KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACIJOS IR INFORMACINIŲ TECHNOLOGIJŲ SAUGOS
STUDIJŲ PROGRAMA

TOMAS MIKELAITIS

PRAĖJIMO KONTROLĖS SISTEMOS SU BLUETOOTH AUTENTIFIKAVIMO MODULIO CHARAKTERISTIKŲ TYRIMAS

Magistro baigiamasis darbas

Darbo vadovas
lekt. D. Rimkus

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACIJOS IR INFORMACINIŲ TECHNOLOGIJŲ SAUGOS
STUDIJŲ PROGRAMA

TOMAS MIKELAITIS

PRAĖJIMO KONTROLĖS SISTEMOS SU BLUETOOTH AUTENTIFIKAVIMO MODULIO CHARAKTERISTIKŲ TYRIMAS

Magistro baigiamasis darbas

Darbo vadovas
lekt. D. Rimkus

Recenzentas
dr. K. Paulikas

KAUNAS, 2013

AUTORIŲ GARANTINIS RAŠTAS

DĖL PATEIKIAMO KŪRINIO

2013 - 05 -23 d.
Kaunas

Autoriai, Tomas Mikelaitis,
(vardas, pavardė)

patvirtina, kad Kauno technologijos universitetui pateiktas baigiamasis bakalauro (magistro) darbas (toliau vadinama – Kūrinys) Praėjimo kontrolės sistemos su bluetooth autentifikavimo modulio charakteristikų tyrimas
(kūrinio pavadinimas)
pagal Lietuvos Respublikos autorių ir gretutinių teisių įstatymą yra originalus ir užtikrina, kad

1) jį sukūrė ir parašė Kūrinyje įvardyti autoriai;
2) Kūrinys nėra ir nebus įteiktas kitoms institucijoms (universitetams) (tiek lietuvių, tiek užsienio kalba);
3) Kūrinyje nėra teiginių, neatitinkančių tikrovės, ar medžiagos, kuri galėtų pažeisti kito fizinio ar juridinio asmens intelektinės nuosavybės teises, leidėjų bei finansuotojų reikalavimus ir sąlygas;
4) visi Kūrinyje naudojami šaltiniai yra cituojami (su nuoroda į pirminį šaltinį ir autorių);
5) neprieštarauja dėl Kūrinio platinimo visomis oficialiomis sklaidos priemonėmis.
6) atlygins Kauno technologijos universitetui ir tretiesiems asmenims žalą ir nuostolius, atsiradusius dėl pažeidimų, susijusių su aukščiau išvardintų Autorių garantijų nesilaikymu;
7) Autoriai už šiame rašte pateiktos informacijos teisingumą atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

Autoriai

Tomas Mikelaitis	_____
(vardas, pavardė)	(parašas)
_____	_____
(vardas, pavardė)	(parašas)
_____	_____
(vardas, pavardė)	(parašas)
_____	_____
(vardas, pavardė)	(parašas)

SANTRAUKA

Magistiniame darbe tiriamos praėjimo kontrolės sistemos su Bluetooth autentifikavimo moduliu charakteristikos. Pirmojoje dalyje aprašoma Bluetooth technologijos raida, standartai, sistemos architektūra, privalumai, pritaikymo galimybės. Šioje dalyje didžiausias dėmesys kreipiamas į Bluetooth technologijos paplitimą ir įrenginių, turinčių įdiegtą Bluetooth technologiją, pritaikymą praėjimo kontrolės autentifikacijos modeliui. Nagrinėjama, kokius žingsnius turi atlikti įrenginys norėdamas užmegzti tarpusavio ryšį. Taip pat dėmesys kreipiamas į įrenginyje saugomus duomenis, kurie gali būti panaudojmi indentifikacijai: Bluetooth MAC, Mobilaus įrenginio IMEI kodas, Sim kortelės duomenys. Analizuoti kitų autorių siūlomi autentifikacijos mechanizmai.

Antrojoje dalyje detaliai aprašomas praėjimo kontrolės sistemos su Bluetooth technologija autentifikacijos modelis ir pagal jį sukurta praėjimo kontrolės sistema. Šis modelis nuo anksčiau nagrinėtų modelių skiriasi autentifikavimo saugumo lygiu. Jis papildytas nesuklastojamomis arba sunkiai suklastojamomis autentifikacijos žymomis. Pagal šį modelį suprojektuota praėjimo kontrolės sistema, kuri fiksuoja vartotojo judėjimo kryptį ir įvykio laiką.

Eksperimentinio tyrimo dalyje koncentruojamasi į sukurtos sistemos veikimo greitaveiką ir serverio resursų naudojimą esant skirtingiems vartotojų kiekiams. Eksperimentų metu nustatyta, kad sistema kokybiškai gali aptarnauti iki 7 vienu metu prisijungusių klientų. Norint padidinti vartotojų aptarnavimo kiekius reikia papildomai prijungti Bluetooth priedėlius, kurie pagreitintų praėjimo kontrolės sistemos autentifikacijos laiką.

SUMMARY

This thesis of Master studies the characteristics of access control systems over Bluetooth authentication model. First part describes Bluetooth technology development, standards, system architecture, benefits, application possibilities. In this part the most focus is on the spreading of Bluetooth technology and Bluetooth enabled devices adaptation to access control authentication model. Here are analyzed steps device takes to establish a connection with another device. Also described data stored in the device which are used for authentication: Bluetooth MAC, mobile device IMEI and Sim card data. Other authors suggested authentication mechanics are introduced.

Second part contains detailed description about created access control authentication system based on Bluetooth technology. This model differs from others by its authentication security level. It contains hard to forge authentication tags. So access control system is created based on that model, which trace user direction of movement and incident time.

In part of experimental study system throughput and use of server recourses given different amount of users are analyzed. During the experiment is determined that system can qualitatively maintain to seven connected users at a time. If more users is required to maintain, Bluetooth set-top must be connected to enchance control system authentication time.

Turinys

Paveikslėlių sąrašas

Lentelių sąrašas

Terminų santrumpų žodynas

Bluetooth (angl. *blue tooth*, „mėlynas dantis“) – belaidžio ryšio gamybinė specifikacija, naudojama asmeniniuose tinkluose.
Piko tinklas (angl. Piconet) - ad hoc kompiuterių tinklas, jungiantis belaidę vartotojų grupę prietaisų per "Bluetooth" protokolą.

Įvadas

Tyrimo sritis

Bevielės technologijos dėl prieinamos kainos ir lankstumo yra labai populiari alternatyva laidinėms jungtims. Bluetooth technologija - viena iš bevielių technologijų, kuri pritaikoma įvairiose sistemose, pavyzdžiui: praėjimo kontrolės, atliekant mokėjimus, reguliuojant žmonių srautus įvairiose organizacijose ir t.t.

Dauguma praėjimo kontrolės sistemų, veikiančių bluetooth technologijos pagrindu, sukurtos rinkti statistikai apie žmonių judėjimą pro tam tikrą atskaitos tašką. Tokia sistema yra tinkama rinkti tik statistiniams duomenis ir nereikalaujama, kad vartotojas būtų unikalus, tai pat judėjimo kryptis - nesvarbi.

Autentifikacijos mechanizmas yra vienas svarbiausių praėjimo kontrolės sudedamųjų dalių, kuri privalo užtikrinti vartotojų unikalumą ir nustatyti vartotojo tapatybę iš jo turimų duomenų. Taip pat sumažinti patekimo galimybę neautorizuotiems vartotojams prie saugomo resursų. Šiai sudedamajai daliai veikiant netinkamai, organizacija gali patirti didelius finansinius ir moralinius nuostolius. Moksliniuose darbuose yra aprašyta keletas būdų, kaip būtų galima įvykdyti autentifikaciją pasinaudojant bluetooth technologija.

Darbo tikslas

Pasiūlyti praėjimo kontrolės sistemos autentifikacijos mechanizmą, veikiantį bluetooth technologijos pagrindu, ir įvertinti bei ištirti pasiūlytos praėjimo kontrolės su bluetooth sistemos moduliu veikimo charakteristikas.

Darbo uždaviniai

- ✓ Išnagrinėti bluetooth esančias versijas ir jų galimybes taikant praėjimo kontrolės sistemoje.
- ✓ Panaudoti autentifikavimo arba alternatyvius saugumo padidinimo metodus praėjimo kontrolės sistemoje.
- ✓ Pasiūlyti praėjimo kontrolės sistemai, veikiančiai bluetooth technologijos pagrindu, identifikavimo ir autentifikavimo mechanizmą.
- ✓ Sukurti eksperimentinę praėjimo kontrolės sistemą su įdiegtu saugos moduliu
- ✓ Atlikti sukurto modelio įvertinimą.

1 Analizė

1.1 Bluetooth technologija

Bluetooth – nesena technologija, kuri naudoja radijo ryšį trumpais atstumais. Taip siekiama pakeisti stacionarių ir nešiojamų prietaisų sujungimus kabeliais į sujungimus radijo ryšiu. Bluetooth technologijos standartas nusako bendrą daugumos elektrinių prietaisų apsikeitimo duomenimis struktūrą. Pagrindiniai šios technologijos privalumai: ilgaamžiškumas, mažos energijos sąnaudos, paprastumas ir sąlyginai nedidelė įrenginio kaina lyginant su kitokio tipo panašias galimybes turinčiu įrenginiu. Šis standartas siekia užtikrinti plačias pritaikymo galimybes, pavyzdžiui, kiekvienas Bluetooth įrenginys turi turėti galimybę keistis duomenimis su kitais įrenginiais, esančiais veikimo zonoje,

nepriklausomai nuo to kurioje valstybėje ar vietoje juo naudojamasi. Bluetooth įrenginiai duomenimis keičiasi radijo ryšio pagalba. Ryšį užtikrina piko tinklai (angl. piconet). Vienas įrenginys vienu metu gali keistis duomenimis ne daugiau kaip su septyniais įrenginiais, bet tuo pačiu metu daug įrenginių gali būti laukimo zonoje. Šioje zonoje laukiama kol atsilaisvins susijungimo kanalas arba kuris nors greta esantis įrenginys panorės su juo užmegzti ryšį duomenų perdavimui. Kiekvienas įrenginys vienu metu gali susijungti į keletą tinklų ir taip padidinti perdavimo galimybes ir spartą [7]. Iki šių dienų yra sukurtos keturios Bluetooth versijos. Su kiekviena versija didėja duomenų perdavimo spartos ir susijungimo sauga.

1 Lentelė Bluetooth standartai

Bluetooth standarto versija	Duomenų perdavimo sparta	Didžiausias pralaidumas
V 1.2	1Mbit/s	0,7 Mbit/s
V 2.0 +EDR	3 Mbit/s	2.1 Mbit/s
V 3.0 + HS	Apie 24 Mbit/s	Su stiprintuvu galimybės didėja. Be stiprintuvo 2.1 Mbit/s
V 4.0	Apie 24 Mbit/s	Su stiprintuvu galimybės didėja. Be stiprintuvo 2.1 Mbit/s

Šiuo metu labiausiai pasaulyje paplitę Bluetooth įrenginiai, turintys v2.0 standartą.

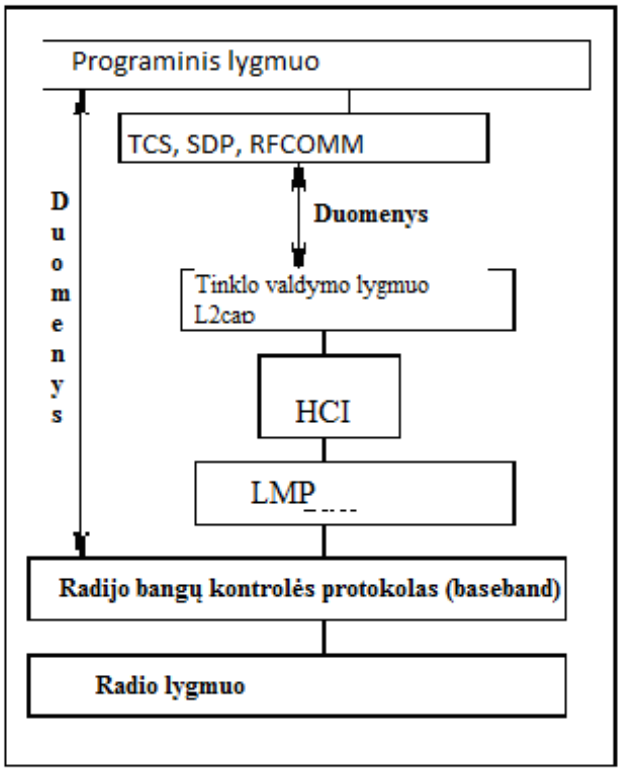
Bluetooth populiariausi standartai pateikti 1 lentelėje. Bluetooth standartas skirstomas į tris klases (2 lentelė): pagal veikimo nuotolį ir suvartojamą energijos kiekį. Kuo mažesnis nuotolis, tuo mažesnės energijos sąnaudos. Bluetooth technologija gali veikti ne daugiau kaip 100 metrų spinduliu.[7]

Ketvirtojoje Bluetooth versijoje energijos sąnaudos pačios mažiausios lyginant su ankstesnėmis versijomis. Taip pat ši versija pasižymi dideliu duomenų perdavimo atstumu. Lyginant su antrąja ir trečiąja bluetooth versija duomenų perdavimo sparta ketvirtojoje versijoje neišaugo dėl siekio taupyti energijos resursus. Bluetooth ketvirtoje versijoje yra įdiegtas saugus duomenų perdavimas pasinaudojant AES šifravimo algoritmą.[7]

2 Lentelė Bluetooth klasių skirstymas

	Maksimali energija		Maksimalus atstumas
	mW	dBm	
1 klasė	100	20	~100m
2 klasė	2.5	4	~10m
3 klasė	1	0	~1m

1.1.1 Bazinė Bluetooth sistemos architektūra



1 pav. Bazinio Bluetooth protokolo sudėtis

1 paveikslėlyje pateiktos protokolo sudėtinės dalys 1) radijo lygmuo, kuris formuoja fizinę ryšio sąsają, 2) radijo bangų kontrolė (angl. baseband), 3) nukreipimo protokolas LMP (angl. Link Manager Protocol), kurie paveiksle grafiškai pavaizduoti virš radijo lygmens. Jie skirti ryšio užmezgimui ir jo kontroliavimui tarp Bluetooth įrenginių. Minėtieji trys lygmenys paprastai būna realizuoti aparatiniame (angl. firmware/hardware) lygmenyje. Tinklo valdymo lygmuo reikalingas formuojant sąsają su aukštesniuoju protokolu – L2CAP (angl. Logical Link Control and Adoptation Protocol). Tinklo valdymo lygmuo naudojamas tik tuomet, jei L2CAP protokolas įgyvendintas programiniame lygmenyje. Jeigu L2CAP integruotas į bluetooth modulį, tinklo valdymo lygmuo praleidžiamas, nes L2CAP gali tiesiogiai užmegzti ryšį su LMP.

Radijo lygmuo

Radijo bangų dažnio juosta yra ties 2.4GHz. Naudojimasis šia dažnių juosta yra neapmokestintas, t.y. tam nereikia licenzijos. Ryšiui skleisti naudojama spektro (angl. spread spectrum) technologija – dažnių juostos plotis nuo 2400 iki 2483,5 MHz.

Radijo bangų kontrolės protokolas

Šis protokolas kontroliuoja radijo ryšį. Dažnių šokinėjimas, pirminis signalo kodavimas bei paketų formavimas valdomi radijo lygmens. Gali būti formuojami du ryšių tipai:

SCO: sinchroninis ryšys (angl. Synchronous Connection Oriented). Toks ryšys skirtas sinchroniniam duomenų perdavimui.

ACL: asinchroninis ryšys (angl. Asynchronous Connection Less). Toks ryšys gali būti naudojamas duomenų, nereikalaujančių SCO, perdavimui.

Radijo bangų kontrolės protokolas atlieka įrenginių taktavimo sinchronizavimo ir ryšio palaikymo ir tinklo veikimo zonoje esančių prietaisų adresų nustatymo funkcijas.

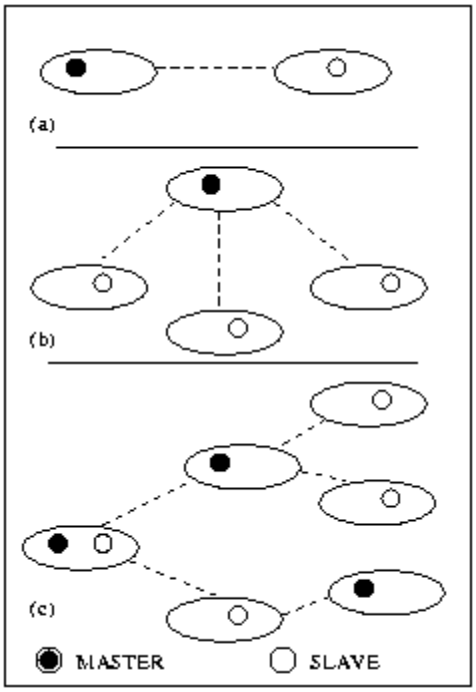
Nukreipimo protokolas

Pagrindinės nukreipimo protokolo (LMP) funkcijos yra šios:

- Piko tinklų administravimas
- ryšio parametrų konfigūravimas
- apsaugos funkcijos

Piko tinklas – tai įrenginių, prisijungusių prie bendro tinklo, grupė. Vienas iš įrenginių (paprastai pirmasis prisijungęs prie tinklo) yra valdantysis (angl. master). Vienu metu iki septynių kitų įrenginių gali aktyviai keistis informacija su valdančiuoju įrenginiu. Dar daugiau įrenginių gali būti savotiškoje laukimo būsenoje (angl. low power "parked" state), kol vienas iš septynių aktyviai besikeičiančių duomenimis įrenginių baigs šią operaciją pereidamas į laukimo būseną ir užleis savo vietą kitam įrenginiui. Bet kurie du tarpusavyje norintys užmegzti ryšį įrenginiai turi sukurti tarpusavio piko tinklą. Įrenginys tuo pat metu gali priklausyti keletui piko tinklų (žr. 2 pav.).

Apibendrinant galima sakyti, kad LMP protokolas atlieka valdomųjų (angl. slave) įrenginių įjungimo arba išjungimo iš ryšio linijos, perjungimo tarp valdančiojo ir valdomojo būsenų funkcijas, užtikrina ACL/SCO tipo ryšius. Šiam protokolui priskiriama ir laukimo būsenos inicijavimas, siekiant geriau naudoti įrenginio energetinius išteklius, kai nesiunčiami ir nepriimami jokie duomenys.



2 pav. pikotinklo pavyzdžiai: a) tarp dviejų įrenginių, b) tarp daugelio įrenginių, c) kombinacija tarp įrenginių, priklausančių keletui pikotinklų.

L2CAP protokolas

Pagrindinės L2CAP funkcijos:

- multipleksavimas. Protokolas turi užtikrinti, kad keletui tuo pačiu metu vykdomų programų būtų galima naudotis ryšiu tarp dviejų įrenginių.
- segmentavimas ir jam inversinė operacija. Protokolas turi sumažinti paketų dydį, kad užtikrintų optimalų duomenų srauto pralaidumą be iškraipymų. L2CAP gali suformuoti net iki 64 kb dydžio paketus, tačiau ryšio kanalu perduodami ne didesni kaip 2745 bitų paketai. Inversinė segmentavimo operacija skirta segmentuotų paketo dalių sujungimui nustatytu eiliškumu į vientisą paketą. Sujungiama tokia tvarka, kokia ir buvo prieš segmentavimą.

Trumpai tariant, L2CAP protokolas atlieka sąsajos vaidmenį tarp tinklinio lygmens ir "aukštesnių" protokolų.

Tinklo kontrolės sąsaja

Daugeliui įrenginių Bluetooth priedėlis gali būti įdiegtas kaip atskiras Bluetooth įrenginys. Pavyzdžiui, asmeniniuose/nešiojamuose kompiuteriuose Bluetooth aparatinė įranga gali būti integruota į PCI (angl. Peripherial Components Interconnection) jungtį arba USB (angl. Universal Serial Bus) pritaikytuvą. Aparatinė įranga dažniausiai realizuoja radijo ir LMP lygmenis. Duomenys, siunčiami į LMP ir perduodami fizine duomenų šyna (angl. bus), pvz. USB. "Tinkle", t.y. kompiuteryje, reikalingos specialios tvarkyklės (angl. drivers), o Bluetooth įrenginyje - tinklo kontrolerio sąsajos (ang. host controller interface), priimančios duomenis, gaunamus duomenų šyna. Jeigu L2CAP ir "aukštesni" protokolai realizuoti programiškai, o "žemesni" aparatiškai, reikalingi sekantys papildomi lygmenys:

1. **HCI tvarkyklės**

Tai tinklo kontrolerio sąsajos tvarkyklės. Jos suteikia duomenims formatą, suprantamą tinklo kontroleriui.

2. **Tinklo kontrolės sąsaja**

Sąsaja įgyvendinta Bluetooth aparatiniame lygmenyje ir skirta duomenų apsikeitimui su kompiuterio duomenų šyna.

3. **Programinis lygmuo**

L2CAP protokolas gali būti susietas su programiniu lygmeniu tiesiogiai arba per palaikomus protokolus, tokius kaip RFCOMM, TCS ir SDP. Galimas ir TCP-IP bei WAP protokolų palaikymas. Priklausomai nuo poreikių, programos gali naudotis PPP (angl. Point to Point Protocol) arba FTP (angl. File Transfer Protocol) tipų protokolais.

1.1.2 Ryšio užmezgimas ir palaikymas

Šioje dalyje panagrinėsime kokius žingsnius turi atlikti įrenginys norėdamas užmegzti tarpusavio ryšį.

1. Paklausimas: įrenginys, patekęs į naują aplinką, pats automatiškai inicijuoja užklausą norėdamas sužinoti apie savo aprėptyje esančio piko tinklo veikimo zoną ir jame esančius įrenginius:

a)Visi gretimi tinklai ir įrenginiai pasiųs įrenginiui savo adresus.

b) Bus pasirinktas vienas iš adresų.

Jeigu tinklas nebus rastas, tai įrenginio programinė įranga praneš apie tai automatiškai.

2. Šaukimas: įrenginys inicijuos procedūrą, vadinamą šaukimu. Šaukimo rezultate gaunamas įrenginio sinchronizavimas su tinklu (t.y. sinchronizuojamas taktavimas, fazės poslinkis ir dažnių šokinėjimo intervalai).

3. ryšio užmezgimas: LMP protokolas užmegs ryšį tarp įrenginio ir tinklo.

4. paslaugų nustatymas: LMP kartu su SDP (angl. Service Discovery Protocol) nustatys kokios tinklo paslaugos yra tiekiamos ir ar yra galimybė išsiųsti bei gauti elektroninį paštą. Tarkim, ši paslauga tinkle yra tiekiama. Informacija apie kitas tinklo paslaugas gali būti taip pat pateikiama vartotojui.

5. L2CAP kanalo sukūrimas: įrenginys, gavęs informaciją iš SDP, sukurs L2CAP kanalą su tinklu. Sukurtas kanalas gali būti tiesiogiai naudojamas programos arba kito protokolo.

6. Apsauga: jeigu tinklas uždraudžia arba atvirkščiai – pasiūlo konfidencialų ir apsaugotą ryšį su žmonių, turinčių išskirtines saugumo teises, grupe, tuomet siunčiama speciali užklausa. Vartotojas privalo įvesti asmeninės identifikacijos kodą (angl. PIN). Saugumo sumetimais PIN nėra siunčiamas radijo bangomis. PIN pagrindu sugeneruojamas specialus raktas, todėl sunku "įsilaužti" į sistemą. Keičiantis duomenimis apsaugotu režimu - duomenys yra koduojami.

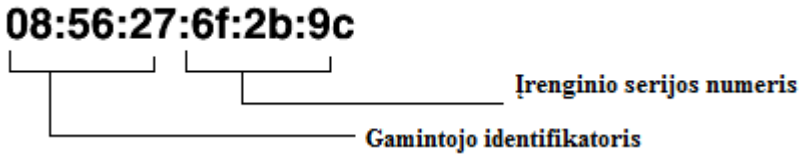
7. PPP (angl. Point to Point Protocol): žinant, kad PPP sąsaja naudojama ryšiui su modemais ir telekomunikaciniais tinklais, programos gali vykdyti PPP per RFCOMM (atliekant serijinio prievado emuliaciją). PPP leidžia vartotojui prisijungti prie jo elektroninio pašto sąskaitos.

9 Tinklo protokolai: tokie tinklo protokolai kaip TCP/IP, IPX, Appletalk taip pat gali siųsti ir priimti duomenis per PPP sąsają.[7][12]

1.2 Mobilaus įrenginio ir lustuose saugomi duomenys kurie gali būti panaudoti identifikacijai

1.2.1 Bluetooth MAC

MAC adresas (*angl. Media Access Control address*) yra unikalus daugelio tinklo plokščių ir kitų tinklo įrenginių identifikatorius, kurį priskiria gamintojas. Yra saugomas įrenginio nemodifikuojamoje atmintyje (read-only memory) ar kitoje aparatinėje dalyje. Kiekvienas įrenginys turi tik jam vienam priskirtą MAC unikalų adresą, kuriame yra užšifruotas gamintojo kodas, įrenginio serijos numeris(3 pav.).



3 pav. MAC adreso schema

Šis adresas nėra tinkamas sistemos vartotojui autentifikuoti dėl keleto priežasčių:

- ✓ Lengvai klonuojamas
- ✓ Greitai sužinomas pasiklausant tinklą[10].

1.2.2 Mobilaus įrenginio IMEI kodas

IMEI (International Mobile Station Equipment Identity) tai kodas kuris yra unikalus, identifikuojantis mobiliuosius telefonus. Šis kodas būna užrašytas ant mobiliojo telefono korpuso ir įdiegtas mobiliojo įrenginio operacinėje sistemoje ar telefono pastoviojoje atmintyje. IMEI kodas padeda mobiliųjų tinklų operatoriui atpažinti mobilųjį įrenginį ir reikalui esant gali uždrausti vartotojo prisijungimą prie tinklo (pvz. vagystės atveju, kai iš vartotojo pavagiamas telefonas). IMEI naudojamas tik identifikuoti prietaisą, bet negali būti naudojamas mobiliojo abonento atpažinimui, tam naudojamas IMSI (tarptautinis judriojo ryšio abonento identifikatorius), kuris yra saugomas SIM kortelėje.

IMEI kodo sandara

IMEI kodas susideda iš 14 dešimtainių skaitmenų arba IMEISV- 16. IMEI kode saugoma informacija apie kilmę, modelį ir įrenginio serijinį numerį. IMEI/SV savyje prie viso to saugo ir programinės įrangos versiją.

Pirmi aštuoni skaitmenys yra paskirties kodas(TAC- Type Allocation Code), sekantys šeši skaitmenys - serijos numeris. Likę skaitmenys nurodo Luhn algoritmu gautą reikšmę (jai likęs vienas skaitmuo) arba programinės įrangos versiją (kai likę būna trys skaitmenys). IMEI kodo sandara pateikta 4 pav.

	AA	**-**	**BB**	**BB**	**BB**	**-**	**CC**	**CC**	**CC**	**D arba EE**
IMEI	TAC					Serijinis numeris				Luhn algoritmu suskaičiuota kontrolinė suma
IMEISV	TAC					Serijinis numeris				Programinės įrangos versijos numeris

4 pav. IMEI kodo sandara

Norint suklastoti IMEI kodą naujuose mobiliojo ryšio įrenginiuose reikia pakeisti visą pagrindinę telefono plokštę. Dėl to IMEI kodas negali būti suklastojamas, kaip buvo galimas suklastoti senesnio modelio įrenginiuose, kuriuose kodas buvo saugoma operacinėje sistemoje.[15]

1.2.3 Sim kortelės duomenys

Judriojo vartotojo abonento identifikavimo modulis- kortelė (Subscriber identity module- SIM). Šiame modulyje saugomas tarptautinis judriojo ryšio identifikatorius (IMSI) ir atitinkamas raktas, kuris naudojamas nustatyti ir patvirtinti judriojo ryšio telefonijos prietaisai (pavyzdžiui, mobiliųjų telefonų ir kompiuterių).

SIM kortelė turi savo unikalų serijos numerį (ICCID), tarptautinį judriojo ryšio abonento identifikatorių (IMSI), saugumo, autentifikavimo ir kodavimo informaciją. SIM kortelėje tai pat saugoma laikina informacija, susijusi su vietiniu tinklu ir vietinio tinklo teikiamomis paslaugomis. Vartotojas norėdamas pasiekti SIM kortelėje esančius duomenis turi įvesti asmens identifikavimo kodą (PIN), o tris kartus neteisingai įvedus, ir asmeninį

SIM kortelės atblokavimo kodą (PUK). PUK galima įvesti devynis kartus, devintą kartą įvedus neteisingai SIM kortelė užsiblokuoja negrįžtamai.

SIM kortelėje saugoma mobilaus tinklo specifinė ir unikali informacija naudojama autentifikuoti ir identifikuoti abonentus tinkle. Svarbiausia iš jų yra ICCID, IMSI ir autentifikavimo raktas (Ki), vietos nustatymo identifikatorius (LAI) ir operatoriaus pagalbos centro numeris. SIM kortelėje tai pat saugoma kiti su konkrečiu tiekėju susiję duomenys, SMSC skaičius (Short message service center), paslaugų tiekėjo pavadinimas (SPN), paslaugos rinkimo numerius (SDN).

SIM kortelės gaminamos su įvairias atminties kiekiais nuo 32 KB iki 128 KB. Ši atmintis naudojama vartotojo kontaktams ir išorinių tinklo operatorių duomenims saugoti.

ICCID

Kiekviena SIM kortelė tarptautiniu mastu identifikuojama pagal ICCID (integrated circuit card identifier). ICCID yra saugomi SIM kortelės atmintyje ir tai pat yra išgraviruoti ar atspausdinti SIM kortelės išorėje. Jo išdėstymas pagrįstas ISO/IEC7812.E.118 standartu. ICCID yra iki 19 skaitmenų ilgio skaičius, įskaitant vieną kontrolinį skaitmenį, kuris apskaičiuojamas naudojant Luhn algoritmą. Tačiau ICCID ilgis yra apibrėžtas 10 baitų (20 skaitmenų) su operatoriaus specifine struktūra.

ICCID numeris susideda iš šių poskyrių:

(a) Išdavėjo numeris (IIN)- ne daugiau kaip septyni skaitmenys:
- Pramoninis identifikatorius, 2 fiksuoti skaitmenys, 89, telekomunikacijų tikslais
- Šalies kodas, 1-3 skaitmenys
- Išdavėjo (operatoriaus) kodas, 1-4 skaitmenys.

(b) Individualaus įrašo identifikatorius - jo ilgis yra kintamas, bet kiekvieno išdavėjo numerio skaičiai turės tokį pat ilgį.

(c) Kontrolinis skaitmuo - tai paskutinis skaitmuo apskaičiuojamas nuo kitų skaitmenų naudojant Luhn algoritmą

Tarptautinis judriojo ryšio abonento identifikatorius (IMSI)

SIM kortelė identifikuojama pagal kiekvieno operatoriaus tinklo unikalų tarptautinio judriojo ryšio identifikatorių (IMSI). Mobiliojo ryšio tinklo operatoriai naudodamiesi IMSI prisijungia mobilųjį telefoną prie savo teikiamų paslaugų.

IMSI formatas:

- Pirmieji trys skaitmenys sudaro mobiliojo ryšio operatoriaus šalies kodą (MCC).
- Sekantys du arba trys skaitmenys sudaro mobiliojo ryšio operatoriaus tinklo kodą (MNC).
- Kiti skaičiai rodo judriojo ryšio abonento identifikavimo numerį (MSIN). Paprastai būna 10 skaitmenų.

Autentifikacijos raktas (Ki)

Ki yra 128 bitų reikšmė autentifikuojanti SIM kortelę mobiliajame tinkle. Kiekviena SIM kortelė turi unikalų Ki priskirtą operatoriaus (tiekėjo) per personalizavimo procesą gamybos metu. Ki tai pat yra saugoma paslaugos tiekėjo duomenų bazėje.[13][14]

1.3 Šiuo metu egzistuojantys autentifikacijos mechanizmai su bluetooth

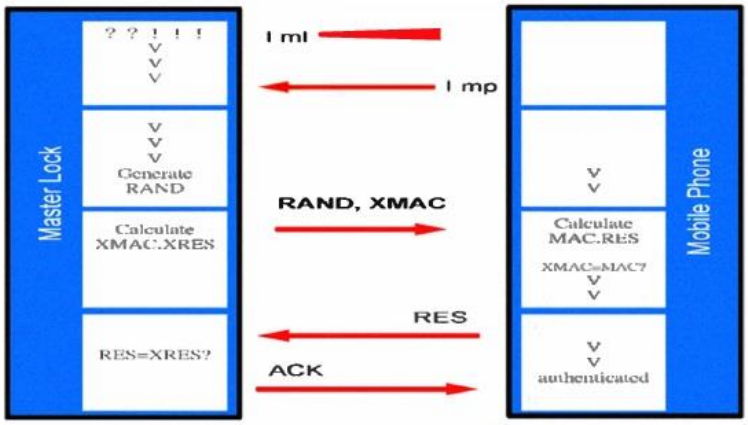
1.3.1 Sustiprinto saugumo praėjimo kontrolės modelis

Chia-Sheng Tsai ir Cheng-I Hung pristato praėjimo kontrolės modelį, kuris remiamasi bluetooth technologija. Šio modelio komponentai: praėjimo kontrolės įrenginys

su integruotu bluetooth siųstuvu/imtuvu. Vartotojas autentifikuojasi su savo turimu mobiliuoju įrenginiu.

Pasiūlyta vartotojo autentifikacija praėjimo kontrolės sistemoje, kuri remiasi simetriniu šifravimu. Simetrinis šifravimas buvo pasirinktas dėl to, kad šie algoritmai yra greitesni nei asimetrinio šifravimo algoritmai, o tai įtakoja mobiliojo įrenginio energijos suvartojimo sąnaudas. Duomenys perduodami sukuriant saugų duomenų perdavimo kanalą tarp abiejų komunikuojančių pusių.

Autentifikacijos protokolo schema pateikta 5 paveikslėlyje



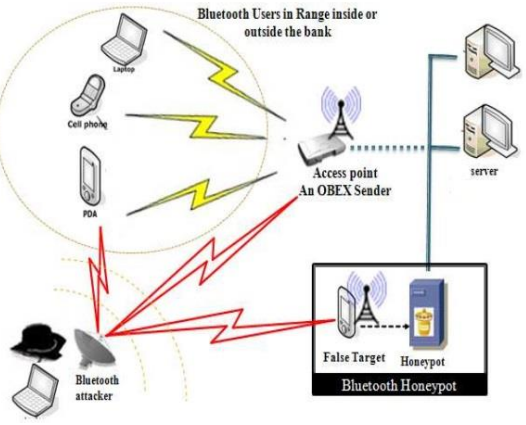
5 pav. Autorių Chia-Sheng Tsai ir Cheng-I Hung autentifikacijos modelis

Vartotojas identifikuojamas pagal iš anksto abiem pusėms žinomą simbolių seką - raktą. Vartotojo mobilus įrenginys siunčia prisistatymo žinutę „I mp“. Praėjimo kontrolės įrenginys atpažįsta vartotojo mobilųjį įrenginį ir išsiunčia užšifruotą vartotojo mobiliojo įrenginio bluetooth MAC adresą - xmac su atsitiktiniu skaičiumi - RAND. Vartotojo mobilus įrenginys gavęs šį paketą sulygina MAC adreso reikšmes ir jei reikšmės sutampa, siunčia RES paketą, kuriame užšifruotas slaptas raktas, praėjimo kontrolės įrenginiui. Praėjimo kontrolės įrenginys patikrinęs gautą reikšmę priima sprendimą ir siunčia sesijos nutraukimo pranešimą ACK.

Slaptus autentifikavimo duomenis siūloma saugoti mobiliojo telefono SIM kortelėje. Norint nuskaityti kortelės duomenis reikia įvesti kortelės PIN kodą. Siekiant išvengti vartotojo duomenų vagystės praėjimo kontrolės Bluetooth įrenginio veikimo diapazoną reikia sumažinti iki 2-3 metrų.[5]

1.3.2 Saugaus susijungimas pasinaudojant „medaus puodynės“ principu

K. Zolfaghar siūlo autentifikavimą vykdyti pasinaudojant medaus puodynės principu (angl. honeypot). Šiuo metodu autorius siūlo sukurti vieną ar daugiau netikrų prieigos taškų, kurie vykdytų visas autentifikavimo funkcijas, tik negalėtų manipuliuoti realiais sistemos duomenimis. Jie su bet kokiais duomenims autentifikuotų vartotoją ir taip sumažinanti įsilaužimo tikimybę į tikrąjį autentifikuojantįjį įrenginį taip sumažindami organizacijos nuostolius. Šio modelio koncepcinė schema pateikta 6 paveikslėlyje [6].



6 pav. sistemos panaudojant medaus puodynės koncepciją principinė schema [6]

1.3.3 Bluetooth autentifikacija panaudojant PIN kodą

Daugumos straipsnių autoriai siūlo atlikti autentifikavimą pasinaudojant Bluetooth standarte numatyta galimybe sukurti slaptą duomenų perdavimo kanalą, kuris sukuriamas abiem pusėms žinomo PIN kodo pagalba. [1][2][3][4][5][6]

M. Othman, W.H. Hassan ir A.H. Abdalla teigia, kad Bluetooth duomenų perdavimui sukuriamas kanalas nėra saugus dėl per trumpo PIN kodo. Ilgiausias galimas PIN kodas - 16 baitų ilgio ir dažniausia programiškai būna įprogramuota PIN kodas su reikšme 00000. Autentifikacijos mechanizmą siūloma vykdyti padidinant PIN kodo ilgį ir duomenis prieš perduodant užšifruoti.[2]

Outeirino, F.J.B.Siulo siūlo praėjimo kontrolės sistemą kuri paremta duomenų persiuntimo tunelio sugeneravimu pasinaudojant PIN kodu. Šis autorius siūlo sujungti bluetooth įrenginius sukuriant privatų bluetooth tinklą ir šį tinklą paslėpti nuo išorinio aptikimo, o šiame tinkle vartotoją autentifikuoti pagal MAC adresą. [1]

1.4 Skyriaus apibendrinimas

Šiame skyriuje išanalizuota bluetooth technologija. Yra sukurtos keturios bluetooth versijos. Autentifikavimo mechanizme tikslinga naudoti įrenginius palaikančius ketvirtąją bluetooth versiją. Apžvelgti mobiliajame įrenginyje saugomi duomenys su kuriais vartotojas gali būti identifikuotas ir autentifikuotas praėjimo kontrolės sistemoje. Autentifikavimui naudojami duomenys turi būti nesuklastojami arba sunkiai suklastojami.

Išanalizuoti kitų autorių siūlomi autentifikacijos mechanizmai. Dauguma autorių siūlo autentifikuoti vartotoją saugiu kanalu, kuriuo persiunčiamas duomenų paketas, pagal kurį bus atpažįstamas vartotojas.

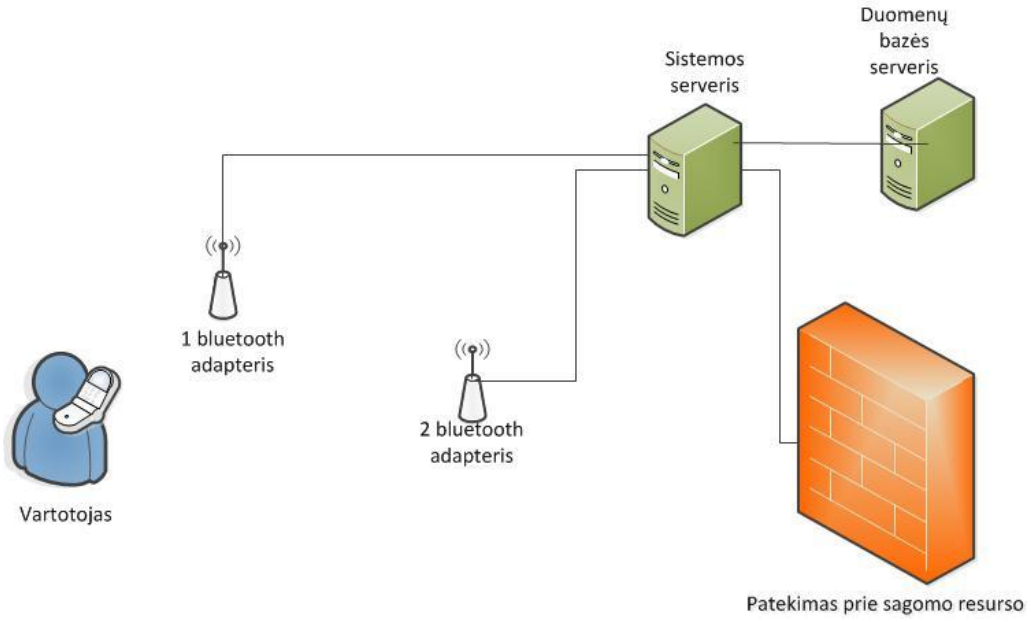
2 Projektinė dalis

Atlikus sistemoje naudojamų technologijų apžvalgą pastebėta, kad tai yra tobulinama technologija ir išleistos keturios bluetooth technologijos versijos. Pasaulyje labiausia paplitusi antroji versija, šios versijos trūkumas, kad duomenys perduodami nešifruoti, todėl naudoti šią versiją nėra visiškai saugu. Dėl šios priežasties identifikavimosi duomenys gali būti labai lengvai atskleisti, todėl šioje sistemoje būtų tikslinga naudoti ketvirtosios kartos Bluetooth technologiją palaikančius įrenginius. Ketvirtojoje Bluetooth versijoje įdiegta siunčiamų duomenų šifravimas bei papildomo kodo įvedimas pasinaudojant AES šifravimo standartą. Antrojoje versijoje norint saugiai persiųsti duomenis reikia įvesti apsaugos PIN kodą ir pagal šį kodą sugeneruojamas duomenų persiuntimo tunelis. Vartotojo autentifikavimui bus naudojamas modifikuotas Chia-Sheng Tsai ir Cheng-I Hung pasiūlytas sustiprintos saugos praėjimo kontrolės modelis. Vartotojo atpažinimui bus naudojama Bluetooth įrenginio unikalus MAC kodas, o autentifikacijai naudoti pasirinkti sunkiai suklastojami ar visiškai nesuklastojami duomenys, tokie kaip mobiliojo įrenginio IMEI kodas bei SIM kortelės vidiniai duomenys.

2.1 Sistemos loginė schema

Praėjimo kontrolės sistema susideda iš: dviejų išorinių Bluetooth prietaisų (esant reikalui jų skaičius gali didėti). Bluetooth įrenginiai sujungti su organizacijos parėjimo kontrolės serveriu. Bluetooth įrenginių pagalba serveryje esantis įdiegtas praėjimo kontrolės programos klientas komunikuos su vartotojo mobiliajame įrenginyje įdiegtu programinės įrangos klientu per bluetooth sąsają. Du ir daugiau bluetooth adapterių sistemai reikalingi norint nustatyti sistemos vartotojų tikslią judėjimo kryptį bei judėjimo laiką sekundžių tikslumu. Sistemos vizuali koncepcinė loginė schema pateikta 7 paveikslėlyje.

7 pav. Loginė sistemos schema



Serveryje, sujungtame su bluetooth adapteriais ir įdiegta klientine programine įranga, saugomi duomenys apie sistemos vartotojus bei jų mobiliajame įrenginį esančius sisteminius duomenis.

Vartotojo mobiliajame įrenginyje, turinčiame operacinę sistemą (pvz. android) įdiegta klientinė programinė įranga, kuri identifikuojasi serveryje ir serveriui paprašius su serverio atsiųsta žyma suformuoja autentifikacinį paketą.

Pirmasis Bluetooth adapteris reikalingas nustatyti vartotojo judėjimo krypčiai. Per šį Bluetooth adapterį duomenys nėra nei siunčiami, nei priimami. Jis veikia pasiklausymo rėžimu. Bet koks sesijos užmezgimas su šiuo įrenginiu kitiems išoriniams įrenginiams turi būti negalimas.

Antrasis Bluetooth adapteris atlieka visas sisteminiais funkcijas: identifikuoja ir autentifikuoja vartotoją, siunčia ir gauna duomenis. Įrenginys užmezga sesiją su kitais įrenginiais, siunčia vartotojui leidimą autentifikuotis, priima vartotojo siunčiamą autentifikacinį paketą.

2.2 Reikalavimų praėjimo kontrolės sistemai specifikacija

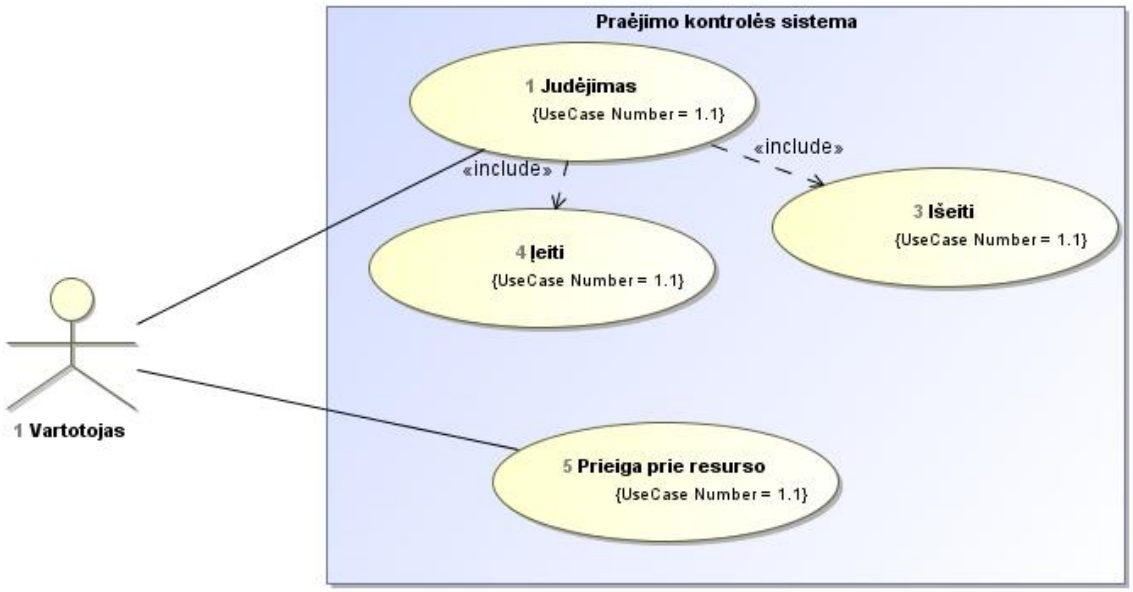
Sistemos paskirtis yra pagal organizacijos saugos politiką autentifikuoti vartotojus ir valdyti jų patekimą prie organizacijos saugomų resursų.

2.2.1 Sistemos vartotojų rolės

Toliau pateiktoje lentelėje (žiūrėti 3lentelę) nurodyta vartotojų rolės ir kas jiems suteikia leidimą patekti prie saugomų resursų. Vartotojai bus skirstomi į darbuotojų grupes. Neribojamą patekimą prie saugomų resursų turi organizacijos vadovybė, kuri ir suteikinės leidimus organizacijos darbuotojams ir svečiams. Svečias tai toks organizacijos vartotojas, kuris organizacijoje prie saugomų resursų gali prieiti labai ribotą laiko tarpą.

3 lentelė vartotojų rolės

Vartotojų rolės	Kas suteikia leidimą	Ribojimai patekimui prie resursų
Organizacijos vadovybė	-	-
Sistemos administratorius	Organizacijos vadovybė	Prieigos laikas gali būti ribojamas pagal organizacijos vadovybės nurodymus
Darbuotojai	Sistemos administratorius organizacijos vadovybei leidus	Priėjimas prie saugomų resursų tik darbo metu
Sargai	Sistemos administratorius organizacijos vadovybei leidus	Priėjimas prie saugomų resursų tik sargo darbo metu
Svečiai	Sistemos administratorius organizacijos vadovybei leidus	Tik numatytą laiko tarpą kuris numatytas organizacijos saugos politikoje



8 pav. Panaudojimų atvejų diagrama.

8 paveikslėlyje pavaizduota panaudojimų atvejų diagrama. Panaudojimų atvejų diagramoje esantis vartotojas vaizduoja bendrąsias organizacijos praėjimo kontrolės funkcijas.

2.2.2 Apribojimai sprendimui

- Sistemos kūrimui ir funkcionavimui turi visiškai pakakti atviro kodo programinės įrangos (teksto redaktoriai, kompiliatoriai, duomenų bazės ir t.t.), išskyrus tą programinę įrangą, kuri įsigyjama kartu su aparatine įranga ir be kurios aparatinė įranga negali veikti (tvarkyklės, įmontuotoji programinė įranga (angl. *firmware*), operacinė sistema ir t.t.).
- Sistema veiks su ne žemesne kaip bluetooth 2.0 versija.
- Serverio programinė įranga turi veikti UNIX/LINUX operacinėje aplinkoje.
- Sistema, kiek įmanoma turi greičiau aptarnauti organizacijos vartotoją.
- Sistemoje vartotojo duomenys turi būti saugomi atskirame serveryje.
- Galimybė sistemą išplėsti (prijungiant daugiau praėjimo punktų).
- Vartotojo mobiliajame įrenginyje turi būti atviro kodo operacinė sistema

2.2.3 Diegimo aplinka

- Sistema veiks Bluetooth technologijos pagrindu.
- Praėjimo kontrolės programinė įranga veiks UNIX/Linux operacinėje sistemoje.
- Programos kūrimui ir funkcionavimui naudojamos atviro kodo programinės įrangos, išskyrus tą programinę įrangą, kuri įsigyjama kartu su aparatine įranga ir be kurios aparatinė įranga negali veikti (tvarkyklės, įmontuotoji programinė įranga (angl. *firmware*), operacinė sistema ir t.t.)
- Naudojama duomenų bazių valdymo sistema- MySQL

- Vartotojo mobiliajame įrenginyje turi būti atviro kodo operacinė sistema

2.2.4 Numatoma sistemos darbo aplinka

- Organizacijos vartotojai naudodamiesi mobiliaisiais įrenginiais su įdiegta klientine programine įranga turėdami reikiamus leidimus galės patekti prie saugomų resursų.
- Sistema gali veikti tiek lauke tiek pastato viduje.
- Sistema gali būti integruojama į kitas sistemas.

2.2.5 Funkciniai ir nefunkciniai reikalavimai

Reikalavimai saugos politikai:

1) Saugos politika turi numatyti leidimų išdavimą prieigai prie saugomų resursų.
2) Saugos politika turi užtikrinti vartotojų turinčių leidimą patekimui prie saugomų resursų.
3) Saugos politikoje turi būti nurodyta, kad vartotojo atpažinimui naudojama jo mobiliojo telefono vidiniai duomenys.
4) Saugos politikoje turi būti nurodyta, kad leidimus suteikti ir atimti gali tik organizacijos vadovybė.
5) Saugumo politikoje turi būti nurodoma, kad sistemoje naudojami ir saugomi asmeniniai duomenys negali būti prieinami viešai.
6) Saugumo politikoje turi būti numatyta, kas gali prieiti prie sistemoje saugomų duomenų.
7) Saugos politikoje turi būti numatyta kad vartotojas negali pakeisti savo mobiliojo įrenginio PIN kodo prieš tai nesuderinęs su įmonės saugos administratoriumi.

Reikalavimai praėjimo kontrolės sistemai paremtai bluetooth technologija:

1) Praėjimo kontrolės sistema turi veikti pagal organizacijos saugos politiką.
2) Sistema turi veikti praėjimo kontrolės serveryje.
3) Sistema turi būti pritaikyta, kiek įmanoma labiau, sistemos plėtrai.
4) Sistema turi identifikuoti vartotoją pagal vartotojo mobiliojo įrenginio Bluetooth adapterio fizinį MAC adresą.
5) Sistema turi priimti sprendimą ar vartotojas gali patekti prie saugomų resursų.
6) Sistema nesulaukus vartotojo mobilaus įrenginio autentifikacijos paketo per 20 sekundžių po leidimo autentifikuotis privalo nutraukti aktyvią sesiją.
7) Praėjimo kontrolės sistema turi būti kiek įmanoma labiau pritaikyta kitų Bluetooth standarto versijų panaudojimui.

2.2.6 Bluetooth versijos parinkimas

Bluetooth antrosios versijos paplitimas nulėmė, kad kuriamam sistemos prototipe bus naudojama antroji Bluetooth versija. Nors ketvirtoji versijoje jau ir yra įdiegtas saugus perduodamų duomenų, bet ši versija dar nėra plačiai diegiama mobiliuosiuose įrenginiuose.

Naudojant antrosios versijos Bluetooth įrenginius prieš perduodant duomenis reikia sukurti saugų duomenų perdavimo kanalą kuris sukuriamas abejoms pusėms žinomu slaptu kodu.

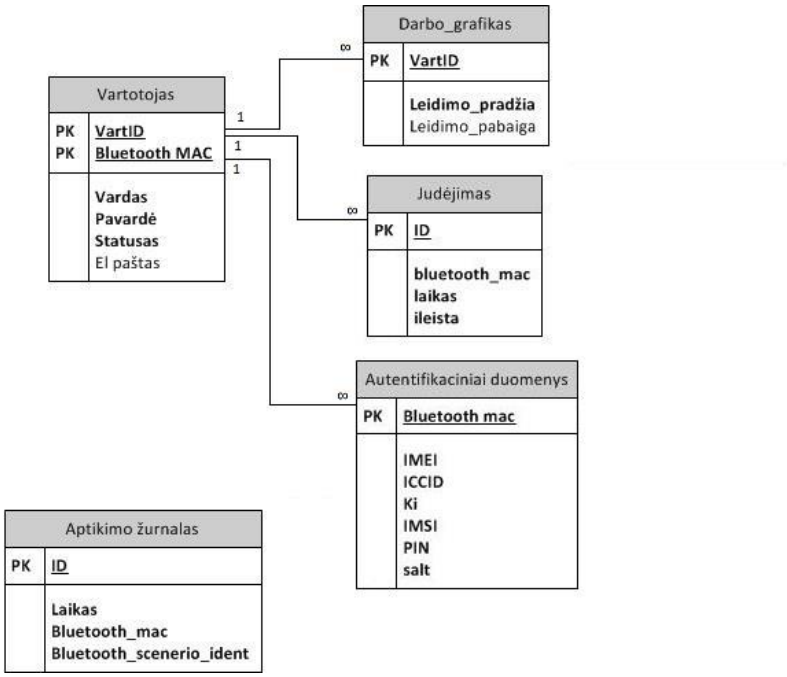
2.3 Duomenų struktūros

Praėjimo kontrolės korektiškam veikimui reikalingi tokie duomenys: informacija apie vartotoją (jo vardas, pavardė, ICCID ir pan.) informacija apie jam suteiktus leidimus (ar gali šiuo metu patekti prie saugomų resursų). Praėjimo kontrolės valdymo politikos gali būti išreiškiamos taisyklėmis, tokiomis kaip neįleisti vartotojo prie resurso švenčių dienomis.

Veiksmai, kuriuos gali atlikti vartotojai su duomenų bazės objektais - ištekliais, gali būti tokie: skaityti, rašyti, spausdinti, kopijuoti, vykdyti ir panašiai. Vieno objekto ir veiksmo, kurį gali atlikti su tuo objektu, kombinacija gali būti pavadinta leidimu. Norint realizuoti praėjimo kontrolės valdymą, tokį leidimą ar analogiškų leidimų sąrašą galima priskirti vartotojui. Objektų ir veiksmų, kuriuos galima atlikti su jais, analizavimas nėra šio darbo tikslas, todėl detaliau analizuojami duomenys susiję su sistemos vartotojais ir praėjimo kontrole.

Duomenų bazės loginėje schemoje pateiktoje 9 paveikslėlyje matyti duomenų bazės lentelės reikalingos praėjimo kontrolės sistemai funkcionuoti. Sistemai yra svarbu suregistruoti visus patenkančius prie saugomo resurso vartotojus ir visus aptiktus Bluetooth įrenginius su bet kuriuo įrenginiu turinčiu Bluetooth.

Įrašai apie aptiktus Bluetooth įrenginius saugomi duomenų bazės lentelėje ir negali būti modifikuojami praėjimo sistemos kontrolės vartotojų. Jie saugomi lentelėje Aptikimo_žurnalas. Lentelėje Darbo_grafikas saugomi vartotojui suteikiami leidimai ir laiko limitai, kuriuos jis gali praleisti prie saugomo resurso. Lentelėje Judėjimas saugomi įrašai apie vartotojo praėjimą pro praėjimo kontrolės daviklius - Bluetooth įrenginius. Lentelėje Autentifikaciniai_duomenys saugomi duomenys apie kiekvieno vartotojo individuliai turimus unikalius duomenis, kurie privalo būti unikalūs. Lentelėje vartotojas saugomi duomenys apie vartotoją: vardas, pavardė bei identifikatorius - Bluetooth MAC adresas.



9 pav. duomenų bazės loginė schema

2.4 Saugos politika

Šiame skyrelyje aptarta praėjimo kontrolės sistemos Bluetooth technologijos pagrindu saugos politika, pagal kurią ir veiks sistema.

Norint sukurti saugos politiką, reikia identifikuoti visas reikalingas sistemos veikimui rolių schemas ir roles. Nurodyti kada ir kurią rolę turintis vartotojas gali patekti prie saugomų resursų. Skirtingoms rolėms ir rolių schemoms reikia priskirti skirtingus leidimų sąrašus. Vartotojų rolių sąrašas pateiktas 4 lentelėje.

4 lentelė vartotojų patekimo laikas prie saugomo resurso pagal rolių sąrašą

Vartotojų rolės	Patekimo prie resursų laikas
Organizacijos vadovybė	Neribojamas
Sistemos administratorius	Prieigos laikas gali būti ribojamas pagal organizacijos vadovybės nurodymus
Darbuotojai	Priėjimas prie saugomų resursų tik darbo metu
Sargai	Priėjimas prie saugomų resursų tik sargo darbo metu
Svečiai	Tik numatytą laiko tarpą, kuris numatytas organizacijos saugos politikoje

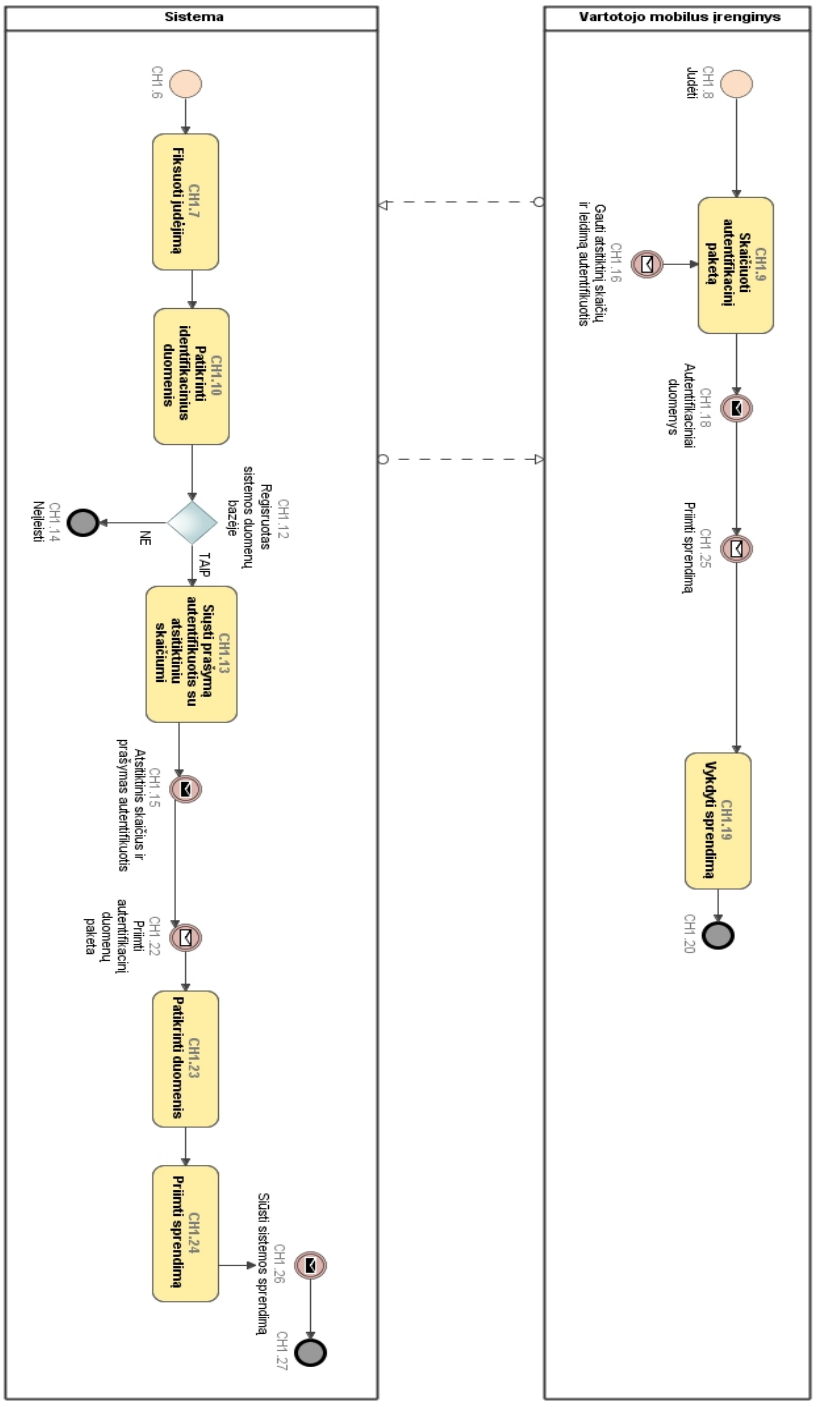
Kiekvienam vartotojui ar vartotojų grupei turi būti numatyta priskirti bendri patekimo laikai pagal organizacijos vadovybės nurodymus.

10 pav. organizacijos hierarchija

Organizacijos vadovybė turi didžiausias teises bei leidimus patekti prie saugomų resursų. Organizacijos hierarchija pateikta 10 paveikslėlyje. Sistemos administratorius pagal organizacijos valdybos liepimą suteikia vartotojui ar grupei reikalingus leidimus.

Organizacijos vadovybė kartu su sistemos administratoriumi turi numatyti per kiek laiko sistemos vartotojas turi autentifikuotis. Autentifikavimasis negali užtrukti ilgiau nei 20 sekundžių.

2.5 Sistemos veikimo logika



11 pav. Sistemos veiklos schema

Aukščiau pateiktoje schemoje (11 pav.) pavaizduotos sistemos veiklos, kurias būtina atlikti, kad sistemoje būtų pasiektas norimas rezultatas - saugomi resursai. Šią veiklą inicijuoja vartotojas su savo mobiliuoju įrenginiu, patekęs į antrojo Bluetooth įrenginio aprėpties zoną.

2.6 Sistemos vartotojo atpažinimas

Sistemos vartotojas atpažįstamas pagal jo mobiliajame įrenginyje esančio Bluetooth įrenginio MAC adresą. MAC adresas yra skelbiamas visiems įrenginiams, kurie yra Bluetooth tinklo pasiklausymo rėžime. Sistemos serveris aptikęs registruotą, su teise patekti prie saugomų resursų, mobilųjį įrenginį, užmezga sesiją ir atsiunčia atsitiktinę skaičių seką su nuoroda autentifikacijai sistemoje. Mobilusis įrenginys gavęs atsitiktinę skaičių seką suformuoja identifikacinį paketą kurį išsiunčia sistemos serveriui. Serveris sulygina duomenis su saugomais duomenimis duomenų saugykloje. Jai duomenys sutampa, vartotojas įleidžiamas prie saugomų resursų.

2.7 Identifikacinio paketo duomenų formavimas

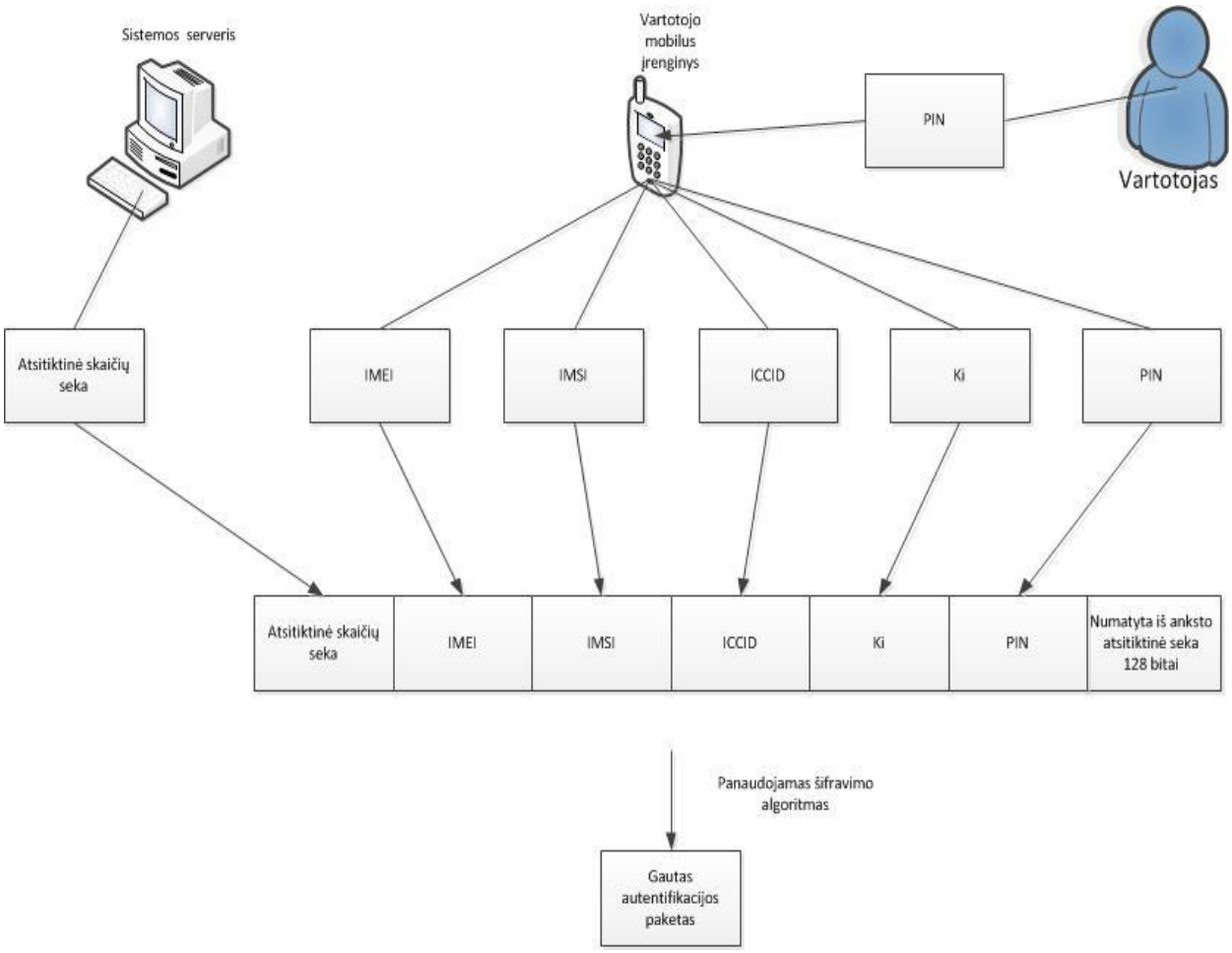
Visi duomenys reikalingi formuoti identifikaciniam paketui saugomo vartotojo mobiliajame įrenginyje. Įvedami vartotojui įjungus mobilųjį įrenginį ir sugeneruojami realiu laiku praėjimo kontrolės sistemos serveryje. Likę duomenys saugomi mobiliajame įrenginyje ir sistemos duomenų bazės serveryje.

Serveriui užmezgus sesiją su mobiliuoju įrenginiu ir leidus identifikuotis, vartotojo mobilusis įrenginys gauna atsitiktinę skaičių reikšmę, kurią sugeneruoja sistemos serveris. Gavęs šią reikšmę, vartotojo mobilus įrenginys surenka reikiamus duomenis identifikaciniam paketui suformuoti.

Identifikaciniam paketui suformuoti naudojami vidiniai mobilaus įrenginio duomenys:

- Mobiliojo įrenginio IMEI kodas.
- SIM kortelės vidiniai duomenys:
  - IMSI- tarptautinis judriojo ryšio identifikatorius.
  - ICCID- SIM kortelės tarptautinis unikalus numeris.
  - Ki- unikalus autentifikacijos raktas priskirtas mobilų paslaugų operatoriaus.
  - PIN- Kodas kurį įvedą vartotojas norėdamas prieiti prie SIM kortelėje saugomų duomenų.
- Atsitiktinė simbolių seka 128 bitų ilgio, kuri kiekvienam vartotojo mobiliam įrenginiui yra unikali ir įdiegiama iš anksto į SIM kortelės atmintį, vartotojo registracijos praėjimo kontrolės sistemoje metu. Taip siekiama pasunkinti užšifruotų duomenų atstatymą nežinant šifravimo algoritmo.

Identifikacinio duomenų paketo formavimas pateiktas 12 paveikslėlyje.

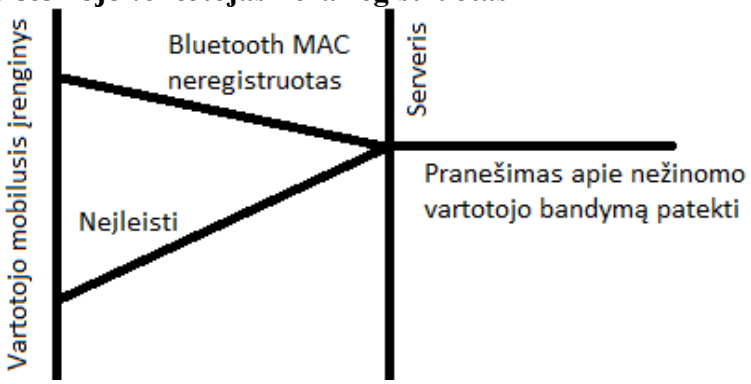


12 pav. identifikacinio duomenų paketo formavimas

Iš visų duomenų suformuojamas vienas paketas ir užšifruojamas panaudojus simetrinį šifravimo algoritmą. Simetrinis šifravimo algoritmas pasirinktas dėl šio algoritmo greitaveikos, tai įtakoja mobiliojo įrenginio energijos suvartojimą. Serveryje saugomi visi duomenys identiški esantiems mobiliajame įrenginyje. Visi skaičiavimai atliekami mobiliajame įrenginyje ir organizacijos praėjimo kontrolės sistemos serveryje.

2.8 Galimi sistemos veikimo scenarijai

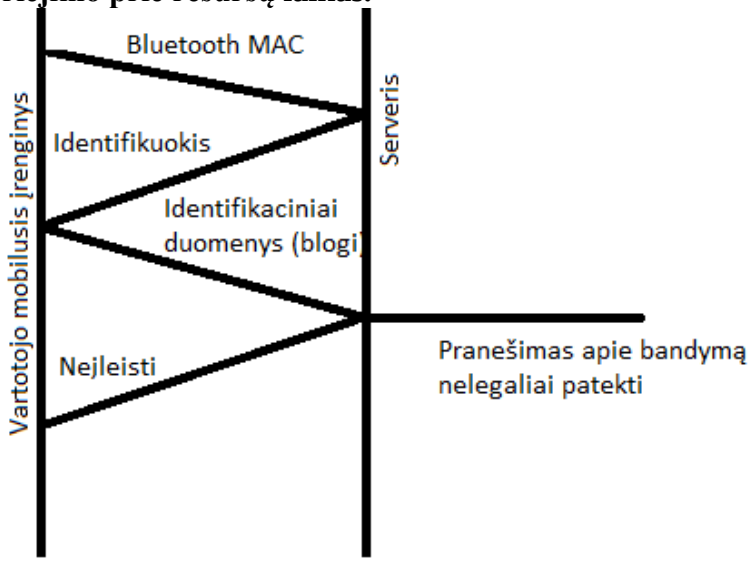
Sistemoje vartotojas nėra registruotas



13 pav. Scenarijus kai sistemoje vartotojas nėra registruotas

Šis scenarijus (13 pav.) parodo, kad nebus įleidžiamas vartotojas, kuris nėra registruotas sistemoje. Iš jo nebus prašoma, kad jis atsiųstų savo identifikacinius duomenis ir taip neapsunkins serverio darbo ir neapkraus nereikalingais duomenimis. Neįleidus - neužmezgama aktyvi sesija, kurios metu klientas serveriui pateikia autentifikacinius duomenis. Siekiant sumažinti įsilaužimo į sistemą galimybes tuo pačiu Bluetooth MAC adresu galima autentifikuotis tik po tam tikro laiko, kuris privalo būti numatytas organizacijos saugos politikoje.

Sistemoje yra registruotas, bet neidentifikuotas vartotojas arba pasibaigęs jo priėjimo prie resursų laikas.



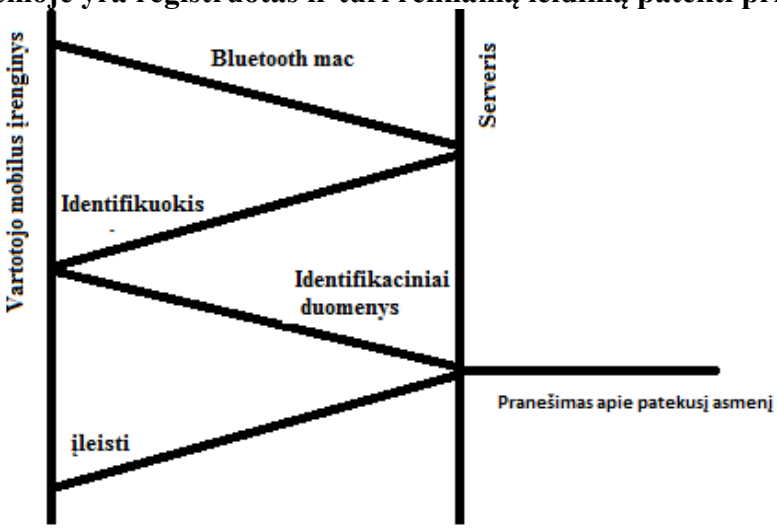
14 pav. Scenarijus kai klientas negali identifikuotis sistemoje

Scenarijaus iliustracijoje (14 pav.) vaizduojama, kai klientas bando prisijungti prie sistemos žinodamas registruoto vartotojo Bluetooth MAC adresą, bet neturi ar nežino vartotojo identifikacinių duomenų paketo turinio. Serveris gavęs vartotojo autentifikacijos duomenis paprašo vartotojo mobilaus įrenginio identifikuotis. To jam nepavykus atlikti sistemos administratoriui (prižiūrinčiam asmeniui kuris saugo resursą) sugeneruojamas

pavojaus pranešimas apie neteisėtą mėginimą patekti, o vartotojo mobiliam įrenginiui nusiunčiamas klaidos pranešimas, kad patekimas nėra galimas. Siekiant sumažinti identifikacinio paketo sugeneravimo galimybes ir įsilaužimo į sistemą galimybes tuo pačiu Bluetooth MAC adresu galima autentifikuotis tik po numatyto laiko tarpo, kuris privalo būti numatytas organizacijos saugos politikoje.

Per 20 sekundžių mobiliajam įrenginiui neatsiuntus autentifikacinio paketo, vartotojo mobiliam įrenginiui atsiunčiamas klaidos pranešimas ir vartotojas neįleidžiamas. Toks pat scenarijus galioja ir vartotojui turinčiam pasibaigusį priėjimo prie saugomų resursų laiko limitą ar leidimą.

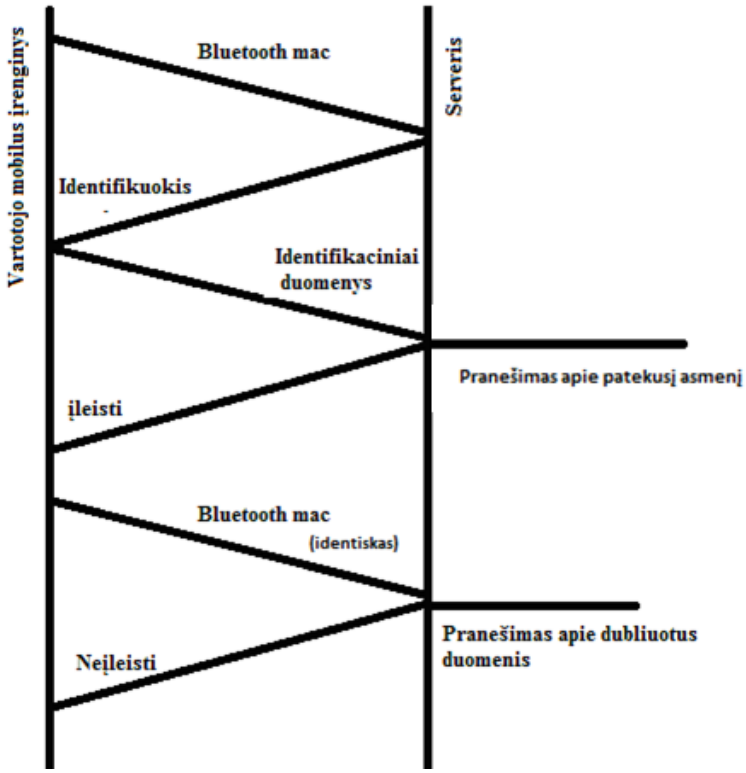
Sistemoje yra registruotas ir turi reikiamą leidimą patekti prie saugomo resurso



15 pav. Scenarijus kai klientas autentifikuojasi ir identifikuojasi

Scenarijaus iliustracijoje (15 pav.) vaizduojama, kai klientas bando prisijungti prie sistemos turėdamas registruoto vartotojo Bluetooth MAC adresą, turi visus teisingus reikiamus identifikacijos duomenis ir sėkmingai gali patekti prie saugomų resursų.

Scenarijus kai bando patekti antras vartotojas su tokiais pat autentifikaciniais duomenimis



16 pav. Scenarijus kai bando patekti vartotojas jau esantis viduje

Atsitikus 16 pav. pateiktam scenarijui atsakingas žmogus už resursų apsaugą turi atitinkamai sureaguoti ir išsiaiškinti, ar tai tikrai bandymas patekti prie resursų ne savais duomenimis, ar jau įvyko draudžiamas veiksmas ir įsilaužėlis viduje, o prie užkardos sulaikytas tikrasis asmuo turintis visus tai patvirtinančius duomenis. Šiuo atveju atsakingas žmogus turi priimti tam tikrą sprendimą, kuris leistų išspręsti atitinkamą problemą. Sprendimas turi atnešti mažiausia žalos saugomiems resursams.

Šiuo atveju sistema pirmą kartą prižiūrėtojui sugeneruoja teisingą pranešimą. O antrą kartą, kai įvyksta bandymas patekti į sistemą tais pačiais duomenimis, gaunamas klaidos pranešimas apie neteisėtą bandymą patekti į sistemą.

Visais atvejais serveris leisdamas autentifikuotis vartotojui atsiunčia atsitiktinį skaičių – žymą, kurią mobilusis įrenginys privalo panaudoti formuojant identifikacinį paketą prieš autentifikuodamasis praėjimo kontrolės serveryje.

2.9 Vartotojo judėjimo krypties nustatymas

Sistemos vartotojo krypties nustatymui naudojami Bluetooth priedėlio užfiksuojamas vartotojo patekimas į pirmo ar antro Bluetooth priedėlio veikimo zoną. Pagal laiko skirtumą nustatoma vartotojo judėjimo kryptis.

Judėjimo kryptis apskaičiuojama, kai abu Bluetooth priedėliai aptinka tą patį mobilųjį įrenginį trumpo laiko bėgyje. Apskaičiuojama iš antrojo Bluetooth priedėlio užfiksuoto patekimo į jo zoną laiką atimant į pirmojo Bluetooth priedėlio patekimo zoną

laiką. Jai laiko skirtumo reikšmė yra teigiama vartotojas pateko prie saugomo resurso, jai neigiama - vartotojas pasišalino nuo saugomų resursų.

2.10 Autentifikacinių duomenų saugojimas mobiliajame įrenginyje

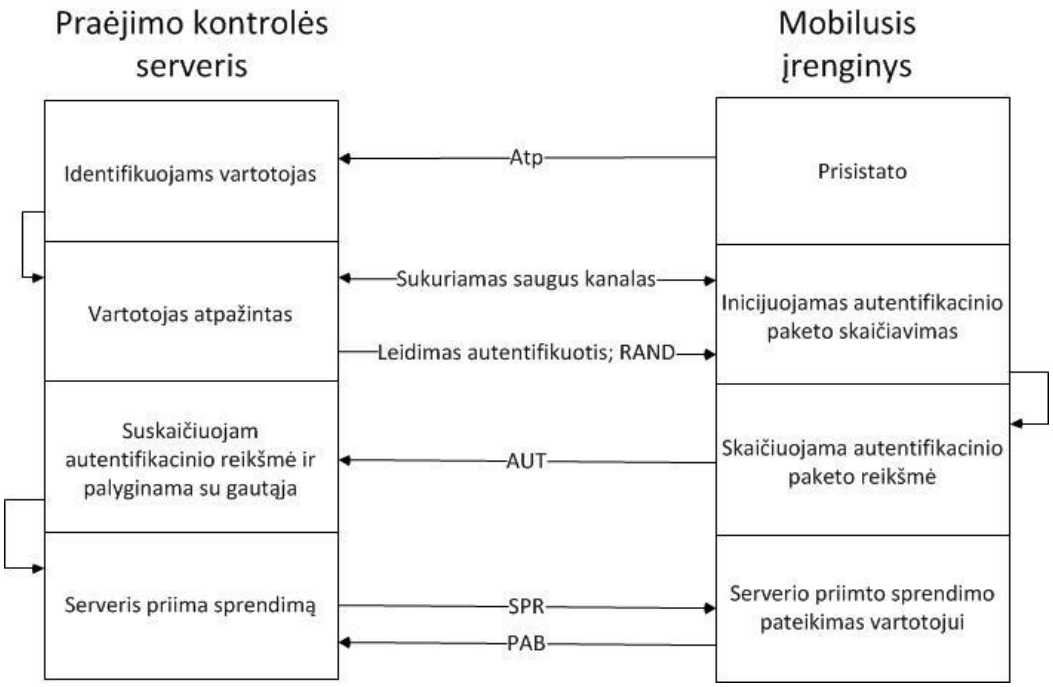
Siekiant sumažinti autentifikacinių duomenų vagystę, dalį programinės įrangos kodo ir reikalingas reikšmes, kurios skirtos skaičiuoti autentifikaciniams paketams, saugoti naudojama mobiliojo įrenginio SIM kortelė. SIM kortelėje esantys duomenys pasiekiami tik mobiliojo įrenginio savininkui suvedus SIM kortelės PIN kodą.

2.11 Papildoma sauga siekiant išvengti duomenų vagystės

Siekiant sumažinti autentifikacinių duomenų vagystės galimybes duomenų perdavimo metu, yra tikslinga sumažinti autentifikacijai naudojamo Bluetooth priedėlio veikimo atstumą iki 1-2 metrų. Visi autentifikaciniai duomenys privalo būti perduodami tik sugeneruotu saugiu kanalu.

2.12 Projektuojamos sistemos architektūra

17 paveikslėlyje pavaizduota projektuojamos praėjimo kontrolės sistemos autentifikacijos modulio autentifikavimosi protokolas. Vartotojo mobiliojo įrenginio patekimas į praėjimo kontrolės serverio Bluetooth veikimo zoną inicijuoja serverio darbą. Vartotojo mobilusis pasiskelbia kas jis toks ir nusiunčia Atp pranešimą serveriui. Atp pranešime yra mobiliojo įrenginio Bluetooth MAC adresas. Serveriui atpažinus mobilųjį įrenginį pagal Bluetooth MAc adresą, serveris inicijuoja saugaus duomenų perdavimo kanalo sukūrimą. Kai sukurtas saugus duomenų perdavimo kanalas serveris nusiunčia žymę apie leidimą autentifikuotis ir atsitiktinį skaičių seką RAND. Vartotojo mobilus įrenginys gavęs leidimą ir atsitiktinių skaičių seką pradeda skaičiuoti autentifikacinio paketo reikšmę (autentifikacinio paketo skaičiavimo metodas pateiktas ankstesniuose skyriuose). Suskaičiavęs autentifikacinio paketo reikšmę vartotojo mobilusis įrenginys pasiunčia pranešimą AUT serveriui su jau suskaičiuota autentifikacine paketo reikšme. Serveris gavęs AUT pranešimą suskaičiuoja SAUT autentifikacinę reikšmę iš turimų duomenų bazės vartotojo duomenų. Abi reikšmes palygina ir priima sprendimą. Priimtą sprendimą nusiunčia vartotojo mobiliajam įrenginiui pranešimu SPR. Kai vartotojo mobilus įrenginys gauna pranešimą SPR su serverio sprendimu, tada vartotojo mobilusis įrenginys inicijuoja saugaus kanalo sunaikinimą. Jai šio veiksmo neatlieka mobilusis įrenginys serveris saugų kanalą sunaikina po 10 sekundžių po SPR pranešimo.



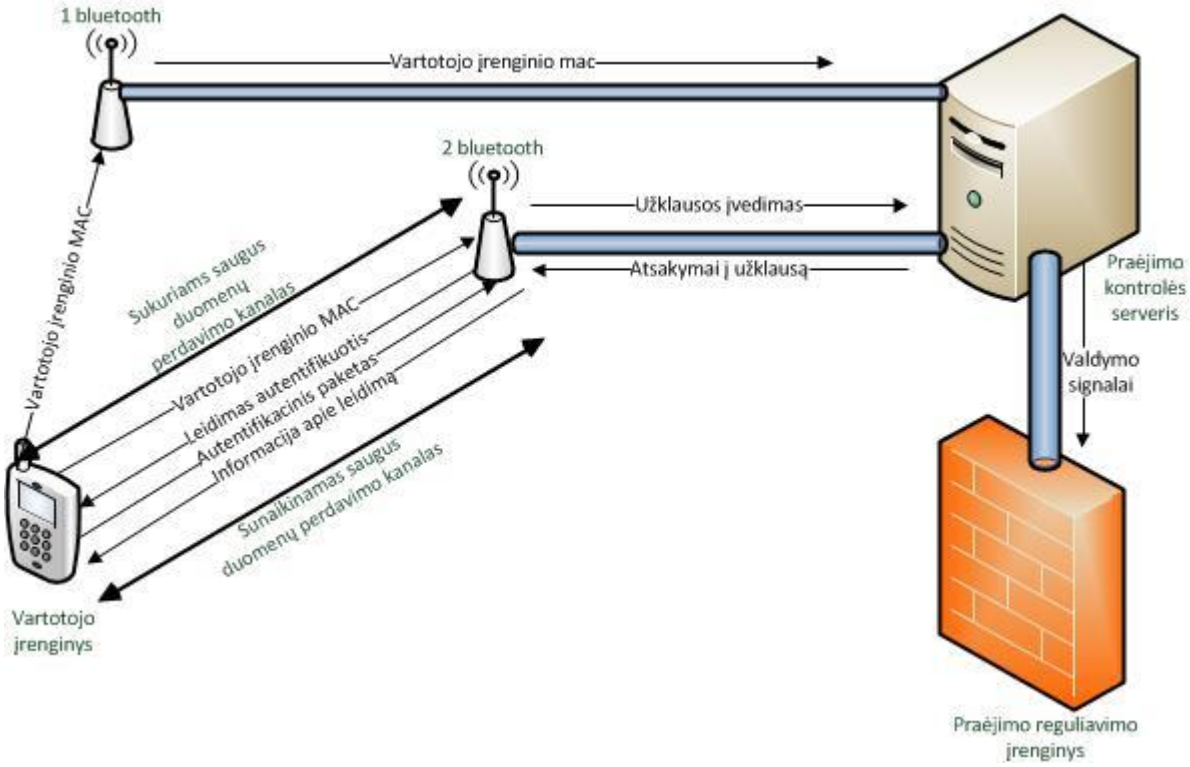
17 pav. pasiūlytas autentifikavimosi protokolas

Praėjimo kontrolės sistemoje siekiant išvengti duomenų atspėjimo, reikia apriboti autentifikavimosi praėjimo kontrolės sistemoje kartus. Tris kartus neteisingai pateikti duomenys vartotojui neleidžiama autentifikuotis su tuo pačiu Bluetooth MAC adresu penkias valandas.

18 paveikslėlyje pavaizduota projektuojamos sistemos architektūra. Kaip parodyta, vartotojas norėdamas patekti prie saugomų išteklių, turi gauti leidimą iš praėjimo kontrolės serverio. Bluetooth įrenginiai veikia tik kaip tarpininkai tarp vartotojo ir praėjimo kontrolės serverio. Praėjimo kontrolės serveris turi įvertinti ar vartotoją įleisti prie saugomo resurso.

Autentifikacijos metu praėjimo kontrolės serveris bendru atveju patikrina ir kitus vartotojo duomenis nusakančius jo tapatybę. Viską įvertinęs pagal saugos politikas, praėjimo kontrolės serveris priima sprendimą dėl patekimo prie saugomų resursų ir grąžina vartotojui atsakymą. Autentifikavimo algoritmas pateiktas 3.8 pav.

Praėjimo kontrolės serveris autentifikuoja vartotoją tik tuomet jai jo turimo mobilaus įrenginio Bluetooth yra aktyvus ir Bluetooth MAC yra serverio duomenų bazėje. Jei anksčiau paminėtus požymius turi vartotojo mobilus įrenginys, praėjimo kontrolės serveris Bluetooth sąsaja atsiunčia į vartotojo mobilųjį įrenginį atsitiktinę skaičių seką su leidimu autentifikuotis serveryje. Siekiant sumažinti vartojo duomenų atskleidimą atsitiktinė skaičių sekas galioja 20 sekundžių nuo išsiuntimo vartotojui. Vartotojo mobilus įrenginys suskaičiavęs autentifikacinę reikšmę perduoda praėjimo kontrolės serveriui, kuris patikrinęs paketą bei įvertinęs jam pateiktas organizacijos saugos politikos taisykles, priima sprendimą ar įleisti vartotoją prie saugomų resursų. Vienam vartotojui gali būti priskirtas tik viena saugos politikos taisyklė.



18 pav. projektuojamos sistemos architektūra

Autentifikacijos ir politikų vykdymo moduliai skaito duomenis iš duomenų bazės, kurioje saugoma informacija apie visus vartotojus, jų turimus autentifikacinius duomenis, priskirtas roles bei leidimus, kuriuos vartotojai turi.

Vienu metu sistema gali aptarnauti iki 7 vartotojų. Likusieji vartotojai sustatomi į eilę ir autentifikuojami eilės principu. Siekiant padidinti aptarnaujamų vartotojų greitį būtų tikslinga papildomai prijungti Bluetooth priedėlių, kurie esant maksimaliam susijungimų skaičiui prie vieno Bluetooth priedėlio aktyvuotųsi ir aptarnautų vartotojus, kurie bando patekti prie saugomų resursų.

2.13 Panaudotos techninės ir programinės įrangos specifikacija

Tyrimo sistemos kūrimui buvo panaudota atviro kodo programinė įranga. Buvo suprojektuotas praėjimo kontrolės valdymo serveris ir paleistas kompiuteryje su Linux Ubuntu operacine sistema. Serverio programa parašyta python ir java programavimo kalbomis. Kliento mobiliajame įrenginyje diegiama programinė įranga suprogramuota panaudojant JAVA programavimo kalbą. Serveris sukonfigūruotas taip, kad reikalingus duomenis apie vartotoją: autentifikacinius duomenis, roles bei leidimus gautų iš MySQL duomenų bazės. Taip pat vestų praėjimo kontrolės sistemos istoriją ir atliktų atitinkamus įrašus MySQL duomenų bazėje.

Suprojektuotą sistemą sudaro praėjimo kontrolės serverio funkcijas imituojanti programa ir sąsajai su vartotoju skirta klientinė programa diegiama virtualiame bei realiame mobiliajame įrenginyje.

2.14 Skyriaus apibendrinimas

Buvo pasiūlytas praėjimo kontrolės sistemos su Bluetooth technologija autentifikacijos modelis. Modelis nuo siūlomų kitų autorių modelių skiriasi tuo, kad yra papildytas sunkiai arba nesuklastojamomis autentifikacijos žymomis. Pagal pasiūlytą modelį buvo suprojektuota praėjimo kontrolės sistema. Suprojektuotas ir įdiegtas praėjimo kontrolės autentifikacijos mechanizmas. Suprojektuota sistema buvo išbandyta sukūrus serverio ir kliento programas imituojančias vartotojo praėjimą pro praėjimo kontrolę. Praėjimo kontrolės sistema fiksuoja vartotojo judėjimo kryptį ir įvykio laiką.

Bandymų metu nustatyta, kad praėjimo kontrolės serveris veikia gerai, teisingai atpažįsta vartotojus bei juos autentifikuoja. Neįleidžia bei neprašo autentifikuotis vartotojų, kurių Bluetooth MAC nėra įtraukti į praėjimo sistemos kontrolės serverio duomenų bazę.

3 Sistemos testavimas ir eksperimentiniai tyrimai

Praėjimo kontrolės sistemoje labai svarbi sistemos veikimo greitaveika. Sistema turi veikti taip, kad vartotojas nepajustų kaip jis yra identifikuojamas ir autentifikuojamas. Dėl šios priežasties praėjimo kontrolės sistema vartotoją privalo autentifikuoti kaip galima greičiau. Eksperimentų metu buvo tiriama pasiūlytos sistemos greitaveika ir serverio resursų naudojimas esant skirtingiems vartotojų kiekiams. Eksperimentinė sistema ištestuota pagal numatytus sistemos veikimo scenarijus. Sistema veikia korektiškai.

3.1 Eksperimentų metu panaudota techninė ir programinė įranga

Testavimams ir eksperimentiniams tyrimams buvo panaudota sistema su intel core duo E8400 3,0 GHz CPU, 512 MB RAM virtualiu kompiuteriu (įdiegtas naudojant VMware Workstation virtualizacijos aplinką) su Linux Ubuntu operacine sistema. Eksperimentinių tyrimų metu buvo paleidžiamos specialiai šiems tyrimams parašytos programos, padedančios valdyti serverinės pusės darbą bei vartotojų aptarnavimą bei apdoroti eksperimentų rezultatus.

Testavimams ir eksperimentiniams tyrimams buvo panaudota mobiliuose įrenginiuose įdiegta programinė įranga realizuota virtualiame mobiliajame įrenginyje su 1,2 GHz CPU ir 512 MB RAM su Android 4.0 operacine sistema ir realiame mobiliajame įrenginyje su 1,2GHz CPU bei 512 MB RAM su Android 4.0.

Vartotojų judėjimui fiksuoti panaudota du Bluetooth adapteriai palaikantys Bluetooth antrąją kartą.

Eksperimento pradžioje duomenų bazėje buvo sukurta 30 skirtingų įrašų apie vartotojus ir jų turimus identifikacinius duomenis bei priskirtus leidimus patekti į patalpą. Mobiliuosiuose įrenginiuose įdiegtoje programinėje įrangoje įdiegti analogiški saugomi duomenys duomenų bazėje apie vartotoją.

3.2 Eksperimentų eiga

Pirmo eksperimento metu buvo tiriama, per kiek laiko aptarnaujama vienu metu priimamos vartotojų užklausos. Vartotojo mobilaus įrenginio simuliatorius paleidžiamas daug kartų tuo pačiu metu (tai atlieka komanda ./emulator –avd vartojomobilus & ./emulator –avd vartojomobilus & ./emulator –avd vartojomobilus ...), tai turėtų atitikti vartotojų kreipimąsi į praėjimo kontrolės serverį. Mobilieji įrenginiai autentifikuojami per

vieną Bluetooth priedėlį eilės tvarka: kada pasikreipė į praėjimo kontrolės serverį. Pirmiau pasikreipęs vartotojas bus autentifikuotas greičiau, nei vartotojas pasikreipęs po tam tikro laiko tarpo.

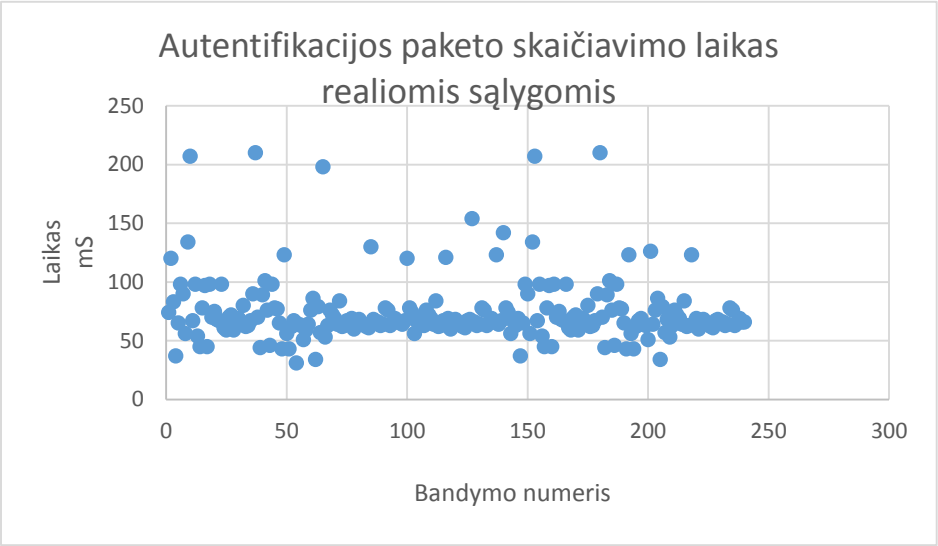
Šiuo eksperimentu buvo tikrinama, per kiek laiko iš anksto numatytas vartotojų skaičius bus aptarnautas vienu metu. Tyrimo rezultatai surašyti 5 lentelėje. Lentelės stulpelyje „visi klientai“ nurodyta per kiek vidutiniškai laiko aptarnaujami klientai. Stulpelyje „vienas klientas“ nurodyta per kiek laiko vidutiniškai aptarnaujamas vienas praėjimo kontrolės sistemos vartotojas atskirai. Iš šios lentelės galime pamatyti kiek laiko vidutiniškai gali užtrukti vartotojo aptarnavimas bandant patekti prie saugomo resurso, priklausomai nuo vienu metu bandančių patekti vartotojų. Šio eksperimento metu mobilieji įrenginiai veikė idealiomis sąlygomis (t.y. nebuvo įvertinamos mobiliojo įrenginio apkrovos esant skambučiui ar naudojantis kitomis mobiliojo įrenginio funkcijomis). 5 lentelėje laikas nurodomas sekundėmis.

5 Lentelė Klientų autentifikavimo laikas

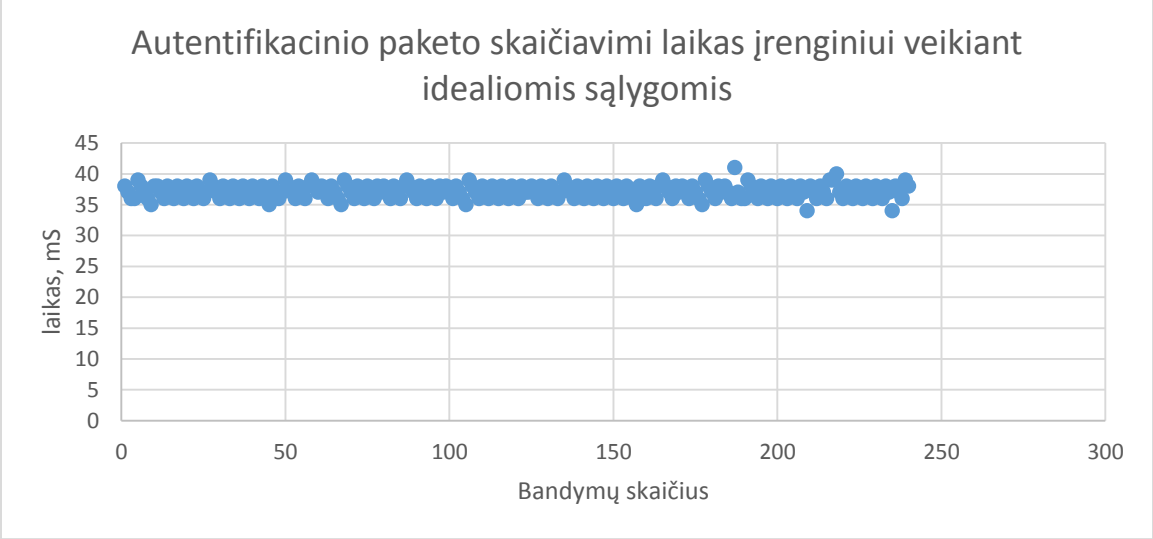
Vartotojų mobiliųjų įrenginių skaičius	**Aptarnavimo trukmė, s**	
	Visi klientai	**Vienas klientas**
1	0,42	<1
5	0,93	<1
7	1,1	<1
10	3,3	<1
50	5,2	<1
100	13,3	<1
200	24,7	<1
500	61,7	<1
1000	126,4	<1

Antro tyrimo metu tiriama, per kiek laiko realus mobilusis įrenginys, veikiant įvairiais darbo režimais suskaičiuos identifikacinio paketo reikšmę. Tai pat buvo tiriamas virtualus mobilus įrenginys, kuris veikė idealiomis sąlygomis, ir su juo nebuvo atliekami jokie pašaliniai veiksmai, pavyzdžiui, skambutis, trumpoji tekstinė žinutė ar kita. Kliento programa buvo paleidžiama daug kartų esant įvairioms mobiliojo įrenginio apkrovoms (esant skambučiui, siunčiant trumpąją tekstinę žinutę, naudojantis išmaniojo įrenginio funkcijomis). Tyrimo metu buvo išmatuotas kliento autentifikavimosi paketo skaičiavimo laikas. 19 paveikslėlyje pateikta 240 kartų atsitiktinių bandymų laiko reikšmės esant įvairioms sąlygoms. Bandymų metu pastebėta, kad ilgiausia skaičiavimus atlieka, kai

naudojamasi išmaniojo įrenginio funkcijomis. Išmaniajam įrenginiui būnant budėjimo rėžime skaičiavimo laikas trunka nuo 50 iki 70 ms.



19 pav. autentifikacinio paketo skaičiavimo mobiliajame įrenginyje, veikiančiame realiomis sąlygomis, laiko pasiskirstymas



20 pav. autentifikacinio paketo skaičiavimo mobiliajame įrenginyje, veikiančiame idealiomis sąlygomis, laiko pasiskirstymas

Įrenginiui veikiant idealiomis sąlygomis gauti rezultatai parodė, kad vidutiniškai įrenginys suskaičiuoja autentifikacinio paketo reikšmę per 36,5 mS.

Trečio eksperimento metu buvo tiriama serverio resursų išnaudojimas praėjimo kontrolės sistemoje su skirtingu skaičiumi prisijungusių vartotojų. Rezultatai surašyti į 6 lentelę. RES stulpelyje surašyti fizinės atminties kiekiai, skirti skirtingoms užduotims (kodui ir duomenims saugoti). VIRT stulpelyje surašyti, kiek tam tikra užduotis naudoja virtualios atminties. RAM stulpelyje – RAM atminties naudojimas, CPU stulpelyje–

pastebėti didžiausi CPU naudojimo parodymai. „Vykdymo laikas“ stulpelyje nurodyti atitinkamai vidutiniai (gauta iš 8 reikšmių) ir maksimalūs pakartotinės vartotų autorizacijos laikai. Bandymai buvo atlikti su Intel core duo E8400 3,0 GHz CPU, 512 MB RAM virtualiu kompiuteriu su Linux Ubuntu operacine sistema. Iš 6 lentelės galima matyti, kokių resursų reikia, kad praėjimo kontrolės sistema veiktų greičiu.

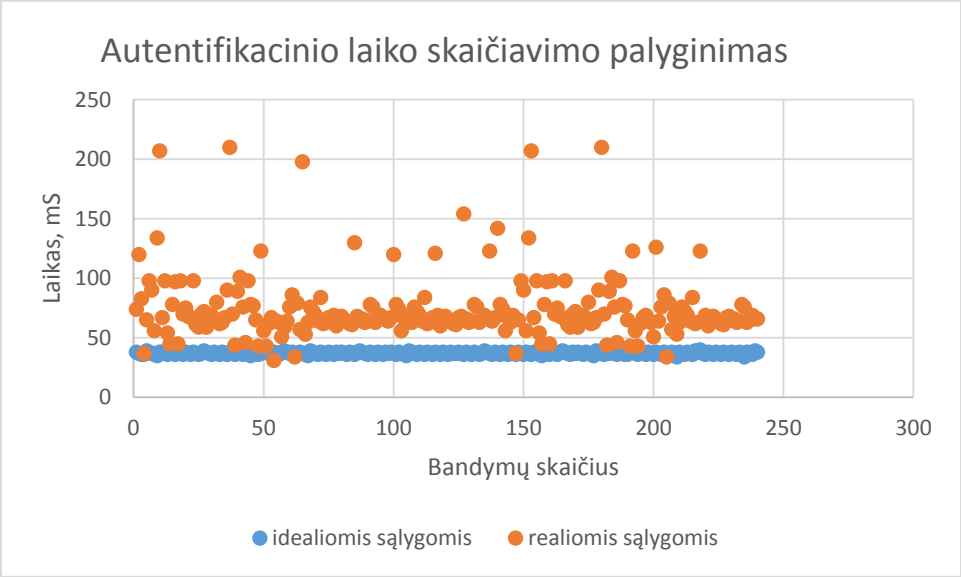
6 lentelė serverio resursų išnaudojimas

Vartotojų kiekis	**Vidutinis autentifikavimo laikas, s**	**Maksimalus autentifikavimo laikas, s**	**RES, kb**	**RAM, %**	**CPU max, %**
1	0,42	1	1652	0,8	30
5	0,93	1,8	1668	0,8	32.7
7	1,1	2,1	1669	0,8	33,8
10	3,3	4,2	1692	0,8	38,9
50	6,3	7	1704	0,8	39,3
100	13,3	17,5	1740	0,8	41,6
200	24,7	30,5	1844	0,9	53,2
500	61,7	94,4	2316	1,0	65,4

3.3 Eksperimentų rezultatai

Iš pirmo eksperimentinio tyrimo gautų rezultatų galima pastebėti, kad matuojant vieno vartotojo autentifikavimo laiką - vartotojas autentifikuojamas greičiau nei per 1s, nepriklausomai nuo vienu metu autentifikuojamų vartotojų skaičiaus. Tuo tarpu apskaičiavus vieno vartotojo autentifikavimo laiką iš rezultatų, gautų matuojant visų vartotojų autentifikavimo trukmę, gauta, kad jis gali būti net daugiau nei 1 min. ir priklauso nuo vienu metu autentifikuojamų vartotojų skaičiaus. Toks rezultatų neatitikimas gali būti paaiškinamas tuo, kad net ir vienu metu visiems klientas pradėjus vykdyti autentifikavimą, vis dėl to jų autentifikavimas pradedamas ne visai tuo pačiu metu – vartotojai pradedami autentifikuoti vienas po kitos. Anksčiau pradėtos užklausos baigiamos anksčiau, o vėliau pradėtos – vėliau, nepaisant to, kad vartotojai iš tikro bando autentifikuotis vienu metu. Autentifikacijos vykdomos tik iš dalies lygiagrečiai, dėl to, kad serverio programos vykdymui naudojamas tik vienas procesorius. Šio tyrimo metu vartotojo mobilieji įrenginiai veikė vienodomis sąlygomis viso bandymo metu (nebuvo atliekami jokie pašaliniai veiksniai su jais).

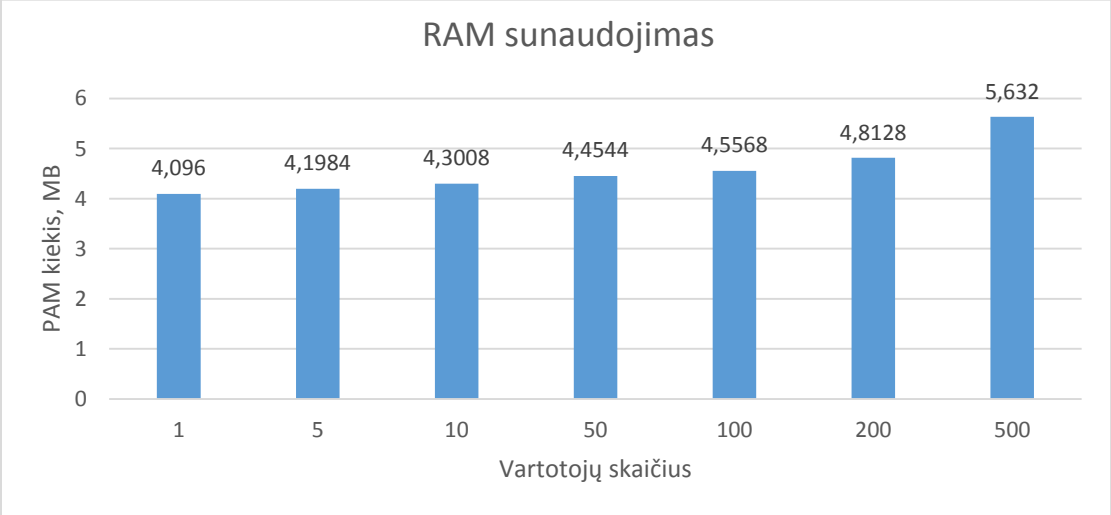
Iš antro eksperimento tyrimo gautų rezultatų galima pastebėti, kad matuojant realiomis sąlygomis veikiančio mobiliojo įrenginio autentifikacinio paketo skaičiavimo laikai ženkliai skiriasi dėl jame veikiančių įvairių procesų (skambučiai, trumposios tekstinės žinutės ir kita). Vidutiniškai mobilusis įrenginys gavęs teisę autentifikuotis praėjimo kontrolės sistemoje sugaišta 60 ms kol suskaičiuoja autentifikacinio paketo reikšmę. Šie rezultatai gan ženkliai skiriasi nuo teorinių rezultatų, gautų mobiliajam įrenginiui veikiant idealiomis sąlygomis. Grafiškai pateikti rezultatų palyginimai (21 paveikslėlyje), parodo ženkliai padidėjusius autentifikacinio paketo skaičiavimo laikus.



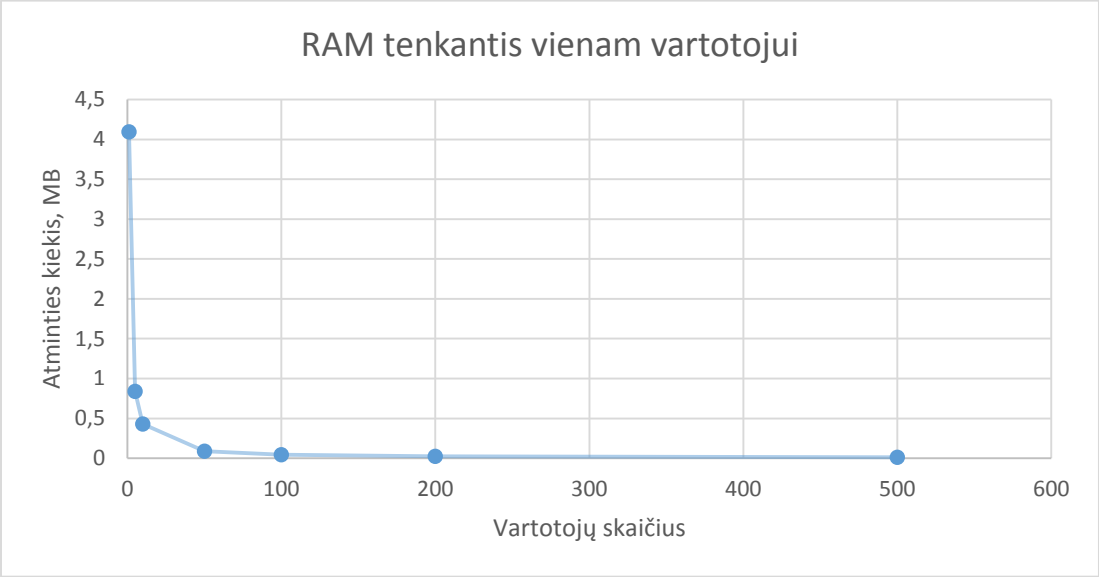
21 pav. Autentifikacinio paketo skaičiavimo laiko palyginimas

Trečio eksperimento metu buvo tirtas serverio resursų išnaudojimas. Pirmojo ir trečiojo eksperimentų metu pastebėta, kad praėjimo kontrolės sistema greitai gali aptarnauti iki septynių sistemos vartotojų. Praėjimo kontrolės sistemai septynis klientus aptarnauti trunka apie vieną sekundę. Didėjant vartotojų kiekiui didėja ir laikas reikalingas sistemos vartotojus autentifikuoti. Atliekant praėjimo kontrolės sistemos tyrimus nustatyta, kad vienas vartotojas sistemoje autentifikuojamas greičiau nei per 1 sekundę. Šitoks praėjimo kontrolės autentifikavimo laikas yra tinkamas praėjimo kontrolės diegimui realiomis sąlygomis.

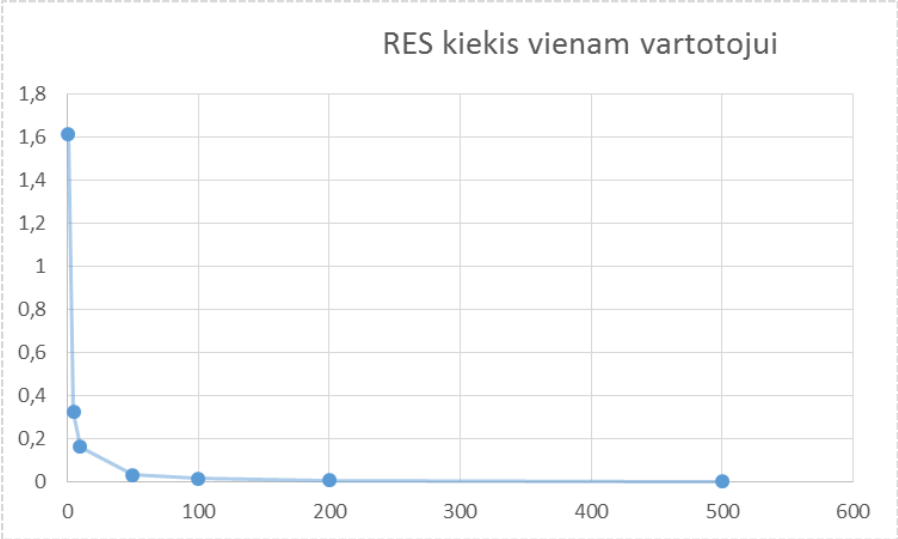
Pirmo ir trečio eksperimentų metu gauti rezultatai atvaizduoti žemiau pateiktose diagramose.



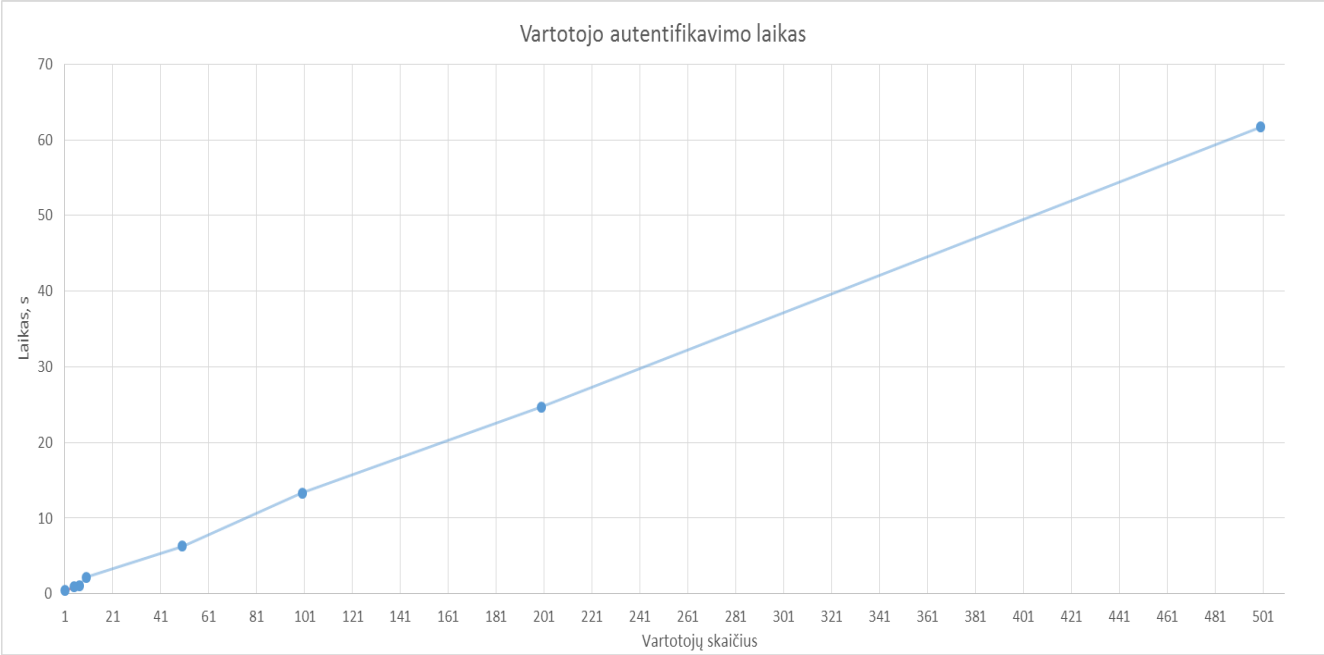
22 pav. Serverio RAM atminties sunaudojimas esant skirtingiems vartotojų kiekiams



23 pav. RAM kiekis tenkantis vienam vartotojui



24 pav. Atminties sunaudojimas vienam vartotojui autentifikuoti



25 pav. Sistemos vartotojų autentifikavimo laikas

22 ir 23 paveikslėliuose pavaizduota vienam klientui skirtų RAM išteklių priklausomybė nuo autentifikuojamų vartotojų skaičiaus. Iš diagramos matosi, kad atminties kiekis, reikalingas aptarnauti vieną klientą didėja nežymiai.

24 paveikslėlyje pavaizduota koks atminties kiekis tenka vienam vartotojui, priklausomybės nuo autentifikuojamų vartotojų kiekio. Galima daryti išvadą, kad kuo daugiau vartotojų reikia autentifikuoti, tuo mažiau atminties sunaudojama kiekvienam iš vartotojų autentifikuoti.

25 paveikslėlyje pateikta vartotojų autentifikacijos trukmė esant skirtingam vartotojų skaičiui. Grafike matosi, kad vartotojų aptarnavimo laikas tiesiškai priklauso nuo vartotojų skaičiaus ir augant vartotojų skaičiui vieno vartotojo aptarnavimo laikas išlieka pastovus – apie 120 - 130 milisekundžių. Galima daryti išvadą, kad sistema kokybiškai gali aptarnauti iki 7 vartotojų. Jei vartotojų skaičius didesnis, vidutinis autentifikavimo ir politikų vykdymo laikas išauga. Norint sistemą naudoti 10 ar daugiau vartotojų autentifikvimui, reikėtų prijungti papildomus Bluetooth priedėlius bei modifikuoti eksperimentinę praėjimo kontrolės sistemą. Tai leidžia paspartinti praėjimo kontrolės sistemos darbą esant didesniems vartotojų kiekiams ir didinti sistemos skaičiavimo pajėgumus (CPU) ar optimizuoti praėjimo kontrolės sistemos algoritmus.

3.4 Pasiūlymai ir ateities eksperimentiniams tyrimams

Suprojektuoti ir įdiegti pozicionavimo sistemą praėjimo kontrolės sistemoje. Kuri pagal Bluetooth signalo stiprumą galėtų nustatyti vartotojo atstumą iki autentifikuojančiojo Bluetooth priedėlio. Taip neleidžiant vartotojui autentifikuotis, kol jis nesa arčiau nei numatytas atstumas iki praėjimo kontrolės bluetooth adapterio. Ištirti praėjimo kontrolės sistemos

Praėjimo kontrolės veikimas ir sparta galėtų būti ištirta su didesniu duomenų bazėje įvestų duomenų skaičiumi. Galima būtų atlikti tuos pačius bandymus su realiomis

sąlygomis turint daug skirtingų mobiliųjų įrenginių su įdiegta klientine programine įranga, taip gaunant tikslesnius tyrimo duomenis. Bandymus atlikti su daugiau nei vienu Bluetooth priedėliu modifikuojant praėjimo kontrolės sistemą.

3.5 Skyriaus apibendrinimas

Buvo atlikti trys eksperimentai, kurių metu ištirta autentifikacijos (norinčių patekti prie saugomų resursų vartotojų) bei saugos politikos vykdymo trukmė ir išnaudojami kompiuterio resursai. Gauti rezultatai parodė, kad suprojektuota sistema, veikianti Intel core duo E8400 3,0 GHz CPU, 512 MB RAM serveryje gali kokybiškai aptarnauti iki 7 vienu metu prisijungusių klientų. Autentifikacija (vartotojo užklausų aptarnavimas) veikia pakankamai greitai ir vienas klientas aptarnaujamas greičiau nei per 20 s net ir 100 vartotojų bandant patekti prie saugomų resursų vienu metu. Atlikus realiomis ir idealiomis sąlygomis veikiančio mobiliojo įrenginio autentifikacinio paketo skaičiavimo laiko analizę(realus ir virtulaus mobilus įrenginys turi vienodus sisteminius parametrus: 1,2 GHz CPU ir 512 MB RAM su Android 4.0), pastebėta, kad mobiliajam įrenginiui veikiant idealiomis sąlygomis, kur kas greičiau suskaičiuojamas autentifikacinis paketas nei veikiančiame realiomis sąlygomis, tai įtakoja papildomos mobiliojo įrenginio apkrovos.

Praėjimo kontrolės veikimas ir sparta galėtų būti ištirta su didesniu duomenų bazėje įvestų duomenų skaičiumi. Galima būtų atlikti tuos pačius bandymus su realiomis sąlygomis turint daug skirtingų mobiliųjų įrenginių su įdiegta klientine programine įranga, taip gaunant tikslesnius tyrimo duomenis. Bandymus atlikti su daugiau nei vienu Bluetooth priedėliu modifikuojant praėjimo kontrolės sistemą bei modelį praplečiant signalo stiprumo matavimo funkcija.

4 Išvados

1. Atlikus sistemoje naudojamų technologijų apžvalgą pastebėta, kad jau yra sukurtos keturios Bluetooth technologijos versijos. Dėl ketvirtosios versijos įrenginių mažo paplitimo, tyrimas atliktas su antrosios versijos įrenginiais. Praėjimo kontrolės sistemoje tikslinga naudoti ketvirtosios kartos Bluetooth technologijos įrenginius dėl jame esančio įdiegtos duomenų perdavimo saugos mechanizmo.
2. Atlikta Bluetooth technologijos analizė parodė, kad vienu metu vienas Bluetooth adapteris gali aptarnauti iki septynių vartotojų. Dėl šios priežasties tikslinga statyti papildomus Bluetooth adapterius, siekiant padidinti sistemos našumą autentifikuojant vartotojus.
3. Atlikta praėjimo kontrolės sistemų, veikiančių Bluetooth technologija, analizė parodė, kad praėjimo kontrolės sistemai su Bluetooth galima naudoti įvairius mobiliojo įrenginio vidinius duomenis. Vartotoją patogiausia identifikuoti pagal Bluetooth MAC adresą.
4. Darbe pasiūlytas praėjimo kontrolės modelis, kuris suderintas su Bluetooth technologijoje esančiu saugiu duomenų perdavimo kanalu, kuriuo bus perduodami autentifikaciniai vartotojo duomenys. Modelyje pasiūlyta vartotojo krypties nustatymo metodika.
5. Pasiūlyto modelio pagrindu suprojektuota praėjimo kontrolės sistema su vartotojo judėjimo krypties nustatymo moduliu bei vartotojo identifikavimo ir autentifikavimo moduliais
6. Pasiūlyta praėjimo kontrolės sistema ištestuota. Gauti rezultatai parodė, kad ji veikia teisingai. Jos savybės ištirtos eksperimentiniu būdu. Tyrimais nustatyta, kad sistema, veikianti Intel core duo E8400 3,0 GHz CPU, 512 MB RAM kompiuteryje, gali kokybiškai ir greitai aptarnauti iki 7 vartotojų vienu metu, didėjant vartotojų kiekiui, eksponentiškai auga vartotojų aptarnavimo laikas. Siekiant sumažinti vartotojų aptarnavimo laiką reikia papildomai prijungti Bluetooth priedėlius, kurie pagreitintų praėjimo kontrolės sistemos autentifikacijos laiką.
7. Atliekant praėjimo kontrolės sistemos tyrimus nustatyta, kad vienas vartotojas sistemoje autentifikuojamas greičiau nei per 1 sekundę. Šitoks praėjimo kontrolės autentifikavimo laikas yra tinkamas praėjimo kontrolės diegimui realiomis sąlygomis.
8. Modelį galima praplėsti panaudojant signalo stiprumo matavimą, kurio pagalba būtų galima nustatyti vartotojo judėjimo kryptį ir atstumą iki Bluetooth autentifikuojančio imtuvo. Vartotojas galėtų būti autentifikuojamas, jei jis būtų netoliau nuo imtuvo nei tam tikras iš anksto numatytas atstumas.

5 Literatūra:

[1] **Outeirino F.J.B..** Universal Bluetooth Access Control and Security System for e-Keys Enviroments. *Emerging Security Information Systems and Technologies (SECURWARE), 2010 Fourth International Conference on*

[2] **Othman, M..** Developing A Secure Mechanism for Bluetooth-based Wireless Personal Area Networks (WPANs). *Electrical Engineering, 2007. ICEE '07. International Conference on*

[3] **Huaizhi Li.** A key establishment protocol for Bluetooth scatternets. *Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference on*

[4] **Saravanan K.** An new secure mechanism for bluetooth network. *Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on*

[5] **Chia-Sheng Tsai ir Cheng-I Hung.** An enhanced secure mechanism of access control. *Communication Systems, Networks and Applications (ICCSNA), 2010 Second International Conference on*

[6] **Zolfaghar K.** Securing Bluetooth-based payment system using honeypot. *Innovations in Information Technology, 2009. IIT '09. International Conference on*

[7] **Robert F. Heile, Thomas M. ....** 802.15.1-2002 - IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)

[8] The Bluetooth Special Interest Group (SIG). Bluetooth. [Žiūrėta 2012-12-04] prieiga per internetą: http://www.bluetooth.com/Pages/In-theNews.aspx

[9] The Bluetooth Special Interest Group (SIG). Bluetooth technology [žiūrėta 2012-10-14] prieiga per internetą: http://www.bluetooth.com/Pages/Basics.aspx

[10] The Bluetooth Special Interest Group (SIG). Bluetooth. how it works? [žiūrėta 2012-10-14] https://www.bluetooth.org/Building/HowTechnologyWorks/Architecture/Overview.htm

[11] **Ling Pei** Inquiry-Based Bluetooth Indoor Positioning. *RSSI Probability Distributions 13-19June2010*

[12] **Jaap Haartsen** BLUETOOTH—The universal radio interface for ad hoc, wireless connectivity. *Ericsson Review No. 3, 1998*

[13] **Asif, Saad Z**. Next Generation Mobile Communications Ecosystem. John Wiley & Sons. p. 306. ISBN 1119995817. (2011).

[14] **Gaby Lenhart** "The Smart Card Platform". *ETSI Technical Committee Smart Card Platform (TB SCP). Retrieved 30 January 2010. "SCP is co-operating on both technical and service aspects with a number of other committees both within and outside the telecommunications sector." (1 April 2006).*

[15] GSM Association, IMEI Allocation and Approval Guidelines, *[žiūrėta 2012-10-14] prieiga per internetą* *http://www.gsma.com/newsroom/wpcontent/uploads/2012/03/ts0660tacallocationprocessapproved.pdf*

6 Priedai

6.1 Antro tyrimo metu gauti rezultatai

7 lentelė antro eksperimento rezultatai

bandymo nr.	idealiomis sąlygomis	realiomis sąlygomis
1	38	74
2	37	120
3	36	83
4	36	37
5	39	65
6	38	98
7	37	90
8	36	56
9	35	134
10	38	207
11	38	67
12	37	98
13	36	54
14	38	45
15	37	78
16	36	97
17	38	45
18	37	98
19	36	70
20	38	75
21	37	68
22	36	67
23	38	98
24	37	61
25	36	59
26	37	70
27	39	72
28	38	59
29	37	63
30	36	69
31	38	65
32	37	80
33	36	62
34	38	63
35	37	67
36	36	90
37	38	210
38	37	70
39	36	44
40	38	89
41	37	101
42	36	76
43	38	46
44	37	98
45	35	78
46	38	77
47	37	65
48	36	43
49	37	123
50	39	56
51	38	43
52	37	62
53	36	67
54	38	31

55	37	64
56	36	63
57	38	51
58	39	59
59	38	64
60	37	76
61	38	86
62	37	34
63	36	79
64	38	57
65	37	198
66	36	53
67	35	63
68	39	76
69	38	72
70	37	69
71	36	64
72	38	84
73	37	62
74	36	63
75	38	67
76	37	64
77	36	69
78	38	60
79	37	67
80	38	68
81	37	65
82	36	64
83	38	62
84	37	61
85	36	130
86	38	68
87	39	65
88	38	66
89	37	63
90	36	64
91	38	78
92	37	76
93	36	63
94	38	65
95	37	69
96	36	66
97	38	66
98	37	64
99	38	67
100	37	120
101	36	78
102	38	74
103	37	56
104	36	67
105	35	63
106	39	69
107	38	63
108	37	76
109	36	72
110	38	69
111	37	64
112	36	84
113	38	62
114	37	63
115	36	67
116	38	121
117	37	69

118	36	60
119	38	67
120	37	68
121	36	65
122	38	64
123	37	62
124	37	61
125	38	67
126	37	68
127	36	154
128	38	66
129	37	63
130	36	64
131	38	78
132	37	76
133	36	63
134	37	65
135	39	69
136	38	66
137	37	123
138	36	64
139	38	67
140	37	142
141	36	78
142	38	74
143	37	56
144	36	67
145	38	63
146	37	69
147	36	37
148	38	65
149	37	98
150	36	90
151	38	56
152	37	134
153	36	207
154	38	67
155	37	98
156	36	54
157	35	45
158	38	78
159	37	97
160	36	45
161	38	98
162	37	70
163	36	75
164	38	68
165	39	67
166	38	98
167	37	61
168	36	59
169	38	70
170	37	72
171	38	59
172	37	63
173	36	69
174	38	65
175	37	80
176	36	62
177	35	63
178	39	67
179	38	90
180	37	210

181	36	70
182	38	44
183	37	89
184	38	101
185	37	76
186	36	46
187	41	98
188	37	78
189	36	77
190	36	65
191	39	43
192	38	123
193	37	56
194	36	43
195	38	62
196	37	67
197	36	69
198	38	64
199	37	63
200	36	51
201	38	126
202	37	64
203	36	76
204	38	86
205	37	34
206	36	79
207	38	57
208	37	68
209	34	53
210	38	63
211	37	76
212	36	72
213	38	69
214	37	64
215	36	84
216	39	62
217	39	63
218	40	123
219	37	64
220	36	69
221	38	60
222	37	67
223	36	68
224	38	65
225	37	64
226	36	62
227	38	61
228	37	67
229	36	68
230	38	65
231	37	66
232	36	63
233	38	64
234	37	78
235	34	76
236	38	63
237	37	65
238	36	69
239	39	66
240	38	66