Kauno technologijos universitetas

Informatikos fakultetas

Asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistema

Baigiamasis magistro krypties studijų projektas

Andrej Zagorodnij

Projekto autorius

Prof. dr. Jevgenijus Toldinas

Vadovas

Kaunas, 2020

Kauno technologijos universitetas

Informatikos fakultetas

Asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistema

Baigiamasis magistro krypties studijų projektas

6211BX008 Informacijos ir informacinių technologijų sauga

Andrej Zagorodnij

Projekto autorius

Prof. dr. Jevgenijus Toldinas

Vadovas

doc. Stasys Maciulevičius

Recenzentas

Kaunas, 2020

Kauno technologijos universitetas

Informatikos fakultetas

Andrej Zagorodnij

Asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistema

Akademinio sąžiningumo deklaracija

Patvirtinu, kad mano, Andrej Zagorodnij, baigiamasis projektas tema „Asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistema“ 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)

Zagorodnij, Andrej. Asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistema. Magistro krypties studijų baigiamasis projektas vadovas Prof. dr. Jevgenijus Toldinas; Kauno technologijos universitetas, informatikos fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Informacijos ir informacinių technologijų sauga.

Reikšminiai žodžiai: Asmeniniai įrenginiai, autentifikavimas, saugumas.

Kaunas, 2020. 69 p.

Santrauka

Šiais laikais vis dažniau pastebima tendencija, kad vis daugiau įmonių leidžia darbuotojams naudotis savo išmaniais įrenginiais. Nešiojamųjų kompiuterių našumo galimybės nenusileidžia, o kartais net ir pranoksta įmonės įrengtas kompiuterines darbo vietas. Tokia greita technologinio našumo kaita leidžia darbuotojui pasirinkti darbą ne ofiso aplinkoje, o iš jam patogios, namų arba kitos aplinkos, kurią jis pasiriks tinkamą atlikti savo pareigas.

Kai kurie darbuotojai pasirenka savo asmeninę įrangą dėl skirtingų priežasčių: kartais jį yra galingesnė negu įmonės siūlomą, arba darbuotojui tiesiog patogiau naudoti savo asmeninį įrenginį, kuris yra visada su jais. Kaip rodo Gartner vykdytos įmonių apklausos, BYOD politikos naudojimas įmonėse tampa vis dažniau sutinkama praktika. Naudojantis asmeniniais įrenginiais buvo pastebėtas darbuotojų produktyvumo bei satisfakcijos padidėjimas, papildomai leidžiant įmonei sutaupyti įrenginiu pirkimui bei darbuotojų darbo vietos priežiūrai.

Tipiškai BYOD apima tokius įrenginius kaip mobiliuosius įrenginius bei planšetinius kompiuterius, bet BYOD gali būti taikomas ir asmeniniams nešiojamiems kompiuteriams. Nors BYOD integracija įmonėje suteikia daug privalumų, įmonė privalo atsižvelgti ir į saugumo spragas. Prieš leidžiant BYOD įrenginių darbą įmonėje, turi būti sudarytas planas kaip apsisaugoti nuo tokių įrenginių, praradimo arba įsilaužimo atveju , valdyti juos bei autentifikuoti sistemoje. Dažniausiai saugiam prisijungimui prie įmonės infrastruktūros, įmonės naudoja VPN sprendimus, leidžiančius darbuotojams lengvai prisijungti prie visų jiems darbui reikalingų resursų. BYOD yra vienas iš populiaresnių strategijų, naudojamų įmonėse, leidžiančių asmeninių įrenginių naudojimą darbui.

Magistro darbo tyrimo objektas – mobiliųjų įrenginių saugaus autentifikavimo sistema.

Darbo struktūra:

- Pirmoje dalyje apžvelgiame nešiojamų įrenginių, naudojamų įmonėse, saugumo analizė. Analizėje detaliau išnagrinėjame minimų įrenginių pažeidžiamumus, kylančias saugumo grėsmes bei saugos technologijas, skirtas saugumo grėsmėms spręsti.
- Antroje dalyje pateikiamas asmeninių įrenginių, naudojamų įmonėse saugaus autentifikavimo sistemos modelis. Pateikiame sistemos architektūrą, kliento, serverio bei tarpinio brokerio komunikacijos schemos, bei sistemos veikimo proesus. Šioje dalyje pateikiame ir sistemos prototipo realizavimo aprašą.
- Trečioje dalyje yra tiriama autentifikavimo sistemos klaidingai autentifikuotų klientų rodiklis, esant dviem skirtingoms sistemos konfigūracijoms. Taipogi yra tiriama autentifikavimo sistemos greitaveika, kartu su neleistinų programų nutraukimo greitaveika bei nutrauktų programų veikimo rodiklis. Pagal gautus rezultatus yra sudaromos rekomendacijos kokia konfigūracija geriausia kokiam atvejui.
- Darbo pabaigoje pateikiamos išvados.

Zagorodnij, Andrej. Title Secure Authentication System of Enterprise Employee Owned Devices. Master's Final Degree Project, supervisor prof. dr. Jevgenijus Toldinas; Faculty of Informatics, Kaunas University of Technology.

Study field and area (study field group): Information and Information Technology Security.

Keywords: BYOD, authentication, security.

Kaunas, 2020. 69.

Summary

Nowadays, there is an increasing trend that more and more companies are allowing employees to use their smart devices. The performance of laptops is not inferior, and sometimes even surpasses that of enterprise workstations. Such a rapid change in technological performance allows an employee to choose a job not from an office environment, but from a comfortable, home, or other environment that he or she will choose to perform his or her duties.

Some employees choose their personal equipment for different reasons: sometimes it is more powerful than what the company offers, or the employee is simply more comfortable using their personal device that is always with them. According to Gartner's business surveys, the use of BYOD policies in companies is becoming an increasingly common practice. When using personal equipment, an increase in employee productivity and satisfaction was observed, additionally allowing the company to save on the purchase of equipment and maintenance of employees' workplaces.

BYOD typically includes devices such as mobile devices and tablets, but BYOD can also be applied to personal laptops. While BYOD integration offers many benefits to the company, the company must also consider security vulnerabilities. Before allowing BYOD devices to work in a company, a plan must be drawn up for how to protect such devices in the event of loss or burglary, how to manage them, and authenticate them in the system. Typically, to securely connect to a company's infrastructure, companies use VPN solutions that allow employees to easily connect to all the resources they need to work. BYOD is one of the more popular strategies used in businesses to allow the use of personal devices for work.

The object of the master's thesis research is a system of secure authentication of mobile devices.

Work structure:

- In the first part, we review the security analysis of portable devices used in enterprises. In the analysis, we examine in detail the vulnerabilities of the mentioned devices, emerging security threats and security technologies designed to address security threats.
- The second part presents a model of a secure authentication system for personal devices used in enterprises. We present the system architecture, client, server and proxy broker communication schemes, and system operation mechanisms. In this section, we also provide a description of the system prototype implementation.
- The third part examines the rate of false-authenticated clients of the authentication system with two different system configurations. The speed of the authentication system is also studied, together with the speed of termination of unauthorized programs and the performance indicator of terminated programs. Based on the obtained results, recommendations are made as to which configuration is best for which case.
- Conclusions are presented at the end of the work

Turinys

Lentelių sąrašas

Paveikslų sąrašas

Santrumpų ir terminų sąrašas

Santrumpos:

Dr. – daktaras;

Prof. – profesorius;

MDM – Mobiliųjų įrenginių valdymas (angl. *Mobile Device Management*);

MAM – Mobiliųjų programėlių valdymas (angl. *Mobile Application Management*);

MIM – Mobiliosios informacijos valdymas (angl. *Mobile information Management*);

BYOD – Atsinešk savo asmeninį įrenginį (angl. Bring Your Own Device) ;

AĮ – Asmeninis įrenginys;

IT – Informacinės technologijos;

OS – Operacinė sistema;

Wi-Fi – Belaidis internetas;

DES – Duomenų šifravimo standartas (angl. *Data encryption standard*) ;

AES – Pažangus šifravimo standartas (angl. *Advanced encryption standard*);

WMI – Windows valdymo instrumentai (angl. *Windows management instrumentation*);

IPSec – Internetinio protokolo apsauga (angl. *Internet Protocol Security*);

L2TP – Antrojo lygmens tuneliavimo protokolas (angl. *Layer 2 Tunneling Protocol*) ;

PPTP – Taškas į tašką tuneliavimo protokolas (angl. *Point-to-Point Tunneling Protocol*) ;

VPN – virtualus privatus tinklas (angl. virtual private network);

FPR – neteisingai atpažinti įrenginiai (angl. false positive rate).

Įvadas

Šiais laikais vis dažniau pastebima tendencija, kad vis daugiau įmonių leidžia darbuotojams naudotis savo išmaniais įrenginiais. Nešiojamųjų kompiuterių našumo galimybės nenusileidžia, o kartais net ir pranoksta įmonės įrengtas kompiuterines darbo vietas. Tokia greita technologinio našumo kaita leidžia darbuotojui pasirinkti darbą ne ofiso aplinkoje, o iš jam patogios, namų arba kitos aplinkos, kurią jis pasiriks tinkamą atlikti savo pareigas.

Kai kurie darbuotojai pasirenka savo asmeninę įrangą dėl skirtingų priežasčių: kartais jį yra galingesnė negu įmonės siūlomą, arba darbuotojui tiesiog patogiau naudoti savo asmeninį įrenginį, kuris yra visada su jais. Kaip rodo Gartner vykdytos įmonių apklausos, BYOD politikos naudojimas įmonėse tampa vis dažniau sutinkama praktika. Naudojantis asmeniniais įrenginiais buvo pastebėtas darbuotojų produktyvumo bei satisfakcijos padidėjimas, papildomai leidžiant įmonei sutaupyti įrenginiu pirkimui bei darbuotojų darbo vietos priežiūrai.

Tipiškai BYOD apima tokius įrenginius kaip mobiliuosius įrenginius bei planšetinius kompiuterius, bet BYOD gali būti taikomas ir asmeniniams nešiojamiems kompiuteriams. Nors BYOD integracija įmonėje suteikia daug privalumų, įmonė privalo atsižvelgti ir į saugumo spragas. Prieš leidžiant BYOD įrenginių darbą įmonėje, turi būti sudarytas planas kaip apsisaugoti nuo tokių įrenginių, praradimo arba įsilaužimo atveju , valdyti juos bei autentifikuoti sistemoje. Dažniausiai saugiam prisijungimui prie įmonės infrastruktūros, įmonės naudoja VPN sprendimus, leidžiančius darbuotojams lengvai prisijungti prie visų jiems darbui reikalingų resursų. BYOD yra vienas iš populiaresnių strategijų, naudojamų įmonėse, leidžiančių asmeninių įrenginių naudojimą darbui.

Saugos problemos apibrėžimas – situacija, kai darbuotojams leidžiama dirbti asmeniniais įrenginiais įmonės viduje. Asmeniniai įrenginiai tampa rimta saugumo spraga vidiniame įmonės tinkle taip kaip ne visada atitinka įmonės išsikeltus saugumo reikalavimus. Pasinaudoję tokiais įrenginiais piktavaliai gali pasisavinti įmonės konfidencialią informaciją, arba sutrikdyti įmonės darbą. VPN sprendimas tikrina tik įrenginio MAC adresą, neužtikrinant jog įrenginio vientisumas nebuvo pažeistas.

Magistro darbo tyrimo sritis – saugus nutolusiu vartotojų autentifikavimo ir autorizavimo valdymas organizacijose.

Magistrinio darbo tikslas – sukurti asmeninių mobiliųjų įrenginių, naudojamųjų įmonėse, saugaus vartotojo ir įrenginio autentifikavimo sistemą.

Darbo tikslui pasiekti išsikelti uždaviniai:

- Atlikti asmeninių įrenginių, naudojamųjų įmonėse , saugumo grėsmių ir spragų analizę
- Išnagrinėti asmeninių įrenginių saugos užtikrinimo priemones
- Sudaryti asmeninių įrenginių, naudojamų įmonėse, saugaus vartotojo įrangos autentifikavimo sistemos modelį
- Remiantis sudarytu modeliu, realizuoti sistemos prototipą ir atlikti prototipo tyrimą

1. Asmeninių įrenginių, naudojamų įmonėse, saugumo analizė

Dėl padidėjusio mobiliųjų įrenginių patogumo, efektyvumo ir produktyvumo, vis daugiau ir daugiau organizacijų ieško būdų įsidiegti asmeninius įrenginius savo informacinių technologijų (IT) infrastruktūrose, norėdami pasinaudoti šių įrenginių teikiamu lankstumu. Nors ir daug dėmesio yra skiriama pačių įrenginių operacinių sistemų ir programų saugumui, tačiau juose vis tiek išlieka daug pažeidžiamumu, tokiu kaip [6]:

- Tiesioginės įsilaužėlių atakos
- Tinklo srauto perėmimas
- Neteisinga vartotojų elgsena
- Piktavališkos programėlės
- Pavogti arba pamesti įrenginiai

Dėl paminėtų ir nepaminėtų saugumo spragų, įmonėms gali iškilti tokios problemos, kaip:

- Asmeninės ir konfidencialios informacijos atskleidimas tretiesiems asmenims.
- Įmonės resursų išnaudojimas įsilaužėliais.
- Darbo nutraukimas įsilaužimo likvidavimo laikotarpiui.

1.1. Bendros saugumo problemos

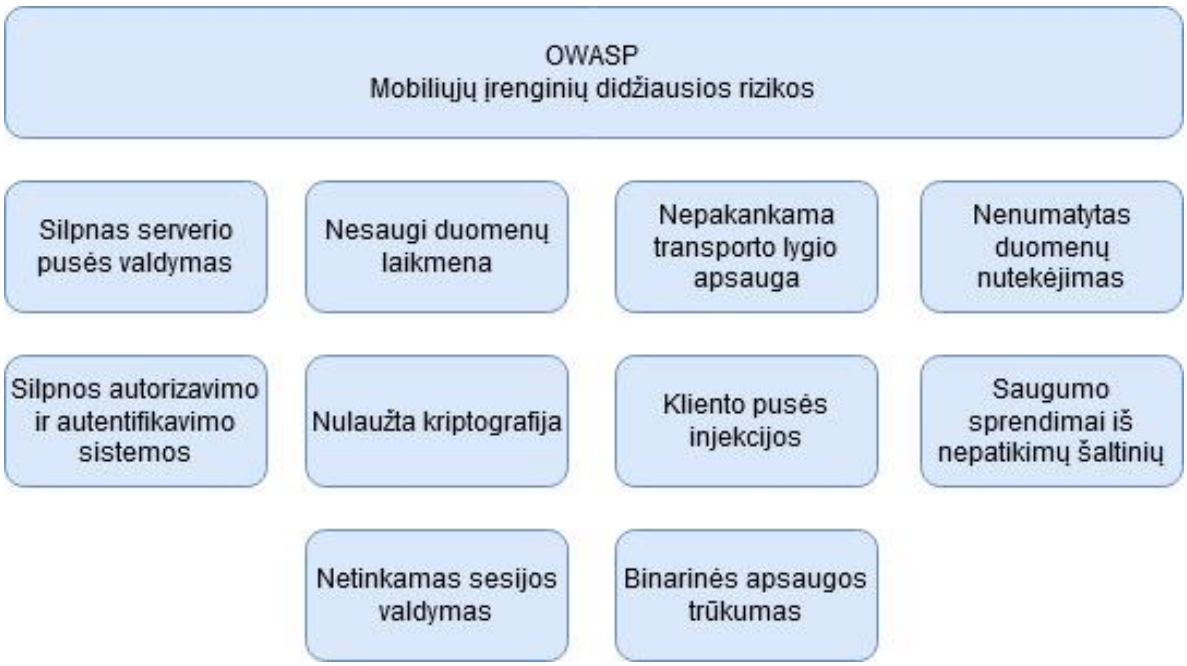
Įmonės duomenys yra vienas iš svarbiausių jos resursų. Įdiegus BYOD dramatiškai padidėjo puolimo galimybių saugumo atžvilgiu, atsirado didelė galimybė prarasti konfidencialią įmonės bei kliento informaciją.

Keletas reikšmingų punktų susijusių su BYOD informacijos saugos problemomis [1, 2, 3, 6]:

- Didėjantis asmeninių įrenginių, naudojančių įmonės resursus, skaičius.
- Spartus BYOD plėtimasis apsunkina probleminių zonų apsaugą.
- Įmonės bei jos klientų duomenis yra laikomi asmeniniuose įrenginiuose.
- Asmeninio įrenginio praradimas

Kaip rodo 2013 metų informacijos saugumo apklausos rezultatai, pagrindiniai trys saugumo susirūpinimai – kliento arba įmonės duomenų praradimas (75 proc.), neautorizuotas priėjimas prie įmonės resursų (65 proc.), kenkėjiškų programų užkrėtimai (47 proc.).

OWASP [6] pateikė 10 didžiausių mobiliųjų įrenginių saugumo rizikos šaltinių, kurios yra pateiktos 1 paveikslėlyje. Kiekvieną jos nišą aptarsime sekančiose skiltyse [4].



1 pav. OWASP Mobiliųjų įrenginių didžiausios rizikos

Silpnas serverio pusės valdymas

Šis pažeidžiamumas atitinka susijusio pažeidžiamumo techninį poveikį, kurį priešininkas naudoja per mobilųjį įrenginį. Pavyzdžiui, puolėjas gali išnaudoti „*Cross-Site Scripting*“ (XSS) pažeidžiamumą per mobilųjį prietaisą.

Nesaugi duomenų laikmena:

Nesaugi duomenų laikmena gali privesti prie duomenų praradimo, geriausiu atveju vienam vartotojui, blogiausiu – daugeliui vartotojų. Dažniausiai pasitaikanti svarbi informacija yra autentifikavimo raktai, slaptažodžiai, slapukai, vietos duomenys, perdavimo istorija, vartotojo prisijungimo vardas bei konfidenciali informacija.

Nepakankama transporto lygio apsauga:

Šita spraga atskleidžia individualius vartotojo duomenis ir gali leisti piktavaliui pavogti vartotojo paskyrą. Jeigu puolėjas perima administratoriaus paskyrą, visa sistema gali būti kompromituota. Silpna SSL sąranka gali palengvinti sukčiavimo (*phishing*) ir MITM puolimus.

Nenumatytas duomenų nutekėjimas:

Šis pažeidimas gali pavirsti tokiais galimais techniniais poveikiais: jautrios informacijos atskleidimas per kenkėjišką programą, modifikuotos programos arba sekimo programėlės.

Silpnos autorizavimo ir autentifikavimo sistemos:

Autentifikavimo sistemos sutrikimai gali atskleisti esmines autorizavimo problemas. Kai autentifikavimo valdymas sutrinka, jis negali nustatyti vartotojo identiteto. Kiekvieno vartotojo identitetas yra susietas su jam priskirta role ir ją lydinčiomis teisėmis. Jeigu piktavalis gali anonimiškai vykdyti kritines komandas, tai parodo jog programos kodas netikrina vartotojo leidimų vykdyti komandą.

Nulaužta kriptografija:

Šį spraga leis neautorizuotą konfidencialios informacijos ištraukimą iš asmeninio įrenginio.

Kliento pusės injekcijos:

Injekcijos puolimai, tokie kaip SQL injekcijos puolimas prieš asmeninį įrenginį gali būti skausmingas jeigu programa dirba su daugiau negu viena vartotojo paskyra vienoje programoje, bendrame (angl. *shared*) įrenginyje arba mokamame turinyje. Kiti injekcijos taškai yra skirti perpildyti programos komponentus, tačiau mažiau tikėtina jog pasieks didelio poveikio dėl kodo valdymo apsaugos naudojamos skirtingose programavimo kalbose.

Saugumo sprendimai iš nepatikimų šaltinių:

Saugumo sprendimai gauti iš nepatikimo šaltinio kompromituoja viso saugumo modelio arba saugumo architektūros prasmę. Nežinant iš kokio šaltinio atėjo saugumo nustatymai negalime teigti jog jų neatsiuntė piktavalis.

Netinkamas sesijos valdymas:

Netinkamas sesijos valdymas atsiranda tada, kai sesijos raktas yra nesąmoningai perduodamas puolėjui vykstant duomenų perdavimui tarp mobiliosios programėlės ir vidinio serverio. Blogiausiu atveju, puolėjas išduoda save už sistemos administratorių bei siunčia užklausas abiem dalyviams administratoriaus teisėmis, kas gali turėti katastrofiškų pasekmių.

Binarinės apsaugos trūkumas:

Binarinė apsauga neleidžia puolėjui keisti pagrindinį programos kodą ar jos elgesį leidžianti jam pridėti papildomą arba atjungti jau esamą funkcionalumą. Tai gali įvykti jei programa saugo , perduoda arba tvarko asmeninę informaciją ar kitą konfidencialią informaciją tokia kaip slaptažodžius arba kreditines korteles informaciją. Kodo modifikacijos dažniausiai atrodo kaip kenkėjiškos informacijos įpakavimas ar įterpimas į jau esamas mobiliąsias programas.

1.2. BYOD puolimo vektoriai

Norint jog pasirinkti saugumo sprendimai optimaliai galėtu apsaugoti sistemą BYOD aplinkoje, turime nustatyti bei kategorizuoti į skirtingas kategorijas potencialius puolimo vektorius, kuriais pasinaudojus piktavaliai gali įvykdyti puolimus prieš asmeninius įrenginius. Šioje skiltyje apžvelgsime potencialius puolimo vektorius [6, 10].

Pamesti arba pavogti mobilus įrenginiai:

Mobilius įrenginius yra ganėtinai lengva pamesti arba pavogti ir neatrodo kad kažkas šituo klausimu greitai pasikeis. Taipogi, kaip patogumo pasekmė, mobiliuosiuose įrenginiuose yra laikoma daug asmeninės bei konfidencialios įmonės informacijos. Statistika rodo, apie 1.3 milijardo mobiliųjų telefonų yra pavagiama kiekvienais metais tik jungtinėje karalystėje. Be to , didelės Jungtinių valstijų korporacijos kiekvieną savaitę praranda 1075 išmaniuosius telefonus ir 640 nešiojamus kompiuterius. Prarasti įrenginiai yra atsakingi už didelę sumą prarastų duomenų. Remiantis tuo galime teigti jog prarasti ar pavogti asmeniniai įrenginiai kelia didėlę grėsmę visam BYOD aplinkos saugumui.

Slaptas pasiklausymas:

Mobilieji įrenginiai yra labai pažeidžiami per bendrus pažeidžiamumus ir spragas (angl. Common vulnerabilities and exposures, CVE) ir greičiausiai yra užkrėsti slapto pasiklausymo programomis. Kartu su belaidžiu ryšiu, puolėjai gali operuoti mobiliuoju tinklu ir gali pasiklausinėti per tinklą, kas gali atskleisti įmonės informacija. Panašiai kaip ir anksčiau minėtas pavyzdys, bet kokia informacija pvz. el. paštas ir slaptažodžiai perduodami LAN arba belaidžiu tinklu gali būti perimti .

SQL injekcijos:

SQL injekcijos naudojasi kodo injekcijos technikomis kurios yra nukreiptos prieš programas ir interneto puslapius, stengiamasi įdiegti informacija vagiančias kenkėjiškas programas. SQL injekcijos puolimas buvęs ne kartą pagrindine duomenų centro saugumo incidento priežastimi, dėl BYOD tendencijų darbovietėje. Dėl tendencijos naudoti asmeninius įrenginius darbo aplinkoje, įdiegus BYOD tapo kur kas sunkiau atsekti SQL injekcijos šaltinį.

Pažangi pastovioji grėsmė:

Pažangi pastovioji grėsmė (angl. *Advanced Persistent Threat*, toliau APT) yra slaptų ir nepertraukiamų (angl. *continuous*) nulaužimo procesų rinkinys. APT dažniausiai kėsinasi į organizacijas ar įmones pasipelnymo tikslais. Tačiau skirtingai negu trumpi greitai įvykdomi puolimai, APT puolimai reikalauja aukšto lygio slaptumo ilgam laiko tarpui. APT susideda iš trijų pagrindinių komponentų : pažangumo (angl. *Advanced*), atkaklumo (angl. *Persistent*) ir grėsmės (angl. *threat*). Puolėjai pasinaudoja APT puolimo strategija tuo atveju, kai randa anomalinį srautą tinkle. BYOD gali leisti neautorizuotiems asmenims prisijungti prie serverio, kuo pasinaudoję puolėjai gali rasti nešifruotus duomenis tinkle , kuriu pagalbą bus vykdomas APT tipo puolimas.

Įmonės bei kliento duomenų saugumas:

Asmeninio įrenginio duomenų srauto bei programų sekimas sukelia teisinių klausimų apie duomenų privatumą. Dauguma keblumu iškylą dėl įmonės BYOD politikos, kokiu lygiu prižiūrimi asmeniniai įrenginiai, ką gali ir ko negali daryti darbdavys. Įmonei yra labai sunku įsitikinti jog kliento ar įmonės informacija nenutekės per įmonės darbuotojų šeimos narius, kurie taipogi gali naudoti tą patį įrenginį kaip ir darbuotojas darbo aplinkoje. Tai tampa labai dideliu saugumo susirūpinimu , taip kaip įrenginiai gali būti naudojami BYOD aplinkoje darbo ir ne darbo aplinkoje bei darbo ir ne darbo laiku.

Socialinė inžinerija:

Socialinė inžinerija yra puolimo technika skirta konfidencialios informacijos gavimui psichologinio manipuliavimo pagalba. Pagrindinė puolėjo užduotis yra pasinaudojus socialinės inžinerijos pagalba gauti konfidencialią ir brangią informaciją. Vienos iš dažniausiai pasitaikančių socialinės inžinerijos puolimų BYOD aplinkoje yra sukčiavimas ir apgaulingos kenkėjiškos programos. Kenkėjiškos nuorodos ir neautorizuotos mobiliosios programos yra pagrindiniai puolimo vektoriai kuriais pasinaudoja puolėjai , tokios rūšies puolimai yra priskiriami prie socialinės inžinerijos.

Kenkėjiškos programos:

Pastaraisiais metais augant kenkėjiškų programų bei užkrėstų įrenginių skaičiui, kenkėjiškos programos tapo viena iš pagrindinių grėsmių įmonėms kurios praktikuoja BYOD aplinka. Skirtingi puolimo vektoriai yra prieinami kenkėjiškoms programoms įvykdyti savo puolimus, ypač BYOD aplinkose , kur įrenginių ir vartotojų skaičiai gali tapti sunkiai valdomais.

Saugaus prievado lygio puolimai (SSL):

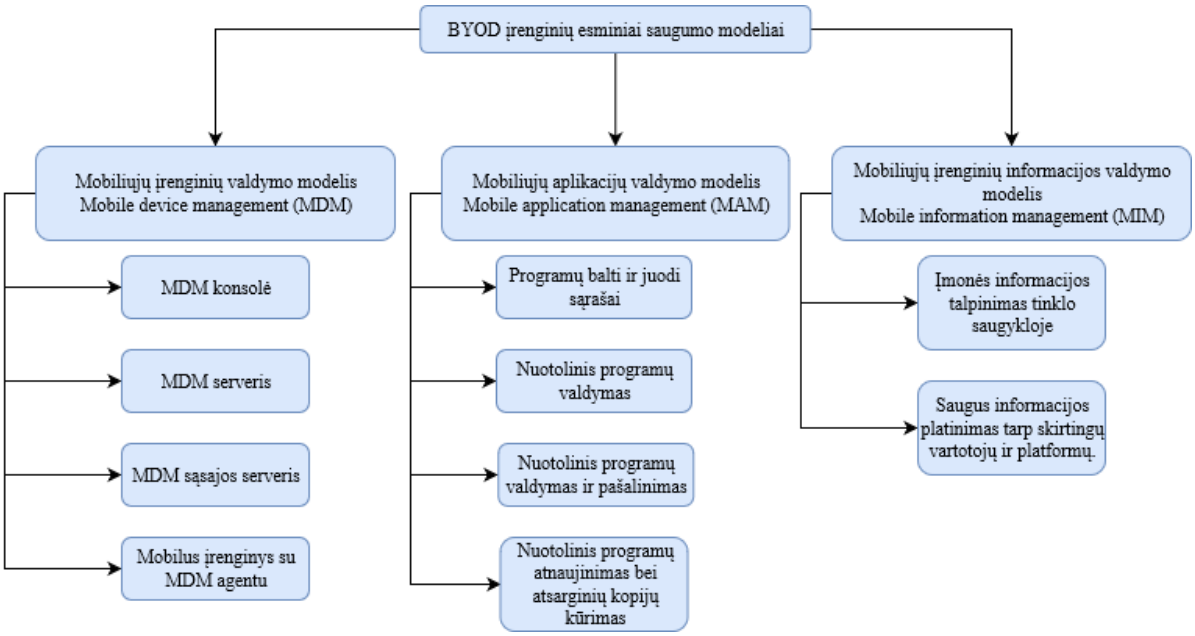
Saugaus prievado lygio puolimas yra orientuotas į tinklo protokolo silpnybių pažeidimą. SSL/TLS yra pagrindinis protokolas kuri puolėjai pasirenka savo puolimo vykdymui. „*Heartbleed*“ yra geriausia atvejo analizė skirta pademonstruoti pagrindinius šio puolimo tikslus. „*Heartbleed*“ protrūkio pasekmėje, viena trečioji visų pasaulio serverių prisijungimo vardų ir slaptažodžių buvo nulaužti. BYOD aplinkoje šis puolimas yra labai efektyvus prieš mažai arba visiškai neapsaugotus įrenginius , kuriuose yra įmonės duomenų. Kaip pavyzdį paimsime Android versija 4.1.1 kuri yra pažeidžiama „*Heartbleed*“ pažeidimu. 2014 metais buvo apskaičiuota jog 50 milijonų vartotojų buvo užkrėsti šio protrūkio.

1.3. Saugumo technologijos

Šiuo metu egzistuoja trys esminiai BYOD įrenginių saugumo valdymo moduliai [5, 8, 11] :

- *Mobile device management* (MDM) – mobiliųjų įrenginių valdymas:
  - Mobilus įrenginys su valdymo agentu.
  - MDM įrenginio valdymo sąsajos serveris.
  - MDM įrenginių valdymo aplinka.
- *Mobile application management* (MAM) – mobiliųjų programų valdymas:
  - Programų baltieji ir juodieji sąrašai.
  - Nuotolinis programų valdymas.
  - Nuotolinis programų konfigūravimas ir pašalinimas.
  - Nuotolinis programų atnaujinimas bei atsarginių programų kopijų kūrimas.
- *Mobile information management* (MIM) – mobiliosios informacijos valdymas:
  - Įmonės informacijos talpinimas tinklo saugykloje.

– Saugus informacijos platinimas tarp skirtingų vartotojų ir platformų.



2 pav. Mobiliųjų įrenginių saugumo modeliai

1.3.1. Mobiliųjų įrenginių valdymas

Mobiliųjų įrenginių valdymas leidžia įmonėms valdyti , sekti , apsaugoti bei palaikyti įmonei ir darbuotojams priklausančius įrenginius, naudojamus darbo aplinkoje. MDM funkcionalumas tipiškai apima nuotoliniu būdu paskirstytas programas, duomenis ir konfigūracijos nustatymus visų asmeninių įrenginių. Valdydama ir apsaugodama duomenis ir konfigūracijos nustatymus tinkle, MDM gali sumažinti palaikymo kaštus ir verslo rizikas. Pagrindinė MDM paskirtis yra optimizuoti asmeninių įrenginių funkcionalumą įmonėje ir apsaugoti įmonės tinklą nuo galimų puolimų.

Gartnerio magiškojo kvadrato MDM programinės įrangos sudėtinių dalių ataskaita parodo esmines MDM sudedamąsias dalis:

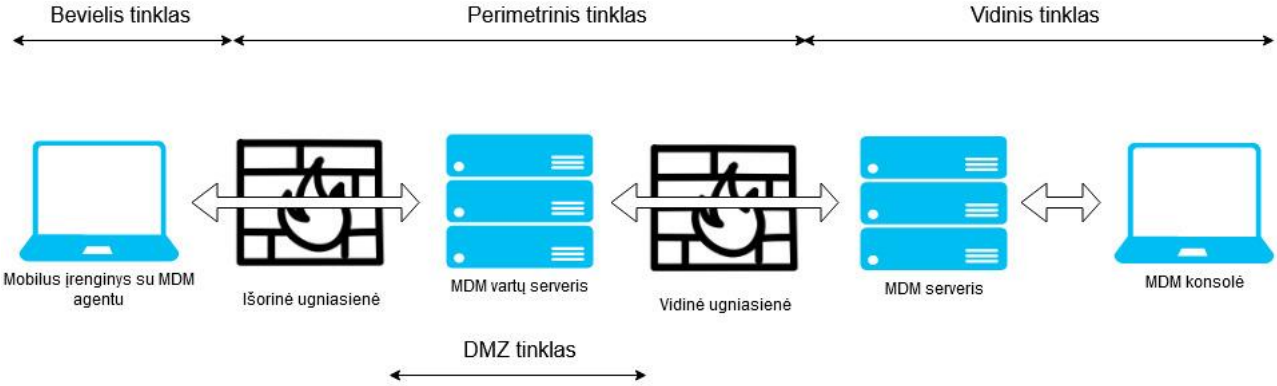
– Programinės įrangos valdymas: galimybė valdyti ir palaikyti mobiliąsias programas, duomenis ir operacines sistemas.
– Tinklo paslaugų valdymas: galimybė gauti informaciją iš įrenginių kurie gauna vietovės , naudojimo ir belaidžio tinklo informaciją, naudodama GPS technologijas. Tinklo prieigos valdymo funkcijos taip pat randamos čia.
– Techninės įrangos valdymas: apima įrenginių aprūpinimą ir palaikymą.
– Saugumo valdymas: standartinio duomenų autentifikavimo ir šifravimo saugumo priverstinis vykdymas ir palaikymas.

MDM platforma siūlo platų saugumo funkcijų pasirinkimą:

– Priverstinė stiprių įrenginio slaptažodžių naudojimo politika: užtikrina, jog įrenginys gali būti pasiekiamas tik po to kai yra naudojamas atitinkamo sudėtingumo slaptažodis.
– Duomenų šifravimas: įrenginio duomenų šifravimo galimybių naudojimas.

– Nuotolinis įrenginio užrakinimas arba ištrynimas: galimybė nuotoliniu būdu užrakinti arba pilnai ištrinti visus konfidencialius duomenis iš pamesto arba pavogto įrenginio.
– Komunikacijos: leidžia sukonfigūruoti *Wi-Fi* ir VPN nustatymus.
– Netinkamos ir kenkėjiškos programos : galimybė valdyti , blokuoti ir pašalinti nežinomas programas nešiojamuosiuose įrenginiuose kartu užtikrinant didelį produktyvumą ir mažinant kenkėjiškų programų rizikas.

MDM sistemos nuotoliniu būdu stebi nešiojamų įrenginių būklę, kartu leidžia valdyti jų funkcijas. MDM sistema yra sudaryta iš kelių komponentų, tokių kaip MDM serveris, MDM tinklo vartų serveris, MDM konsolės ir nešiojamųjų įrenginių agentas. Paveikslėlyje 3 matome bazine MDM sistemos schema naudojama įmonės tinkle.



3 pav. Bazinė MDM architektūrą

Šioje architektūroje , MDM tinklo vartų serveris yra pagrindinis valdomų įrenginių prieigos taškas. Tipiškai šis serveris yra diegiamas įmonės vidinio tinklo perimetre, kur yra naudojama giluminės apsaugos metodas, kuris padeda apsaugoti tinklo saugumą. MDM agentas yra programėlė kuri diegiama nešiojamuosiuose įrenginiuose ir ji persiunčia savo būklę ir duomenis MDM serveriui. MDM serveris valdo gautus duomenis ir atitinkamai taiko saugumo politikas ir administracines operacijas registruotuose įrenginiuose. Tačiau įrenginiai, naudojantys Apple iOS operacinę sistemą negali naudoti agentų. Tai yra Apple operacinės sistemos dizaino apribojimai. iOS įrenginių valdymas yra realizuotas konfigūracijos profiliais.

MDM agentas yra naudojamas gauti prieiga prie belaidžio BYOD tinklo. Jeigu MDM agentas yra aptinkamas, įrenginiui kuriame jis įdiegtas leidžiama prieiga prie įmonės resursų. Jeigu agento nėra, įrenginys yra prijungiamas prie viešojo „svečių“ tinklo. Nulaužtiems iOS bei Android įrenginiams yra uždraudžiamas priėjimas prie tinklo, įskaitant ir „svečių“ tinklą. Įrenginio nulaužimo būklę nustato MDM agentas.

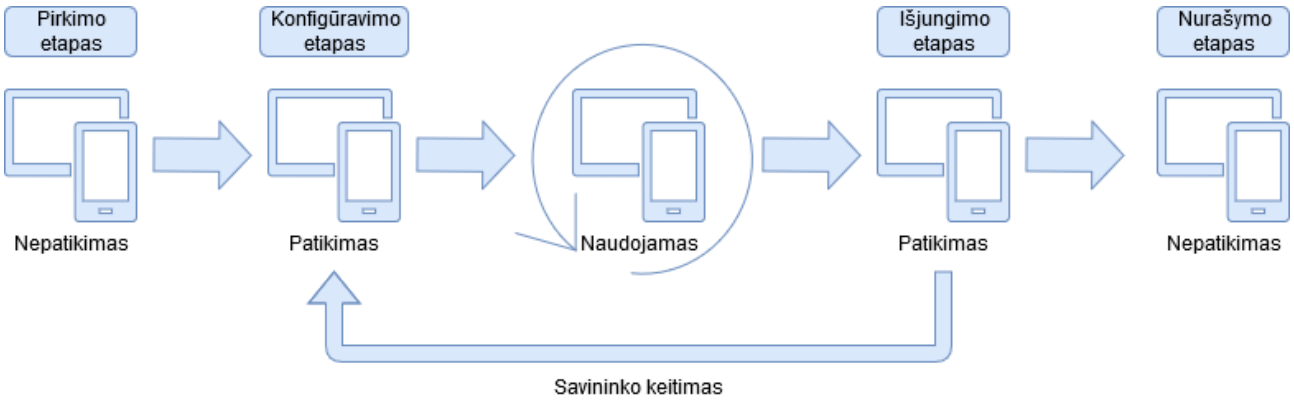
MDM sistemų pasirinkimas neapsiriboja anksčiau paminėta sistema. Jos gali būti kaip ir vidinės MDM (kaip ir paminėta anksčiau) , debesų kompiuterija grįsta MDM sistema arba hibridine sistema, kuri turi abiejų sistemų elementų. Valdymo paslaugos yra prieinamos ten kur valdymo funkcijos yra pateiktos trečiąją šalimi. MDM veikimas realizuotas per kliento ir serverio valdymą. Nešiojamasis įrenginys turi palaikyti MDM klientą (programėlę arba agentą) per diegimo procesą kuris įdiegia klientą ir komunikuoja su MDM serveriu.

MDM saugumo valdymas:

BYOD politika yra neatsiejama saugumo sumažinimo ir koncerno dalis [7, 8, 9]. Kiekviena organizacija privalo susikurti saugumo politikas, kurios yra pritaikytos jos unikaliems poreikiams bei situacijoms. Keičiantis technologijoms, politikos susijusios su jomis turi irgi keistis. Mobiliojoje industrijoje pokyčiai yra spartesni negu bendrojoje IT industrijoje ir valdymo procesai, kurie valdo nešiojamuosius įrenginius turi būti atnaujinti, kad jie galėtų atitinkamai reaguoti į naujas saugumo rizikas, sukurtas tokių pokyčių. MDM yra techninis mobiliųjų įrenginių bei programų valdymo sprendimas ir privalo būti BYOD politikos dalimi. MDM sprendimai, kurie pateikia centralizuotą mobiliųjų įrenginių valdymą, gali automatizuoti ir valdyti patvirtintus įrenginius, remdamiesi saugumo politikomis ir gali imtis veiksmų, atsakydami į politikos nesilaikymą. MDM technologijos gali būti naudojamos įrenginiui sekti, tai padeda aptikti veiksmus, kurie neatitinka saugumo politika. Įmonės politika turi įvertinti vartotojo įrenginio praradimo arba vagystės atvejį, kuriuo jis naudojosi įmonės resursams pasiekti. MDM sistema taipogi gali pasiūlyti atsako strategiją – ištrinti įmonės informaciją arba išvalyti visą prarastą įrenginį nuotoliniu būdu. Sujungus MDM sistemą su NAC sprendimais, galima optimizuoti įmonės susisiekimo ryšių funkcionalumą bei saugumą.

Vadovaujantis NIST rekomendacijomis, ne mažiau svarbu yra atsižvelgti į kiekvieno mobiliojo įrenginio gyvavimo ciklą. Ciklo struktūrą nėra visiškai atitinkanti projektų valdymo metodologijos arba produkto gyvavimo ciklo schemos, tačiau struktūra, ciklo etapai ir eilės tvarka atitinka daugelį produkto gyvavimo ciklų. Pateiktoje rekomendacijoje yra įvardijami 5 produkto gyvavimo ciklo etapai[12]:

1. inicijavimo etapas (įrenginio pirkimo fazė);
2. konfigūravimo etapas;
3. naudojimo etapas;
4. išjungimo etapas;
5. nurašymo etapas.



4 pav. Produkto gyvavimo ciklo etapai

Gyvavimo cikle įrenginio būsena gali kisti tarp trijų skirtingų būsenų: nepatikimas, patikimas ir naudojamas [12, 5].

Pirmajame etape yra įvertinami norimi įsigyti įrenginiai, įvertinamos jų saugumo spragos, kaip įrenginiai paveiks tolimesnį įmonės darbą. Įvertinami visi įmanomi aspektai, kurie gali paveikti įmonės saugumą bei įrenginio apsaugojimo galimybes nuo anksčiau išvardintų grėsmių.

Antrajame etape yra įvardijamos techninės specifikacijos, skirtos nuotolinio darbo su įmonės resursais sprendimo ir su sprendimu susijusių komponentų įgyvendinimu. Techninė specifikacija apima savyje tokias dalis kaip: autentifikavimo metodus, kriptografinius procesus, skirtus užtikrinti saugią komunikaciją tarp įrenginių, bei kitus sprendimus, užtikrinančius tinklo bei įmonės resursų saugumą. Turime nepamiršti įvertinti ir sistemos vartotojų skirtingų tipų ir profilių, taip kaip tai gali paveikti saugos politikos pasikeitimus. Turi būti užtikrinta, jog visiems vartotojams yra taikomos atitinkamos saugumo politikos, nepriklausomai nuo jų pareigų įmonėje.

Trečiajame etape įranga yra konfigūruojama pagal iškeltus įmonės saugumo reikalavimus. Pirma yra išbandomas įrangos prototipas, kuris turi parodyti esamas saugumo politikos ir sprendimo spragas. Tik įsitikinus jog visos spragos yra pašalintos, galima įrenginį aktyvuoti produkcinėje aplinkoje.

Ketvirtame etape yra įgyvendinamos saugumo politikos. Saugos politikos yra vykdomos reguliariu grafiku, tikrinant tokius parametrus kaip žurnalinių įrašų tikrinimas, puolimų nustatymas bei atsakas į incidentus bei atstatymas po incidentų. Nustačius pažeidimo faktą, įrenginys yra pašalinamas iš sistemos.

Penktajame etape yra vykdomos visos užduotys, kurios skirtos senų komponentų bei įrangos nurašymui. Užduotys privalo atlikti įrenginio informacijos ištrynimą arba jos išsaugojimą jei to reikalaujama įstatymais. Įrenginio nurašymas turi atitikti visus senos įrangos utilizavimo įstatymus.

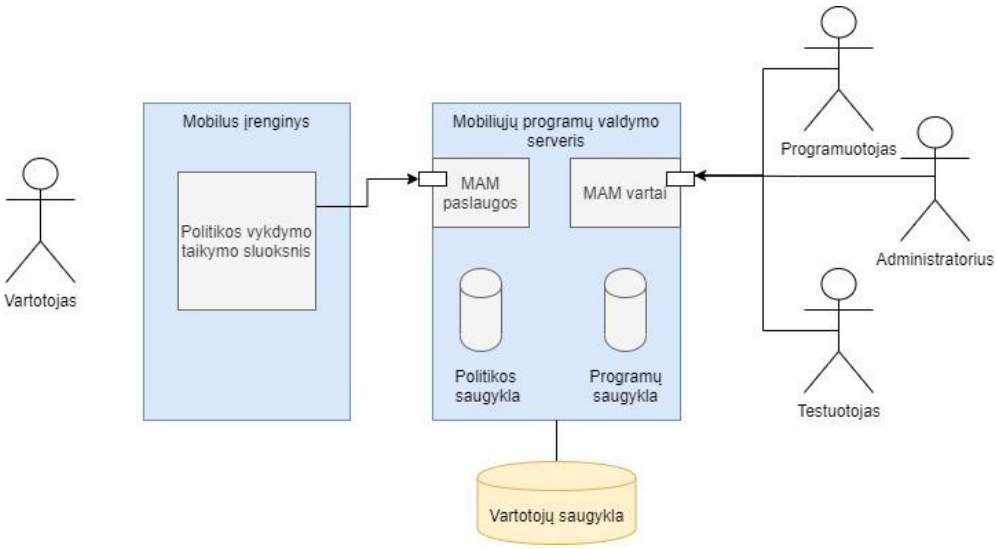
1.3.2. Mobiliųjų programų valdymas

MDM leidžia saugumo nustatymus vartoti įrenginio lygyje [13]. Tai yra reikalinga norint pasiūlyti įrenginio lygio apsaugą, tokia kaip priverstinis IT politikos laikymasis, nuotolinis įrenginio uždarymas arba ištrynimas, atitikties stebėsena ir įrenginio naudojimas. Tačiau didesnis dėmesys yra skiriamas programų lygio apsaugai ir duomenų saugumui. Mobiliųjų programų valdymas (toliau MAM) yra įrankių bei technologijų rinkinys, kuris padeda apsaugoti informaciją kuri yra tiek įrenginyje, tiek yra pasiekiama iš jo. MAM leidžia įmonėms sumažinti prieigą prie nepatvirtintų mobiliųjų programėlių, valdyti prieigą prie leidžiamų programų, saugiai diegti juos įrenginiuose bei nustatyti programinės įrangos elgesio politikas.

Skirtingai nuo MDM , MAM leidžia valdyti programinės įrangos prieigą. MDM ir MAM papildo vienas kitą, įmonei reikia abiejų įrenginio lygio (MDM) ir programų lygio (MAM) apsaugos, norint visapusiškai apsaugoti nešiojamuosius įrenginius.

MAM siūlo daugybę saugumo funkcijų, tokiu kaip :

- Programinės įrangos lygio saugumo politikos priverstinis naudojimas
- Leidžiamų (angl. *Whitelist*) arba blokuojamų (angl. *Blacklist*) programų paleidimas.
- Paskirstyti mobiliąsias programas nešiojamiems įrenginiams automatizuotu ir valdomu būdu.
- Automatiškai atnaujinti mobiliąsias programas.
- Stebėti ir pranešti apie mobiliųjų programų naudojimą.
- Integracijos su MDM.

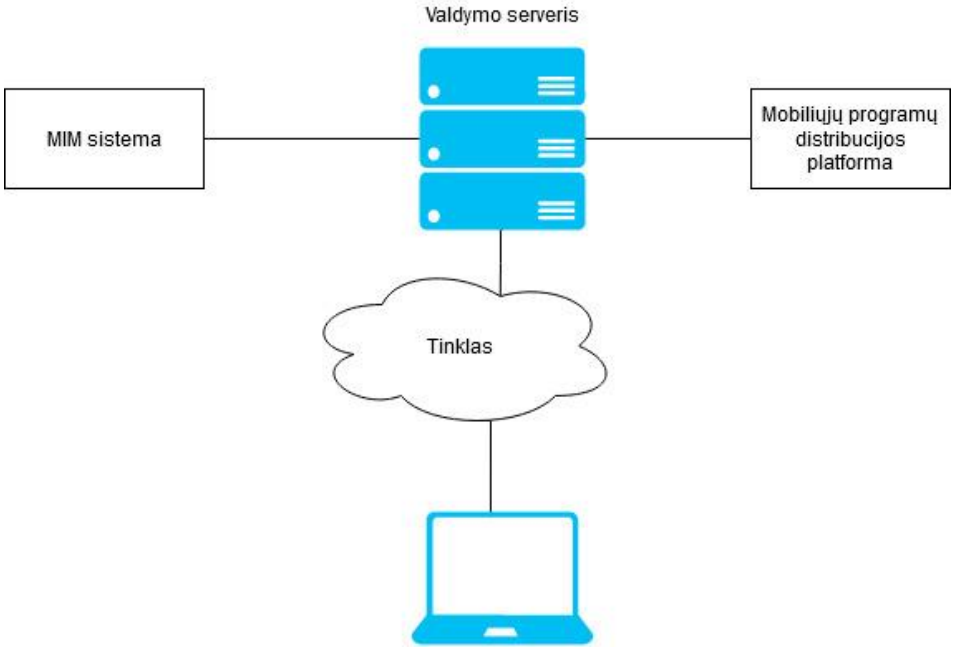


5 pav. MAM sistemos architektūra

MAM yra naudojamas nuotoliniu būdu įdiegti programinę įrangą BYOD įrenginiuose. Be nuotolinio programų stebėjimo, IT administratoriai taipogi gali audituoti bei stebėti esamą programų būklę mobiliuosiuose įrenginiuose. Tačiau ne visos programos papuola į MAM valdomųjų akiratį. Pateiktoje schemoje (5 pav.) matome tik įmonės valdomų programėlių sistemos schemą.

1.3.3. Mobiliosios informacijos valdymas

Mobiliosios informacijos valdymo sistema (MIM) yra skirta informacijos integralumui bei šifravimui užtikrinti, kartu atliekant prieigos prie informacijos valdymą: įrenginiams, programoms ir vartotojams [14]. Skirtingai nuo MDM ir MAM , MIM neatlieka įrenginio valdymo funkcijų, tačiau gali teikti saugumo administravimo funkcionalumą, pvz., kenkėjiškų programų skenavimą.



6 pav. MIM sistemos architektūra

Įmonės duomenys yra saugomi vienoje, nutolusioje vietoje, tokioje kaip debesų serveris. Visi duomenys saugomi nutolusiame serveryje yra prieinami vadovaujantis saugumo politikos

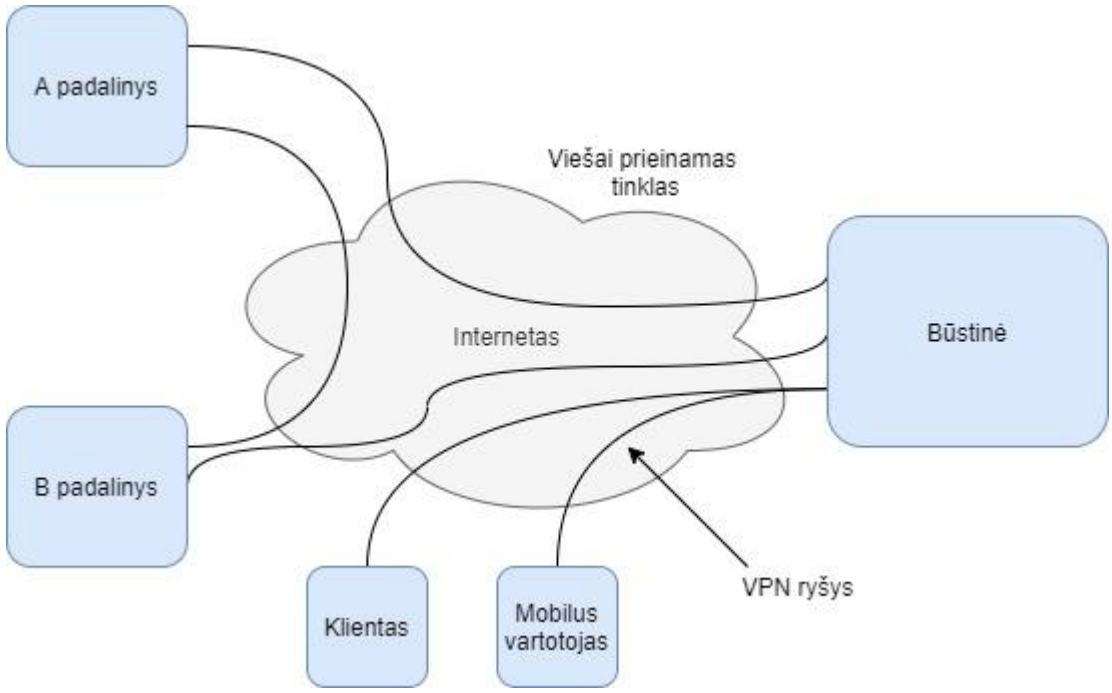
nustatymais bei saugumo nustatymais programose bei įrenginiuose. MIM sinchronizuoja duomenys tarp visų įrenginių panašiai kaip debesų duomenų saugyklos, taip kaip duomenys yra laikomi centralizuotoje virtualioje aplinkoje.

1.4. VPN saugumas

Virtualus privatus tinklas [16, 17] (toliau, VPN) yra tinklo architektūrą, kuri yra realizuota pasinaudojant viešojo tinklo prieiga, skirta užtikrinti privatumą viešajame tinkle. VPN užtikrino savo pranašumą kaip ganėtinai pigus ir patikimas tinklo prieigos sprendimas tarp įmonės padalinių ir nutolusių darbuotojų. VPN yra viena svarbiausių bet kurios IT pramonės dalis, nes sutaupo nemažą dalį resursų skirtu IT infrastruktūros palaikymui. VPN leidžia naudojantis viešuoju internetu sukurti labai saugią komunikacijos terpę tarp įmonės biuro, nutolusiais padaliniais ir nuotoliniais vartotojais.

VPN naudoja tuneliavimo metodą, skirta funkcionalumui palaikyti. Tunelio sudarymo protokolas suteikia saugią transportavimo terpę tarp vartotojų pasinaudoję viešo tinklo paslaugomis, kuriu bazinis viešas tinklas nepalaiko tiesiogiai. VPN nustato loginį saugų kanalą, ryšiui tarp dviejų klientų naudojant tuneliavimo metodą, kuris apjungia IP datagramą į tunelinį protokolą, paslėpdamas pirminius duomenis nuo įsibrovėlių ar įsilaužėlių, kurie yra beveik visuose tinkluose.

Tradicinis VPN tinklas naudoja DES (angl. *Data encryption standart*, duomenų šifravimo standartą, AES (angl. *Advance encryption standart*, pažangų šifravimo algoritmą) ir „*Blowfish*“ vartotojo duomenų šifravimo algoritmą.



7 pav. VPN architektūros schema

Šiuo metu yra plačiai naudojami 4 VPN protokolai: PPTP, L2TP, IPSec ir SSL/TLS. Žemiau pateiktoje lentelėje parodyti kiekvieno iš naudojamų VPN protokolo privalumai ir trūkumai.

1 lentelė. VPN protokolų privalumai ir trūkumai

	Privalumai	Trūkumai

PPTP	• Mažesnė tinklo perdanga • Nereikalauja PKI • Palaiko daugiau PPTP sujungimu VPN serveryje • PPTP ir NAT traverse, palaikomas NAT suderinamumas	• Saugumo ir tinklo ugniasienės problemos • Palaikomas tik vienas tunelis vartotojui, tuo pačiu metu • Jokio papildomo autentifikavimo • Jokios prieigos kontrolės paketų filtravime
L2TP	• Palaiko IP ir ne IP grįstus tinklų struktūras • Gali palaikyti daugiau negu vieną protokolą vienu metu • Palaiko papildomo autentifikavimo protokolus, • Palaiko keletą tuneliu vienu metu • IpSec ir NAT traverse, palaiko NAT suderinamumą	• Greitaveikos problemos • Palaiko mažiau tuneliniu sujungimu vienu metu.
IPSEC	• Lankstus • Nereikalaujantis vartotojo įrenginio papildomos konfigūracijos • Saugesnis duomenų bei raktų apsikeitimas • Palaiko siunčiamų duomenų integralumą • Palaiko dauguma šifravimo algoritmų • Optimalus naudojant kaip vartų-vartų VPN sprendimą • Geriausias naudojant kaip pastoviai prieinamą ryšį • Suderinamas su NAT	• Yra sudėtingas naudojime • Identifikuoja tik įrenginius, bet ne vartotojus • Maršrutizavimo galimybės nėra įterptos • Palaikomas tik IP protokolas • Sumažina tinklo pralaidumą • Nulaužimo atveju pažeidžiamas visas tinklas arba potinklis.
SSL/TLS	• Nereikalingas VPN klientas • Saugesnis duomenų ir raktų apsikeitimas • Leidžia nustatyti tinklo resursų prieiga tinkle.	• Suderinamas tik su Web-based programomis • Sudėtingesnis ugniasienės konfigūravimas • Padidina IT personalo darbo valandų skaičių atremiant DoS

Kaip matome iš lentelės, kiekvienas VPN protokolas turi savo pliusu ir minusų. Nei vienas iš protokolų negali pilnai padengti viso tinklo saugumo, apsaugodamas įmonės resursus nuo piktavalių kenkėjų. Toliau darbe apžiūrėsime keletą saugumo karkasu, kurie naudojasi VPN teikiamais privalumais, norint įdiegti įmonėje įrenginių valdymo saugumo karkasus.

1.5. Kelių veiksnių autentifikavimo procesas, saugiam autentifikavimui

Vartotojo prisijungimai yra informacijos dalis, kuri leidžia individui prieiti prie kompiuterinių sistemų teikiamos informacijos. Vartotojo vardas ir slaptažodis yra vienas iš dažniausiai naudojamu būdu vartotojo identifikavimui. Slaptažodžio autentifikavimo sistema išlieka viena dažniausiai naudojamu saugumo procesų, tačiau turi savo spragų, kelios iš kurių yra blogai pasirinktas slaptažodžio sudėtingumas bei perėmimo pažeidžiamumas. Papildoma problema sudaro slaptažodžio pakartotinis naudojimas kitose sistemose. Keletas straipsniu teigia, jog 70% kenkėjiškų veiksmų yra susiję su sukčiavimo tipo puolimais, dėl ko yra labai svarbu apsaugoti vartotojo prisijungimo informacija nuo neteisėto pasisavinimo.

Kai sistema naudoja vartotojo vardą ir slaptažodį prisijungimui, tai yra vadinama vieno veiksnio autentifikavimo sistema (angl. *one factor authentication* – toliau OFA). Kitas metodas yra žinomas

kaip kelių veiksnių autentifikavimas (angl. *multi factor authentication* – toliau MFA). MFA – kai naudojama daugiau negu vienas autentifikavimo veiksnys vartotojo autentifikavimo procese.

Mobilus autentifikavimas yra vienas iš pagrindiniu kelių veiksnių autentifikavimo būdų. Tokiam autentifikavimui yra naudojamas mobilus įrenginys (po programinės žymės diegimo įrenginyje), kuris yra naudojamas kaip antrinė autentifikavimo priemonė, pakeičianti kietąją autentifikavimo žymę (angl. *hard token*), *smart* žymę arba *smart* lustinę kortelę. Norint pasinaudoti tokiu autentifikavimo būdu, reikia sudiegti specialia programine įrangą įrenginyje, kuri sugeneruos vienkartinį slaptažodį. Vienkartinis slaptažodis galioja tik vienai prisijungimo sesijai ar duomenų transliacijai. Taipogi, vienkartiniai slaptažodžiai leidžia išvengti problemų, su kuriomis susiduria tradiciniai autentifikavimo metodai.

Mobilaus įrenginio naudojimas autentifikavimui gali sukelti papildomu nepatogumu vartotojui. Daugelis šiuo metu naudojamu sprendimu kompromituoja saugumą, arba pritaikomumą.

Keletas trūkumu, susijusiu su mobiliųjų įrenginių naudojimu vartotojų autentifikavimui [15]:

- Vartotojams tenka dažnai suvedinėti slaptažodžius norint naudotis mobiliosiomis programėlėmis. Painius slaptažodžius sudėtinga suvedinėti mobiliuosiuose įrenginiuose, ko pasekmėje vartotojas išsisaugo slaptažodį įrenginyje, arba pasirenka paprastesnį slaptažodį, kurį yra nesunku suvesti naudojamame įrenginyje.
- Kai vartotojas praranda savo įrenginį, piktavaliai gali prieiti prie visos informacijos talpinamos įrenginyje. Tai tapo rimta saugumo spraga, įskaitant naudojamų mobilių įrenginių naudojimo kiekį. Piktavaliai išnaudoja šita spragą pavogdami įrenginius ir parduodant jį, arba prieinant prie informacijos, kuri randasi įrenginyje. Jei vartotojo įrenginys yra pavogtas, piktavalis gali pasinaudoti juo vienkartinio slaptažodžio generavimui.

Autentifikavimo metodai yra skaitoma kaip esminis reikalavimas vartotojo autentifikavime, kai yra gaunama užklausa patvirtinti vartotoja. Yra skirstomi 4 pagrindiniai klasifikatoriai, kurie yra laikomi autentifikavimo pagrindu:

2 lentelė. Autentifikavimo tipu klasifikavimas

Klasifikatorius	**Aprašymas**	**Pavyzdys**
1 tipas	Kažkas, ką žinai	Slaptažodis, PIN
2 tipas	Kažkas, ką turi	Mobilus įrenginys
3 tipas	Kažkas, kas esi	Akies rainelės atvaizdas, piršto antspaudas
4 tipas	Kažkas, ką darai	Balsas

Vienkartinio prisijungimo procesas sukuria slaptažodį tik vienam prisijungimui, kartu sukuriant papildomus parametrus: vartotojo sertifikatą ir elektroninio perdavimo saugumą, skirtus apsaugoti vartotojo pateikta informaciją bei išspręsti statinio slaptažodžio keliamas problemas. Tačiau iškyla problema su elektroniniu autentifikavimu, neįmanoma sudaryti „*face to face*“ komunikacijos. Norint patvirtinti prie sistemos prisijungusio asmens tapatybę, egzistuojančiame vienkartinio slaptažodžio procese susiduriama su tokiomis problemomis, kaip nesugebėjimas garantuoti sertifikavimo (autentiškumo tapatumo) ir nepaneigimo.

Toliau apžvelgsime vieną iš pasiūlytų procesų, skirtu išspręsti vienkartinio slaptažodžio problemas bei užtikrinti vartotojo sertifikavimą ir nepaneigimą. Apžvelgiamas sprendimas reikalauja jog kiekvienas vartotojas į sistemą užregistruotu savo asmenine informaciją: asmens tapatybės kortelės numerį, mobilųjį numerį, IMEI ir PIN. Serveris sugeneruoja vienkartinį slaptažodį, sujungdamas įvairias vartotojo asmeninės informacijos laukus (kaip aprašyta aukščiau) ir persiųsdamas sukurtą vienkartinį slaptažodį vartotojui, užkoduodamas jį, pasinaudojęs išplėstiniu šifravimo standartu (AES). Vartotojas užregistruoja savo asmeninę informaciją sistemoje registracijos etape. Registracijos metu serveris patikrins IMEI galiojimą, nurodydamas, ar numeris yra galiojantis. Tada vartotojas bus perkeliamas į prisijungimo etapą, kuriame tikrinamas vartotojo vardas ir slaptažodis.

Kai vartotojas įves teisingą vartotojo vardą ir slaptažodį, serveris perkels vartotoją į antrąją autentifikavimo fazę (naują sluoksnį), vadinamą patvirtinimo etapu. Šiame etape vartotojas bus paprašytas įvesti savo asmeninę informaciją, kuri buvo pateikta sistemai registracijos metu. Šį sluoksnį jungia du veiksniai: ką vartotojas žino ir ką vartotojas turi, vartotojui pateikus šiuos du veiksnius informaciją pateikiama į serverį. Gavęs informaciją, serveris sugeneruos vienkartinį slaptažodį ir nusiųs jį vartotojui šifruota trumpąją žinute. Šiame etape serveris patikrins IMEI galiojimą, tuo pačiu metu suteikdamas sertifikavimo garantiją ir neatsisakomumą, nes vienkartinis slaptažodis nebus siunčiamas tiesiogiai vartotojui, kol serveris tikrins, ar mobilusis įrenginys yra to paties vartotojo rankose, ar ne.

Serveris išsiųs užšifruota vienkartinį slaptažodį, vartotojui patogiu būdu, trumpąją žinute arba elektroniniu paštu. Po pranešimo gavimo, vartotojas yra nukreipiamas į kitą langą, kuriame yra paprašomas suvesti savo PIN slaptažodį bei kartu yra iššifruojamas vienkartinis slaptažodis. Įvedus klaidingą PIN, sesija yra nutraukiama.

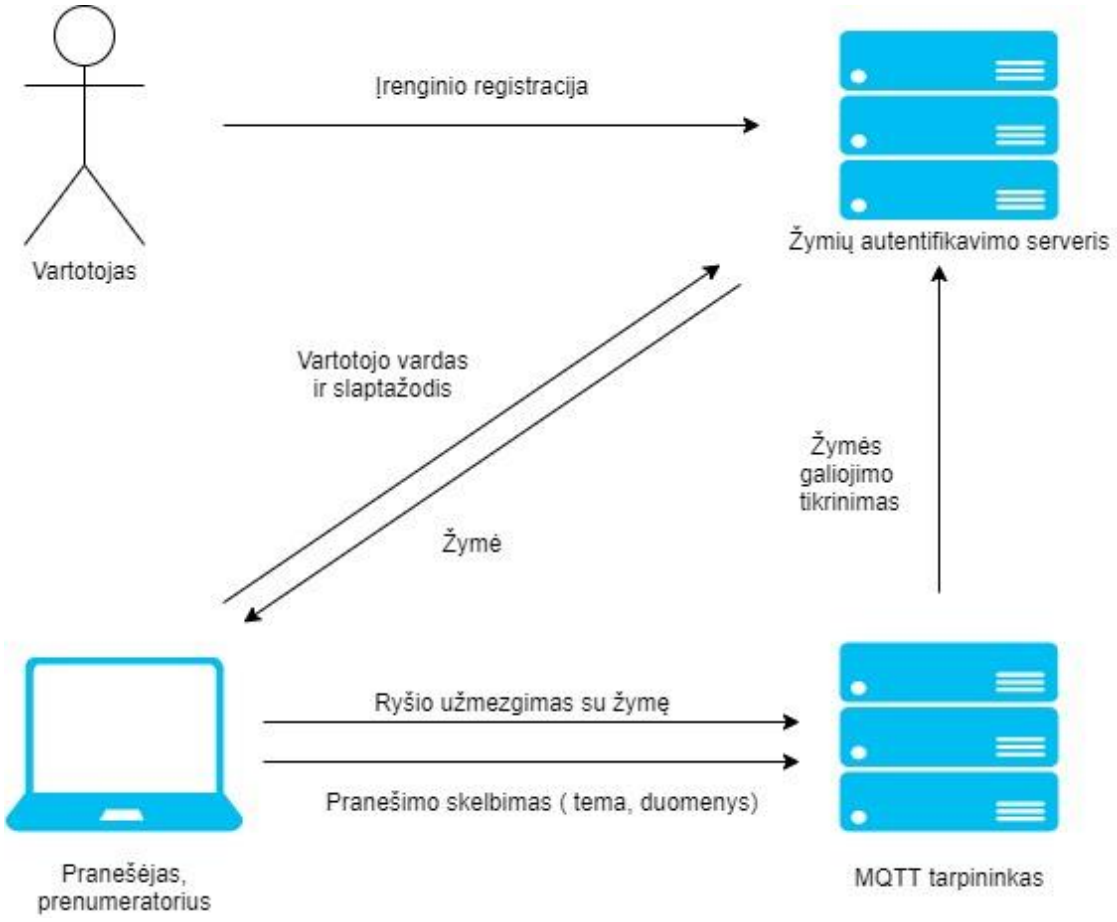
1.6. Žymėmis paremtas MQTT protokolo autentifikavimas

Vienas populiaresnių programų lygmens protokolų daiktų internete yra „ *Message queue Telemetry Transport*“ protokolas (sutrumpintai MQTT). Lyginant su HTTP protokolu, MQTT yra TCP paremtas pranešimų protokolas su publikavimo, prenumeratos architektūrą. Architektūroje egzistuoja trys aktorių tipai: pranešėjas, prenumeratorius ir tarpininkas. Pranešėjas siunčia žinute su nurodyta specifine tema tarpininkui, kuris persiunčia žinutę toliau visiems temos prenumeratoriams. Šiuo atveju, prenumeratoriui nereikia žinoti iš kur ateina žinutė; savo ruoštu siuntėjui nėra svarbu kam žinutė yra perduodama. Tokio tipo architektūra yra tinkama daiktų interneto atveju, nes gali pateikti labiau į duomenis orientuotą protokolą, kuris gali sumažinti resursais suvaržyto prietaiso naštą pranešimu apsikeitimui. Tačiau kadangi tiek pranešėjas, tiek prenumeratorius nežino vienas kito, atsiranda didelis autentifikavimo metodo poreikis užtikrinti siuntėjo ir gavėjo mazgo galiojimą.

Norint atlikti tokį autentifikavimą, kelios MQTT tarpininkų programos suteikia vartotojo vardas ir slaptažodis sistemą kaip pagrindinį autentifikavimo procesą. Taikant šį metodą, pranešėjas ar prenumeratorius turi išsiųsti savo vartotojo vardą ir slaptažodį ryšio užmezgimo metu. Nors vartotojo ir slaptažodžio schema gali užtikrinti gana gerą pagrindinę saugos funkciją, ji gali susidurti su keliomis problemomis. Kadangi ryšio užmezgimo metu pranešėjas turi visada siųsti savo kredencialus, pasyvus piktavalis gali lengviau perimti kredencialus šnipinėjimo (angl. *sniffing*) procesą. Taipogi slaptažodis neturi galiojimo laiko, kuris reiškia, jog piktavaliui gavus vartotojo kredencialus, jis galės naudotis jais tol, kol jie nebus pakitę. Norint išvengti minimos problemos, tarpininkas gali įsiminti sesijos informaciją, susijusia su patikimu įrenginiu, tuo pačiu leidžiant

klientui nesiųsti savo kredencialų prisijungimo metu. Tačiau tai gali sukelti papildomą apkrovą tarpininkui saugant sesijos informaciją, ypač jei sistemoje yra daug pranešėjų ir prenumeratorių. Tokiu atveju, norint išspręsti minėtas problemas, yra reikalingas autentifikavimo procesas, kuris naudoja kliento sesijos informacijos talpinimo procesą.

Minint išvardintas aukščiau problemas, savo darbe *„Architectural Design of Token based Authentication of MQTT Protocol in Constrained IoT Device“* [23] autoriai siūlo savo sprendimą. Siūlomas sprendimas yra sudarytas iš 4 komponentų: pranešėjo, prenumeratoriaus, MQTT tarpininko ir žymių autentifikavimo serverio. Pranešėjas ir prenumeratorius prisijungimo metu pirma siunčia savo vartotojo vardą ir slaptažodį autentifikavimo serveriui iš kurio gauną unikalią žymę (angl. *token*). Reikia įsidėmėti – žymės generavimas yra vykdomas tik tuomet, jei iškyla viena iš sąlygų: 1) žymė nebuvo sugeneruota ir 2) kai žymės galiojimas išseko. Kai pranešėjas ir prenumeratorius gauna galiojančias žymes, jos yra saugomos lokalioje atmintyje ir ji bus naudojama tolimesnėms autentifikacijoms. Tokiu atveju tarpininkui nereikia saugoti sesijos savo duomenų bazėje, tuo pačiu išvengiant pranešėjo ir prenumeratoriaus periodinio kredencialų perdavimo.



8 pav. Žymėmis grįstos MQTT autentifikavimo sistemos architektūra

8 pav. yra parodyta bendroji sprendimo architektūra. Ji yra sudaryta iš keturių komponentų: pranešėjo, prenumeratoriaus, MQTT tarpininko ir žymių autentifikavimo serverio. MQTT protokolu grįstoje sistemoje, pranešėjas yra pagrindinis informacijos gamintojas, kuria naudoja prenumeratorius. Tarp pranešėjo ir prenumeratoriaus, egzistuoja MQTT tarpininkavimo serveris, kuris atlieka duomenų perdavimo funkciją. Norint užtikrinti pranešėjo ir prenumeratoriaus autentiškumą, yra pasiūlytas žymių autentifikavimo serveris, kurio vaidmuo yra skirti žetonus ir

tikrinti jų galiojimą su kiekviena autentifikavimo užklausą. Pranešėjas arba prenumeratorius, pirma siunčia savo prisijungimo duomenis žymių serveriui, kuris sugeneruoja naujos sesijos žymę. Patikrinus kredencialus su duomenimis, saugomais duomenų bazėje ir jiems sutapus, yra gražinama autentifikavimo žymė. Žymę sudaro antraštė, siunčiami duomenys ir parašas. Kai pranešėjas arba prenumeratorius nori siųsti duomenis, pirma yra inicijuojamas prisijungimas prie tarpinio serverio žymės pagalba. Tarpinis serveris patikrina žymės galiojimą autentifikavimo serveryje. Patvirtinus žymės galiojimą yra leidžiamas prisijungimas prie norimos specifinės temos ir yra leidžiami informacijos mainai.

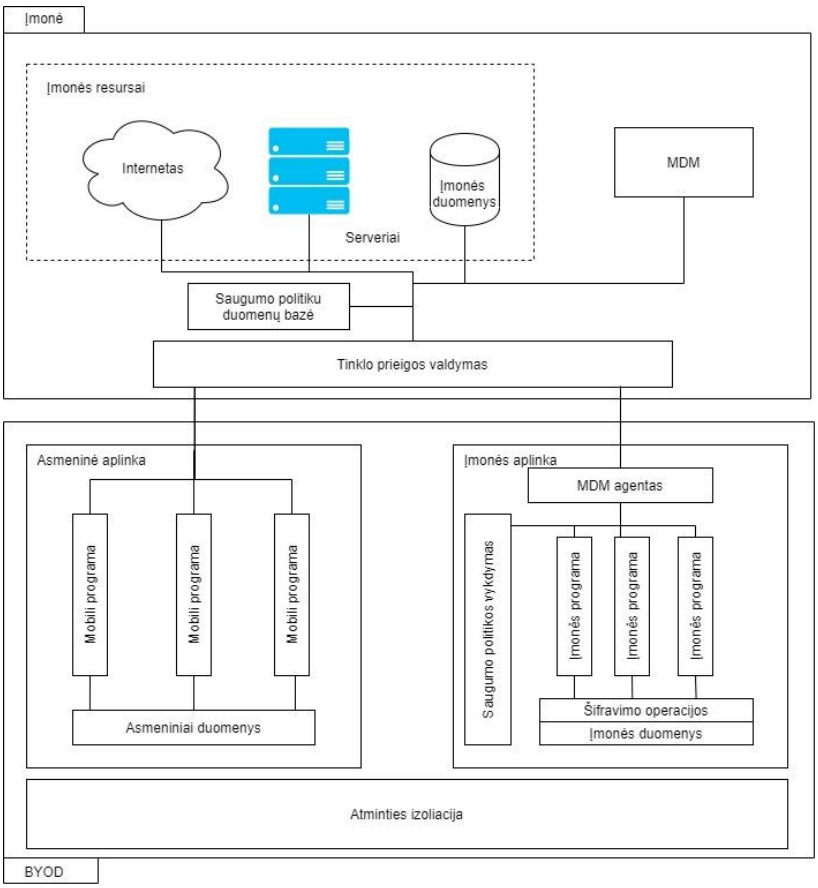
1.7. BYOD saugumo karkasas su atskirta įmonės ir asmenine dalimi

BYOD saugumas yra esminis punktas norint apsaugoti įmonės tinklą. Tačiau dėl BYOD unikalumo, apsaugoti tokia sistema tampa dideliu iššūkių. Minėjome keletą sprendimų skirtų BYOD saugumo spragoms spręsti, tačiau visi jie turi ir savo spragų.

BYOD saugumo sprendimai turi atitikti keliamus reikalavimus[2]:

1. Erdvės izoliacija: sprendimas turi gebėti atskirti asmeninę erdvę ir įmonės erdvę BYOD aplinkoje, jog galima būtų skirti atitinkamas politikas kiekvienoje aplinkoje.
2. Įmonės duomenų apsauga: įmonės duomenys turi būti užšifruoti kai jie yra asmeniniame įrenginyje. Bet koks neautorizuotas ir nelegalus bandymas pasiekti šiuos duomenis turi būti stebimas ir uždraudžiamas.
3. Saugumo politikos priverstinis laikymasis: turi gebėti priverstinai diegti saugumo politikas BYOD įrenginiuose ir užtikrinti jog įrenginiai atitinka įmonės saugumo reikalavimus.

Šie reikalavimai suteikia norimą prieigos kontrolę, konfidencialumą ir saugos politikų valdymą BYOD sistemoje. Idealus sprendimas turi atitikti visus tris saugumo reikalavimus. Paveikslėlis 8 atvaizduoja BYOD sprendimo saugumo karkasą įmonės tinkle, kuris atitinka visus reikalavimus. Karkasas yra sudarytas iš dviejų dalių: darbinės ir BYOD (asmeninės) dalies.



9 pav. BYOD saugumo karkasas

BYOD saugumas, įmonės pusė:

Įmonės puse sudaro įvairūs įmonės resursai tokie kaip internetas, serveriai, įmonės duomenys, tinklo prieigos kontrolė BYOD įrenginiams ir prieigos kontrolė prie įmonės resursų. Prieiga yra skiriama arba uždraudžiama remiantis įmonės saugumo politika. Įmonės puse taipogi sudaro įrenginių valdymo sistema , tokia kaip MDM , skirta valdyti BYOD įrenginius.

Tinklo prieigos kontrolė (NAC) suteikia prieigos taškus BYOD įrenginiams ir leidžia jiems prisijungti prie tinklo resursų vadovaujantis įmonės saugumo politikomis. NAC turi skirti užklausas pagal tai iš kokios aplinkos jos atėjo, asmeninės ar darbinės. Vienas iš atskyrimo būdu yra skirtingų sertifikatų naudojimas. Vienas skirtas asmeninei terpei, kitas darbinei.

Saugumo politikų duomenų bazė apibrėžia įmonės politikas BYOD įrenginių valdymui. Pavyzdžiui, kaip apdoroti prieigos užklausas ateinančias iš asmeninės BYOD įrenginio terpės, kuriems įrenginiams yra leista prisijungti prie tinklo, koks šifras yra naudojamas, koks rakto ilgis ir t.t.

BYOD saugumas, asmeninė aplinka:

Asmeninė BYOD pusė suteikia įmonės duomenų izoliavimo funkcionalumą, priverstinį saugumo politikų naudojimą ir įmonės duomenų apsaugą [2].

Vietos izoliavimas leidžia atskirti asmenine ir įmonės BYOD puses. Jis reikalingas norint skirstyti skirtingas saugumo politikas asmeninei ir įmonės aplinkoms. Asmenine aplinka sudaro darbuotojo įdiegtos programos ir duomenys. Kaip ir asmenine aplinka , įmonės aplinka sudaro įmonės įdiegtos programos ir duomenys skirti darbui įmonėje arba nuotoliniu būdu. Mobiliosios programėlės ir duomenys turi atitikti įmonės išsikeltas saugumo politikas. Idealiu atveju, asmeninė aplinka neturi turėti galimybės pasiekti įmonės resursų, bet gali turėti ribotą prieigą prie tokių resursų kaip intraneto puslapis ir internetas. Taipogi yra tokios programos kaip SKYPE kurios yra naudojamos kaip ir asmeninėje taip ir darbo aplinkoje. Tačiau vietoj to jog abi aplinkos kreiptųsi į vieną ta pačią programą, turime naudoti dvi atskiras programas įdiegtas skirtingose aplinkose, kas užtikrina įmonės duomenų saugumą.

MDM-Agent yra mobili programėlė kuri yra įdiegta įmonės aplinkoje. *MDM-Agent* siunčia BYOD valdymo informaciją MDM ir atstovaują sistemos administratorių priverstinai diegiant nustatytas saugumo politikas įrenginyje. Kaip pavyzdys, MDM gali nusiųsti nuotolinio išvalymo komandą kuri ištrins visus įmonės duomenis esančius BYOD įrenginyje.

Saugumo politikos priverstinis laikymasis užtikrina jog BYOD įrenginys atitinka visas įmonės saugumo politikas. Saugumo politikos gali apimti tokius parametrus kaip kokias šifravimo operacijos turi būti naudojamos, raktų ilgius, ir taip toliau. Saugumo politikos duomenų bazė (angl. *security policy database,* toliau SPD) apima informacija tokia kaip duomenų tipai, saugumo protokolai ir raktai.

Įmonės duomenų apsauga apsaugo įmonės duomenis. Ji gali ne tik užtikrinti kad įmonės duomenys yra laikomi užšifruotoje laikmenoje, bet kartu ir užtikrinti jog duomenys nebus nukopijuoti arba perkelti nelegaliai neautorizuoto vartotojo. Šifravimo operacijos suteikia norimas kriptografines bazines funkcijas (tokias kaip šifrai, *hash* funkcijos ir skaitmeniniai parašai) kurios palaiko įmonės duomenų saugumą.

BYOD saugumo karkaso įgyvendinimas:

BYOD saugumo karkasas suteikia bendrąjį supratimą norint įsidiegti BYOD darbinėje aplinkoje[2]. Esami dabartiniai sprendimai, tokie kaip MDM, mobilios virtualios mašinos ir *Cisco Smart BYOD* , gali būti integruotos tarpusavyje, norint pilnai padengti skirtingų sistemų trūkumus darbinėje aplinkoje. Dabartiniai sprendimai labiau orientuoti yra į įmonės duomenų konfidencialumą. Neautorizuotas ir nelegalus duomenų prieigos BYOD įrenginyje turi būti svarstomos BYOD saugumo sprendime.

1.8. Saugumo modelis paremtas MDM ir VPN modeliu

Siūlomas [11] straipsnyje sprendimas siūlo MDM ir VPN modelio naudojimą, skirtą įmonės resursų apsaugai:

Norėdami tinkamai apsisaugoti nuo galimų grėsmių, įmonės turi įsidiegti saugumo modelį kuris užtikrina prieigos kontrolę ir įmonės duomenų konfidencialumą bei vientisumą. Siūlomas sprendimas sprendžia tokio tipo problemas [11]:

- Įmonė gali nustatyti minimalius įrenginių specifikacijos ir galimybių reikalavimus skirtus BYOD įrenginiams, tokius kaip OS versiją, autentifikavimo galimybes ir t.t. Jeigu įrenginys atitinka iškeltus reikalavimus , jis gali būti pridėtas prie BYOD įrenginių tinklo.
- Remdamiesi darbuotojo pareigomis, įmonė gali nustatyti atskirą prieigos modelį kiekvienam darbuotojui. Aukšto rango personalui dirbančiam su slapta informacija, galime suteikti modelį, kur priėjimas prie duomenų yra suteikiamas tik per tinklo sąsaja. Jokie duomenys nebus saugomi vartotojo įrenginyje. Vartotojas gali atlikti tokias operacijas kaip informacijos skaitymas ir rašymas, bet negali kopijuoti informacijos į naudojamą įrenginį. Ryšio saugumas yra užtikrinamas VPN sujungimu.
- Darbuotojams dirbantiems su ribotos prieigos informacija, gali būti naudojamas šifruoto konteinerio modelis kartu su VPN sujungimu.
- Darbuotojams dirbantiems su neribotos prieigos duomenimis pakanka tik VPN grįsto saugumo modelio naudojimo. Nėra reikalo saugoti laisvai prieinamos informacijos.

Nežiūrint į tai koks saugumo modelis buvo pasirinktas darbuotojui, saugumo politikos (tokios kaip slaptažodžio sudėtingumas, nuotolinis įrenginio išvalymas ir pan.) gali būti vykdoma kiekviename darbuotojo įrenginyje naudojantis MDM sistema, taip suteikiant daugiau įrenginio valdymo kontrolės įmonei. 2 lentelėje yra pateikti saugumo modeliai kurie gali būti vykdomi skirtingo lygio personalui organizacijoje [11]:

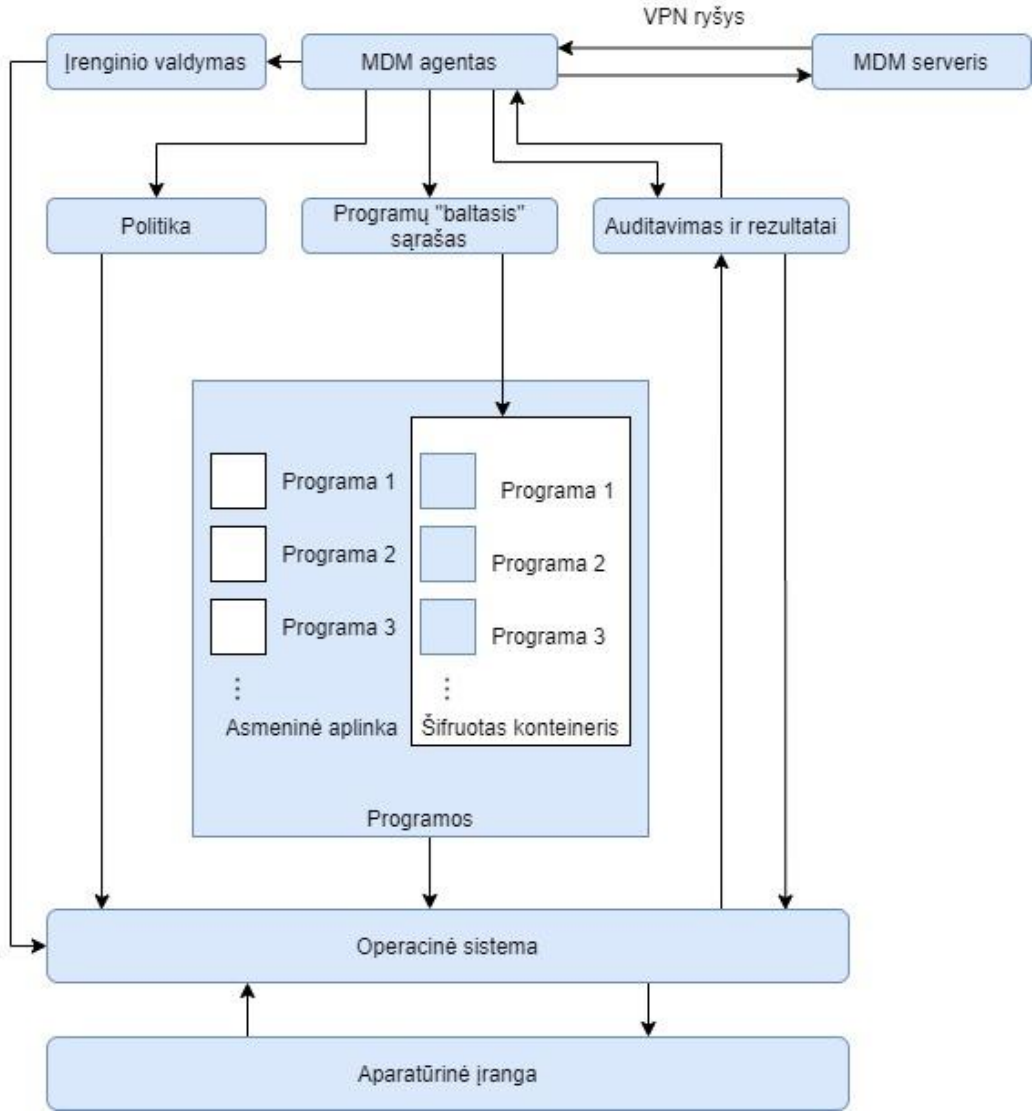
3 lentelė. Saugumo karkaso modeliai

Darbo tipas	Slaptas	Ribotos prieigos	Neribotos prieigos
Saugumo modelis	Tinklu grįstas prieigos modelis (su duomenų kopijavimo ribojimų) + MDM + VPN	Šifruoto konteinerio modelis + MDM + VPN	VPN

1.8.1. MDM ir VPN sprendimo architektūra

10 paveikslėlyje [11] yra pavaizduotas esamos BYOD saugumo modelis. Architektūra yra sudaryta iš MDM agento kuris yra įdiegtas darbuotojo įrenginyje programėlės pavidale ir MDM serverio, kurį valdo IT administratorius arba įmonė. Darbuotojo įrenginyje yra sukuriamas izoliuotas šifruotas konteineris, kuriame yra saugomi įmonės duomenys bei programėlės. Asmeninėje aplinkoje darbuotojas gali įsidiegti bet kokias programas. Serveris siunčia leidžiamų įdiegti programų sąrašą konteineryje. Programos konteineryje gali komunikuoti tarpusavyje norint pasiekti norimo funkcionalumo (pvz. naudojant *Inter Process Communications*, IPC). Programoms už konteinerio ribų nėra leidžiama komunikuoti su programomis konteineryje, tokiu būdu užtikrinant duomenų saugumą jame. Be „*Whitelist*“ (baltojo) sąrašo , serveris siunčia saugumo politikas agento programai. Šitas politikas sudaro slaptažodžio sudėtingumas, neteisingų slaptažodžio surinkimų skaičius, nuotolinis įrenginio išvalymas, pilnas įrenginio šifravimas ir pan. Agento programa reguliariai siunčia serveriui ataskaitas apie vykdomas saugumo politikas ir pastebėtus pažeidimus. Remiantis surinkta

informacija serveris gali siųsti komandas įrenginiui , tokias kaip padaryti nuotrauką naudojantis priekinę kamerą, uždaryti įrenginį arba ištrinti visus duomenis laikomus konteineryje.



10 pav. Saugumo karkaso architektūrinis modelis

Karkasas įgyvendintas Android platformoje, įrenginio saugumo politikos yra vykdomos naudojantis įrenginio saugumo politikų vadovu (angl. *DevicePolicyManager*) , Android API klasės dalimi. Šifruotas konteineris yra sukuriamas pasinaudojus *Android kriptos* bibliotekomis. Visi duomenys susiję su įmonę yra laikomi šifruotame konteineryje. Įmonės programos dirba konteineryje su įmonės duomenimis. Ryšio saugumas yra užtikrinamas parašu grindžiamu saugumo modeliu, t.y., tik įmonės sertifikatu pasirašytos programos gali komunikuoti tarpusavyje bei perduoti duomenis tarpusavyje. Visos užklausos iš kitų programų tuo tarpu yra blokuojamos.

1.9. Išvados

Asmeninių įrenginių naudojimas įmonėse šiuo metu vis labiau populiarėja ir tendencija įgauna vis didesnį populiarumą. Tačiau su teikiamais tokios tendencijos privalumais, tokiais kaip darbo našumo padidėjimas, efektyvumo ir kokybės padidėjimai, atsiranda ir papildomas galvos skausmas įmonės

saugos specialistams. Norint efektyviai apsisaugoti nuo galimų grėsmių iš BYOD pusės, įmonė privalo naudoti technologijas, skirtas asmeniniams įrenginiams valdyti.

Kaip ir visos technologijos, asmeninių įrenginių valdymo technologijos turi savo spragų. Neteisingai sukonfigūravus tokias technologijas kaip MDM arba MAM atsiranda daug spragų, kurios kelia grėsmę visos sistemos saugumui. Pasinaudojus tomis spragomis piktavaliai puolėjai gali perimti konfidencialius duomenis, perimti tinklo srautą, kompromituoti saugius prisijungimus bei visiškai suniokoti visą sistemą.

Norint apsisaugoti nuo panašaus scenarijaus yra būtina sudaryti BYOD saugumo politiką ir ją įgyvendinti pasinaudojant visais turimais įmonės resursais. Kuriant politika reikia įvertinti įmonės unikalumą, kokia prieigos prie duomenų sistema jie naudoja dabar, atsižvelgti į atskirų darbuotojų grupes ir jų funkcionalumą. Tik atsižvelgus į visus niuansus galima pasirinkti labiausiai tinkančias saugumo priemones.

Sudarius bendra sistemos vaizdą galime dalinti įmone į atskiras zonas, priskiriamas kiekvienai darbuotojų grupei. Nemažai svarbu yra laikytis saugumo politikos ne tik darbuotojams, bet ir visiems administraciniams bei saugumą diegiantiems specialistams. Sudarius bendrą saugumo politika reikia ja koreguoti su įmonės valdžia, jog politika ne tik apsaugotu įmonės resursus, bet ir padidintų įmonės našumą ir darbuotojų pasitenkinimą, teiktu visus BYOD siūlomus privalumus: saugumas, patogumas ir kaštu mažinimas.

Turint bendrą saugumo politiką galime pradėti kurti saugumo sistema, kuri leis darbuotojams prisijungus nuotolinių būdu dirbti su įmonės duomenimis saugiu VPN tuneliu. Pasinaudoję Virtualių darbalaukių infrastruktūros teikiamomis galimybėmis galime naudotis pilnu sistemos saugumu bei patogiu darbu iš bet kokio darbuotojo įrenginio. Visi veiksmai bus atliekami pačiame serveryje vartotojui prisijungus prie virtualaus darbalaukio tiek įmonės viduje tiek iš savo namų patogumo.

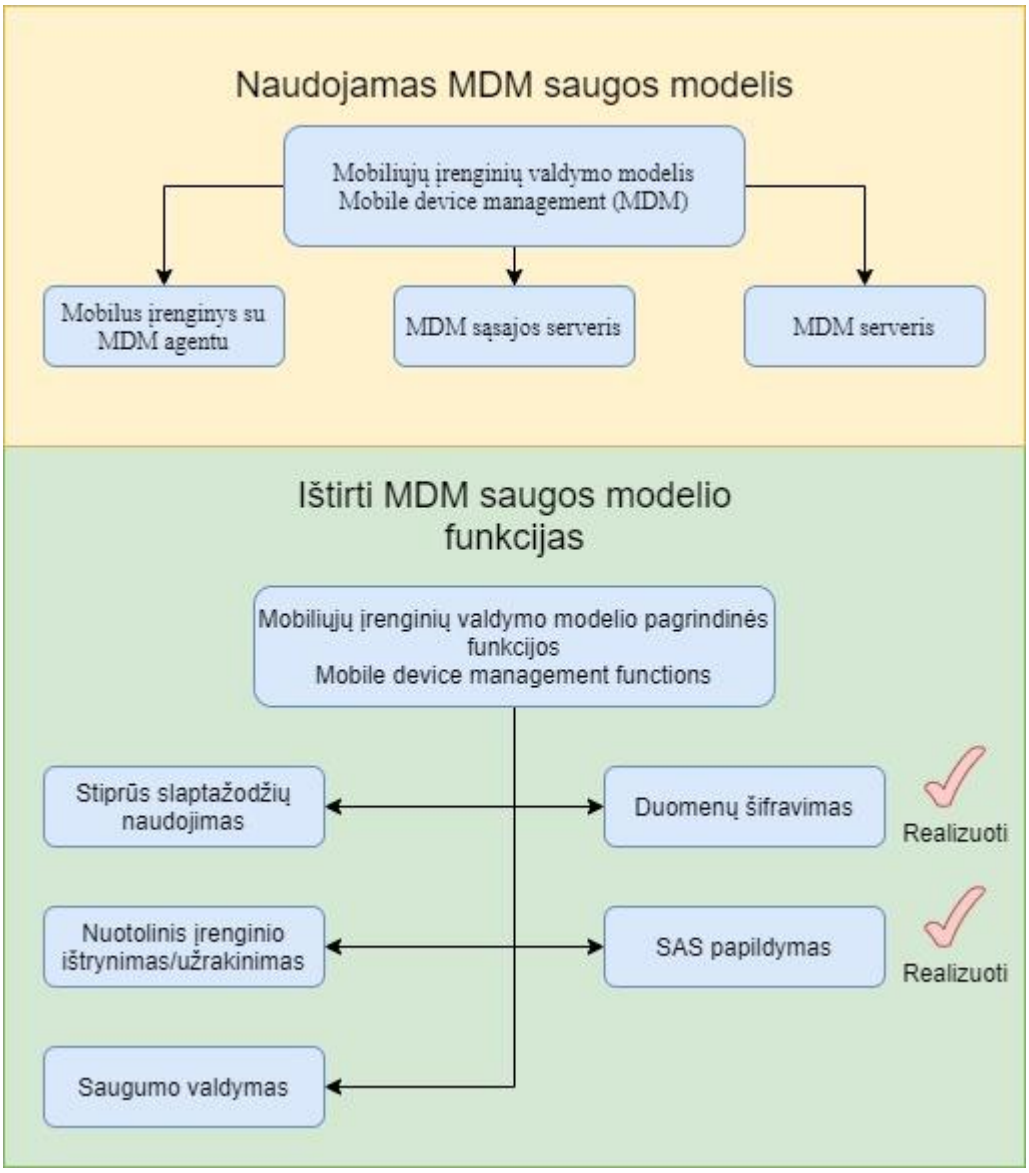
Analizės metu buvo ištirta keletas metodu, kurie sprendžia įrenginių valdymo problemą pasinaudoję MDM karkaso teikiamais privalumais, tačiau nei vienas sprendimas neatsižvelgė į įrenginio saugumą ir vientisumą. Didžiausias dėmesys buvo skirtas tik programų apsaugai konteinerio pagalba, bei saugaus ryšio užtikrinimui. Taipogi nebuvo sekamos tuo metu įrenginyje paraleliai vykdomos programos. Piktavaliai gali pasinaudoti tokia spraga, bei pasileidę „*keylogger*“ kenkėjišką programą įrašyti visus mygtukų paspaudimus, tuo pasisavindami vartotojo konfidencialią informaciją.

Analizės rezoliucija : yra būtina sudaryti sprendimą, kuris apimtu savyje ne tik saugaus ryšio užtikrinimą bei vartotojo autentifikavimą ir autorizavimą, bet ir paleistų ir įdiegtų programų tikrinimą, įrenginio komponentų integralumą ir kompiuterio komponentų identifikavimą ir autorizavimą.

2. Asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistema

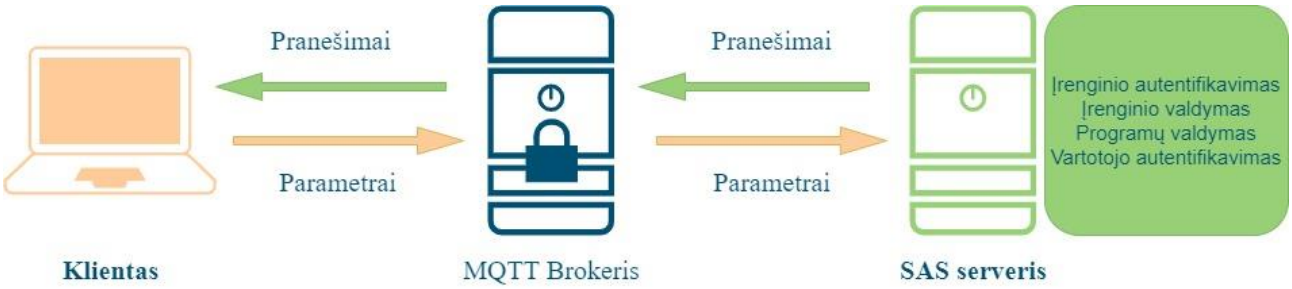
Šiame skyriuje aprašomas siūlomas kuriamo sprendimo sistemos modelis. Pateikiamas siūlomos sistemos koncepcinis modelis, architektūra, serverio ir kliento komunikacijų modeliai.

Magistro darbe yra siūloma asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistema (Toliau SAS). Darbe naudojamas MDM saugos modelis, kuris papildytas papildomu funkcionalumu.



11 pav. Asmeninių įrenginių saugaus autentifikavimo sistemos modelis

2.1. Asmeninių įrenginių saugaus autentifikavimo sistemos modelis ir koncepcija



12 pav. Asmeninių įrenginių saugaus autentifikavimo sistemos koncepcija

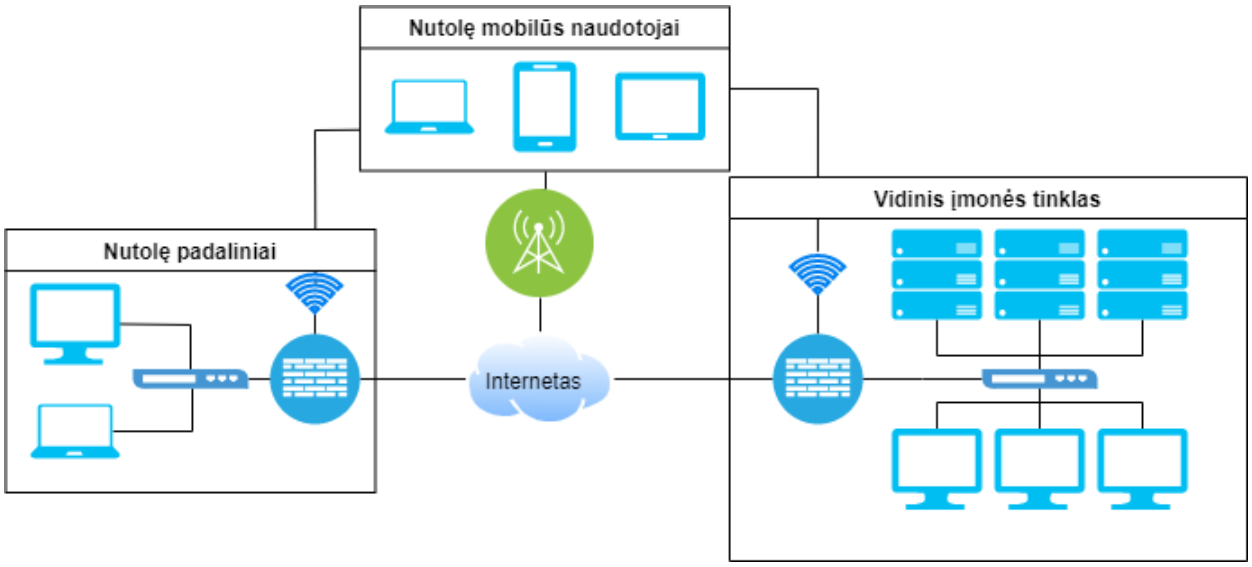
Darbuotojai norintys naudotis SAS sistema turi suteikti teisę įmonės IT administratoriams įdiegti SAS sistemos agentą jų įrenginyje. Įdiegus agento PĮ, IT administratorius registruoja įrenginį sistemoje. Registravimo metu perduodami serveriui visi parametrai apie kompiuterį ir jo vartotoją. Užregistravus įrenginį sistemoje naudotojas gali prisijungti prie įmonės privataus tinklo. Įrenginys yra dar tikrinamas iki prisijungimo į sistemą, bei vartotojas turi įsitikinti, jog agentas nerado jokių pažeidimu jo kompiuteryje. Prisijungimo prie sistemos metu yra autentifikuojamas vartotojas ir įrenginys sistemoje. Darbo metu yra tikrinama įrenginio, ryšio su įrenginių bei sesijos būklė. Nustačius, jog įrenginys arba serveris nutraukia ryšį su įrenginių arba serveriu, įrenginys yra atjungiamas nuo sistemos. Taipogi, prisijungus prie sistemos periodiškai yra tikrinamos paleistos programos kompiuteryje.

SAS sistema yra skirta darbui su asmeniniais darbuotojų įrenginiais. Jį turėtu būti lengvai diegiama bei dirbti be jokio vartotojo įsikišimo į procesą. Sistemos klientas turi būti autonominis agentas, kuris netrukdys darbuotojui jo darbo metu, tačiau praneš vartotojui apie ryšio nutraukimą dėl iškilusios problemos su jo įrenginiu. Taip pat sistema turėtų suteikti centralizuotą įrenginių administravimo aplinką, kurios pagalba IT administratoriai galės peržiūrėti visus sistemoje registruotus įrenginius bei juos valdyti.

SAS sistema turėtų atlikti šias funkcijas:

- Registruoti įrenginius sistemoje agento programos pagalba
- Surinkti įrenginio bazinę informaciją ir pateikti ja sistemai (modelis, gamintojas, OS , įrenginio identifikacinius numerius ir t.t.)
- Pateikti įdiegtos įrenginyje programinės įrangos sąrašą
- Registruoti įrenginio techninės įrangos pasikeitimus, automatiškai pranešant apie juos administratoriui
- Neleisti prisijungti vartotojui prie sistemos su neregistruotu įrenginiu
- Neleisti naudoti įmonėje neleistinos programinės įrangos
- Suteikti galimybę užrakinti ir išvalyti visus jame esančius duomenis nuotoliniu būdu.

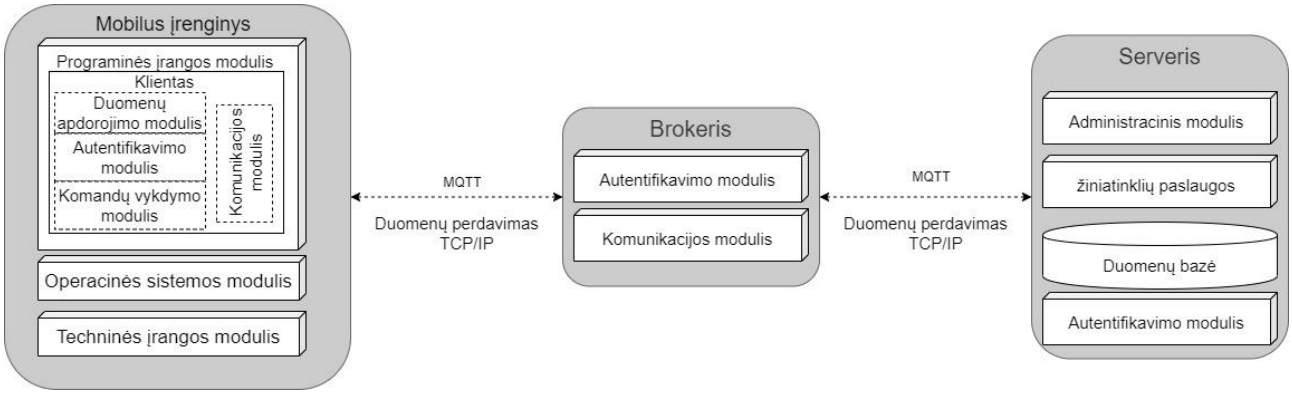
2.2. Asmeninių įrenginių saugaus autentifikavimo sistemos architektūra



13 pav. Tipinis įmonės kompiuterinio tinklo modelis

Dažniausiai įmonės tipinis tinklas susideda iš trijų pagrindinių dalių: nutolusiu įrenginių, vidinio įmonės tinklo ir nutolusių mobilių vartotojų įrenginių. Kiekvienos dalies tinklo saugumo užtikrinimas reikalauja skirtingų saugos priemonių bei įrankių. Šiame darbe nagrinėsime tik nutolusių vartotojų asmeninių įrenginių sauga bei tokių įrenginių naudojimo įmonėje saugumas.

Atsižvelgiant į tipinį įmonės nuotolinės prieigos saugumo sprendimą – VPN naudojimą ir jo teikiamas įrenginio tikrinimo galimybes, nuspręsta praplėsti VPN saugumą siūlant papildomo autentifikavimo užtikrinimo priedą. Priedas leis dar iki prisijungimo prie sistemos patikrinti, ar įrenginys yra saugus prisijungti prie įmonės vidinio tinklo.



14 pav. Siūloma SAS sistemos architektūra

Sistemos architektūra yra sudaryta iš trijų pagrindinių elementų : kliento įrenginio programinės įrangos, tarpinio MQTT brokerio serverio ir SAS serverio. Jie yra sudaryti iš kelių esminių modulių, skirtų atlikti tokias funkcijas:

Kliento programinė įrangą:

- Duomenų apdorojimo modulis – Surenka papildomus duomenis apie kompiuterio techninius parametrus, paruošia juos perdavimui į pagrindinį valdymo serverį. Panaudojęs komunikavimo modulį perduoda duomenis pagrindiniam valdymo serveriui
- Autentifikavimo modulis – Generuoja unikalų autentifikavimo kodą kuri perduoda komunikacijos modulio pagalba pagrindiniam serveriui.
- Komandų vykdymo modulis – Modulis atsakingas už komandų, gaunamų iš serverio, vykdymą.
- Komunikacijos modulis – Modulis skirtas saugaus ryšio sudarymui bei duomenų mainams su serveriu. Pasinaudojant autentifikavimo modulio generuotais slaptažodžiais vykdo įrenginio autentifikavimą, pasinaudojant šifravimo pagalba.

MQTT brokeris:

- Autentifikavimo modulis – Modulis skirtas autentifikuoti įrenginį bei leisti užmegzti ryšį per tarpinį serverį.
- Komunikacijos modulis – Modulis perduoda pranešimus iš kliento į serverį bei iš serverio į klientą jiems esant prisijungus ir autentifikavus.

Serverio programinė įrangą:

- Komunikacijos modulis – Komponentas skirtas administravimo sąsajos ir autentifikacijos apdorojimui. Papildomai atlieka komunikavimo funkcionalumą, komandų persiuntimą įrenginiams, įrenginių valdymą, vartotojų bei įrenginių autentifikavimą bei vientisumo tikrinimą.
- Administravimo sąsaja –Valdymo aplinka skirta darbui su sistema. Suteikia platų įrankių rinkinį, skirta registruotu sistemoje įrenginių valdymui, jų būklės peržiūrai, komandų siuntimui.
- Autentifikavimo modulis – modulis skirtas įrenginio autentifikavimui bei valdymui. Tikrina gautus pranešimus iš komunikacijos modulio, gavus autentifikavimo užklausą.
- Duomenų bazė – Komponentas saugantis duomenis, susijusius su sistemos veikimu. Privalo būti apsaugota nuo nesankcionuotos prieigos, taip kaip joje yra saugomi visi registruotų kompiuterių parametrai.

Sistemos modelis nevaržo sistemos realizacijos ir jos komponentų sudedamųjų dalių. Pasirinkti realizacijos būdai privalo atitikti bei patenkinti toliau darbe aprašomus komunikavimo ypatumus, bei privalo užtikrinti pilną pateiktų sistemos procesų veikimą.

2.3. Asmeninių įrenginių saugaus autentifikavimo sistemos komunikavimas

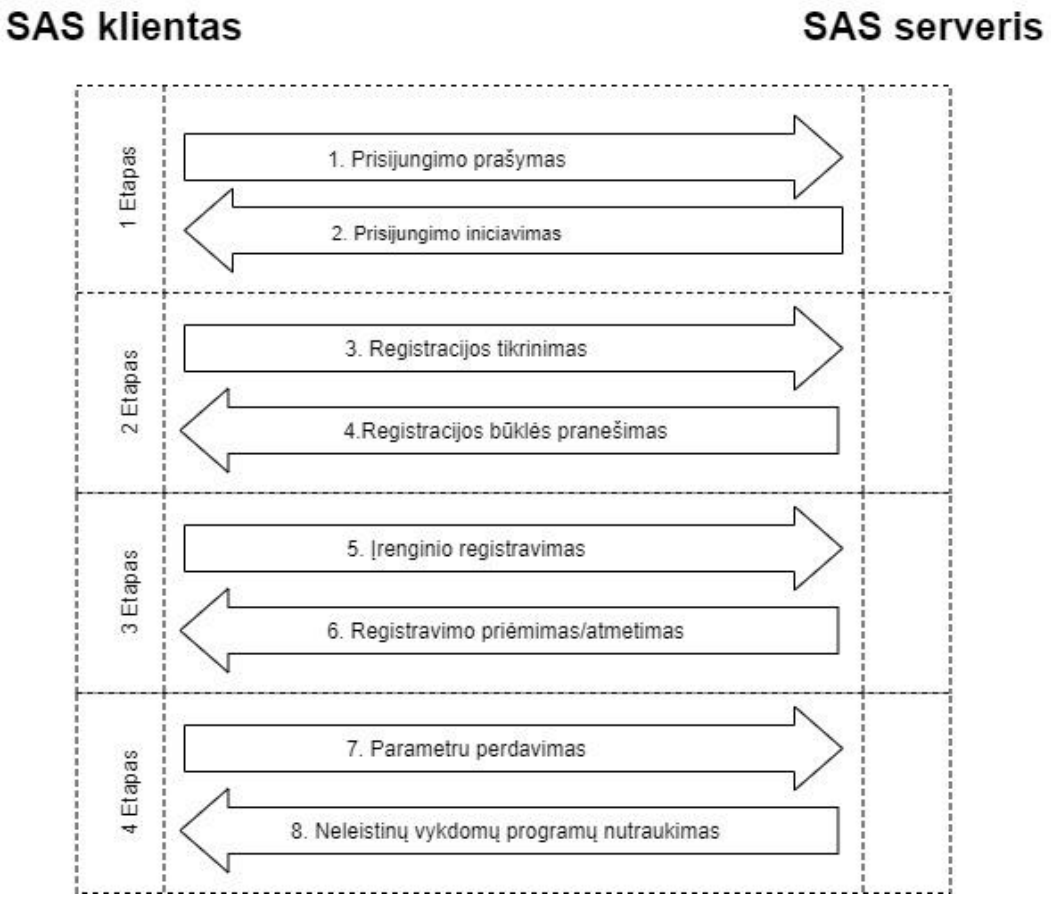
Komunikacijoms tarp kliento ir serverio yra naudojamas MQTT sistemos ypatumas, kur visos žinutės keliauja iš pranešėjo prenumeratoriui per tarpinį brokerio serverį. MQTT brokerio serveriu gali būti bet koks įrenginys tinkle, svarbiausia jis būtų pasiekiamas išoriniams vartotojams įrenginių bei vartotojų autentifikavimui.

15 pav. Asmeninių įrenginių saugaus autentifikavimo sistemos komunikavimo schema

Kiekvienas SAS sistemos klientas, kaip ir SAS serveris pirma užmezga ryšį su MQTT brokerio serveriu pasinaudojęs saugiu TLS ryšių bei x.509 sertifikato pagalba. Tokiu būdu yra užkertama prieiga piktavaliams, gavusiems prisijungimo prie brokerio informaciją, prisijungi ir gauti pranešimus siunčiamus iš brokerio į klientą arba serverį. TLS yra naudojamas įrenginio autentifikavimui, šifruojant siunčiamus duomenis viešuoju raktu, kuriuos serveris perskaito savo privataus rakto pagalba. Tai leidžia išvengti paketų perėmimo pažeidžiamumo, kuris leis piktavaliui pasisavinti perduodamus duomenis, arba pakeisti duomenis. Šitos problemos galime išvengti pasinaudoję x.509 sertifikato teikiamomis vartotojo autentifikavimo funkcionalumu. Tokiu būdu yra tikrinamas ne tik serveris, bet ir vartotojas norintis prisijungti prie brokerio serverio. Norint papildomai apsisaugoti nuo minimos duomenų perėmimo (MITM) grėsmės, reikia MQTT žinutės turinį užšifruoti, jog net ir perėmus žinutę jos būtų neįmanoma perskaityti.

Komunikacijos tarp serverio ir kliento ryšio bei žinučių apsauga yra reikalinga dėl žinutės turinio. Žinučių pagalbą yra perduodamos visos komandos iš serverio pusės į klientą. Šifravimo ir saugaus ryšio sudarymo pagalba mes pasiekiame jog žinučių apsikeitimas vyks tik su trimis sistemos dalyviais: klientu, brokeriu ir serveriu. SAS sistemos brokeris atlieka tik žinutės perdavimo procesą ir nežino nei kas yra parašytą žinutėje nei kam ją siunčia. Brokeris nesaugo jokios informacijos apie prisijungimus bei nekaupia adresų lentų, kuris IP adresas kam priklauso ir kokie vartotojai priklauso kokiam klientui. Taipogi SAS serveris nežino kur randasi klientas. Tai leidžia apsaugoti tiek klientus nuo serverio nulaužimo, tiek serverį kliento nulaužimo metu, tiek serverį su klientu nuo brokerio nulaužimo atvejo.

2.4. Asmeninių įrenginių registravimo procesas



16 pav. SAS sistemos įrenginių registravimo procesas

Norėdami autentifikuoti įrenginį bei vartotoją turime užregistruoti ne tik vartotoją, bet ir patį įrenginį. Įrenginio registravimas serveryje yra atliekamas 4 etapų procesu, kuriu metu serveris ir klientas apsikeičia informacija saugiu susijungimu.

1.Etapas: Saugaus ryšio užmezgimas tarp įrenginių, kurio metu yra tikrinami sertifikatai, naudojami saugaus ryšio sudarymui.

- Prisijungimo prašymas (16 pav.). Jo metu brokeriui yra siunčiama prisijungimo užklausa skirta saugaus ryšio sudarymui. Sudarius saugų ryšį tarp įrenginio ir brokerio, yra siunčiama autentifikavimo užklausa SAS serveriui (kliento autentifikavimo atveju).
- Prisijungimo iniciavimas. Vykdomas tik po prisijungimo prašymo autentifikavimo atsako. Sutapus visiems autentifikavimo parametrams yra leidžiama įrenginiui prisijungti prie serverio ir prie SAS serverio (kliento prisijungimo atveju).

2.Etapas: Įrenginio registracijos tikrinimas. Etapas skirtas patikrinti ar įrenginys yra registruotas SAS sistemoje.

- Registracijos tikrinimas – tikrinama įrenginio registracijos būklė. Jeigu įrenginys yra registruotas sistemoje 3 etapas yra praleidžiamas.
- Gavus atsakymą iš SAS serverio, jog įrenginys yra neregistruotas sistemoje, pereinama prie 3 etapo.

3.Etapas: Įrenginio registravimas sistemoje. Jeigu įrenginys yra neregistruotas sistemoje, pereinama prie įrenginio registravimo sistemoje.

- Įrenginio registravimas. Serveriui yra perduodamas unikalus registravimo kodas, kurį administratorius perduoda iš kliento įrenginio serveriui.
- Įrenginio registravimo priėmimas/atmetimas. Tikrinamas įrenginio siunčiamas registracijos kodas. Sutapus registracijos kodui yra pereinama į sekantį etapą , kuriame perduodami visa įrenginio informaciją, reikalinga registracijos užbaigimui.

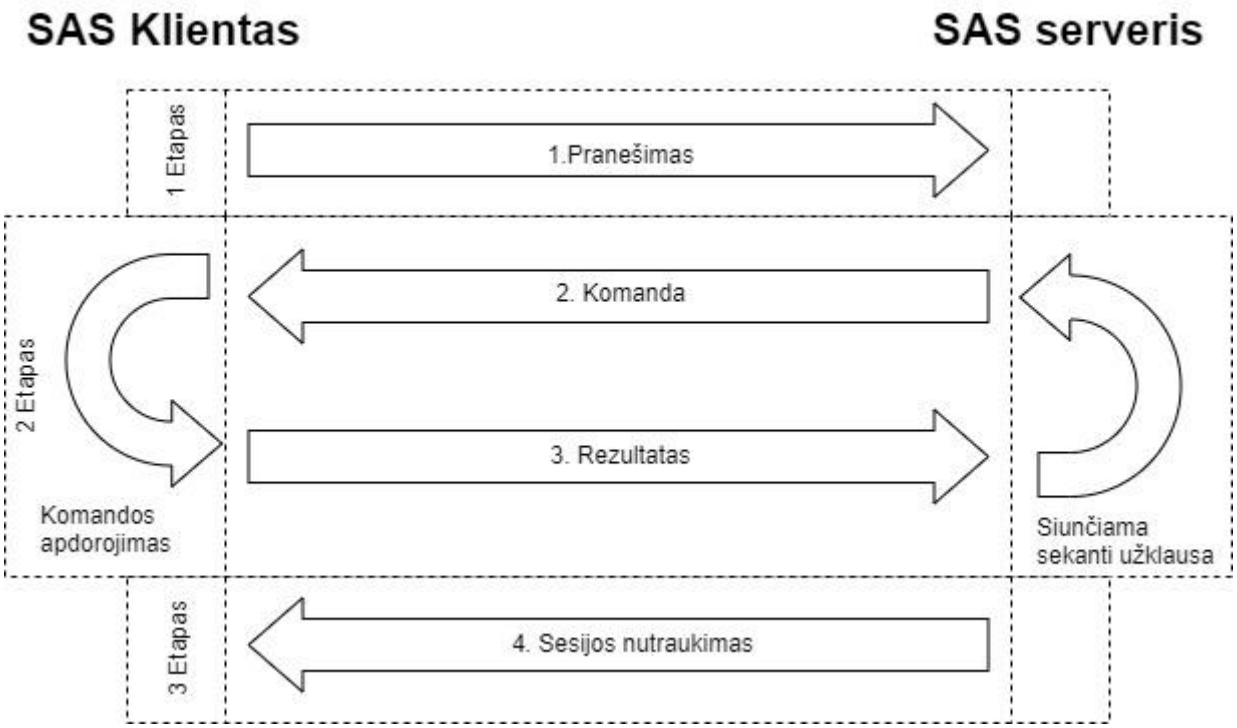
4.Etapas: Įrenginio informacijos perdavimas SAS serveriui.

- Parametrų perdavimas. Įrenginio registravimo metu sistemoje, serveris užprašo įrenginio persiųsti savo unikalius parametrus. Kartu su įrenginio parametrais yra siunčiamos ir vykdomos programos įrenginyje, kurios yra nutraukiamos kito žingsnio metu.
- Neleistinų vykdomų programų nutraukimas. SAS serveris persiunčia programų sąrašą, kurias SAS kliento programa nutraukia be jokio vartotojo įsikišimo.

4 lentelė. Įrenginio siunčiami parametrai

Parametras	Apibūdinimas
Vartotojo vardas	Dabar prisijungusio prie įrenginio vartotojo vardas (SID)
Kompiuterio vardas	Vardas kuriuo identifikuojamas įrenginys sistemoje
CPU revizija	Unikalus kodas kuris priklauso konkrečiam procesoriui, rodo procesoriaus revizija, kuri gali priklausyti keletui procesorių.
CPU Procesoriaus ID	Unikalus kodas, priklausantis konkrečiam procesoriui, rodo identifikacinį numerį.
RAM atminties dydis	RAM atminties dydis sistemoje, kiekvieno lusto atskirai.
RAM įrenginio vieta	RAM atmintinės vieta motininėje plokštėje, kiekvieno įrenginio atskirai.
RAM serijinis numeris	Unikalus RAM atmintinės lusto numeris.
RAM greitis	RAM atmintinės greitis, kiekvieno lusto atskirai
Pagrindinės atminties serijinis numeris	Sistemoje instaliuotu atminties įrenginio (-inių) serijiniai numeriai, unikalūs tik tam įrenginiui.
Pagrindinės atminties valdymo kodo revizija	Versijos numeris , kokia valdymo kodo revizija yra įdiegta įrenginyje
Pagrindinės atminties pajungimo tipas	Atminties pajungimo tipas SATA, SAS, PCI-E
Pagrindinės atminties modelis	Įrenginio modelis su jo tipu SSD, HDD
Pagrindinės atminties dydis	Atminties dydis šiuo metu esantis kompiuteryje
Motininės plokštes produkto vardas	Faktinis motininės plokštės gamintojo suteiktas vardas
Motininės plokštės serijinis numeris	Unikalus numeris priklausantis konkrečiai plokštei
BIOS gamintojas	Gamintojo pavadinimas
BIOS versija	Versija įrašyta motininėje plokštėje

2.5. Asmeninių įrenginių tikrinimo ir valdymo procesas



17 pav. SAS sistemos tikrinimo ir valdymo procesas

Autentifikavus įrenginį jam leidžiama prisijungti prie sistemos. 17 pav. yra pavaizduota SAS sistemos vientisumo tikrinimo ir įrenginių valdymo procesas. Serverio komandų perdavimui įrenginiui gali būti tiek inicijuojama nauja sesija, tiek naudojama anksčiau užmegzta sesija.

1.Etapas: Pranešimas. Siunčiamas SAS serveriui, apie įrenginio pasiruošimą vykdyti komandas bei jo būklę.

- Pranešimas. Prisijungęs prie sistemos įrenginys persiunčia SAS serveriui pasiruošimo vykdyti komandas pranešimą, kartu pranešdamas apie savo būklę sistemoje. Pranešimas yra siunčiamas tik po sėkmingos autentifikacijos ir registracijos patikrinimų.

2.Etapas: Serverio siunčiamu komandų vykdymas. Šiame etape SAS kliento įrenginys vykdo SAS serverio siunčiamas užklausas.

5 lentelė. Serverio klientui perduodamos komandos

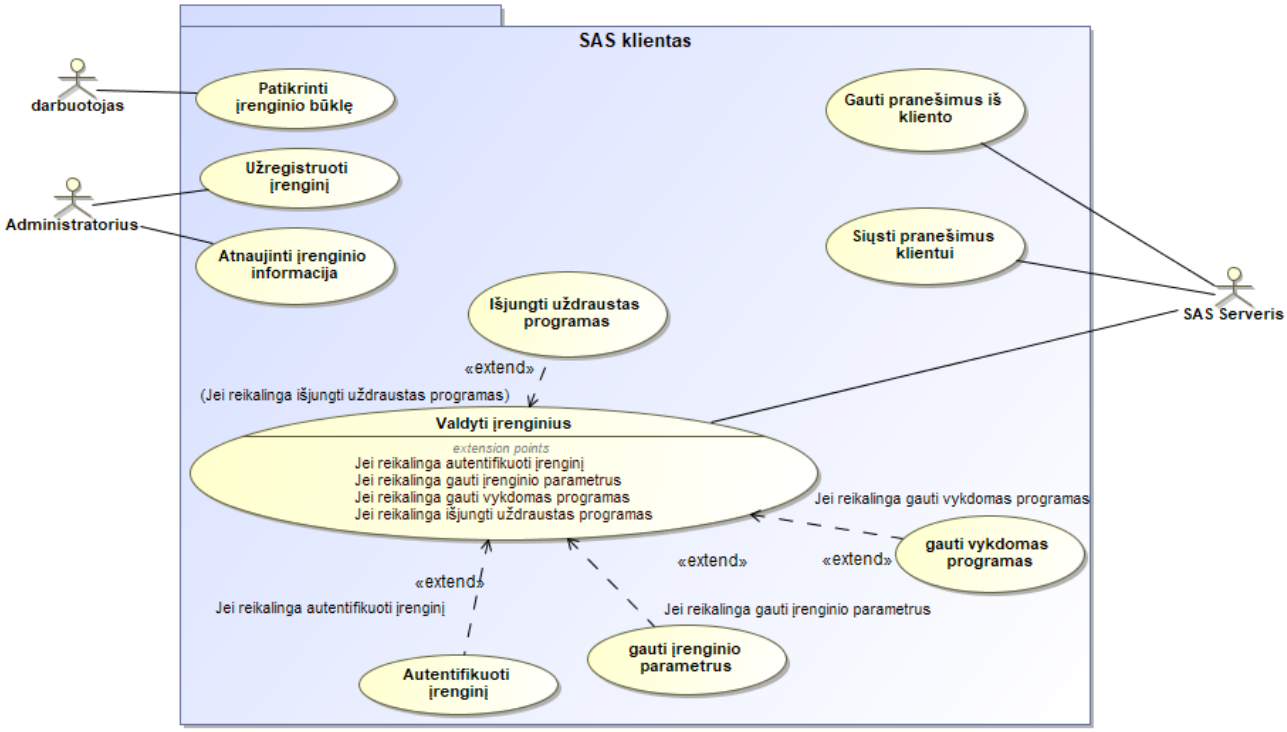
Komanda	Aprašymas
Pasisveikinimo komanda	Serveris persiunčia pasisveikinimo su įrenginių komanda, tuo pačiu pranešant kad pasiruošęs priimti užklausas iš kliento bei apie saugaus ryšio sudarymą
Registracijos būklės atsakymas	Serveris persiunčia dabartinės įrenginio būklės parametrus įrenginiui, esant neregistruotam, įrenginys persiunčia užklausa įrenginio registravimui.
Registracijos kodo siuntimo komanda	Šį komanda persiunčia įrenginio registracijos kodą serveriui.
Duomenų atnaujinimo kodo siuntimo komanda	Šį komanda persiunčia įrenginio duomenų atnaujinimo kodą serveriui.

Blogo kodo pranešimo komanda	Serveris praneša apie neteisingą gautą kodą. Gavus šita komanda yra nutraukiamas darbas su sistema ir atjungiama programa.
Pažeisto įrenginio vientisumo pranešimo komanda	Šį komanda praneša įrenginiui jog yra pasikeitę jo parametrai, nutraukiamas darbas su sistema ir jam nebus toliau leidžiama dirbti sistemoje. Leidimą dirbti sistemoje gali grąžinti tik sistemos administratorius.
Programos darbo nutraukimo komanda	Šį komanda vykdo neleidžiamų programų nutraukimą SAS kliento įrenginyje, nutraukiant visų gautų programų sąrašą, gauta kartu su komanda.
Parametrų perdavimo komanda	Šį komandą surenka, bei perduoda juos serveriui kartu su unikaliu įrenginio kodu. Įrenginio perduodami parametrai surašyti 4 lentelėje.

3. Etapas: Sesijos nutraukimas. Vykdomas keletu atveju. Dažniausiai norėdamas apsisaugoti, serveris pirmas nutraukia sesiją, pastebėjęs bet kokius neatitikimus sistemos veikime. Taipogi sesija gali būti nutraukiama praradus ryšį su SAS serveriu arba tarpiniu MQTT brokeriu.

2.6. Asmeninių įrenginių saugaus autentifikavimo sistemos prototipas

Asmeninių įrenginių saugaus autentifikavimo sistemos prototipo veikimą aprašome SAS kliento ir SAS serverio panaudos atvejų diagramomis.



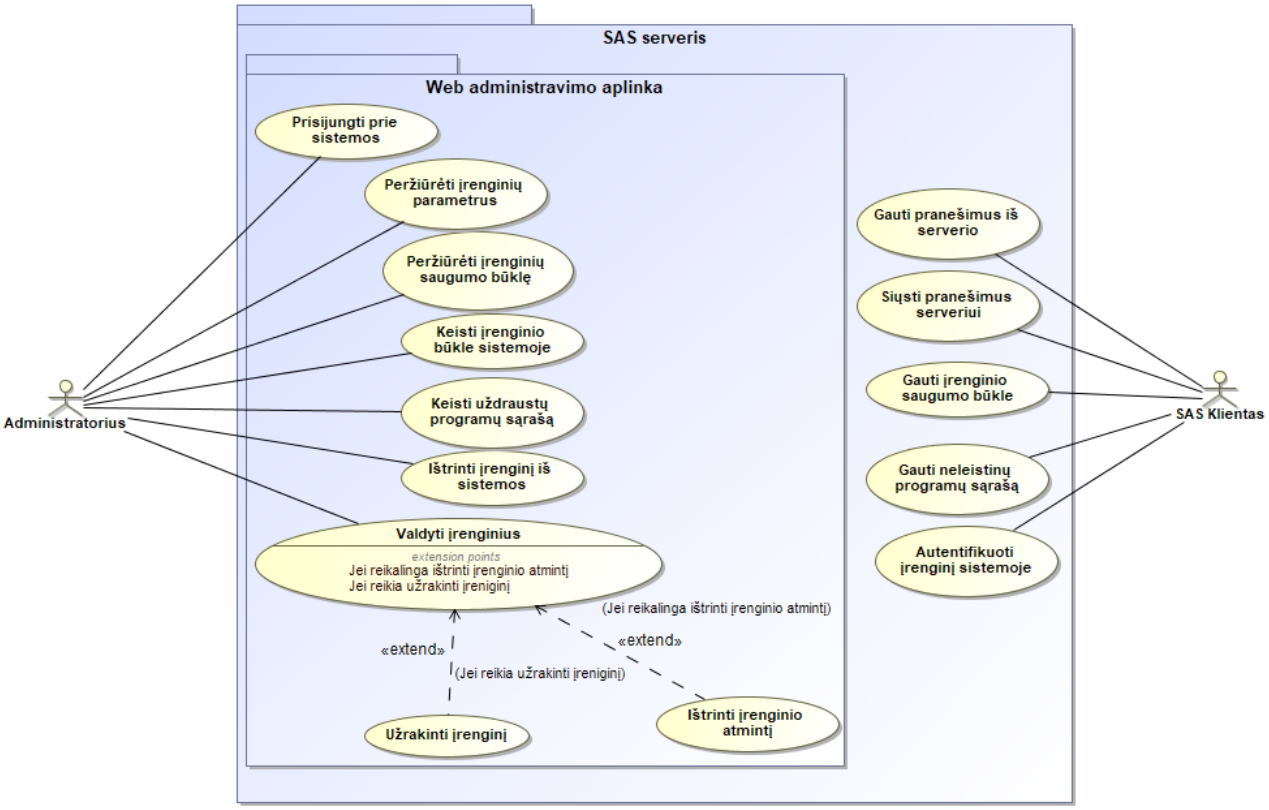
18 pav. SAS sistemos kliento panaudos atvejų diagrama

18 pav. pateikta SAS sistemos kliento pusės programos panaudos atveju diagrama. Joje matome keturis aktorius, kurie sąveikauja su kliento programinę įrangą. 6 lentelėje pateikiame panaudos atveju sąveikas su aktoriais, kokius duomenis perduoda bei kokį funkcionalumą atlieka.

6 lentelė. SAS sistemos kliento panaudos atvejai

Panaudos atvejis:	Patikrinti įrenginio būklę
Tikslas: Patikrinti įrenginio būklę sistemoje Aktorius: darbuotojas	Aprašymas: Darbuotojas prieš pradedant darbą su sistema ir prisijungdamas prie sistemos įsitikina jog įrenginys yra saugus. Programa pateikia saugumo būklę.
Panaudos atvejis:	Užregistruoti įrenginį
Tikslas: Užregistruoti įrenginį sistemoje Aktorius: Administratorius	Aprašymas: Administratorius įrenginio registravimo etape perduoda registravimo slaptažodį serveriui. Serveriui pateikus teigiamą atsakymą apie slaptažodžio sutapimą yra užprašomi įrenginio parametrai. Kartu su parametrais yra registruojamos visos įrenginyje įdiegtos programos, nutraukiant neleistinų programų darbą procese.
Panaudos atvejis:	Atnaujinti įrenginio informacija
Tikslas: Atnaujinti įrenginio registruotus parametrus sistemoje pakeitimo atveju Aktorius: Administratorius	Aprašymas: Įrenginio parametrų pakeitimo atveju, įrenginys praranda vientisumo žymę. Norint gražinti įrenginiui saugumo žymę, administratorius inicijuoja įrenginio parametrų atnaujinimą, perduoda atnaujinimo kodą sistemoje. Sėkmės atveju, serveris užprašo įrenginio parametru ir atnaujina juos sistemoje.
Panaudos atvejis:	Valdyti įrenginius
Tikslas: Valdyti įrenginį Aktorius: SAS serveris	Aprašymas: Sistema, siunčiant pranešimus brokerio pagalbą, gali valdyti įrenginį, kartu jį autentifikuojant. Valdymo metu serveris gali : gauti įrenginio parametrus, gauti šiuo metu vykdomų programų sąrašą bei siųsti neleistinų programų darbo nutraukimo komandą, kuri nutrauks visas programas iš pateikto sąrašo.
Panaudos atvejis:	Autentifikuoti įrenginį
Tikslas: Autentifikuoti įrenginį sistemoje Aktorius: SAS serveris Susiję PA: Valdyti įrenginį	Aprašymas: Norėdami užtikrinti saugų darbą sistemoje turime įsitikinti jog įrenginys yra registruotas sistemoje ir jo parametrai atitinka sistemoje registruotus parametrus. Serveris išsiunčia autentifikavimo užklausa klientui, kurios metu įrenginys persiunčia savo parametrus kartu su unikaliu kodu. Sėkmės atveju įrenginys yra autentifikuojamas sistemoje.
Panaudos atvejis:	Gauti įrenginio parametrus
Tikslas: Gauti visus įrenginio parametrus Aktorius: SAS serveris Susiję PA: Valdyti įrenginį	Aprašymas: Serveris siunčia užklausa kliento programai, perduoti visus įrenginio parametrus. Įrenginys atsakymo metu persiunčia visus parametrus.
Panaudos atvejis:	Gauti vykdomas programas
Tikslas: Gauti visų įrenginyje vykdomu programų sąrašą Aktorius: SAS serveris Susiję PA: Valdyti įrenginį	Aprašymas: Serveris įrenginiui atsiunčia užklausa, skirta gauti visas programas kurios yra vykdomos šiuo metu įrenginyje. Sugeneruotas sąrašas persiunčiamas serveriui.
Panaudos atvejis:	Išjungti uždraustas programas
Tikslas: Nutraukti neleistinų programų veikimą įrenginyje Aktorius: SAS serveris Susiję PA: Valdyti įrenginį	Aprašymas: Serveris klientui persiunčia sąrašą programų, kuriu darbas turi būti nutrauktas įrenginyje. Sąrašas yra generuojamas patikrinus visas paleistas programas įrenginyje su neleistinų vykdyti programų sąrašu sistemoje.
Panaudos atvejis:	Gauti pranešimus iš kliento
Tikslas: gauti pranešimus Aktorius: SAS serveris	Aprašymas: SAS serveris priima pranešimus siunčiamus kliento. Pranešimai gali būti informacinio tipo, apie įvykdytas komandas arba klaidos tipo, pranešantis apie klaidą sistemos veikime.

Panaudos atvejis:	Siųsti pranešimus klientui
Tikslas: Siųsti žinutes skirtas kliento programai	Aprašymas:. SAS serveris gali siųsti pranešimus klientui. Pranešimas gali būti tiek informacinio tipo, skirto pranešti apie įrenginio būkle sistemoje, tiek gali turėtu savyje komandą, kuria įrenginys turi įvykdyti ir atsakyti į serverio užklausą.
Aktorius: SAS serveris	



19 pav. SAS sistemos serverio panaudos atvejų diagrama

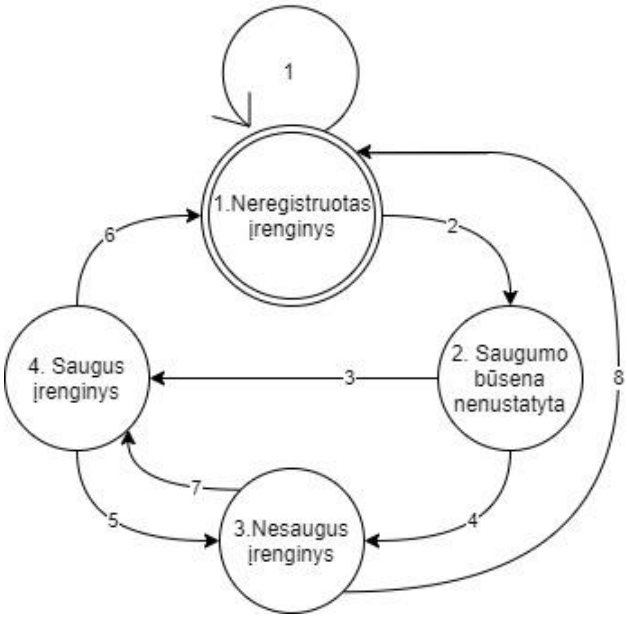
19 pav. Pateikiame SAS sistemos serverio dalies panaudos atvejų diagramą. Iš jos matome, jog WEB administravimo aplinka gali naudotis tik vienas aktorius: administratorius. Panaudos atvejai kuriais sistema sąveikauja su kitais sistemos dalyviais yra aprašoma 7 lentelėje.

7 lentelė. SAS sistemos serverio panaudos atvejai

Panaudos atvejis:	Prisijungti prie sistemos
Tikslas: Prisijungti prie WEB administravimo aplinkos	Aprašymas: Prieš pradedant darbą su sistema, administratorius turi prisijungti prie sistemos. Prisijungimui naudojami vartotojo vardas ir slaptažodis
Aktorius: Administratorius	
Panaudos atvejis:	Peržiūrėti įrenginių parametrus
Tikslas: Peržiūrėti sistemoje registruotų įrenginių išsaugotus parametrus	Aprašymas: Administratorius sistemoje gali peržiūrėti visus registruotus įrenginius, bei pažiūrėti jų vidinius parametrus pateiktus 4 lentelėje.
Aktorius: Administratorius	
Panaudos atvejis:	Peržiūrėti įrenginių saugumo būklę

Tikslas: Peržiūrėti esama visų registruotų sistemoje įrenginių būklę Aktorius: Administratorius	Aprašymas: Administratorius sistemoje gali peržiūrėti visų įrenginių saugumo būkles, kurios kinta automatiškai sistemai aptikus įrenginio parametrų pakitimus.
Panaudos atvejis:	Keisti įrenginio būklę sistemoje
Tikslas: Pakeisti įrenginio būklę iš registruotas nesaugus į registruotas saugus Aktorius: Administratorius	Aprašymas: Pakitus įrenginio parametrams, bei Administratoriui įsitikinus jog įrenginio parametrai buvo pakeisti paties vartotojo o ne buvo bandymas MITM atakos, administratorius turi galimybę atnaujinti įrenginio parametrus sistemoje , perdavęs įrenginiui vienkartinį atnaujinimo kodą.
Panaudos atvejis:	Keisti uždraustų programų sąrašą
Tikslas: Keisti leidžiamų ir neleidžiamų vykdyti programų sąrašus sistemoje Aktorius: Administratorius	Aprašymas: Administratorius turi galimybę sistemoje sudaryti leidžiamų ir neleidžiamų vykdyti programų sąrašus. Esant poreikiui administratorius turi galimybę juos koreguoti.
Panaudos atvejis:	Ištrinti įrenginį iš sistemos
Tikslas: Pašalinti įrenginį iš sistemos. Aktorius: Administratorius	Aprašymas: Administratorius turi galimybę ištrinti įrenginį iš sistemos, tuo pačiu uždraudžiant įrenginiui tolimesnį darbą su sistema.
Panaudos atvejis:	Valdyti įrenginius
Tikslas: Siųsti įrenginiui komandas Aktorius: Administratorius	Aprašymas: Administratorius turi galimybę savo noru siųsti komandas įrenginiams. Administratorius gali siųsti dvi komandas: užrakinti įrenginį bei ištrinti įrenginio atmintį.
Panaudos atvejis:	Užrakinti įrenginį
Tikslas: Nutraukti darbuotojo dirbančio su įrenginiu darbo sesija Aktorius: Administratorius Susiję PA: Valdyti įrenginius	Aprašymas: Administratorius turi galimybę nuotoliniu būdu užrakinti įrenginį. Įrenginio atrakinimas gali būti vykdomas nuotoliniu būdu arba gavus vienkartinį atblokavimo kodą.
Panaudos atvejis:	Ištrinti įrenginio atmintį
Tikslas: pašalinti visą konfidencialią informaciją iš įrenginio Aktorius: Administratorius Susiję PA: Valdyti įrenginius	Aprašymas: įrenginio praradimo atveju, arba esant poreikiui Administratorius turi galimybę nuotoliniu būdu paleisti įrenginio atminties išvalymo komandą. Atminties išvalymo metu gali būti ištrinama visa įrenginio atmintis.
Panaudos atvejis:	Gauti pranešimus iš serverio
Tikslas: Gauti pranešimus siunčiamas serverio klientui. Aktorius: SAS klientas	Aprašymas: SAS klientas bendrauja su serveriu pranešimu pagalbą, klientas turi galimybę gauti visas žinutes siunčiamas serverio klientui. Žinutės gali būti tiek informacinio tipo, tiek komandos vykdymui.
Panaudos atvejis:	Siųsti pranešimus serveriui
Tikslas: Siųsti pranešimus su komandų vykdymo rezultatais Aktorius: SAS klientas	Aprašymas: klientas turi galimybę siųsti pranešimus serveriui. Pranešimai yra informacinio tipo, skirti pranešti apie įrenginio pasiruošimą priimti ir vykdyti komandas, bei rezultatu tipo, skirti pranešti apie komandos vykdymo rezultatus.
Panaudos atvejis:	Gauti įrenginio saugumo būklę
Tikslas: Gauti įrenginio saugumo būklės ataskaitą Aktorius: SAS klientas	Aprašymas: klientas kiekvieno prisijungimo metu, bei periodiškai praėjus nustatytam laiko tarpui turi galimybę gauti informaciją apie savo saugumo būklę. Įrenginiui gavus komandą perduoti savo parametrus serveriui, atsakas į tokia komandą klientui išsiuntus savo parametrus yra saugumo būseną. Pakitus parametrams kinta ir saugumo būseną.
Panaudos atvejis:	Gauti neleistinų programų sąrašą
Tikslas: Gauti neleistinų vykdyti programų sąrašą iš serverio Aktorius: SAS klientas	Aprašymas: klientas turi galimybę gauti sąrašą programų, kuriu negalima vykdyti įrenginyje. Klientui radus vykdomą programą kuri yra neleistinų sąraše, programos vykdymas yra nutraukiamas.

Panaudos atvejis:	Autentifikuoti įrenginį sistemoje
Tikslas: Patvirtinti įrenginio ir vartotojo tapatybes	Aprašymas: Klientas turi galimybę prašyti SAS serverio patvirtinti įrenginio bei dabartinio vartotojo tapatybes. Sutapus tapatybėms, įrenginiui yra leidžiama dirbti sistemoje.
Aktorius: SAS klientas	

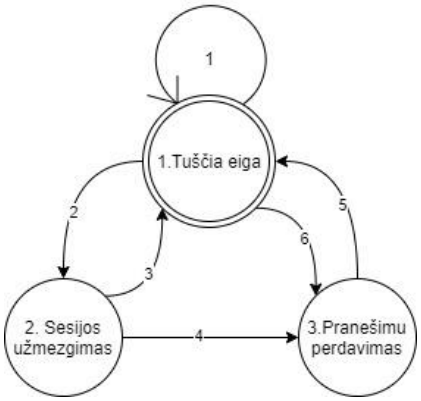


20 pav. SAS sistemos kliento būsenų diagrama

20 pav. Matome, jog kliento programa turi 4 būsenas. Įrenginys visada yra skaitomas neregistruotu tol, kol nėra patikrinama jo registravimo būseną. Patikrinus registravimo būsena toliau yra tikrinamas įrenginio saugumas, įrenginiui nėra leidžiama dirbti sistemoje kol jis neatsiranda 4 saugumo būsenoje. Būsenų pasikeitimai yra aprašomi 8 lentelėje.

8 lentelė. SAS sistemos kliento būsenų pasikeitimai

Perėjimo Nr.	Pradinė būseną	Pokytis	Sekanti būsena	Rezultatas
1	Įrenginys neregistruotas	Nepavyko užregistruoti / patikrinti registracijos	Įrenginys neregistruotas	Neleidžiama dirbti, pranešama administratoriui, parodomas klaidos pranešimas.
2		Įrenginys registruotas / leidžiama registracija	Saugumo būsena nenustatyta	Pradedama registracija su visų duomenų surinkimu.
3	Saugumo būsena nenustatyta	Įrenginys atitiko visus saugumo reikalavimus	Saugus įrenginys	Įrenginiui yra leidžiama dirbti sistemoje
4		Įrenginys neatitiko saugumo reikalavimų	Nesaugus įrenginys	Įrenginiui neleidžiama dirbti sistemoje
5	Saugus įrenginys	Pakito įrenginio parametrai / nenutraukta neleistina programa	Nesaugus įrenginys	Įrenginio darbas sistemoje yra nutraukiamas.
6		Įrenginys ištrinamas iš sistemos	Neregistruotas įrenginys	Įrenginiui neleidžiama dirbi sistemoje
7	Nesaugus įrenginys	Administratorius atnaujino įrenginio parametrus sistemoje	Saugus įrenginys	Įrenginiui yra leidžiama dirbti sistemoje
8		Įrenginys ištrinamas iš sistemos	Neregistruotas įrenginys	Įrenginiui neleidžiama dirbi sistemoje

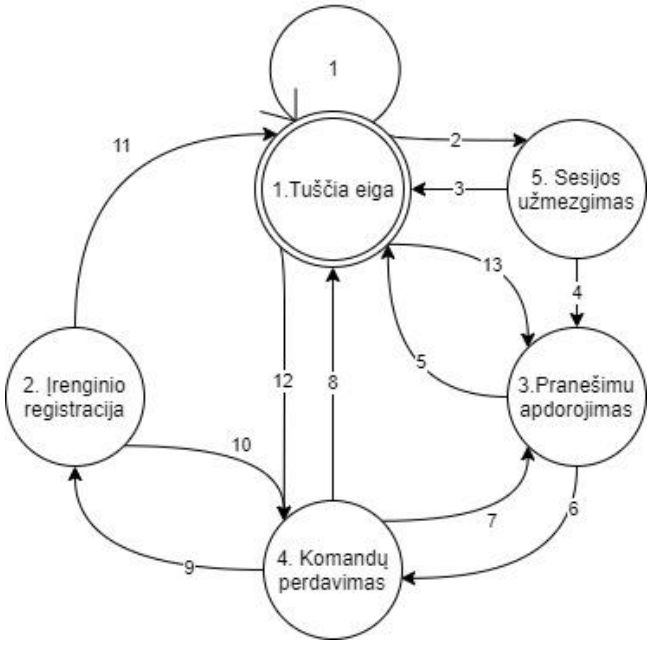


21 pav. SAS sistemos brokerio būsenų diagrama

21 pav. matome SAS sistemos brokerio veikimo būsenas. Brokeris gali būti trijose būsenose. Pagrindinė būseną yra „ tuščia eiga“. Šioje būsenoje brokeris būna klientams ir serveriui sudarius ir nesudarius sesijos. Visi pranešimai yra persiunčiami tik prenumeratorių registruotomis temomis. Būsenų pasikeitimai aprašomi 9 lentelėje.

9 lentelė. SAS sistemos brokerio būsenų pasikeitimai

Perėjimo Nr.	Pradinė būseną	Pokytis	Sekanti būsena	Rezultatas
1	Tuščia eiga	-	Tuščia eiga	-
2		Serveris arba klientas prašo sesijos užmezgimo	Sesijos užmezgimas	Autentifikuojamas įrenginys, leidžiama sudaryti sesija
3	Sesijos užmezgimas	Sesija nutraukiama arba neleidžiama sudaryti sesijos	Tuščia eiga	-
4		Sudaryta sesija ir vienas iš dalyvių pradeda siųsti pranešimus	Pranešimu perdavimas	Pranešimai perduodami prenumeratoriams
5	Pranešimu perdavimas	Visi gauti pranešimai yra perduoti	Tuščia eiga	-
6	Tuščia eiga	Gaunami nauji pranešimai iš jau sudarytos sesijos	Pranešimu perdavimas	Visi gauti pranešimai perduodami prenumeratoriams



22 pav. SAS sistemos serverio būsenų diagrama

22 pav. matome, jog SAS sistemos serveris turi 5 būsenas. Pagrindinė būseną yra „ tuščia eiga“ . Serveris šioje būsenoje būna iki tol, kol nepraranda ryšio su brokeriu, negauna naujo pranešimo, arba naujos komandos. Serverio dalies būsenų pasikeitimai aprašomi 10 lentelėje.

10 lentelė. SAS sistemos serverio būsenų pasikeitimai

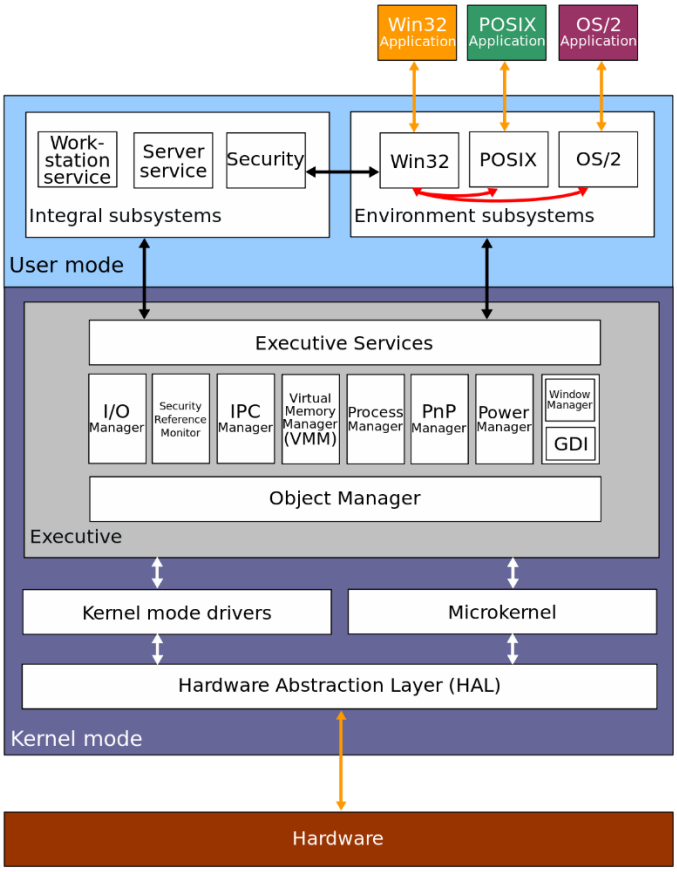
Perėjimo Nr.	Pradinė būseną	Pokytis	Sekanti būsena	Rezultatas
1	Tuščia eiga	-	Tuščia eiga	-
2		Serveris sudaro sesija su brokeriu	Sesijos užmezgimas	Bandoma užmegzti sesija su brokeriu.
3	Sesijos užmezgimas	Nesėkmingas sesijos sudarymas	Tuščia eiga	-
4		Sėkmingai sudaryta sesija	Pranešimu apdorojimas	Apdorojami pranešimai gaunami iš brokerio
5	Pranešimu apdorojimas	Apdoroti visi pranešimai gauti iš brokerio	Tuščia eiga	-
6		Pranešimas yra atsakymas į komandą	Komandų perdavimas	Perduodamas pranešimas komandų perdavimo moduliui
7	Komandų perdavimas	Siunčiama komanda įrenginiui	Pranešimu apdorojimas	Pranešimas yra išsiunčiamas įrenginiui brokerio pagalba
8		Visos komandos perduotos	Tuščia eiga	-
9		Gauta įrenginio registracijos komanda	Įrenginio registracija	Registruojamas įrenginys sistemoje
10	Įrenginio registracija	Perduodamas klaidos pranešimas	Komandų perdavimas	Perduodamas klaidos pranešimas persiuntimui į įrenginį
11		Įrenginys registruotas sistemoje	Tuščia eiga	-
12	Tuščia eiga	Gaunama ciklinės komandos užklausa	Komandų perdavimas	Išsiunčiamas pranešimas įrenginiui įvykdyti komandą.
13		Gaunamas naujas pranešimas iš sudarytos sesijos	Pranešimu apdorojimas	Pranešimas yra apdorojamas ir perduodamas toliau grandine

2.7. Pasirinktų Asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistemos prototipas

Šiame skyriuje yra pateikiamas asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistemos prototipas. Pateikiama realizacijai panaudotų technologijų apžvalga bei apibrėžiama kokios sistemos dalys yra realizuotos prototipe.

2.7.1. Pasirinktų technologijų apžvalga

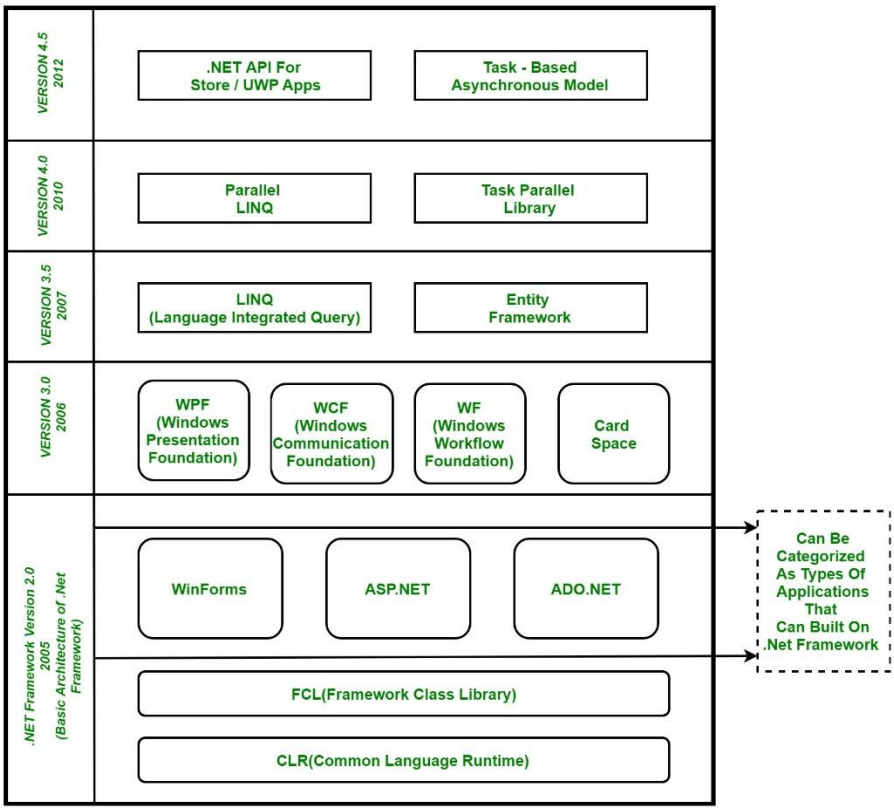
Tyrimą buvo nuspręsta atlikti naudojant Windows OS platformą. Todėl šiai platformai buvo sukurtas kliento programinės įrangos prototipas ir serverio programinės įrangos prototipas. Sprendimą įtakojo tai, jog „Windows“ yra plačiausiai naudojamą nešiojamų kompiuterių operacinė sistema [18], bei gali būti naudojama ne tik nešiojamiems įrenginiams.



23 pav. Windows NT architektūra

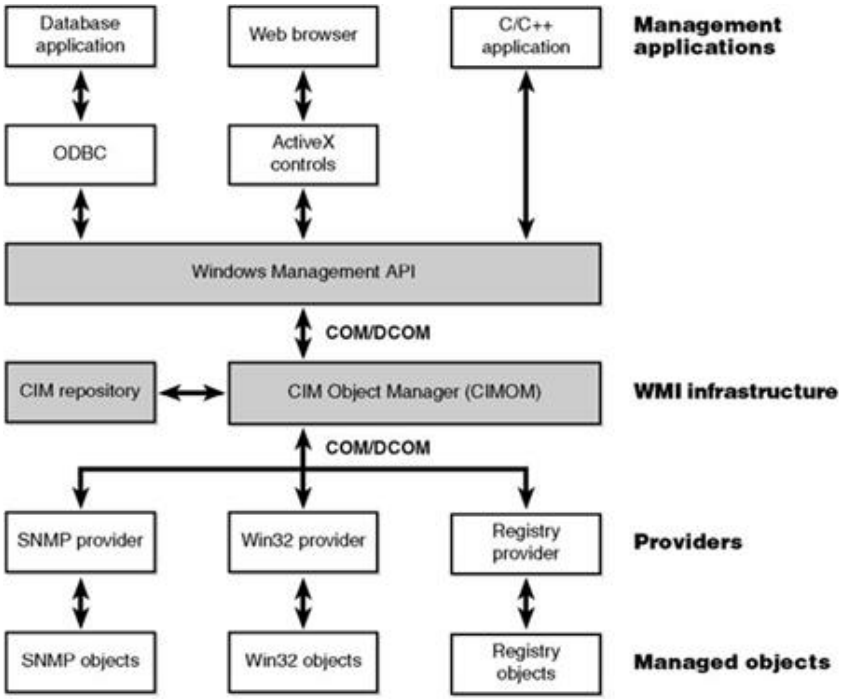
Microsoft Windows operacinė sistema yra grafinė operacinė sistema, sukurta ir platinama Microsoft korporacijos. Ji teikia platų funkcionalumą, tačiau galime išskirti tris pagrindines Windows funkcijas: grafine vartotojo sąsaja, failų sistema ir interneto naršyklė. Šiame darbe apžvelgsime naujausią darbo rašymo metu „Windows 10” operacinę sistema. Operacinė sistema yra labai lanksti valdymo atžvilgiu, priklausomai nuo naudojamo įrenginio, ja galima valdyti tiek gestais, tiek išoriniais manipuliatoriais (pelytė, klaviatūra, rašiklis...). Taipogi vartotojas gali apsieiti visiškai be išoriniu manipuliatorių. Esant poreikiui, vartotojas gali pasinaudoti virtualia klaviatūrą ir gestu pagalbą valdyti visą Windows operacinės sistemos teikiamas galimybes. Nors Windows operacinės sistemos buvo pritaikytos tik asmeniniams kompiuteriams, nuo 2004 metų pastebima nešiojamų įrenginių tendencija, nukreipė Windows operacinę sistemą universalumo keliu. Windows 10 operacinė sistema gali būti naudojama tiek personaliniuose kompiuteriuose, tiek mobiliuosiuose įrenginiuose.

Windows operacinei sistemai programos gali būti kuriamos įvairiomis kalbomis. Šiame darbe pasirinkta yra c# programavimo kalba. Sprendimą įtakojo tai, kad C# kalba yra populiariausia kuriant programine įranga Windows platformai, taipogi jos integracija su Windows OS ir teikiamais privalumais sumažinti naudojamų išorinių bibliotekų kiekį darbe.



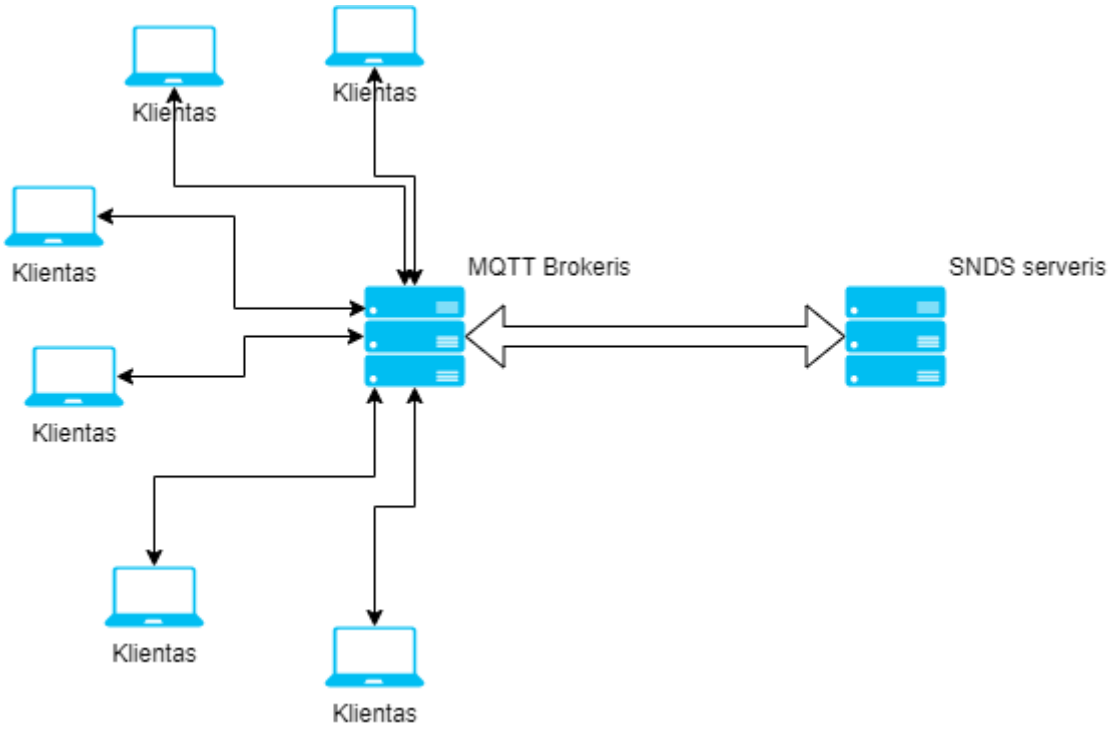
24 pav. C# karkaso architektūra

Taipogi darbe yra naudojama *Windows Management instrumentation* (toliau WMI) standartas. WMI suteikia vieningą prieigą prie visos kompiuterio administracinės informacijos. Informacija galima pasiekti per scenarijus (angl. scripts), C++ programavimo sąsajas, *dot net* klases (*system.management*, kurios yra naudojamos darbe) bei „*command line tool* (cmd, WMIC) teikiamas galimybes.



25 pav. WMI karkaso architektūra

Duomenų perdavimui buvo pasirinktas MQTT protokolas. MQTT protokolas buvo pasirinktas dėl jo pranešimų siuntimo proceso, bei sistemos resursų naudojimo. Ateityje yra planuojama sistema praplėsti į resursais suvaržytas sistemas, tokias kaip mobilieji telefonai.



26 pav. MQTT architektūra

MQTT žinučių siuntimui naudoja MQTT brokerio serverį, prie kurio jungiasi visi vartotojai. Prisijungimas vyksta tik su MQTT brokerio pagalba [19, 20]. Ne vienas iš klientų nežino kur randasi SAS serveris, taip kaip SAS serveris jungiasi prie brokerio tuo pačiu būdu kaip ir klientai, tik skirtingai nuo klientu, turi visus duomenis apie esamus klientus. Sujungimai su brokeriu yra realizuojami *publish / subscribe* metodo pagalbą, kur kiekvienas klientas siunčia (*publish*) duomenis tik į jam skirtą temą (*topic*). Taipogi klientai prisijungia (*subscribe*) prie jiems skirtos temos, kur gauną komandas siunčiamas įrenginiui. SAS serveris prisijungia (*subscribe*) prie visų registruotų įrenginių temų (*topic*) sistemoje. Prisijungęs serveris gauna visus pranešimus, siunčiamus klientu brokeriui. Norint išvengti žinučių praradimo, yra naudojamas MQTT *QoS* teikiamos galimybės, kur brokeris turi įsitikinti jog gautas žinutes gaus prisijungęs prie tų temų SAS serveris.

MQTT teikia ryšio modelį, kuris tinka apsaugoti SAS serverį nuo tiesioginio prisijungimo prie klientų. Tačiau MQTT siunčia pranešimus ir gauna juos atviru tekstu. Norint tinkamai apsaugoti pranešimus tarp nutolusių vartotojų, turime užtikrinti saugų ryšį tarp klientu, MQTT brokerio ir SAS serverio.

Saugaus ryšio, nesaugioje viešoje terpėje, užtikrinimui pasinaudosime VPN teikiamais saugumo sprendimais [16]. Naudosime *IPSec* VPN protokolą, dėl jo teikiamų įrenginio autentifikavimo galimybių ir kitų teikiamų privalumų. Autentifikuojant kliento įrenginį, yra atsižvelgiama tik į jo MAC tinklo plokštės adresą, bet ne į kitus prijungtus komponentus. Norint užtikrinti kompiuterio aparatūrinį vientisumą, turime atsižvelgti į visus kompiuterio įrenginius , registracijos metu sudokumentuoti kokie yra prijungti įrenginiai ir kokia yra jų konfigūracija.

Prisijungę prie įmonės tinklo, tinklo viduje MQTT žinutės vis tiek bus atviru tekstu. Sprendžiant šitą problemą buvo pasitelkta TLS protokolo pagalbą. Srautas tarp kliento ir brokerio yra papildomai apsaugomas TLS protokolu, kas sudaro dviguba paketų apsaugą.
Trečio lygio apsauga bus teikiama šifruojant MQTT pranešimo turinį, pasinaudojant šifravimo algoritmu.

Sprendžiant iš [17, 21, 22] straipsniuose pateiktos informacijos, apie saugius šifravimo algoritmus buvo nuspręsta naudoti „Blowfish“ šifravimo algoritmą, taip kaip jis suteikia didžiausią šifravimo lygį bei yra sunkiausiai nulaužiamas.

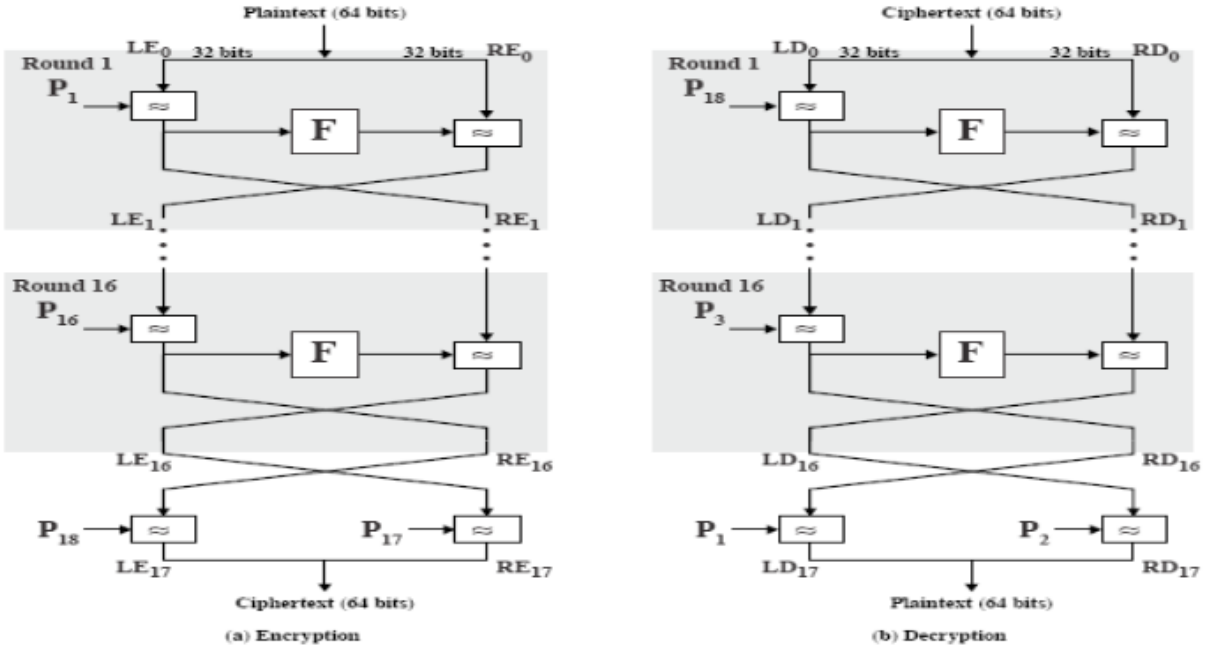


Figure 6.3 Blowfish Encryption and Decryption

27 pav. *Blowfish* šifravimo algoritmo kodavimas ir dekodavimas

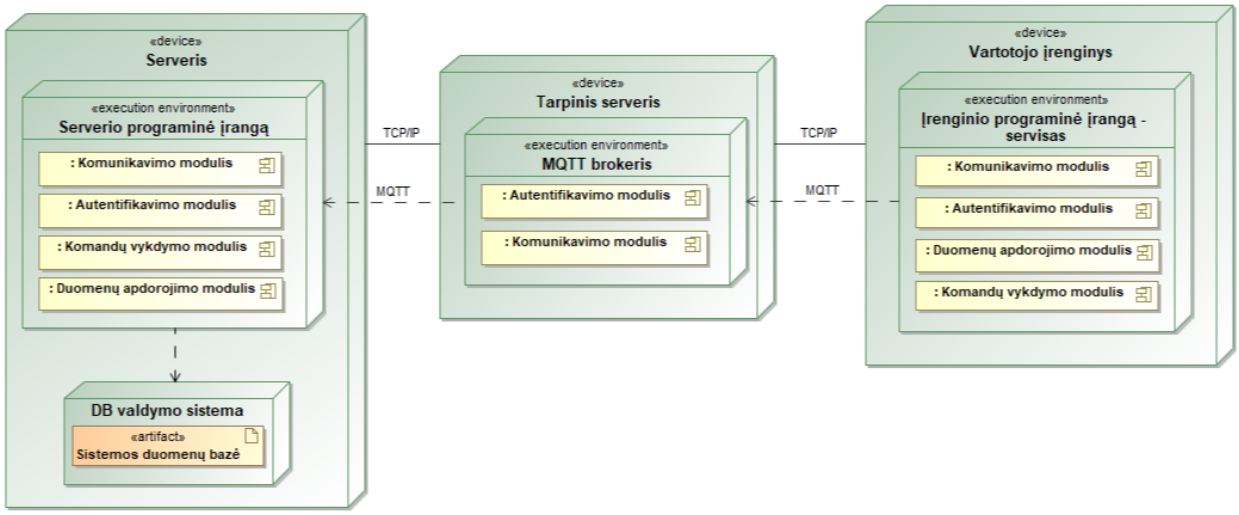
Panaudojant visas aukščiau išvardintas technologijas, bus pasiektas pakankamas sistemos apsaugos lygis, leidžiantis konfidencialiai autentifikuoti vartotoją ir jo įrangą.

2.7.2. Saugaus autentifikavimo sistemos prototipo struktūra

Tyrimui įvykdyti buvo sukurtas asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistemos prototipas. Prototipo struktūrą yra pateikiama 28 pav. Prototipas susideda iš serviso , įdiegto kliento įrenginyje, tarpinio brokerio skirto žinučių perdavimui tarp serverio ir kliento, bei serverio programinės įrangos.

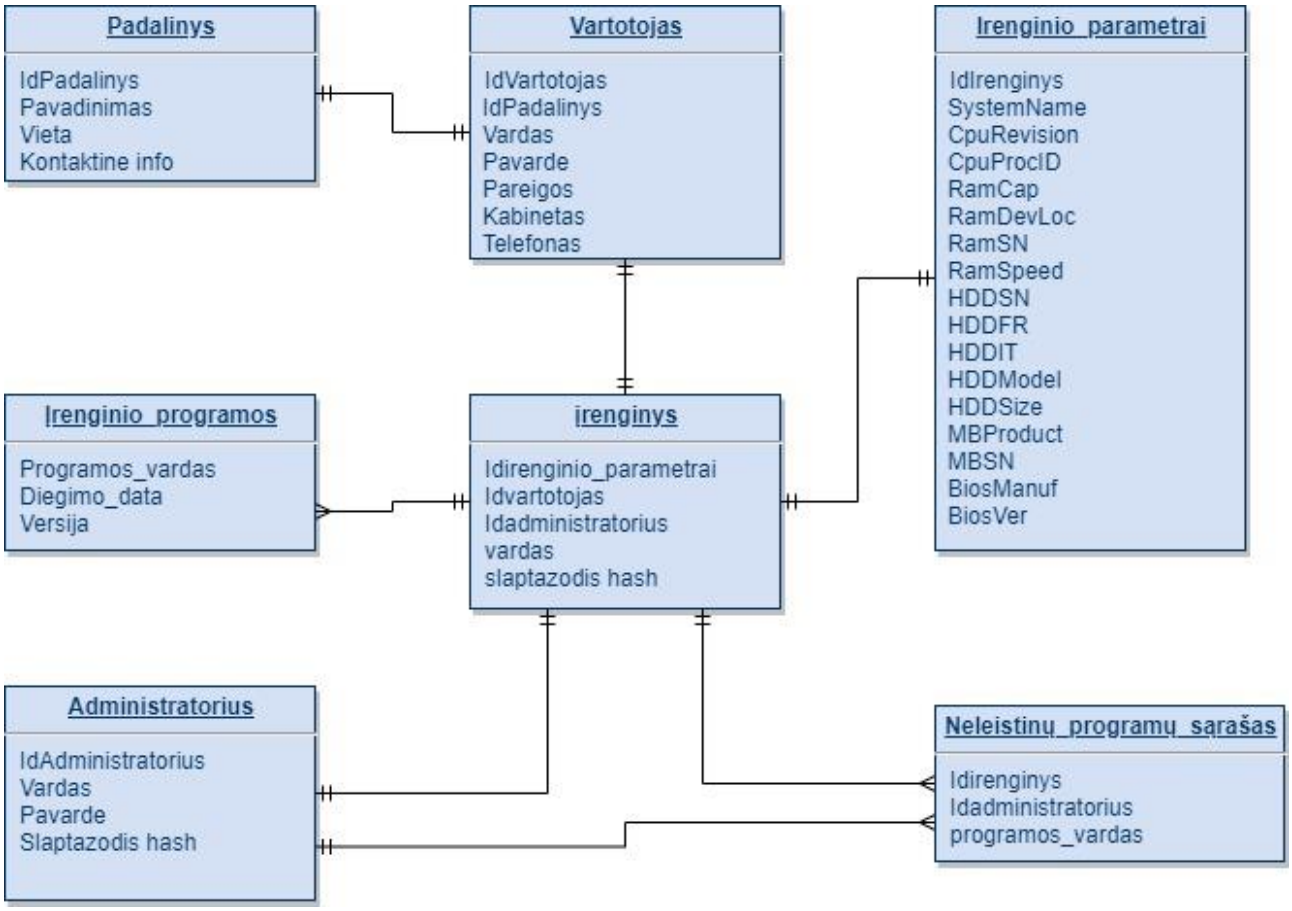
Sistemos serveryje realizuotos įrenginių autentifikavimo, duomenų apdorojimo, komandų siuntimo bei komunikavimo moduliai. Duomenų apdorojimo modulis apdoroja užklausas, gaunamas iš kitų trijų modulių bei atitinkamai nukreipia užduotis kitiems moduliams komunikacijai su vartotojo įrenginiu, per tarpinį brokerį. Autentifikavimo modulis , kartu su komunikavimo moduliu , tikrina sistemoje ar įrenginys yra registruotas. Neužregistruoti įrenginiai turi būti pirma užregistruoti sistemoje ir tik po to klientui leidžiamas darbas. Komandų siuntimo modulis yra naudojamas siųsti komandoms vartotojo įrenginiui, tokioms kaip išjungti neleidžiama programa, užrakinti įrenginį arba ištrinti įrenginio atmintį. Serveris su vartotojo įrenginiu gali komunikuoti MQTT pranešimu pagalbą,

kurie yra siunčiami saugiu TLS kanalu, papildomai šifruojant jų pranešimus „*Blowfish*“ šifravimo algoritmu, per tarpinį brokerį. Tarpinis MQTT brokeris leidžia apsaugoti įrenginius nuo serverio bei serverį nuo įrenginių, jeigu vienas iš jų būtų užvaldytas piktavalių.



28 pav. SAS sistemos prototipo struktūra

2.7.3. Saugaus autentifikavimo sistemos prototipo koncepcinis duomenų modelis



29 pav. SAS sistemos prototipo koncepcinis duomenų modelis

Koncepcinis kuriamos sistemos prototipo duomenų modelis yra pateiktas 29 pav. Modelis yra sudarytas iš 7 esybių: Įrenginys, įrenginio parametrai, įrenginio programos, administratorius, neleistinų programų sąrašas, vartotojas ir padalinys.

Vienam vartotojui negali priklausyti daugiau vieno įrenginio, bei negali būti registruotų įrenginių be duomenų įrašo įrenginio parametro lentelėje. Po įrenginio registravimo yra sudaromas įrenginio programų sąrašas, kuriame yra atrenkamos neleistinos programos ir yra rekomenduojama jas ištrinti, kartu jas išjungiant kiekvieno paleistų programų tikrinimo metu.

Neleistinų programų sąrašą gali keisti tik sistemos administratorius. Neleistinos programos yra tikrinamos visuose sistemos įrenginiuose.

2.7.4. Saugaus autentifikavimo sistemos serverio ir kliento prototipai

Sistemos kliento įrenginio prototipas buvo realizuotas kaip agentas – servisas skirtas „Windows“ platformai. Agentas yra skirtas autonominiam darbui, be vartotojo įsikišimo į procesą.

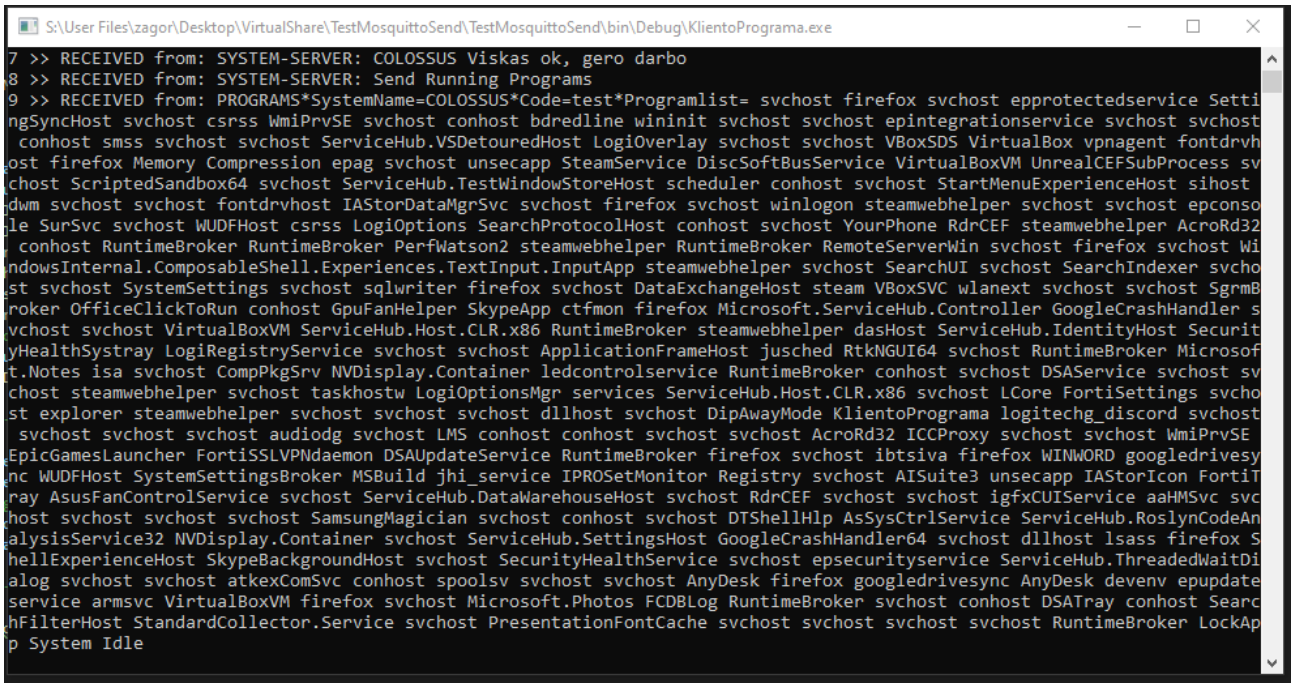
Įrangos registracija sistemoje atlieka administratorius, registruodamas įrenginį sistemoje perdavęs unikalų registracijos kodą serveriui. Užregistravus įrenginį agentas surenka tokia informacija apie , pateikta 11 lentelėje:

11 lentelė. SAS sistemos kliento būsenų pasikeitimai

Parametras	Apibūdinimas
Vartotojo vardas	Dabar prisijungusio prie įrenginio vartotojo vardas (SID)
Kompiuterio vardas	Vardas kuriuo identifikuojamas įrenginys sistemoje
CPU revizija	Unikalus kodas kuris priklauso konkrečiam procesoriui, rodo procesoriaus revizija, kuri gali priklausyti keletui procesorių.
CPU Procesoriaus ID	Unikalus kodas, priklausantis konkrečiam procesoriui, rodo identifikacinį numerį.
RAM atminties dydis	RAM atminties dydis sistemoje, kiekvieno lusto atskirai.
RAM įrenginio vieta	RAM atmintinės vieta motininėje plokštėje, kiekvieno įrenginio atskirai.
RAM serijinis numeris	Unikalus RAM atmintinės lusto numeris.
RAM greitis	RAM atmintinės greitis, kiekvieno lusto atskirai
Pagrindinės atminties serijinis numeris	Sistemoje instaliuotu atminties įrenginio (-inių) serijiniai numeriai, unikalūs tik tam įrenginiui.
Pagrindinės atminties valdymo kodo revizija	Versijos numeris , kokia valdymo kodo revizija yra įdiegta įrenginyje
Pagrindinės atminties pajungimo tipas	Atminties pajungimo tipas SATA, SAS, PCI-E
Pagrindinės atminties modelis	Įrenginio modelis su jo tipu SSD, HDD
Pagrindinės atminties dydis	Atminties dydis šiuo metu esantis kompiuteryje
Motininės plokštes produkto vardas	Faktinis motininės plokštės gamintojo suteiktas vardas
Motininės plokštės serijinis numeris	Unikalus numeris priklausantis konkrečiai plokštei
BIOS gamintojas	Gamintojo pavadinimas
BIOS versija	Versija įrašyta motininėje plokštėje

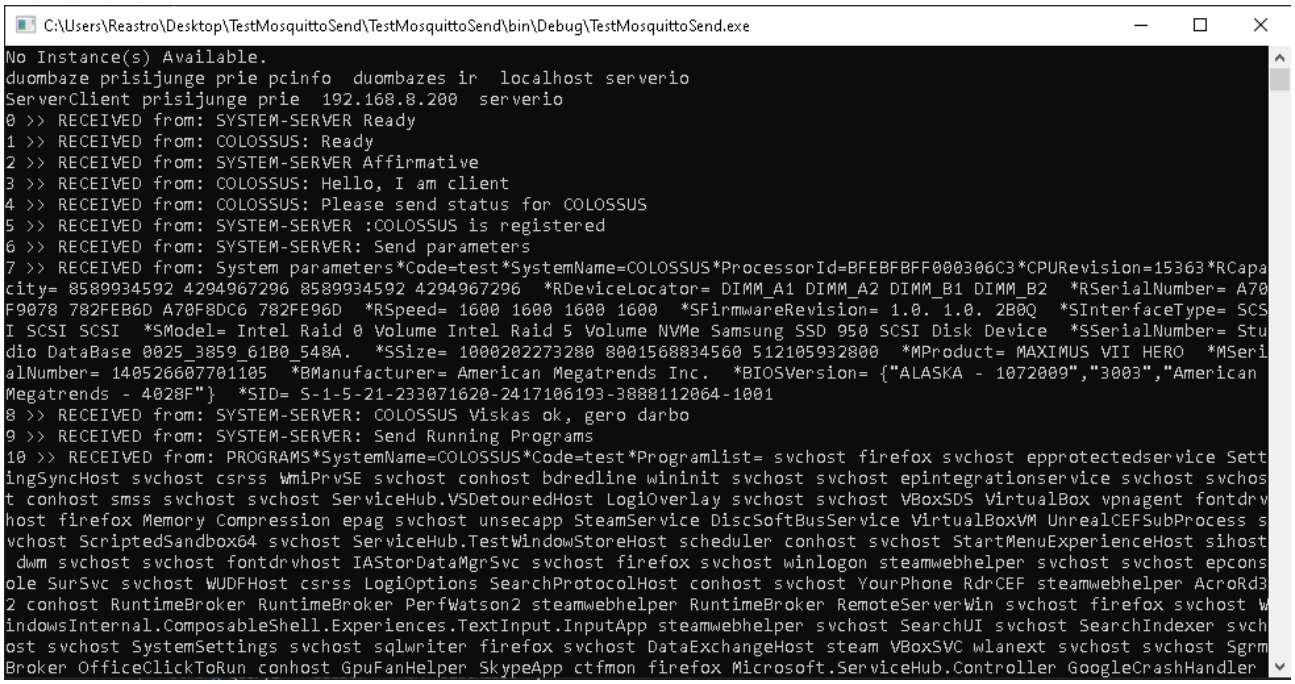
Surinktus duomenis kliento programa perduoda serveriui, kuriuos serveris apdoroja kaip parodyta 29 pav. duomenų modelyje. Kartu su parametrais perduodamos ir įdiegtos įrenginyje programų sąrašas, tikrinama ar nėra vykdoma neleistinų programų. Radus neleistinas programas yra bandoma nutraukti jų vykdymą. Nepavykus nutraukti neleistinos programos darbo yra nutraukiamas programos darbas su sistema ir pakeičiama įrenginio būklė sistemoje iš saugaus įrenginio į nesaugų. Pasikeitus sistemoje komponentams, netgi sukeitus komponentus vietomis, serveris neleis prisijungti prie

sistemos. Bus neleista prisijungti prie sistemos dėl to, jog buvo pažeistas kompiuterio vientisumas bei tokio įrenginio laikyti saugiu jau nebegalime iki to momento, kol jo neapžiūrėjo administratorius bei nesuregistravo jo iš naujo sistemoje.



30 pav. SAS sistemos prototipo kliento programos pranešimai

30 pav. parodytos kliento programų pranešimai siunčiami iš serverio klientui ir siunčiami kliento serveriui. Paveiksle matome vykdomų programų siunčiama sąrašą, kuris iš karto bus patikrintas serverio ar nėra vykdomos neleistinos programos. Jei tokių bus rasta, serveris siųs naują pranešima su sąrašų programų, kurių darbą reikia nutraukti.



31 pav. SAS sistemos prototipo serverio programos pranešimai

31 paveiksle matome serverio ir kliento pasisveikinimo žinutes. Jos yra skirtos pranešti vienas kitam apie savo pasiruošimą vykdyti komandas. Įrenginys gavęs pranešimą jog serveris yra pasiruošęs priimti užklausas vykdymui siunčia pranešimą apie savo pasiruošimą. Serveris atsako įrenginiui apie sėkmingą pranešimo gavimą. Kitas žingsnis yra įrenginio registracijos tikrinimas, jeigu įrenginys yra registruotas pereinama prie kito žingsnio. Jeigu įrenginys yra neregistruotas pereinama prie įrangos registravimo, kuriuo metu perduodami visi kompiuterio parametrai kartu su įdiegtų programų sąrašu. Po registracijos, kiekvieno prisijungimo metu yra tikrinami visi kompiuterio parametrai bei sulyginami serveryje su registruotais. Nesutapus parametrams įrenginiui neleidžiama dirbti su sistema. Sutapus parametrams yra perduodamos vykdomos programos įrenginyje. Radus neleistinų programų yra bandoma jas nutraukti. Nesėkmės atveju yra atjungiamas įrenginys nuo sistemos ir pakeičiama įrenginio būklė sistemoje

2.8. Išvados

- Pasiūlytas asmeninių įrenginių, naudojamųjų įmonėse, saugaus autentifikavimo sistema, skirta asmeninių įrenginių saugiam autentifikavimui, programų tikrinimui bei įrenginio vientisumui užtikrinti.
- SAS sistemos modelis leidžia ne tik autentifikuoti įrenginius, bet kartu ir tikrinti vykdomas programas įrenginyje, tikrinami įrenginio esami parametrai, lyginant juos su registruotais sistemoje, bei užtikrinama jog įrenginyje vykdomos tik tos programos, kurios yra leidžiamos sistemoje.
- Vienas iš sistemos bruožu – klientas nežino kur randasi serveris. Esant nulaužtam įrenginiui jis negali tiesiai prieiti prie serverio. Komunikacijos su serveriu yra vykdomos tarpinio brokerio pagalba, kuris perduoda pranešimus prenumeratoriams, prisijungusiems prie atitinkamos sesijos.
- Remiantis aprašytu prototipo modeliu buvo realizuotas sistemos prototipas, kuris yra skirtas Windows sistemos pagrindu veikiantiems įrenginiams.

3. Asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistemos eksperimentinis tyrimas

Vadovaujantis bei remiantis 2-ame skyriuje „Asmeninių įrenginių, naudojamų įmonėse, saugaus autentifikavimo sistemos prototipas“ minimu sistemos prototipu buvo atliktas tyrimas.

Tyrimo metu naudota techninė įrangą:

- Nešiojamas kompiuteris „Lenovo T580 SL10T84532“
- Stalinis kompiuteris „Padarytas pagal užsakymą, kompiuterio vardas: COLOSSUS“;
- Stalinis kompiuteris „Padarytas pagal užsakymą, kompiuterio vardas: Gamer-Full“;
- 4G+ maršrutizatorius ir *Wi-fi* prieigos stotelė „Huawei b535“.

Detali įrangos specifikacija pateikiama 12 lentelėje.

Tyrimui naudota programinė įrangą:

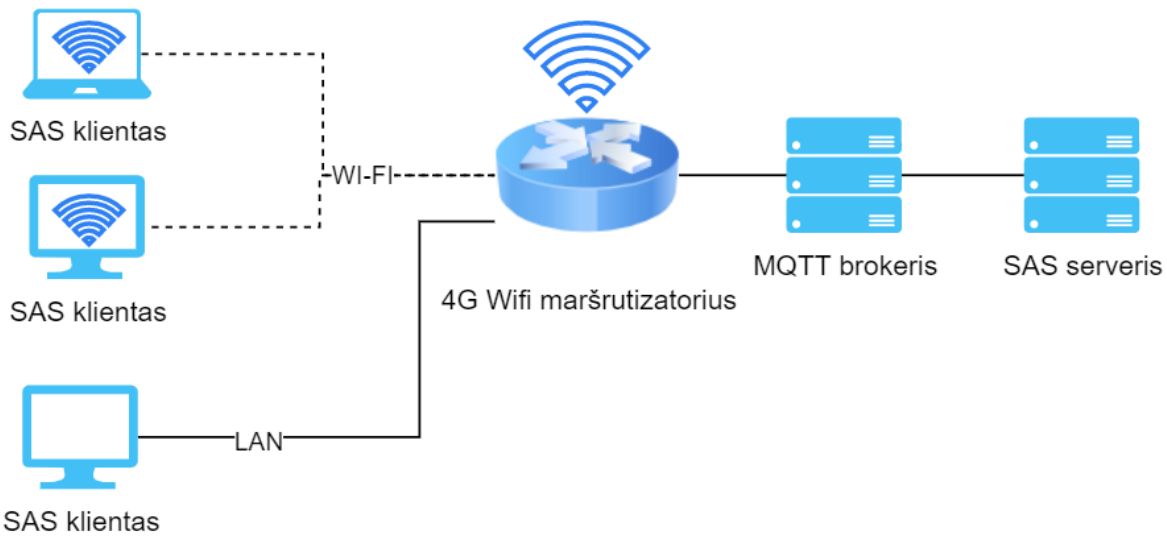
- Microsoft Visual Studio 2019;
- Wireshark;
- Oracle VM Virtualbox.

12 lentelė. Naudotos techninės įrangos surinkti parametrai

Kompiuterio vardas	C13604971
UserID	S-1-5-21-4252426894-525236942-355215321-1214 (pakeistas dėl saugumo sumetimų)
CPUPROCID	BFEBFBFF000806EA
Cpurevision	NOrevisionID
RamCapacity	8589934592 8589934592
Ramdevloc	ChannelA-DIMM0 ChannelB-DIMM0
RamSerialNr	31763940 31673DB0
Ramspeed	2400 2400
StorFirmNR	24879
Storintertp	SCSI
Stormodel	LITEON CA3-8D256
Storsernr	0023_0356_300B_C48C.
StorSize	256052966400
BBoardname	20LAS2XN00
BBoardsernr	W1KS953114V
Biosmanuf	LENOVO
Bios ver.	{"LENOVO - 1240","N27ET38W (1.24)","Lenovo - 1240"}
Kompiuterio vardas	COLOSSUS
UserID	S-1-5-21-233071620-2417106193-3888112064-1001
CPUPROCID	BFEBFBFF000306C3
Cpurevision	15363
RamCapacity	8589934592 4294967296 8589934592 4294967296

Ramdevloc	DIMM_A1 DIMM_A2 DIMM_B1 DIMM_B2
RamSerialNr	A70F9078 782FEB6D A70F8DC6 782FE96D
Ramspeed	1600 1600 1600 1600
StorFirmNR	1.0. 1.0. 2B0Q
Storintertp	SCSI SCSI SCSI
Stormodel	Intel Raid 0 Volume Intel Raid 5 Volume NVMe Samsung SSD 950 SCSI Disk Device
Storsernr	Studio DataBase 0025_3859_61B0_548A.
StorSize	1000202273280 8001568834560 512105932800
BBoardname	MAXIMUS VII HERO
BBoardsernr	140526607701105
Biosmanuf	American Megatrends Inc.
Bios ver.	{"ALASKA - 1072009","3003","American Megatrends - 4028F"}
Kompiuterio vardas	GAMER-FULL
UserID	S-1-5-21-323290011-4104250532-4215374033-1001
CPUPROCID	BFEBFBFF000306A9
Cpurevision	14857
RamCapacity	8589934592 8589934592
Ramdevloc	DIMM_A1 DIMM_A2
RamSerialNr	4069396391 27533734
Ramspeed	1600 1600
StorFirmNR	1.0. 1.0. PMAP
Storintertp	SCSI SCSI USB
Stormodel	Intel Raid 0 Volume Intel Raid 1 Volume Wilk USB DISK 3.0 USB Device
Storsernr	System Games 017C00039080
StorSize	480101368320 1000202273280 31066882560
BBoardname	H77M-HD3
BBoardsernr	To be filled by O.E.M.
Biosmanuf	American Megatrends Inc.
Bios ver.	{"ALASKA - 1072009","F2","American Megatrends - 4028D"}

Tyrimo metu naudojome vieną kompiuterį prijungtą laidu, kiti du įrenginiai buvo prijungti belaidžiu būdu. Tokiu būdu tikriname ir autentifikavimo priklausomybę nuo ryšio stiprumo.



32 pav. Tyrimo tinklo schema

3.1. Autentifikavimo ryšio saugumo ir greitaveikos tyrimas

Pirmąjį tyrimą buvo nuspręsta atlikti *false positive rate* (toliau FPR) tyrimą, pasinaudojant dviem skirtingomis sistemos konfigūracijomis:

- Šifruotas ryšys tarp brokerio ir įrenginio;
- Šifruotas ryšys tarp brokerio ir įrenginio, bei šifruotos žinutės.

FPR tyrimas parodys kiek sistema klientų praleidžia neautentifikavus, kiek buvo praleista su klaidomis bei kiek klientų prisijungimu buvo atmesta, įrenginiui esant be jokių trūkumų. Papildomai su FPR tyrimu buvo tiriama ir greitaveika bei sistemos apkrova, esant skirtingoms sistemos konfigūracijoms.

13 lentelė. FPR tyrimo lentelė

	Numatytas rezultatas: anomalus	Numatytas rezultatas: normalus
Gautas rezultatas: anomalus	Tikras teigiamas	Klaidingai neigiamas
Gautas rezultatas: normalus	Klaidingai teigiamas	Tikras neigiamas

Pagal 13 lentelės FPR tyrime yra nustatomos 4 pagrindinės reikšmės :

- Tikras teigiamas (angl. True Positive, toliau TP): anomalaus rezultato nustatymas, kai yra tikimasi sistemos klaidos ir jį yra gaunama eksperimento metu.
- Tikras neigiamas (angl. True Negative, toliau TN) : normalaus rezultato nustatymas, kai yra tikimasi suprojektuoto sistemos rezultato, be klaidos pranešimo.
- Klaidingai teigiamas (angl. False Positive, toliau FP): neteisingas rezultato nustatymas, kai rezultatas yra nustatomas anomalus, o iš tikrųjų rezultatas yra normalus
- Klaidingai neigiamas(angl. False Negative, toliau FN): neteisingas rezultato nustatymas, kai rezultatas yra nustatomas anomalus, o iš tikrųjų yra normalus.

Pasinaudojus FPR tyrimo gautais duomenimis, skaičiuosime sistemos tikslumo rodiklį.

$$Acc = \frac{TP + TN}{TP + TN + FP + FN}$$

33 pav. FPR tyrimo tikslumo skaičiavimas

Tyrimas buvo atliekamas pasinaudojant dviem skirtingomis sistemos konfigūracijomis. Pirmoji konfigūracija šifruotu ryšiu, žinutės yra atviro tipo, pagrindinės apsaugos yra apsaugotas ryšys ir logika jog nei klientas nei serveris nežino kur yra vienas arba kitas sistemos dalyvis. Abu dalyviai žino tik tarpinio brokerio adresą, kurio pagalba yra perduodami pranešimai iš serverio į klientą. Antroji konfigūracija yra apsaugotu ryšiu tarp brokerio ir kliento, bei su apsaugota šifruota žinute. Antra konfigūracija apsaugo žinutes net įrenginio nulaužimo atveju.

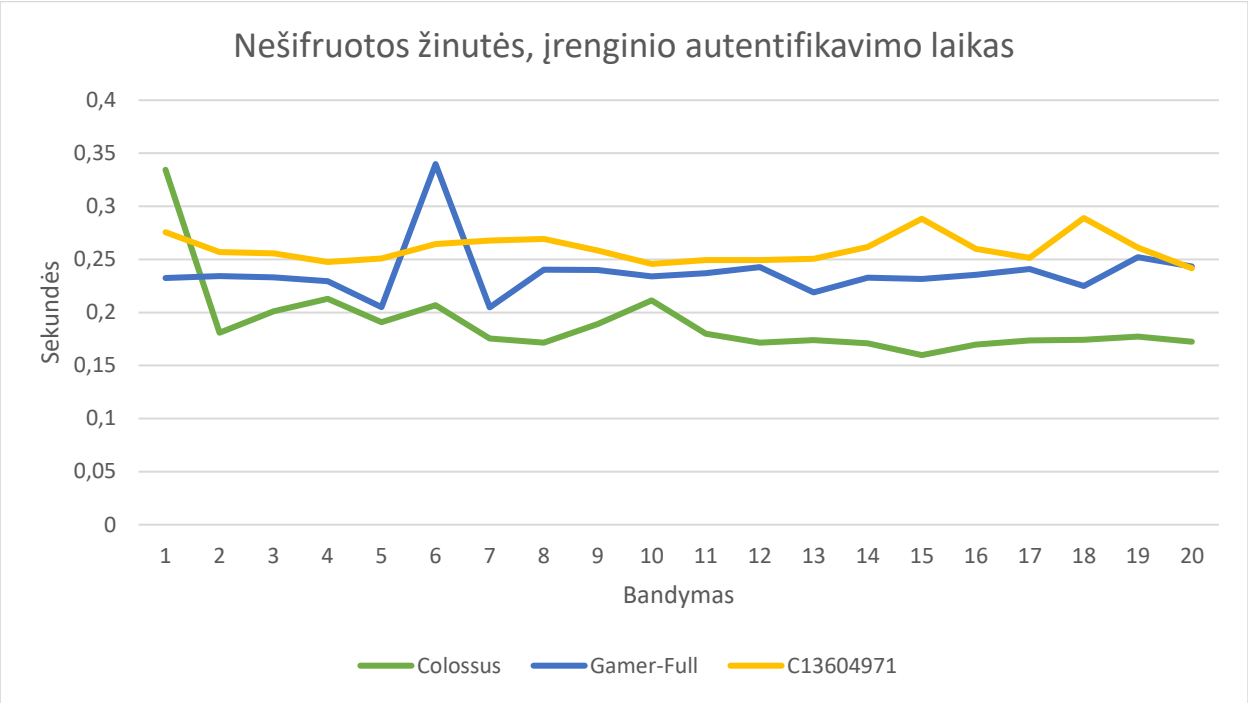
Papildomai FPR tyrime buvo tiriamas įrenginių prisijungimas prie sistemos, su neteisingais parametrais. Buvo imituotas įrenginio parametrų pasikeitimas, bei tiriama kiek kartų tokius įrenginius sistema priims kaip tinkamus.

31 pav. yra pateikta tyrime naudojama tinklo schema. Kaip matome schemoje du įrenginiai yra pajungti pasinaudojus *Wi-Fi* belaidžiu tinklu ir vienas įrenginys yra pajungtas laidiniu sujungimu. Viso tyrimo metu buvo atlikta daugiau 300 bandymu su skirtingomis įrenginio bei sistemos konfigūracijomis. Tyrimo rezultatai yra pateikiami žemiau.

14 lentelė. Nešifruotos žinutės įrenginio autentifikavimo laikai

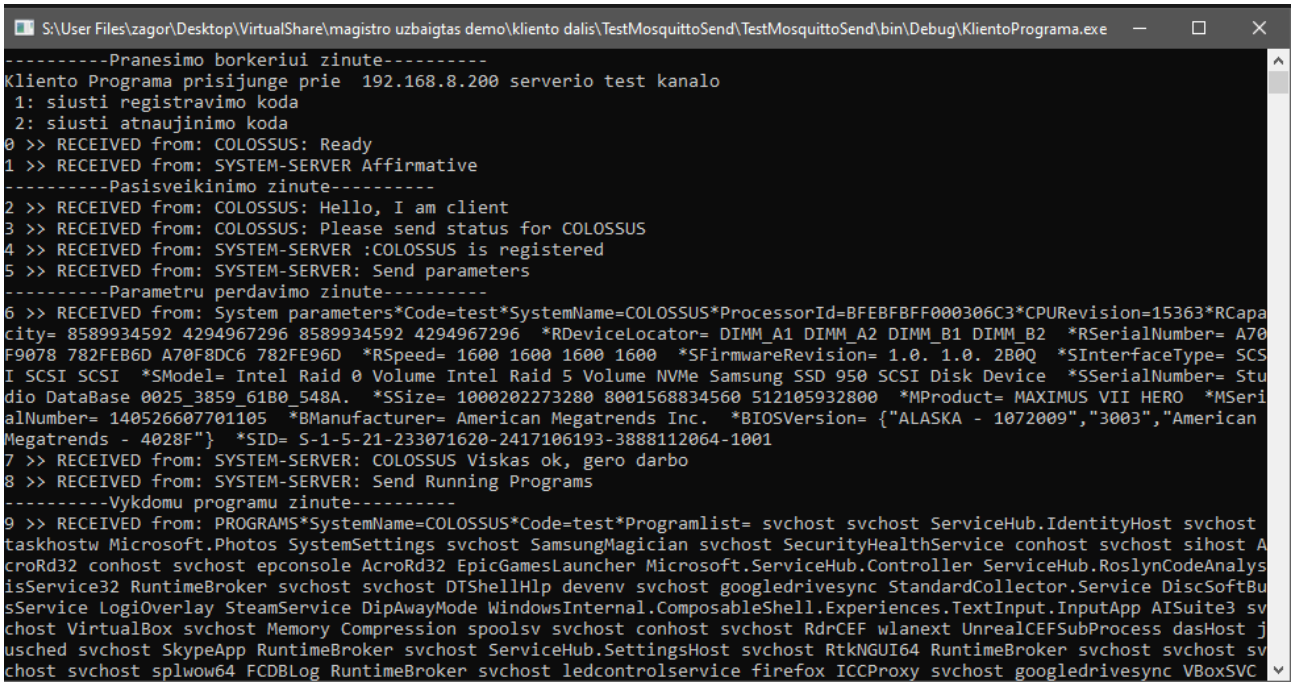
Colossus: bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.	Gamer-Full: bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.	C13604971 bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.
1	18,329291	18,663733	0,334442	1	5,873	6,105367	0,232367	1	58,275938	58,55164	0,275702
2	28,367673	28,548698	0,181025	2	11,042662	11,276972	0,23431	2	65,384062	65,640981	0,256919
3	33,801643	34,002617	0,200974	3	14,903327	15,136313	0,232986	3	70,736688	70,992288	0,2556
4	38,938258	39,151063	0,212805	4	20,766353	20,995705	0,229352	4	75,923385	76,170978	0,247593
5	43,02401	43,2147	0,19069	5	24,197641	24,402716	0,205075	5	81,18114	81,432023	0,250883
6	49,194178	49,401035	0,206857	6	28,302552	28,642379	0,339827	6	86,340135	86,604585	0,26445
7	54,531594	54,707056	0,175462	7	32,13466	32,339416	0,204756	7	91,37524	91,643014	0,267774
8	58,42255	58,594214	0,171664	8	36,233927	36,474325	0,240398	8	96,082428	96,351639	0,269211
9	62,464111	62,653174	0,189063	9	39,255725	39,495598	0,239873	9	105,555255	105,813677	0,258422
10	66,362287	66,573506	0,211219	10	42,88679	43,120627	0,233837	10	111,05655	111,302331	0,245781
11	70,214552	70,39455	0,179998	11	46,39945	46,636298	0,236848	11	116,751967	117,001399	0,249432
12	73,606765	73,778207	0,171442	12	52,065525	52,308284	0,242759	12	121,775068	122,024466	0,249398
13	77,559982	77,733801	0,173819	13	55,293062	55,512037	0,218975	13	126,66102	126,911596	0,250576
14	81,28491	81,455956	0,171046	14	58,669238	58,901969	0,232731	14	132,157143	132,418938	0,261795
15	84,695022	84,854836	0,159814	15	62,265564	62,496992	0,231428	15	138,885868	139,174284	0,288416
16	88,884802	89,054439	0,169637	16	65,916619	66,15205	0,235431	16	145,823518	146,08351	0,259992
17	93,955111	94,128703	0,173592	17	68,864649	69,105552	0,240903	17	150,321075	150,572492	0,251417
18	98,327405	98,501624	0,174219	18	72,33413	72,558994	0,224864	18	155,592955	155,881899	0,288944
19	101,811437	101,98878	0,177347	19	75,853112	76,105131	0,252019	19	160,893837	161,154931	0,261094
20	106,188468	106,36094	0,172468	20	79,301007	79,544431	0,243424	20	166,350691	166,592311	0,24162
		Vidutinis	0,18987915			Vidutinis	0,237608			Vidutinis	0,259751

Iš pateiktos lentelės matome vidutinius laikus, per kuriuos sistema sėkmingai autentifikavo vartotoją ir įrenginį sistemoje. Sprendžiant iš vidutinių laikų, per kuriuos sistema autentifikavo įrenginį bei vartotoją, matome jog kaip ir buvo tikėtasi autentifikavimas užtruko ilgiau Wi-Fi tinklu veikiantiems įrenginiams. Autentifikavimo sutrikimu nebuvo pastebėta pirmoje eksperimento dalyje. Vidutiniškai sistema užtruko 0,229079 sekundės įrenginio autentifikavimui. Taipogi pirmos dalies metu buvo tikrinamos ir autentifikacijos su neteisingais parametrais, nebuvo pastebėta autentifikuotu įrenginiu su netinkamais parametrais.



34 pav. Nešifruotos žinutės įrenginio autentifikavimo laikas

Kaip matome iš 33 pav. grafiko, vieno bandymo metu buvo sutrikimas dėl kurio pailgėjo autentifikavimo laikas, tačiau vidutiniškai autentifikavimo laiko tarpas nepadidėjo ženkliai ir nebuvo nustatyta ne vieno nesėkmingo autentifikavimo naudojant nešifruotas žinutes, o tik pasinaudojus saugiu šifruotu ryšiu. 34 pav. matome žinučių apsikeitimo proceso veikimą, kaip vyksta užklausos iš serverio dalies įrenginiui, bei kokie parametrai yra naudojami įrenginio autentifikavimui.

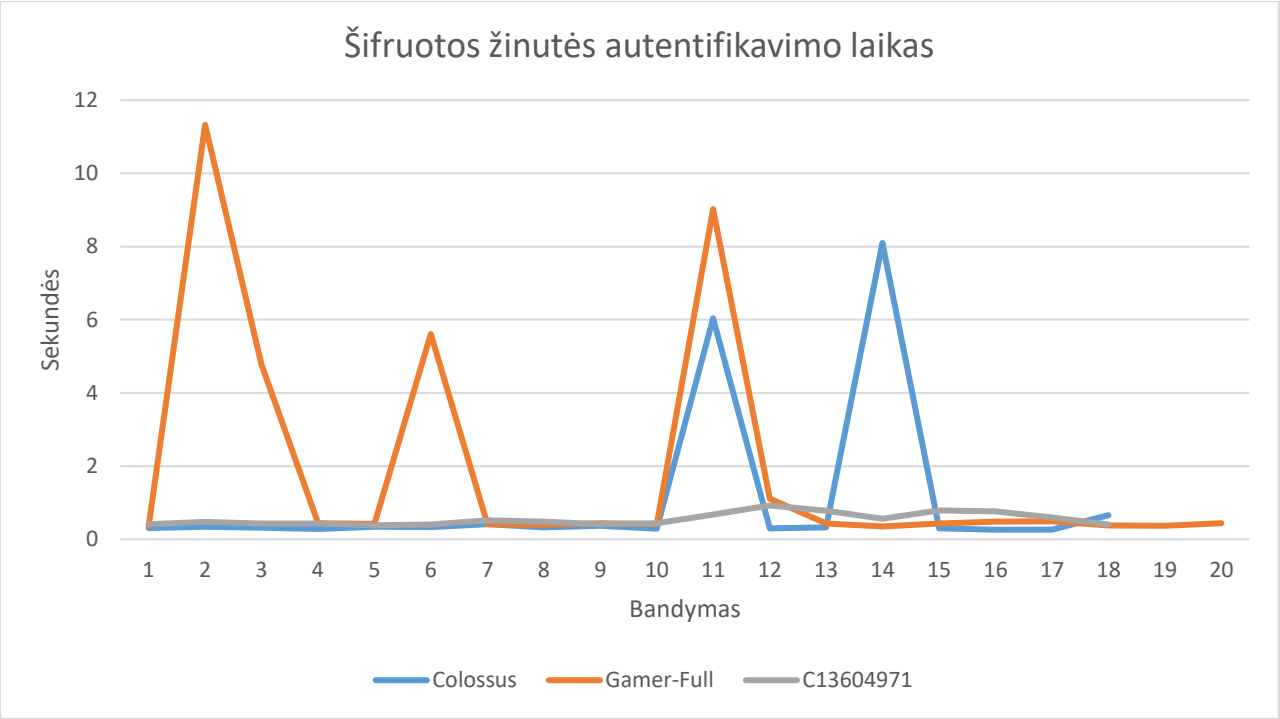


35 pav. Nešifruotos žinutės įrenginio pranešimu perdavimas

15 lentelė. Šifruotos žinutės įrenginio autentifikavimo laikai

Colossus: bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.	Gamer-Full: bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.	C13604971 bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.
1	21,2061	21,516314	0,310214	1	7,430609	7,784477	0,353868	1	6,553995	6,968871	0,414876
2	29,903455	30,249828	0,346373	2	12,965853	24,292803	11,32695	2	12,979254	13,448759	0,469505
3	37,020466	37,340307	0,319841	3	35,062832	39,84239	4,779558	3	19,397108	19,828238	0,43113
4	43,886678	44,166519	0,279841	4	46,113609	46,552024	0,438415	4	25,52151	25,948284	0,426774
5	52,229916	52,568762	0,338846	5	51,264429	51,682362	0,417933	5	32,148655	32,53026	0,381605
6	60,308246	60,64438	0,336134	6	56,245581	61,852292	5,606711	6	38,598619	38,99764	0,399021
7	68,888864	69,304325	0,415461	7	65,626189	66,038795	0,412606	7	45,303055	45,820986	0,517931
8	77,154382	77,481632	0,32725	8	70,027362	70,422091	0,394729	8	53,01668	53,499901	0,483221
9	86,811109	87,180944	0,369835	9	74,36299	74,803092	0,440102	9	62,739791	63,150136	0,410345
10	94,922863	95,208402	0,285539	10	80,446064	80,862323	0,416259	10	69,564045	70,003206	0,439161
11	104,06148	110,10263	6,041153	11	85,069992	94,091779	9,021787	11	76,941062	77,614657	0,673595
12	128,85156	129,14633	0,294766	12	98,315333	99,429744	1,114411	12	85,073713	85,995855	0,922142
13	137,683705	138,01098	0,32727	13	104,08711	104,51324	0,426133	13	92,137607	92,920258	0,782651
14	146,633572	154,73031	8,096735	14	114,77029	115,1213	0,351013	14	99,838581	100,403306	0,564725
15	161,931829	162,22676	0,29493	15	119,46405	119,89328	0,429224	15	120,179958	120,970457	0,790499
16	168,588306	168,84851	0,260203	16	123,96457	124,44331	0,478738	16	128,061797	128,827396	0,765599
17	178,99435	179,2619	0,2675487	17	131,83751	132,32794	0,490434	17	134,561604	135,159672	0,598068
18	187,750151	188,40708	0,656925	18	137,68726	138,06661	0,379347	18	150,578347	150,979517	0,40117
19			0	19	148,4923	148,85819	0,365886	19			0
20			0	20	153,43408	153,87387	0,439798	20			0
		Vidutinis	1,01271551			Vidutinis	1,704195			Vidutinis	0,504529

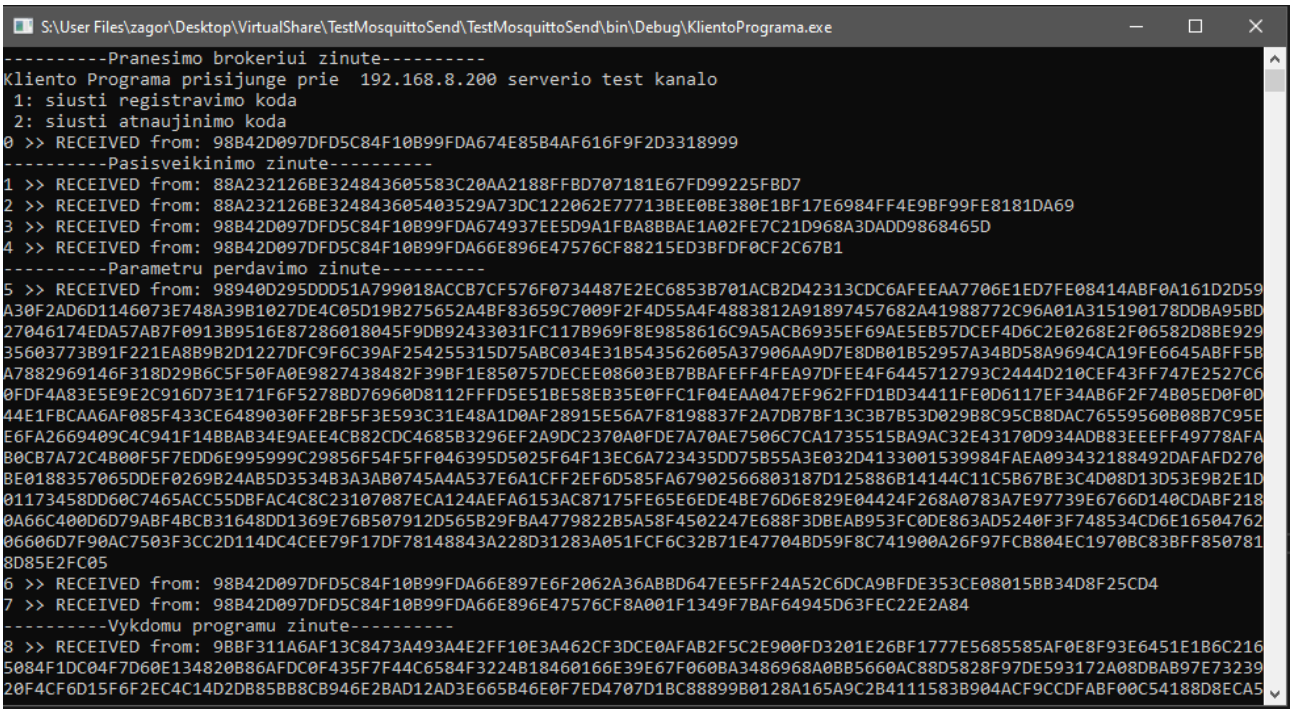
Kaip matome iš 14 lentelės, vidutinis laiko tarpas lyginant su nešifruota žinute padidėja 6,63 karto. Matome sistemos sutrikimus tiek LAN jungtimi pajungtu įrenginiu (Colossus) tiek *Wi-Fi* būdu (C13604971). Vidutiniškai matome jog sistema sutrinka 6,667% savo veikimo laiko. Ne vieno sutrikimo metu įrenginys nebuvo klaidingai autentifikuotas. Pakartotinai bandant autentifikuoti įrenginį po sistemos sutrikimo, įrenginys buvo sėkmingai autentifikuotas.



36 pav. Šifruotos žinutės įrenginio autentifikavimo laikas

Kaip matome iš 35 pav. grafiko, įrenginio autentifikavimo laiko tarpas užšifravus žinutes viršijo vidutinį šifruoto autentifikavimo laiko tarpą net 11 kartų. Lyginant su nešifruotu autentifikavimu, labiausiai nukenčia sistemos stabilumas, kur 33 pav. matome nežymius nukrypimus nuo vidutinio laiko.

Taipogi naudojant pilną žinutės šifravimą buvo pastebėtas padidėjęs sistemos apkrovimas. Padidėjimas sudaro 30% įrenginio procesoriaus apkrovos ir 20% įrenginio RAM atminties naudojimo. 36 pav. parodome kaip atrodo žinučių apsikeitimas tarp įrenginių.



37 pav. Šifruotos žinutės įrenginio pranešimu perdavimas

Pagal gautus pirmojo tyrimo rezultatus galime teigti, jog sistema veikia korektiškai, taip kaip ir buvo suprojektuota. Tiriant autentifikavimą su imituotais neteisingais įrenginio parametrais, iš 120 bandymų, 60 šifruotu ir 60 nešifruotu žinučių pagalbą nebuvo pastebėta ne vieno įrenginio autentifikavimo atvejo. Sistema tikrina visus įrenginio parametrus, kurie buvo pateikti įrenginio registravimo metu, bei neleidžia autentifikuoti įrenginį arba vartotoją radus net ir menkiausius neatitikimus. Sistemos administratoriui taipogi yra pranešama apie neatitikimus sukėlusį komponentą, pranešant būtent kuris parametras neatitiko sistemoje. Savo nuožiūra administratorius gali grąžinti įrenginiui saugumo būklę sistemoje, kuri yra automatiškai keičiama iš saugios į nesaugią kiekvieno neatitikimo metu.

Tiriant sistemos tikslumo rodiklį, kaip pateikta 33 pav. buvo suskaičiuoti sistemos tikslumo rodikliai kiekvienam įrenginiui visų testu metu. Iš visų įrenginių rodiklių buvo išvestas sistemos tikslumo rodiklio vidurkis.

16 lentelė. FPR tyrimo rezultatų lentelė

Įrenginys: Colossus	Numatytas rezultatas: anomalus	Numatytas rezultatas: normalus	Įrenginys: Gamer-Full	Numatytas rezultatas: anomalus	Numatytas rezultatas: normalus	Įrenginys: C13604971	Numatytas rezultatas: anomalus	Numatytas rezultatas: normalus
Gautas rezultatas: anomalus	60	12	Gautas rezultatas: anomalus	60	10	Gautas rezultatas: anomalus	60	9
Gautas rezultatas: normalus	9	219	Gautas rezultatas: normalus	7	223	Gautas rezultatas: normalus	8	223

Paskaičiavus visus sistemos tikslumo rodiklius kiekvienai sistemai, buvo gautas visos sistemos tikslumo rodiklis, kuris sudaro 93,88%

3.2. Programų nutraukimo greitaveikos priklausomybė nuo saugumo lygio naudojimo tyrimas

Antrojo tyrimo metu tikrinsime programų darbo nutraukimo vykdymą, pasinaudojant skirtingomis sistemos konfigūracijomis:

- Šifruotas ryšys tarp brokerio ir įrenginio;
- Šifruotas ryšys tarp brokerio ir įrenginio, bei šifruotos žinutės.

Antrasis tyrimas yra skirtas ištirti, kiek programų sistema sėkmingai uždaro ir kiek sistema praleidžia neleistinų programų. Tyrimo metu buvo tiriama programų atrinkimo, tikrinimo bei uždarymo komandų veikimas, imituojant programų paleidimą kliente ir jų uždarymą pasinaudojant serverio juodojo sąrašo tikrinimu.

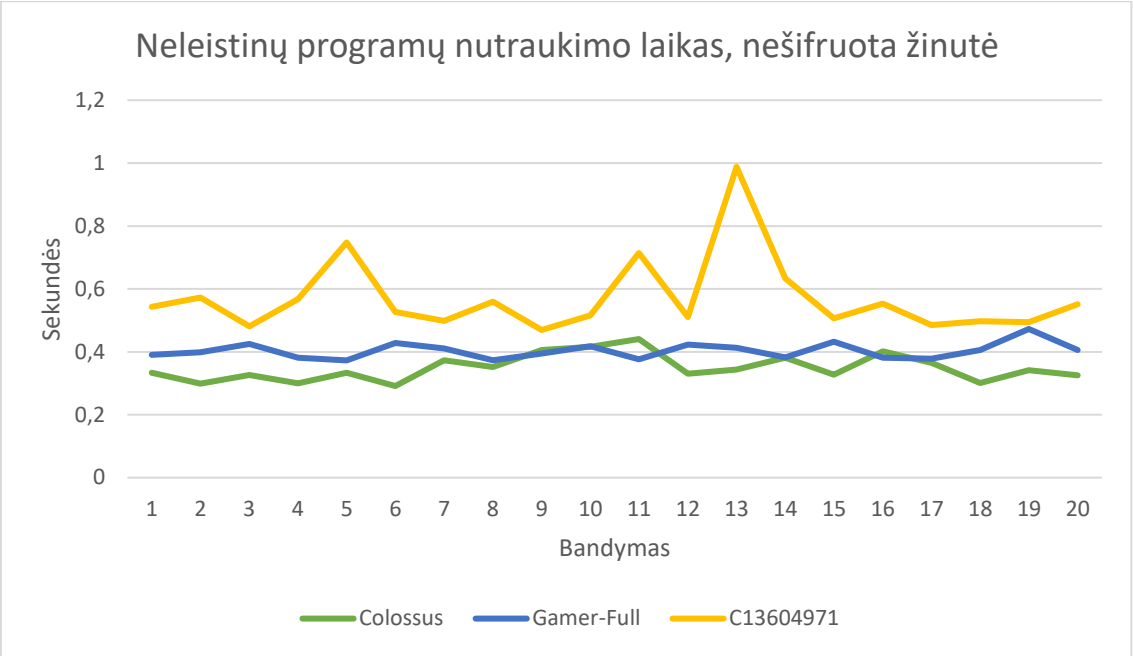
Tyrimui buvo naudojamos keletas programų, kurios buvo surašytos juodajame sąraše. Kliento pusėje buvo paleidžiamos skirtingos programos, po keletą instancijų kiekvienos programos. Tuo buvo tirta sistemos galimybė atpažinti visas programas, esančias paleistas įrenginyje, bei sistemos galimybę jas visas uždaryti vienu metu, nutraukiant jų darbą be vartotojo įsikišimo į procesą.

15 lentelėje pateikiame neleistinų programų nutraukimo laikus, naudojant nešifruotas žinutes duomenų perdavimui.

17 lentelė. Nešifruotos žinutės, neleistinų programų nutraukimo laikai.

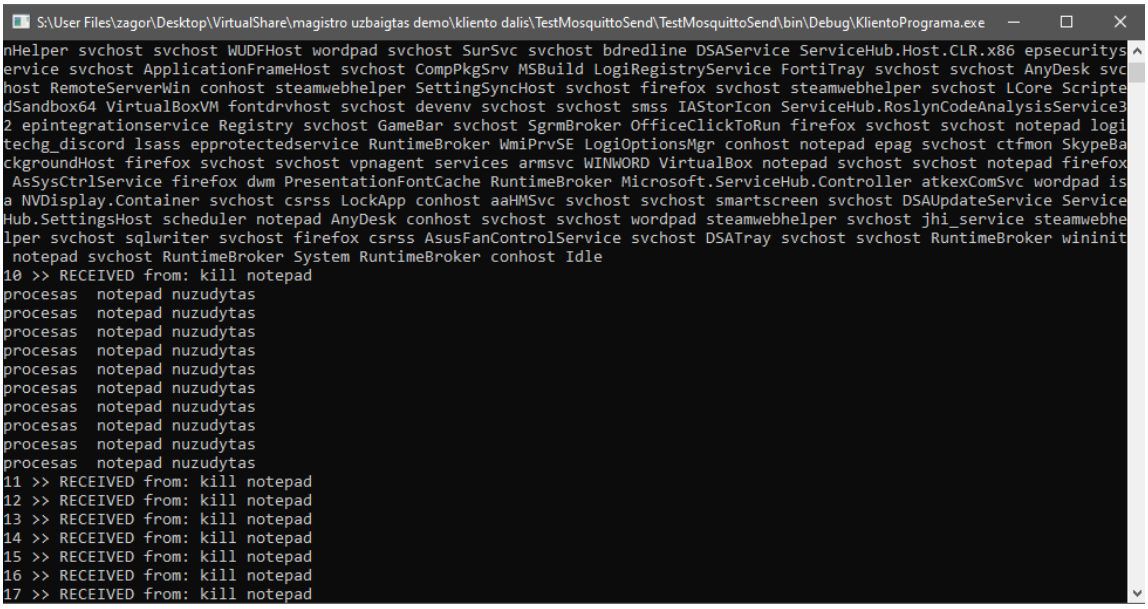
Colossus: bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.	Gamer-Full: bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.	C13604971 bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.
1	8,198975	8,531937	0,332962	1	10,012659	10,403039	0,39038	1	9,267738	9,810815	0,543077
2	15,38341	15,682681	0,299271	2	27,785862	28,18435	0,398488	2	18,467159	19,039811	0,572652
3	22,660023	22,985977	0,325954	3	32,477775	32,902768	0,424993	3	27,768672	28,249228	0,480556
4	31,616105	31,91544	0,299335	4	37,225308	37,606609	0,381301	4	35,981598	36,54938	0,567782
5	38,201369	38,534829	0,33346	5	42,718171	43,090874	0,372703	5	44,903423	45,6511221	0,7476991
6	44,843299	45,134498	0,291199	6	47,787316	48,21548	0,428164	6	53,473211	54,00012	0,526909
7	51,583307	51,955935	0,372628	7	52,633496	53,044385	0,410889	7	63,07327	63,571108	0,497838
8	58,347416	58,698997	0,351581	8	57,795685	58,16878	0,373095	8	71,191314	71,750362	0,559048
9	65,014533	65,420195	0,405662	9	62,336173	62,731113	0,39494	9	79,181832	79,651276	0,469444
10	71,875425	72,291693	0,416268	10	67,906846	68,324996	0,41815	10	87,276015	87,791324	0,515309
11	78,839307	79,279941	0,440634	11	72,636621	73,012348	0,375727	11	97,016817	97,731112	0,714295
12	85,760137	86,090544	0,330407	12	78,028069	78,451182	0,423113	12	105,220542	105,731005	0,510463
13	94,009364	94,353051	0,343687	13	83,599231	84,012535	0,413304	13	112,625083	113,613186	0,988103
14	99,985446	100,366671	0,381225	14	88,942161	89,324899	0,382738	14	121,698609	122,332305	0,633696
15	105,973	106,299848	0,326848	15	94,003908	94,435756	0,431848	15	130,125358	130,632004	0,506646
16	112,273511	112,675146	0,401635	16	98,771657	99,153064	0,381407	16	138,987605	139,541321	0,553716
17	118,842243	119,207581	0,365338	17	105,58737	105,96589	0,378526	17	146,836115	147,321676	0,485561
18	125,320919	125,62202	0,301101	18	110,4355	110,84089	0,405389	18	156,383471	156,881087	0,497616
19	131,332389	131,673678	0,341289	19	115,60258	116,07522	0,472635	19	164,748959	165,242986	0,494027
20	139,652355	139,977426	0,325071	20	120,13855	120,54385	0,405298	20	173,040649	173,592105	0,551456
		Vidutinis	0,34927775			Vidutinis	0,403154			Vidutinis	0,570794655

Kaip matome iš 16 lentelės, neleistinų programų nutraukimo, sistema korektiškai įvykdė visus eksperimento bandymus. Nebuvo rasta ne vieno sistemos sutrikimo visos programos buvo nutrauktos. Programos buvo nutrauktos be vartotojo įsikišimo bei neišsaugant programos padarytu pakeitimų (notepad programos atveju). Vidutinis užklausos įvykdymo laiko tarpas sudaro 0,441076 sekundės. Palyginus vien su įrenginio autentifikavimu, programų nutraukimo komanda vidutiniškai užima 0,211997 sekundės, uždarant po 20 paleistų neleistinų programų.



38 pav. Neleistinų programų nutraukimo laikas, nešifruota žinutė

Kaip matome iš 37 pav. pateikto grafiko, sistemos veikimas nebuvo nutrauktas. Pastebėtas vieno įrenginio užklausų vykdymo laiko pailgėjimas. Laiko pailgėjimas siejamas su įrenginio programų apdorojimo greičiu, bei interneto tinklo užklausų kiekiu. Kaip matome iš 12 lentelės techninių įrenginio specifikacijų, trečias įrenginys (C13604971) yra nešiojamas kompiuteris, kuris buvo prijungtas prie sistemos *Wi-Fi* būdu. Tyrimo metu nebuvo pastebėta ne vieno sutrikimo, kurio metu nebūtų nutrauktos programos, pateiktos juodajame sąraše. 38 pav. pateikiame pranešimų apsikeitimo tarp kliento ir serverio vaizdą, kokios žinutės yra siunčiamos ir koks komandos atsakas yra gaunamas iš kliento.

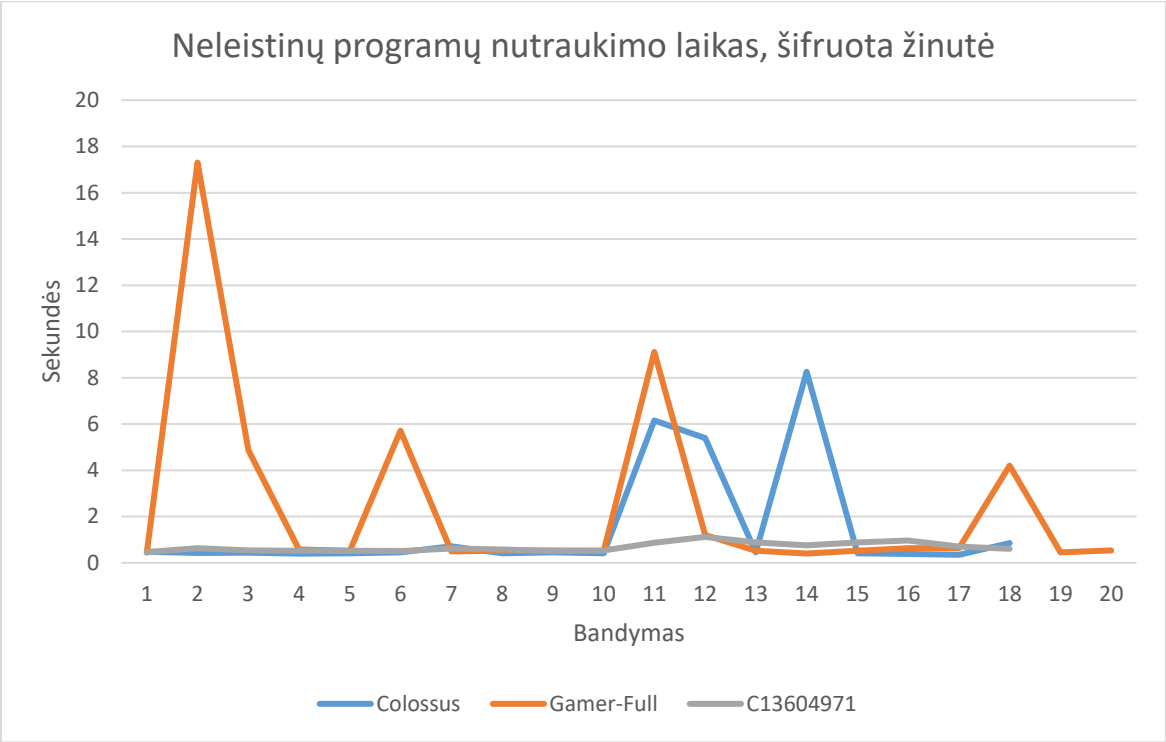


39 pav. Neleistinų programų nutraukimo pranešimai, nešifruota žinutė

18 lentelė. Neleistinų programų nutraukimo laikai, šifruota žinutė

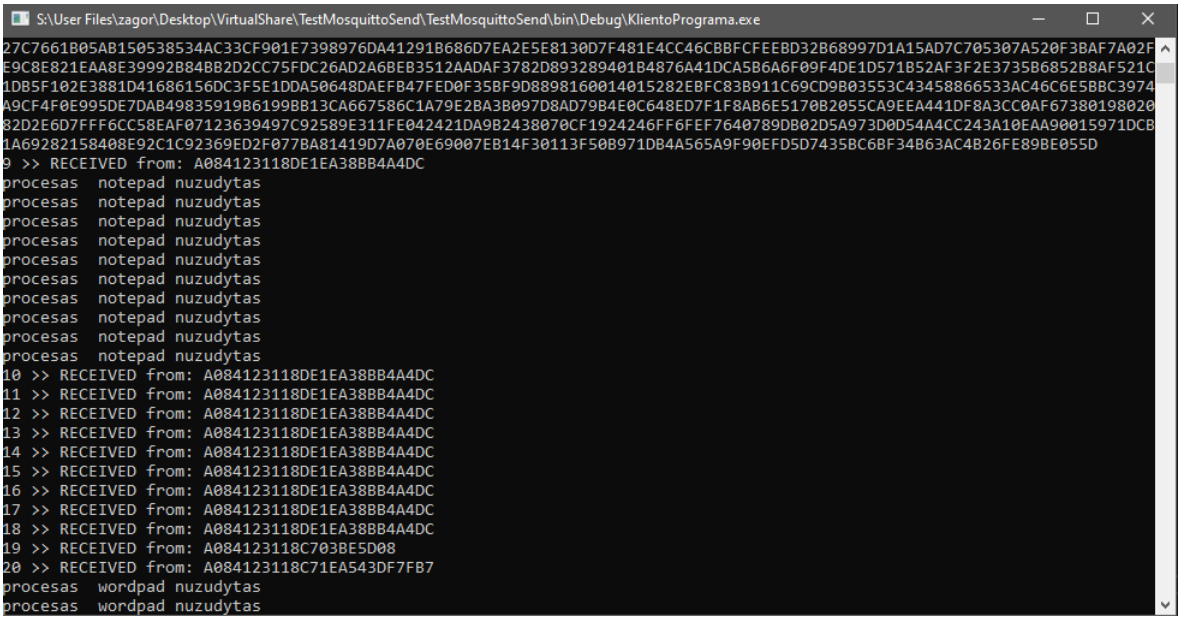
Colossus: bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.	Gamer-Full: bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.	C13604971 bandymo Nr.	Pradžios laikas, s.	Pabaigos laikas, s.	Laikas, s.
1	21,2061	21,682532	0,476432	1	7,430609	7,869539	0,43893	1	6,553995	7,018792	0,464797
2	29,903455	30,330865	0,42741	2	12,965853	30,271091	17,305238	2	12,979254	13,608778	0,629524
3	37,020466	37,467105	0,446639	3	35,062832	39,928791	4,865959	3	19,397108	19,930704	0,533596
4	43,886678	44,28853	0,401852	4	46,113609	46,691774	0,578165	4	25,52151	26,048162	0,526652
5	52,229916	52,648484	0,418568	5	51,264429	51,785142	0,520713	5	32,148655	32,678356	0,529701
6	60,308246	60,766791	0,458545	6	56,245581	61,952077	5,706496	6	38,598619	39,108028	0,509409
7	68,888864	69,603278	0,714414	7	65,626189	66,125648	0,499459	7	45,303055	45,92395	0,620895
8	77,154382	77,561658	0,407276	8	70,027362	70,551899	0,524537	8	53,01668	53,600446	0,583766
9	86,811109	87,262956	0,451847	9	74,36299	74,902477	0,539487	9	62,739791	63,25025	0,510459
10	94,922863	95,329586	0,406723	10	80,446064	80,956082	0,510018	10	69,564045	70,097284	0,533239
11	104,06148	110,22273	6,16125	11	85,069992	94,191775	9,121783	11	76,941062	77,815433	0,874371
12	128,85156	134,244164	5,392604	12	98,315333	99,523043	1,20771	12	85,073713	86,195385	1,121672
13	137,683705	138,133985	0,45028	13	104,087106	104,60641	0,519304	13	92,137607	93,020448	0,882841
14	146,633572	154,894308	8,260736	14	114,770285	115,173528	0,403243	14	99,838581	100,597626	0,759045
15	161,931829	162,345792	0,413963	15	119,464053	119,994237	0,530184	15	120,179958	121,069655	0,889697
16	168,588306	168,968574	0,380268	16	123,964569	124,593806	0,629237	16	128,061797	129,027083	0,965286
17	178,9943503	179,342933	0,3485827	17	131,837505	132,472493	0,634988	17	134,561604	135,261239	0,699635
18	187,750151	188,607237	0,857086	18	137,687262	141,892583	4,205321	18	150,578347	151,182406	0,604059
19			0	19	148,492302	148,953391	0,461089	19			0
20			0	20	153,434076	153,973831	0,539755	20			0
		Vidutinis	1,441542428			Vidutinis	2,487081			Vidutinis	0,6304971

Kaip matome 16 lentelėje, užklausos laiko tarpas naudojant pilna žinutės šifravimą vidutiniškai pailgėjo 3,445 karto lyginant su nešifruota žinute. Taipogi buvo pastebėtas nekorektiškas programos veikimas. Pastebėtas 6,7% sistemos sutrikimu skaičius, visų bandymu metu. Sistemos sutrikimo metu buvo pastebėta, jog ne visų programų darbas buvo nutrauktas, tačiau įvykus sutrikimui kliento programa buvo atjungiama nuo ryšio su serveriu.



40 pav. Neleistinų programų nutraukimo laikas, šifruota žinutė

Iš 39 pav. matome, jog pilnas žinutės šifravimas sumažina sistemos stabilumą, bei pailgina užduočių atlikimo greitį. Taipogi matome jog sistemos sutrikimai atsiranda ne viename įrenginyje o visose trijuose bandomuose įrenginiuose. Kaip matome iš grafiko, pirmas (Colossus) ir trečias (C13604971) įrenginiai veikė stabiliau palyginus su antru (Gamer-Full) įrenginiu, tačiau turėjo sistemos sutrikimų, bei neįvykdė užduočių iki galo. Šitame tyrime stebime labai panašų vaizdą kaip ir pirmame tyrime: sistemos stabilumas ir greitaveika sumažėja padidinus sistemos apsaugos lygį. Tačiau norint tinkamai apsaugoti visus įrenginius bei užtikrinti atitinkamą saugumo lygį, yra rekomenduojama naudoti pilną ryšio ir žinutės šifravimą, tokiu būdu užkertant daugelį puolimo vektorių. 40 pav. pateikiame serverio ir kliento žinučių apsikeitimo vaizdą, ką gauna ir persiunčia brokeris.



41 pav. Neleistinų programų nutraukimo pranešimai, šifruota žinutė

3.3. Eksperimentinio tyrimo rezultatų apibendrinimas

- Pirmoje tyrimo dalyje buvo ištirtas sistemos *false positive rate* (neteisingai atpažintų įrenginių rodiklis, toliau FPR) kuris skirtas parodyti kiek kartų sistema autentifikuoja įrenginį jam esant nesaugiu, arba kiek kartu įrenginys buvo klaidingai neautentifikuotas esant saugiam įrenginiui. Papildomai su FPR tyrimu buvo tiriama autentifikavimo vykdymo greitaveika pasinaudojus dviem skirtingomis sistemos konfigūracijomis : šifruotu ryšiu ir šifruotu ryšiu su šifruota žinute.
- Buvo atlikta daugiau 300 bandymu, kuriu metu buvo ištirtas autentifikavimo proceso veikimas. Sistemos sutrikimų skaičius sudarė 6,667%. Vidutinis nešifruotos žinutės autentifikavimo užklausos laiko tarpas sudaro 0,229079 sekundės. Naudojantis nešifruotos žinutės sistemos konfigūracija, sistemos sutrikimu pastebėta nebuvo. Buvo bandomas įrenginio autentifikavimas esant saugiam įrenginiui, bei imitavus įrenginio saugumo būsenos praradimą. Nepastebėta ne vieno atvejo kai sistema būtų klaidingai autentifikavusi sistema.
- Pilnai šifruotos žinutės atveju pablogėjo sistemos stabilumas, vidutinis užklausos vykdymo laiko tarpas pailgėjo 4,6875 karto. Sutrikimų skaičius sudarė 6,7% visų bandymų. Eksperimento metu buvo naudojamos skirtingos įrenginių konfigūracijos, aprašytos 12 lentelėje. Pagrindiniai sutrikimai buvo pastebėti vykdant programos kodą bei gaunant blogai užšifruotą žinutę, dėl kurios ir buvo nutraukiamas sistemos darbas.
- Gavus FPR tyrimo rezultatus buvo nustatytas sistemos veikimo tikslumas, kuris sudaro 93,88%.

- Antroje tyrimo dalyje buvo ištirtas neleistinų programų nutraukimo greitaveika, bei tokių sistemos užklausų neįvykdymo skaičius. Tyrimui buvo naudojamas stabilus skaičius paleistu programų, su skirtingais programų parametrais, kurie reikalauja vartotojo įsikišimo į programos uždarymą. Sistemai nenutraukus programos vykdymo, be vartotojo įsikišimo, yra traktuojama kaip sistemos klaida ir skaitoma jog sistema neįvykdė užduoties.
- Vidutinis neleistinos programos nutraukimo laiko tarpas sudaro 0,441076 sekundės. Palyginus su sistemos autentifikavimu be programų nutraukimo, laiko tarpas pailgėja 0,22 sekundės. Tiriant duotąją konfigūracija nebuvo pastebėta ne vienos nenutrauktos programos.
- Lyginant su nešifruotos žinutės sistemos konfigūracija, pilnai šifruotos žinutės užklausos įvykdymo laiko tarpas vidutiniškai pailgėjo 3,445 karto ir sudarė 1,519707 sekundės. Sistemos stabilumas ir neleistinų programų nutraukimo nesėkmingų užklausų kiekis sudarė 6,7% visų bandymų.

- Remiantis tyrimo gautais rezultatais yra rekomenduojama naudoti pilną žinutės šifravimą, taip kaip tai leidžia geriausiai apsaugoti sistemą nuo nesankcionuotos piktavalių prieigos, bei užtikrinti sistemos saugumą. Naudojantis tokia konfigūracija yra prarandamas sistemos stabilumas, dėl ko reikėtų ištirti mažiau resursų reikalaujančius šifravimo metodus.

Išvados

- Šiais laikais vis dažniau pastebima tendencija, kad vis daugiau įmonių leidžia darbuotojams naudotis savo išmaniais įrenginiais. Tipiškai BYOD apima tokius įrenginius kaip mobiliuosius įrenginius bei planšetinius kompiuterius, bet BYOD gali būti taikomas ir asmeniniams nešiojamiems kompiuteriams. Nors BYOD integracija įmonėje suteikia daug privalumų, įmonė privalo atsižvelgti ir į saugumo spragas;
- Nors ir daug dėmesio yra skiriama pačių įrenginių operacinių sistemų ir programų saugumui, tačiau juose vis tiek išlieka daug pažeidžiamumu, tokiu kaip: Tiesioginės įsilaužėlių atakos, tinklo srauto perėmimas, neteisinga vartotojų elgsena, piktavališkos programėlės, pavogti arba pamesti įrenginiai;
- Norint apsaugoti įmonę nuo konfidencialių duomenų praradimo, yra būtina sudaryti sprendimą, kuris apimtu savyje ne tik saugaus ryšio užtikrinimą bei vartotojo autentifikavimą ir autorizavimą, bet ir paleistų ir įdiegtų programų tikrinimą, įrenginio komponentų integralumą ir kompiuterio komponentų identifikavimą ir autorizavimą;
- Pasiūlytas asmeninių įrenginių, naudojamųjų įmonėse, saugaus autentifikavimo sistema, skirta asmeninių įrenginių saugiam autentifikavimui, programų tikrinimui bei įrenginio vientisumui užtikrinti;
- SAS sistemos modelis leidžia ne tik autentifikuoti įrenginius, bet kartu ir tikrinti vykdomas programas įrenginyje, tikrinami įrenginio esami parametrai, lyginant juos su registruotais sistemoje, bei užtikrinama jog įrenginyje vykdomos tik tos programos, kurios yra leidžiamos sistemoje;
- Vienas iš sistemos bruožu – klientas nežino kur randasi serveris. Esant nulaužtam įrenginiui jis negali tiesiai prieiti prie serverio. Komunikacijos su serveriu yra vykdomos tarpinio brokerio pagalba, kuris perduoda pranešimus prenumeratoriams, prisijungusiems prie atitinkamos sesijos;
- Atlikus sistemos prototipo tyrimą buvo nustatytą:
    - Saugiausia sistemos konfigūracija yra pilnas ryšio tarp serverio ir kliento šifravimas su papildomu žinutės šifravimu;
    - Šifruotos žinutės autentifikavimas lyginant su nešifruotos žintutės autentifikavimu užtrunka 4,6875 kartų ilgiau;
    - FPR tyrimo metu nebuvo nustatyta klaidingų autentifikavimų;
    - Sistemos įrenginio autentifikavimo sutrikimu skaičius, naudojant pilną ryšio ir žinutės šifravimą, sudaro 6,667%;
    - Šifruotos žinutės neleistinų programų nutraukimo komandos vykdymo laiko tarpas, lyginant su nešifruotos žinutės neleistinų programų nutraukimo komandos vykdymo laiko tarpu skiriasi 3,455 kartų;
    - Sistemos neleistinų programų nutraukimo sutrikimu skaičius, naudojant pilną ryšio ir žinutės šifravimą sudaro 6,7%;
- Remiantis tyrimo gautais rezultatais yra rekomenduojama naudoti pilną ryšio ir žinutės šifravimą. Pilnas šifravimas užtikrina, jog net piktavaliui perėmus šifruotus paketus ir juos iššifravus, piktavaliui nepavyks perskaityti žinutės turinio.

Literatūros sąrašas

[1] Mohammed Ketel, Thomas Shumate, „Bring Your Own Device: Security Technologies“, IEEE SoutheastCon, 2015.

[2] Yong Wang, Jinpeng Wei, Karthik Vangury, „Bring Your Own Device Security Issues and Challenges“, The 11th Annual IEEE CCNC, 2014.

[3] Alessandro Armando, Gabriele Costa, Luca Verderame, Alessio Merlo, „Securing the “Bring Your Own Device” Paradigm“, 30th IEEE International Conference on Software Maintenance and Evolution, 2014.

[4] „THE IMPACT OF MOBILE DEVICES ON INFORMATION SECURITY:A SURVEY OF IT PROFESSIONALS“, Dimensional research. 2013.

[5] Nima Zahadat, Paul Blessner, Timothy Blackburn, Bill A. Olson, „BYOD security engineering: A framework and its analysis“, The GeorgeWashington University, USA. 2015.

[6] Manmeet Mahinderjit Singh, Soh Sin Siang,Oh Ying San, Nurul Hashimah Ahamed Hassain Malim, Azizul Rahman Mohd Shariff, „SECURITY ATTACKS TAXONOMY ON BRING YOUR OWN DEVICES (BYOD) MODEL“, International Journal of Mobile Network Communications & Telematics, 2014.

[7] J. Morris Chang, Pao-Chung Ho, Teng-Chang Chang, „Securing BYOD“, IT Professional (Volume: 16 , Issue: 5 , Sept.-Oct. 2014).

[8] Meisam Eslahi, Maryam Var Naseri, H. Hashim, N.M. Tahir1, Ezril Hisham Mat Saad, „BYOD: Current State and Security Challenges“, 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), 2014.

[9] Shigeaki Tanimoto, Susumu Yamada, Motoi Iwashita, Hiroyuki Sato, Toru Kobayashi, Atsushi Kanai, „Risk Assessment of BYOD: Bring Your Own Device“, 2016 IEEE 5th Global Conference on Consumer Electronics, 2016.

[10] Mark A. Harris, Karen P. Patten, „Information Management & Computer Security“, Information Management & Computer Security, 2014.

[11] Sara Ali, Muhammad Nauman Queshi, Abdul Ghafoor Abbasi, „Analysis of BYOD Security Frameworks“, 2015 Conference on Information Assurance and Cyber Security (CIACS) 2015.

[12] Murugyah Souppaya, Karen Scarfone, „ Guide to enterprise telework, remote access, and bring your own device (BYOD) security“, NIST Special publication 800-46 revision 2, 2016.

[13] Koneru et al. „Mobile application management systems and methods thereof“, US patents No.9,405,723 B2. 2016.

[14] Kathleen Downer, Maumita Bhattacharya, „BYOD Security: A new Business Challenge“, 2015 IEEE International Conference on Smart City/SocialCom/SustainCom together with DataCom 2015 and SC2. 2015

[15] Khalid Waleed Hussein, Dr. Nor Fazlida Mohd. Sani, Professor Dr. Ramlan Mahmood, Dr. Mohd. Taufik Abdullah, “ Design and Implementation of Multi Factor Mechanism for Secure Authentication System. IJCSIS. 2013

[16] Kuwar Kuldeep VV Singh, Himanshu Gupta, „A new approach for the security of VPN“, ICTCS’16, 2016.

[17] M.A. Mohamed, M.E.A. Abou-El-Seoud, A.M. El-Feki,“ A survey of VPN security Issues“, Mansoura University. 2014.

[18] Starcounter,“ Operating System Market Share Worldwide“,2019. [Tinkle]. Available: https://gs.statcounter.com/os-market-share. Kreiptasi: 2019-04-20.

[19] Christian Lesjak, Daniel Hein, Michael Hofmann ir kt., „Securing Smart Maintenance Services: Hardware-Security and TLS for MQTT“, 2015.

[20] Aimaschana Niruntasukat, Chavee Issariyapat, Panita Pongpaibool ir kt., „Authorization Mechanism for MQTT-based Internet of Things“, NSTDA. 2016.

[21] Ajay Kakkar, M.L. Singh, P.K. Bansal,“ Comparison of various encryption algorithms and techniques for secured data communication in multinode network“, 2013.

[22] Saikumar Manku, K.Vasanth,“Blowfish encryption algorithm for information security“, 2015.

[23] Adhitya Bhawiyuga, Mahendra Data, Andri Warda, “Architectural Design of Token based Authentication of MQTT Protocol in Constrained IoT Device”.IEEE. 2017