) dažniausiai komunikuoja su kompiuteriais, o tai yra lengvas būdas kenksmingoms aplikacijoms plisti. Visų pirma tokie kompiuteriai turi būti apsaugoti ugniasiene, kaip aprašyta 2.5 skyriuje.

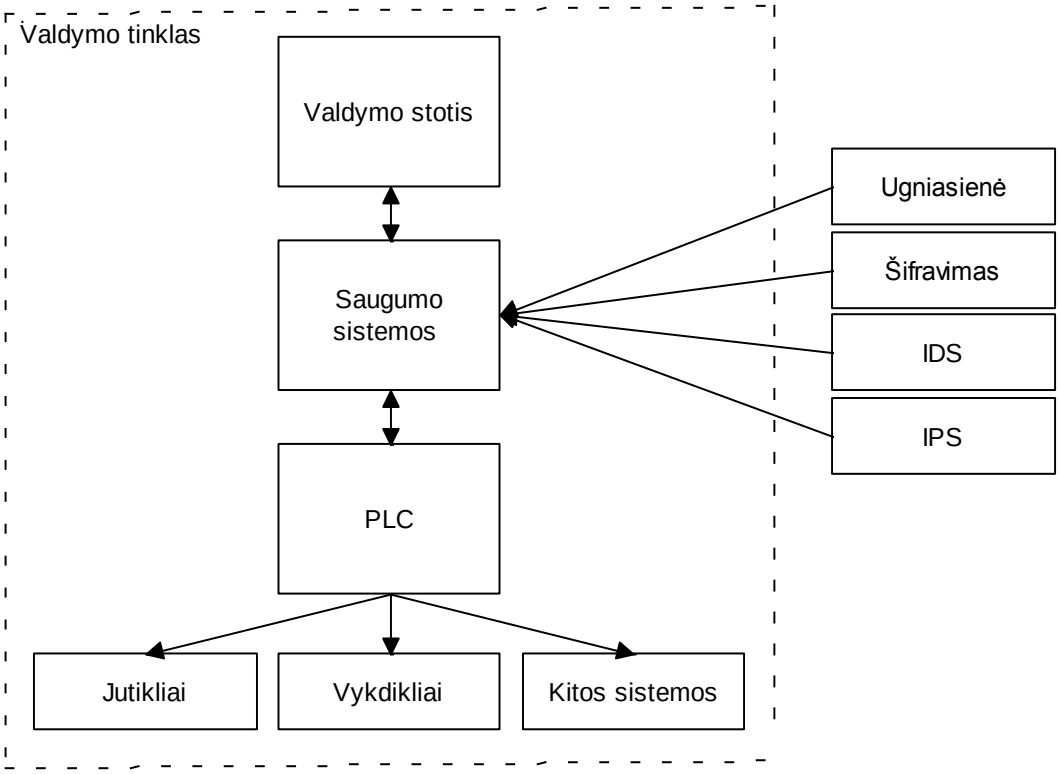
Pramonėje naudojant PLC valdiklius ir jutiklius bei vykdiklius, dažnai esminis kriterijus yra operacijos greitis, tai ypač svarbu realaus laiko sistemose. Dėl šios priežasties turi būti gerai įvertinama saugos sistemų įtaka duomenų perdavimo greičiui. Pagal tai siūlomi du saugumo sistemų tipai: atsižvelgiant į greitaveiką (a) ir neatsižvelgiant į greitaveiką (b).

a) Visų pirma, valdymo tinklas, kurį sudaro PLC valdikliai, HMI sąsajos, valdymui reikalingi serveriai atskiriami nuo bendro įmonės tinklo saugumo sistemomis, kaip parodyta 16 pav. schemoje. Pagrindinė priemonė – ugniasienė (2.5 skyrius), taip pat IDS, IPS sistemos bei duomenų šifravimas (2.6, 2.7 ir 2.3 skyriai).



16 pav. Duomenų srauto schema naudojant kompiuterio apsaugą

b) Itin griežto saugumo reikalaujantiems procesams valdyti naudotinas tiesioginės PLC apsaugos metodas. Schema pavaizduota 17 pav. Kaip ir (a) atveju, įmonės ir valdymo tinklai turi būti atskirti saugumo priemonėmis. Kaip ir įprasti, taip ir PLC skirti pranešimai gali būti šifruojami. Nors šifravimo-dešifravimo procesas užima tam tikrą laika, kas yra kritinis veiksnys realaus laiko sistemose, modernūs algoritmai (2.3 skyrius) leidžia skirtumą tarp šifruoto ir nešifruoto pranešimų sumažinti iki mažiau nei 1% [24].



17 pav. Duomenų srauto schema naudojant tiesioginę PLC apsaugą

3.3 SCADA sistemų apsauga

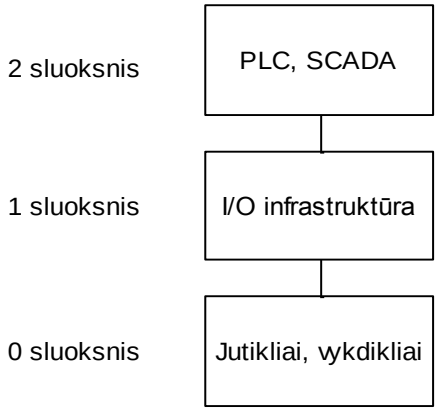
SCADA sistemų architektūra yra panaši į PLC sistemas, taigi, ir apsaugos sistemos yra panašios. Būtina atskirti valdymo tinklą nuo viso įmonės tinklo saugumą užtikrinančia sistema (3.1 skyrius). SCADA atakos pasekmės gali būti ne tik klaidingi valdymo signalai, bet ir klaidinga informacija apie sistemą, kas verstų vartotojus priimti neteisingus sprendimus. Siekiant užkirti kelią patiems vartotojams dėl neteisingai interpretuotų duomenų sugadinti sistemą, valdymo programa turi blokuoti rankinius nustatymus, jei yra pavojus sistemai, atsižvelgiant į proceso struktūrą.

Dauguma SCADA protokolų nenaudoja apsaugos sistemų, kaip šifravimas ar autentifikavimas, prieigos kontrolė. Specifinė grėsmė SCADA sistemoms – BYOD (1.4 skyrius).

Pagrindinis uždavinys yra naudoti antivirusines programas BYOD įrenginiuose: nešiojamuose kompiuteriuose, išmaniuose telefonuose, kuriais jungiamasi prie SCADA įrenginių.

Apsaugai nuo BYOD naudotinas duomenų šifravimo metodas (2.3 skyrius). Taip pat reikalaujama naudoti slaptažodžius keletu lygių, t.y. naudoti skirtingus slaptažodžius prieigai prie tinklo ir konkretiems veiksmams jame atlikti. Turi būti ribojama prieiga prie didelės svarbos parametrų.

Siekiant maksimaliai apsaugoti SCADA tinklą, turi būti gerai suprantamas tinklo veikimas. Jei duomenų mainai vienkrypčiai, kanalas turi veikti diodo principu, t.y. nepriimti atgalinio ryšio duomenų. Visas tinklas suskirstomas į sluoksnius, įprastinė struktūra pavaizduota 18 pav.



18 pav. SCADA tinklo sluoksnių struktūra

3.4 Prieigos kontrolės sistemos

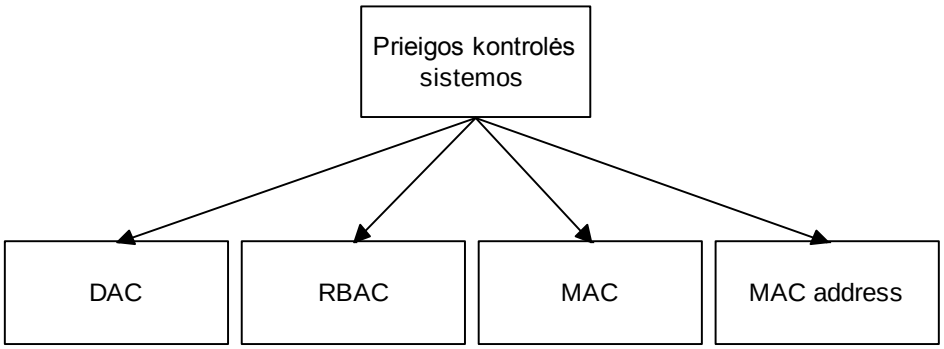
Pagrindinė apsaugos sistema nuo neautorizuoto prisijungimo yra prieigos kontrolės sistema. 19 pav. parodyti išskiriami pagrindiniai prieigos kontrolės sistemų tipai.

DAC (angl. *Discretionary Access Control*) – diskretinė prieigos kontrolė vykdoma remiantis vartotojo ar vartotojų grupės ID, t.y. vartotojo vardu, slaptažodžiu, naudojama įranga.

RBAC (angl. *Role-Based Access Controll*) – nediskretinė arba funkcija pagrįsta prieigos kontrolė. Šiuo atveju kiekvienam vartotojui suteikiamas atskiras leidimas prieiti prie tam tikrų duomenų. Kiekvienam vartotojui skirti leidžiami duomenys gali skirtis.

MAC (angl. *Mandatory Access Controll*) – leidimo (mandato) prieigos kontrolė. Šis metodas pagrįstas tuo, kad prisijungimo leidimą turi tik iš anksto numatyti vartotojai (įrenginiai).

MAC adreso (angl. *Media Access Control address*) kontrolės sistema remiasi nuikaliu IP tinklo adresu. Jį sudaro 48 bitai. Šis adresas dar vadinamas fiziniu adresu, nes jį unikalų suteikia gamintojas. Pirmi 6 simboliai nurodo gamintoją, paskutiniai 6 simboliai nurodo įrenginio serijos numerį. MAC adreso pavyzdys: 48-3F-0A-91-00-BC [25].



19 pav. Prieigos kontrolės sistemų tipai

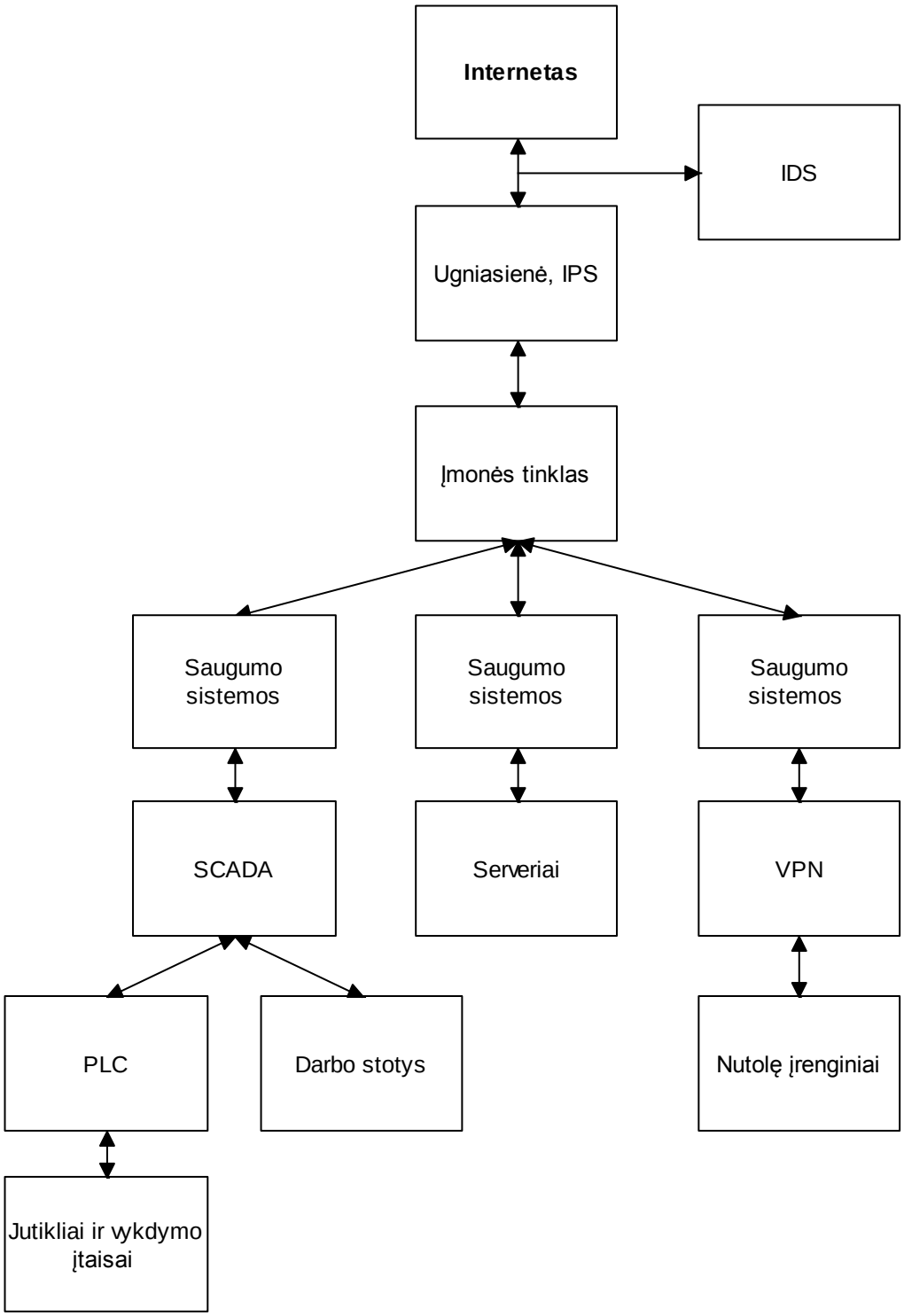
3.5 Belaidžių tinklų apsauga

Belaidžiai tinklai yra lengviau pasiekiami nei įprasti laidiniai, dėl to ir apsaugai turi būti skiriama daugiau dėmesio. Kaip ir įprastiems tinklams, naudojamos ugniasienės ir antivirusinė įranga, taip pat šifravimas ir kitos priemonės. Belaidžių tinklų specifinė apsauga – signalo slopinimas už įmonės tinklo ribų, kryptiniai siųstuvai.

Signalui perduoti belaidžiu ryšiu naudojami specialūs WEP (angl. *Wired Equivalent Privacy*), WPA (angl. *Wi-Fi Protected Access*), WPA2, TKIP (angl. *Temporal Key Integrity Protocol*), AES (angl. *Advanced Encryption Standard*) protokolai (2.3 skyrius). Kitas būdas nutolusių įrenginių sąsajai – VPN (2.4 skyrius). Skirtumas tarp šifravimo protokolų ir VPN yra šifruojamų duomenų kelias. VPN atveju, duomenys būna šifruoti nuo vidinio vartotojo įrenginio iki galutinio vartotojo taško. Tai yra sprendimas didelio jautrumo duomenims apsaugoti, arba jei nėra galimybės naudoti stipresnį nei statinį WEP šifrą.

3.6 Kompiuterinių tinklų apsauga

20 pav. pavaizduota bendra pramoninio tinklo schema įtraukiant saugumo įrangą. Įmonės tinklas atskiriamas nuo interneto ugniasiene, filtruojami siunčiami duomenys taip apsaugant tinklą nuo grėsmių iš interneto.

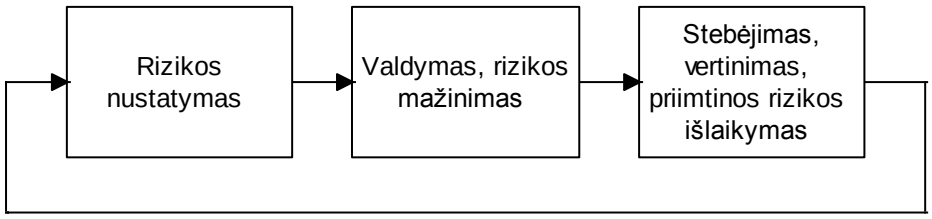


20 pav. Pramoninio kompiuterinio tinklo schema

Didžiausi tinklo saugumo įrangos gamintojai: WatchGuard, Cisco, HP, Ventus ir kiti. Šie gamintojai siūlo ne tik atskiras vieno tipo įrangos modulius, bet ir daugiau saugumo įrangos,

apjungtos į vieną sistemą. Kuriant naują tinklo saugumo sistemą rekomenduojama rinktis vieną gamintoją, taip nepaliekant saugumo spragos dėl skirtingų saugumo sistemų nekomunikavimo. Visgi, specializuotą įrangą teikia ne visi gamintojai, tad tam tikrais atvejais reikia derinti skirtingų gamintojų įrangą.

Tinklo saugumas yra nuolatinio tobulėjimo reikalaujantis procesas, pavaizduotas 21 pav., naudojant specializuotą įrangą, kurios programinė dalis gamintojo nuolat atnaujinama žengiama koja kojon su naujausiais saugumo sprendimais, išvengiama modernių įsilaužimo metodų.

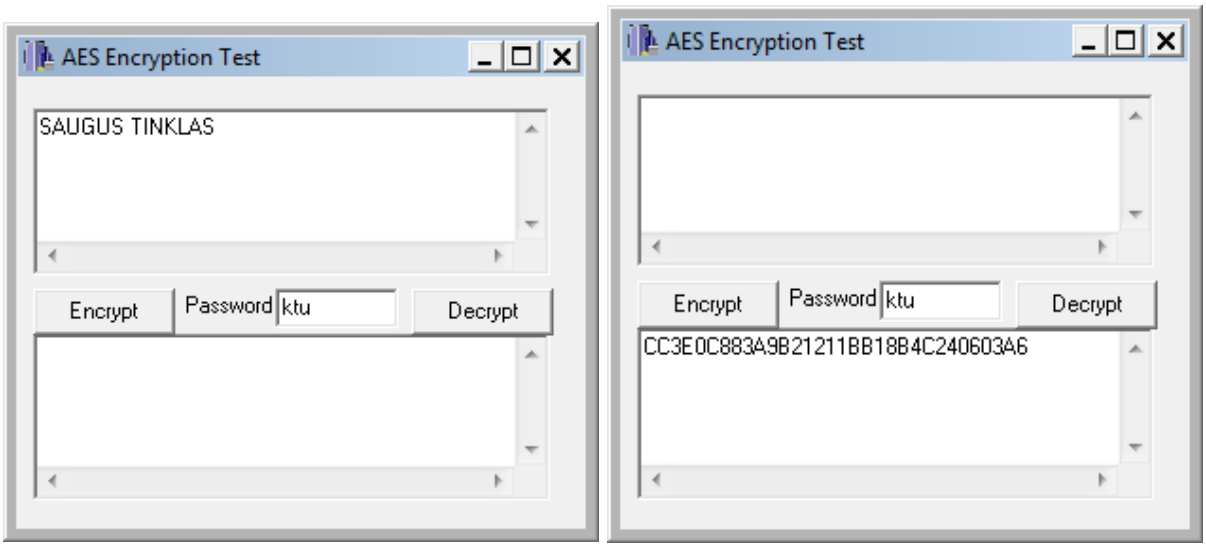


21 pav. Tinklo saugumo sistemų tobulinimo ciklas

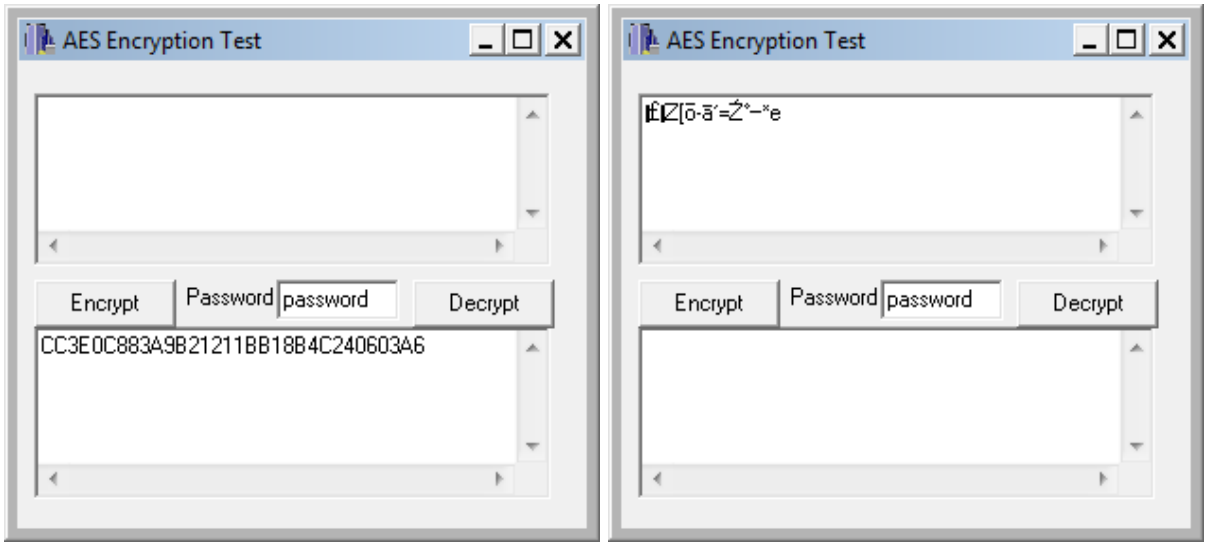
4. Įmonės kompiuterinio tinklo saugumo sistemų tyrimas ir projektavimas

4.1 Kompiuterinio tinklo šifravimo sistemų tyrimas

Šifravimo testavimui ir tyrimui naudota AES Encryption Test programa. AES (2.3 skyrius) algoritmu užšifruotas pranešimas „SAUGUS TINKLAS“, naudojant slaptažodį „ktu“. Gautas šifruotas pranešimas „CC3E0C883A9B21211BB18B4C240603A6“, kaip pavaizduota 22 paveiksle. Bandant tą patį pranešimą dekoduoti kitu slaptažodžiu, pradinis pranešimas negaunamas, 23 paveiksle vaizduojamas dekodavimas naudojant „password“ slaptažodį. Dešifruojant gaunamas „˙£ □Z[ō-ā’=Ź°—*e“ pranešimas, nesutampantis su pradiniu.



22 pav. AES šifravimo protokolo testavimas



23 pav. AES šifravimo protokolo testavimas dešifruojant neteisingu slaptažodžiu

4.2 Pranešimų skenavimo tyrimas

Tyrimui naudojami CAIDA [29] duomenys, 24 pav. ir Wireshark 1.12.5 programa. Pastaroji programa nėra skirta atakų aptikimui, tačiau kaupia statistiką, ir naudojant papildomus algoritmus leidžia aptikti neįprastą veiklą tinkle. Skenavimas atliekamas skenuojant siuntėjo IP adresą („0000 3c 1c 02 4f“ šešioliktainiu formatu, 25 pav.), protokolą („0000 06“ šešioliktainiu formatu, 25 pav.), pranešimo ilgį („0028“ šešioliktainiu formatu, 25 pav.), taip pat galimas filtravimas pagal kontrolinę sumą, tačiau šiuo atveju ji netikrinama („0000 d7 c2“ šešioliktainiu formatu, 25 pav.). Šiuo atveju turime didelį kiekį duomenų, tačiau neturime informacijos, ar buvo vykdomos atakos, taigi iš tam tikro duomenų kiekio atrinkti siųsti pranešimai, kuriuos galima traktuoti kaip kompiuterinio tinklo ataką pagal pasirinktus požymius. Duomenys yra surinkti per 1 valandos laiko tarpą, su tiksliu prisijungimo laiku.

```
Maximum capture length for interface 0:             99999
First timestamp:                      1226523600.001247000
Last timestamp:                       1226527199.995064000
Unknown encapsulation:                                    0
IPv4 bytes:                                        40754970
IPv4 pkts:                                           961801
Unique IPv4 addresses:                               527791
Unique IPv4 source addresses:                          5981
Unique IPv4 destination addresses:                   521810
Unique IPv4 TCP source ports:                         51096
Unique IPv4 TCP destination ports:                    56530
Unique IPv4 UDP source ports:                             0
Unique IPv4 UDP destination ports:                        0
Unique IPv4 ICMP type/codes:                             12
IPv6 pkts:                                                0
IPv6 bytes:                                               0
non-IP protocols:                                         0
non-IP pkts:                                              0
```

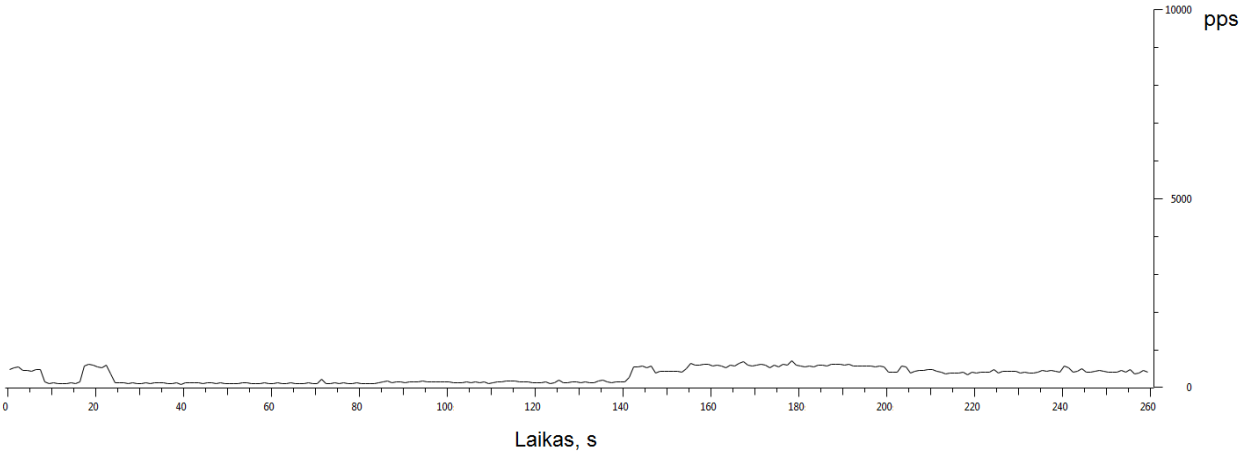
24 pav. Tyrimui naudotų duomenų statistika

Vieno iš pranešimų duomenys pavaizduoti 1 priede. Tie patys duomenys šešioliktainiu formatu pavaizduoti 25 pav.

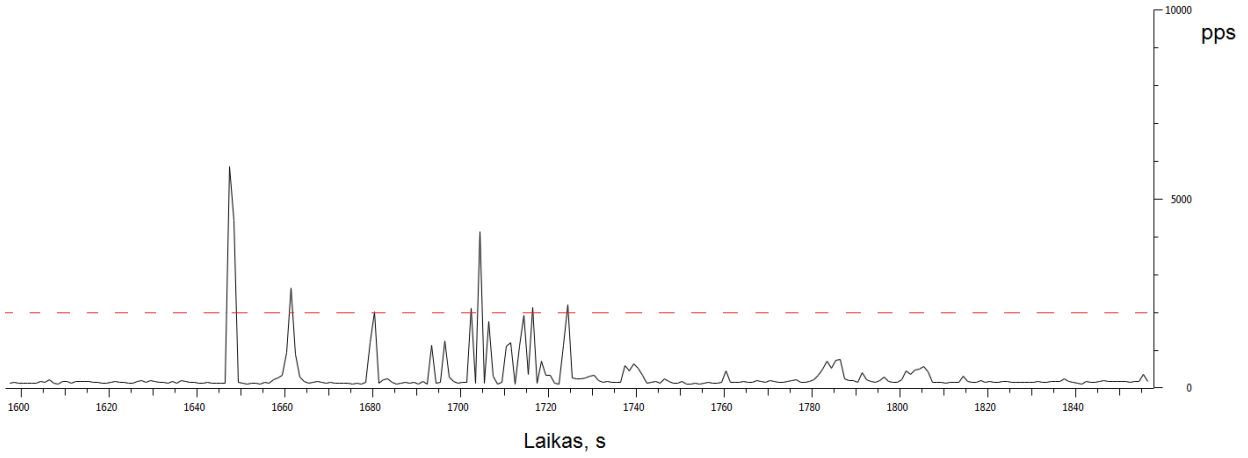
```
0000  00 03 47 9c e2 31 00 0a 8b ee e8 00 08 00 45 00
0010  00 28 e7 98 00 00 6b 06 c3 1b 3c 1c 02 4f 00 66
0020  66 4b 00 50 ad 27 00 00 00 00 a9 32 dc 47 50 14
0030  00 00 d7 c2 00 00 ab 00 00 00 00 00
```

25 pav. 1 priedo duomenys šešioliktainiu formatu

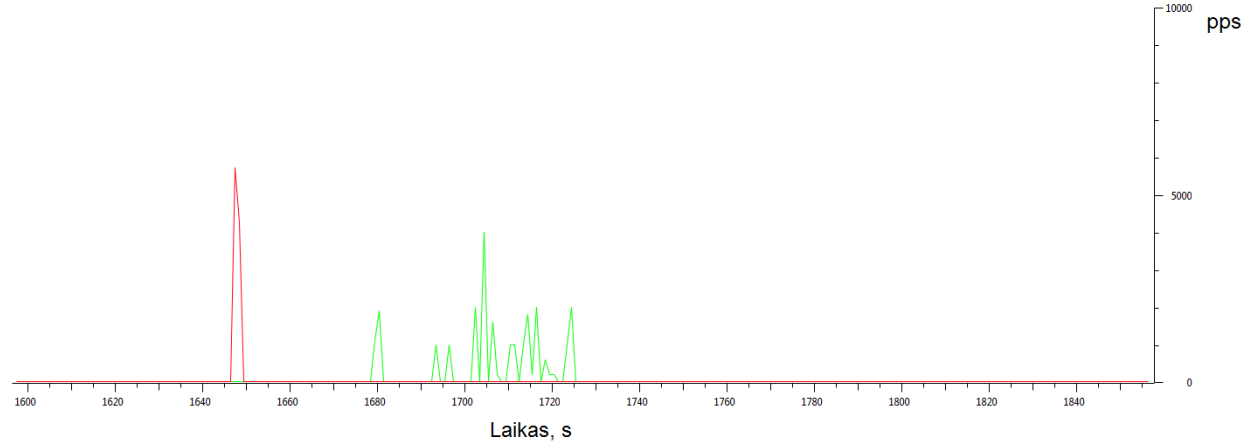
26 pav. pavaizduota įprasta tiriamo tinklo veikla. Šiuo atveju per sekundę gaunama iki 1000 pranešimų paketų, vidurkis yra 267 paketai per sekundę. 27 pav. pavaizduota galimai atakuojamas tinklas, kai pranešimų skaičius per 1 sekundę išauga iki 5000 (1645s-1650s) ir iki 4000 (~1705s), punktyrine linija pažymėta 2000 pranešimo paketų per sekundę tolerancijos riba. 28 pav. išskirti įtarimą keliančių IP adresų („221.123.133.196“ ir „218.92.19.186“) pranešimų srautai.



26 pav. Įprasta tinklo veikla



27 pav. Galimai atakuojamas tinklas



28 pav. Išskirti įtarimą keliantys IP adresai

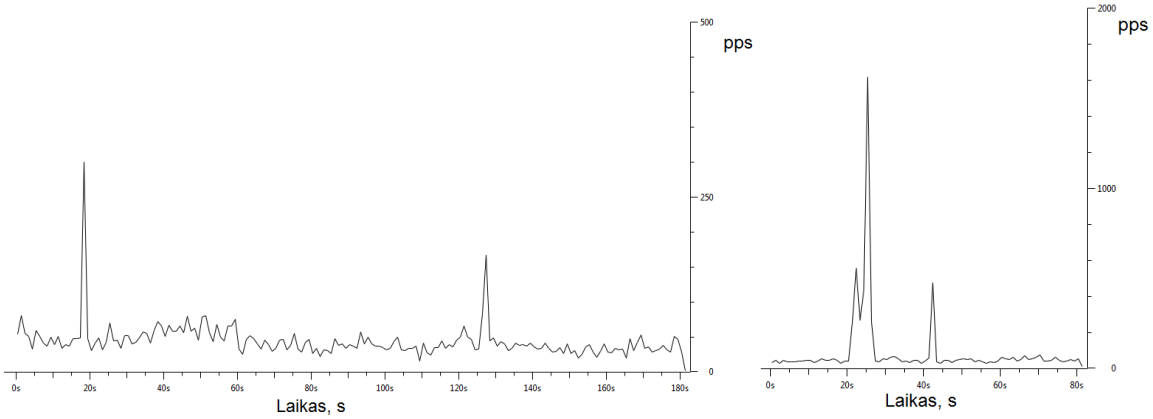
Kadangi nepateikiami duomenys apie pranešimų turinį, nustatyti ar vyko DoS ataka tiesiogiai negalime, reikia tikrinti siuntėjo IP adreso patikimumą, tačiau, atsižvelgiant, kad gavėjai skirtingi, galime teigti, kad buvo vykdoma DoS ataka. Nustačius kad šis IP adresas yra pavojingas, atliekamas filtravimas pagal IP=221.123.133.196 adresą, rasti 357720 šio siuntėjo pranešimų, o tai yra 37% visų pranešimų. Nustačius tokį duomenų kiekį tikrinamas siutėjas pagal IP adresą ir siųsti pranšimai. Kadangi turima statistika pagal pranešimo antraštę, pranešimo turinys nėra žinomas. Skenuojant pranešimus realiu laiku, naudojamos įsilaužimo aptikimo ir prevencijos sistemos (4.3 skyrius).

29 pav. neįprastos veiklos sąrašo didžiąją dalį (net 70%) sudaro pakartotino prisijungimo bandymai (673861 pranešimas). Sugeneravus keletą kito tinklo analizės failų, 30 pav., šis rodiklis gaunamas žymiai mažesnis (0,2%, 0,1%). 30 (a) pav. programa Matlab rasti 64 unikalūs prisijungimo šaltiniai. Kiti įspėjimo pranešimi – nepriimtas ankstesnis pranešimas – sudaro 1,8%, pranešimas siųstas ne iš eilės – 1,2. Šiuo atveju tikrinama tik pranešimo antraštė. Detalesnei analizei įsilaužimo aptikimo ir prevencijos sistemoms naudojamas tikrinimas pagal antraštę ir pranešimo turinį (4.3 skyrius).

Errors: 0 (0) | Warnings: 22 (703607) | Notes: 8 (100253) | Chats: 200 (252605) | Details: 1056465 | Packet Comments: 0

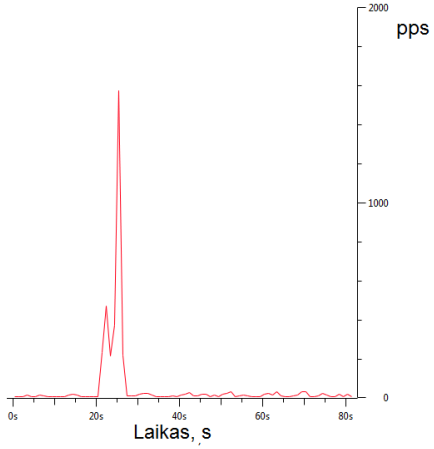
Group	Protocol	Summary	Count
Sequence	TCP	Connection reset (RST)	673861
Sequence	TCP	Previous segment not captured (common at capture start)	17796
Sequence	TCP	This frame is a (suspected) out-of-order segment	11917
Protocol	IPv4	Unknown (0xd5) (option length = 79 bytes says option goes past end of options)	15
Protocol	IPv4	Record Route (option length = 218 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x02) (option length = 188 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x03) (option length = 68 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x10) (option length = 165 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x2c) (option length = 44 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x33) (option length = 194 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x51) (option length = 14 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x5c) (option length = 211 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x67) (option length = 52 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x6e) (option length = 12 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x72) (option length = 105 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x74) (option length = 118 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x7b) (option length = 26 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0x96) (option length = 194 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0xa3) (option length = 123 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0xc1) (option length = 183 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0xd8) (option length = 212 bytes says option goes past end of options)	1
Protocol	IPv4	Unknown (0xfd) (option length = 128 bytes says option goes past end of options)	1

29 pav. Įspėjimų apie neįprastą veiklą tinkle sąrašas



(a) (b)

30 pav. Sugeneruoti patikimų internetinių svetainių (a) ir nepatikimų internetinių svetainių (b) pranešimų grafikai

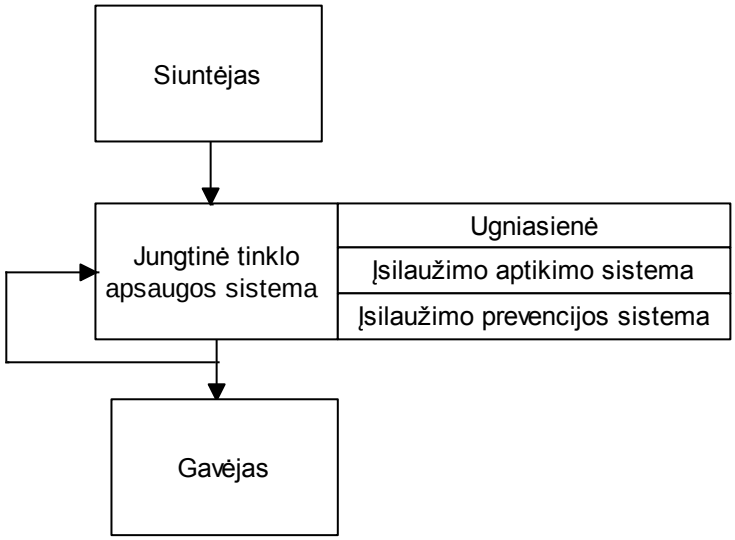


31 pav. Aptikta žalinga veikla tinkle (30 pav. b)

30 pav. vaizduojami sugeneruoti patikimų svetainių (a) ir nepatikimų svetainių (b) pranešimų grafikai. 30 (a) paveiksle matomi atsitiktiniai duomenų srauto šuoliai, vidutinis srautas 42,9 pranešimo per sekundę, šuoliai 320 ir 170 pranešimų per sekundę, tai sudaro 745% ir 396% vidutinio srauto. Tuo tarpu 30 (b) pav. tinkle vidutinis srautas yra 84,3 pranešimo per sekundę, šuolis 1600 pranešimo per sekundę užkrovus nepatikimą svetainę. Tai sudaro 1897% vidutinio srauto. Be to, pabrėžtina, kad šiuo atveju vidutinė srauto reikšmė apskaičiuota kartu su nepatikimų svetainių duomenimis, lyginant su patikimų svetainių vidurkiu, gaunamas 3729% šuolis, pavaizduotas 31 pav.

4.3 Kompiuterinio tinklo įsilaužimo aptikimo ir prevencijos sistemų tyrimas

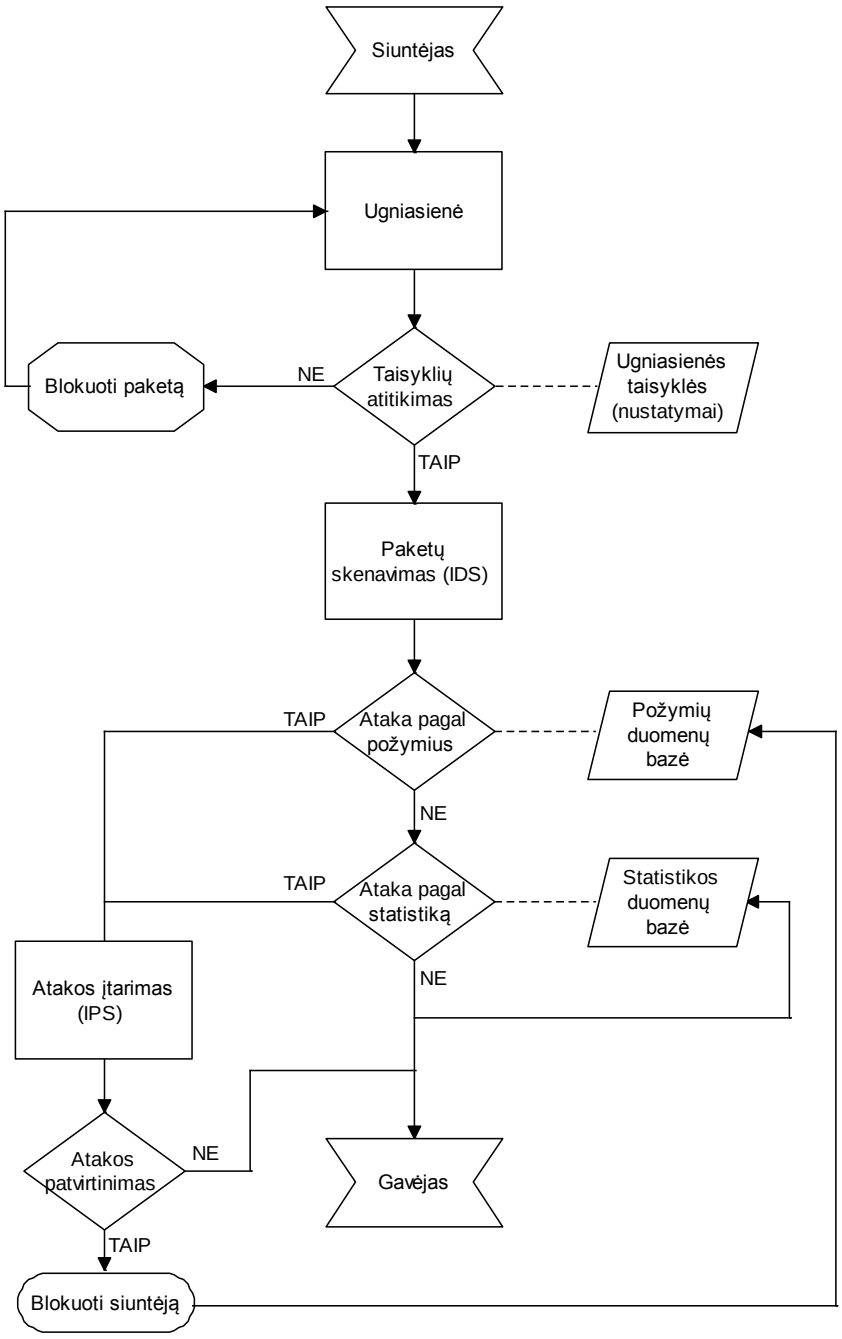
Ugniasienė (2.5 skyrius), IDS (2.6 skyrius) ir IPS (2.7 skyrius) sistemos yra atskiri saugumo prevencijos metodai, besiskiriantys veikimo principu ir paskirtimi. Visgi, siekiant maksimalaus tinklo saugumo šias sistemas galima sutalpinti į vieną komponentą, kaip pavaizduota 32 pav.



32 pav. Kompiuterinio tinklo saugumo sistema

Jei ugniasienė ir įsilaužimo aptikimo sistemos veikia nuspėjamai ir aptinka tik tam tikrus žinomus įsilaužimo bandymus, įsilaužimo aptikimo pagal statistiką sistema veikia sudėtingiau (2.6 skyrius).

33 paveiksle pavaizduota saugumo sistema atlieka ne tik IPS ir IDS, bet ir ugniasienės funkciją. Šiuo atveju Jungtinė tinklo apsaugos sistema veikia kaip NGFW (angl. *Next Generation Firewall*) (2.5 skyrius). Naudojama ugniasienė, IDS pagal statistiką ir požymius ir IPS algoritmas. Šiuo atveju naudojamos dvi duomenų bazės: pirmoji – požymių duomenų bazė, apsaugai nuo žinomų atakų tipų ir antroji – statistinė, ši yra nuolat atnaujinama, fiksuojami įprastai gaunami pranešimai, kai neaptinkamas saugumo pažeidimas. Pirmuoju atveju pažeidimas fiksuojamas, jei yra atitikmnenų duomenų bazėje, antruoju atveju – priešingai, pažeidimas fiksuojamas aptikus neįprastą reiškinį. Aptikus galimą saugumo pažeidimą atliekama patvirtinimo procedūra, pažeidimo tipo nustatymas, pagal tai atliekami tolesni veiksmai. Tai gali būti vartotojo informavimas, leidžiant tolesnį ryšį, siuntėjo blokavimas, pakartotinis sujungimo bandymas ar kiti veiksmai. Patvirtinus tinklo ataką, požymiai įrašomi į požymių duomenų bazę, taip ją išplečiant ir užkertant kelią kitai tokio tipo atakai. Jei ataka neaptinkama, tinklo darbo duomenys kaupiami statistikos duomenų bazėje, jei staiga einamieji duomenys pakinta, įtariama ataka.



33 pav. Tinklo saugumo sistemos algoritmas naudojant ugniasienę, IDS pagal statistiką ir požymius ir IPS

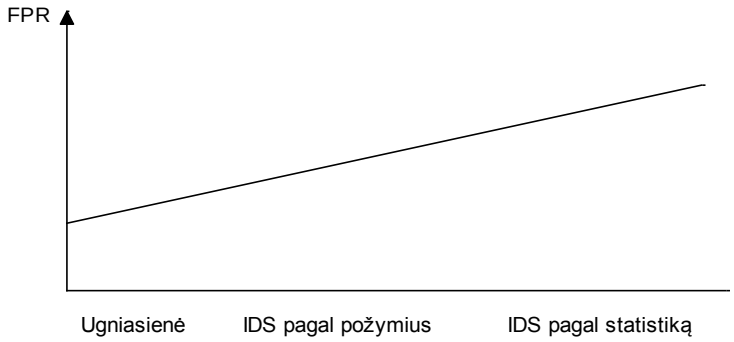
FPR (angl. *False Positive Risk*) – klaidingo teigiamumo rizika – parametras, įvertinantis galimo klaidingo atakos diagnozavimo pavojų. Jis apskaičiuojamas atpažntų tikrų atakų skaičių padalinus iš bendro atpažintų atakų skaičiaus:

$$FPR = \frac{TP}{(TP + FP)}$$

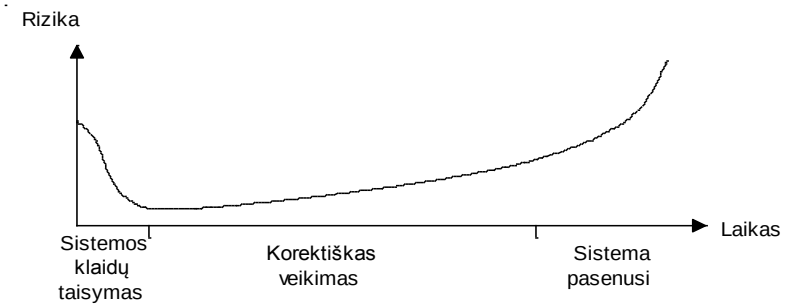
Čia FPR – klaidingo teigiamumo rizika (angl. *False Positive Risk*), TP – teisingas teigiamumas (angl. *True Positive*), FP – klaidingas teigiamumas (angl. *False Positive*).

31 paveiksle pavaizduoto algoritmo sistemų palyginamasis FPR grafikas pavaizduotas 34 pav. Grafikas gautas vertinant sistemų darbo pobūdį, t.y. kaip jos atpažįsta ataką.

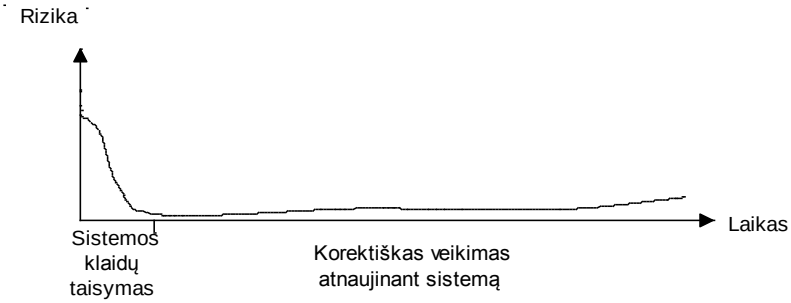
Kompiuterinio tinklo apsaugos sistemą būtina nuolat atnaujinti, įsilaužimo rizikos įvertinimas neatnaujinant sistemos pavaizduotas 35 pav. Nuolat atnaujinant sistemą, rizikos įvertinimas pavaizduotas 36 pav. Tobulėjant kompiuterinie įrangai, įsilaužimų algoritmai sparčiau veikia, ypač kalbat apie slaptažodžių ar šifruotų pranešimų neautorizuotą dešifravimą. Siekiant išvengti nepageidaujamo informacijos nutekinimo, saugumo sistemos turi būti nuolat atnaujinamos, kaip minėta 3.6 skyriuje.



34 pav. Nagrinėjamų sistemų klaidingo teigiamumo rizikos (FPR) palyginimas



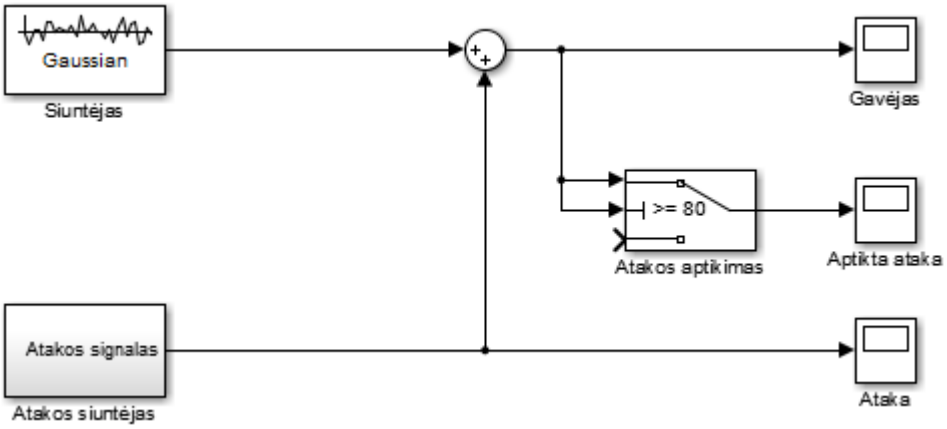
35 pav. Rizikos laiko bėgyje įvertinimas neatnaujinant sistemos



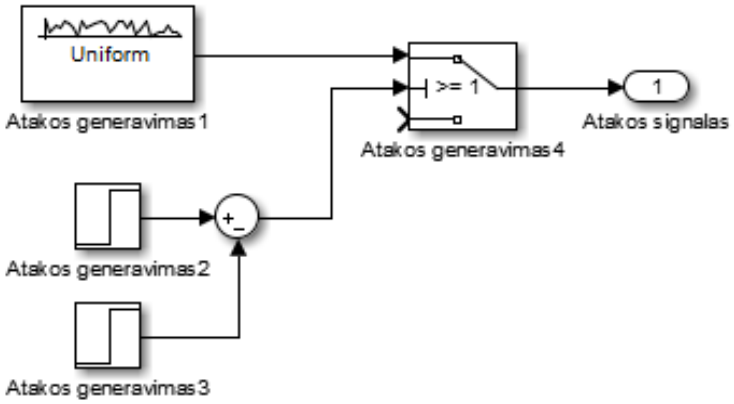
36 pav. Rizikos laiko bėgyje įvertinimas atnaujinant sistemą

4.4 Pranešimų skenavimo ir ugniasienės variacijų tyrimas Matlab Simulink programiniu paketu

Remiantis 4.2 skyriuje atliktu kompiuterinio tinklo pranešimų tyrimu, Matlab Simulink aplinkoje sukurtas 37 pav. pavaizduotas modelis, ataką aptinkantis pagal duomenų srautą (pranešimai per sekundę - pps). 38 pav. pavaizduotas atakos generavimo modelis. Šiuo atveju ataka fiksuota, kai pranešimų skaičius per sekundę viršija 70 pps.

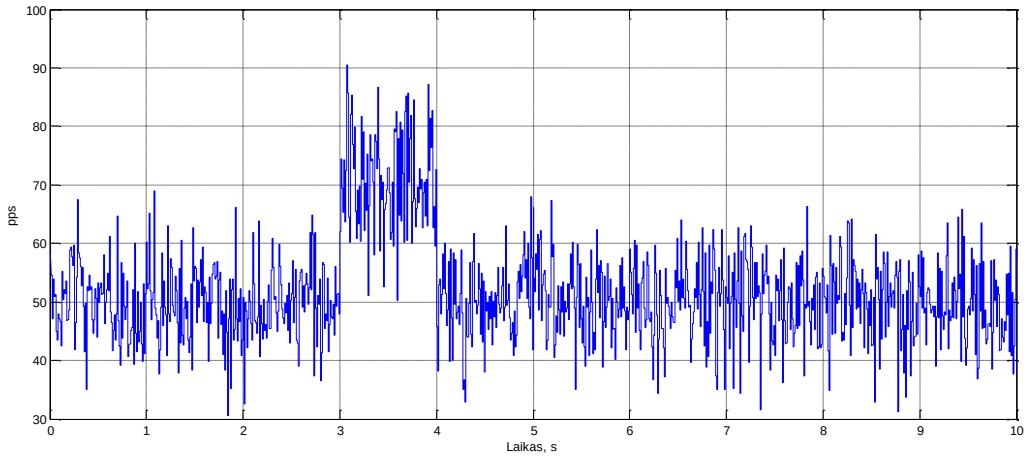


37 pav. Matlab aplinkoje realizuotas atakos aptikimo modelis pagal pps

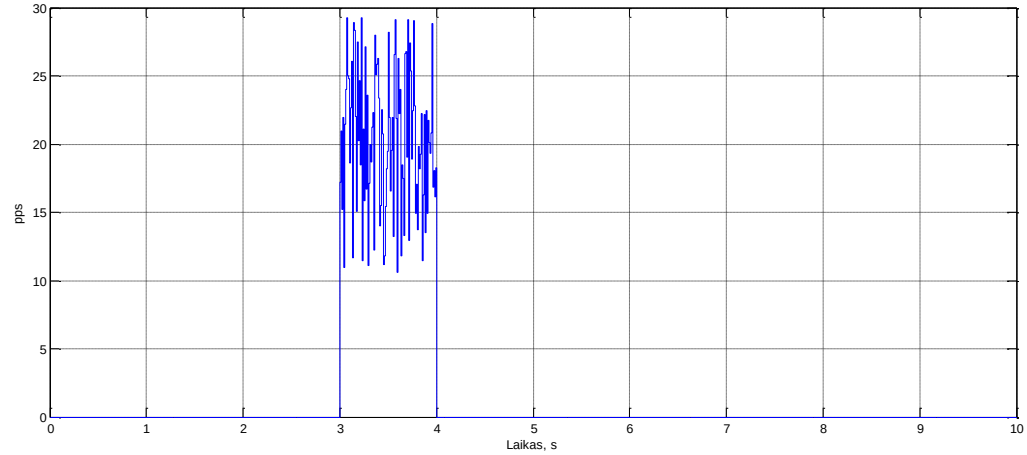


38 pav. „Atakos siuntėjas“ subsistemos modelis

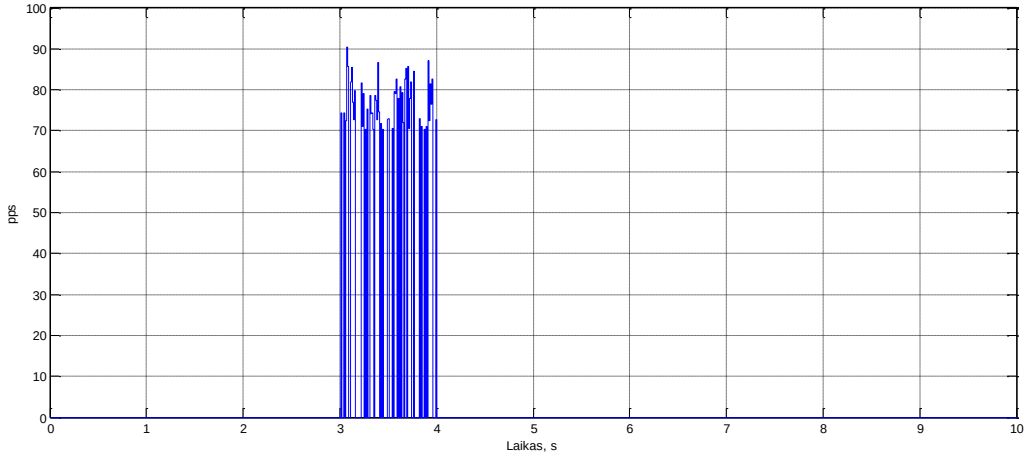
Šiuo atveju aptinkamas tik galimos atakos faktas, o ne užpuoliko duomenys, todėl šis metodas reikalauja gilesnės atakos aptikimo momentu pranešimų analizės. Kaip matyti iš 39 pav., 40 pav. ir 41 pav., aptikti ne visi atakos pranešimai. Kadangi generuojamas atsitiktinis duomenų srautas, aptinkama apie 80-90% atakos.



39 pav. Sugeneruotas pranešimų srautas ir ataka 3-4 sekundę

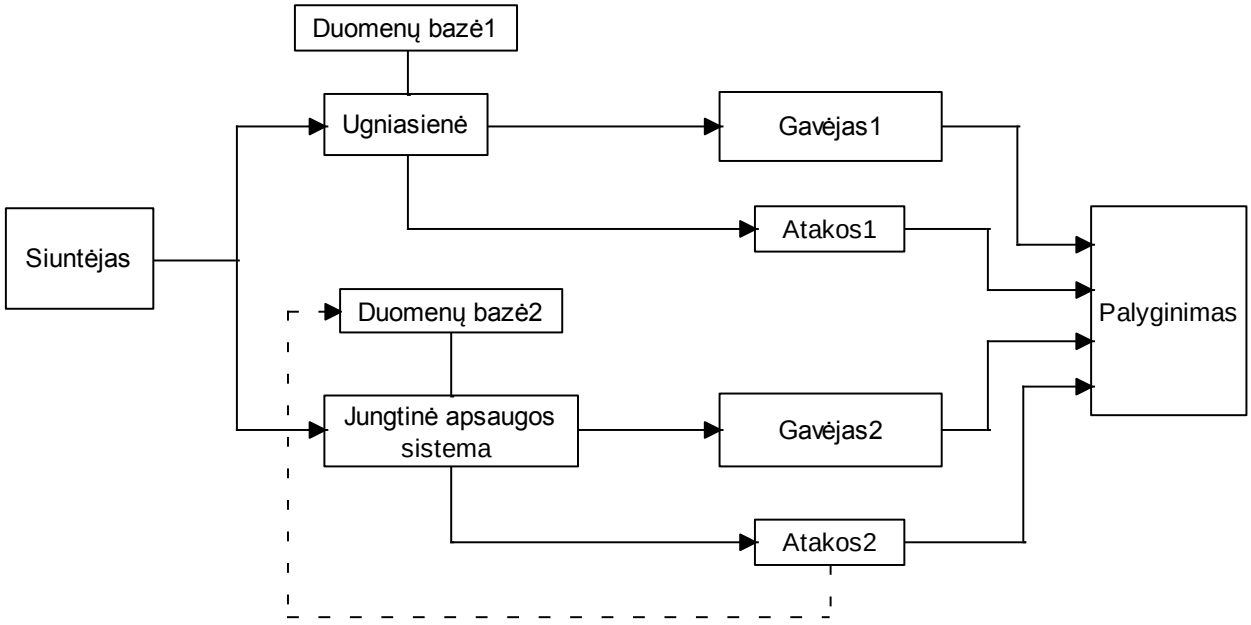


40 pav. Sugeneruotas atakos pranešimų srautas



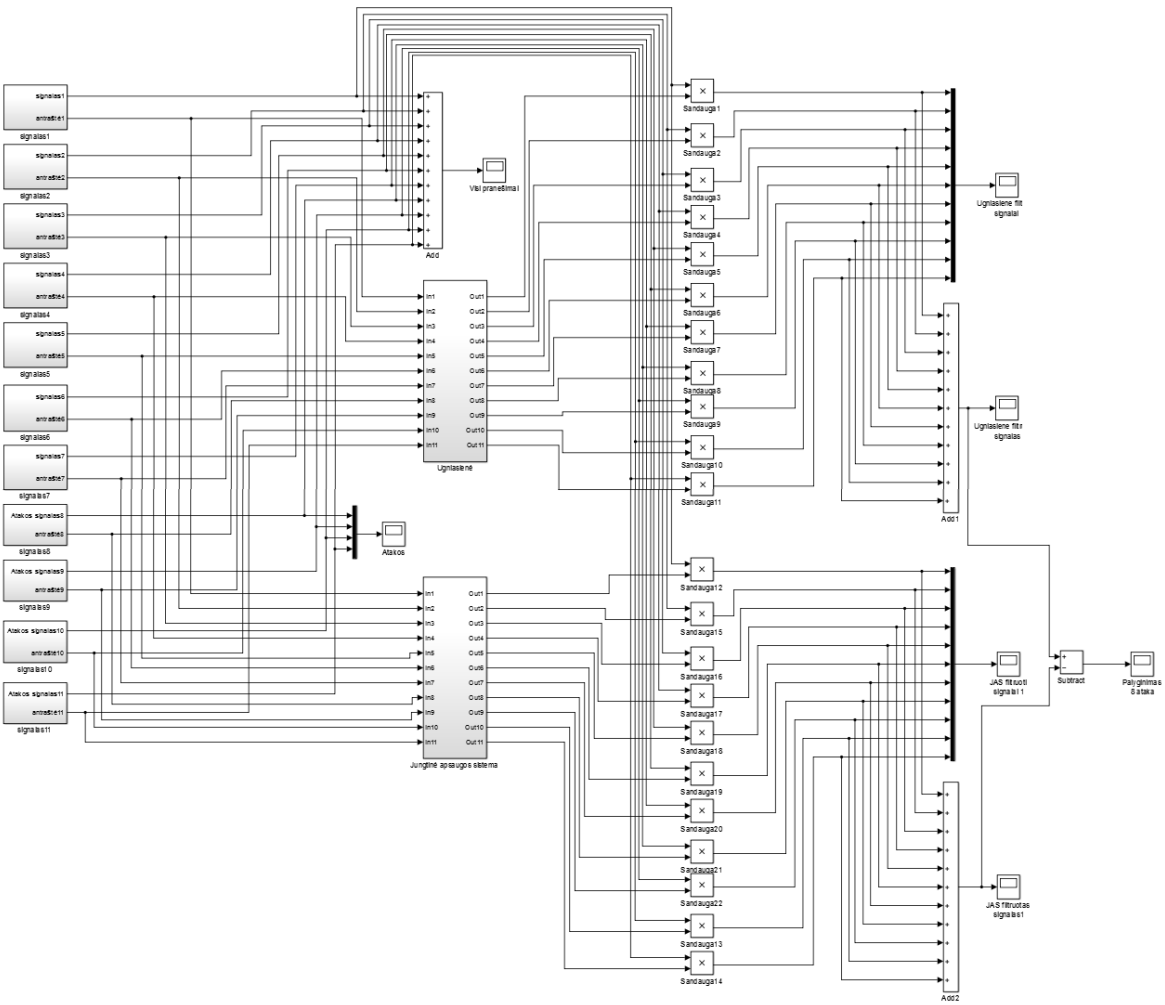
41 pav. Aptikta ataka pranešimų sraute

Sudaryta ugniasienės ir Jungtinės apsaugos sistemos (ugniasienė, įsilaužimo aptikimo ir prevencijos sistemos) schema pavaizduota 42 paveiksle. Ji realizuota Matlab Simulink pakete. Siuntėjas – tai 11 skirtingų pranešimų, besiskiriančių turiniu ir antrašte. Trys kenksmingų pranešimų antraštės yra žinomos. Ugniasienė praleidžia tik žinomus nekenksmingus antraščių tipus, tačiau duomenų bazė nėra atnaujinama, dėl ko gali atsitikti atvejis, kai pagal nutylėjimą nekenksmingas failo tipas praleidžiamas ir sukelia nuostolius. Apsaugai nuo to naudojama Jungtinė apsaugos sistema, filtruojanti ne tik antraštę, bet ir patį pranešimą, o aptikus ir/ar patvirtinus naujas atakų formas, jų požymiai įtraukiami į atakų požymių duomenų bazę, taip užkertant kelią vėlesniai tokio paties tipo atakai.

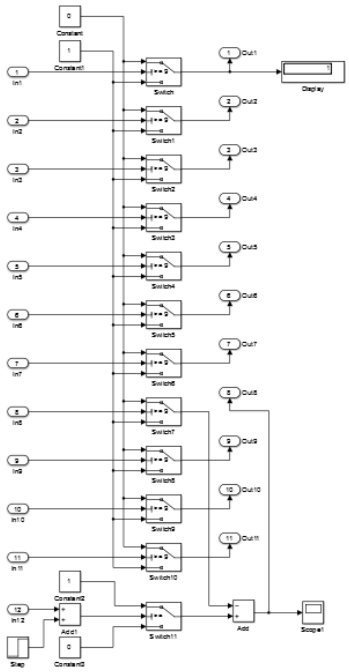


42 pav. Ugniasienės ir Jungtinės apsaugos sistemos tyrimo schema

43 pav. pavaizduotas Matlab Simulink aplinkoje realizuotas tyrimo algoritmas. Sukurti 11 signalų su skirtingomis antraštėmis. Iš jų 3 (9, 10 ir 11) yra žinomos atakos. 1 (8) yra nežinoma ataka. Šiuo atveju ugniasienė praleidžia visus pranešimus, išskyrus 9, 10 ir 11. 44 pav. pavaizduotas ugniasienės modelio realizavimas Matlab Simulink aplinkoje. Pranešimai tikrinami pagal antraštę ir praleidžiami tik leistini. Tas pats modelis naudotas Jungtinei apsaugos sistemai realizuoti tačiau pakeisti filtravimo nustatymai. Šis sistema realiu laiku atnaujina savo duomenų bazę, todėl aptikus ataką, tokio tipo antraštė yra blokuojama.

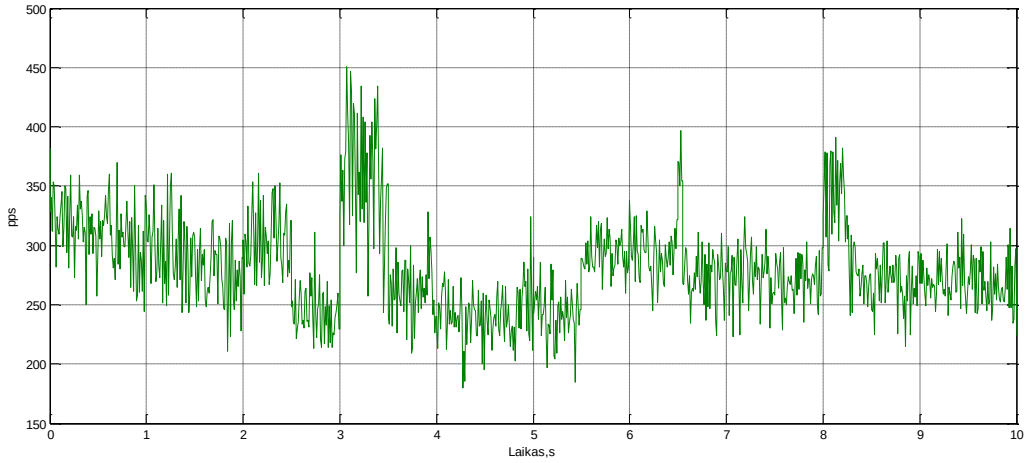


43 pav. Ugniasienės ir Jungtinės apsaugos sistemos palyginimo schema realizuota Matlab Simulink aplinkoje

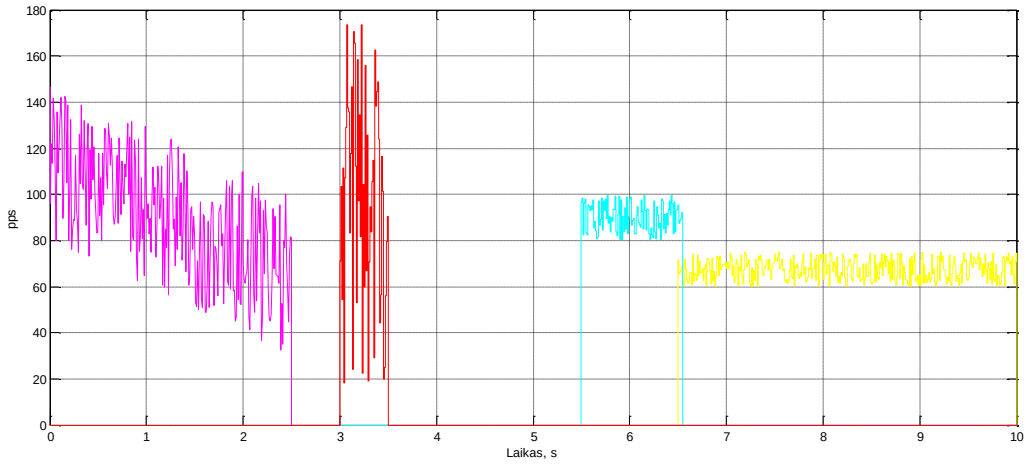


44 pav. Ugniasienės, realizuotos Matlab Simulink aplinkoje, subsistemos modelis

45 pav. pavaizduotas visų pranešimų bendras siunčiamas srautas. Jame taip pat yra 46 pav. pavaizduoti atakų pranešimai. Ugniasienė ir Jungtinė apsaugos sistema filtruoja srautą pagal antraštę.

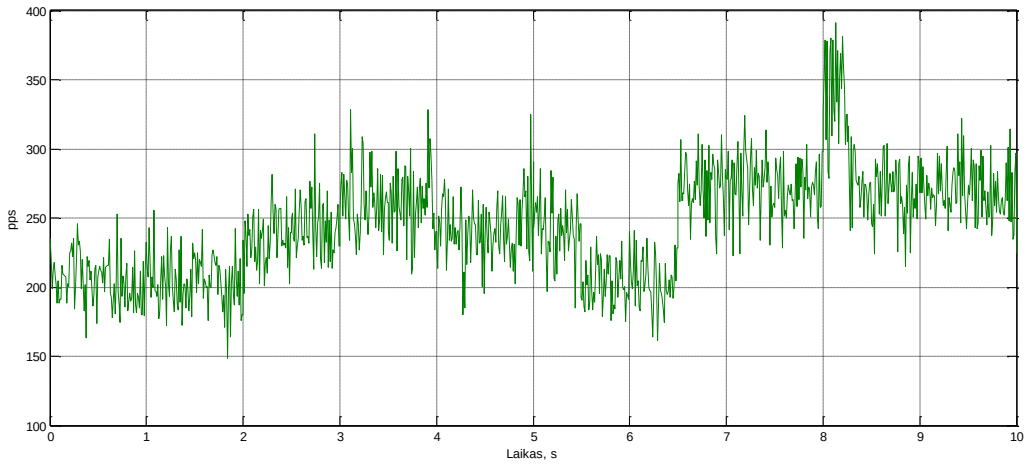


45 pav. Visų siųstų pranešimų bendras srautas

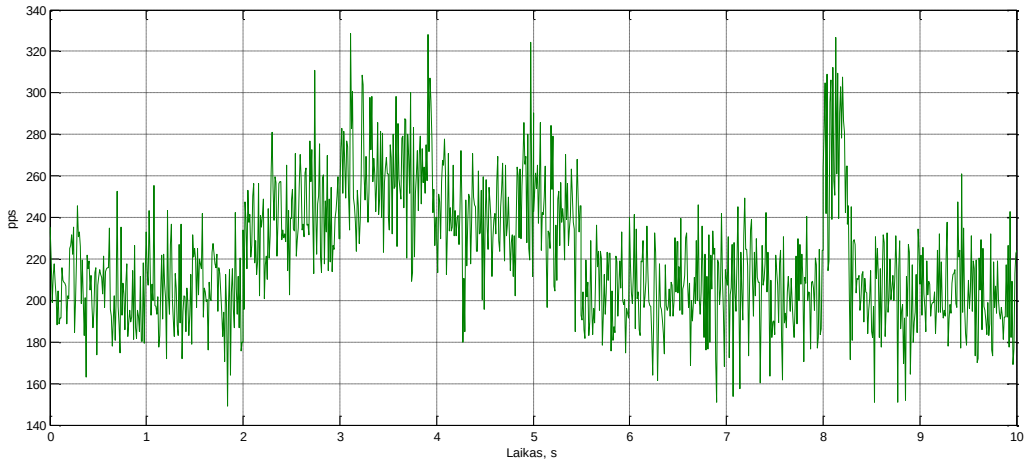


46 pav. Visų atakų pranešimų srautai

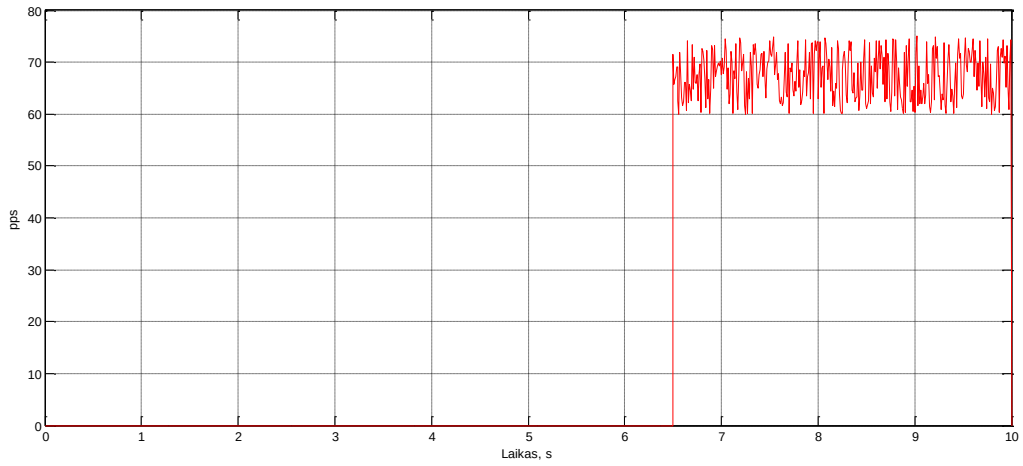
47 pav. ir 48 pav. pavaizduoti ugniasienės ir Jungtinės apsaugos sistemos prafiltruoti duomenų srautai. 49 pav. vaizduojamas šių srautų skirtumas yra ketvirtoji ataka, kurios pranešimuus praleido ugnasienė. Ugniasienė praleidža pranešimų tipą pagal antraštę, kuris gali būti kenksmingas. Šiuo atveju jei Jungtinė apsaugos sistema aptinka galimai žalingo tipo duomenis, blokuojama šio tipo duomenų antraštė ir duomenys negaunami (nepraleidžiami).



47 pav. Ugniasiene filtruotų pranešimų srautas

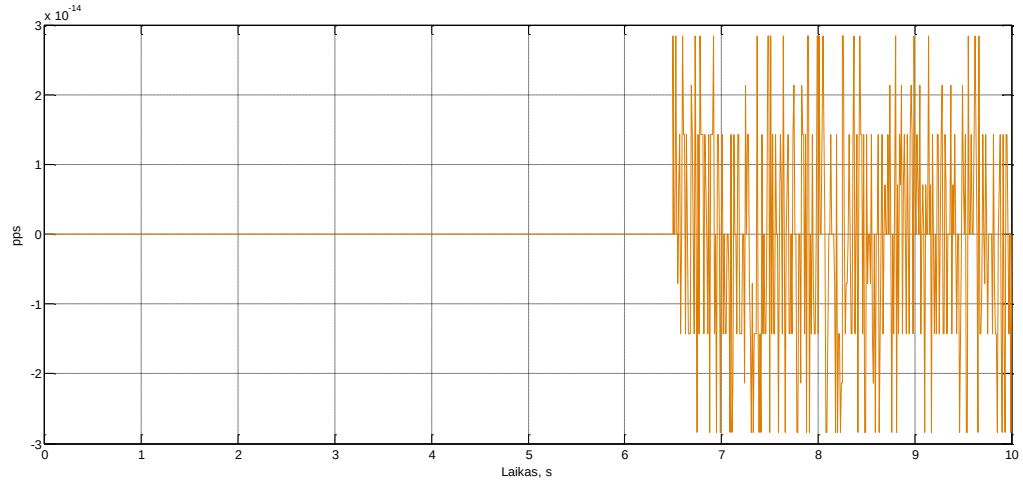


48 pav. Jungtine apsaugos sistema filtruotų pranešimų srautas



49 pav. Skirtumas tarp gautų 47 pav. ir 48 pav. signalų srautų

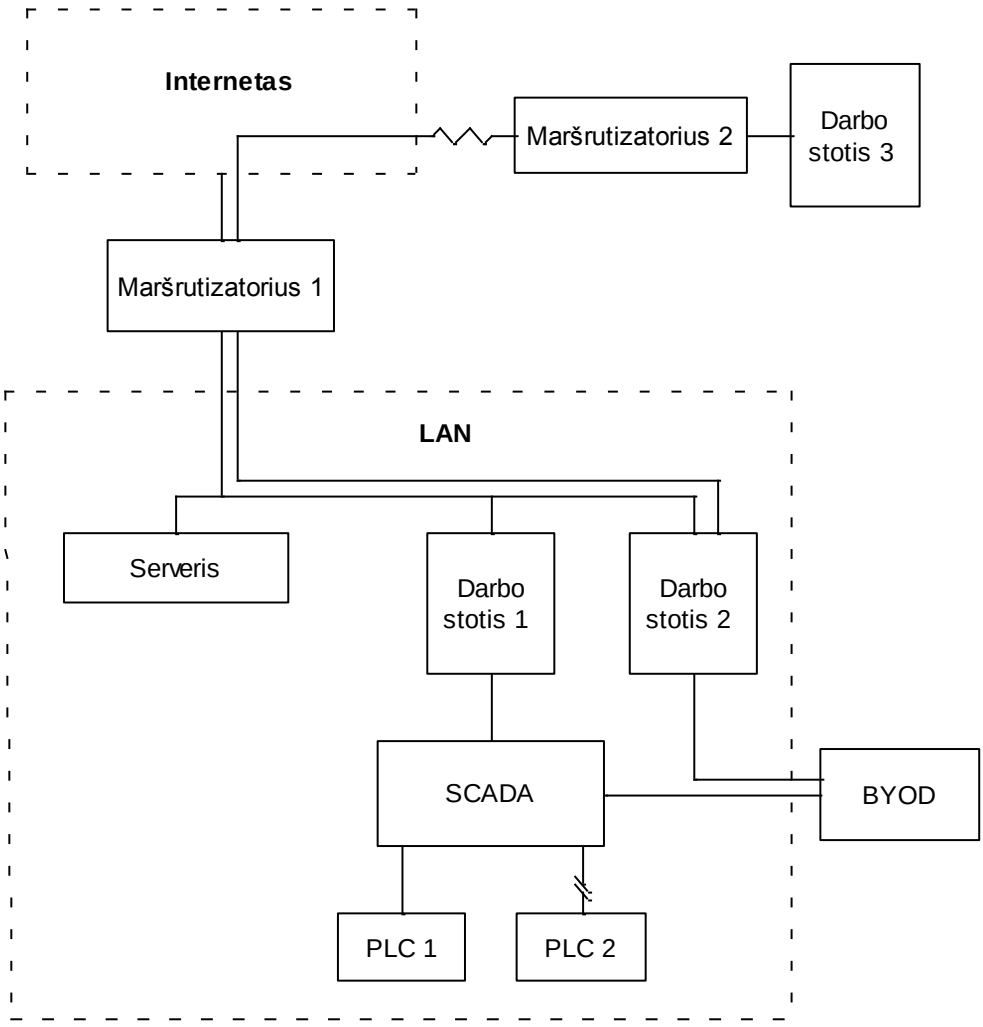
50 pav. pavaizduotas skirtumas tarp sugeneruoto atakos pranešimų srauto signalo (8) ir Jungtinės apsaugos sistemos aptiktos ketvirtosios atakos. Signalas yra 10^{-14} eilės. Jis atsiranda dėl Matlab programos skaičiavimo apvalinimo paklaidos.



50 pav. Sugeneruotos ir aptiktos ketvirtosios atakos paklaida

4.5 Įmonės kompiuterinio tinklo saugumo sistemų projektavimas

Pramoninio tinklo saugomo sistemų projektavimas pradedamas nuo tinklo įvertinimo. Visų pirma, tinklas suskirtomas į nedidelius blokus (mazgus) pagal paskirtį, padėtį, komunikacijų tipus, prieigos leidimus ir galimybes, saugumo reikalavimus, galimų įsilaužimų pasekmių reikšmingumą ir t.t. Kiekvienam mazgui pritaikoma saugumo sistema ar sistemos. 51 paveiksle pavaizduota nagrinėjamo tinklo struktūrinė schema. Čia „PLC 2“ su valdymo stotimi bendrauja belaidžiu ryšiu, „Darbo stotis 3“ yra fiziškai nutolusi nuo LAN tinklo. Pagrindinės siūlomos šakų apsaugos priemonės pateiktos 4 lentelėje.



51 pav. Nagrinėjamo tinklo struktūrinė schema

Lentelė 4 34 pav. tinklo apsaugos priemonės

Mazgo pavadinimas	Saugos sistemos
Maršrutizatorius 1	Jungtinė apsaugos sistema
Maršrutizatorius 2	Jungtinė apsaugos sistema
Serveris	Prieigos kontrolė
Darbo stotis 1	Ugniasienė
Darbo stotis 2	Ugniasienė
Darbo stotis 3	VPN, ugniasienė
SCADA	Ugniasienė, IPS
PLC 1	IPS
PLC 2	IPS, VPN
BYOD	IDS, ugniasienė

Pramoninio kompiuterinio tinklo svarbiausia grandis yra įmonės tinklo atskirtis nuo interneto. Šią funkciją atlieka 4.3 ir 4.4 skyriuose tirta Jungtinė tinklo apsaugos sistema su ugniasiene ir įsilaužimo aptikimo bei prevencijos priemonėmis. Nagrinėjamu atveju tai yra „Maršrutizatorius 1“. Siekiant visapusiškai apsaugti tinklą, kiekvienam objektui naudojama atskira saugumo sistema atsižvelgiant į jo pažeidžiamumą ir saugumui keliamus reikalavimus. 4.3 skyriuje pavaizduoto algoritmo tipo sistema atlieka ne tik ugniasenės, bet ir IDS ir IPS funkcijas. Iš rinkoje esančių pavyzdžių naudotinos Cisco ar McAfee Next Generation Firewall sistemos su ugniasiene, įsilaužimo aptikimo, prevencijos sistemomis, pranešimų skenavimo algorimais.

PLC ir SCADA sistemų apsaugai naudotinos ugniasienės ir IPS įrenginiai. Vieni tokių yra Cisco ASA 5500-X serijos gaminiai. Tikslus modelis parenkamas pagal naudojamą magistralės tipą, įrangą, reikalaujamą pralaidumą, įrenginių skaičių ir kitus parametrus. Jei PLC jungiamas belaidžiu ryšiu, itin didelio saugumo reiklaujančiose sistemose galima naudoti VPN, taip šifruojant siunčiamus duomenis.

Darbo stoties apsaugai naudojamos ugniasienės, jei tai pavienis kompiuteris, dauguma atvejų užtenka programinio tipo ugniasienės (2.5 skyrius). Papildomas pavojus darbo stotims ir SCADA sistemoms – BYOD (3.3 skyrius). Jei prisijungimas vyksta internetu, tinklą saugo įprastos saugumo sistemos, tačiau jungiantis tiesiogiai iškyla grėsmė užkrėsti įmonės tinklo įrenginį (ar patį tinklą) kenksminga programine įranga. Dėl to pačiame BYOD įrenginyje turi būti įdiegta ugniasienė bei IDS sistema.

Paprasčiausia serverio apsaugos priemonė yra slaptažodžių ir prisijungimo vardų naudojimas – prieigos kontrolė. Serveriams būtina kurti atsargines duomenų kopijas.

Išvados

1. Atlikta pramoninių kompiuterinių tinklų saugumo pažeidimų analizė, išskirti pagrindiniai saugumo pažeidimų tipai: pasyvios ir aktyvios atakos. Pasyvios atakos sunkiau aptinkamos, bet paprastesnė prevencija. Tuo tarpu aktyvių atakų prevencija sudėtinga dėl įvairesnių atakų būdų ir didesnės galimos žalos. Suklasifikuoti saugumo problemų sprendimo būdai: šifravimo metodai, VPN, ugniasienė, įsilaužimo aptikimo ir įsilaužimo prevencijos sistemos. Sudaryta standartinių tinklo mazgų apsaugos sistemų lentelė.
2. Sukurtas ugniasienės, IDS ir IPS sistemų Jungtinis algoritmas. Tai leidžia padidinti saugumo pažeidimo aptikimo galimybes dėl naudojamų keleto saugumo sistemų, tačiau išauga klaidingo atakos atpažinimo teigiamumo rizika.
3. Panaudojus *CAIDA Data Server* duomenis, aptikta DoS ataka, naudojant aptikimo pagal srautą (statistiką) metodą, aptikus 70% nesėkmingo prisijungimo bandymų. Sugeneravus prisijungimo prie nepatikimos internetinės svetainės pranešimų grafiką, aptiktas tinklo saugumo pažeidimas, kai momentinis pranešimų skaičius vidutinį viršija 1897% tame pačiame bandyme ir 3729% tame pačiame tinkle su patikimomis svetainėmis.
4. Matlab Simulink aplinkoje realizuotas atakos aptikimo algoritmas pagal pranešimų srautą (pps), aptikta apie 50-70% atakos laiko momentų. Šis algoritmas veikia nepatikimai, yra priklausomas nuo konkrečios sistemos. Šiuo atveju reikalinga analizė pagal antraštes ir pranešimo turinį.
5. Matlab Simulink aplinkoje realizuotas ugniasienės ir Jungtinės apsaugos sistemos palyginimas, kai pastarosios sistemos duomenų bazė atnaujinama aptikus ataką. Jungtinė apsaugos sistema veikia geriau, nes gali reaguoti į buvusių patikimų šaltinių atakas, kai jos aptinkamos už ugniasienės.

Literatūra

1. Die Lage der IT-Sicherheit in Deutchland 2014
http://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf
Žiūrėta 2015 m. sausio 21 d.
2. K. Zetter, An Unprecedented Look at Stuxnet, the World´s First Digital Weapon
http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
Žiūrėta 2015 m. sausio 21 d.
3. R. Walters, Cyber Attacks on U.S. Companies in 2014
http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014
Žiūrėta 2015 m. sausio 21 d.
4. 2013 – The Impact of Cybercrime
http://resources.infosecinstitute.com/2013-impact-cybercrime/
Žiūrėta 2015 m. sausio 22 d.
5. P. K. Gajar, A. Ghosh, S. Rai, Bring Your Own Device (BYOD): Security Risks And Mitigating Strategies, 2013
6. A. Serjantonov, P. Sewell, Passive-attack analysis for connection-based anonymity systems, 2005
7. Denial of Service Attacks
http://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html
Žiūrėta 2015 m. sausio 26 d.
8. What is the Difference: Viruses, Worms, Trojans, and Bots?
http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html
Žiūrėta 2015 m. sausio 27 d.
9. P. Gutmann, Network Security
http://www.windowsecurity.com/uplarticle/4/part1.pdf
Žiūrėta: 2015 m. sausio 28 d.
10. INTERNATIONAL STANDARD ISO/IEC 27000, Third edition 2014-01-15
11. Tinklo apsauga
http://tinklai.dkd.lt/administravimas/t.apsauga.htm
Žiūrėta 2014 m. birželio 4 d.
12. J. Newsome, E. Shi, D. Song ir kt., The Sybil Attack is Sensor Networks: Analysis & Defenses, 2004
13. Khabbazian M., Mercier H., Bhargava V. K., Wormhole Attack in Wireless Ad Hoc Networks: Analysis and Countermeasure, 2006

14. Soni V., Pratik M., Chaudhri V., Detecting Sinkhole Attack in Wireless Sensor Network, 2013
15. Song J., Mok A. K., Chen D. ir kt., Challenges of Wireless Control in Process Industry
16. Kriptografija
http://www.esecurity.lt/content/kriptografija
žiūrėta 2014 m. birželio 5 d.
17. Pathan A. S. K., Lee H. W., Hong C. S. Security in Wireless Sensor Networks: Issues and Challenges, 2006
http://arxiv.org/ftp/arxiv/papers/0712/0712.4169.pdf
žiūrėta 2014 m. birželio 11 d.
18. Types of VPNs
http://www.plathome.com/support/packetix/manual/10-1.htm
žiūrėta 2014 m. birželio 11 d.
19. P. Kazlenko, P. Dorosz, Intrusion Detection Systems (IDS) Part 2 – Classification; methods; techniques, 2004
http://www.windowsecurity.com/articles-tutorials/intrusion_detection/IDS-Part2-Classification-methods-techniques.html
Žiūrėta 2015 m. vasario 2 d.
20. Router Security Configuration Guide, Router Security Guidance Activity of the System and Network Attack Center (SNAC), 2001
21. Arana P. Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2), 2006
http://dl.irstu.com/wp-content/uploads/Download/Education/Book/Network/Network%20Security/WEP-WPA-Article/Benefits%20and%20Vulnerabilities%20of%20Wi-Fi%20Protected%20Access%202%20(WPA2).pdf
žiūrėta 2014 m. birželio 9 d.
22. P. Garcia-Teodoro, J. Diaz-Verdejo ir kt. Anomaly-based network intrusion detection: Techniques, systems and challenges, 2009
http://ac.els-cdn.com/S0167404808000692/1-s2.0-S0167404808000692-main.pdf?_tid=f17393bc-c7d3-11e4-baf9-00000aab0f6b&acdnat=1426067563_a0b6eecf085831fa8305d7adb7e8a496
žiūrėta 2015 m. kovo 11 d.
23. Security
http://www.cisco.com/c/en/us/products/security/index.html
žiūrėta 2015 m. kovo 14 d.

24. I. Bestak, M. Orgon, The use of encryption algorythms in PLC networks, 2013
25. Media Access Control (MAC)
http://compnetworking.about.com/od/networkprotocolsip/g/bldef_mac.htm
žiūrėta 2015 m. balandžio 27 d.
26. EAGLE20 Series Industrial Firewall/VPN Router System
http://www.belden.com/products/industrialnetworking/routers/eagle20firewallrouter.cfm
žiūrėta 2015 m. gegužės 3 d.
27. Cisco IPS Industrial Control Protection
http://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/ips_industrial_control_protection.pdf
žiūrėta 2015 m. gegužės 2 d.
28. C. Modi, D. Patel, B. Borisaniya ir kt., A survey of intrusion detection techniques in Cloud, 2012
http://www.sciencedirect.com/science/article/pii/S1084804512001178
žiūrėta 2015 m. gegužės 20 d.
29. CAIDA Data Server: Index of/datasets/security/backscatter/2008/11
http://data.caida.org/datasets/security/backscatter/2008/11/
žiūrėta 2015 m. gegužės 26 d.

1 Priedas

```
⊟ Frame 8: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 12, 2008 23:00:00.010201000 FLE Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1226523600.010201000 seconds
    [Time delta from previous captured frame: 0.000887000 seconds]
    [Time delta from previous displayed frame: 0.000887000 seconds]
    [Time since reference or first frame: 0.008954000 seconds]
    Frame Number: 8
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP RST]
    [Coloring Rule String: tcp.flags.reset eq 1]
⊟ Ethernet II, Src: Cisco_ee:e8:00 (00:0a:8b:ee:e8:00), Dst: Intel_9c:e2:31 (00:03:47:9c:e2:31)
  ⊟ Destination: Intel_9c:e2:31 (00:03:47:9c:e2:31)
      Address: Intel_9c:e2:31 (00:03:47:9c:e2:31)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: Cisco_ee:e8:00 (00:0a:8b:ee:e8:00)
      Address: Cisco_ee:e8:00 (00:0a:8b:ee:e8:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
    Padding: ab0000000000
⊟ Internet Protocol Version 4, Src: 60.28.2.79 (60.28.2.79), Dst: 0.102.102.75 (0.102.102.75)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 40
    Identification: 0xe798 (59288)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 107
    Protocol: TCP (6)
  ⊞ Header checksum: 0xc31b [validation disabled]
    Source: 60.28.2.79 (60.28.2.79)
    Destination: 0.102.102.75 (0.102.102.75)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 44327 (44327), Seq: 1, Ack: 1, Len: 0
    Source Port: 80 (80)
    Destination Port: 44327 (44327)
    [Stream index: 6]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
  ⊞ .... 0000 0001 0100 = Flags: 0x014 (RST, ACK)
    Window size value: 0
    [Calculated window size: 0]
    [Window size scaling factor: -1 (unknown)]
  ⊟ Checksum: 0xd7c2 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
    Urgent pointer: 0
```