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

VAIDA NEVERDAUSKAITĖ

ASMENINIŲ ĮRENGINIŲ SAUGAUS KONFIGŪRAVIMO SPRENDIMŲ PARAMOS SISTEMA

Magistro baigiamasis darbas

Darbo vadovas
doc. dr.J. Toldinas

KAUNAS, 2013

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

VAIDA NEVERDAUSKAITĖ

ASMENINIŲ ĮRENGINIŲ SAUGAUS KONFIGŪRAVIMO SPRENDIMŲ PARAMOS SISTEMA

Magistro baigiamasis darbas

Recenzentas
doc. dr. G. Činčikas
2013-05-27

Vadovas
doc. dr. J. Toldinas
2013-05-27

Atliko
IFN-1/3 gr. stud.
Vaida Neverdauskaitė
2013-05-27

KAUNAS, 2013

AUTORIŲ GARANTINIS RAŠTAS
DĖL PATEIKIAMO KŪRINIO

20.. - ..... - ..... d.
Kaunas

Autoriai,_____
(vardas, pavardė)

_____,

patvirtina, kad Kauno technologijos universitetui pateiktas baigiamasis bakalauro (magistro) darbas (toliau vadinama – Kūrinys)_____
(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

_____ _____
(vardas, pavardė) (parašas)

SUMMARY

The mobile industry is evolving rapidly and new mobile devices with sophisticated capabilities are released almost every day. The technical advancements in mobile industry have resulted in increase of security threats and attacks. To provide strong security mechanism a combination of solutions need to be implemented at different levels based on enterprise mobile application security requirements.

Enterprise mobile security should ensure two key components: enterprise system security and device security. Enterprise system security must ensure that the server framework and the mobile network support security in connection, communication and data handling. Device security ensures that mobile device and applications are secured from attacks. It includes authentication of device, security of content in the device and device features like encryption.

The aim of this paper is to create secure configuration decision support system prototype for personal devices.

This paper is organized as follows:

- In the first part we analyze security threats and attacks for mobile devices. Also we look more deeply into how mobile devices are used by corporation user and what levels of information are reached by different roles of workers. In this part we also look into what kind of software can be installed and which configuration settings can be enforced in order to ensure that device is secure.
- In second part we define relation between corporate's information levels, roles and device security requirements. There we also define secure connection, communication and data handling between server and mobile device. Finally, secure configuration decision support system prototype for personal devices are created.
- In third part we represent results of experiments which cover main pars of secure configuration decision support system for personal devices: secure communication between corporates server and mobile device over wi-fi and device contents cryptography.
- Finally we represent this work's conclusions.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

API – aplikacijų programavimo sąsaja

BES (angl. Blackberry Enterprise Server) komercinė mobiliųjų įrenginių valdymo sistema Blacbery OsS naudotojams.

BIS (angl. BlackBerry Internet Service) ne verslo vartotojams suteikiamas funkcionamas naudojant BlacBerry OS

DLP (angl. *Data Loss Prevention*) - duomenų praradimo prevencija

ECC (angl. Elliptic curve cryptography)- Elipsinės kreivės kriptografija

GSMA- mobiliųjų operatorių asociacija

ICV (angl. Integrity Check Value) -kontrolinių sumų mechanizmas

Java MIDlets - Java mobiliosios programos

JSR (angl. java specification requests) –formalus dokumentas apibrėžiantis technologijas bei specifikacijas java naudojimui.

MĮ- mobilusis įrengins

QoS (angl. *Quality of Service*) - paslaugos kokybė

RRSI (ang. received signal strength indicator) – gaunamo signalo stiprumas (pvz. wi-fi tinkluose).

TCB (ang. trusted computing base) – patikimų kompiuterių pagrindo struktūra.

TKIP (angl. Temporal Key Integrity Protocol) - laikino rakto vientisumo *protokolas*

TrEE (angl. trusted execution environment) -patikima vykdymo aplinka

UID (angl. Unique Identification Number) – unikalus identifikavimo numeris

VPN – virtualus privatus tinklas

WLAN- bevielis vietinis tinklas

WWAN- bevielis teritorinis tinklas

1. ĮVADAS

Šiuolaikinėse organizacijose darbuotojams leidžiama naudotis asmeniniais mobiliaisiais įrenginiais. Šitokių įrenginių prieinamumas tiek prie asmeninės tiek prie verslo informacijos bei mobiliųjų įrenginių saugos sprendimų ir konfigūravimo galimybių skirtumai lyginant su kompiuteriais sukelia papildomų iššūkių organizacijoms. Neteisingai sukonfigūruotas asmeninis mobilus įrenginys (nepriklausomai nuo jo gamintojo ir modelio), kuriam leista naudotis organizacijose esama informacija gali būti lengviau prieinamas įsilaužėliams. Organizacijos darbuotojai savo mobiliuose įrenginiuose taipogi gali tūrėti įvairią papildomą programinę įrangą, kurios patikimumas ir organizacijos saugos politikos atitikimas nėra žinomas. Tai reikalauja papildomų valdymo priemonių, kurios užtikrintų asmeninių įrenginių saugos konfigūravimą, atitinkantį organizacijos saugos politiką.

Organizacijos saugos politika privalo atsižvelgti į dvi pagrindines sritis: organizacijos sistemų saugumą ir mobiliojo įrenginio saugumą [1]. Organizacijos sistemų saugumo dalis užtikrina, kad prisijungimas, komunikacija bei duomenų perdavimas tarp serverio ir mobiliojo įrenginio būtų saugus. Mobiliojo įrenginio saugumo dalis užtikrina, kad įrenginys būtų kuo geriau apsaugotas nuo atakų. Tai pasiekiama atliekant autentifikaciją, saugomų duomenų šifravimą bei mobiliajame įrenginyje nustatant įmonės saugos politiką atitinkančią konfigūraciją.

Magistrinio darbo tikslas – išnagrinėti mobiliesiems įrenginiams keliamas grėsmes bei sudaryti mobiliųjų įrenginių saugios konfigūracijos paramos sistemos prototipą.

Darbo uždaviniai:

- Išnagrinėti mobiliesiems įrenginiams keliamas grėsmes;
- Išnagrinėti galimus mobiliųjų įrenginių konfigūracijos nustatymus, atsižvelgiant į keliamą įtaką duomenų saugumui;
- Sudaryti mobiliųjų įrenginių konfigūracijos rekomendaciją įmonei, atsižvelgiant į prieinamos informacijos tipus;
- Sudaryti mobiliųjų įrenginių saugaus konfigūravimo sistemos prototipą;
- Pasitelkus Microsoft .NET Compact Framework platformos teikiamus programavimo sprendimus, atlikti pagrindinių funkcijų tyrimą;
- Išnagrinėti bei pateikti eksperimento rezultatus.

Darbo struktūra:

- Analizės dalyje nagrinėjame mobiliųjų įrenginių pažeidžiamumus, sukeliamus kenkėjiškų programinių įrangų, programišių atakų, netinkamos konfigūracijos nustatymų bei mobiliojo įrenginio savininko veiksmų. Čia taipogi analizuojame mobiliųjų įrenginių naudojimo atvejus organizacijoje, apibrėžiame saugomos informacijos rūšis bei darbuotojų kategorijas. Galiausiai, analizės dalyje pateikiame programinės įrangos bei konfigūracijos nustatymų sąrašą, galintį padėti užtikrinti saugų mobiliųjų įrenginių vartojimą.
- Antrojoje darbo dalyje pateikiame asmeninių įrenginių saugaus konfigūravimo sprendimų paramos sistemos prototipą, nurodome informacijos slaptumo ir darbuotojų rolių sąryšį bei pasiūlome mobiliųjų įrenginių konfigūracijos nustatymų sąrašą, atsižvelgiant į prieinamos informacijos slaptumą. Šitoje dalyje taipogi rasite serverio ir mobiliojo įrenginio komunikavimo proceso schemas bei būsenų diagramas, leidžiančias geriau įsivaizduoti procesą.

- Trečiojoje darbo dalyje pateikiame atlikto eksperimento rezultatus. Pirmojoje eksperimento dalyje nagrinėjame duomenų parsisiuntimo greičio kintamumą priklausant nuo pasirinkto saugos protokolo bei ryšio kokybės. Antroji eksperimento dalis tiria turimų duomenų užšifravimo ir atšifravimo greičius priklausomai nuo pasirinkto šifravimo metodo. Galiausiai gautus rezultatus apibendriname ir susiejame su antrojoje dalyje pateiktomis konfigūracijos rekomendacijomis priklausomai nuo prieinamos informacijos lygio.
- Paskutinė darbo dalis pateikia bendras darbo išvadas.

2. ASMENINIŲ MOBILIŲ ĮRENGINIŲ SAUGAUS NAUDOJIMO DARBE ANALIZĖ

Įmonėse naudojamų mobiliųjų įrenginių (MĮ) kiekis pastaruoju metu aktyviai auga. Šių įrenginių naudojimas naudingas tiek darbdaviui teik darbuotojui, nes darbuotojų rolės vis dažniau reikalauja dirbti interaktyviai, iš bet ir bet kada, pasitelkiant naujausius techninius bei programinius sprendimus. Didėjantis resursų kiekis, reiškia jog vis daugiau konfidencialios įmonės bei asmeninės informacijos gali būti talpinama MĮ [2]

2.1 pav. saugus mobiliųjų įrenginių naudojimo darbe punktai

2.1 paveikslas [3] iliustruoja kai kuriuos iš svarbiausių saugaus MĮ (mobiliųjų įrenginių) naudojimo darbe punktų:

- Vartotojo identifikavimas. Siekia užtikrinti, kad tik autorizuoti subjektai gali naudoti prietaisą/programinę įrangą.
- Saugi duomenų saugykla. Apima saugumo jautrios informacijos, tokios kaip slaptažodžiai, PIN kodai, raktai, sertifikatai ir t.t., kuri gali būti saugojama vidinėje mobilaus įrenginio atmintyje (angl. flash) .
- Saugi programinės įrangos veikimo aplinka. Siekiant užtikrinti saugią programų vykdymo aplinka yra būtina užtikrinti, kad būtų negalimi išpuoliai nuo kenkėjiškų programų, tokių kaip virusai ar Trojos arkliai.
- Klastojimams atsparių sistemų diegimas. Reikalinga, kad užtikrinti kompiuterinės įrangos saugumą nuo įvairių fizinių ir elektrinių atakų.
- Saugi prieiga prie tinklo. Užtikrina, kad tik autorizuoti įrenginiai gali būti įjungti į tinklą ar naudotis paslaugą.
- Saugus apsikeitimas duomenimis. Apžvelgia saugų duomenų perdavimo privatumą ir vientisumą iš/į mobiluįį įrenginį.
- Turinio saugumas. Bet koks turinys kuris parsiųstas į arba laikomas mobiliame įrenginyje, naudojamas pagal sąlygas, pateiktas turinio teikėjo (pvz., teisė tik skaityti, ne kopijuoti ir pan.)

Tolimesniuose analinės skyriuose išnagrinėsime pagrindinius MĮ pažeidžiamumus, MĮ naudojimo atvejus bei reikalingą konfigūracijos bei automatizavimo nustatymus, kad užtikrinti saugų MĮ naudojimą įmonėse.

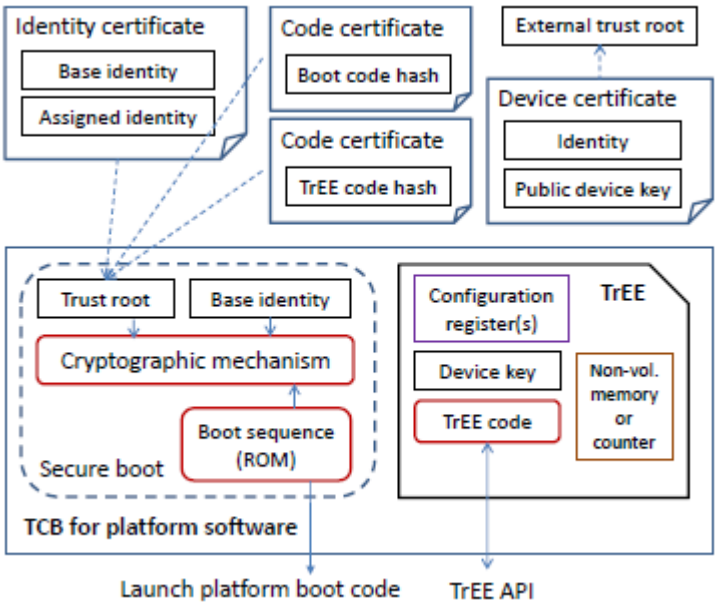
2.1. Asmeninių mobiliųjų įrenginių pažeidžiamumų analizė

Šiuo metu neegzistuoja pripažintų saugos standartų mobiliesiems įrenginiams, kurie nustatytų normas komunikacijai per VPN, MĮ kaupiamų duomenų šifravimui, slaptažodžių naudojamumui, nuotoliam duomenų išvalymui bei kitam funkcionalumui [4]. Vadinasi, gaunami saugos nustatymai MĮ didžiąja dalimi priklauso nuo jų gamintojų. Skirtingos MĮ operacinės sistemos (Symbian iOS, Blackberry OS, Android, Windows mobile) turi skirtingai įgyvendintus funkcionalumo bei saugos sprendimus, į kuriuos reikia atsižvelgti kuriant įmonės saugos politiką. MĮ gali jungtis prie interneto ar kitų įrenginių per WLAN, Bloetooth,VPN . Dauguma MĮ taipogi naudoja Java platformos galimybes, kas sukelia papildomas saugos problemas.

Tolimesniuose skyriuose nagrinėsime MĮ pažeidžiamumus atsižvelgdami į naudojamas technologijas, konfigūracijas, programinę įrangą bei žmogiškąjį faktorių.

2.1.1. Asmeninių mobiliųjų įrenginių konfigūracijos pažeidžiamumai

2.2 pav. [5] pateikia bendrinę aparatinės įrangos saugos schema naudojamą šiuolaikiniuose MĮ.



2.2 pav. Bendrinė aparatinės įrangos saugos schema MĮ

Kiekvienas MĮ turi pagrindinį identifikavimo kodą. Juo gali būti IMEI ar bet koks kitas unikalus kodas. Kodo nekintamumas gali būti pasiektas patalpinant reikšmę tik skaitymo teises turinčioje atmintyje (ROM) gamybos proceso metu. Antra, kiekvienas MĮ turi autentifikuoti išorinę informaciją. Šis veiksmas atliekamas su gamintojo viešojo rakto maišos kodu. Šis kodas yra vienodas visai įrenginių šeimai.

Kiekvienos palaikomos radijo ryšio sąsajos MAC adresui reikalingas daugiau nei vienas priskirtas identifikavimo kodas. Kadangi visus įrenginių identifikatorius surašyti į ROM atmintį gamybos metu sudėtinga, naudojamas identifikavimo sertifikatas. Jis sukuriamas paimant gamintojo maišos kodą ir vieną priskirtą identifikavimo kodą. Naudojantis identifikavimo

sertifikatu, galima leisti pridėti papildomus ryšius pagal poreikį. Papildomai įrenginio aparatinė įranga turi būti apsaugota kriptografiniu mechanizmu, kuris gali patvirtinti identifikavimo sertifikatą. Todėl dažnai šis mechanizmas integruotas kaip dalis ROM atminties.

Kai kurie MĮ gamintojai tikrina įrenginio vientisumą sistemos paleidimo metu ir jei pastebima, kad sistema buvo modifikuota, paleidimo procesas sustabdomas. Šitoks procesas vadinamas saugiu užkrovimu. Tam kad įgyvendinti tokį principą, reikia kad pradinė dalis sistemos paleidimo proceso gulėtų ROM atmintyje. MĮ gamintojai išleidžia grupę paleidimo maišos kodų ir susieja juos su viešuoju įrenginio maišos kodu. Šitoks patikrinimo prieš paleidžiant principas gali būti pritaikytas ne tik OS paleidimui, bet ir bet kokiam kitam kodui ar konfigūracijos failui.

Saugumo sprendimai reikalauja galimybės izoliuotai vykdyti kodą bei turėti saugią informacijos talpyklą. Kai TCB (OS branduolys) yra didelis, viso kodo vienu metu tikrinimas užkrovimo metu daliai nėra tinkamiausias būdas. Tuomet pasitelkiama TrEE (patikima vykdymo aplinka) sprendimas. MĮ gamintojai pasitelkę šį sprendimą užtikrina įrenginyje saugią atmintinę unikaliam įrenginio kodui ir vykdymo aplinką, kurioje maži galiukai kodo gali būti įvykdomi atskirai nuo likusios sistemos. Kadangi TrEE procesas prileidžia priėjimą prie paslapčių, būtina užtikrinti kad jos nebus atskleistos išorei per klaidą arba tikslingai. Šitoks užtikrintumas pasiekiamas naudojant kodo pasirašymą (kodo sertifikatai turintys TrEE maišos kodą) arba TrEE procesą sudarant taip, kad bent koks kodas gautų tik dalį priėjimo prie konfidencialios informacijos (pasitelkiant kriptografinius metodus).

TrEE turi konfigūracijos registrus, kuriuose gali būti talpinami įvairūs matavimai, surenkami iš paleistos sistemos, aparatinės įrangos nustatymai, vartotojo sprendimai. Ši sukaupta informacija gali būti panaudota dviem būdais. Pirma, kodas kuris leidžiamas TrEE gali koreguoti savo veikimą, atsižvelgiant į sistemos būseną. Kitas panaudojamas – sistemos būsena gali būti perduodama kitoms šalims.

Įrenginio kodas, kuris prieinamas tik TrEE gali būti panaudotas viešajam raktui sudaryti ir gauti įrenginio sertifikatą, kuris gali būti panaudoti užtikrinti autentifikuotą bei saugų ryšio kanalą su išorinėmis šalimis.

2.1 lentelė Sistemų palyginimas pagal saugumo ir valdymo kriterijus

Kriterijus	**BB 7.0**	**iOS 5**	**Wp 7.5**	**Android 2.3**
Integruoti saugumo nustatymai	3.13	3.75	3.50	2.50
Programėlių saugumo nustatymai	2.44	2.06	1.88	1.44
Autentifikacija	3.90	2.00	3.20	2.00
Nuotolinis valdymas	4.00	1.25	2.25	0.63
Ugniasienės	4.50	0.00	0.00	0.00
Duomenų apsauga	3.80	1.50	2.40	2.00
Įrenginio apsauga	3.50	0.63	2.38	2.00
Organizacijos e-pašto valdymas	3.42	3.00	0.00	0.00
ActiveSync palaikymas	0.00	2.00	2.50	1.50
MĮ valdymas	3.50	2.50	1.25	2.00
Virtualizacija	0.00	0.83	0.00	1.67
Saugos sertifikatai	2.50	0.83	0.00	0.67
OS vidutinis balas	**2,89**	**1.70**	**1.61**	**1.37**

Kadangi gamintojas gali pasirinkti naudoti, tik dalį saugumo sprendimų iš 2.2 pav. matome jog, skirtingos OS saugos ekspertų vertinamos skirtingai. Trend Micro 2012 metais atliko populiarių MĮ operacinių sistemų palyginimą. Lygindami OS buvo atsižvelgta į 12 MĮ saugumo bei valdymo kriterijų (žr. lentelė nr 2.1). Vertinant individualias OS, ekspertų geriausiai įvertinta Blackberry OS. Pranašumą šiai OS suteikia saugos bei valdymo sistema, kurią galima įsigyti iš gamintojų. [6]

Norint sudaryti gerą saugos politiką įmonei, kuri leidžia darbuotojams naudotis asmeniniais įrenginiais, būtina išnagrinėti kiekvienos OS pažeidžiamumus atskirai.

Blacberry OS

Kaip matėme iš 2.1 lentelės Blacberry OS ekspertų vertinama geriausiai atsižvelgiant į saugos ir valdymo kriterijus. Šitoks pripažinimas rinkoje įgytas dėl Blackberry valdymo įrankio - ‚Blackberry Enterprise Server (BES)'. BlacBerry sukuria vienkartinį raktą, kuris yra panaudojamas užšifruoti ECC privatų raktą ir turinio apsaugos raktą. Raktai yra saugomi Flash /specialioje išliekamojoje atmintyje (ang. non-volatile memory), prie kurios vartotojas neturi priėjimo. Šitokiu būdu yra užtikrinamas įrenginio lygio apsaugą, kuri yra valdoma iš BES valdymo sistemos. Turinio apsauga yra užtikrinama naudojant asimetrinius raktus. Viešasis raktas panaudojamas užšifruoti turiniui kai MĮ yra užrakintas. Kai MĮ atrakinamas atitinkantis privatus raktas panaudojamas informacijos atšifravimui. Komunikacijų saugumui užtikrinti Blacberry naudoja simetriniais raktus kartu su AES/3DES šifravimo algoritmais. Viršiausiais šifravimo raktas laikomas BES valdymo sistemoje. [7]

Tačiau tokios svarbios galimybės kaip duomenų šifravimas, informacijos ištrynimas nuotoliniu būdu ar griežtesnis prieigos valdymas galimas tik papildomai nusipirkus programinę įrangą- BES (žr. lentelę 2.2). Jei įmonėje leidžiama naudotis ir kitokiais MĮ, prie Blacberry suteikiamo bendrinio funkcionalumo (BIS) reikia taikyti ir kitokias saugos bei valdymo priemones.

2.2 lentelė Blacberry BES ir BIS funkcionalumo palyginimas

Kriterijus	BES	BIS
Šifruotas interneto ryšys	+	+
Duomenų apsauga	+	-
Autentifikacija	+	+
Apsauga nuo virusų	+	+
Duomenų ištrynimas / telefono užrakinimas nuotoliniu būdu	+	-
Rolėmis paremtas valdymas	+	-
Sąsaja su įmonės paštu	+	-

Blackberry programos turi būti pasirašytos koduotais parašais, tačiau juos galima gauti lengvai iš gamintojo už nedidelę kaina, todėl tai neužtikrina didelio patikimumo. Be to vartotojas gali įdiegti trečiųjų šalių sukurtą nepasirašytą programinę įrangą, suteikdamas sutikimą jai vykti įrenginyje bei suteikdamas teisę prieiti prie įrenginio paslaugų.

Vartotojui taipogi leidžiama konfigūruoti prieigos teises (leisti, uždrausti, klausti), tačiau užklausos iššoka kiekvieną kartą aktyvavus įrenginio funkcijas ir tai vartotojus erzina. Vartotojas pernelyg dažnai gaudamas saugos nustatymų užklausas, sutinka duoti prašomas teises nenagrinėdamas užklausos. [7]

Apple iOS

iOS (iki 2010 m. – iPhone OS) – „Apple“ sukurta operacinė sistema, pagrinde projektuota iPhone išmaniajam telefonui, o vėliau pritaikyta ir kitiems „Apple“ įrenginiams, kaip kad iPod Touch, iPad ir Apple TV. Prekyboje pirmą kartą pasirodė 2007-aisiais metais ir susilaukė didžiulės sėkmės dėl išskirtinio dizaino sprendimų ir dėmesio vartotojui parodymo.

Vienas didžiausių Apple OS pliusų yra programinės įrangos parduotuvė, kuri mobiliųjų programų rinkoje yra kontroliuojama bene labiausiai. Tai sumažina tikimybę, jog bus įdiegta kenksminga programinė įranga MĮ. Priedo to, paaiškėjus jog anksčiau patvirtinta saugi programa, vis dėlto yra kenkėjiška, Apple gali nuotoliniu būdu pašalinti ją iš vartotojų įrenginių, taip sustabdydama tolimesnius galimus padarinius. Norint įdiegti bet kokią Apple nesankcionuotą trečiųjų šalių programą, operacinę sistemą reiks nulaužti. Tačiau to nerekomenduojama daryti, nes padidėja saugumo problemų. [8]

Pagrindinės Apple iOS pastebimos problemos:

- Visos programos naudojasi bendrais resursais – root.
- Nėra saugumo zonos (angl. sandbox)- vadinasi sistema yra tiek apsaugota, kiek saugi mažiausiai apsaugota programa.
- Safari naršyklė diegiama visose iOS. Naršyklė turi daug saugumo spragų ir kadangi naudojasi bendrais sistemos resursais, gali būti pagrindinis būdas nulaužti ar sugadinti sistemą.

Norint nulaužti ar nagrinėti iPhone įrenginyje vykstančius procesus rekomenduojama naudoti Metasploit arba iPhoneDbg programinę įrangą.

Google android

Android yra atviro kodo, Linux tipo operacinė sistema, daugiausia naudojama išmaniuosiuose telefonuose, nors ją galima įdiegti ir kituose mobiliuosiuose įrenginiuose, kaip kad planšetiniame kompiuteryje. Tai Linux operacinės sistemos ir įvairių, daugiausia „Google“ sukurtų papildomų plėtinių kombinacija. Pagrindinė šios sistemos programavimo kalba yra Java. Kuriamos programos sąsaja dalinai aprašoma XML. Šiuo metu tai yra labiausiai atakuojama mobiliųjų įrenginių operacinė sistema. [7]

Kiekviena programa Google android sistemoje veikia savo atskiroje zonoje (ang. sandboxing) su skirtingu programos identifikavimo numeriu (UID). Leidimai suteikiami kiekvienai programai atskirai. Iš viso Google apibrėžė 112 leidimų, tačiau Android programuotojai gali apirėžti naujus leidimus, taip augindami jų skaičių. Leidimai skirstomi į lygius: Normalus, Pavojingas, Pasirašomas ir Sisteminis. Normalaus leidimo reikalaujančios programos neprašo vartotojo patvirtinimo. Pavojingai kategorijai priklausančius leidimus turi patvirtinti vartotojas. Pasirašantys leidimai reikalauja, kad programėlė turėtų tokį patį raktą, kaip kad nurodyta leidime. Paskutinės kategorijos leidimai suteikiami OS gamintojo programėlėms. Visos leidimų grupės patvirtinimus gauna programėlės įdiegimo metu ir išlieka visą programėlės gyvavimo laiką.

Naujesni modeliai (pvz. Gooogle android 4) gali pasigirti tokiu funkcionalumu, kaip šifravimo palaikymas. Tačiau bendruoju atveju android operacinės sistemos vartotojai turi aukštą tikimybę parsisiųsti kenksmingą programinę įrangą ar prarasti duomenis kitais būdais.

Windows phone

Tai „Microsoft“ korporacijos sukurta operacinė sistema, skirta išmaniesiems telefonams bei kitiems mobiliesiems įrenginiams Ši „Windows mobile“ pasekėja išleista ganėtinai nesenai, tik 2010 metų Lapkričio mėnesį. Su pirmtake visiškai nesuderinama.

Ši operacinė sistema, panašiai kaip Android, užtikrina saugą savo zonoje (angl. sandboxing) kiekvienai programai atskirai. Instaliuojant naują programą vartotojui leidžiama pasirinkti patikimumo kategorijas. Privilegijuota kategorija leis veikti programai be jokių apribojimų. „Normali“ kategorija ribos prieigą prie nurodytų failų ir kitų programų. ‚Blokuota‘ kategorija neleis programai veikti. [4]

Microsoft išduoda sertifikatus, kai mobiliųjų programų projektuotojai prisiregistruoja prie VeriSigh. Kiekviena vartotojui išduodama programa turi būti pasirašyta galiojančiu parašu. [7] Tačiau yra galimybė įdiegti sertifikatus ir patiems mobiliųjų įrenginių vartotojams: instaliuojamas SDKCerts.cab failas ir programoms galima suteikti kokias tik norima teises. Tačiau tai taipogi atveria didžiulę saugumo spragą, nes esant įdiegtam SDKCerts.cab failui programišiai taipogi gali pasinaudoti juo ir vartotojui nežinant suteikti teises bei įdiegti programas sistemoje [8].

OS naudoja Internet Explorer Mobile naršyklę. Nuo Windows phone 8 naudojama internet Explorer 10 versija, kuri užtikrina šiek tiek saugesnį naršymą, pvz „SmartScreen“ filtras, kuris turi blokuoti pavojingus puslapius bei atpažinti kenkėjišką programinę įrangą.

Dažniausiai MĮ autentifikaciją atliekama vieno PIN kodo pagalba. Windows mobile sistemoje, vartotojui pasirinkus, galima sudaryti papildomą PIN kodą SIM kortelei, be kurio nepavyks išimti kortelės iš telefono bei atlikti skambučių [4]. Šioje operacinėje sistemoje taipogi galima įjungti nustatymą, kad PIN kodas turi būti įvedamas kiekvieną kartą po kiekvieno pristabdymo (ang. stand-by).

Nagrinėti operacinę sistemą galima turint visual studio profesional paketą arba naudojant Airscanner PowerTools ar SKTools, FlexWallet programinę įrangą.

2.1.2. Asmeninių mobiliųjų įrenginių programėlių pažeidžiamumai

Egzistuojant mažiems skaičiavimų ištekliams MĮ, negalima pritaikyti įprastų kompiuterių apsaugos priemonių, nes mobilieji įrenginiai taptų neveiksnūs [4]. Didžiausią grėsmę MĮ prieinamumui, bei informacijos vientisumui bei konfidencialumui kelia tikslingos programišių atakos, komunikacijų perėmimas bei kenkėjiška programinė įranga.

Kenkėjiška programinė įranga

Dar nei viena mobiliųjų įrenginių OS neatsilaikė prieš joms sukurtas kenkėjiškas programas. Kenkėjiškos programos gali prieiti prie žinučių, skambučių, GRPS, baterijos nustatymų, saugomos informacijos ir pridaryti materialinių bei finansinių nuostolių. ([9], [10])

Naujos programėlės, tokios kaip Java MIDlets bei kitos mažos java programėlės gali būti parsisiųstos per žiniatinklį arba įdiegtos per infraredą ar Bluethooth. Netgi ne java pagrindu sukurtos programos dažnai prašo priėjimo prie JSR [11], kas leidžia atsirasti papildomam funkcionalumui, pavyzdžiui, sudaryti sąlygas multimedijų API, asmeninės informacijos valdymo API [12], Dokumentų valdymo API ir kitoms.

Naujesnės Java versijos leidžia pasiekti SIM kortelės informaciją ar net nustatyti artimiausią tinklo bokštą, taip sužinodamas kur MĮ savininkas yra. Tokiu būdu vartotojas gali gauti daug patogių funkcijų, kaip kad navigacija, mobilusis apsipirkimas, orai konkrečiai vietovei ir panašiai. [12] Tačiau tokiu būdu gali būti sukeltos ir įvairios atakos, pavyzdžiui SMS trojanų ataka. Tokios atakos veikimo principas: jar tipo archyvas turi keletą klasių failų, kurie siunčia mokamas sms žinutes. Kiti failai naudojami trojano tikrosios prigimties slėpimui. Pvz.: vartotojui pateikiamas klausimas ar jis nori peržiūrėti tam tikrų nuotraukų albumą ir kiekvieną kartą paspaudus „taip“ išsiunčiama sms žinutė. [9] Vartotojas patiria ne tik informacijos praradimą, bet ir finansinius nuostolius.

Efektyviausias būdas išvengti java pagrindu veikiančių programėlių keliamų grėsmių – saugos zonos ([13], [14]) patikimų programėlių įdiegimas bei e-saugos politikos sudarymas. Efektyvi saugos politika turi atsižvelgti į naudotojo elgsenos niuansus, priėjimą prie MĮ bei tinklo, duomenų laikymą bei priėjimą bei komunikaciją su kitais įrenginiais. Skirtingos MĮ operacinės sistemos turės skirtingus būdus kaip visa tai kontroliuoti.

Tiesioginės programišių atakos

4 simbolių PIN kodas gali būti nulaužiamas per keletą sekundžių, kita vertus 16 simbolių slaptažodžio atskleidimas gali užtrukti tūkstančius metų. Tačiau pastebima tendencija, kad dauguma vartotojų netgi nepasikeičia gamintojo nustatyto slaptažodžio arba naudoja klasikines lengvai atspėjamas kombinacijas [8] PIN nulaužimui taipogi galima panaudoti jėgos (ang. Brute force) metodu ar tiesiog išnaudoti MĮ OS paliktomis saugumo spragomis.

Prie įrenginio taipogi galima prieiti pasinaudojant elektromagnetinių bangų ataką [15], Bluetooth atakas [1], DOS ar MMS atakas [8].

Komunikacijų perėmimas

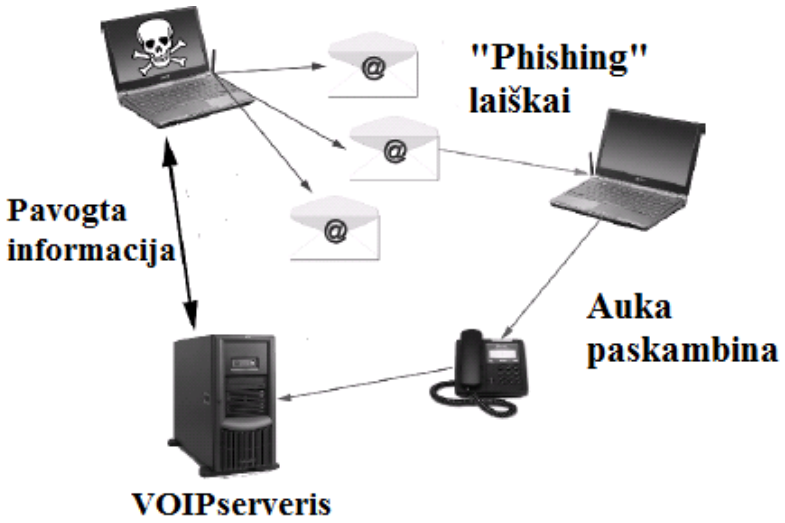
Smobile atlikti tyrimai atskleidė, kad perėmus aukos komunikacijas, galima lengvai sužinoti aukos vedamus vartotojų vardus bei slaptažodžius ar netgi bankinės sistemos kodus. Tam tereikia pasinaudoti tokiomis programomis kaip SSLstrip (HTTP komunikacijos nuskaitymas), Ettercap, webspy ar Wireshark [4]. Žinoma, jei auka būtų naudojęs antivirusinę ir ugniasienės programas, bei nustatęs šifravimo rėžimą, programišius negalėtų pasinaudoti ar netgi perimti duomenų.

2.1.3. Asmeninių mobiliųjų įrenginių saugomos konfidencialios informacijos pažeidžiamumai

Kita kategorija veiksnių, keliančių saugos problemas – vartotojo veiksmai. MĮ naudotojus galima apgauti, kad jie savanoriškai pasidalintų savo turima informacija, MĮ naudotojai dažnai išjungia ar įjungia įvairius MĮ nustatymus dėl naudojimo patogumo ar žinių stokos. MĮ įrenginiai taipogi gali būti pamesti ar pavogti.

Duomenų vagystės bei socialinė inžinerija

Vis dažniau pasitaiko atvejų kai sukčiautojai išsiunčia žinutę/e-laiškus tūkstančiams gavėjų su apgaulinga URN nuoroda ar telefono numeriu, kuriuo prašoma paskambinti. Paskambinus, prašoma pateikti savo asmeninę informaciją, kuri vėliau panaudojama sukčiautojų tikslais. Pažangesni sukčiautojai vis dažniau savo tikslams panaudoja VOIP paslaugų funkcionalumą (2.3 pav.). Vienintelis būdas apsisaugoti nuo socialinės inžinerijos atakų yra darbuotojų mokymai, paaiškinant klasikinius tokio scenarijaus požymius.



2.3 pav. Socialinės inžinerijos pavyzdys, panaudojant e-pašto ir VOIP serverio funkcionalumą

Integracija su kitomis sistemomis

MĮ gali sąveikauti su kitomis sistemomis. Vienas pavyzdžių būtų MĮ jungimasis prie kompiuterio per laidą tam, kad MĮ būtų įkrautas ar būtų galima sinchronizuoti. Kitas pavyzdys – automatiniai atsarginių kopijų darymai ir patalpinimas debesyje ar įmonės serveryje. Kai visos sąveikaujančios pusės yra kontroliuojamos įmonės, didelių grėsmių nekyla, tačiau dažniai viena iš pusių būna asmeniniai ar net trečiųjų šalių įrenginiai. [8]

Taikant MĮ valdymo sistemas galima uždrausti įmonės išduotiems įrenginiams atlikti sinchronizaciją su sąrašuose nesančiais įrenginiais. Taipogi galima uždrausti nuotolinių atsarginių kopijų paslaugos naudojimą.

Pavogti ar prarasti MĮ

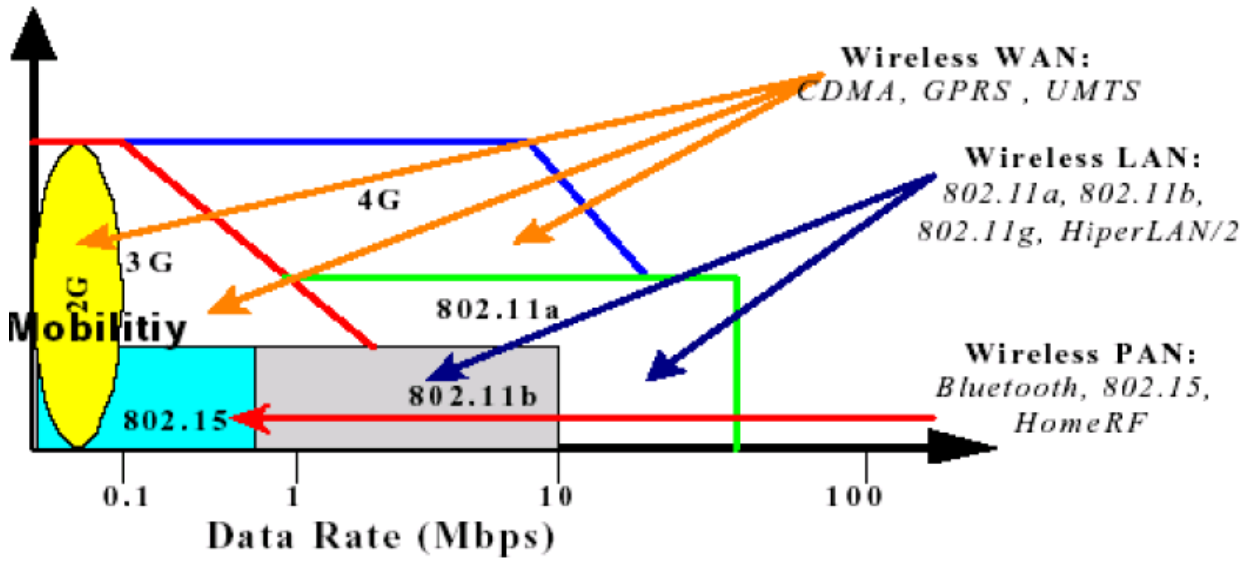
Tyrimai rodo, kad kiekvienas saugos pažeidimas UK kainuoja apie 47£ ir daugiau nei 36 % saugos pažeidimų įvyksta dėl prarastų ar pavogtų įrenginių. Virš 80% verslininkų laiko įrenginiuose jautrią informaciją arba netgi gali prieiti nuotoliniu būdu prie įmonės tinklo. 2010 metais CIO.com atliktas tyrimas atskleidė, kad Niujorko mieste per 6 mėnesių laikotarpį taksi mašinose buvo pamiršti 31544 mobilieji įrenginiai [4]

Naudotojo veiksmai

Darbuotojų elgesys dažnai sukelia saugos pažeidžiamumus. 2009 metais atliktas tyrimas rodo kad 15% didelių saugos pažeidimų yra sukelti vidinių vartotojų. [2] Vartotojas gali būti neatidus, nesusipažinęs su saugos taisyklėmis ar tikslingai jas pažeidinėti. Šitoks elgesys ypatingai aktualus kai vienas įrenginys naudojamas tiek darbui, tiek asmeniniams poreikiams. Tokių situacijų pavyzdžiais galėtų būti ugniasienės išjungimas, užkrėstų programėlių parsisiuntimas iš žiniatinklio, socialinių tinklų naudojimas, konfidencialios informacijos dalinimasis ir kt.

Tinklo pasirinkimas

Tinklo ir tinklo nustatymo pasirinkimas gali atverti duris arba užkirsti kelią įsilaužėliams bei informacijos nutekėjimui. Panagrinėkime atidžiau **2.4** pav. matomus ryšius: WLAN, WWAN ir bluetooth [16].



2.4 pav Belaidžių ryšių apžvalga

Belaidis vietinis tinklas (ang. WLAN) WLAN tinkluose naudojamas IEEE (Institute of Electrical and Electronics Engineers) pasirinktas dažnis IEEE 802.11, kad būtų lengviau atskirti duomenų perdavimo greitį ir dažnį, prie jo nurodoma papildoma raidė. Skiriami tokie dažniai: 802.11b, 802.11g, 802.11a, 802.11n konkrečiai, dabar dažniausiai naudojamas WLAN tinkluose. WLAN nuo 1999 metų buvo šifruojamas WEP standartu. Laikui bėgant šio algoritmo veikime buvo surastos kritinės spragos, leidžiančios parinkti tinklo slaptažodį per labai trumpą laiką– dėl to įsilaužėliai gali be didesnio vargo patekti į tinklus apsaugotus WEP šifravimu. WEP turi dviejų rūšių autentifikavimą: atvirą (angl. Open system) arba bendro rakto (angl. Shared-Key). Tiesa, atviras nėra autentiškumo procedūra, nes tada prieigos taškas (angl.Access point) priima kiekvieną stotelę be tapatybės patikrinimo. Taigi, stotis pasikeičia su prieigos tašku dvejomis žinutėmis, kurių viena nurodo tapatybę, kita prašymą patvirtinti. Prieigos taškas atsako, patvirtindamas sėkmingą autentifikaciją. Po atpažinimo ir susiejimo, WEP gali būti naudojamas duomenų šifravimui, tada klientui reikia turėti atitinkama raktą. Bendro rakto autentifikacijai prisijungimui reikia slapto rakto. Šiuo atveju, autentiškumui pasiekti, stotis pradeda keturių krypčių pranešimų keitimąsi. [16]

WPA (ang. WiFi Protected Access) yra šifravimo mechanizmas, skirtas pakeisti pasenusį WEP šifravimą. WPA naudoja saugesnį TKIP protokolą, kurio pagrindas yra tas pats RC4 šifras, tačiau skirtingai nei WEP atveju saugumui užtikrinti naudojamas 128 bitų raktas, dinamiškai generuojamas kiekvienam atskiram paketui. 2008-2009 metais buvo pademonstruotos kelios atakos, leidžiančios pagreitinti WPA rakto parinkimo procesą, todėl WPA yra laikytinas nesaugiu. Autentifikavimui naudojamas 802.1X autentifikavimo protokolo mechanizmas arba iš anksto padalintų raktų metodas (angl. Pre-Shared Key – PSK), kuris skirtas bevielio ryšio sesijų metu identifikavimo raktams kurti. PSK numatytas naudoti mažuose namų arba ofisų tinkluose, kuriuose kritiškas autentifikavimas nėra svarbus [17]. Duomenų vientisumui tikrinti CRC algoritmą pakeitė MIC (angl. Micheal) algoritmas (64 bitų žinutė). CRC algoritmas, naudotas 802.11 protokole yra nesunkiai apeinamas. MIC algoritmas šiuo atveju yra žymiai stipresnis. Duomenų teisėtumo procedūros tikrina duomenis nuo žalingų bei atsitiktinių duomenų perdavimo iškraipymų. 802.1X (WPA - verslo) kur kas saugesnis nei PSK, tačiau tam reikia turėti RADIUS autentifikavimo serverį [16].

WPA2 yra WPA šifravimo mechanizmo tęsinys, kurio esminis skirtumas yra patikimesnio šifravimo algoritmo CCMP (dar kartais vadinamo AES) naudojimas vietoje TKIP. Nuo 2006 metų visi sertifikuoti Wi-Fi įrenginiai privalo palaikyti WPA2 šifravimą. Konfidencialumui bei

vientisumui užtikrinti WPA2 naudoja skaitiklio rėžimą su CBC-MAC protokolu (angl. Counter-Mode/Cipher Block Chaining – CCMP). Šifravimui ir duomenų vientisumui CCMP naudoja AES šifrą su 128 bitų raktu ir 128 bitų bloko dydžiu. Vientisumui užtikrinti, CCM-MAC operacijos išplečia pradinį MPDU dydį iki 16-8 baitų CCMP antraštei ir 8 baitų MIC laukui. CCM reikalauja naujo laikino rakto kiekvienai sesijai ir unikalios reikšmės kiekvienam kadrui. Šiam tikslui naudojamas 48 bitų paketas. CCM nenaudoja WEP kontrolinių sumų mechanizmo (ICV). CCM apsaugo papildomus autentiškumo duomenis, kurie sudaryti iš MPDU antraštės ir apima polaukius iš MAC kadro kontrolės, šaltinio adresus ir paskirties laukus, sekos kontrolę, QoS kontrolės lauką, todėl užtikrinama didesnė vientisumo apsauga. Autentifikavimui naudojamas 802.1X autentifikavimo protokolo mechanizmas arba iš anksto padalintų raktų metodas PSK. Šiuo metu nėra žinoma atakų, leidžiančių pagreitinti WPA2 rakto parinkimą, tačiau tinklo saugumas priklauso nuo naudojamo rakto sudėtingumo. Rekomenduojama rinktis WPA2 šifravimą, nurodant gerą slaptažodį [18].

2.3 lentelėje matome WEP, WPA ir WPA2 saugos protokolų palyginimą.

2.3 lentelė Wi-Fi saugumo protokolų palyginimas

	WEP	**WPA**	**WPA2**
Tikslas	Užtikrinti apsaugą panašią į laidinių tinklų.	Ištaisyti WEP problemas be techninės įrangos pakeitimų. Realizuota didžioji dalis IEEE 802.11i standarto.	Pilnai remtasi IEEE 802.11i standartu. Patobulintas lyginant su WPA
Šifravimas	Rivest Cipher 4 (RC4)	Laikino rakto vientisumo protokolas (TKIP)	AES-CCM su 128 bitų laikinu raktu.
Autentifikacija	WEP- atviras ir WEP-bendras	WPA-PSK(angl. Pre-Shared Key) ir WPA-verslo	WPA2-asmeninis ir WPA2-verslo
Duomenų vientisumas	CRC-32	Michael (angl. Message Integrity Code (MIC))	Cipher block chaining message authentication code (CBC-MAC)
Rakto valdymas	nėra	Suteikiamos raktų kūrimo/valdymo galimybės. Raktai sugeneruojami per keturis patvirtinimus tarp prieigos taško ir serverio.	Suteikiamos raktų kūrimo/valdymo galimybės. Raktai sugeneruojami per keturis patvirtinimus tarp prieigos taško ir serverio.
Techninės įrangos suderinamumas	Veikia su visa technine įranga	Veikia su visa technine įranga, po programinės įrangos atnaujinimų.	Palaiko Wi-Fi įrenginius sukurtus po 2006.
Diegimo sudėtingumas	Lengvai konfigūruojamas	Sudėtingesnis konfigūravimas WPA-verslo daliai	Sudėtingesnis konfigūravimas WPA2-verslo daliai

Bevielis kompiuterinis tinklas (ang. WWAN). Nuo WLAN skiriasi tuo kad naudoja tokias mobiliojo ryšio technologijas kaip LTE, WiMA, UMTS (angl. *Universal Mobile Telecommunication System*), GSM, MOB ITEX. 2G WAN ryšys palaiko nuo 9.6 Kbps iki 348 Kbps greitį. 3G ryšys dar greitesnis ir gali palaikyti nuo 144 Kbps iki 2Mbps. Kadangi radijo bangomis paremtos komunikacijos nepalaiko fizinės ryšio apsaugos, WWAN ryšys dažnai yra šifruojamas, vartotojai autentifikuojami. Tačiau kai kurios GSM šifravimo technologijos ganėtinai lengvai nulaužiamos, todėl saugos specialistai nelaiko šio ryšio saugiu [17].

Bluetooth - technologija, naudojanti radijo ryšį trumpais atstumais. Bluetooth gali turėti tris saugumo lygius. Pirmasis lygis netaiko jokių saugumo funkcijų. Antrasis lygis įjungia saugumo nustatymus po ryšio sukūrimo ir trečiasis lygis įjungia saugumo nustatymus prieš ryšio sukūrimą. Įrenginiai gali būti skirstomi į nepatikimus bei patikimus, pastariesiems suteikiamos visos prieigos teisės. Labiausiai kenkėjiškų programėlių gamintojus žavi tai, kad pasinaudojant Bluetooth galima patekti į kito vartotojo įrenginį nesukeliant jokio įtarimo. Tokiu būdu kenksminga programinė įranga gali nuskaityti MĮ kaupiamą kontaktinę informaciją, SMS žinutes ar netgi atlikti skambutį. Kitas gana populiarus būdas skleisti kenkėjišką programinę įrangą Bluethooth pagalba – socialinė inžinerija. Vartotojui pasiūloma įsidiegti populiarų funkcionalumą, jam sutikus, programėlė įdiegiama bei pradeda ieškoti kitų artimiausių įrenginių su įjungtu Bluetooth funkcionalumu, taip užtikrindama pastovų plitimą. [8]

Virtualus privatus tinklas (angl. Virtual Private Network, VPN) - atskirų nutolusių vienas nuo kito kompiuterinių tinklų sujungimas į vieną tinklą internetu. Virtualumas pasireiškia tuo, kad tinklas yra organizuojamas ne tiesiogiai, o per internetą. Privatumas - tuo, kad visas duomenų srautas VPN kanalu eina užkoduotas.

VPN naudojimo minusas, kad dažnai vartotojai neįjungia VPN naudojimo savo asmeniniuose įrenginiuose, tuo keldami papildomų grėsmių.

2.2. Asmeninių mobiliųjų įrenginių naudojimo atvejai organizacijoje

Tyrimai rodo jog vidutinis protinį darbą atliekantis darbuotojas darbe vienu metu turi 2,8 veikiantį įrenginį. Ir šis skaičius ateityje tik augs ([19], [20]) Didžiojoje dalyje tokių įrenginių vartotojas talpina ir asmeninę ir konfidencialią.

Prieinamą informaciją galima skirstyti į įslaptinimo lygius. Tą siūlo Bell-LaPadula (BLP) modelis. Šis modelis buvo sukurtas remiantis daugialypės saugos modeliu siekiant apsaugoti įslaptintą informaciją. Šis modelis naudojamas Jungtinių Amerikos Valstijų Gynybos ministerijoje (*DoD – Department of Defence*), kurioje informacija pagal slaptumą klasifikuojama į keturis lygius [21]:

YPATINGAI SLAPTA, labai slaptą (LS), (**TS**)
SLAPTA, slaptą (S), (**S**)
KONFIDENCIALU, Konfidencialų (K) (**C**)
NEKLASIFIKUOTA, neįslaptintą (N) (**UC**)

Pastaraisiais metais įstatymai, ginantys intelektinės nuosavybės teises versle, remiasi koncepcija, kad:

1) informacija turi būti slapta, prieinama tik tiems asmenims, kurie darbe tiesiogiai su ja dirba;
2) informacija turi turėti komercinę vertę, kad ji būtų laikoma slapta;
3) įmonės savininkas ar vadovas turi imtis atsakingų žingsnių, kad išlaikytų informaciją paslaptyje. [22]

Konfidenciali informacija - tai tokia informacija, kurią sužinojo asmuo, dirbantis įstaigoje pagal darbo sutartį arba teikiantis paslaugas pagal paslaugų teikimo sutartį, ir priklausanti įstaigai arba įstaigos užsakovams, kuri turi vertę dėl to, kad jos nežino tretieji asmenys ir negali būti laisvai jiems prieinama apie įstaigos darbuotojų sukurtus intelektinės veiklos produktus arba jų dalis, apie atliekamus tyrimus ir (arba) jų rezultatus, esamų arba potencialių tiekėjų ar kontrahentų sąrašus, darbuotojų atlyginimus ir darbo sąlygas, taip pat bet kokius kitus duomenis, susijusius su įstaigos vykdoma veikla bei informacija, kurią darbdavys laiko gamybine, technologine paslaptimi nepriklausomai nuo to, ar tokia informacija yra tiesiogiai įtraukta į darbdavio gamybinių arba technologinių paslapčių sąrašą, išskyrus tą informaciją, kuri yra viešai skelbiama. [22]

Konfidencialia informacija taip pat laikoma informacija apie trečiuosius asmenis arba susijusi su trečiaisiais asmenimis, kurią asmuo sužinojo atlikdamas savo darbo funkcijas pagal darbo arba paslaugų teikimo sutartį, sudarytą su įstaiga.

Kiekvienas darbuotojas, dirbantis su labai slapta, slapta ar konfidencialia informacija, prisiima atsakomybę šią informaciją identifikuoti, apsaugoti, tinkamai laikyti ir saugoti. Ir nors darbuotojui tenka atsakomybė išsaugoti konfidencialią informaciją, tačiau vadovas privalo aprūpinti darbuotoją reikiamomis priemonėmis [23]. Vadovai turi pasirūpinti, kad darbuotojų įrenginiuose būtų įdiegtos antivirusinės programos, neleidžiančios virusams sugadinti informacijos kompiuterio kietajame diske, atminties rakte, CD. Įmonės vadovas IT specialistui paveda sukurti laikinus slaptažodžius, suteikti prieigas prie slaptos informacijos bei įgyvendina kitas saugos priemones.

2.2.1. Asmeninius mobiliuosius įrenginius naudojančių darbuotojų kategorijos

Virš 3 bilijonų vartotojų naudojasi MĮ. Vartotojai pasiskirstę virš 200 skirtingų šalių ir naudoja apie 700 skirtingų mobiliųjų tinklų operatorių (GSMA). Vartotojų techniniai įgūdžiai labai skiriasi. MĮ naudojami visur ir visada. Nors techninės įrangos gamintojų kiekis taipogi nemažas, tačiau visai nedidelis MĮ operacinių sistemų pasirinkimas egzistuoja rinkose. Dėl OS tarpusavio panašumų programėlės taipogi panašios. [8]

Pats paprasčiausias MĮ vartotojų skirstymas būtų į išmaniųjų MĮ ir neišmaniųjų MĮ vartotojus. Tačiau pastaruoju metu net ir paprasčiausias telefonas gali prisijungti prie interneto, laikyti nuotraukas bei naudotis Java funkcionalumu.

Kitas populiarus vartotojų skirstymas į asmeninio pobūdžio vartotojus ir verslo vartotojus. Verslo pasaulyje viena iš metodikų taikomų užtikrinimui jog prie konfidencialios informacijos prieitų tik reikiami žmonės – rolėmis pagrįstas saugos valdymas.

Tokios rolės kaip bendrinių žinių ar laikini darbuotojai, įmonės svečiai ar netgi tam tikro lygio vadybininkai turėtų turėti griežtą kontrolę ir reikalauja sudėtingų autentifikacijos bei šifravimo sprendimų. Cisco [6] siūlomą verslo klientų skaidymą pagal roles galima matyti 2.4 lentelė **Galimų mobiliųjų rolių apibrėžimai**.

Pasitaiko, kad vienas vartotojas priklauso kelioms rolėms. Tokiu atveju rekomenduotina, jei tik įmanoma, naudoti griežtesnį taisyklių rinkinį turinčios rolės konfigūraciją.

2.4 lentelė Galimų mobiliųjų rolių apibrėžimai

Rolė	**Aprašymas**
Direktoriai (aukščiausi vadovai)	Aukščiausio lygio vadovai, kurie prieina prie visos svarbiausios ir jautrios įmonei informacijos: sutartys, strategijos, produktų informaciją ir t.t. Ypatingo jautrumo jų laikoma kontaktinė informacija bei laiškai. Šitos rolės vartotojai, nori visada galėti prieiti prie informacijos ir ja laisvai manipuliuoti. Dėl plataus informacijos matomumo šios rolės vartotojų įrenginiai turi būti ypač stipriai apsaugoti. .
Vadybininkai	Šitie žmonės prieina prie darbuotojų informacijos bei nemažos dalies intelektinės nuosavybės dokumentų.
Administracinio pobūdžio darbuotojai	Šiam skyriui priskirtume tokius darbuotojus: personalo skyriaus specialistas, buhalteris, teisininkas. Šio skyriaus darbuotojai gali prieiti prie jautrių darbuotojų duomenų, už kurių paviešinimą baudžiama įstatymo. Taipogi prieinama prie įmonės apskaitos informacijos. Šios rolės saugumas turėtų būti užtikrinamas kaip ir vadybininkų.
Bendrinio pobūdžio darbuotojai	Nuo priklausomo darbo pobūdžio, gali prieiti tik prie dalies informacijos. Tačiau mėgsta naudotis asmeninės informacijos valdymo įrankiais
Judrūs darbuotojai (angl. field workers)	Daliai darbuotojų gali reikėti dirbti ne tik darbo vietoje bet ir pas klientus ar iš namų. Jų MĮ tikrai rasime jautrios informacijos. Tad šiems darbuotojams reikalinga atitinkamos saugos taisyklės.
Kontraktoriai/laikini vartotojai	Kontraktoriai bei kiti patikimi asmenys, gali turėti priėjimą prie kompanijos informacijos, tačiau jiems turėtų būti taikoma kitokios kontrolės ir saugos politikos taisyklės nei įprastiniams darbuotojams.

2.2.2. Darbuotojų veiksmai su asmeniniais mobiliaisiais įrenginiais

Mobiliuosius vartotojus pagal jų atliekamus veiksmus su įrenginiais būtų galima skirtyti pagal tai ar įrenginys

- Naudojamas tik komunikacijai
- Naudojamas vietoj kompiuterio

Jei vartotojas naudoja MĮ tik komunikacijai, tai jame netūrėtų būti nuotraukų, dokumentų ir panašiai. Tačiau netgi tokiu atveju, turime kontaktinę informaciją, skambučių istoriją, trumpąsias žinutes – informaciją, kuri gali dominti sukčiautojus.

Kita vartotojų grupė laikys pilnai aprašytą kontaktinę informaciją, kurią gali sudaryti be telefonų numerių ir vardų, dar ir e- pašto adresai, gyvenamųjų vietų adresai ir pnš. Toks vartotojas taipogi turės pilnai naudojamą kalendoriaus funkcionalumą bei automatinį priėjimą prie e-pašto paslaugos. Verslo klientų MĮ tikėtina, kad turės prisijungimą prie darbo tinklo per VPN bei įrenginyje laikys su darbu susijusią informaciją. [8]

2.2.3. Darbuotojų kategorijų ir galimų veiksmų sąryšis

Cisco rekomenduojamas pradinis taisyklių rinkinys, atsižvelgiant į darbuotojų roles, matomas lentelėje 2.5. Lentelės naudojamų ženklų reikšmės nurodytos lentelėje 2.6 Nors Cisco taisyklių rinkinys padengia labai mažą dalį MĮ saugaus valdymo funkcionalumo, galima matyti, kad daugiau atsakomybės įmonėje nešantys darbuotojai turi turėti stipresnius saugos nustatymus.

2.5 lentelė Cisco siūlomas taisyklių rinkinys atsižvelgianti į roles

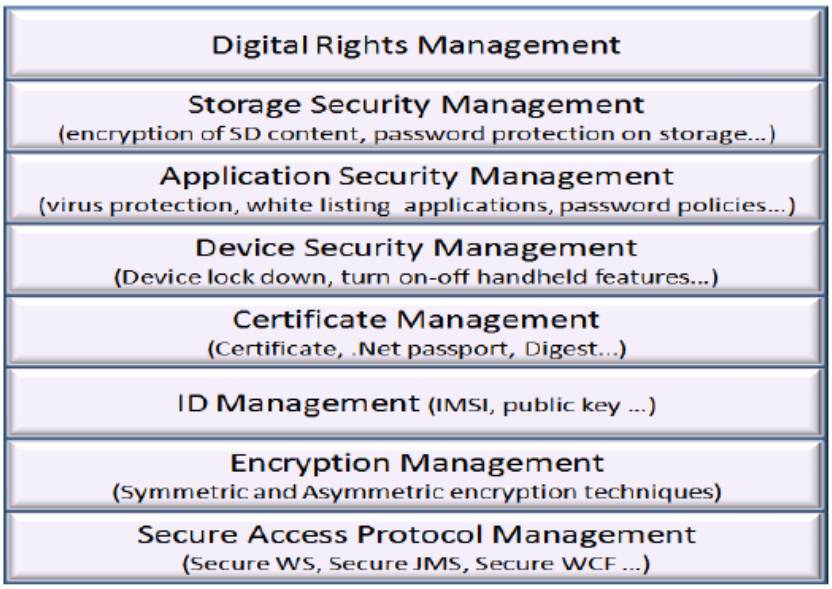
	Įrenginio šifravimas	**Keletos tipų autentifikavimas**	**Sudėtingi slaptažodžiai**	**Duomenų filtravima (DLP)**	**E-laiškų priedų atidarymas**	**Ne tinklo radio ryšio naudojimas**	**Ryšio šifravimas**
Rolės							
Direktoriai	•	•	•	✓	•	•	•
Vadybininkai	•	✓	✓	•	•	•	•
Administracinio pobūdžio darbuotojai	•	•	•	•	•	•	•
Bendrinio pobūdžio darbuotojai	✓	•	•	•	•	•	•
Judrūs darbuotojai	•	•	•	✓	•	•	•
Kontraktoriai/laikini vartotojai	✓	•	•	✓	•	•	✓

2.6 lentelė Taisyklių privalomumo ženklų reikšmės

•	Privaloma
✓	Rekomenduotina
•	Galima

2.3. Asmeninių mobiliųjų įrenginių konfigūravimas ir valdymo automatizavimas

Prieš atliekant įmonėje pakeitimus, būtina susidaryti įmonės saugos politiką. 2.5 Pav. demonstruoja mobiliosios saugos lygius, kuriuos įmonės reiktų apsvarstyti diegiant Mobilios saugos politiką įmonėje. Rinkoje yra produktų, kurie gali patenkinti vieną ar daugiau lygių, tačiau kai kuriam funkcionalumui gali reikėti atskirų programavimo darbų. [1]



2.5 pav. Mobilios saugos platforma

Atsižvelgiant į 2.1.1 skyriuje išvardintus saugos ir valdymo kriterijus ir 2.5 pav. siūlomus lygius , išnagrinėkime galimus konfigūracijos nustatymus norint užtikrinti MĮ saugią ekosistemą.

a) Autentifikacija

Tai būdas užtikrinti, kad tik autorizuoti vartotojai prieis prie sistemų ar įrenginių. Autentifikacija gali būti atlikta atsižvelgiant į tris faktorius:

- Ką vartotojas žino
- Ką vartotojas turi
- Kas yra vartotojas

Vartotojo žiniomis paremta autentifikacija naudoja naudotojo vardus, slaptažodžius bei PIN kodus. Vartotojo nuosavybe paremta autentifikacija dažniausiai tikisi prieigos rakto, kuris gali sugeneruoti kodo seką, kuri turi sutapti su įrenginio. Vartotojo esybe paremta autentifikacija tikisi tam tikrų biologinių duomenų: piršto atspaudo, rainelės nuskenavimo ar veido atpažinimo.

Vienas dažniausių autentifikacijos būdų – slaptažodžių naudojimas. Kadangi paprastus slaptažodžius galima nulaužti labai lengvai ir greitai, įmonės politika turi reikalauti vartotojus naudoti sudėtingus slaptažodžius [8] 2.7 lentelėje matome slaptažodžių pavyzdžius ir jų skirstymą į tipus.

2.7 lentelė Slaptažodžių klasifikacija

Tipas	Apibūdinimas	Pavyzdys
Paprastas	Pasikartojančios, didėjančios ar mažėjančios reikšmės	1111, 1234, 9876, xyz
Skaitiniai simboliai	Reikalauja nors vieno skaičiaus	184, 1058, xyz1
Skaitiniai ir raidiniai simboliai	Reikalauja nors vienos skaičiaus ir nors vienos raidė	184a, vaid1a
Sudėtingas, alfabetinis su specialiaisiais ženklais	Reikalauja nors vienos skaičiaus, nors vienos raidės ir vieno specialiojo simbolio	Tjk1#, wng?45P
Sekos šablonas	Android MĮ OS leidžiama užrakinti/atrakinti įrenginį braukiant ant liečiamojo ekrano tam tikrą sutartą šabloną.	

b) Įsibrovimo aptikimo sistemos

Įsibrovimo aptikimo sistemos gali būti panaudotos apibrėžti ‚normalius' sistemos bei programų veikimo požymius ir tuo remiantis nustatyti nukrypimus nuo normos. IDS sistemos gali atpažinti kenksmingą kodą, riboti skambučius, atpažinti kenksmingą programinę pagal CPU, baterijos ar atminties resursų išnaudojimą. Android OS vartotojai gali įsidiegti ‚Andromaly' ir ‚DroidHuenter' įsibrovimo aptikimo programas. [4]

c) Ugniasienės

Ugniasienės gali užkirsti kelią neautorizuotai prieigai prie MĮ bei konfidencialios informacijos nutekėjimui per tinklo įrenginius. Taigi net jeigu į įrenginį pateko kenkėjiška programa ir mėgina siųsti konfidencialią informaciją, ugniasienė gali tam užkirsti kelią. Jei nėra spragų MĮ operacinėje sistemoje, ugniasienė taipogi užkirs kelią kenkėjiškos programos diegimui. Tačiau ugniasienės negali užkirsti kelio jei kenkėjiška programa pasiekė MĮ per SMS ar MMS žinutes. Smobile siūlo ugniasienes Windows Mobile bei IOS operacinėms sistemoms. Android OS MĮ gali naudotis Netfilter/iptables programine įranga. [4]

d) Antivirusinės programos

Antivirusinės programos gali nuskenuoti MĮ ir surasti vietas kurios gali laikyti kenkėjišką kodą. Šios programos gali skenuoti ne tik egzistuojančius failus, bet ir atsisiunčiamus failus ir priedus. Antivirusinės programos efektyviai apsaugos nuo MMS atakos. [8]

Symantec, Kaspersky bei MCAfee turi antivirusines programas Windows mobile OS įrenginiams.

e) **Kontekstinė prieigos kontrolė**

Šitokia kontrolė gali užtikrinti, kad konfidenciali informacija vartotojui bus pasiekiama tik jeigu bus tenkinamos specifinės sąlygos, pvz: vietos, laiko, prisijungimo tipo. [8]

f) Programėlių atnaujinimai

Jei MĮ įrenginys palaiko programėlių atnaujinimus, šis funkcionalumas turėtų būti visą laiką įjungtas ir atnaujinimai iškart diegiami vos jiems pasirodžius.

g) **Nuotolinio valdymo sistemos**

Nuotolinio valdymo sistemos gali padėti aptikti problemas MĮ, analizuoti juos bei atlikti koreguojamuosius veiksmus. Šios sistemos gali įdiegti antivirusines programas, užtikrinti jog VPN naudojamas teisingai, uždrausti failų parsisiuntimus. Jei MĮ prarandamas galima atlikti įrenginio duomenų išvalymą ar netgi išjungti įrenginį. Nuotolinio valdymo sistemos kartu su ugniasienėmis bei kontekstine prieigos kontrole gali užtikrinti efektyvią apsaugą MĮ. Šio metodo naudojimo minusas- reikalingi darbuotojų resursai, sistemos proceso stebėjimui bei sprendimų priėmimui. [4]

h) **Skaitmeniniai parašai bei sertifikatai**

Skaitmeninis parašas - kodas, paprastai susiejamas su prasmine informacija ir leidžiantis tą informaciją autentifikuoti, t. y. susieti ją su skaitmeninę tapatybę turinčiu asmeniu arba įrenginiu. [4]

Skaitmeninis parašas dažniausiai realizuojamas asimetrinės kriptografijos pagalba ir jo panaudojimas paremtas viešojo rakto kriptografija, kas leidžia:

- identifikuoti pasirašiusįjį (kas pasirašė?)
- užtikrinti, kad informacija nebuvo pakeista po pasirašymo (kas pasirašyta?)

Skaitmeninis sertifikatas - tai elektroninis paso, vairuotojo pažymėjimo arba nario kortelės atitikmuo, kurio pagalba Jūs galite įrodyti savo asmens tapatybę arba teisę prieiti prie Jums reikalingos informacijos internete.

Skaitmeninių sertifikatų veikimas yra paremtas kodavimo viešuoju raktu technologija, kai naudojama vienas kitą papildančių raktų pora - asmeninis ir viešasis. Jie gali funkcionuoti tiktai tada, kai jie naudojami kartu. Viešasis raktas perduodamas asmenims, su kuriais palaikomi kontaktai, o asmeninį raktą saugo sertifikato savininkas. Bet koks pranešimas, užšifruotas asmeninio rakto pagalba, gali būti iššifruotas tiktai tos pačios raktų poros viešuoju raktu. Ir atvirkščiai, jeigu siunčiama informacija yra užšifruota viešuoju raktu, ją gali iššifruoti tik tos pačios raktų poros asmeninis raktas. Dėl to asmeninis raktas turi būti labai gerai apsaugotas.

Taip pat naudojant skaitmeninį sertifikatą yra galimybė patikrinti vartotojo teises į konkretų raktą - tai užkerta kelią neteisėtam asmeninio rakto naudojimui.

Skaitmeninį sertifikatą sudaro ir skiria sertifikavimo paslaugas teikianti organizacija (Certification Authority - CA), pasirašanti savo privačiu raktu. Ji taip pat teikia sertifikatų duomenis parašo naudotojams elektroniniams parašams tikrinti.

Paprastai skaitmeninis sertifikatas susideda iš:

- Savininko viešo rakto
- Savininko vardo
- Viešo rakto galiojimo termino

- Skaitmeninį sertifikatą teikiančios organizacijos (CA) pavadinimo
- Skaitmeninio sertifikato serijinio numerio
- Sertifikatą teikiančios organizacijos skaitmeninio parašo.

i) Saugumo zonos (Sandboxing)

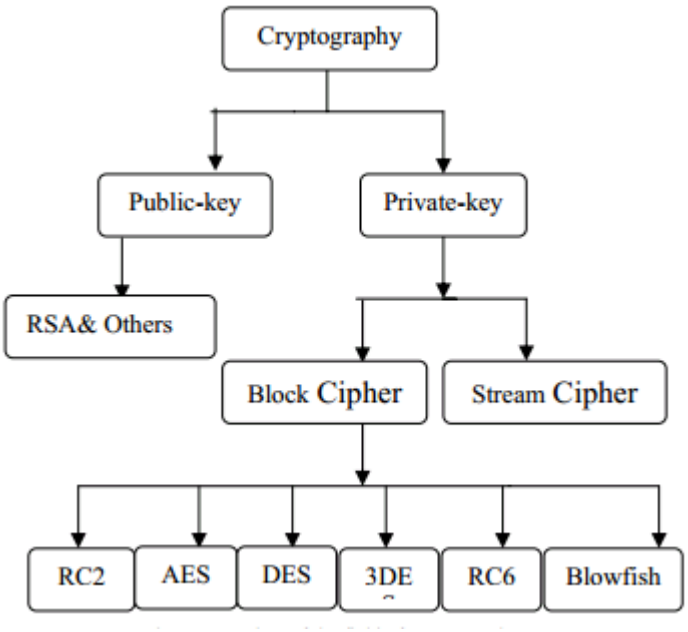
Saugumo zonos užtikrina, jog programos kodas negalės prieiti prie kitų programų ar duomenų bei paveikti pačios MĮ operacinės sistemos. MĮ kurie užtikrina saugumo zonų egzistavimą gali efektyviai apsaugoti nuo kenkėjiškos programinės įrangos. Pavyzdžiui, jei įprastame kompiuteryje iš naršyklės vykdomas kenkėjiškas kodas gali pakenkti visai kompiuteriu sistemai, Android OS šis kodas gali paveikti tik pačią naršyklę. [2]

j) Šifravimo algoritmai

Duomenų šifravimas (angl. encryption) - duomenų pavertimas nesuprantamais, kol jie nebus iššifruoti atitinkamu būdu. Duomenų šifravimas yra svarbus MĮ, nes jie dažnai pametami ar pavagiami, taipogi lengvai nulaužiami programišių.

Pav. 2.6 pavaizduoti kriptografinių metodų tipai. Matome jog, šifravimo metodai visų pirma skirstomi į [24]:

a. simetrinius (privatus raktas),
b. asimetrinius (viešojo ir privataus rakto pora).



2.6 pav. Kriptografinių metodų tipai

Simetrinio šifravimo metode generuojamas vienas šifravimo raktas. Jį gauna du asmenys - duomenų siuntėjas ir gavėjas. Duomenims užšifruoti prieš siunčiant ir gautiems užšifruotiems duomenims iššifruoti yra naudojamas tas pats šifras (raktas). Metodas naudojamas duomenų konfidencialumui užtikrinti, t.y. kai norima apsisaugoti nuo duomenų atskleidimo tretiesiems asmenims.

Simetrinio šifravimo metodo privalumas yra tas, kad duomenų užšifravimas ir iššifravimas vyksta greitai. Trūkumais galima laikyti tai, kad šifrą žino du asmenys, todėl ginčo atveju sunku įrodyti, kuris asmuo neteisus. Be to, šifrui perduoti du asmenys turi susitikti betarpiškai arba naudoti kitokius saugius perdavimo būdus.

Simetrinių šifravimo algoritmų pavyzdžiai [24]:

DES – tai buvo pirmasis šifravimo standartas pripažintas NIST (Nacionalinio standartų ir technologijos instituto). Duomenys skaidomi 64 bitų blokais, rakto ilgis taipogi 64 bitai.

3DES naudojamas kaip stipresnė DES algoritmo alternatyva. Jis yra padarytas pagal DES algoritmo schemą ir atgalinė jo schema yra suderinama su tikruoju DES algoritmu. Pagerinimas yra tas, jog kiekvienas 64 bitų blokas yra užšifruojamas tris kartus, naudojantis DES algoritmu panaudojant tris skirtingus raktus. Triple DES užšifruoja kiekvieną bloką pirmu raktu, tada iššifruoja rezultatą naudodamasis antru raktu ir galų gale užšifruoja vėl panaudojant trečią raktą. Tačiau, kaip galima pastebėti, algoritmo veikimo laikas praktiškai pailgėja tris kartus lyginant su DES algoritmu.

RC2 kriptografinis algoritmas yra simetrinis blokinis šifras, naudojantis 64 bitų įėjimo duomenų bloko dydį. Šis algoritmas kurtas tam, kad būtų pagerintas DES algoritmo veikimo laikas. Be šio pagerinimo buvo gautas kiek saugesnis užšifravimo algoritmas, kadangi jis naudoja kintamo dydžio raktą (nuo vieno iki 128 baitų).

Blowfish yra nepatentuotas, nemokamas ir laisvai platinamos licencijos šifravimo algoritmas. Gali būti naudojamas kaip pakaitalas DES algoritmams. Duomenys skaidomi 64 bitų blokais su kintamo dydžio raktu nuo 32 iki 448 bitų (numatytasis 128)

AES (kitaip Rijndael) algoritmas yra kiek lankstesnis – gali naudoti kelis raktų dydžius (128, 192, 256 bitų). Jeigu DES algoritme duomenų blokas turėjo būti 64 bitų, tai čia blokai gali dirbti su 128, 192, 256 bitų blokais. Vykdomų ciklų skaičius AES algoritme priklauso nuo rakto ir bloko dydžio (žr. 2.8 lentelę)

2.8 lentelė AES algoritmo raktų, blokų, ciklų sąrašas

	Rakto ilgis	**Bloko dydis**	**Ciklų skaičius**
AES – 128	128	128	10
AES – 192	192	192	12
AES – 256	256	256	14

RC6 laikomas vienu pažangiausiu šifravimo standartų. Naudojamas 128 bitų duomenų blokas ir gali naudoti 128, 192, 256 bitų raktų dydžius.

Asimetrinio šifravimo metode generuojami du tarpusavyje susiję raktai. Tikimybė sugeneruoti du kartus tokią pačią šifravimo raktų porą yra labai maža. Jei duomenys užšifruojami vienu raktu, tai juos iššifruoti įmanoma tik kitu tos poros raktu. Žinant tik vieną poros raktą neįmanoma atstatyti kito rakto. Tačiau, palyginus su simetrinio šifravimo metodu, duomenims užšifruoti ir iššifruoti sugaištama žymiai daugiau laiko.

Asimetrinio šifravimo algoritmų pavyzdžiai:

Naudojantis RSA algoritmu reikia užšifruoti duomenis su viešuoju raktu. Iššifruoti duomenis tenka naudojantis slaptuoju raktu, vėliau sutikrinant duomenis su tikraisiais duomenimis.

DSA algoritmo schema – pasinaudojus viešuoju raktu pasirašoma siunčiama žinutė, kuri iš pradžių yra paverčiama į duomenų seką, naudojantis maišos funkcija. Siuntėjas užšifruoja gautą žinutę savuoju slaptuoju raktu, kad būtų sukuriamas siuntėjo asmeninis skaitmeninis parašas. Gaunant žinutę ir parašą, gavėjas iššifruoja parašą naudodamasis siuntėjo viešuoju raktu tam, kad būtų galima gauti žinutės seką ir vėl tuo pačiu maišos algoritmu užšifruoti tą žinutę. Jeigu žinutės seka sutampa su gauta iš siuntėjo, gavėjas gali būti tikras, jog žinutė nebuvo pakeista siuntimo metu.

2.4. Analizės išvados

1. Šiuolaikinėse organizacijose darbuotojams leidžiama naudotis asmeniniais mobiliais įrenginiais. Tai reikalauja papildomų valdymo priemonių, kurios užtikrintų asmeninių įrenginių saugos konfigūravimą, atitinkantį organizacijos saugos politiką.
2. Neteisingai sukonfigūruotas asmeninis mobilus įrenginys (nepriklausomai nuo jo gamintojo ir modelio), kuriam leista naudotis organizacijose esama informacija gali pažeisti organizacijoje esamą saugos politiką. Organizacijos darbuotojai savo mobiliuose įrenginiuose gali tūrėti įvairią papildomą programinę įrangą, kurios patikimumas ir organizacijos saugos politikos atitikimas nėra žinomas.
3. Informacija Bell-LaPadula modelio pagrindu skirstoma į įslaptinimo lygius: ypatingai slapta, slapta, konfidenciali bei neklasifikuota. Organizacijos darbuotojams paskirtos rolės, kurioms priskiriamas atitinkamas įslaptinimo lygis. Įslaptinimo lygio sauga užtikrinama autentifikavimu, antivirusine programine įranga, įsibrovimo aptikimo sistemomis, ryšio protokolo nustatymu, kriptografija ir t.t.
4. Užtikrinti organizacijos saugos politikos įgyvendinimą asmeniniuose mobiliuose įrenginiuose leistų paramos sistema, kurios dėka įrenginys būtų saugiai sukonfigūruotas, patikrintas ar jame nėra papildomos piktavališkos programinės įrangos ir pritaikyti kiti apibrėžti organizacijos saugos politikoje reikalavimai.

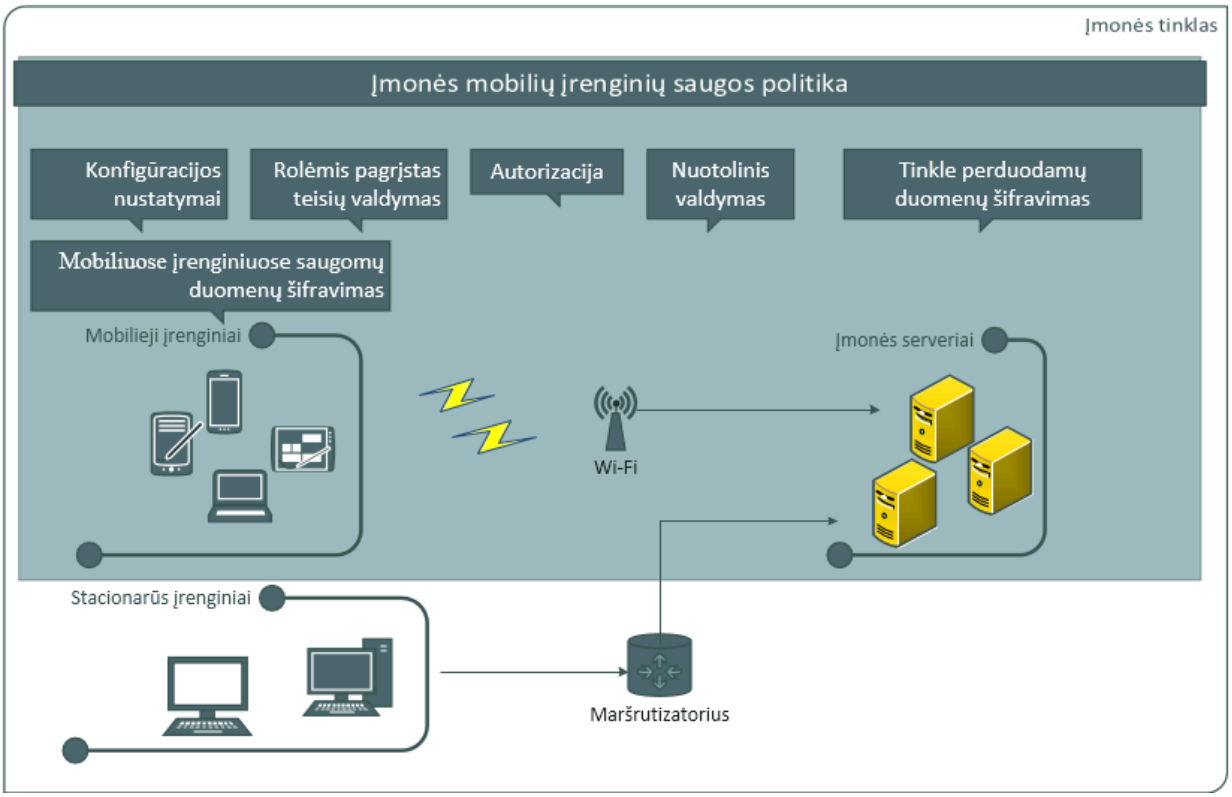
3. ASMENINIŲ MOBILIŲJŲ ĮRENGINIŲ VALDYMO SISTEMOS MODELIS

Šioje darbo dalyje sudarysime mūsų siūlomą MĮ valdymo sistemos modelį. Pagal darbuotojams pasiekiamų duomenų svarbumą, sudarysime rekomendacijas, kokie nustatymai turėtų būti privalomi kiekvienai darbuotojų rolių grupei. Būsenų diagramomis apibrėšime kokius veiksmus turi atlikti serveris ir valdymo programa nuo minutės kai įrenginys bando jungtis prie tinklo iki MĮ patvirtinamas kaip saugus darbui su įmonės duomenimis.

3.1. Asmeninių mobiliųjų įrenginių saugos politikos modelis

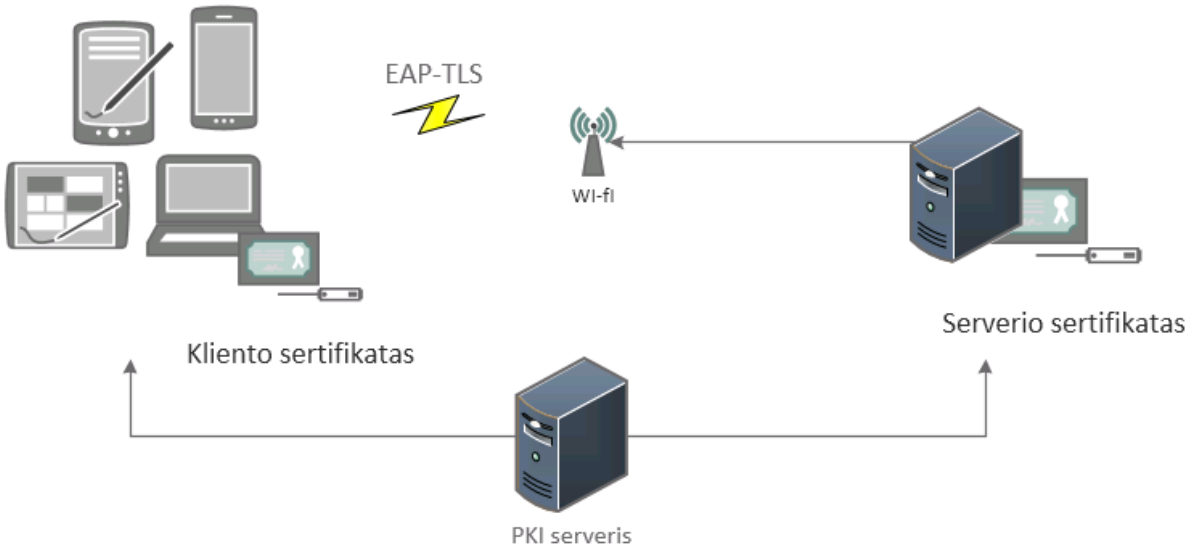
3.1 pav. pavaizduotas įmonės sistemos modelis. Įmonės viduje galima naudoti LAN arba Wi-Fi tinklu. Šiame darbe mes nagrinėsime tik mobiliųjų įrenginių darbą įmonės tinkle Wi-Fi ryšiu. MĮ darbą įmonėje apibrėžia įmonės MĮ saugos politika, kuri nurodo kokie nustatymai privalomi MĮ. Mūsų siūloma valdymo sistema atsižvelgs į :

- Rolėmis pagrįstą priėjimą prie įmonės nustatymų
- Konfigūracijos nustatymų rinkiniai pagal prieinamos informacijos svarbumą.
- Autorizacijos procesą
- Saugų prisijungimą ir darbą tinkle
- Turimų duomenų šifravimą



3.1 pav. Sistemos modelis

Aukščiausią saugumo lygį turinčių pasiekti rolių saugų ryšio seansą MĮ per Wi-Fi tinklą, užtikriname derindami WPA2 ryšio šifravimą ir EAP-TLS autentifikacijos protokolą. EAP-TLS veikimo principas: PKI serveris sugeneruoja klientui ir serveriui sertifikatus. Klientas norėdamas prisijungti prie įmonės tinklo privalo turėti atitinkamą galiojantį sertifikatą savo MĮ (žr. 3.2 pav.)



3.2 pav. Saugaus ryšio seanso užtikrinimas su EAP –TLS

3.2. Saugos sprendimų profiliavimas

Naudodamiesi Bell-LaPadula modeliu (žr. 2.2 skyrių), išskiriame 4 informacijos įslaptinimo lygius:

- Ypatingai slapta
- Slapta
- Konfidencialu
- Neklasifikuota

Pagal Cisco analizę (žr. 2.2.1) išskiriame 6 darbuotojų grupes. Kiekviena iš darbuotojų grupių, turi skirtingus poreikius prieiti prie įslaptintos informacijos. 3.1 lentelė demonstruoja mūsų sudarytą darbuotojų rolių ir įslaptinimo lygio sąryšį. Iš lentelės matome, kad didžiausias prieinamos informacijos spektras reikalingas vyriausias pareigas įmonėje užimantiems darbuotojams – direktoriams. Vadybininkai gali prieiti prie didžiosios dalies informacijos. Administracinio pobūdžio darbuotojai prieina prie kitų darbuotojų informacijos, tokios kaip: atlyginimai, kontaktinė informacija, draudimai ir pan., todėl šios kategorijos darbuotojų saugos nustatymai turi būti griežti. Numatome, kad bendrinio pobūdžio darbuotojai (savo srities specialistai, neprieinantys prie slaptos informacijos) bei judrūs darbuotojai (darbuotojai, dėl darbo specifikos turintys dirbti ne tik iš įmonės patalpų) gali prieiti tik prie konfidencialios bei neklasifikuotos informacijos. Laikinų darbuotojų prieinamos informacijos kiekis turi būti griežtai ribotas.

3.1 lentelė Darbuotojų rolių ir įslaptinimo lygio sąryšis

Įslaptinimas\ rolės	**Direkto-riai**	**Vadybi-ninkai**	**Administra-cinio pobūdžio darbuotojai**	**Bendrinio pobūdžio darbuotojai**	**Judrūs darbuotojai**	**Kontrakto-riai/laikini vartotojai**
Ypatingai slapta	●	○	○	○	○	○
Slapta	●	●	●	○	○	○
Konfidencialu	●	●	●	●	●	○
Neklasifikuotą	●	●	●	●	●	●

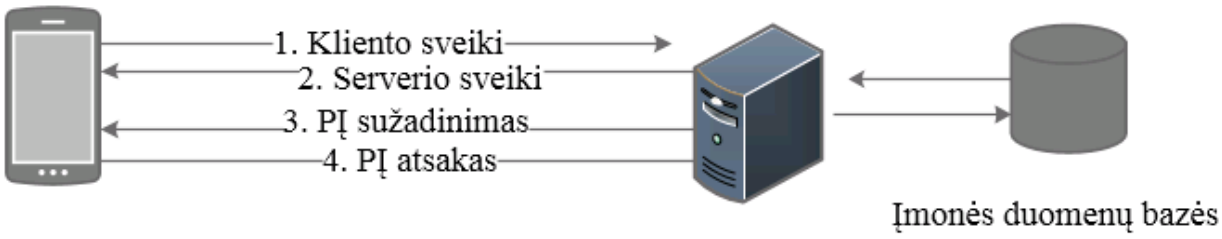
Atsižvelgiant į pasiekiamos informacijos įslaptinimo lygį, MĮ privalo turėti skirtingą konfigūraciją. Darbuotojai, kurių rolės gali prieiti prie ypatingai slaptos informacijos, privalo MĮ nustatyti griežčiausius nustatymus. Darbuotojai, kurių rolės gali prieiti tik prie neklasifikuotos informacijos, bus paprašyti tik pačių paprasčiausių saugumo funkcijų: autentifikacijos bei PIN kodo naudojim. Jei darbuotojas priskiriamas kelioms skirtingoms rolėms, jam turi būti taikomi griežtesnės rolės konfigūracijos nustatymai. 3.3 lentelėje matome mūsų sudarytas 4 konfigūracijos grupes, atsižvelgiant į prieinamos informacijos įslaptinimo lygius.

3.2 lentelė Konfigūracijos nustatymai pagal įslaptinimo lygius

		Įslaptinimas			
		Ypatingai slapta	**Slapta**	**Konfidencialu**	**Neklasifikuotą**
Konfigūracija	**Darbuotojo autentifikcija**	+	+	+	+
	Slaptažodžio tipas	sudėtingas	sudėtingas	sudėtingas	paprastas
	PIN aktyvuotas	+	+	+	+
	SIM kortelės užraktas	+	+	-	-
	Antivirusinė programa	+	+	+	-
	Ugniasienė	+	+	+	-
	Nuotolinio valdymo sistema	+	+	+	-
	Įsibrovimo aptikimo sistema	+	-	-	-
	Atnaujinimų tikrinimas	+	+	+	-
	Nežinomi šaltiniai	-	-	-	+
	Užrakinti po	Iš kart	1 min	1 min	5min
	Duomenų šifravimas	Rijndael	AES	3DES	-
	Ryšio protokolas	WPA2	WPA	WEP	-
	Ryšio autentifikacijos protokolas	EAP-TLS	EAP-TLS	-	-
	GPS	OFF	-	-	-
	Automatinis sinchronizavimas	OFF	OFF	OFF	-
	NFC (angl. Near field communication**)**	OFF	OFF	OFF	-
	Bluetooth	OFF	OFF	OFF	-

3.3. Asmeninių mobiliųjų įrenginių valdymo sistemos ir serverio komunikacijos procesas

Klientas norėdamas pasiekti įmonės duomenis privalo autentifikuotis savo vartotojo vardu bei slaptažodžiu. Autentifikacija vyksta per įmonės valdymo sistemą. MĮ įrenginys prisijungęs prie įmonės tinklo, kreipiasi į serverį su ‚kliento sveiki' žinute, kuri laiko papildomą MĮ informaciją. Serveris gavęs reikiamą informaciją išsiunčia patvirtinimą kliento MĮ bei mėgina sužadinti įmonės valdymo sistemą. Jei mobiliajame įrenginyje programėlė jau įdiegta, ji aktyvuojasi bei išsiunčia patvirtinimą serveriui. (žr. pav 3.3)



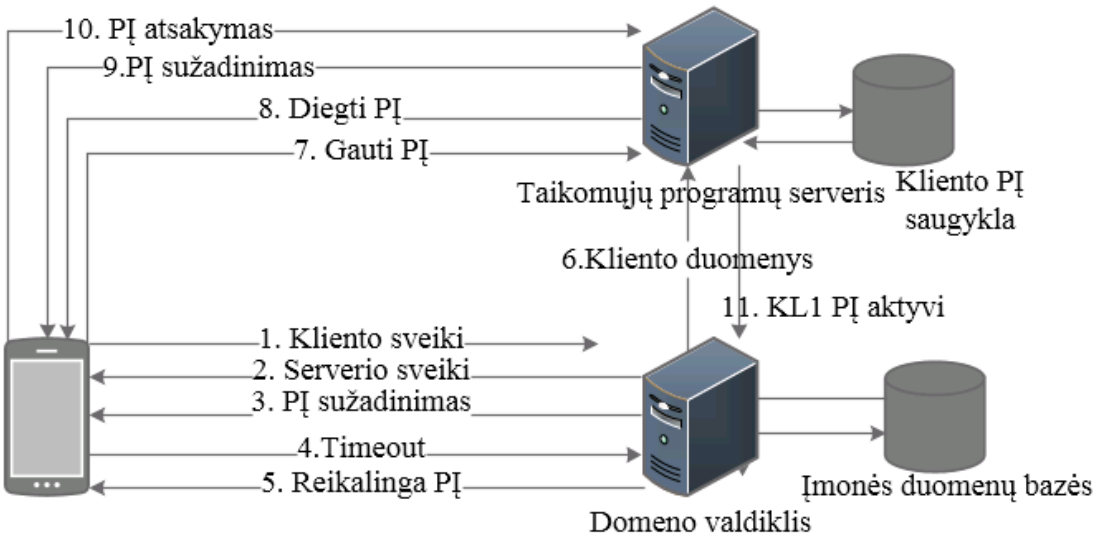
3.3 pav. MĮ valdymo sistemos sužadinimas

Kliento sveiki žinutės metu gaunama informacija:

- MĮ tipas
- MĮ pavadinimas
- Modelio numeris
- IMEI
- Wi-FI
- Wi-Fi MAC adresas
- MĮ OS
- OS versija
- Baterijos energijos likutis
- Baterijos įtampa

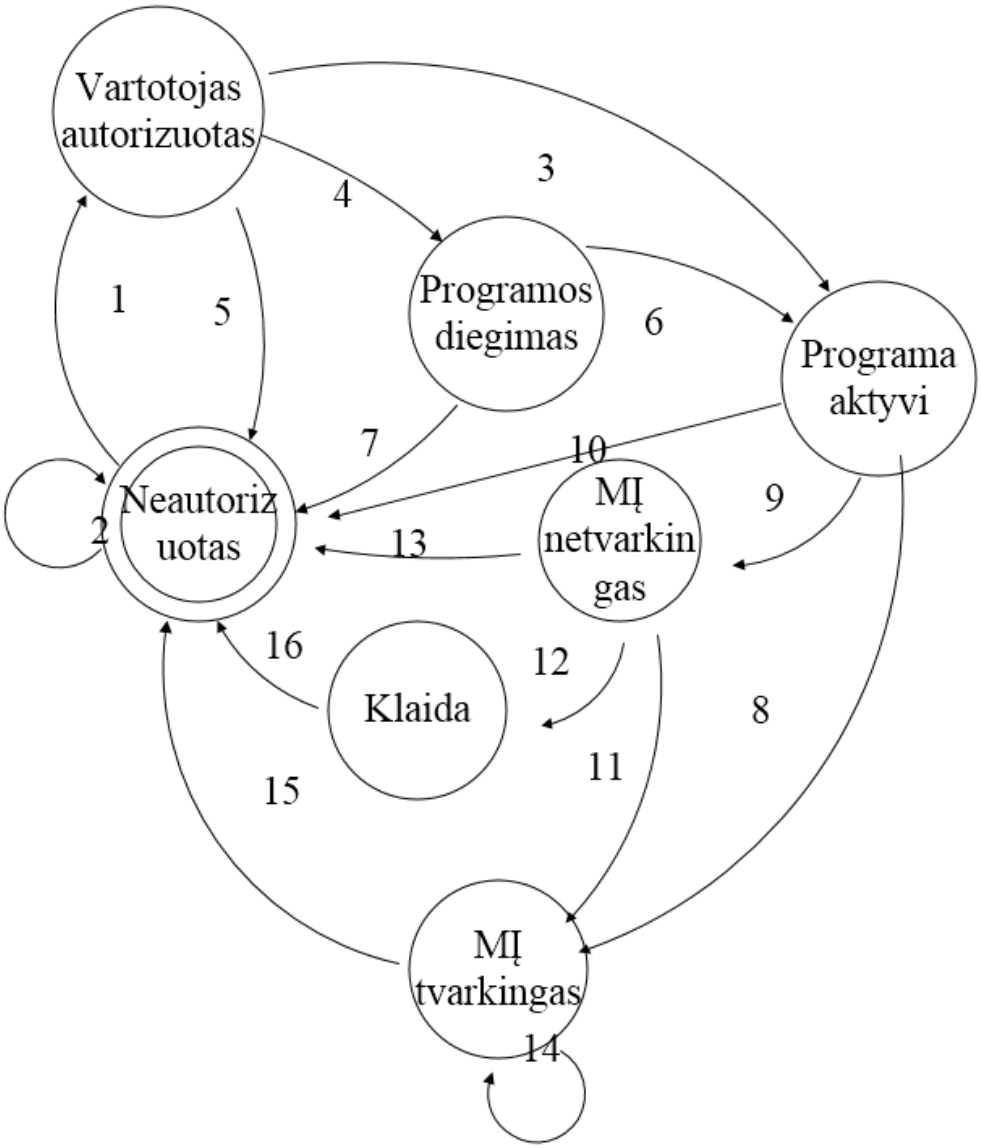
Serverio sveiki žinutės metu siunčiamas patvirtinimas, kad informacija gauta.

Kai vietoj PĮ atsako, serveris gauna „timeout“ klaidos pranešimą, suprantama, kad vartotojas su šiuo MĮ jungiasi primą kartą ir reikalingas programinės įrangos diegimas. Tuomet domeno valdiklis siunčia su ‚kliento sveiki‘ pranešimu gautą informaciją taikomųjų programų serveriui-TKPS1. Klientui išsiunčiamas pranešimas jog reikia susidiegti programinę įrangą. Vartotojui sutikus, TKPS1 gauna pranešimą, kad galima tęsti veiksmus. TKPS1 pasiima iš kliento PĮ saugyklos kliento MĮ operacinei tinkamą diegimo failą ir siunčia jį vartotojui. Vėliau bandoma sužadinti PĮ ir jei instaliacija buvo sėkminga gaunamas PĮ atsakymas. TKPS1 išsiunčia domeno valdikliu, kad programėlė sėkmingai sudiegta ir galima tęsti veiksmus (žr. 3.4 pav.).



3.4 pav. MĮ valdymo sistemos diegimas ir sužadinimas

Tolimesnį sistemos veikimą geriausiai atvaizduos kliento ir serverio būsenų diagramos (žr. 3.5 pav. ir 3.6 pav.)



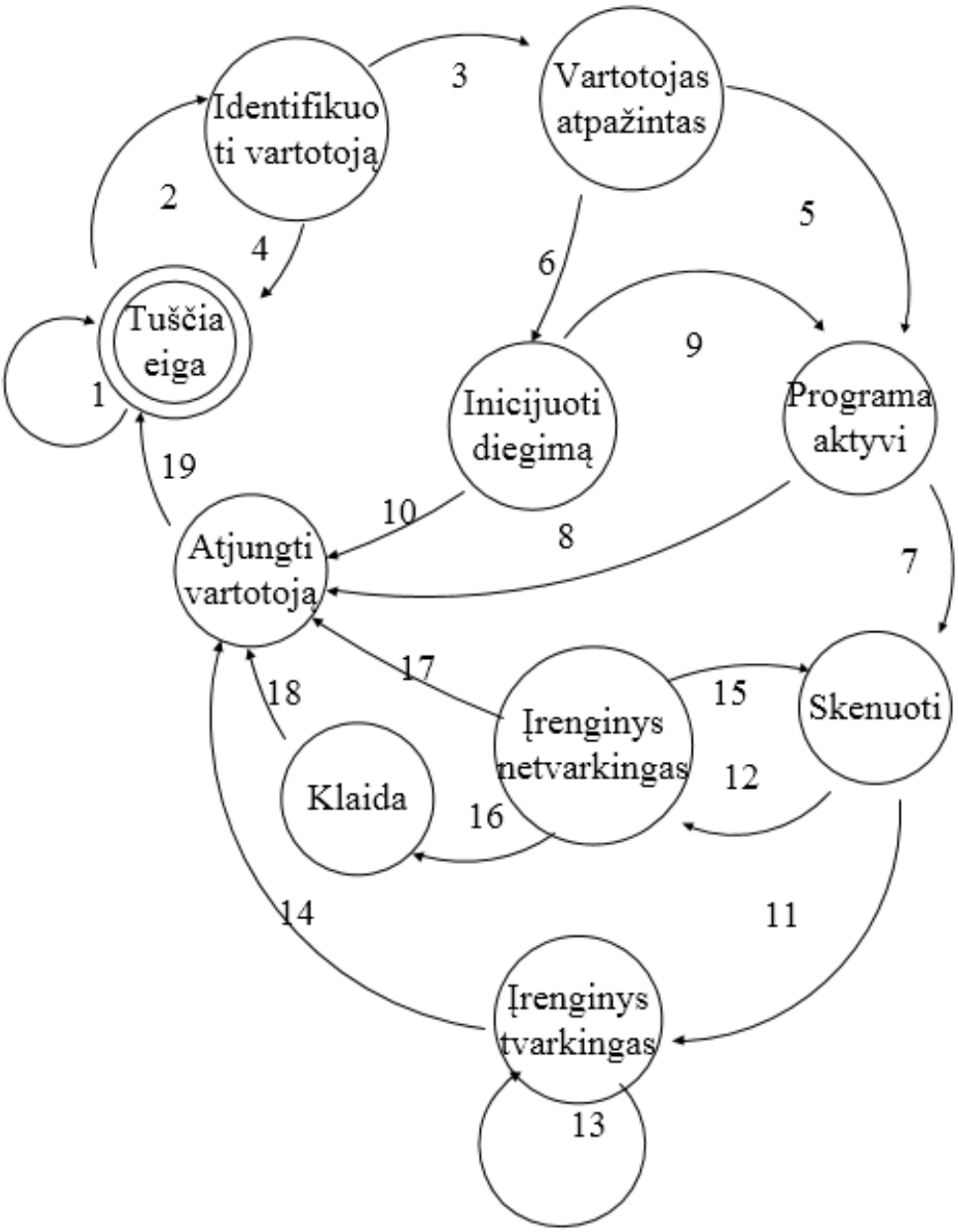
3.5 pav. Kliento būsenų diagrama

3.5 paveikslas demonstruoja,kad kliento MĮ gali praeiti 7 skirtingas būsenas. Pradinė būsena „Neautorizuotas“, bus ir pati paskutinė, kai vartotojas baigs darbą ir išsiregistruos iš sistemos. Perėjimus tarp būsenų aprašome lentelėje 3.3. Numatome, jog viso gali būti 16 skirtingų perėjimų.

3.3 lentelė Kliento būsenų perėjimai

Dabartinė būsena	Pokyčio Nr.	Pokytis	Kita būsena	Rezultatas
Neautorizuotas	**1**	Teisingi prisijungimo duomenys	Vartotojas autorizuotas	Bandoma jungti programą
	2	Neteisingi prisijungimo duomenys	Neautorizuotas	Parodomas pranešimas, kad neteisingi duomenys
Vartotojas Autorizuotas	**3**	MĮ valdymo programa sužadinama	Programa aktyvi	Matomas programos langas
	4	MĮ valdymo programa nerandama	Programos diegimas	Išaukiamas diegimo vedlys
	5	Atšaukti procesą	Neautorizuotas	-
Programos diegimas	**6**	Diegti programą	Programa aktyvi	Matomas programos langas
	7	Atšaukti procesą	Neautorizuotas	-
Programa aktyvi	**8**	Pradėti skenavimą	MĮ tvarkingas	Darbas su MĮ
	9	Pradėti skenavimą	MĮ netvarkingas	Gautas pranešimas, ką reikia keisti
	10	Atšaukti procesą	Neautorizuotas	-
MĮ netvarkingas	**11**	Sutikti atlikti pakeitimus	MĮ tvarkingas	Darbas su MĮ
	12	Sutikti atlikti pakeitimus	Klaida	Gaunamas klaidos pranešimas su paaiškinimu
	13	Atšaukti procesą	Neautorizuotas	-
MĮ tvarkingas	**14**	Darbas su MĮ	MĮ tvarkingas	Darbas su MĮ
	15	Nutraukti darbą	Neautorizuotas	-
Klaida	**16**	Nutraukti darbą	Neautorizuotas	-

Serverio būsenų diagramą atvaizduojame 3.6 paveiksle. Numatome jog tarp serveris gali būti vienoje iš 10 būsenų. Pradinė būsena „tuščia eiga“ – kai kliento MĮ dar nesikreipė į serverį ir jam nereikia apdoroti jokių užklausų. „Tuščia eiga“ taipogi bus ir paskutinė būsena, po to kai vartotojo įrenginys išsiregistruos iš sistemos.



3.6 pav. Serverio būsenų diagrama

Serverio perėjimus tarp būsenų aprašo 3.4 lentelė. Numatome kad viso gali būti 19 skirtingų perėjimų tarp 3.6 pav. pavaizduotų būsenų.

3.4 lentelė Serverio perėjimai tarp būsenų

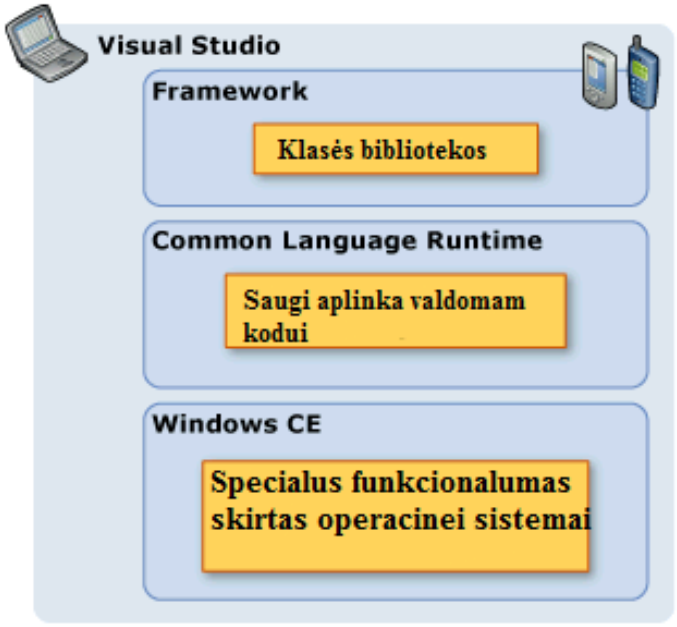
Dabartinė būsena	Pokyčio Nr.	Pokytis	Kita būsena	Rezultatas
Tuščia eiga	1	-	Tuščia eiga	-
	2	Gauti registracijos duomenys	Identifikuoti vartotoją	Gauti registracijos duomenys Lyginami su duomenų bazės įrašais
Identifikuoti vartotoją	3	Vartotojas atpažintas	Vartotojas atpažintas	Vartotojo MĮ išsiunčiamas programos aktyvavimo kodas
	4	Vartotojas neatpažintas	Tuščia eiga	Vartotojui išsiunčimas klaidos pranešimas
Vartotojas atpažintas	5	Išsiųsti programos aktyvavimo kodą/ programa aktyvuojasi	Programa aktyvi	Gaunamas pranešimas, kad programa aktyvuota
	6	Išsiųsti programos aktyvavimo kodą/ programa nerandama	Inicijuoti diegimą	Išaukiamas programos diegimo vedlys
Programa aktyvi	7	Gautas vartotojo leidimas skenuoti	Skenuoti	Skenuojamas vartotojo MĮ
	8	Gautas vartotojo pranešimas 'atšaukti veiksmus'	Atjungti vartotoją	Inicijuojamas vartotojo atjungimas
Inicijuoti diegimą	9	Vartotojas sutinka diegti programą/programa įdiegiama	Programa aktyvi	Gaunamas pranešimas, kad programa aktyvuota
	10	Gautas vartotojo pranešimas 'atšaukti veiksmus'	Atjungti vartotoją	Inicijuojamas vartotojo atjungimas
Skenuoti	11	Skenavimo rezultatas 'įrenginys tvarkingas'	Įrenginys tvarkingas	Vartotojo MĮ leidžiama dirbti pagal priskirtą rolę
	12	Skenavimo rezultatas 'įrenginys netvarkingas'	Įrenginys netvarkingas	Vartotojo MĮ išsiunčiamas klaidos pranešimas
Įrenginys tvarkingas	13	MĮ aktyvus	Įrenginys tvarkingas	Vartotojo MĮ leidžiama dirbti pagal priskirtą rolę
	14	Gautas vartotojo pranešimas 'baigti darbą	Atjungti vartotoją	Inicijuojamas vartotojo atjungimas
Įrenginys netvarkingas	15	Gautas vartotojo pranešimas 'diegti reikiamus pakeitimus'/ pakeitimai usdiegiami	Įrenginys tvarkingas	Vartotojo MĮ leidžiama dirbti pagal priskirtą rolę
	16	Gautas vartotojo pranešimas 'diegti reikiamus pakeitimus'/ vykdant gaunamas klaidos pranešimas	Klaida	Vartotojui išsiunčiamas klaidos pranešimas
	17	Gautas vartotojo pranešimas 'atšaukti veiksmus'	Atjungti vartotoją	-
Klaida	18	Vartotojas atjungiamas	Atjungti vartotoją	Vartotojui išsiunčiamas klaidos pranešimas
Atjungti vartotoją	19	Vartotojas atjungiamas	Tuščia eiga	-

3.4. Asmeninių įrenginių saugaus konfigūravimo sprendimų paramos sistemos prototipas

3.4.1. Programavimo įrankiai

Tyrimą nusprendėme atlikti Windows mobile operacinės sistemos aplinkoje. Sprendimą įtakojo galimybė tyrimą atlikti su žinoma Microsoft Visual Studio 2008 programa, C# kalba. .NET framework bazinės klasės biblioteka Base Class Library suteikia didelį kiekį savybių apimančių vartotojo sąsają (angl. user interface), duomenų prieigą (angl. data access), duomenų bazių sujungimus (angl. database connectivity), kriptografiją (angl. cryptography), žiniatinklių kūrimą (angl. web application), skaitmeninius algoritmus (angl. numeric algorithms) ir tinklinį duomenų apsikeitimą (angl. network communications).

.NET Compact Framework paveldi visą bendrinės kalbos aplinkos (CLR) .NET Framework architektūra valdomo kodo vykdymui [25]. Platforma pateikia suderinamumą su Windows CE operacinę sistemą turintį prietaisą, kas leidžia naudoti esamas funkcijas ir integruoti savo nuosavus komponentus į aplikaciją. .NET Compact Framework platformos architektūra pateikta 12 paveiksle.



3.7 pav. .NET Compact Framework platformos architektūra

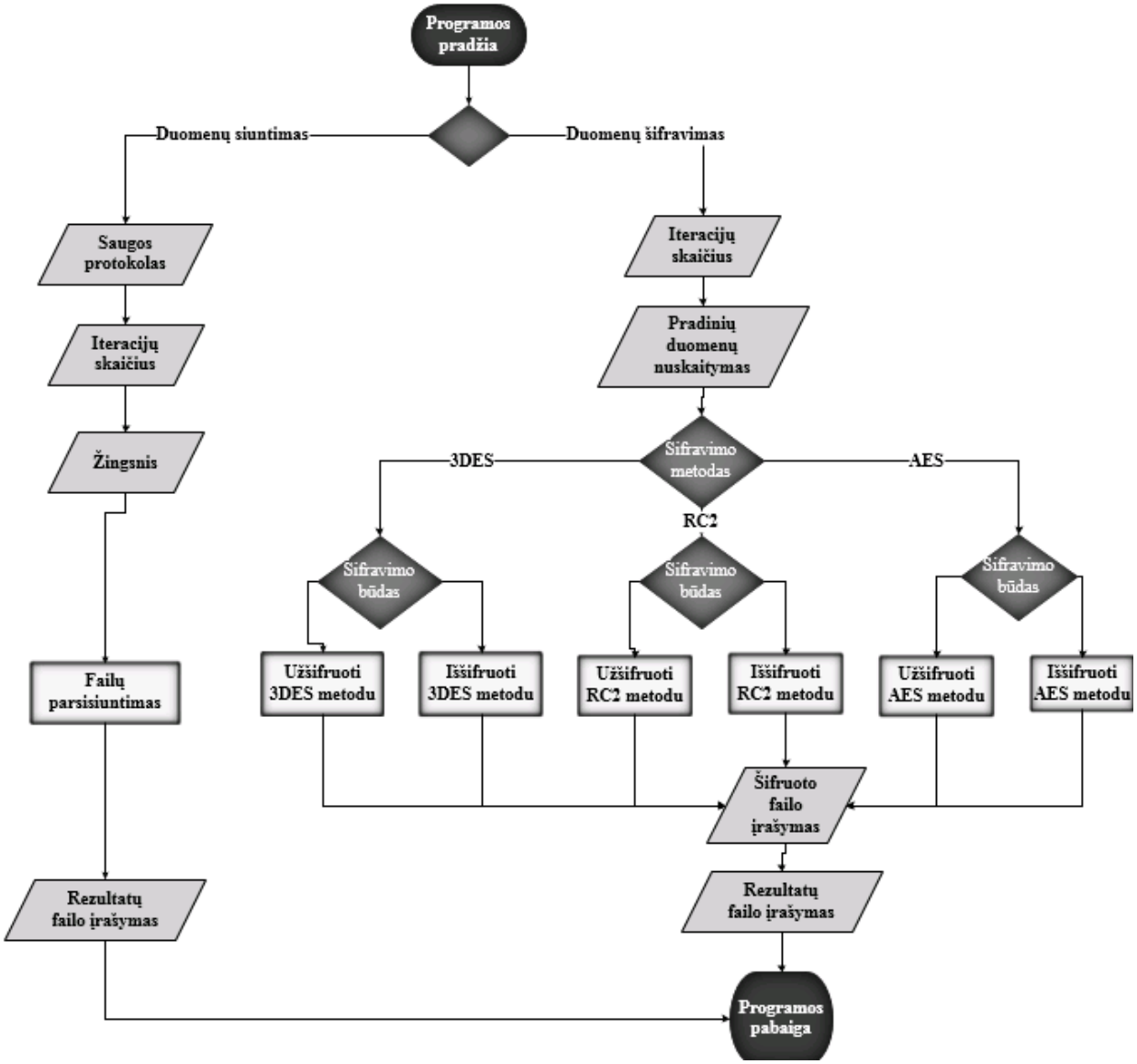
.NET Compact Framework platforma naudoja Windows CE operacinę sistemą pagrindinių funkcijų bei keletui specialių įrenginiui ypatybių vykdymui. Tokios dalys kaip Windows formos, grafinė aplinka, paveikslai, interneto paslaugos buvo pertvarkytos, kad efektyviai veiktų įrenginiuose, o ne tiesiogiai perkopijuoti iš .NET Compact Framework.

NET Compact Framework platforma su Windows Mobile CE operacine sistema uţtikrina šiuos suderinamumo kriterijus:

- Suderinamumą su vietiniu (angl. *native*) saugumu;
- Pilną integraciją su įrenginio OS diegimo (angl. *setup*) programomis;
- Sąveiką su įrenginio kodu, panaudojant COM Interop ir kreipinius į platformos DLL (dynamic link library) bibliotekas, iškviečiant reikalingas funkcijas

3.4.2. Sistemos prototipo struktūra

Numatyta, jog eksperimento tikslais įgyvendinsime etaloninio (angl. *benchmark*) failo atsisiuntimo, užšifravimo ir iššifravimo procedūras. Eksperimento programinės įrangos blokinę schemą galime matyti 3.8 pav.

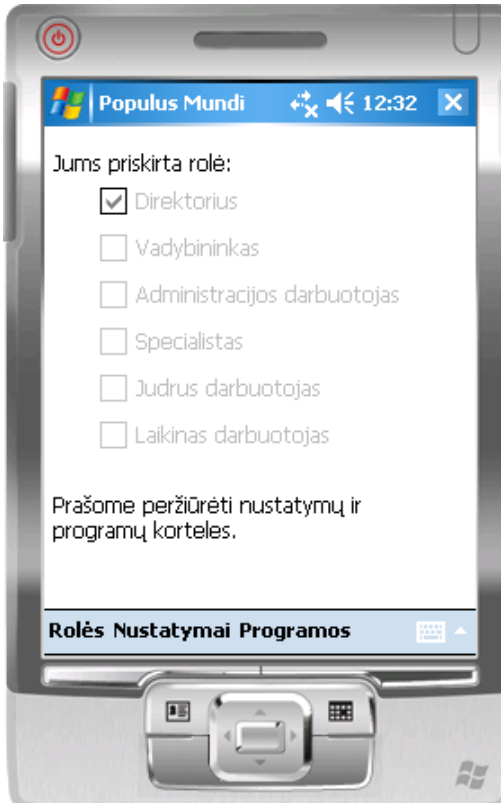


3.8 pav. Apibendrinta eksperimento programinės įrangos blokinė schema

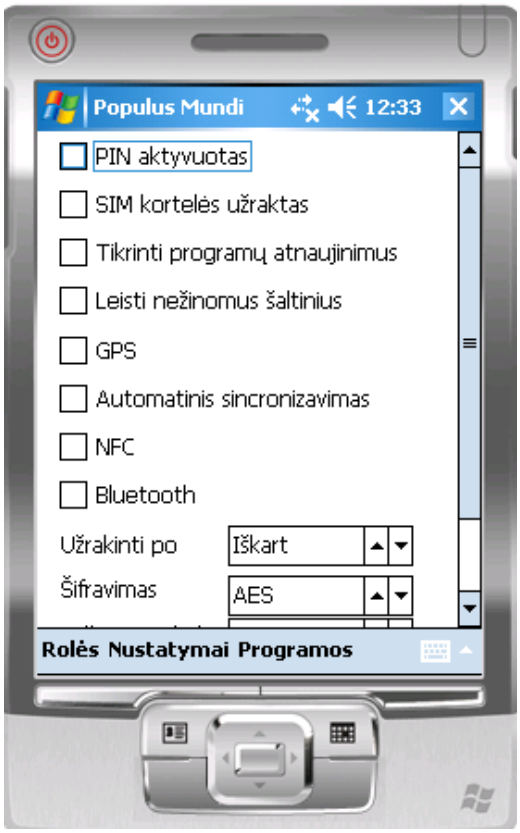
Žinoma realus asmeninio mobiliojo įrenginio naudotojas nesinaudos mūsų tyrimui sukurta programine įranga. Mobiliųjų įrenginių vartotojams siūlomas saugaus konfigūravimo paramos sistemos vaizdas demonstruojamas 3.9-3.12 pav. Vartotojas prisijungęs prie tinklo visų pirma autorizuojamas, tuomet jam leidžiama atlikti norimus veiksmus: automatizuotai konfigūruoti mobilųjį įrenginį, rankiniu būdu konfigūruoti mobilųjį įrenginį arba tikrinti ar mobiliojo įrenginio konfigūracijoje yra nesutapimų su įmonės politika.

3.9 pav. Paramos sistemos prisijungimo langas

3.11 pav. Paramos sistemos veiksmų pasirinkimų langas



3.10 pav. Paramos sitemos priskirtos rolės peržiūros langas



3.12 pav. Paramos sitemos nustatymų pasirinkimo langas

3.5. Išvados

1. Pasiūlytas asmeninių mobiliųjų įrenginių naudojimo organizacijose saugos politikos modelis. Modelyje atvaizduoti saugos politikos elementai: konfigūracijos nustatymai, rolėmis pagrįstas teisių valdymas, autorizacija, duomenų perduodamų tinkle šifravimas, mobiliuose įrenginiuose saugomų duomenų šifravimas ir nuotolinis valdymas.
2. Remiantis Bell-LaPadula modeliu pasiūlytas saugos sprendimų profiliavimas, kur kiekvienam profiliui apibrėžti asmeninių mobiliųjų įrenginių saugos konfigūracijos nustatymai pagal įslaptinimo lygius.
3. Suprojektuotas asmeninių mobiliųjų įrenginių saugaus konfigūravimo paramos sistemos prototipas, grįstas klientas-serveris santykiu. Apibrėžtas paramos sistemos prototipo funkcionavimas iš kliento ir serverio pusės.

4. ASMENINIŲ ĮRENGINIŲ SAUGAUS KONFIGŪRAVIMO SPRENDIMŲ PARAMOS SISTEMOS EKSPERIMENTINIS TYRIMAS

Eksperimentui atlikti naudojama techninė įranga:

- AirPlus G 802.11g/2.4GHz prieigos taškas, kurio parametrai: 802.11g standartas, perdavimo greitis iki 54Mbps, veikia 2,4GHz dažnių diapazone.
- WEB serveris
- Asus nešiojamasis kompiuteris, kurio parametrai: Win7 64bitų OS, 4 GB RAM, Intel procesorius (2,20 GHz)

Eksperimentui atlikti naudojama programinė įranga:

- Microsoft Visual Studio 2008
- Windows Mobile 6 SDK
- Meraki WIFI stumbler

Eksperimentui atlikti naudojamas etaloninis 1346 KB dydžio Northwind.sdf failas. Tyrimo rezultatų failas sudarytas iš 4.1 lentelėje nurodytų laukų.

4.1 lentelė Duomenų tyrimo rezultatų failo aprašymas

Eil. Nr.	Lauko pavadinimas	Lauko aprašymas
1.	IteracijuSk	Programoje nurodytas iteracijų kiekis.
2.	Zingsnis	Matavimo taškai, nurodantys kiek matavimų reikšmių bus nuskaityta į rezultatų failą.
3.	Pradzios laikas	Tyrimo atlikimo laikas: MM/DD/YYYY hh:mm:ss (kur MM-mėnuo, DD-diena, YYYY-metai, hh-valandos, mm-minutės, ss-sekundės).
4.	Baterijos ikrovimas %	Baterijos energija procentais
5.	Baterijos itampa	Bateris įtampa
6.	Pabaigos laikas	Tyrimo pabaigos laikas: MM/DD/YYYY hh:mm:ss (kur MM- mėnuo, DD-diena, YYYY-metai, hh-valandos, mm-minutės, ss-sekundės).
7.	Viso parsisiusta KB	Atsiųstų baitų kiekis

Kiekvieno eksperimento metu nustatytas 100 iteracijų pasikartojimas. Eksperimentui atlikti naudojami prieigos taško bevielio tinklo konfigūracijos nustatymai nurodyti 4.2 lentelėje.

4.2 lentelė Eksperimentui atlikti naudotų prieigos taško bevielio tinklo konfigūracijos nustatymų sąrašas

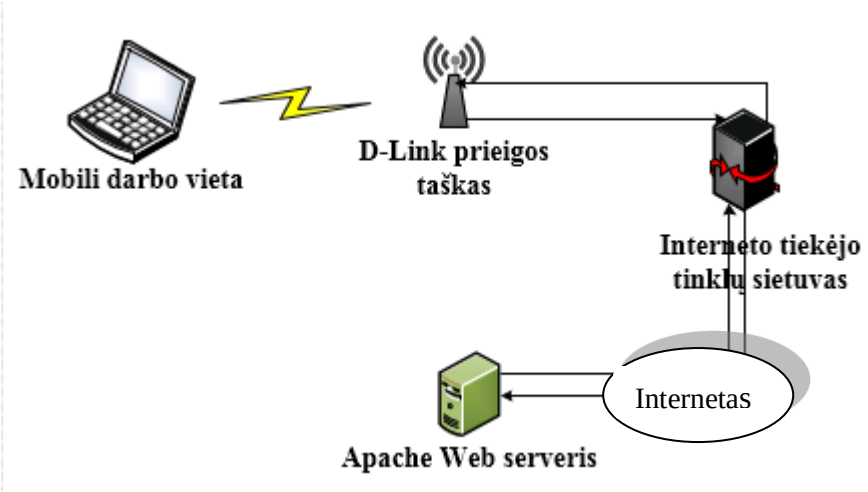
Saugos protokolas	Duomenų šifravimo algoritmas	Raktas
Be protokolo	-	-
WEP	64Bit	10 simbolių
WPA-PSK	TKIP	8 simboliai
WPA2-PSK	AES	8 simboliai

Kai prieigos taške nustatoma bevielio tinklo konfigūracija, norint su mobiliuoju įrenginiu prisijungti prie tinklo, mobiliajame įrenginyje būtina nustatyti prieigos taškui atitinkamus nustatymus. MĮ bevielio tinklo konfigūracijos nustatymai nurodyti 4.3 lentelėje.

4.3 lentelė Eksperimentui atlikti naudotų MĮ bevielio tinklo konfigūracijos nustatymų sąrašas

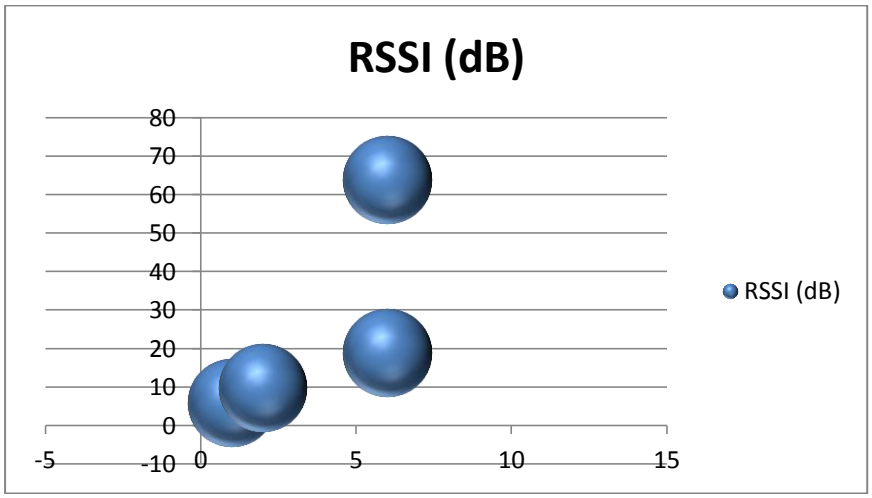
Saugos protokolas	**Duomenų šifravimo algoritmas**	**Raktas**
Be protokolo	-	-
WEP	Open	10 simbolių
WPA-PSK	TKIP	8 simboliai
WPA2-PSK	AES	8 simboliai

Pirmasis duomenų parsisiuntimo eksperimentas atliktas esant nurodytiems skirtingiems saugumo protokolams, atliktas simuliuojant darbuotojo prisijungimą prie įmonės web serverio nuotoliniu būdu. Iš 4.1 matome, kad MĮ jungiasi prie D-Link prieigos taško, tuomet duomenys siunčiami per interneto tinklų sietuvą internetu iki įmonės web serverio, pasiimami duomenys ir parsisiunčiami į mobilųjį įrenginį.



4.1 pav. Tinklo schema, jungiantis prie įmonės serverio internetu

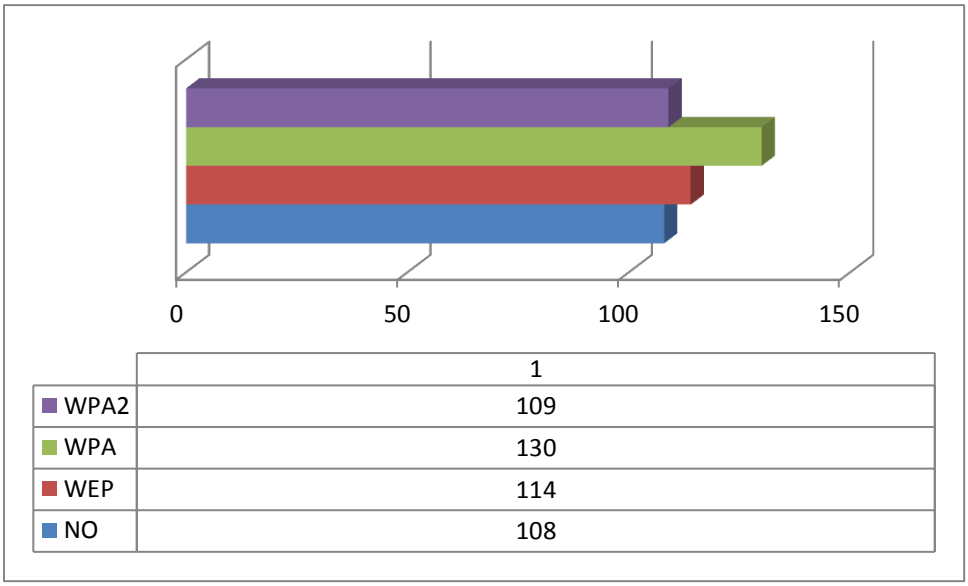
Ištyrus kokie prieigos taškai prieinami tuo pačiu metu kaip ir D-Link kai atliekamas tyrimas, iš 4.2 pav. matome jog be D-Link (64 db RRSI), matomi dar trys prieigos taškai, tačiau jų stiprumas varijuoja nuo 6db iki 19 db.



4.2 pav. Prieigos taškai ir jų stiprumas

Gauti rezultatai matomi 4.3 pav. Nenustačius jokio saugos protokolo, etalononinis failas parsisiunčiamas per 108 sekundes. Įjungus WPA2 saugos protokolą, rezultatas gaunamas panašus,

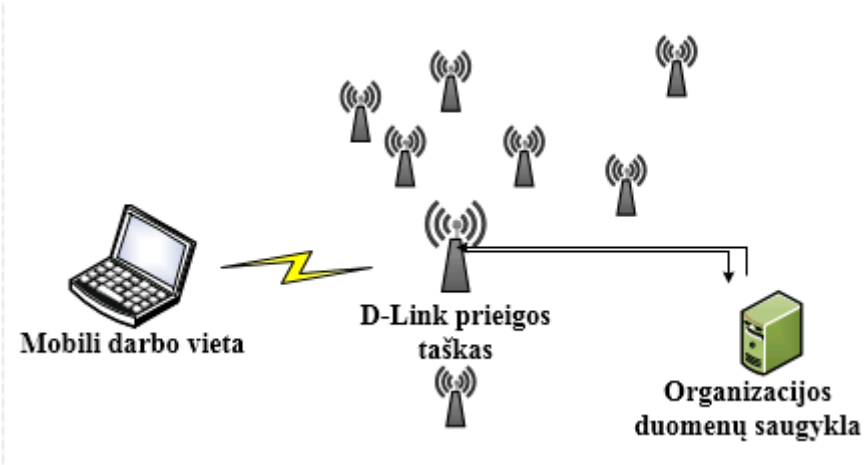
dėl šio protokolo techninių šifravimo galimybių. Iš tiriamų saugos protokolų šiomis sąlygomis prasčiausiai pasirodo WPA protokolas, kuris duomenis siuntėsi 20 % daugiau laiko, nei be jokio saugos protokolo.



	1
WPA2	109
WPA	130
WEP	114
NO	108

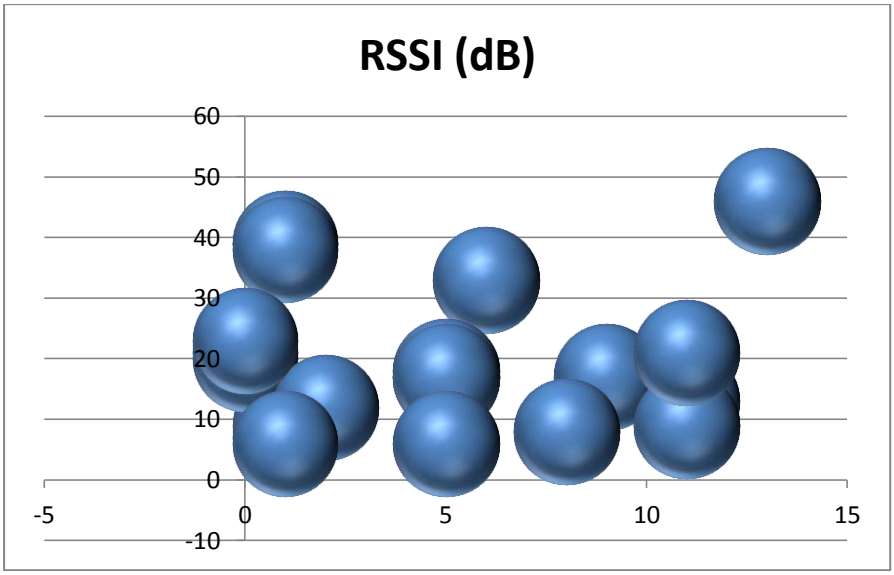
4.3 pav. Duomenų parsisiuntimas greitis be trikdžių tinkle, pasirenkant skirtingus tinklo saugos protokolus

Duomenų parsisiuntimo tyrimas buvo pakartotas, pasikeitus darbo sąlygoms. Iš 4.4 pav. matome jog šį kartą prie organizacijos duomenų saugyklos jungtasi tiesiogiai per D-Link prieigos tašką, be interneto paslaugų tiekėjo. Tačiau buvo užfiksuota didelis kiekis kitų prieigos taškų.



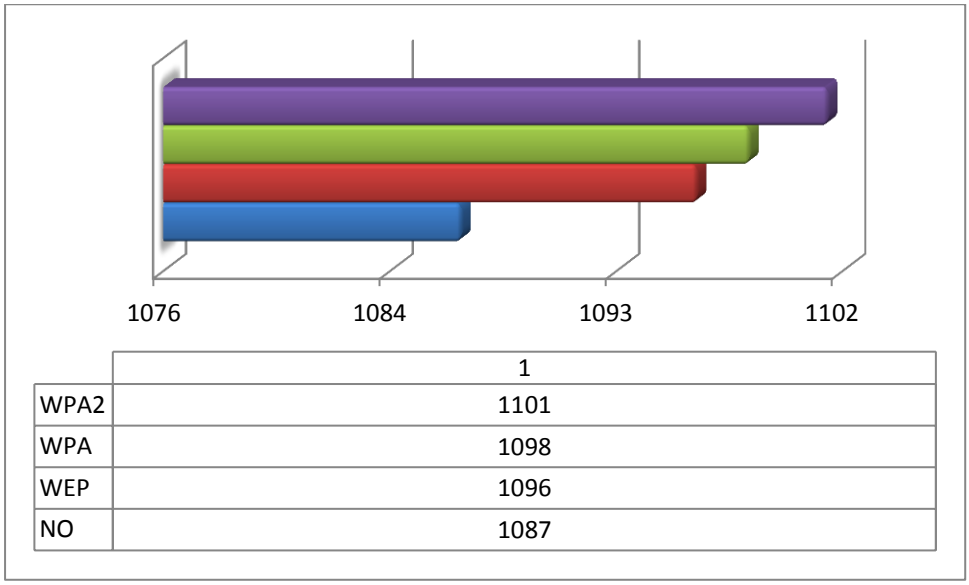
4.4 pav. Tinklo schema, jungiantis prie įmonės serverio tiesiogiai su dideliais trikdžiais tinkle

Ištyrus kokie prieigos taškai prieinami tuo pačiu metu kaip ir D-Link kai atliekamas tyrimas, iš 4.5 pav. matome jog be D-Link (46 db RRSI), matomi dar 22 prieigos taškai. Pastebime, jog netgi 9 iš jų signalo stiprumas viršiją 20 db. Esant tokiai didelei signalų koncentracijai, didėja tikimybė jog siunčiami paketai bus pamesti ir teks siuntimą kartoti. Situaciją gerinti mėginta jungiant prieigos tašką ne prie 6 kanalo kaip įprastai, bet prie 13 kanalo.



4.5 pav. Prieigos taškai ir jų stiprumas, esant dideliam triukšmui tinkle

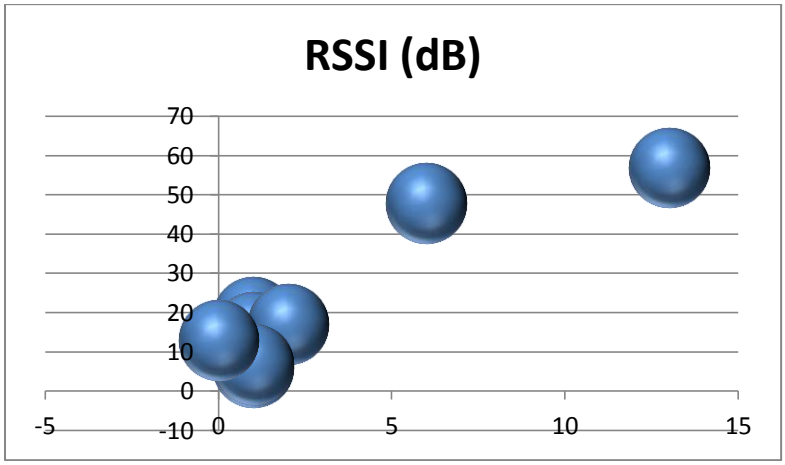
Iš 4.6 paveikslo matome, kad pasikeitus tinklo sąlygoms, duomenų parsisiuntimo laikas prailgėja iki 10 kartų. Sudėtingiausi saugos protokolai tokiomis sąlygomis duomenis siunčia ilgiausiai.4.4



	1
WPA2	1101
WPA	1098
WEP	1096
NO	1087

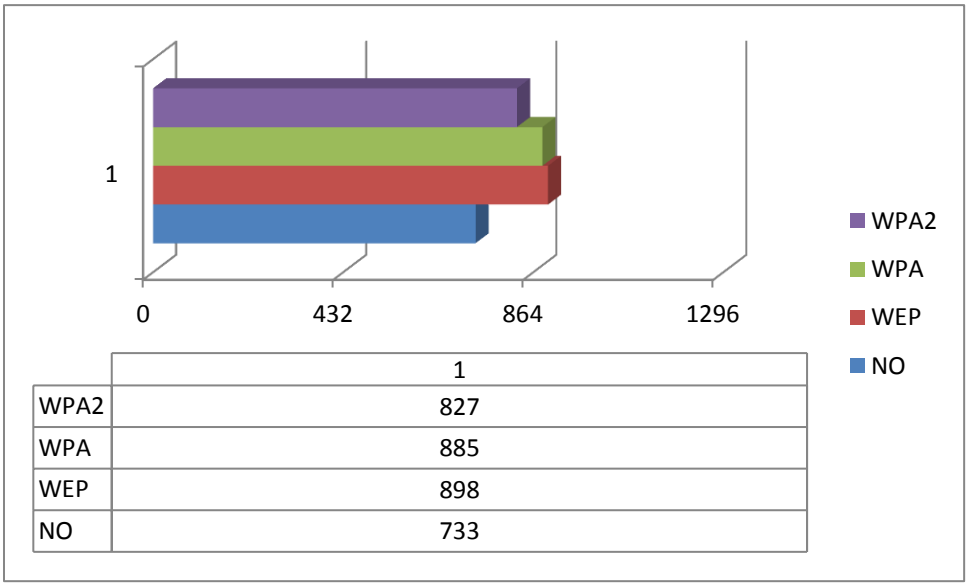
4.6 pav. Duomenų parsisiuntimas greitis su stipriais trikdžiais tinkle, pasirenkant skirtingus tinklo saugos protokolus

Tyrimas pakartotas, sumažinus iki 9 prieigos taškų, pasiekiamų vienu metu. Lyginant su D-Link (57db), matomas dar vienas ypač stiprus signalas 6 kanale (47 db). Likusių signalų stiprumas varijuoja nuo 6db iki 19 db (žr. 4.7 pav.)



4.7 pav. Prieigos taškai ir jų stiprumas, esant vidutiniam triukšmui tinkle

Gauti rezultatai matomi 4.8 pav. Pasikeitus situacijai tinkle, duomenys pasisiunčiami 3 kart greičiau nei esant dideliam triukšmui tinkle be jokių saugos protokolų nustatymų. Siunčiant duomenis, nustačius saugos protokolų konfigūracijas, pastebime kad vėl matoma greičių koreliacija pastebėta vykdant siuntimą, be trindžių tinkle: iš saugos protokolų WPA2 veikia greičiausiai.



	1
WPA2	827
WPA	885
WEP	898
NO	733

4.8 pav. Duomenų parsisiuntimas greitis su vidutiniais trikdžiais tinkle, pasirenkant skirtingus tinklo saugos protokolus

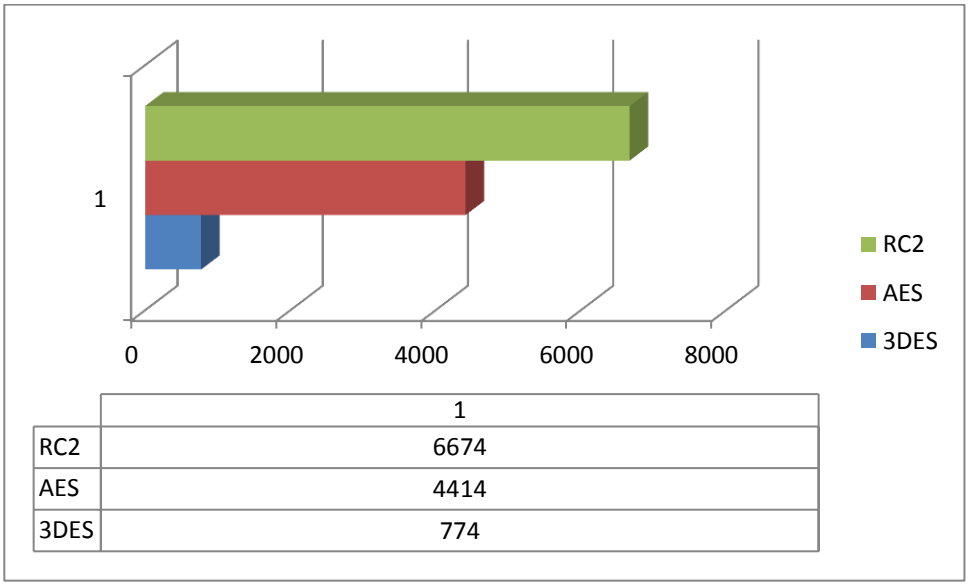
Norint įsitikinti, jog ne tinklo sujungimo schema įtakoja greičių koreliaciją, buvo pakartotas tyrimas prie web serverio jungiantis internetu (4.1 pav), bet esant trikdžiams tinkle (4.7 pav.). Rezultatai gauti analogiški 4.8 pav., todėl darome išvadą, kad žymus duomenų parsisiuntimo greičio pablogėjimas priklauso nuo trikdžių bevieliame tinkle.

Antroji tyrimo dalis nagrinėja populiariausius šifravimo algoritmus: 3DES, RC2 bei AES (žr. 3.4 lentelę).

4.4 lentelė Eksperimente naudojami kriptografiniai algoritmai, bei raktų dydžiai

Eil. Nr.	**Algoritmas**	**Rakto dydis (bit)**	**.Net Framework klases pavadinimas**
1.	3DES	192	TripleDESCryptoServiceProvider
2.	RC2	128	RC2CryptoServiceProvider
3.	AES(RijnDael)	128	RijnDaelManaged

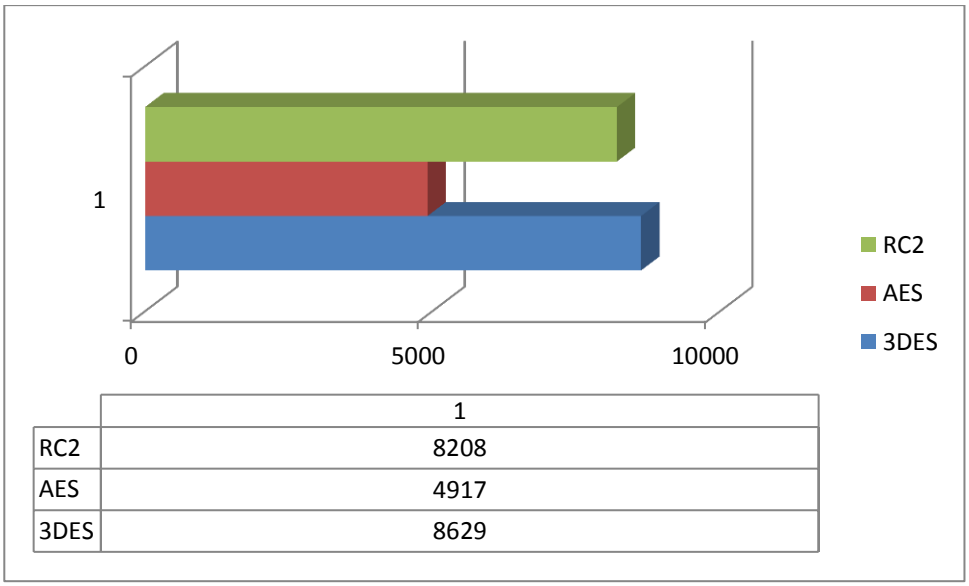
Iš 4.9 pav. matome jog 3DES algoritmas užšifruoja duomenis greičiausiai, net 5,7 karto greičiau nei AES ir netgi 8,6 karto greičiau nei RC2.



	1
RC2	6674
AES	4414
3DES	774

4.9 pav. Duomenų užšifravimo greitis taikant skirtingus šifravimo algoritmus

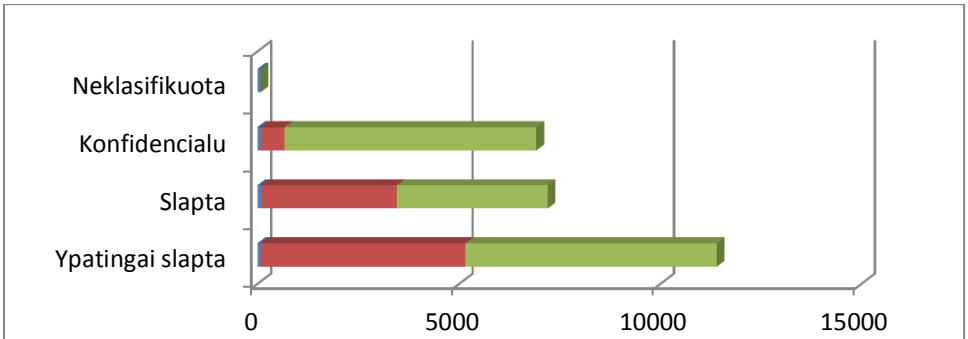
Duomenų iššifravimo atskleidė visiškai skirtingą greičių koreliaciją. Iš 4.10 pav. matome, kad greičiausiai duomenis iššifravo AES metodas, o lėčiausiai 3DES.



	1
RC2	8208
AES	4917
3DES	8629

4.10 pav. Duomenų iššifravimo greitis taikant skirtingus šifravimo algoritmus

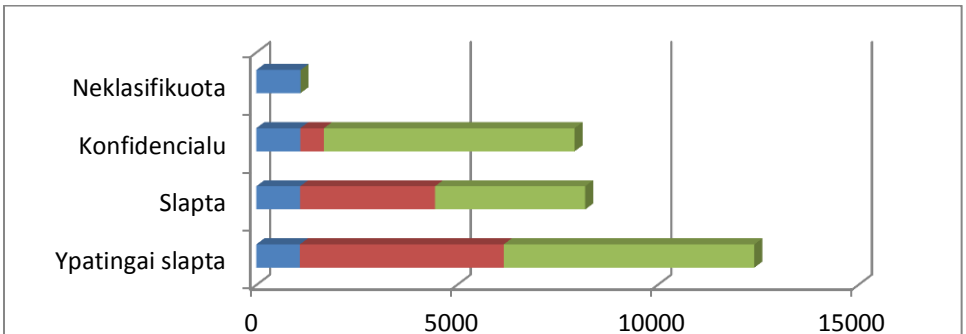
Pagal 4.10 lentelėje nurodytus konfigūracijos nustatymus priklausančius nuo prieinamos informacijos įslaptinimo lygio, sudarome tyrinėto proceso (parsisiųsti-užšifruoti-atšifruoti) greičio koreliaciją pagal įslaptinimo lygius, 100 MB dydžio failui. Palyginimui naudosime idealiomis tinklo sąlygomis gautus parsisiuntimų greičius (4.3 pav.) Iš 4.11 pav. matome, palyginus su kitais profiliais greičiausiai procesas praeina neklasifikuotą informaciją pasiekiančiam vartotojui, nes jo turima informacija neturi būti užšifruojama. Konfidencialios ir slaptos informacijos procesui praeiti prireikia labai panašaus laiko tarpo, nes 3DES ir AES užšifravimo ir atšifravimo bendras laikas labai panašūs, todėl galima rekomenduoti vietoj 3DES šifravimo metodo naudoti AES abiem atvejais. Net 47 % lėčiau už slaptos informacijos proceso praėjimą, užtrunka ypatingai slaptos informacijos praėjimas.



	Ypatingai slapta	Slapta	Konfidencialu	Neklasifikuota
Parsisiuntimas	83	99	87	82
Užšifravimas	5079	3359	589	0
Atšifravimas	6247	3742	6247	0

4.11 pav. Pilno proceso (parsisiųsti-užšifruoti-atšifruoti) greičio palyginimas pagal įslaptinimo lygius 100Mb dydžio failui esant geroms wi-fi sąlygoms.

Bendras parsisiuntimo ir šifravimo – iššifravimo laikas blogiausiomis wi-fi sąlygomis, kai aplinkui veikė 22 kitų prieigos taškų ypatingai slaptam profiliui informacijos užšifravimui sunaudota 4,6 karto daugiau, o iššifravimui 5,7 karto daugiau laiko, nei parsisiuntimui (žr. 4.12 pav.).



	Ypatingai slapta	Slapta	Konfidencialu	Neklasifikuota
Parsisiuntimas	1087	1096	1098	1101
Užšifravimas	5079	3359	589	0
Atšifravimas	6247	3742	6247	0

4.12 Pilno proceso (parsisiųsti-užšifruoti-atšifruoti) greičio palyginimas pagal įslaptinimo lygius 100Mb dydžio failui esant blogoms wi-fi sąlygoms.

4.1. Išvados

1. Organizacijos darbuotojai, kuriems leista naudotis asmeniniais įrenginiais, gali pasiekti informaciją dvejopai: iš išorės, naudojantis interneto paslaugų tiekėju ir iš vidinio tinklo. Mobiliems įrenginiams būdingas bevielio tinklo naudojimas.
2. Remiantis aukščiau minėta išvada eksperimentiniai tyrimai atlikti naudojant bevielį wi-fi tinklą, užtikrinant prieigą prie organizacijos duomenų iš išorės ir iš vidaus.
3. Eksperimento metu, užtikrinta prieiga prie organizacijos duomenų:
    a. iš išorės, naudojant wi-fi tinklą. Aplinkui prieigos tašką veikė trys kitų vartotojų prieigos taškai, kurių stiprumas vyravo nuo 6db iki 19 db.;

   b. iš vidaus, naudojant wi-fi tinklą. Aplinkui prieigos tašką veikė kiti organizacijoje naudojami 22 prieigos taškai, iš kurių net 9 signalų stiprumas viršijo 20 db,;
   c. iš vidaus, naudojant wi-fi tinklą. Aplinkui prieigos tašką veikė kiti organizacijoje naudojami 9 prieigos taškai, iš kurių vieno signalo stiprumas buvo artimas D-Link signalui (47 db), o likusių signalų stiprumas vyravo nuo 6 iki 19 db.;
4. Eksperimentas duomenų prieigai iš vidaus, kur veikia daug wi-fi prieigos taškų (tai būdinga organizacijoms, kuriuose yra atskirai veikiančių padalinių), buvo atliktas Kauno technologijos universiteto kompiuterių katedros patalpose.
5. Atlikus asmeninių įrenginių saugaus konfigūravimo sprendimų paramos sistemos prototipo eksperimentinį tyrimą perduodant duomenis wi-fi tinklu pastebėta:
   a. Prieigai prie organizacijos duomenų iš išorės kai aplinkui veikė trys prieigos taškai WPA protokolas duomenų siuntimui sunaudojo 20% daugiau laiko nei be jokio saugos protokolo, tačiau saugesnis WPA2 protokolas sunaudoja 19 % mažiau laiko nei WPA.
   b. Prieigai prie organizacijos duomenų iš vidaus kai aplinkui veikė 22 prieigos taškai, vidutinis duomenų parsisiuntimo laikas, lyginant su atveju ***a,*** prailgėja iki 10 kartų. Tokiomis sąlygomis WPA protokolas duomenų siuntimui sunaudojo tiktai 1% daugiau laiko nei be jokio saugos protokolo, tačiau saugesnis WPA2 protokolas sunaudoja jau 0,3 % daugiau laiko nei WPA.
   c. Prieigai prie organizacijos duomenų iš vidaus kai aplinkui veikė 9 prieigos taškai, vidutinis duomenų parsisiuntimo laikas , lyginant su atveju ***a,*** prailgėja iki 7 kartų. Tokiomis sąlygomis WPA protokolas duomenų siuntimui sunaudojo 21% daugiau laiko nei be jokio saugos protokolo, tačiau saugesnis WPA2 protokolas vėl sunaudoja 7 % mažiau laiko nei WPA, lyginant su atveju ***b***.
6. Atlikus asmeninių įrenginių saugaus konfigūravimo sprendimų paramos sistemos prototipo eksperimentinį tyrimą šifruojant duomenis asmeniniame mobiliajame įrenginyje pastebėta:
   a. Duomenų šifravimas 3DES algoritmu 5,7 karto greičiau nei AES ir 8,6 karto greičiau nei RC2, o RC2 lėčiau 1,5 karto lėčiau nei AES.
   b. Duomenų iššifravimas 3DES algoritmu 1,7 karto lėčiau nei AES ir 1,05 karto lėčiau nei RC2, o RC2 lėčiau 1,75 karto lėčiau nei AES.
7. Bendras parsisiuntimo ir šifravimo – iššifravimo laikas geresnėmis wi-fi sąlygomis, kai aplinkui veikė 3 kiti prieigos taškai ypatingai slaptam profiliui informacijos užšifravimui sunaudota 61 karto daugiau, o iššifravimui 75 karto daugiau laiko, nei parsisiuntimui.
8. Bendras parsisiuntimo ir šifravimo – iššifravimo laikas blogiausiomis wi-fi sąlygomis, kai aplinkui veikė 22 kitų prieigos taškų ypatingai slaptam profiliui informacijos užšifravimui sunaudota 4,6 karto daugiau, o iššifravimui 5,7 karto daugiau laiko, nei parsisiuntimui.
9. Kai aplinkui veikia ne daugiau 3 prieigos taškų, kurių signalas nėra labai stiprus pagrindinis laikas sunaudojamas informacijos užšifravimui bei iššifravimui. Kai aplinkui veikia 9 arba 22 kitų prieigos taškų, kurių signalai yra stiprūs, parsisiuntimo laikas priartėja prie laiko sunaudojamo duomenų užšifravimui ir iššifravimui.

5. IŠVADOS

1. Šiuolaikinėse organizacijose darbuotojams leidžiama naudotis asmeniniais mobiliais įrenginiais. Tai reikalauja papildomų valdymo priemonių, kurios užtikrintų asmeninių įrenginių saugos konfigūravimą, atitinkantį organizacijos saugos politiką.
2. Organizacijos saugos politikos įgyvendinimą asmeniniuose mobiliuose įrenginiuose leistų paramos sistema, kurios dėka įrenginys būtų saugiai sukonfigūruotas, patikrintas ar jame nėra papildomos piktavališkos programinės įrangos ir pritaikyti kiti apibrėžti organizacijos saugos politikoje reikalavimai.
3. Pasiūlytas asmeninių mobiliųjų įrenginių naudojimo organizacijose saugos politikos modelis. Modelyje atvaizduoti saugos politikos elementai: konfigūracijos nustatymai, rolėmis pagrįstas teisių valdymas, autorizacija, duomenų perduodamų tinkle šifravimas, mobiliuose įrenginiuose saugomų duomenų šifravimas ir nuotolinis valdymas.
4. Remiantis Bell-LaPadula modeliu pasiūlytas saugos sprendimų profiliavimas, kur kiekvienam profiliui, apibrėžti asmeninių mobiliųjų įrenginių saugos konfigūracijos nustatymai pagal įslaptinimo lygius. Suprojektuotas asmeninių mobiliųjų įrenginių saugaus konfigūravimo paramos sistemos prototipas, grįstas klientas-serveris santykiu. Apibrėžtas paramos sistemos prototipo funkcionavimas iš kliento ir serverio pusės.
5. Eksperimentiniai tyrimai atlikti naudojant bevielį wi-fi tinklą, užtikrinant prieigą prie organizacijos duomenų:
    a. iš išorės naudojant wi-fi tinklą aplinkui prieigos taško veikė trys kitų vartotojų prieigos taškai, kurių stiprumas vyravo nuo 6db iki 19 db.;
    b. iš vidaus naudojant wi-fi tinklą aplinkui prieigos tašką veikė kiti organizacijoje naudojami 22 prieigos taškai, iš kurių net 9 signalų stiprumas viršijo 20 db,;
    c. iš vidaus naudojant wi-fi tinklą aplinkui prieigos tašką veikė kiti organizacijoje naudojami 9 prieigos taškai, iš kurių vieno signalo stiprumas buvo artimas D-Link signalui (47 db), o likusių signalų stiprumas vyravo nuo 6 iki 19 db.;
6. Atlikus asmeninių įrenginių saugaus konfigūravimo sprendimų paramos sistemos prototipo eksperimentinį tyrimą perduodant duomenis wi-fi tinklu pastebėta:
    a. Prieigai prie organizacijos duomenų iš išorės kai aplinkui veikė trys prieigos taškai WPA protokolas duomenų siuntimui sunaudojo 20% daugiau laiko nei be jokio saugos protokolo, tačiau saugesnis WPA2 protokolas sunaudoja 19 % mažiau laiko nei WPA.
    b. Prieigai prie organizacijos duomenų iš vidaus kai aplinkui veikė 22 prieigos taškai, vidutinis duomenų parsisiuntimo laikas, lyginant su atveju ***a,*** prailgėja iki 10 kartų. Tokiomis sąlygomis WPA protokolas duomenų siuntimui sunaudojo tiktai 1% daugiau laiko nei be jokio saugos protokolo, tačiau saugesnis WPA2 protokolas sunaudoja jau 0,3 % daugiau laiko nei WPA.
    c. Prieigai prie organizacijos duomenų iš vidaus kai aplinkui veikė 9 prieigos taškai, vidutinis duomenų parsisiuntimo laikas , lyginant su atveju ***a,*** prailgėja iki 7 kartų. Tokiomis sąlygomis WPA protokolas duomenų siuntimui sunaudojo 21% daugiau laiko nei be jokio saugos protokolo, tačiau saugesnis WPA2 protokolas vėl sunaudoja 7 % mažiau laiko nei WPA, lyginant su atveju ***b***.

7. Kai aplinkui veikia ne daugiau 3 prieigos taškų, kurių signalas nėra labai stiprus pagrindinis laikas sunaudojamas informacijos užšifravimui (61 karto daugiau nei parsisiuntimui) bei iššifravimui (75 karto daugiau nei parsisiuntimui).
8. Kai aplinkui veikia 9 arba 22 kitų prieigos taškų, kurių signalai yra stiprūs, parsisiuntimo laikas priartėja prie laiko sunaudojamo duomenų užšifravimui (4,6 karto daugiau nei parsisiuntimui) ir iššifravimui (5,7 karto daugiau nei parsisiuntimui).

6. LITERATŪRA

[1] J. Sathyan, „Multi-layered collaborative approach to address enterprise mobile security challenges,“ įtraukta *Collaborative Security Technologies (CoSec), 2010 IEEE 2nd Workshop*, Bangalore, 2010.

[2] A. Distefano et.al, „SecureMyDroid: enforcing security in the mobile devices lifecycle,“ įtraukta *CSIIRW '10 Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, New York, 2010.

[3] M. Becher, „Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices,“ įtraukta *SP '11 Proceedings of the 2011 IEEE Symposium on Security and Privacy*, Washington, 2011.

[4] M. Landman, „Managing Smart Phone Security Risks,“ įtraukta *InfoSecCD '10 2010 Information Security Curriculum Development Conference*, New York, 2010.

[5] K. Kostiainen et. al., „Old, new, borrowed, blue --: a perspective on the evolution of mobile platform security architectures,“ įtraukta *CODASPY '11 Proceedings of the first ACM conference on Data and application security and privacy*, Niujorkas, 2011.

[6] „Enterprise Readiness of Consumer Mobile Platforms,“ TREND micro, 2012.

[7] S. Adappa, „User controllable security and privacy for mobile mashups,“ įtraukta *HotMobile '11 Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*, New York, 2011.

[8] K. Dunhan, Mobile malware attacks and defence, Burlington: Syngress Publishing, Inc., 2009.

[9] S. Karsten, „Software Security Aspects of Java-Based Mobile Phones,“ įtraukta *SAC '11 Proceedings of the 2011 ACM Symposium on Applied Computing*, New York, 2011.

[10] M. Mun et.al., „Personal data vaults: a locus of control for personal data streams,“ įtraukta *Co-NEXT '10 Proceedings of the 6th International COnference*, New York, 2010.

[11] „List of all JSRs,“ Java Comunity Process, 2013. [Tinkle]. Available: http://jcp.org/en/jsr/all.

[12] D. Stenett ir S. Sankaranarayanan, „Personal mobile information system,“ įtraukta *ICIS '09 Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human*, Niujorkas, 2009.

[13] J. Siefers, T. Gang ir G. Morrisett, „Robusta: taming the native beast of the JVM,“ įtraukta *CCS '10 Proceedings of the 17th ACM conference on Computer and communications security*, Niujorkas, 2010.

[14] D. Sehr et.al., „Adapting software fault isolation to contemporary CPU architectures,“ įtraukta *USENIX Security'10 Proceedings of the 19th USENIX conference on Security*, 2010.

[15] B. A. W. C. H. Gebotys, „Methodology for attack on a Java-based PDA,“ įtraukta *CODES+ISSS '06 Proceedings of the 4th international conference on Hardware/software codesign and system synthesis*, New York, 2006.

[16] H. I. Bulbul, I. Batmaz ir O. Mesut, „Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols,“ įtraukta *e-Forensics '08 Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, Briuselis, 2008.

[17] P. Trimintzios ir G. Georgiou, „WiFi and WiMAX secure deployments,“ *Journal of Computer Systems, Networks, and Communications - Special issue on WiMAX, LTE, and WiFi interworking*, 2010.

[18] S. Sukhija ir S. Gupta, „Wireless Network Security Protocols, A Comparative Study,“

International Journal of Emerging Technology and Advanced Engineering, t. 2, nr. 1, 2012.

[19] K. Miller, „BYOD: Security and Privacy Considerations," t. 14, nr. 5, Sept.-Oct. 2012.

[20] T. Vainio et.al., „User needs for metadata management in mobile multimedia content services," įtraukta *Mobility '09 Proceedings of the 6th International Conference on Mobile Technology, Application & Systems*, New York, 2009.

[21] A. Venčkauskas ir J. Toldinas, „Kompiuterių ir operacinių sistemų sauga," 2007, p. 39.

[22] N. R. Antanaitienė M. V., Praktinis įvadas į intelektinę nuosavybę, Vilnius, 2001.

[23] „www3.lrs.lt," [Tinkle]. Available: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=436874&p_query=&p_tr2=2. [Kreiptasi 2013-05-01].

[24] D. S. A. Elminaam, H. M. A. Kader ir M. M. Hadhoud, „Performance Evaluation of Symmetric Encryption," *IJCSNS International Journal of Computer Science and Network Security*, t. 8, nr. 20, pp. 280-286, 2008.

[25] Microsoft, „MSDN library," 2013. [Tinkle]. Available: http://msdn.microsoft.com/lt-lt/library/9s7k7ce5.aspx. [Kreiptasi 15 02 2013].