KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Vladas Drejeris

ASMENINIŲ MOBILIŲJŲ ĮRENGINIŲ, NAUDOJAMŲ ĮMONĖSE, SAUGAUS KONFIGŪRAVIMO PARAMOS SISTEMA

Baigiamasis magistro darbas

Vadovas
Doc. dr. Jevgenijus Toldinas

KAUNAS, 2015

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

TVIRTINU
Katedros vedėjas
(parašas) Prof. dr. Algimantas Venčkauskas
(data)

ASMENINIŲ MOBILIŲJŲ ĮRENGINIŲ, NAUDOJAMŲ ĮMONĖSE, SAUGAUS KONFIGŪRAVIMO PARAMOS SISTEMA

Baigiamasis magistro darbas

Informacijos ir informacinių technologijų sauga (kodas 621E10003)

Vadovas
(parašas) Doc. dr. Jevgenijus Toldinas
(data)

Recenzentas
(parašas) Prof. habil. dr. Vytautas Štuikys
(data)

Projektą atliko
(parašas) Vladas Drejeris
(data)

KAUNAS, 2015

KAUNO TECHNOLOGIJOS UNIVERSITETAS

.....

(Fakultetas)

.....

(Studento vardas, pavardė)

.....

(Studijų programos pavadinimas, kodas)

Baigiamojo projekto „Asmeninių mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistema“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 ___ m. _____ ____ d.

Kaunas

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

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

_____ _____

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

Drejeris, V. Asmeninių mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistema. Magistro baigiamasis projektas / vadovas doc. dr. Jevgenijus Toldinas; Kauno technologijos universitetas, Informatikos fakultetas, Kompiuterių katedra. Kaunas, 2015. 71 psl.

SANTRAUKA

Šiuolaikiniai mobilieji įrenginiai, dar vadinami išmaniaisiais, pasiekė tokius skaičiavimų ir atminties kiekius, kurie prieš keletą metų buvo prieinami tik personaliniams ir nešiojamiems kompiuteriams. Dėl šio technologinio proveržio mobilieji įrenginiai vartotojams suteikia daug daugiau galimybių nei vien tik telefono funkcijas. Šiais įrenginiais galima naršyti internete, klausytis muzikos, žiūrėti filmus, saugoti duomenis. Taip pat į juos galima įrašyti įvairias programėles, kurios dar labiau praplečia šių įrenginių galimybes. Dėl to mobilieji įrenginiai tapo labai populiarūs ir šiandien yra mūsų kasdienybės dalis. Jie plačiai naudojami ne tik asmeniniams tikslams, bet ir darbui.

Darbuotojams yra nepatogu, kai jie darbui turi naudoti įmonės išskirtus mobiliuosius įrenginius, o ne asmeninius. Tokiu atveju tam pačiam darbuotojui tenka naudotis dviem ar daugiau įrenginiais vienu metu. Tai sumažina darbuotojo darbo našumą bei padidina įmonės IT infrastruktūros išlaidas. Norint išvengti šių priežasčių ir sukurti dar patogesnę darbo sferą darbuotojui, pasaulyje ėmė plačiai plisti asmeninių įrenginių naudojimo įmonėse tendencija, dar vadinama atsinešk savo įrenginį (*angl. Bring your own device*).

Asmeninių mobiliųjų įrenginių naudojimas įmonėse darbuotojams suteikia daug privalumų, tačiau tuo pačiu įmonei sukelia papildomas saugumo grėsmes. Darbuotojai dažnai piktnaudžiauja mobiliaisiais įrenginiais, jungiasi prie atvirų viešųjų bevielio ryšio tinklų ir naudoja netinkamai sukonfigūruotus įrenginius. Dėl to jie gali būti pažeidžiami virusų, piktavališkų programėlių, programišių atakų ar tiesiog pametami. Įvykus saugumo pažeidimui, įmonė rizikuoja prarasti konfidencialią informaciją, esančią mobiliajame įrenginyje. Vienas iš būdų šioms problemoms spręsti yra mobilių įrenginių kontrolės sistemos.

Magistrinio darbo objektas - mobiliųjų įrenginių saugaus konfigūravimo paramos sistema.

Šio darbo struktūra:

- Pirmojoje darbo dalyje pateikiama mobiliųjų įrenginių, naudojamų įmonėse, saugumo analizė. Joje nagrinėjami mobiliųjų įrenginių pažeidžiamumai, įmonėms kylančios saugumo grėsmės bei mobiliųjų įrenginių saugos technologijos. Šioje darbo dalyje taipogi analizuojamas mobiliųjų įrenginių saugumo politikų sudarymas ir pritaikymas įmonėse.
- Antrojoje darbo dalyje pateikiamas asmeninių mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos modelis. Jame apibrėžiama sistemos architektūra, kliento ir serverio komunikacijų schemos ir sistemos veikimo principai. Įvairūs sistemoje vykstantys procesai yra iliustruoti grafikais. Taip pat šioje dalyje rasite pateiktą ir sistemos prototipą.
- Trečiojoje darbo dalyje pateikiami eksperimentinio tyrimo rezultatai. Eksperimento metu buvo ištirta žiniatinklio paslaugų konfigūracijų įtaka sistemos greitaveikai. Tyrimo metu išnagrinėta transporto lygmens protokolų ir perduodamų pranešimų formatų įtaką atliekamų užklausų trukmei. Pagal gautus rezultatus pateiktos rekomendacijos kokios žiniatinklio paslaugų konfigūracijos turėtų būti naudojamos sistemoje.
- Darbo pabaigoje pateiktos išvados.

Drejeris, V. Enterprise employee-owned mobile devices secure configuration support system. Master's thesis / supervisor Assoc. Prof. Dr. Jevgenijus Toldinas; Department of Computer Science, Faculty of Informatics, Kaunas University of Technology. – Kaunas, 2015. – 71 p.

SUMMARY

Nowadays mobile devices, also called smart devices, have reached memory and processing power almost equal to personal and laptop computers. This technological breakthrough has opened a lot of new possibilities for the users. They can use the mobile device to surf the internet, listen to music, watch movies or store data. Moreover, it is possible to install various mobile applications on these devices, which expand their functionality even more. Therefore, smart phones, tablets and other mobile devices have become very popular and now are an integral part of our lives. These devices are widely used not only for personal purposes but for the work too.

It is very inconvenient for an employee when they have to use separate enterprise issued devices for the work needs. In this case the employee is forced to use two or more devices at the same time. It reduces the work efficiency and increases the costs of IT infrastructure. To solve these problems and create a more comfortable work environment more and more enterprises are allowing their employees to use their own personal mobile devices for the work tasks. This trend is called "bring your own device".

The use of personal mobile devices gives a lot of advantages but at the same time it exposes the enterprise to additional security threats. Employees tend to misuse their devices, they aren't educated enough for IT security, often connect to public wireless networks and use incorrect configurations. Therefore their mobile devices are vulnerable to viruses, malware or hacker attacks. Moreover, these devices can be lost or stolen. When security breach occurs, enterprise risks losing their confidential information stored on mobile device. One of the solutions to these problems is a mobile device management system.

The aim of this work is to create a mobile devices secure configuration support system.

This paper is organized as follows:

- In the first part of the work, the analysis of the mobile device security vulnerabilities and threats to enterprises is presented. We study mobile device vulnerabilities, security threats emerging for business and mobile device security technologies. Moreover we look at enterprise mobile security policy creation and application.
- In the second part of the work, we define an enterprise employee-owned mobile devices secure configuration support system model. This model consists of system architecture, client and server communication scheme and system operating principles. Various system processes are illustrated by graphs. Also the prototype of the secure configuration support system is provided in this part of the work.
- In the third part of the work, we present the results of our experiments. During the experiment, we studied the web service configurations influence to the system speed. We researched transport and message layer protocol configurations impact to request execution time. Based on the result we provide recommendations for what web service configurations should be used in the system.
- Finally, we present the conclusions of the work.

TURINYS

PAVEIKSLĖLIŲ SĄRAŠAS

LENTELIŲ SĄRAŠAS

TERMINŲ IR SUTRUMPINIMŲ SĄRAŠAS

ISO	Tarptautinė standartizacijos organizacija (*angl. International Organization for Standardization*)
GSM	Globalus mobilių telefonų ryšio standartas (*angl. Global Standart for Mobile Communications*)
PIN	Asmeninis identifikavimo numeris (*angl. Personal identification number*)
IMEI	Tarptautinis mobilaus įrenginio identifikatorius (*angl. International Mobile Station Equipment Identity*)
GPS	Globali vietos nustatymo sistema (*angl. Global Positioning System*)
MAC adresas	Duomenų prieigos kontrolės adresas (*angl. Media Access Control Address*)
DoS	Paslaugų atsisakymo aptarnauti ataka (*angl. Denial of Service*)
VPT	Virtualus privatus tinklas
RADIUS	Centralizuotas kompiuterinių tinklų autentifikavimosi protokolas (*angl. Remote Authentication Dial In User Service*)
WPA	Wi-fi prieigos apsaugos protokolas (*angl. Wi-Fi Protected Access*)
WPA2	Wi-fi prieigos apsaugos protokolas (*angl. Wi-Fi Protected Access II*)
IPSec	Internetinio protokolo apsauga (*angl. Internet Protocol Security*)
L2TP	Antrojo lygmens tuneliavimo protokolas (*angl. Layer 2 Tunneling Protocol*)
PPTP	Taškas į tašką tuneliavimo protokolas (*angl. Point-to-Point Tunneling Protocol*)
IEEE	Elektros ir elektronikos inžinerijos institutas (*angl. Institute of Electrical and Electronics Engineers*)
WEP	Wi-fi prieigos apsaugos protokolas (*angl. Wired Equivalent Privacy*)
CCMP	Šifravimo protokolas skirtas bevieliams tinklams (angl. *Cipher Block Chaining Message Authentication Code Protocol*)
UMTS	Universali mobiliųjų telekomunikacijų sistema (*angl. Universal Mobile Telecommunications System*)
LTE	Ketvirtosios kartos mobiliojo korinio ryšio technologija (*angl. Long-Term Evolution*)

WCDMA	Trečiosios kartos mobiliojo korinio ryšio technologija (*angl. Wideband Code division multiple Access*)
XML	Bendros paskirties duomenų struktūra (*angl. Extensible Markup Language*)
WAP	Bevielis taikomųjų programų protokolas (*angl. Wireless Application Protocol*)
RS-232	Nuoseklaus duomenų perdavimo sąsaja
ROM	Tik skaitomojo tipo atmintis (*angl. Read-only Memory*)
HTTP	Tai užklausimo - atsakymo protokolas, jungiantis klientą ir serverį (*angl. Hypertext Transfer Protocol*)
HTTPS	Apsaugotas HTTP protokolas (*angl. Hypertext Transfer Protocol Secure*)
SIM	Abonento identifikavimo modulis (*angl. Subscriber Identity Module*)
TKIP	Bevielių tinklų apsaugos prototkolas (*angl. Temporal Key Integrity Protocol*)
OS	Operacinė sistema
CPU	Procesorius (*angl. central processing unit*)
RAM	Operatyvioji atmintis (*angl. Random Access Memory*)
IAS	Įsilaužimo aptikimo sistema
URL	Universali resurso nuoroda kompiuteriniame tinkle (*angl. Uniform Resource Locator*)
RSS	Internetinių naujienlaiškių rinkimo duomenų formatas (*angl. Rich Site Summary*)
JSON	Atviras tekstinėje formoje perduodamų duomenų formatas (*angl. JavaScript Object Notation*)
SOAP	Protokolas skirtas struktūrizuotų duomenų perdavimui (*angl. Simple Object Access Protocol*)
MNC	Mobilaus ryšio operatoriaus tinklo kodas (*angl. Mobile Network Code*)
MCC	Mobilaus ryšio šalies kodas (*angl. Mobile Country Code*)
SSID	Unikalus bevielių vietinių tinklų identifikatorius (*angl. Service Set Identification*)
NFC	Ryšių mažame lauke technologija (*angl. Near Field Communication*)

1. ĮVADAS

Šiuolaikiniai mobilieji įrenginiai, dar vadinami išmaniaisiais, pasiekė tokius skaičiavimų ir atminties kiekius, kurie prieš keletą metų buvo prieinami tik personaliniams ir nešiojamiems kompiuteriams. Dėl šio technologinio proveržio mobilieji įrenginiai vartotojams suteikia labai plačias galimybes. Šiais įrenginiais galima naršyti internete, klausytis muzikos, žiūrėti filmus ar saugoti duomenis. Taip pat į juos galima įrašyti įvairias programėles, kurios dar labiau praplečia įrenginių galimybes. Dėl to mobilieji įrenginiai labai išpopuliarėjo ir tapo mūsų kasdienybės dalimi.

Šių įrenginių privalumai atveria ne tik plačias galimybes asmeniniam naudojimui, bet ir darbui. Daugelyje šiuolaikinių įmonių mobilieji įrenginiai tapo neatsiejama IT infrastruktūros dalimi. Jie padidina darbuotojų pasiekiamumą, kontrolę ir suteikia galimybę efektyviai dirbti bet kur ir bet kada, taip padidindami jų našumą.

Darbuotojams yra nepatogu, kai jie darbui turi naudoti įmonės išskirtus mobiliuosius įrenginius, o ne asmeninius. Tokiu atveju tam pačiam darbuotojui tenka naudotis dviem ar daugiau įrenginiais vienu metu. Norint to išvengti ir sukurti patogesnę darbo sferą, pasaulyje ėmė plačiai plisti asmeninių įrenginių naudojimo įmonėse tendencija, dar vadinama atsinešk savo įrenginį (*angl. Bring your own device*). Asmeninių įrenginių naudojimas įmonėse darbuotojui suteikia labai daug privalumų, tačiau tuo pačiu metu ši tendencija sukelia papildomas saugumo grėsmes įmonei.

Asmeninių įrenginių naudojimas įmonėse sukelia grėsmę jos konfidencialiems duomenis ir informaciniams resursams. Ši problema atsiranda dėl to, kad šiuolaikiniai mobilieji įrenginiai turi daug saugumo spragų, tokių kaip [1]: piktavališkos programėlės; komunikacijų perėmimas (*angl. Man-in-the-midle*), tiesioginės įsilaužėlių atakos, neteisinga vartotojų elgsena ar pavogti ir pamesti įrenginiai.

Asmeninių įrenginių, naudojamų įmonėse, saugumui užtikrinti yra būtina sudaryti mobiliųjų įrenginių saugumo politiką. Saugumo politika – tai taisyklių ir dokumentų rinkinys, kuris nurodo kokias saugos priemones reikia diegti į įrenginius, kaip jais naudotis bei apibrėžia įmonės darbuotojų pareigas ir atsakomybes. Vienas didžiausių iššūkių su kuriais susiduria įmonė – kaip užtikrinti, kad jos darbuotojai laikytųsi saugumo politikos. Įmonės saugumo politikos įgyvendinimą ir kontrolę, leistų užtikrinti saugaus konfigūravimo paramos sistema, kuri suteiktų nuotolinio mobiliųjų įrenginių konfigūravimo ir priežiūros funkcijas.

Magistrinio darbo tikslas – sukurti asmeninių mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos (SKP) sistemą.

Darbo tikslui pasiekti išsikelti uždaviniai:

- Atlikti mobiliųjų įrenginių pažeidžiamumų ir įmonėms kylančių grėsmių analizę;
- Išnagrinėti mobiliųjų įrenginių saugos priemones;
- Sudaryti asmeninių mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos modelį;
- Remiantis sudarytu modeliu realizuoti sistemos prototipą;
- Naudojantis prototipu atlikti sistemos greitaveikos priklausomybės nuo žiniatinklio paslaugų konfigūracijų eksperimentinį tyrimą;
- Išnagrinėti eksperimentų metu gautus rezultatus ir pateikti rekomendacijas, kokios žiniatinklio paslaugų konfigūracijos turėtų būti naudojamos sistemoje.

2. MOBILIŲ ĮRENGINIŲ, NAUDOJAMŲ ĮMONĖSE, SAUGUMO ANALIZĖ

Pačioje pradžioje, kuriant pirmuosius mobiliuosius įrenginius jiems nereikėjo aukšto lygio apsaugos, nes tuo metu nebuvo jokių rimtų saugumo grėsmių. Tačiau šiandien pasikeitus situacijai ir atsiradus daugybei saugumo grėsmių mobilieji įrenginiai vis dar turi daug saugumo spragų, kurias gali išnaudoti piktavaliai. Nors ir kuriant naujas mobiliųjų įrenginių operacinių sistemų versijas daug dėmesio yra skiriama jų saugai, tačiau juose vis tiek išlieka daug pažeidžiamumų, tokių kaip [1]:

- Piktavališkos programėlės;
- Komunikacijų perėmimas;
- Tiesioginės įsilaužėlių atakos;
- Pavogti ar pamesti įrenginiai;
- Neteisinga vartotojų elgsena.

Dėl paminėtų mobiliųjų įrenginių saugumo spragų įmonėms iškyla tokios grėsmės kaip:

- Konfidencialios informacijos praradimas ar vagystė;
- Prieigos prie įmonės informacinių resursų suteikimas neautorizuotiems asmenims.

Asmeninių įrenginių, naudojamų įmonėse, saugumui užtikrinti yra būtina sudaryti mobiliųjų įrenginių saugumo politiką. Saugumo politika – tai taisyklių ir dokumentų rinkinys, kuris nurodo kokias apsaugos priemones reikia naudoti ir diegti į įrenginius, kaip reikia saugiai jais naudotis bei apibrėžia įmonės darbuotojų pareigas ir atsakomybes. Remiantis sudaryta saugumo politika turi būti realizuotos atitinkamos techninės priemonės, kurios apsaugo mobiliuosius įrenginius nuo saugumo grėsmių ir užtikrina, kad darbuotojai laikytųsi apibrėžtų taisyklių.

2.1. Saugumo grėsmės

Viena iš grėsmių su kuriomis susiduria mobilieji įrenginiai - virusai, tačiau skirtingai negu personaliniuose kompiuteriuose tai nėra pati didžiausia saugumo spraga. Daug didesnį pavojų kelia nesaugus programinis kodas ar neteisingai veikiančios programėlės. Nuo šių pavojų neapsaugo standartinės apsaugos priemonės, nes jos dažniausiai yra orientuotos į apsaugą nuo virusų. Taip pat įmonėms didelę grėsmę kelia netyčinis arba piktavališkas darbuotojų piktnaudžiavimas mobiliaisiais įrenginiais. Gan dažnai, įrenginiai, kuriuose yra konfidencialių įmonės duomenų, yra pametami ar netgi pavagiami. Dažniausiai nuo šio pavojaus neapsaugo ir slaptažodžiai bei duomenų šifravimas.

Užkirsti kelią saugumo pažeidimams trukdo ir tai, kad dauguma įmonių neturi nuotolinio mobiliųjų įrenginių valdymo ir audito įrankių. Naudojantis šiais įrankiais, įvykus saugumo pažeidimui, įmonė gali sužinoti kokia informacija buvo paveikta, taip pat gali nuotoliniu būdu šiuos duomenis ištrinti ar susekti kur yra prarastas mobilusis įrenginys. Informacinių sistemų valdymo specifikacija „ISO 27001“ apibrėžia, kad įmonėse privalo būti naudojami nuotolinio mobiliųjų įrenginių valdymo ir audito įrankiai [1].

2.1.1. Kenkėjiškos programėlės

Šiuolaikiniai mobilieji įrenginiai pasiekė galingumus artimus personaliniams kompiuteriams. Tai padėjo išpopuliarėti mobiliųjų įrenginių operacinėms sistemos: „Android“, „iOS“ ir „Windows phone“, kurios suteikia galimybę savo įrenginyje įsidiegti įvairias programėles. Galimybė mobiliajame įrenginyje diegti papildomą programinę įrangą pavertė šiuos įrenginius kenkėjiškų programėlių taikiniu. Jos yra skirtos mobiliųjų įrenginių darbo sutrikdymui ir juose esančios informacijos vientisumo ir konfidencialumo pažeidimui. Šios programos gali būti įvairių formų: programinio kodo, scenarijų (*angl. Script*), aktyviojo turinio ir kitos.

Apsaugą nuo kenkėjiškų programų mobiliuosiuose įrenginiuose apsunkina riboti šių įrenginių resursai. Diagnostinės informacijos rinkimas ir kitos apsaugos technologijos naudojamos personaliniuose kompiuteriuose šiuo atveju netinka, nes jos stipriai sumažintų išmaniųjų įrenginių darbo našumą. Saugumo grėsmių valdymas mobiliuosiuose įrenginiuose yra daug brangesnis procesas negu personaliniuose kompiuteriuose. Šią kainą iškelia nuolatinis mobiliųjų įrenginių technologijų kitimas. Tuo tarpu kai kurios atakos nukreiptos prieš šiuos įrenginius, tokios kaip slaptas GSM ryšio pasiklausimas (*angl. Eavesdropping*), yra ganėtinai pigios [2].

Toks spartus išmaniųjų telefonų, planšetinių kompiuterių ir kitų mobiliųjų įrenginių tobulėjimas suteikia ne tik platesnes darbo ir pramogų galimybes, bet ir papildomas galimybes programišiams. Piktavališkos programos į šiuolaikinius mobiliuosius įrenginius gali patekti keletu kelių: atsisiunčiant jas iš programėlių parduotuvių („Google play“ ar „Apple App Store“), naršant po internetą, „bluetooth“ ar kitais bevielio ryšio kanalais. Šios piktavališkos programos gali atlikti tokius veiksmus kaip: persiųsti konfidencialią informaciją, neteisėtai prisijungti prie įrenginio mikrofono ar kameros, nuskaityti įrenginio identifikavimo informacija (PIN, IMEI ir t.t.), naudojantis GPS ar GSM operatorių celių informacija nustatyti vartotojo būvimo vietą, išnaudoti įrenginio bateriją, ir įvairius kitus piktavališkus veiksmus [3, 4].

2.1.2. Sukčiavimas apsimetant ir socialinė inžinerija

Dar viena šiuo metu labai aktuali mobiliųjų įrenginių grėsmė yra sukčiavimas apsimetant (*angl. Phishing*) ir socialinė inžinerija. Programišiai pasinaudodami šiomis atakomis stengiasi iš mobiliųjų įrenginių vartotojų išgauti konfidencialią informaciją tokią kaip elektroninės bankininkystės ar socialinių tinklų prisijungimo duomenys. Tam atlikti gali būti pasitelkiamas SMS žinučių ar elektroninių laiškų su netikromis nuorodomis siuntimas, netikri internetiniai puslapiai ar mobiliosios programėlės, kurios reikalauja vieningo prisijungimo (*angl. Single sign on*) ir kiti metodai [5].

Siunčiant suklastotas SMS žinutes dažniau reikalaujama, kad vartotojas perskambintų suklastotu numeriu negu, kad atidarytų nuorodą. Kuomet yra atliekamas skambutis, dažniausiai atsiliepia mašina su iš anksto įrašytu garso įrašu, kuris prašo, kad auka pateiktų tam tikrą asmeninę informaciją [1].

Taip pat socialiniams tinklapiams tapus neatsiejama mūsų kasdienybės dalimi, programišiai savo atakas nukreipė ir į juos. Dažniausiai atakoms yra išnaudojama vieningo prisijungimo sistema, kuri leidžia kažkokioje sistemoje autorizaciją atlikti su socialinio tinklapio paskyra („Facebook“, „Twitter“, „Google+“ ir kt.). Programišiai tai išnaudoja kurdami netikrus interneto puslapius ar mobiliąsias programėles, kurios naudoją vieningo prisijungimo funkciją. Vartotojui prisijungus prie tokios suklastotos sistemos, užpuolikas gali pasiekti visą jo asmeninę informaciją esančią socialinio puslapio paskyroje [1].

2.1.3. Tiesioginės programišių atakos

Vienas iš tiesioginės programišių atakos pavyzdžių gali būti PIN kodo arba šablono, kuris yra naudojamas mobiliojo įrenginio atrakinimui, nulaužimas. Naudojant standartinius 4 simbolių PIN kodus arba standartinius šablonus, jų nulaužimas kvalifikuotam programišiui nesudaro jokių problemų. Atlikus šią ataką puolėjas gali prieiti prie visų mobiliajame įrenginyje saugomų duomenų ir nepalikti nusikaltimo vietoje jokių pastebimų įkalčių. Dėl šios priežasties auka net nesupras, kad jos duomenų konfidencialumas buvo pažeistas.

Norint apsisaugoti nuo šitokių atakų reikėtų naudoti sudėtingus slaptažodžius nes 4 simbolių PIN kodas panaudojant šiuolaikines technologijas yra nulaužiamas per keletą sekundžių, tuo tarpu 16 simbolių kodui nulaužti reikia keliasdešimties metų. Taip pat nereikėtų naudoti dažnai pasitaikančių

ar labai parastų slaptažodžių, kurie sudaryti iš tam tikrų žodžių ir viešai prieinamos vartotojo informacijos, tokios kaip įvairios datos [1].

Kitas tiesioginių atakų kelias yra operacinių sistemų pažeidžiamumai. Pavyzdžiui, iOS 7 operacinės sistemos pažeidžiamumas, kuomet atitinkamu metu iškviečiant programų perjungimo meniu (du kart spustelėjus „namų“ mygtuką) yra apeinamas slaptažodžio užraktas ir galima atidaryti, bet kurią vartotojo mobiliajame įrenginyje tuo metu foniniame rėžime veikiančią programėlę [6]. Šitaip galima gauti neautorizuotą prieigą prie vartotojo kameros, nuotraukų galerijos, elektroninio pašto bei socialinių puslapių paskyrų.

Programišiai tiesiogines atakas prieš mobiliuosius įrenginius gali atlikti ir panaudodami įvairius priedelius, kurie prie mobiliojo įrenginio jungiasi tiesiogiai arba per „bluetooth“, „wi-fi“ bei kitokius bevielio ryšio kanalus.

2.1.4. Komunikacijų perėmimas

Komunikacijų perėmimas arba dar kitaip vadinama žmogaus viduryje ataka (*angl. Man-in-the-*middle) kelia didelę grėsmę mobiliesiems įrenginiams. Atlikti tyrimai rodo, kad dauguma mobiliuosiuose įrenginiuose naudojamos programinės įrangos yra neatspari komunikacijų perėmimo atakoms [1].

Prisijungus prie bevielio ryšio prieigos taško ir naudojant atitinkamus tinklo analizės įrankius galima nesudėtingai perimti visą per šį tinklo įrenginį praeinantį duomenų srautą. Vėliau, panaudojant tuos pačius įrankius, analizuojant duomenis galima sužinoti įvairią perduodamą informaciją. Paprasčiausiu atveju naudojant šią ataką galima sužinoti įvairius vartotojų autorizacijos duomenis, pvz. elektroninės bankininkystės ar socialinių tinklapių prisijungimo vardus ir slaptažodžius. Šioms atakoms gali būti panaudojami tokie įrankiai kaip: „Arpspoof“ ar „Arpoison“ skirti MAC adresų klastojimui, „SSLstrip“ skirtas HTTPS ryšio perėmimui, „Wireshark“ ar „Capsa“ skirti paketinių duomenų analizavimui.

Komunikacijų perėmimo atakos gali būti panaudotos ir duomenų perduodamų „bluetooth“ ryšiu perėmimui. Pavyzdžiui, tokios atakos taikiniu gali būti „bluetooth“ spausdintuvas. Šioje atakoje yra išnaudojamas neautorizuoto „bluetooth“ ryšio sudarymas. Visų pirma puolėjas, panaudodamas DoS ataką, sutrikdo ryšio sudarymą tarp mobiliojo įrenginio ir spausdintuvo. Kai auka bando sudaryti sujungimą iš naujo, puolėjo naudojamas įrenginys vienu metu apsimeta ir spausdintuvu, ir sujungimą inicijuojančiu įrenginiu, šitaip jis sujungimą sudaro su abiem ryšį sudarančiais subjektais. Vėliau nieko neįtardamas mobilusis įrenginys visus duomenis į spausdintuvą siunčia per puolėjo įrenginį, šitaip jis gauna prieigą prie visų siunčiamų duomenų.

2.1.5. Pamesti ir pavogti mobilieji įrenginiai

Labai didelę grėsmę įmonių saugumui sukelia pamesti arba pavogti mobilieji įrenginiai. Pasak „Kaspersky Lab“ įmonės 2014 m. atliktos apklausos [7] net 26% apklausoje dalyvavusių įmonių, pasauliniu mastu, patyrė incidentų su pamestais ar pavogtais mobiliaisiais įrenginiais. Apklausa taip pat byloja, kad apie 50% įvykių įmonei buvo pranešta vėliau kaip po dienos, dėl to įmonės aptyrė dar didesnę žalą. Iš tikrųjų, mobiliųjų įrenginių praradimas įmonėms atneša daug didesnius finansinius nuostolius negu piktavališkos programos. O tokia neigiama statistika byloja, kad egzistuoja labai didelė rizika, kad įrenginys su konfidencialiais įmonės duomenimis bus prarastas. Norint parodyti šios grėsmės pavojingumą galima pateikti pavyzdį kuomet vienas Volstryto (*angl. Wall Street*) biržos makleris išeidamas iš darbo pardavė savo tariamai nebeveikiantį mobilųjį telefoną „Blackberry“. Pirkėjui tereikėjo pakeisti šio įrenginio bateriją ir jis vėl veikė. Šitaip pirkėjas gavo prieigą prie šimtų privačių elektroninių laiškų ir didžiulio, detalaus kontaktų sąrašo.

Įmonei norint apsisaugoti nuo konfidencialios informacijos praradimo, pametus ar buvus pavogtam mobiliajam įrenginiui, yra būtina diegti mobiliųjų įrenginių valdymo (*angl. Mobile device management*) sistemas. Šios sistemos gali užrakinti ir ištrinti duomenis iš mobiliųjų įrenginių nuotoliniu būdu, nustatyti įrenginio būvimo vietą bei suteikia įvairias kitas mobiliųjų įrenginių kontrolės ir audito funkcijas.

2.1.6. Pavojingi vartotojų veiksmai

Labai dažnai neteisingas įrenginių naudojimas sukelia įvairias saugumo grėsmes. Darbuotojai naudodamiesi įrenginiu gali netyčia, nesuprasdami, kad pažeidžia saugumo politiką, arba piktavališkai ją pažeisti. Dažniausiai darbuotojai tai atlieka siekdami patogesnio darbo su įrenginiu arba jie tiesiog nesuvokia kylančių saugumo grėsmių. Šis pažeidžiamumas yra ypač aktualus mobiliesiems įrenginiams, kuriuose riba tarp įrenginio naudojimo asmeniniams ir darbo tikslams dažniausiai yra sunkiai apibrėžiama arba tiesiog ignoruojama.

Labai dažnai, vartotojai nenaudoja apsauginės programinės įrangos, antivirusinių programų bei užkardų. Siunčiasi užkrėstas ir kenkėjiškas programėles iš interneto. Nesilaiko įmonės saugumo politikos siunčiant žinutes ar dalinantis failais, šitaip konfidenciali įmonės informacija gali būti išsiųsta neautorizuotiems asmenims. Čia tik keletas grėsmių pavyzdžių, kurias gali sukelti vartotojai neteisingai besinaudodami mobiliaisiais įrenginiais. Apklausos rodo, kad didžioji dauguma darbuotojų nėra susipažinę su įmonės saugumo politika, o trečdalis apklaustųjų teigė, kad jie yra priversti nusižengti saugumo politikai, tam kad galėtų atlikti savo darbą [1].

Piktavaliai darbuotojai taip pat kelia labai didelį pavojų įmonės saugumui. Tai gali būti nepatenkinti darbuotojai siekiantys keršto, buvę darbuotojai, kurie konfidencialia informacija pasidalina su būsimais darbuotojais arba ją parduoda siekdami pasipelnyti. Šiuos piktavališkus veiksmus labai palengvina mobiliųjų įrenginių naudojimas, nes vartotojas darbe naudoja asmeninius įrenginius, todėl ir visą konfidencialią informaciją, kartu su įrenginiu parsineša namo.

2.2. Apsaugos priemonės

Efektyvios įmonių saugumo programos turi atsižvelgti į keletą mobiliųjų įrenginių saugumo aspektų: vartotojų elgsena, prieiga prie įrenginio ir įmonės tinklų, komunikacijas ir duomenų saugojimą. Vartotojai yra įpratę mobiliaisiais įrenginiais naudotis nekreipiant dėmesio į jų saugumo aspektus. Dėl šios priežasties duomenų, esančių mobiliuosiuose įrenginiuose, apsaugai įmonės turėtų naudoti šifravimą, užkardas, antivirusines programas, skaitmeninius sertifikatus, nuotolinio įrenginio užrakinimo ir duomenų ištrynimo funkcijas. VPT technologijos gali būti naudojamos norint užtikrinti saugius komunikacijų kanalus viešaisiais tinklais. Tinklų apsaugai gali būti naudojami įvairūs autentifikavimo protokolai tokie kaip „RADIUS“, o bevielio ryšio tinklai turėtų būti apsaugomi naudojant WPA ar WPA2 saugos protokolus. Taip pat yra būtina atsižvelgti į skirtingų mobiliųjų įrenginių platformų saugumo aspektus, kadangi darbdavys ne visada gali kontroliuoti arba uždrausti tam tikrų įrenginių naudojimą įmonėje.

2.2.1. Darbuotojų kontrolė

Didžiausias iššūkis su kuriuo susiduria įmonė siekdama mobiliųjų įrenginių saugumo yra ne technologinis, bet socialinis. Tai reiškia, kad daug sudėtingiau yra užtikrinti arba priversti darbuotojus teisingai ir saugiai naudotis mobiliaisiais įrenginiais negu įdiegti saugumo technologijas tokias kaip antivirusinės programos ar užkardos. Įmonės turi ribotas galimybes priversti darbuotojus laikytis saugumo politikos, todėl šiuo atveju yra labai svarbus darbuotojų požiūris į mobiliųjų įrenginių saugumą. Netgi ir tuo atveju kai mobiliuosius įrenginius išduoda įmonė, dauguma

darbuotojų į juos žiūriu kaip į asmeninius įrenginius skirtus ne tik darbui, bet ir pramogoms bei asmeniniam naudojimui. Šis požiūris darbuotojus nukreipia link neprofesionalaus ir nesaugaus mobiliųjų įrenginių naudojimo. Saugumo problemų suvokimas yra labai svarbus faktorius siekiant užtikrinti įmonės duomenų konfidencialumą ir vientisumą. Vienintelis būdas užtikrinti, kad darbuotojai tinkamai naudotųsi mobiliaisiais įrenginiais yra įvairūs mokymai orientuoti į informacinių technologijų saugą, tačiau dar svarbesnis šios problemos aspektas yra grėsmių ir rizikos suvokimas. „Economist Intelligence Unit“ įmonės atlikta apklausa parodo, kad tik trečdalis įmonių pasauliniu mastu vykdo mokymus orientuos į mobiliųjų įrenginių saugą. Tai parodo, kad didžioji dalis įmonių administracijos vis dar nesuvokia grėsmių, kurias sukelia mobilių įrenginių naudojimas. Darbuotojai privalo turėti pagrindines žinias apie visą informacinių technologijų saugą pradedant nuo duomenų praradimo ar vagystės iki kenkėjiškos programinės įrangos ir duomenų šifravimo. Darbuotojai turi prisiimti atsakomybę už savo naudojamų mobiliųjų telefonų ir kitų įrenginių saugumą ir juose esančius įmonės duomenis [1].

2.2.2. Saugumo politikos ir jų sudarymas

Saugos mechanizmų ir įrankių diegimo į mobiliuosius įrenginius efektyvumas priklauso nuo įmonės saugumo programos ir joje naudojamų saugumo politikų išsamumo. Prieš perkant ir diegiant antivirusines programas, užkardas ar įsilaužimo aptikimo sistemas reikia sukurti detalias saugumo politikas, kurios aprašytų šių saugumo įrankių naudojimo ir konfigūravimo reikalavimus. Pradedant kurti saugumo politikas mobiliesiems įrenginiams galima pasinaudoti nešiojamųjų kompiuterių saugomo politikomis, kaip pradžios tašku. Aukšto lygio mobiliųjų įrenginių saugumo politikos yra neatsiejama įmonės saugumo programos dalis. Jose turėtų būti aprašyta:

- Įmonės duomenų klasifikaciją, kad įmonės darbuotojai žinotų, kurie duomenys yra konfidencialūs ir kaip su jais reikia elgtis.
- Kokius mobiliųjų įrenginių modelius galima naudoti įmonėje.
- Kokios programėlės gali ar privalo būti įdiegtos į įrenginį.
- Kada, kokiomis ir kaip programėlėmis galima naudotis.
- Aprašytos nuotolinio prisijungimo taisyklės.
- Darbuotojų pareigos ir atsakomybės.
- Kitos mobiliųjų įrenginių saugą apibrėžiančios taisyklės ir reikalavimai.

Saugumo politikos taip pat turėtų atsižvelgti į mobiliųjų įrenginių duomenų apsaugos galimybes, kurios gali būti daug mažesnės už personalinių kompiuterių. Apsauginė programinė įranga ir jos konfigūracijos turėtų būti parenkamos remiantis įmonės saugumo politikomis. Papildomos procedūros skirtos mobiliųjų įrenginių kontrolei ir priežiūrai taip pat yra būtinos [1].

Saugumo politikos, procedūros ir technologijos yra trys keliai kuriais įmonė gali kontroliuoti mobiliųjų įrenginių keliamą grėsmę. Politikos turėtų uždrausti duomenų, nesusijusių su darbu, tokių kaip žaidimai, vaizdo klipai ar muzikos failai, siuntimąsi iš interneto. Apriboti MMS žinučių siuntimo funkcijas. Reikalauti, kad įrenginyje būtų įdiegta apsauginė programinė įranga. Procedūros turėtų apibrėžti kokie mobilūs įrenginiai ir taikomosios programos gali būti naudojamos įmonėje, valdyti apsauginę programinę įrangą ir pateikti metodus saugumo politikų įgyvendinimui. Technologijos turėtų būti panaudotos prieigos kontrolei, duomenų vientisumo ir konfidencialumo užtikrinimui ir apsaugai nuo tiesioginių atakų. Taip pat kritiškai svarbus įmonės saugumo programos aspektas darbuotojų mokymai ir supažindinimas su mobiliųjų įrenginių keliamomis grėsmėmis.

Dauguma įmonių, mobiliųjų įrenginių saugos valdymui naudoja centralizuotas sistemas. Šiose sistemose saugumo politikos ir audito programinė įranga yra naudojama kontroliuoti mobiliųjų

įrenginių darbą nuotoliniu būdu. Svarbiausios centralizuotų mobiliųjų įrenginių valdymo sistemų savybės: prie tinklo prisijungusių įrenginių sekimas ir kontrolė bei programinės įrangos ir saugumo atnaujinimai nuotoliniu būdu. Įmonės siekia, kad šių sistemų naudojimas, dėl griežtų reikalavimų, nesumažintų mobiliųjų įrenginių patrauklumo darbui ir darbuotojams būtų priimtina įmonėje naudoti savo asmeninius įrenginius. Nors ir stipri saugumo politika yra būtina įmonės duomenų ir informacinių resursų apsaugai, tačiau ji neturėtų sumažinti darbo efektyvumo ir turėtų būti priimtina darbuotojams.

Pirmosios mobiliųjų įrenginių saugumo valdymo rekomendacijos buvo išleistos 2008 metai standartų agentūros NIST (*angl. National Institute of Standards and Technology*). Naujausia šių rekomendacijų versija buvo išleista 2013 metais. NIST pateiktos rekomendacijos aprašo penkias mobiliųjų įrenginių saugumo programos sudarymo sritis [1].

1. Mobiliųjų įrenginių saugumo politikos kūrimą;
2. Saugumo plano, kuris aprašo įrenginių išdavimą ir naudojimą įmonėje, sudarymą;
3. Rizikos analizę;
4. Įmonės darbuotojų mokymus mobilių įrenginių saugumo tema;
5. Centralizuotos mobiliųjų įrenginių priežiūros ir konfigūravimo sistemos reikalavimus.

2.2.3. Prieigos kontrolė

Autentifikavimas

Autentifikavimas tai procesas kuris užtikrina, kad tik autorizuoti asmenys, kuriems yra suteikta prieiga prie sistemos ar įrenginio, galėtų jais pasinaudoti. Autorizacijai atlikti yra naudojamos trys technologijos: tai ką tu žinai; tai kas tu esi arba tai ką tu turi. Pirmuoju atveju autentifikavimui yra naudojama kokia nors informacija, kurią žino tik autorizuotas asmuo, dažnai tai yra prisijungimo vardas ir slaptažodis ar PIN kodas. Antroji technologija vartotojų autentifikavimui naudoja įvairius unikalius žmogaus biometrinius duomenis, tokius kaip: pirštų anspaudai, veido atpažinimas ar akies rainelės skanavimas. Ką tu turi, metodai dažniausiai naudoja žetonus, tai yra tam tikras fizinis objektas, kuris naudojamas asmeniui autentifikuoti. Tai gali būti: skaitmeninė kortelė ar USB raktas su elektroniniu parašu. Norint užtikrinti didesnį saugumo lygį yra naudojamas dviejų pakopų autentifikavimas. Šis mechanizmas reikalauja panaudoti dvi iš trijų paminėtų autentifikavimo technologijų [8].

Nors dažniausiai mobilusis įrenginys turi tik vieną šeimininką, tačiau dėl anksčiau minėtų praradimo ir vagystės grėsmių yra būtina prieigai prie įrenginio naudoti aukšto saugumo lygio autentifikavimo mechanizmą.

Kontekstu pagrįsta prieigos kontrolė

Kontekstu pagrįsta prieigos kontrolė suteikia galimybę prieigą prie įmonės duomenų, informacinių resursų ar programėlių mobiliajame įrenginyje suteikti atsižvelgiant į tam tikras sąlygas. Šios sąlygos gali būti: vieta kurioje yra vartotojas, data, laikas, tinklo, prie kurio yra prisijungęs įrenginys, parametrai ar mobiliojo įrenginio konfigūracijos. Galima pateikti tokį pavyzdį, darbuotojas įmonės konfidencialią informaciją savo išmaniajame telefone gali pasiekti tik fiziškai būdamas įmonės ofise, būnant kur nors kitur prieiga prie šių duomenų yra uždraudžiama. Šitaip konfidencialią informaciją, esančią įrenginyje, galima apsaugoti nuo netinkamo naudojimo ar vagystės [9].

Duomenų šifravimas

Mobilieji įrenginiai yra ganėtinai dažnai pametami ar pavagiami. Norint užtikrinti duomenų konfidencialumą yra būtina naudoti šifravimą, tuomet net ir pametus įrenginį neautorizuoti asmenys

negalės nuskaityti jame esančių duomenų. Dauguma mobiliųjų įrenginių operacinių sistemų, tokių kaip „Android“ ar „iOS“, turi integruotus šifravimo įrankius, kuriuos tereikia įsijungti įrenginio nustatymuose. Šie įrankiai suteikia galimybę automatiškai šifruoti visus arba tam tikrus duomenis esančius įrenginyje. Esant būtinybei galima naudoti ir papildomą programinę įrangą skirtą duomenų šifravimui [10, 11].

Skaitmeniniai parašai ir sertifikatai

Skaitmeniniai parašai naudoja maišos funkcijas tam, kad užtikrintų duomenų vientisumą ir įrodytų duomenis siunčiančių asmenų tapatybę. Tapatybės įrodymui yra naudojamas neatsižadėjimo (*angl. Non-repudiation*) principas. Jis užtikrina, kad asmuo išsiuntęs duomenis ir asmuo juos gavęs niekaip to negalėtų paneigti. Taip pat skaitmeniniai parašai yra naudojami programinio kodo pasirašymui. Kodo pasirašymas leidžia garantuoti, kad jis nebuvo pakeistas ar kaip nors sugadintas. Norint užtikrinti parašų ir asimetrinių raktų, kurie yra naudojami jiems generuoti, teisėtumą yra naudojami skaitmeniniai sertifikatai. Šiuos sertifikatus išduoda patikimos sertifikavimo institucijos (*angl. Certificate authority*) [1].

2.2.4. Saugaus ryšio užtikrinimas

Šifravimas ir VPT

Duomenų šifravimas yra neatsiejama saugaus duomenų perdavimo ryšio kanalais dalis. Šifravimas panaudoja matematinius algoritmus tam, kad perduodamus duomenis paverstų nesuprantamais asmenims, kurie neturi šifravimo rakto. Duomenų šifravimui gali būti naudojami simetrinio ir asimetrinio šifravimo algoritmai. Simetrinio šifravimo atveju duomenų užšifravimui ir iššifravimui yra naudojamas vienodas šifravimo raktas. Asimetrinio šifravimo atveju yra naudojami skirtingi raktai (viešasis ir privatusis).

Virtualūs privatūs tinklai – tai technologija, kuri leidžia naudojantis interneto tinklu sudaryti saugius sujungimus ir jais saugiai perduoti duomenis. Saugumo užtikrinimui ši technologija naudoją duomenų šifravimo ir paketų tuneliavimo mechanizmus. Dažniausiai yra naudojami IPSec, L2TP ar PPTP virtualių privačių tinklų protokolai [1].

Korinio mobiliojo ryšio tinklai

Korinio mobiliojo ryšio tinklų kategorijai priklauso daug skirtingų bevielio ryšio technologijų, tai tokios technologijos kaip GSM, UMTS, WCDMA ar LTE. Šiose technologijose naudojami protokolai užtikrina vartotojų identifikavimą, apmokestinimą, duomenų šifravimą ir privatumo apsaugą. Vartotojų ir įrenginių identifikavimui šiose technologijose yra naudojami unikalūs identifikatoriai, kurie yra įrašomi į telefoną (įrenginio identifikacija) ir į SIM kortelę (vartotojo identifikacija). Pranešus mobiliojo ryšio paslaugų tiekėjui, kad telefonas yra pavogtas, jį galimą užblokuoti, pasinaudojant įrenginio identifikatoriumi, šitaip užkertant kelią vagiui juo pasinaudoti. Komunikacijų konfidencialumui užtikrinti, korinio ryšio technologijos naudoja vartotojų ir įrenginių autentifikavimą bei duomenų šifravimą [1].

Bevieliai vietiniai tinklai

Bevielės vietinio tinklo technologijos dar vadinamos „Wi-Fi“ (IEEE 802.11) apsaugai pačioje pradžioje buvo sukurtas WEP saugumo protokolas. Jis apibūdina kokie autentifikavimo ir šifravimo mechanizmai turėtų būti naudojami tinklo apsaugai. Tačiau pasinaudojant šiuolaikinėmis technologijomis WEP slaptažodžiai gali būti nesunkiai „nulaužiami“, todėl jis yra nesaugus ir neturėtų būti naudojamas „Wi-Fi“ tinklų apsaugai.

Vėliau buvo sukurtas WPA saugos protokolas. Jis vartotojų autentifikavimui naudoja bendruosius (*angl. Prie-shared*) raktus arba RADIUS autentifikavimo serverius ir TKIP šifravimo

algoritmą. Nors ir pažangesnis už WEP, WPA protokolas yra neatsparus slaptažodžių „nulaužimo“ atakoms. Šis procesas naudojant standartinį personalinį kompiuterį gali užtrukti apie 100 valandų, tačiau panaudojus debesų kompiuteriją ir paskirstytuosius kompiuterinius skaičiavimus WPA slaptažodį galima „nulaužti“ per keliasdešimt minučių.

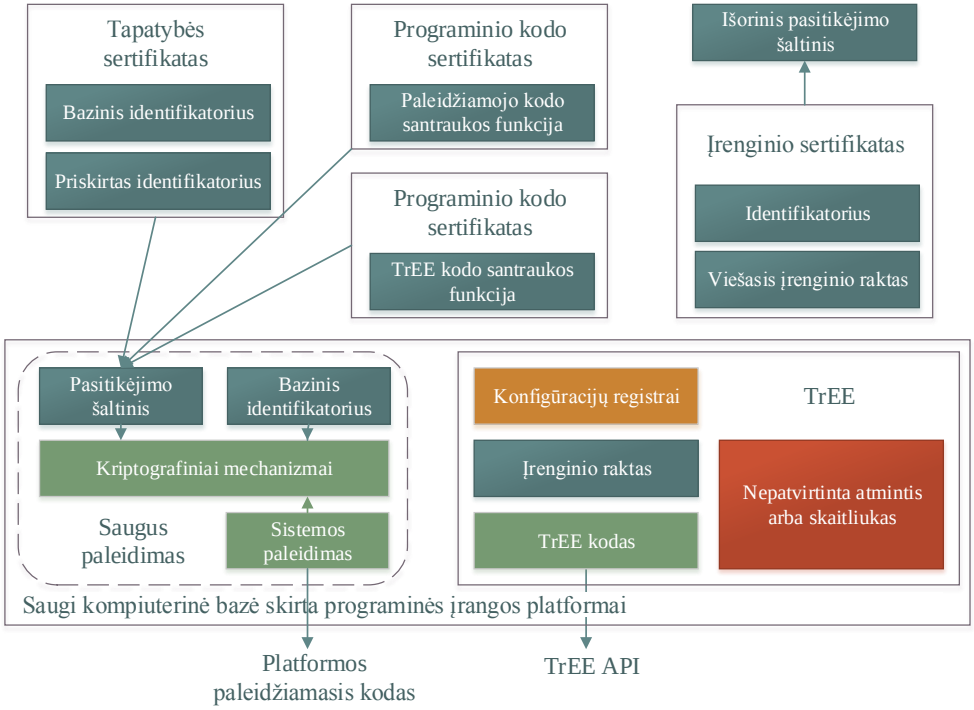
Įvertinus tai, efektyviai bevielių vietinių tinklų apsaugau yra rekomenduojama naudoti WPA saugos protokolą. Tai patobulinta WPA protokolo versija, kuri naudoja CCMP ir AES šifravimo algoritmus tinklo apsaugai užtikrinti [12].

„Bluetooth“

„Bluetooth“ bevielio ryšio technologija turi tris saugumo rėžimus. Pirmasis rėžimas nenaudoja jokių saugumo mechanizmų. Antrasis – saugumo mechanizmus pritaiko po sujungimo sudarymo, o trečiasis – saugumo mechanizmus pritaiko prieš sudarant sujungimą. Mobilieji įrenginiai bandantys prieiti prie tam tikrų paslaugų gali būti laikomi patikimais arba nepatikimais. Prieiga yra suteikiama tik patikimiems įrenginiams. „Bluetooth“ ryšio paslaugos yra skirstomos į tris lygius: nereikalaujančius jokių saugumo mechanizmų, reikalaujančius autentifikavimo ir reikalaujančius autentifikavimo ir autorizacijos. „Bluetooth“ ryšys yra neatsparus piktavališko kodo atakoms, todėl įrenginiuose, kurie naudojasi šiuo ryšiu turėtų būti naudojama antivirusinė programinė įranga [13].

„Bluetooth“ bevielis ryšys gali būti panaudotas įvykdyti stebėjimą, atlikti tiesiogines atakas ar pasiklausimą, kenkėjiško programinio kodo skleidimui ar komunikacijų perėmimui. Norint apsisaugoti nuo šių atakų, yra būtina naudoti įrenginių ir vartotojų autentifikavimą, duomenų šifravimą ir nepalikti įrenginio aptikimo rėžime, kai yra baigiama naudotis „bluetooth“ ryšio paslaugomis.

2.2.5. Aparatinė apsauga



2.1 pav. Bendrinė mobiliųjų įrenginių aparatinės apsaugos schema [14]

Mobilieji įrenginiai be programinių apsaugos priemonių taip pat naudoja ir aparatines apsaugos priemones (žr. 2.1 pav.). Visų pirma, kiekvienas įrenginys privalo turėti bent vieną bazinį identifikatorių. Mobiliuosiuose telefonuose tai yra IMEI numeris, tačiau juo gali būti ir bet koks kitas unikalus numeris. Numerio nekintamumą galima garantuoti jį įrašant įrenginio gamybos metu į ROM

atmintį. Antra, išorinės informacijos, tokios kaip sertifikatai, autentifikavimui įrenginys turi gamintojo viešojo rakto maišos reikšmę. Taip pat labai dažnai reikia, kad įrenginys turėtų daugiau negu vieną identifikatorių. To reikia pavyzdžiui, visų radijo ryšio sąsajų identifikacijai įrenginyje. Šie identifikatoriai yra rašomi ne į ROM atminty tam , kad juos būtų galima redaguoti ir po gamybos [14].

Kai kurie gamintojai savo įrenginiuose diegia saugaus paleidimo funkciją. Ši funkcija prieš paleisdama operacinę sistemą, patikrina jos vientisumą ir ji yra paleidžiama tik tuo atveju jeigu sistema nebuvo pažeista. Tai atliekama lyginant operacinės sistemos paleidimo maišos kodus. Šis saugaus paleidimo mechanizmas gali būti pritaikytas net tik OS paleidimui, bet ir kitokiai programinei įrangai.

Kai kurie apsaugos atvejai reikalauja izoliuoto programinio kodo vykdymo. Vienas iš būdų sukurti izoliuotą vykdymo aplinką - patikimą kompiuterinę sistemą tikrinti paleidimo metu, tačiau kai ši sistema yra visa operacinė sistema (jos branduolys), ji yra per didelė, kad nebūtu paliekamą jokių saugumo spragų. Dėl šios priežasties buvo sukurta patikimo vykdymo aplinka TrEE. Ši aplinka yra skirta izoliuotam programinio kodo elementų vykdymui.

„Smėlio dėžės“ (*angl. Sanbox*) mechanizmas yra dar vienas būdas apsaugoti mobiliuosius įrenginius nuo kenkėjiško programinio kodo. Vietoj to, kad jis užtikrintų programos kodo vientisumą, šis mechanizmas apriboja programų prieigą prie failų sistemos ir įrenginio funkcijų, taip užkirsdamas kelią kenkėjiškiems veiksmams. Mobiliųjų įrenginių operacinės sistemos, kurios naudoją „smėlio dėžės“ mechanizmą, gali sumažinti kenkėjiško kodo žalą iki tiek, kad žala bus padaroma tik užkrėstai programėlei. „Smėlio dėžės“ apsaugos mechanizmą naudoja didžioji dauguma šiuolaikinių mobiliųjų įrenginių operacinių sistemų [15].

„Google“ kompanijos plėtojama „Android“ operacinė sistema yra sukurta „Linux“ operacinės sistemos pagrindu. Šioje sistemoje kiekviena programa yra laikoma tarsi atskiras vartotojas. Todėl, jeigu „Android“ operacinėje sistemoje virusu užsikrėstų kokia nors programėlė (pavyzdžiui interneto naršyklės), žala bus padaroma tik jai ir sistema liks apsaugota. Tuo tarpu tipiniuose personaliniuose kompiuteriuose užkrėtęs vieną programą virusas gali laisvai plisti toliau po visą sistemą.

2.2.6. Programinė apsauga

Įsilaužimo aptikimo sistemos

Įsilaužimo aptikimo sistemos yra naudojamos identifikuoti neįprastus mobiliojo įrenginio ir jame esančių programėlių veiksmus. Jos leidžia aptikti ir apsaugoti įrenginį nuo kenkėjiškų programų veiksmų tokių kaip: baterijos, CPU, RAM ar kitų įrenginio resursų išnaudojimo. Taip pat IAS gali apsaugoti įrenginį nuo tiesioginių programišių atakų ar kenkėjiškų veiksmų (pvz. brangių skambučių atlikimo). Naudojant įsilaužimo aptikimo sistemas, jas yra būtina reguliariai atnaujinti, nes kenkėjiškos programos labai greitai vystosi ir pasenusi IAS gali nebeaptikti naujesnių kenkėjiškų programų atliekamų piktavališkų veiksmų [12].

Užkardos

Užkardos gali būti naudojamas užkirsti kelia neautorizuotai prieigai prie mobiliojo įrenginio. Jos gali apsaugoti konfidencialią informaciją nuo nutekėjimo. Net jeigu mobiliajame įrenginyje ir yra įdiegta tam tikra kenkėjiška programinė įranga, užkardos gali užkirsti kelią šioms programoms konfidencialius duomenis išsiųsti per įrenginio tinklo sąsajas. Taip pat užkardos gali užkirsti kelią kenkėjiškoms programoms patekti į mobilųjį įrenginį. Tačiau jos neužkerta kelio kenkėjišką programinį kodą persiųsti SMS ar MMS žinutėmis [1].

Antivirusinės programos ir kita apsauginė programinė įranga

Taip pat kaip ir personaliniuose kompiuteriuose, mobiliuosiuose įrenginiuose apsaugai nuo virusų galima diegti tam skirtas antivirusines programas. Šią programinę įrangą siūlo tokios įmonės kaip „Symantec“, „Kaspersky lab“ ar „McAfee“. Taip mobiliuosiuose įrenginiuose gali būti naudojama ir kita programinė įranga skirta apsaugai nuo „kirminų“, „trojos arklių“ ir įvairų kitų kenkėjiško programinio kodo atakų [12].

Nuotolinė mobiliųjų įrenginių kontrolė

Nuotolinės mobiliųjų įrenginių kontrolės sistemos gali aptikti įvairias problemas ir saugumo pažeidimus kylančiu įrenginiuose, atlikti jų auditą ir esant problemai imtis atitinkamų veiksmų jai išspręsti. Šios sistemos gali būti naudojamos mobiliųjų įrenginių būklės sekimui ar programinės įrangos, tokios kaip antivirusinės programos, įrašymui, atnaujinimui ir konfigūravimui. Taip pat šios sistemos suteikia vienus iš efektyviausių apsaugos mechanizmų duomenų apsaugai kai mobilieji įrenginiai yra pametami ar pavagiami. Šie apsaugos mechanizmai yra nuotolinis įrenginio išjungimas ir duomenų ištrynimas. Nuotolinės mobiliųjų įrenginių kontrolės sistemos naudojimas kartu su užkarda ir kontekstu paremtais prieigos valdymo mechanizmais dažniausiai užtikrina pakankamą saugumo lygį įmonei [16].

2.3. Mobiliųjų operacinių sistemų saugumo analizė

Mobiliųjų įrenginių gamintojai savo įrenginiuose pasirenka diegti skirtingas aparatinės apsaugos technologijas ir skirtingas operacines sistemas. Dėl šios priežasties sudarant įmonės mobiliųjų įrenginių saugumo politiką yra būtina atlikti skirtingų mobiliųjų įrenginių platformų saugumo analizę ir įvertinti jų saugumo pažeidžiamumus. Toliau šiame darbe analizuojame trijų šiuo metu pačių populiariausių mobiliųjų įrenginių platformų: „iOS“, „Android“ ir „Windows Phone“ saugumo galimybės.

2.3.1. iOS

Tai pirmoji tiesioginio manipuliavimo metodu veikianti operacinė sistema skirta mobiliesiems įrenginiams. Pirmoji šios operacinės sistemos versija buvo išleista 2007 m. ir ji buvo skirta tik „iPhone“ mobiliesiems įrenginiams. Vėliau ši operacinė sistema buvo pritaikyta ir „iPad“, „iPod Touch“ ir „Apple TV“ įrenginiams. Šiuo metu yra naudojama 8-oji šios operacinės sistemos versija.

„Apple“ kompanijos sukurta ir plėtojama platforma pasižymi programėlių parduotuve „App store“, kuri kelia pačius griežčiausius reikalavimus iš visų mobiliųjų platformų. Visos programėlės keliamos į šią parduotuvę yra patikrinamos „Apple“ kompanijos specialistų ir į parduotuvę patenka tik tos, kurios atitinka keliamus griežtus reikalavimus. Šie reikalavimai apibūdina ne tik programėlės vartotojo sąsają bet ir jos darbo našumą, bei saugą. Dėl šios priežasties ženkliai sumažinama kenkėjiškų programėlių grėsmė. „iOS“ programėlių architektūra suteikia aukštą saugumo lygį, nes kiekviena taikomoji programa yra leidžiama atskiroje „smėlio dėžėje“, t.y. visos programėlės dalinasi bendra atmintimi, tačiau jų duomenys tarpusavyje yra izoliuoti. Šios architektūros trūkumas yra tai, kad teoriniame lygmenyje bendras sistemos saugumo lygis yra tik toks aukštas kaip silpniausios programėlės. Taip pat „iOS“ operacinė sistema suteikia papildomas programėlių prieigos kontrolės galimybes. Programėlės be vartotojo leidimo negali pasiekti jokių įrenginio resursų (vietos nustatymas, kontaktai, nuotraukos ir t.t.) [10, 11].

„iOS“ platformos saugumas yra išplečiamas ir techninėmis įrenginio charakteristikomis. Visų pirma, šios platformos pagrindų veikiantys įrenginiai nenaudoja jokių išimamų duomenų laikmenų (atminties kortelių). Tai suteikia papildomą saugumo lygį. Taip pat, „5s“ ir naujesnio modelio

„iPhone“ mobilieji įrenginiai turi integruotą piršto antspaudų skenerį, kuris suteikia galimybę naudoti aukštesnio saugumo lygio autentifikavimą. Taip pat operacinė sistema turi ir standartinius PIN kodo ar slaptažodžio autentifikavimo mechanizmus.

Įmonėms „iOS“ operacinė sistema suteikia galimybę mobiliuosius įrenginius valdyti nuotoliniu būdu. Šiam tikslui gali būti naudojama „Apple“ kompanijos siūloma programinė įranga arba trečiųjų šalių produktai. Labai svarbu paminėti, kad „iOS“ operacinė sistema yra orientuota į vartotoją, tai reiškia, kad be darbuotojo leidimo IT administratorius naudodamasis nuotolinio valdymo programine įranga negalės atlikti jokių veiksmų su darbuotojo įrenginiu.

2.3.2. Android

„Android“ tai „Linux“ operacinės sistemos pagrindu sukurta mobiliųjų įrenginių operacinė sistema skirta įrenginiams su lietimui jautriais ekranais. Pirmasis mobilusis įrenginys, kuris veikė naudodamas šią OS buvo 2008 m. išleistas „HTC Dream“. Šiuo metu egzistuojanti pati naujausia stabili šios sistemos versija yra 5, kurios kodinis pavadinimas - „Lollipop“.

Kuriant „Android“ operacinę sistemą daug dėmesio buvo skirta jos saugumui. Tai teisėmis paremta operacinė sistema. Taikomosios programos šioje sistemoje veikia atskirose izoliuotose aplinkose. Kiekvienai programai vartotojas teises priskiria atskirai, diegimo metu. Tačiau labai dažnai vartotojai neįsigilina į tai kokių teisių reikalauja programėlė ir jai suteikia neaiškias teises, nesuvokdami ką ji gali su jomis atlikti. Nors šis modelis teoriškai ir yra saugesnis už bendrinį programų atskyrimą, naudojamą „iOS“ operacinėje sistemoje, tačiau jis visą atsakomybę už įrenginio saugumą perduoda, iš operacinės sistemos, vartotojui. Tai sukelia papildomą grėsmę kai įrenginį naudojantis darbuotojas nenusimano apie mobiliųjų įrenginių saugumą. Taip pat „Android“ operacinė sistema nuo 4.x versijos turi pilną įrenginio šifravimo galimybę, skirtą duomenų apsaugai. Ši platforma vartotojų autentifikavimui gali naudoti PIN kodus, slaptažodžius ar šablonus [10, 17].

„Android“ mobiliųjų įrenginių platforma susiduria su dviem labai didelėmis saugumo grėsmėmis. Visų pirma, labai didelė rinkos fragmentacija. Tai reiškia, kad vienu metu yra naudojama labai daug įvairių „Android“ operacinės sistemos versijų. Tai įvyksta dėl to, kad įrenginių gamintojai nesivargina leisti operacinės sistemos atnaujinimų senesniems įrenginių modeliams. Senų operacinės sistemos versijų naudojimas reiškia, kad šie įrenginiai neturi naujausių saugumo atnaujinimų, todėl jie yra pažeidžiami įvairiomis atakomis. Antroji problema, keliami per maži reikalavimai programėlėms keliamoms į „Google play“ ir įvairias trečiųjų šalių parduotuves. Piktavaliai tai panaudoja kenkėjiškų programėlių platinimui. Pasinaudojant sumania socialine inžinerija mobiliosios programėlės yra apipavidalinamos kaip naudingos ir reklamuojamos internete. Šitaip apgautas vartotojas nieko nenutuokdamas įsirašo piktavališką programėlę. „Android“ operacinė sistema pasižymi tuo, kad jai yra sukurta daugiausia kenkėjiškų mobiliųjų programėlių [17].

„Android 4.2 Jelly Bean“ operacinėje sistemos versijoje buvo pristatyti papildomi apsaugos mechanizmai skirti kovai su kenkėjiškomis programėlėmis. Šioje sistemos versijoje buvo pateiktas patobulintas taikomųjų programų teisių mechanizmas, taip pat įdiegta realaus laiko anti-kenkėjiškų programėlių aptikimo programinė įranga. Tačiau tai nereiškia, kad kenkėjiškų programėlių pavojus visiškai išnyko, nors ir naudojant papildomas saugumo priemones, vis tiek yra būtina atidžiai tikrinti kokios programėlės yra diegiamos į mobilųjį įrenginį [11].

2.3.3. Windows Phone

„Windows Phone“ – tai „Microsoft“ kompanijos sukurta operacinių sistemų serija skirta mobiliesiems įrenginiams. Pirmoji „Windows Phone“ sistemos versija buvo išleista 2010 m. Šiuo metu egzistuojanti naujausia šios operacinės sistemos versija yra „Windows Phone 8.1“.

Ši operacinė sistema naudoja panašų saugumo modelį kaip ir „Android“. Joje naudojamos minimalių privilegijų ir procesų izoliavimo technologijos. „Windows Phone“ terminais tai vadinama kambarių (*angl. Chamber*) suteikimu, kurie atitinka individualią proceso erdvę. Šie kambariai naudoja politikų sistemą. Šios politikos nurodo kokias sistemos funkcijas procesas esantis tame kambaryje gali naudoti. Įrenginio funkcijos, kurios programėlei suteikia konfidencialią vartotojo informaciją (vietos nustatymo ar kontaktų) yra vadinamos sugebėjimais (*angl. Capabilities*). Programėlėms prieiga prie šių įrenginio resursų yra suteikiama diegimo metu [10].

Į oficialiąją „Microsoft“ programėlių parduotuvę, programėles gali įkelti tik licencijuoti programuotojai, kurie yra užsiregistravę programėlių kūrimo programoje. Taip pat visos į parduotuvę keliamos programėlės privalo praeiti patikrinimą prieš pateikiant jas vartotojams. Dar viena apsaugos sistema skirta nelicencijuotų programėlių platinimui užkirsti yra skaitmeniniai sertifikatai ir parašai. Kuomet programuotojas užsiregistruoja į programėlių kūrimo programą jis gauna sertifikatą. Visos sukuriamos programėlės privalo būti pasirašytos su šiuo sertifikatu, nes „Windows Phone“ operacinėje sistemoje veikia tik pasirašytos taikomosios programos, kitu atvejo vartotojui programos paleisti nepavyks.

Vartotojų autentifikavimui „Windows Phone“ operacinė sistema naudoja standartinius PIN kodus ir slaptažodžius, tačiau atsisiuntus papildomą programinę įrangą galima naudoti ir šablonų mechanizmą. Taip pat, ši sistema suteikia galimybę SIM kortelę apsaugoti papildomu PIN kodu. Nežinant šio kodo nebus įmanoma atlikti skambučiu ar siųsti SMS žinučių.

Naujausia „Windows Phone 8.1“ operacinės sistemos versija suteikia dar didesnes saugumo galimybes. Visų pirma, ši sistema turi patobulintas informacijos teisių valdymo ir automatinio duomenų šifravimo funkcijas. Šios funkcijos yra skirtos vartotojo prieigos, prie elektroninių laiškų ir kitų duomenų saugomų „Windows“ serveriuose, kontrolei. Šiuo metu nei „Android“, nei „iOS“ operacinės sistemos šių funkcijų neturi. Kita saugumo sistema – realaus laiko pavojingų internetinių puslapių ekranas „SmartScreen“. Ši sistema yra įdiegta į „Microsoft Internet Explorer“ interneto naršyklę. Jeigu vartotojas nueina į pavojingą interneto puslapį jam apie tai yra parodomas įspėjamasis pranešimas. Galiausiai, „Microsoft“ kompanija pasiūlė vaikų kampelio (*angl. Kids Corner*) apsaugos sistema, ji skirta svarbių su darbu susijusių duomenų apsaugai nuo vaikų [11].

2.4. Vartotojų profiliavimas

Sudarant įmonės mobiliųjų įrenginių saugumo politiką yra būtina atsižvelgti į juos naudojančius darbuotojus. Kadangi įvairūs įmonės darbuotojai turi prieigą prie skirtingo saugumo lygio informacijos, todėl jiems turi būti keliami skirtingi saugumo reikalavimai. Dėl šios priežasties yra būtina naudoti vartotojų profiliavimą. Šiuo metu plačiausiai naudojami rolėmis pagrįsti prieigos metodai, tačiau kuriant saugumo politiką vartotojų profiliavimui galima panaudoti ir kitus diskrecinius ar mandatinius prieigos kontrolės modelius [8].

Naudojant rolėmis pagrįstus metodus yra sukuriama keletas vartotojų profilių atitinkančių tam tikras darbuotojų grupes. Tai galėtų būti tokios grupės kaip: eiliniai darbuotojai, vadybininkai ar direktoriai. Tuomet kiekvienai darbuotojų grupei atsižvelgiant į jų darbo specifiką ir prieinamus įmonės duomenis turi būti nustatoma kokias saugumo priemones reikia įdiegti mobiliuosiuose įrenginiuose. Dažniausiai tokios grupės kaip paprasti darbuotojai, rangovai ar laikini vartotojai nenaudoja labai griežtų saugumo priemonių, į kurias įeina sudėtingi autentifikavimo ir duomenų šifravimo mechanizmai. Kai kuriais atvejais vadybininkai turi prieigą prie aukšto konfidencialumo lygio informacijos tokios kaip darbuotojų asmeniniai duomenys ar jų atlyginimai, tuomet šios informacijos apsaugai įrenginyje turi būti naudojamos griežtos apsaugos priemonės. Rangovų arba

atsitiktinių vartotojų grupės sukelia papildomas saugumo grėsmes dėl labai dažno įrenginių savininkų kitimo ar įrenginio patekimo į kitos įmonės darbuotojų rankas. 2.1 lentelėje pateikiamas „Trend Micro“ įmonės sudarytas pavyzdinis darbuotojų profilių rinkinys [10].

2.1 lentelė Pavyzdinių vartotojų profilių apibrėžimai [10]

Profilis	Aprašymas
Direktoriai	Tai aukščiausią prieigos prie įmonės duomenų lygį turintys asmenys. Jie turi prieigą prie pačios slapčiausios ir jautriausios įmonei informacijos. Dėl didelio viešumo, jų įrenginiai gali būti atakuojami užpuolikų. Dėl šių priežasčių, jų įrenginiuose turi būti diegiami patys griežčiausi saugumo įrankiai ir technologijos.
Administracinio pobūdžio darbuotojai	Šiam profiliui yra priskiriami tokie darbuotojai kaip: personalo skyriaus specialistai, teisininkai ar finansininkai. Kadangi jie prieina ir prie įmonės ir prie kitų darbuotojų konfidencialios informacijos, todėl jiems būtina taikyti griežtus saugumo reikalavimus.
Vadybininkai, projektų vadovai	Šie asmenys prieina prie konfidencialios įmonės produktų ar projektų informacijos. Kai kuriais atvejais ir prie darbuotojų asmeninių duomenų. Šių darbuotojų įrenginiai turėtų turėti panašaus lygio saugumą kaip ir administracinio pobūdžio darbuotojų.
Ofiso darbuotojai	Šie darbuotojai turi tik ribotą prieigą prie įmonės informacinės sistemos. Prieinamus duomenis apibrėžia jų darbo sritis. Jiems gali būti taikomi ir žemesnio lygio saugumo reikalavimai.
Judrūs darbuotojai	Atsižvelgiant į prieigos prie įmonės informacinės sistemos lygį, ši darbuotojų grupė yra panaši į ofiso darbuotojų grupę. Šiai grupei priklauso darbuotojai, kurie darbinės veiklos metu palieka įmonės teritoriją. Dėl šios priežasties jų įrenginiuose esantiems duomenims turi būti naudojami papildomi apsaugos mechanizmai.
Rangovai, laikini vartotojai	Kadangi šie vartotojai nėra įmonės darbuotojai, todėl jiems negalioja įmonės saugumo politikos, tačiau jie vis tiek gali prieiti prie tam tikrų įmonės duomenų. Tai kelia papildomas saugumo kontrolės problemas.

Taip pat yra galimybė, kad tas pats vartotojas priklausys kelioms vartotojų grupėms. Tokiu atveju siūloma arba labiau detalizuoti ir sudaryti naujus vartotojų profilius arba šiam vartotojui taikyti griežtesniojo saugumo profilio taisykles.

Žemiau 2.2 lentelėje yra pateikiamas „Trend Micro“ įmonės sudarytas pavyzdinis saugumo taisyklių priskyrimo vartotojų profiliams rinkinys. Ši lentelė neatstoja saugumo politikos, o yra tik viena iš jos sudedamųjų dalių. Joje pateikiami darbuotojų profiliai atitinka šiuolaikinės įmonės darbuotojų grupes. Nors ir panašios, tačiau kiekvienos įmonės darbuotojų grupės skiriasi todėl ir reikiamos saugumo technologijos ir metodai turėtų būti parenkami atitinkamai.

2.2 lentelė Vartotojų profiliams priskiriamų saugumo taisyklių pavyzdys [10]

Būtina	■	Įrenginio šifravimas	Kelių tipų autentifikavimas	Vietinių duomenų prieigos kontrolė	Duomenų filtravimas	Sudėtingi slaptažodžiai	Prieiga prie E-laiškų priedų	Ne korinio radijo ryšio naudojimas	Komunikacijų šifravimas
Rekomenduojama	●								
Nereikalinga	○								
Profilis									
Direktoriai		■	■	○	●	■	■	■	■
Vadybininkai, projektų vadovai		■	●	■	■	●	■	○	■
Administracinio pobūdžio darbuotojai		■	■	○	■	■	○	○	■
Ofiso darbuotojai		●	○	○	○	○	○	○	■
Judrūs darbuotojai		■	○	■	●	○	■	■	■
Rangovai, laikini vartotojai		●	■	○	●	■	○	○	●

2.5. Mobilių įrenginių valdymo technologijos

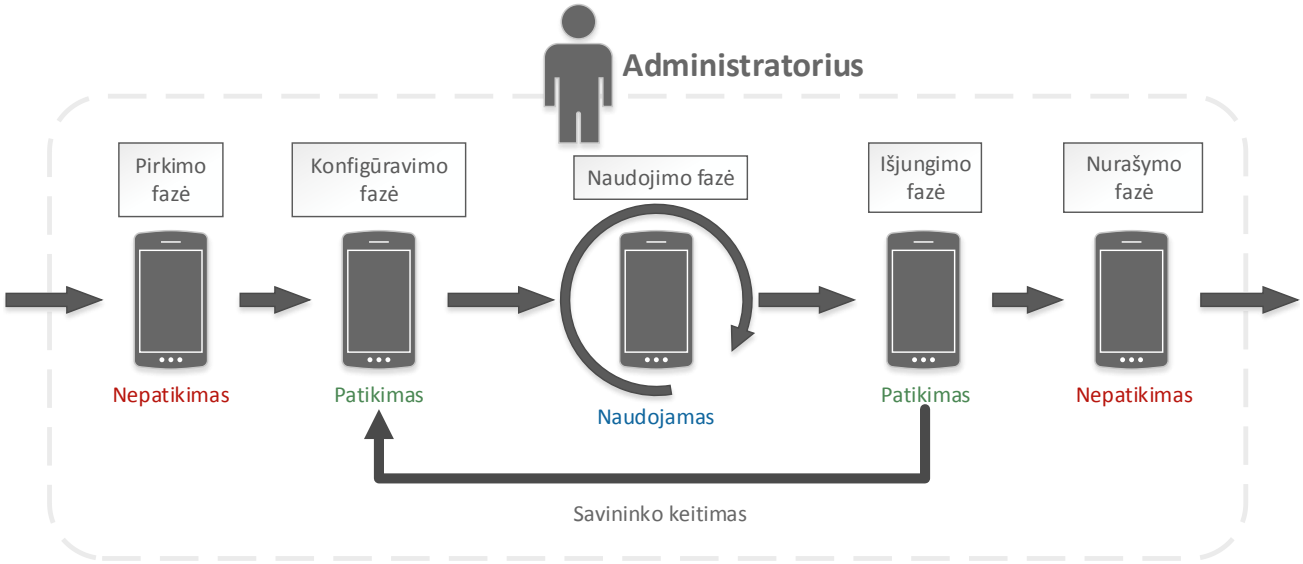
Didelėse įmonėse, dėl labai didelio darbuotojų skaičiaus, sudėtingu uždaviniu tampa mobiliųjų įrenginių saugumo politikų vykdymo užtikrinimas. IT sistemų administratoriai fiziškai nebesugeba rankiniu būdu aptarnauti ir sukonfigūruoti tokio didelio mobiliųjų įrenginių skaičiaus. Be atitinkamo įrenginių konfigūravimo saugumo politikos įgyvendinti neįmanoma. Taip pat sudėtinga nustatyti ar darbuotojai nepažeidžia įmonės saugumo politikos keliamų reikalavimų. Šioms problemoms išspręsti yra pritaikomi įvairūs mobiliųjų įrenginių valdymo modeliai. Šiame skyriuje bus aptariami keli tokių modelių pavyzdžiai.

2.5.1. Gyvavimo ciklo kontrolė

Įmonės leidžiančios darbuotojams jos viduje naudoti savo asmeninius mobiliuosius įrenginius susiduria su įvairiomis dėl to kylančiomis grėsmėmis. Deja, bet šiems įrenginiams lyginant su personaliniais kompiuteriais trūksta daugelio saugumo ypatybių (pvz. efektyvių anti-kenkėjiško kodo apsaugos ar įsilaužimo aptikimo programų). Šie saugumo apribojimai sukelia pavojų tiek asmeniniams, tiek įmonės duomenis, esantiems įrenginyje. Taip pat šie įrenginiai, dėl technologinių apribojimų, sukelia papildomus sunkumus diegiant apsauginę programinę įrangą. Menkos kompiuterinių skaičiavimų galimybės apriboja aktyviosios anti-kenkėjiško kodo programinės įrangos naudojimą. Dar viena problema, saugumo programinės įrangos atnaujinimai, kuri priklauso nuo paketinio duomenų perdavimo ryšio prieinamumo ir kaštų. Dėl šios problemos mobiliuosiuose įrenginiuose gali būti naudojama pasenusi programinė įranga, kuri nebeužtikrina saugumo nuo naujausių pažeidžiamumų. Galiausiai, kiekvienas mobilusis įrenginys dažniausiai yra susietas su vienu savininku ar vartotoju. Dėl šios sąsajos ir šiuolaikinio įrenginio vaidmens mūsų gyvenime, juose yra saugoma labai daug asmeninės informacijos, kuri turi būti atskirta nuo įmonės duomenų. Taip pat būtina paminėti, kad mobilieji įrenginiai gali būti pamesti ar pavogti, tai kelia dar didesnę riziką įmonei.

Alessandro Distefano, Antonio Grillo, Alessandro Lentini, Giuseppe F. Italiano mobiliųjų įrenginių saugumo užtikrinimui, darbe „SecureMyDroid: Enforcing Security in the Mobile Devices Lifecycle“ [18], pasiūlė gyvavimo ciklo kontrolės modelį. Šis darbas pateikia naują požiūrį į saugumo politikų ir tarnybų panaudojimą mobiliuosiuose įrenginiuose. Jame aprašytas naujoviškas metodas skirtas mobiliųjų įrenginių gyvavimo ciklo apsaugai, kuomet šių įrenginių saugumą kontroliuoja pats darbuotojas arba įmonė. Taip pat šiame darbe pateikiamas patobulintos „Android“ operacinės sistemos prototipas „SecureMyDroid“, kuriame yra įdiegti papildomi saugumo įrankiai ir realizuotas siūlomas modelis.

Bendruoju atveju, produkto gyvavimo ciklo kontrolė – tai išsami informacinė sistema, kuri koordinuoja visus produkto gyvavimo aspektus, pradedant nuo produkto projektavimo ir baigiant jo utilizavimu. Produkto gyvavimo ciklo kontrolės metodas yra aprašytas daugeliui produktų, tačiau jokių standartų ir saugumo procesų skirtų mobiliesiems įrenginiams dar nėra. Bendru atveju įmonė negali dalyvauti pilname įrenginio gyvavimo ciklo valdyme, nes ji negali kontroliuoti jo gamybos proceso, todėl, autoriai darbe pasiūlė gyvavimo ciklo kontrolės metodą, kuris prasideda įrenginio pirkimu ir tęsiasi iki naudojimo pabaigos. Modelyje įrenginio gyvavimo ciklas yra padalintas į penkias fazes (žr. 2.2 pav.) [18]: pirkimo fazę, konfigūravimo fazę, naudojimo fazę, išjungimo fazę ir nurašymo fazę.



2.2 pav. Mobilaus įrenginio gyvavimo ciklo kontrolė [18]

Mobilusis įrenginys gyvavimo metu gali įgyti tris būsenas: *patikimas, nepatikimas* ir *naudojamas*. Kai įrenginys yra *nepatikimos* būklės, nei organizacija, nei jos darbuotojai neprisiima atsakomybės už šį įrenginį. Kai įrenginys yra pažymėtas kaip *nepatikimas* jokie konfidencialūs įmonės duomenys negali būti įrašomi į įrenginį ir jis negali būti prijungiamas prie įmonės vidinio tinklo. Kitu atveju, kai įrenginys yra *patikimos* būsenos, visą atsakomybę už jį prisiima įmonė. Įrenginiui esant šioje būsenoje jame galima saugoti konfidencialią įmonės informaciją. Kol įrenginys yra *patikimoje* būsenoje, asmeniniai darbuotųjų duomenys į įrenginį negali būti įrašyti. Pati sudėtingiausia įrenginio būsena yra *naudojimo* būsena. Įrenginys patenka į šią būseną tuomet, kai jis yra išduodamas įmonės darbuotojui. Šiuo metu jis prisiima visą atsakomybę už įrenginio ir jame esančių duomenų saugumą. Darbuotojo naudojamas įrenginys gali turėti ir konfidencialią įmonės informaciją ir asmeninius darbuotojo duomenis. *Naudojimo* būsenoje esantis įrenginys ir yra įmonės duomenų saugumo ir konfidencialumo atakų taikinys.

Pirmojoje šio modelio fazėje „pirkimo fazėje“, įmonei įsigijus mobilųjį įrenginį, jis privalo pakeisti savo būseną iš *nepatikimos* į patikimą, nes prieiga prie įmonės duomenų ir tinklo yra suteikiama tik *patikimiems* įrenginiams. Paprasčiausiu atveju, tai galima pasiekti panaudojant gamintojo duomenų atkūrimo funkciją, kuri yra įdiegta beveik visose mobiliųjų įrenginių operacinėse sistemose. Ši operacija skirta pradinės įrenginio būsenos atkūrimui, t.y. įrenginyje yra ištrinamos visos įrašytos programėlės, visi jame esantys duomenys ir nustatomi standartiniai įrenginio nustatymai. Kadangi šios operacijos efektingumas nepriklauso nuo įmonės galimybių, todėl jos atlikimas gali būti patikrintas rankiniu būdu arba naudojant automatizuotus įrankius.

Antroji įrenginio gyvavimo fazė – „konfigūravimo fazė“. Ši fazė turi būti atliekama prieš įteikiant įrenginį kažkuriam konkrečiam įmonės darbuotojui. Mobilusis įrenginys turi būti sukonfigūruotas atitinkamai pagal jo naujojo savininko turimas teises įmonėje. Būtina paminėti, kad tik šioje įrenginio gyvavimo fazėje jame gali būti įdiegiamos programėlės. Tai yra atliekama dėl to, kad būtų galima užtikrinti griežtą mobiliųjų įrenginių kontrolę ir sumažinti galimas saugumo grėsmes.

Pagrindinė įrenginio gyvavimo ciklo fazė – „naudojimo fazė“. Šios fazės metu yra atliekama eilė įrenginio priežiūros operacijų. Grupė procedūrų turi būti atliekamas reguliariai, tam kad užtikrinti du pagrindinius tikslus: įsitikinti ar įrenginys nebuvo pažeistas išorinių atakų ir įsitikinti ar darbuotojas įrenginiu naudojasi pagal paskirtį. Nustačius, kad mobilusis įrenginys yra pažeistas jo

būsena turi būti pakeista į *nepatikimą*, atitinkamos procedūros skirtos duomenų praradimo užkirtimui ir saugumo politikos, skirtos pavogtų duomenų keliamos žalos likvidavimui, turi būti atliekamos. Procedūros atliekamos „naudojimo fazėje" gali būti suskirstomos į tokias grupes [18]:

- Duomenų kontrolės procedūros – tai operacijos, kurios skirtos įmonės duomenų išsaugojimui. Tai tokios operacijos kaip atsarginių duomenų kopijų darymas ar duomenų vientisumo tikrinimas. Atliekant šias operacijos, net ir tuo atveju, kai įrenginys yra prarandamas ar pažeidžiamas, jame esančiu įmonės duomenis galima atkurti.
- Konfigūracijų valdymo operacijos – tai visos operacijos, kurios yra skirtos užtikrinti, kad įrenginio nustatymai nebuvo pakeisti į netinkamus.
- Programėlių valdymo operacijos – šiomis operacijomis yra užtikrinama, kad įrenginyje įrašytos programėlės nekeltu jokių grėsmių įrenginiui ar jame saugomiems duomenims. Pateiktame modelyje tai yra tokios grėsmės kaip: raktų registratoriai, kirminai, šnipinėjančios programos ir kitokios kenkėjiškos programėlės, kurios yra skirtos mobiliųjų įrenginių operacinėms sistemoms.
- Saugumo valdymo operacijos – tai operacijos kurios skirtos užtikrinti, kad įrenginio saugumo konfigūracijos yra teisingos, t.y. „Wi-Fi" ar „Bluetooth" ryšio ir kiti saugumo nustatymai.
- Nuotolinio valdymo operacijos – tai tokios operacijos, kurios yra skirtos tam tikrų įrenginio funkcijų atlikimui nuotoliniu būdu. Pats paprasčiausias tokios funkcijos pavyzdys yra nuotolinis įrenginio duomenų ištrynimas. Ši funkcija gali būti panaudota tokiu atveju, kai mobilusis įrenginys yra pametamas ar pavagiamas. Tokiu atveju įmonės duomenys yra apsaugomi nuo nutekėjimo.

„Išjungimo fazė" yra atliekama, kai darbuotojas grąžina įrenginį įmonei. Įmonės požiūriu, šioje fazėje iš įrenginio yra išgaunami visi naudingi duomenys, kuriuos sukūrė darbuotojas, ir panaudojant atitinkamą politiką atsakomybė už įrenginį yra sugrąžinama įmonei. Darbuotojo požiūriu, yra būtina suteikti galimybę iš įrenginio išgauti visą asmeninę informaciją ir po to ją ištrinti iš įrenginio. Šios fazės pabaigoje, įrenginyje turi būti atliekamas gamintojo duomenų atkūrimas ir įrenginio būsena pakeičiama iš *naudojamo* į *patikimą*. Kadangi po šios fazės įrenginys gali pakeisti savo šeimininką, todėl prieš pradedant konfigūravimo fazę yra būtina įsitikinti ar išjungimo fazė buvo sėkminga. Kuomet ši fazė yra baigiama, buvęs įrenginio savininkas jau nebėra laikomas atsakingu už jį.

Paskutinė įrenginio gyvavimo fazė yra „nurašymo fazė". Ši fazė atliekama tuomet kai įrenginys yra nebetinkamas naudojimui arba nebereikalingas įmonei. Jeigu įrenginys yra parduodamas, tuomet prieš pardavimą yra būtina visiškai ištrinti jame esančiu duomenis. Jeigu įrenginys nebeturi jokios ekonominės vertės, tuomet yra siūloma jį fiziškai sunaikinti. Net ir antruoju atveju prieš sunaikinant visus įrenginyje saugomus duomenis reikėtų ištrinti.

2.5.2. Taikomųjų programų ir duomenų profiliavimas

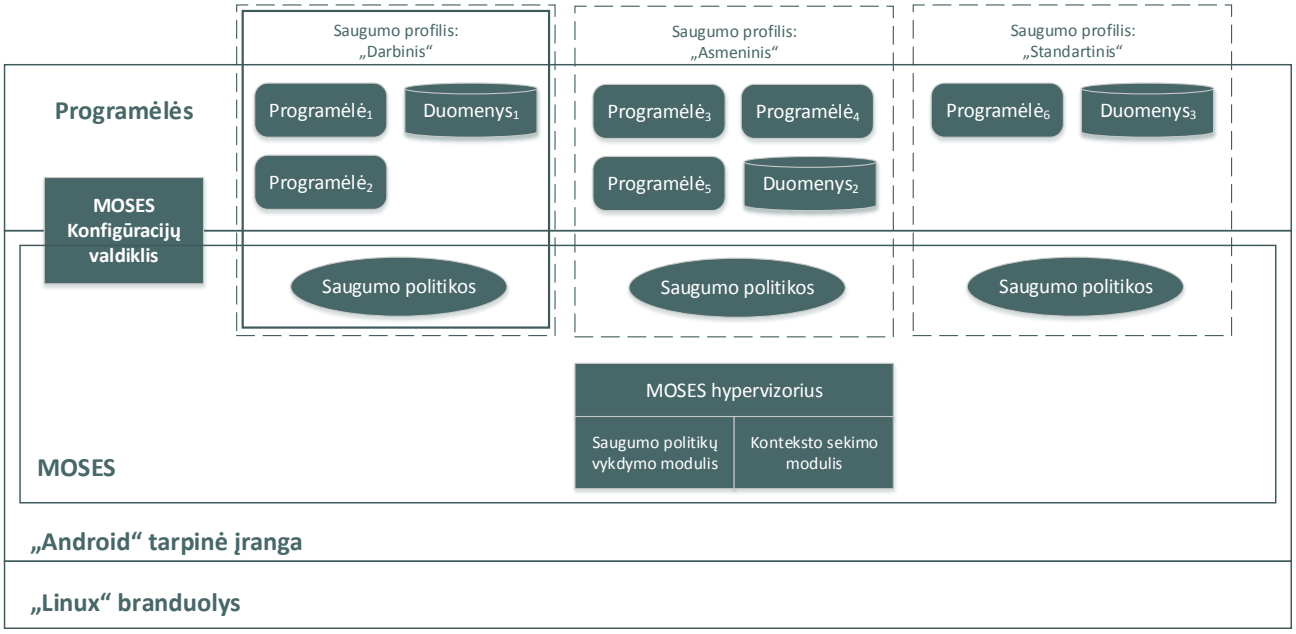
Įmonės darbuotojai į mobiliuosius įrenginius gali įdiegti trečiųjų šalių programėles, dėl to iškyla keletas saugumo grėsmių. Pavyzdžiui, kenkėjiškos programėlės gali prieiti prie įrenginyje saugomų elektroninių laiškų, SMS ir MMS žinučių, kuriose gali būti konfidencialių įmonės duomenų. Tai sukelia didelę grėsmę įmonei, ypač tokiuose mobiliuosiuose įrenginiuose, kuriuose naudojama operacinė sistema neturi pakankamai integruotų įrankių ir mechanizmų saugumui užtikrinti.

Vienas iš šios problemos sprendimų yra naudoti programėlių ir atminties profiliavimą, t.y. padalinti įrenginį į atskirus profilius ar aplinkas, šitaip atskiriant darbui skirtas programėles ir

duomenis nuo skirtų asmeniniam naudojimui. Tame pačiame įrenginyje gali egzistuoti kelios skirtingos saugumo aplinkos: pirmoji skirta jautriai ir konfidencialiai įmonės informacijai ir patikimoms programėlėms, o antrojoje būtų galima įdiegti įvairius trečiųjų šalių žaidimus ar kitas populiarias programėles. Įmonės duomenų konfidencialumo grėsmė bus ženkliai sumažinta tol, kol programėlės iš antrosios saugumo aplinkos negalės prieiti prie duomenų esančių pirmojoje.

Toks saugumo mechanizmas gali būti įgyvendintas naudojant virtualizavimo technologijas, kuomet kelios operacinės sistemos gali vienu metu atskirai viena nuo kitos veikti tame pačiame įrenginyje. Nors ir plačiai naudojamos pilnavertėse kompiuterinėse sistemose (personaliniuose kompiuteriuose ar serveriuose), jos vis dar reikalauja per daug resursų, kad jas būtų galima efektyviai panaudoti integruotose sistemose, tokiose kaip išmanieji telefonai. Kitas šios problemos sprendimas yra dalinio virtualizavimo technologijos. Šios technologijos yra diegiamos į mobiliuosius įrenginius, tačiau norint išgauti aukštą įrenginio našumą būtina papildomai modifikuoti pačią operacinę sistemą. Taip pat naudojant virtualizavimo technologijas perėjimas nuo vienos aplinkos prie kitos užtrunka ganėtinai ilgai ir šios technologijos sunaudoja daug energijos.

Giovanni Russello, Mauro Conti, Bruno Crispo ir Earlence Fernandes darbe „MOSES: Supporting Operation Modes on Smartphones“ [15] pateikia lengvojo virtualizavimo sprendimą skirtą „Android“ platformos pagrindu veikiantiems mobiliesiems įrenginiams. Jie savo saugumo modelį pavadino MOSES (*angl. Mode of uses seperation for Smartphones*). MOSES – tai saugumo politikomis paremtas karkasas (*angl. Framework*), skirtas programiniam taikomųjų programų ir duomenų atskyrimui. Naudojant šį modelį mobiliajame įrenginyje galima apibrėžti skirtingus saugumo profilius. Kiekvienas saugumo profilis yra susietas su tam tikromis prieigos prie programos ir duomenų politikomis. Viena pagrindinių MOSES ypatybių yra dinaminis saugumo profilių perjungimas. Kiekvienas saugumo profilis be visa ko yra susietas su tam tikru kontekstu (vieta, laikas, aplinka ir kt.). Pasinaudojant mobiliajame įrenginyje esančiais sensoriais, MOSES sugeba aptikti konteksto pokyčius ir automatiškai perjungti saugumo profilį į tokį, kuris atitinka dabartinį įrenginio kontekstą.



2.3 pav. Apibendrinta MOSES architektūra [15]

2.3 pav. yra pateikta apibendrinta MOSES karkaso architektūra. MOSES karkasas yra parašytas tarpiniame „Android“ įrangos lygmenyje ir perrašo arba papildo kai kuriuos šio lygmens modulius. Pagrindinė MOSES sistemos idėja yra saugumo profiliai. Saugumo profilis atitinka įrenginio darbo

rėžimą, kuris gali būti naudojamas kaip loginis izoliavimo vienetas, kuris susideda iš: programėlių, duomenų ir saugumo politikų. Panaudojant saugumo politikas priskirtas atitinkamam saugumo profiliui, MOSES garantuoja, kad profilyje esančios programėlės galės prieiti tik prie tų duomenų, kurie taip pat priklauso tam profiliui. MOSES pasiekia labai aukštą saugumo politikų vykdymo lygį panaudodamas saugumo politikų vykdymo modulį (*angl. Policy enforcement module*). Šis modulis panaudoja programėlių ir duomenų žymėjimą (yra pažymimas saugumo profilio pavadinimas) tam, kad užtikrinti prieigos kontrolę [9, 15].

Naudojant šią sistemą, įrenginyje gali būti sukuriama keletas saugumo profilių. Pagal nutylėjimą, sistemoje yra sukuriamas „standartinis“ saugumo profilis. Šis profilis gali būti panaudotas diegiant naujas programėles, kurios dar nėra susietos su jokiu saugumo profiliu, arba duomenų, kurie nėra priskirti nei vienam saugumo profiliui saugojimui. Vartotojai naudodamiesi MOSES konfigūracijų valdikliu (*angl. MOSES Configuration manager*) gali sukurti naujus saugumo profilius ir jiems priskirti programėles bei duomenis. Taip pat naudojant šį valdiklį galima redaguoti ir jau egzistuojančius saugumo profilius. Kai kurių saugumo profilių redagavimui gali reikėti specialių prieigos teisių, pavyzdžiui, saugumo profilio „Darbinis“ (žr. 2.3 pav.) pats įmonės darbuotojas redaguoti negali. Šis profilis buvo sukurtas įmonės IT administratorius, todėl tik jis turi teisę jį redaguoti. Šitaip įmonė gali būti garantuota, kad tik patikimos programėlės galės prieiti prie konfidencialių įmonės duomenų. Saugumo profilių skaičius įrenginyje yra neribojamas, tačiau dėl paprastumo šiame darbe yra kalbama tik apie du profilius: darbinį – kuris skirtas darbui su įmonės duomenimis ir asmeninį – kuris skirtas asmeniniam darbuotojo naudojimui. Į pastarąjį galima įdiegti, bet kokias trečiųjų šalių programėles.

Saugumo profilių įjungimą ir išjungimą kontroliuoja MOSES hipervizorius (*angl. MOSES Hypervisor*). Kai saugumo profilis yra aktyvuojamas hipervizorius užkrauna jo saugumo politikas į saugumo politikų vykdymo modulį. Kuomet programėlė paprašo teisių prieiti prie kažkokių duomenų, saugumo politikų vykdymo modulis prieiga suteikia tik tuo atveju jeigu saugumo profilio saugumo politikos tai leidžia. Vartotojas saugumo profilius gali perjunginėti rankiniu būdu, tačiau MOSES pateikia daug pažangesnį mechanizmą, kuomet saugumo politikos yra automatiškai perjungiamas atsižvelgiant į kontekstinę informaciją (pvz. laiką ar vietą). Kuomet yra aptinkamas atitinkamas kontekstas MOSES hipervizorius automatiškai įjungia su šiuo kontekstu susijusią saugumo politiką. Konteksto pokyčiu sekimui yra naudojamas konteksto sekimo modulis. Pavyzdžiui, saugumo profilis „darbinis“ gali būti aktyvuojamas darbo valandomis esant įmonės ofiso teritorijoje.

Taip pat konteksto sekimas gali būti panaudotas automatiniam duomenų ir programėlių priskyrimui saugumo profiliams. Pavyzdžiui, jeigu darbuotojas į mobilųjį telefoną įtraukią naują kontaktą darbo valandų metu, tuomet šis kontaktas yra automatiškai priskiriamas „darbiniam“ saugumo profiliui. Šis automatinis duomenų priskirimas yra labai patogi sistemos ypatybė, tačiau ji gali sukelti ir neigiamų padarinių. Jeigu darbuotojas darbo valandų metu gaus asmeninį SMS pranešimą, jis automatiškai bus priskirtas „darbiniam“ saugumo profiliui ir vartotojas nepamatys, kad gavo pranešimą tol kol neaktyvuos šio profilio.

2.5.3. Standartizavimas

Neatsiejama asmeninių įrenginių, naudojamų įmonėse, saugumo politikos dalis yra nuotolinio mobiliųjų įrenginių valdymo sistemos. Tačiau įmonėje naudojant įvairių gamintojų ir modelių įrenginius nuotolinė jų kontrolė tampa sudėtinga, dėl to, kad skirtingi gamintojai dažniausiai siūlo savo asmeninius įrankius ir sistemas šiam darbui atlikti, o jie dažniausiai tarpusavyje nėra

suderinami. Dėl šios priežasties „Open Mobile Alliance“ (OMA) standartizavimo organizacija išleido OMA DM (*angl. Device management*) atviras mobiliųjų įrenginių nuotolinio valdymo specifikacijas. Šį standartą palaiko tokios mobiliųjų įrenginių platformos kaip „Windows mobile“ ar „BlackBerry“.

OMA DM specifikacijos yra skirtos mobiliųjų įrenginių tokių kaip mobilieji telefonai ar planšetiniai kompiuteriai valdymui. Šios specifikacijos aprašo tokias įrenginių valdymo funkcijas [19]:

- įrenginio funkcijų valdymas – suteikia galimybę įjungti ir išjungti atitinkamas įrenginio funkcijas;
- įrenginio konfigūravimas – leidžia keisti įvairius įrenginio nustatymus ir parametrus;
- programinės įrangos atnaujinimai – suteikia galimybę į įrenginį įdiegti programinės įrangos atnaujinimus;
- klaidų kontrolė – suteikia galimybę pranešti apie įrenginyje įvykusias klaidas arba jo būsenos pokyčius.

Kuriant mobiliųjų įrenginių valdymo sistemą, pasinaudojant šiomis specifikacijomis, sistemoje gali būti įdiegtos nebūtinai visos funkcijos, o tik kelios iš jų. Kadangi ši specifikacija yra orientuota į mobiliuosius įrenginius, todėl joje yra atsižvelgta į [19]:

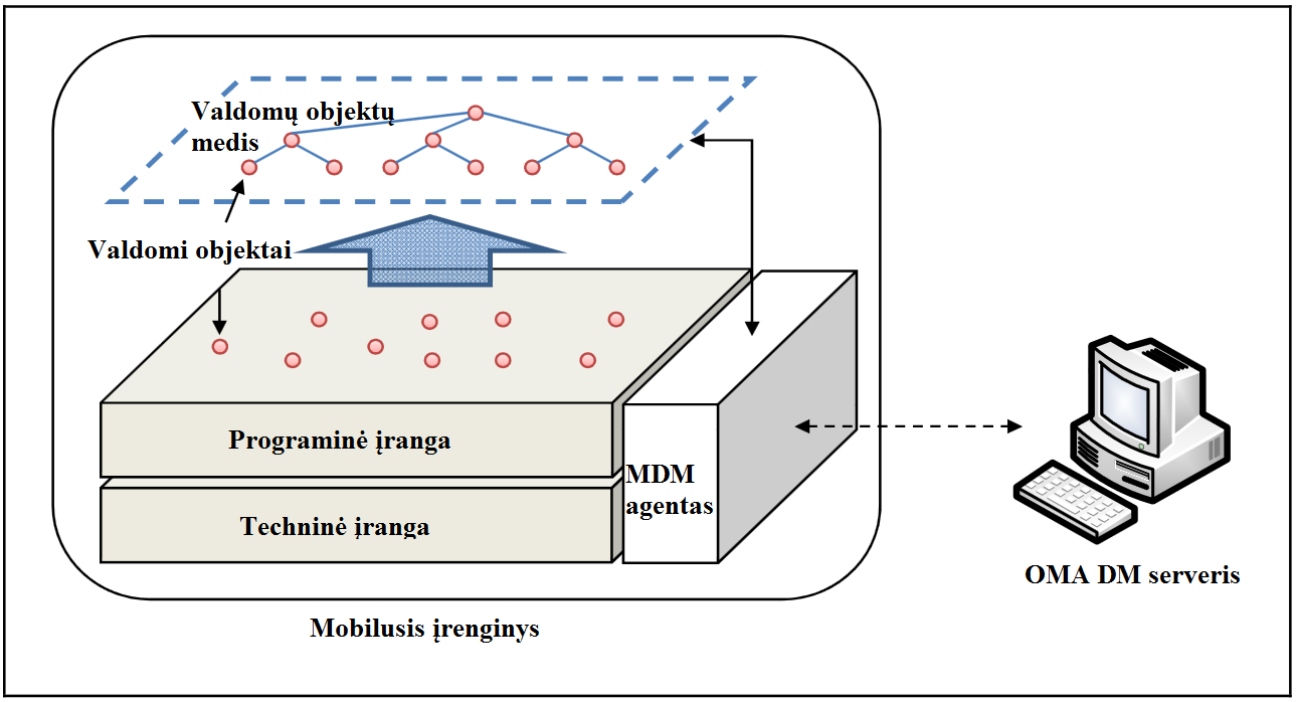
- tai, kad šių įrenginių atminties ir kitų kompiuterinių resursų kiekis yra ribotas;
- duomenų perdavimo apribojimus bevielio ryšio tinkluose;
- griežtą saugumą, kadangi mobilieji įrenginiai yra pažeidžiami kenkėjiškos programinės įrangos ir komunikacijų perėmimo, todėl specifikacijoje yra aprašomi autentifikavimo ir iššūkių mechanizmai.

Techniniu aspektu, OMA DM protokolas perduodamiems duomenims naudoja XML duomenų kodavimo formatą. Įrenginių valdymas vyksta komunikacijos tarp serverio (sistemos subjekto, kuris valdo) ir kliento (įrenginio, kuris yra valdomas) būdu. OMA DM yra suprojektuota taip, kad galėtų duomenų perdavimui naudoti įvairius kanalus [19]:

- Fizinius – tiek laidinius (USB, RS-232), tiek belaidžius (GSM, WCDMA ar Bluetooth);
- Transportinio lygmens – WAP, HTTP ar bet kokius kitus protokolus.

OMA DM protokolas komunikacijoms naudoja užklausos-atsakymo bendravimo metodą. Protokole yra įdiegtas autentifikavimo ir iššūkių mechanizmas, tam kad užtikrinti komunikacijoje dalyvaujančių subjektų autentiškumą. Ryšio sesiją užmezga serveris, jis tam tikru metodu (WAP ar SMS žinute) siunčia įrenginiui pranešimą. Įrenginys gavęs šį pranešimą jungiasi prie serverio. Kuomet ryšys tarp serverio ir kliento yra sudarytas sesijos metu tarp jų gali būti apsikenčiama eile pranešimų, kurie yra skirti tam tikrai užduočiai atlikti. OMA DM taip pat turi ir įspėjamųjų pranešimų mechanizmą, šis mechanizmas leidžia pranešimus, tiek iš įrenginio, tiek iš serverio, siųsti nesudarius sesijos. Šie pranešimai yra siunčiami įvykus klaidoms, pasikeitus įrenginio būsenai ir pan. Protokolas aprašo paketų apsikeitimą sesijos metu, kiekvienas paketas yra sudarytas iš kelėtos žinučių, o kiekviena iš jų yra sudaryta iš kelėtos komandų. Serveris inicijuoja šias komandas ir tikisi, kad įrenginys jas įvykdys ir atsiųst atsakymo žinutę.

OMA DM sistemoje laikoma, kad įrenginys yra sudarytas iš techninės įrangos, programinės įrangos modulių, skirtų techninės įrangos valdymui, ir mobiliųjų įrenginių valdymo (*angl. Mobile device management*) MDM agento, kuris atlieka programinės įrangos atnaujinimus, valdymą ir komunikacijas su serveriu. OMA DM sistemos struktūra yra pateikta 2.4 pav. [16].



2.4 pav. OMA DM struktūra [16]

Programinės įrangos atnaujinimai yra atliekami pridedant, redaguojant arba ištrinant kiekvienos programos valdomus objektus. Valdomi objektai atitinka programinės įrangos nustatymus, kiekvienas nustatymas yra atskiras objektas. Šie valdomi objektai yra kontroliuojami komunikuojant OMA DM serveriui su MDM agentu.

Virtualaus medžio struktūra sudaryta iš valdomųjų objektų sistemai suteikia didelį efektyvumą. Per MDM agentą valdymo serveris gali prieiti prie kiekvieno individualaus objekto esančio medyje arba pasiekiant tėvinį objektą serveris gali prieiti prie visų jo vaikinių objektų. Valdomų objektų medis yra iliustruotas 2.4 pav.

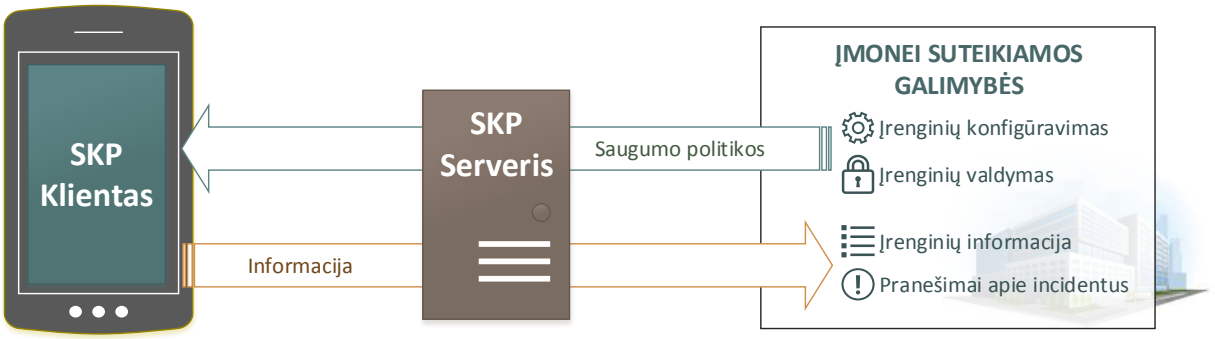
2.6. Analizės išvados

1. Šiuo metu pasaulyje labai plačiai plinta asmeninių įrenginių naudojimo įmonėse tendencija. Nors mobilieji įrenginiai ir padidina darbo efektyvumą bei jo kokybę, tačiau kartu atneša ir papildomas saugumo grėsmes įmonėms. Norint išspręsti šias problemas įmonės privalo diegti papildomas mobiliųjų įrenginių kontrolės ir saugumo technologijas.
2. Neteisingas mobiliųjų įrenginių naudojimas ir konfigūravimas atveria kelią įvairioms saugumo grėsmėms ir atakoms. Tai tokios grėsmės kaip: kenkėjiškos programėlės, socialinė inžinerija, komunikacijų perėmimas ar konfidencialių įmonės duomenų praradimas ir nutekinimas.
3. Norint apsaugoti įmonės duomenis nuo konfidencialumo ir vientisumo pažeidimų yra būtina sudaryti mobiliųjų įrenginių saugumo politiką ir ją įgyvendinti pasinaudojant organizacinėmis ir techninėmis priemonėmis.
4. Kuriant įmonės mobiliųjų įrenginių saugumo politiką yra būtina atsižvelgti į skirtingų mobiliųjų įrenginių platformų turimas saugumo funkcijas. Ir tik išanalizavus ir įvertinus jas reikia pasirinkti papildomas saugumo priemones.
5. Sudarant įmonės mobiliųjų įrenginių saugumo politiką, būtina atsižvelgti ir į vartotojų prieigos, prie įmonės duomenų, teises. Pasitelkiant prieigos teisių priskyrimo modelius reikia sudaryti vartotojų profilius, kurie atitiktų vartotojų prieigos teises. Tuomet pagal šiuos profilius reikia nuspręsti kokių saugumo taisyklių būtina laikytis ir kokias apsaugos technologijas reikia diegti į įrenginius.
6. Įmonės saugumo politikos įgyvendinimą ir kontrolę, asmeniniuose, mobiliuosiuose įrenginiuose, leistų užtikrinti saugaus konfigūravimo paramos sistema, kuri suteiktų mobiliųjų operacinių sistemų, vartotojų ir tinklų profiliavimo bei nuotolinio mobiliųjų įrenginių konfigūravimo ir priežiūros funkcijas.

3. ASMENINIŲ MOBILIŲJŲ ĮRENGINIŲ, NAUDOJAMŲ ĮMONĖSE, SAUGAUS KONFIGŪRAVIMO PARAMOS SISTEMOS MODELIS

Šiame skyriuje aprašomas siūlomas mobiliųjų įrenginių saugaus konfigūravimo paramos sistemos modelis. Pateikiamas siūlomos sistemos koncepcinis modelis, architektūra, serverio ir kliento komunikacijų modeliai ir apibrėžiami mobiliųjų įrenginių saugumo profiliai bei jų sudedamosios dalys.

3.1. Koncepcinis saugaus konfigūravimo paramos sistemos modelis



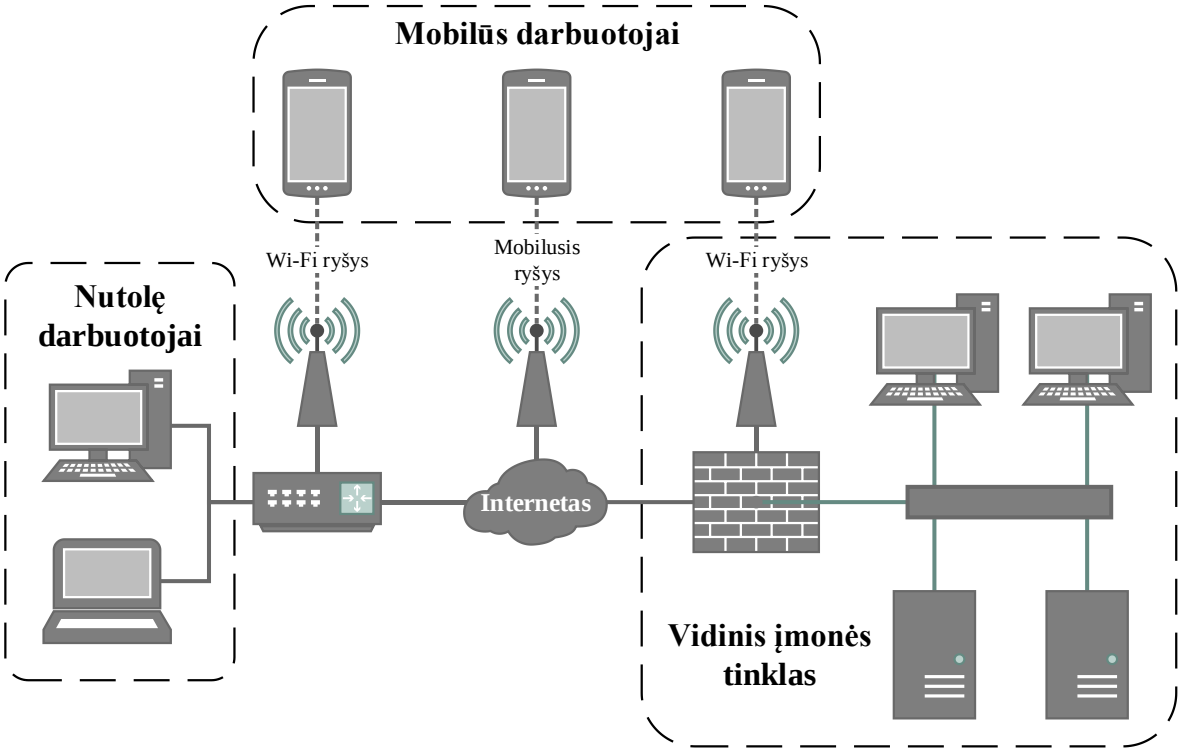
3.1 pav. Koncepcinis saugaus konfigūravimo paramos sistemos modelis

Dauguma mobiliųjų įrenginių valdymo sistemų yra orientuotos į dideles įmonės, jos suteikia labai daug funkcijų, yra sudėtingos architektūros ir reikalauja specialios techninės įrangos norint jas įdiegti. Šios priežastys dažnai užkerta kelią smulkaus ir vidutinio dydžio įmonėms naudoti įrenginių valdymo technologijas, nes jų kaštai yra per dideli. Nedidelėms įmonėms skirta saugaus konfigūravimo paramos sistema (žr. 3.1 pav.) turėtų būti paprastos architektūros ir lengvai diegiama. Paprastumą mes traktuojame kaip galimybę sistemą naudoti įmonėse su ribotais techniniais ištekliais. Kadangi sistema yra orientuota į asmeninius darbuotojų mobiliuosius įrenginius, todėl ji turėtų būti lengvai įdiegiama, neapsunkinti darbo su įrenginiu ir nepažeisti vartotojo privatumo (nerinkti informacijos apie siunčiamas žinutes, atliekamus pokalbius ir pan.). Atsižvelgiant į šiuos kriterijus sistemos klientas turėtų būti realizuotas kaip mobilioji programėlė. Taip pat sistema turėtų suteikti centralizuotą įrenginių administravimo sąsają, per kurią įmonės IT administratorius galėtų peržiūrėti visus sistemoje registruotus įrenginius bei juos konfigūruoti.

Saugaus konfigūravimo paramos sistema turėtų atlikti šias funkcijas:

- Surinkti ir įmonei pateikti bazinę mobiliųjų įrenginių informaciją (gamintoją, modelį, operacinę sistemą ir jos versiją, įrenginio identifikatorių ir pan.);
- Įmonei pateikti įrenginyje įrašytų mobiliųjų programėlių veikimo istoriją;
- Registruoti įrenginyje vykstančius įvykius ir pranešti apie saugumo incidentus bei įtartiną mobiliojo įrenginio veikimą, pvz. tris kartus įvestas neteisingas slaptažodis;
- Suteikti galimybę pateikti mobiliųjų įrenginių konfigūravimo instrukcijas arba automatiškai juos sukonfigūruoti taip, kad jie atitiktų įmonės saugumo programoje keliamus reikalavimus;
- Suteikti galimybę nuotoliniu būdu užrakinti įrenginį ir išvalyti visus jame esančius duomenis.

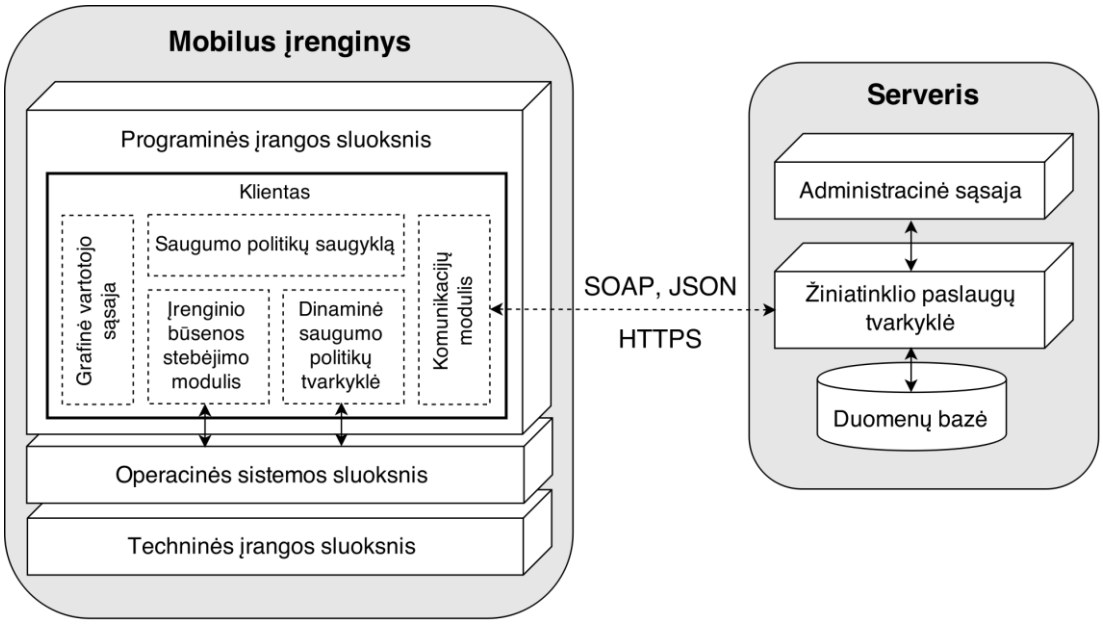
3.2. Saugaus konfigūravimo paramos sistemos architektūra



3.2 pav. Tipinė nedidelės įmonės kompiuterinio tinklo struktūra

Dažniausiai nedidelės įmonės kompiuterinis tinkas (žr. 3.2 pav.) susideda iš trijų pagrindinių dalių: vidinio įmonės tinklo, nutolusių įrenginių ir mobiliųjų įrenginių. Kiekviena tinklo dalis reikalauja skirtingų saugos priemonių bei saugumo programų. Šiame darbe bus nagrinėjama tik trečioji įmonės tinklo dalis mobilūs įrenginiai arba mobiliųjų įrenginių naudojimas įmonės tinkle.

Atsižvelgiant į tipinę įmonės kompiuterių tinklo struktūrą ir sistemos orientaciją į smulkaus ir vidutinio verslo įmones, nuspręsta sistemoje naudoti paprastą klientas serveris architektūrą. Siūloma mobiliųjų įrenginių saugaus konfigūravimo paramos sistema yra sudaryta iš dviejų komponentų: kliento programinės įrangos ir serverio (žr. 3.3 pav.).



3.3 pav. Siūloma sistemos architektūra

Kiekviena sistemos dalis yra sudaryta iš kelėtos elementų (modulių), kurie atlieka tokias funkcijas:

- Kliento programinė įranga (žr. 3.3 pav.):
  - **Grafinė vartotojo sąsaja –** skirta vartotojo komandų įvesčiai ir informacijos atvaizdavimui.
  - **Komunikacijų modulis** – šis modulis atsakingas už ryšio su serveriu sudarymą, duomenų perdavimą ir priėmimą. Sudarant ryšį su serveriu šis modulis atlieka vartotojų ir mobiliųjų įrenginių autentifikavimo funkciją, autentifikavimas gali būti įgyvendinamas naudojant tiek slaptažodžius, tiek sertifikatus.
  - **Saugumo politikų saugykla** – tai duomenų bazė, kurioje yra laikomos įrenginiui priskirtos saugumo politikos, ši duomenų bazė turėtų būti šifruojama.
  - **Įrenginio būsenos stebėjimo modulis** – yra atsakingas už mobiliojo įrenginio būsenos sekimą (laiko, pozicijos, techninių komponentų veikimo ir pan.) ir įrenginyje įvykstančių įvykių, kurie yra apibrėžti saugumo politikoje, registravimą ir perdavimą serveriui.
  - **Dinaminė saugumo politikų tvarkyklė** – yra atsakinga už saugumo politikų pritaikymą įrenginyje atsižvelgiant į kontekstinę informaciją. Taip pat šis modulis suteikia galimybę trečiųjų šalių programinei įrangai (pvz.: įmonės elektroninių dokumentų sistemai) sužinoti ar mobilusis įrenginys yra saugios būsenos, t.y. ar jis atitinka saugumo politikoje keliamus reikalavimus. Jeigu vartotojas kliento programinei įrangai suteikia pakankamas teises šis modulis yra atsakingas ir už įrenginio nustatymų keitimą, jo komponentų konfigūravimą, išjungimą ir įjungimą.
- Serverio programinė įranga (žr. 3.3 pav.):
  - **Administravimo sąsaja** – tai grafinė sąsaja skirta darbui su serveriu, ji suteikia įrankius informacijos peržiūrai, vartotojų ir saugumo politikų valdymui, tiesioginių komandų (įrenginio užrakinimo ir pilno duomenų ištrynimo) perdavimui įrenginiams.
  - **Žiniatinklio paslaugų tvarkyklė –** pagrindinis serverio komponentas, kuriame yra realizuojamos įvairios žiniatinklio paslaugos skirtos darbui sistemoje. Šis serverio komponentas pateikia vartotojų autentifikavimo, įrenginių registravimo, komandų perdavimo ir sistemos administravimo žiniatinklio paslaugas.
  - **Duomenų bazė** – šiame sistemos komponente yra saugomi visi duomenys susiję su vartotojais, jų įrenginiais bei saugumo politikomis.

Sistemos modelyje nėra apibrėžiama, kaip turėtų būti realizuotos sistemos dalys ir moduliai. Tai priklauso nuo konkrečios sistemos realizacijos, taip pat siūlomas sistemos modelis neriboja programinės įrangos kūrėjų nuo papildomų modulių diegimo, tačiau sistemos realizacija privalo atitikti toliau darbe apibrėžiamus kliento ir serverio komunikacijų, saugumo profilių, mobiliųjų įrenginių valdymo ir sistemos veikimo modelius.

3.3. Kliento ir serverio komunikacijų modelis

Komunikacijoms tarp kliento ir serverio yra naudojamas užklausos-atsakymo mechanizmas. Pranešimai yra perduodami HTTP protokolu. Saugaus ryšio užtikrinimui rekomenduojama naudoti saugų HTTPS protokolą.

Mobiliųjų įrenginių konfigūravimas ir valdymas yra labai jautrios operacijos, kurios gali būti susijusios su konfidencialios informacijos perdavimu (pvz.: slaptažodžiai ar įrenginio būvimo vieta), todėl rekomenduojama komunikacijas tarp serverio ir kliento vykdyti tik saugiais ryšio kanalais.

Sistemos modelis neapibrėžia visų apsaugos mechanizmų, kurie turėtų būti diegiami ir naudojami sistemos realizacijose, bet pateikia rekomendacijas kai kuriems sistemos saugos aspektams.

Komunikacijos tarp serverio ir kliento yra atliekamos dviem būdais: sudarant sesiją arba ne. Kadangi dėl vartotojų mobilumo serveris dažniausiai neturi galimybės sudaryti sujungimo su mobiliuoju įrenginiu, todėl sesijas visuomet privalo inicijuoti klientas. Nors serveris ir neturi galimybės inicijuoti sesijos, tačiau jis gali klientui išsiųsti pranešimą su prašymu sudaryti su juo sesiją. Šiam tikslui yra naudojami SMS pranešimai arba standartinės nuotolinių pranešimų perdavimo paslaugos, kurias suteikia mobiliųjų įrenginių ar mobiliųjų operacinių sistemų gamintojai (pvz.: *„Apple Push Notification“* ar *„Google Cloud Messaging“* paslaugos).

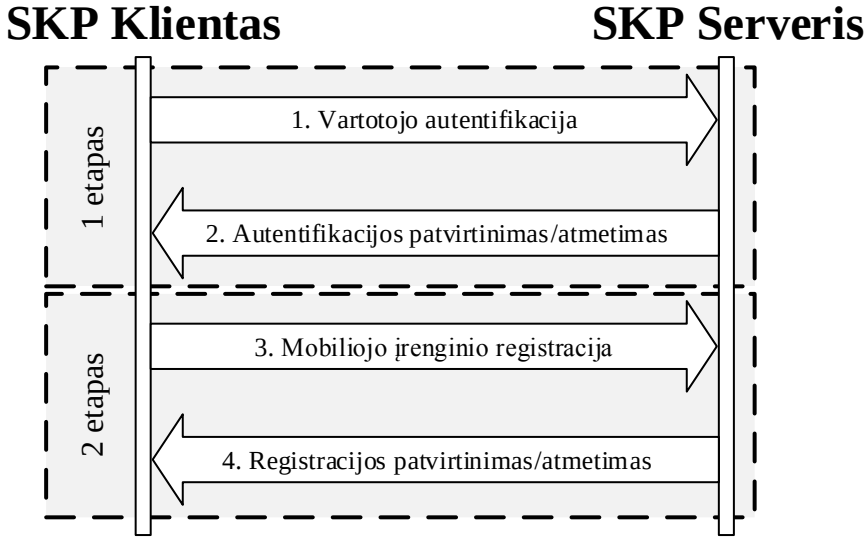
Įrenginių registravimo/išregistravimo ir komandų (konfigūravimo bei valdymo) perdavimo įrenginiui funkcijos reikalauja sesijos sudarymo, tuo tarpu pranešimai į serverį gali būti perduodami nesudarant sesijos. Vienos sesijos metu gali būti atliekama nuo vienos iki kelėtos šių funkcijų. Nors sesiją sudaro klientas, tačiau ją visuomet nutraukia serveris perduodamas sesijos pabaigos pranešimą.

Visų pirma prieš pradedant mobiliojo įrenginio konfigūravimą jį būtina užregistruoti serveryje. Registracijos procesas yra skirtas tam, kad susietų tam tikrą sistemos vartotoją su registruojamu mobiliuoju įrenginiu. Šiam tikslui yra naudojamas vartotojo ir įrenginio autentifikavimo mechanizmas detaliau aprašytas „3.3.1. Įrenginių registravimo/išregistravimo mechanizmas“ skyriuje.

Kita funkcija kurią gali atlikti serveris sesijos metu yra komandų perdavimas įrenginiui. Komandos gali būti perduodamos tiek SOAP, tiek JSON formato žinutėmis. Serveris vienu pranešimu gali perduoti keletą komandų. Priėmęs komandas, klientas jas vykdo visas iš eilės (atitinkamai kokia tvarka buvo paduotos žinutėje). Įvykdžius visas priimtas komandas klientas serveriui perduoda pranešimą su gautais rezultatais. Detaliau šis mechanizmas yra aprašomas „3.3.2. Įrenginių konfigūravimo ir valdymo mechanizmas“ skyriuje.

Klientas serveriui taip pat gali perduoti pranešimus. Šiais pranešimais serveris yra informuojamas apie įrenginio būsenos pokyčius. Detaliau šis mechanizmas yra aprašomas „3.3.3. Pranešimų perdavimo mechanizmas“ skyriuje.

3.3.1. Įrenginių registravimo/išregistravimo mechanizmas



3.4 pav. Mobiliųjų įrenginių registravimo mechanizmas

Prieš pradedant vykdyti mobiliojo įrenginio konfigūravimą jis privalo būti užregistruotas serveryje. MĮ registravimas serveryje yra atliekamas 2 etapų mechanizmu, kurių metu serveris ir

klientas apsikeičia keturiais pranešimais.

1. **Etapas: vartotojo autentifikavimas -** skirtas vartotojo norinčio atlikti įrenginio registravimo veiksmą autentifikavimui.
    1. Vartotojo autentifikavimosi užklausa (žr. 3.1 lent.) – klientas inicijuodamas sesiją serveriui perduoda savo autentifikavimo informaciją. Šiam tikslui gali būti naudojami įvairūs autentifikavimo mechanizmai, tokie kaip vartotojo vardas ir slaptažodis ar skaitmeniniai sertifikatai.
    2. Vartotojo autentifikavimosi atsakymas (žr. 3.2 lent.) – jeigu vartotojo pateikta autentifikavimosi informacija yra teisinga, serveris grąžina sėkmės pranešimą, prie kurio yra prisegtas autentifikavimosi žetonas. Šis žetonas yra naudojamas antrajame įrenginio registravimo etape. Jeigu pateikta autentifikavimosi informacija yra neteisinga, serveris grąžina klaidos pranešimą.

3.1 lentelė Vartotojo autentifikavimosi užklausos pranešimo parametrai

Parametras	Aprašymas
Autentifikavimo tipas	Autentifikavimo tipas nurodo naudojamą autentifikavimo mechanizmą.
Autentifikavimo informacija	Autentifikavimo duomenys priklausantys nuo sistemoje naudojamo autentifikavimo mechanizmo (pvz.: vartotojo vardas ir slaptažodis, skaitmeninis sertifikatas).

3.2 lentelė Vartotojo autentifikavimosi atsakymo pranešimo parametrai

Rezultatas	Parametras	Aprašymas
Sėkmingas vartotojo autentifikavimas	**Autentifikavimo žetonas**	Autentifikavimo žetonas, tai šešioliktainio formato simbolių eilutė, kuri yra naudojama vartotojo identifikacijai įrenginio registravimo etape.
	Žetonas galioja iki	Data, kuri parodo kiek laiko galioja iš serverio gautas žetonas. Pasibaigus šiam laikui žetonas yra laikomas negaliojančiu ir norint atlikti įrenginio registraciją reikia pakartoti vartotojo autentifikavimą.
Nesėkmingas vartotojo autentifikavimas	**Klaidos kodas**	Sveikasis skaičius, kurio vertė yra lygi 4xx. Klaidos kodas parodo kokia klaida įvyko. Naudojami standartiniai HTTP protokolo klaidų kodai.
	Klaidos žinutė	Grąžinama žinutė su žmogui suprantamu tekstu apibūdinančiu įvykusią klaidą.

2. **Etapas: įrenginio registravimas/išregistravimas** – antrajame etape mobilusis įrenginys yra susiejamas su arba atsiejamas nuo vartotojo.
    3. Mobiliojo įrenginio registracijos užklausa (žr. 3.3 lent.) – darydamas užklausą vartotojas serveriui perduoda mobilųjį įrenginį identifikuojančią informaciją (unikalus įrenginio identifikatorius) ir pirmajame etape iš serverio gautą autentifikavimosi žetoną.
    4. Mobiliojo įrenginio registracijos atsakymas (žr. 3.4 lent.) – jeigu įrenginys dar nėra susietas su kitu vartotoju klientui grąžinamas registracijos patvirtinimo atsakymas ir įrenginio autorizacijos žetonas. Jeigu įrenginys jau priklauso kitam vartotojui serveris grąžina klaidos pranešimą. Įvykus sėkmingai įrenginio registracijai sesija gali būti pratęsiama. Tai atliekama kartu su sėkmingos registracijos pranešimu įrenginiui perduodant konfigūracijos ar valdymo komandas. Tolimesnis sesijos veikimas yra aprašomas „3.3.2. Įrenginių konfigūravimo ir valdymo mechanizmas“ skyriuje. Vykdant įrenginio išregistravimą serveris patikrina ar išregistruojamas įrenginys tikrai priklauso šiam vartotojui, jeigu taip, grąžinamas patvirtinimo pranešimas ir įrenginys yra išregistruojamas, jeigu ne, yra gražinamas klaidos pranešimas, o įrenginys nėra išregistruojamas.

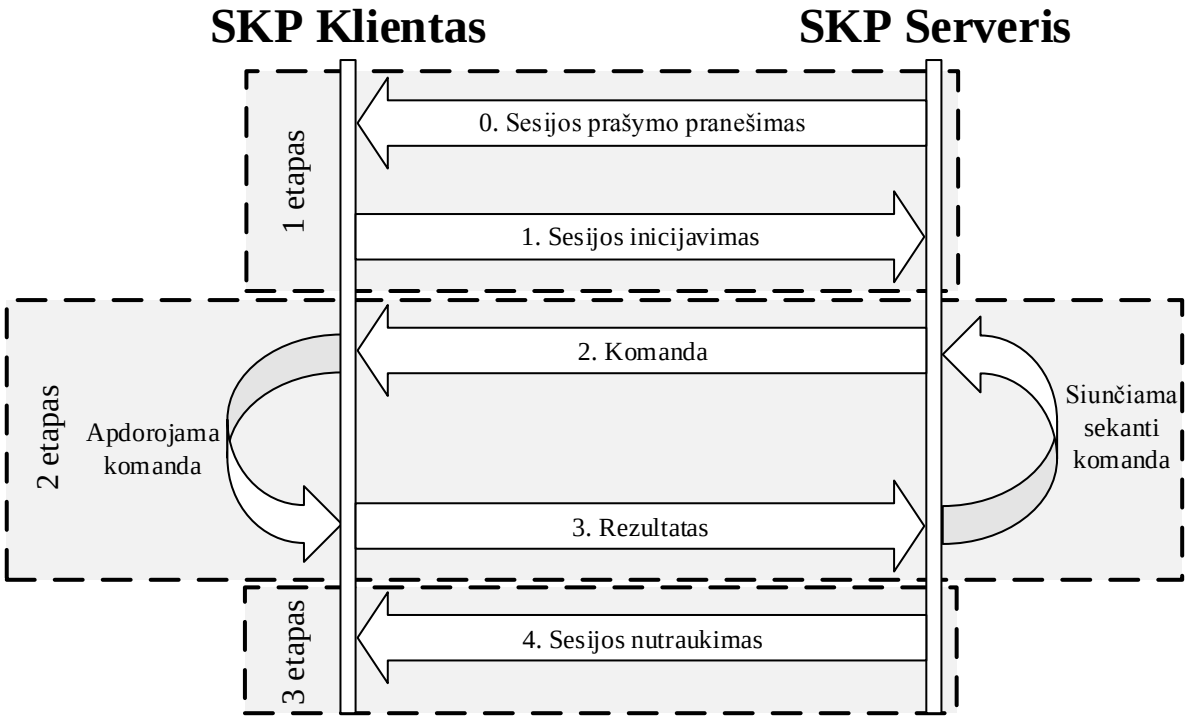
3.3 lentelė Mobiliojo įrenginio registracijos užklausos pranešimo parametrai

Parametras	Aprašymas
Įrenginio identifikatorius	Standartinis įrenginio identifikacinis numeris, kurį suteikia operacinė sistema.
Autentifikavimosi žetonas	Pirmajame etape gautas vartotojo autentifikavimo žetonas, skirtas vartotojo identifikacijai.

3.4 lentelė Mobiliojo įrenginio registracijos atsakymo pranešimo parametrai

Komanda	Rezultatas	Parametras	Aprašymas
Registracija	Sėkminga registracija	**Įrenginio autorizacijos žetonas**	Šis žetonas yra naudojamas visuose tolimesniuose komunikacijų mechanizmuose mobiliojo įrenginio autentifikavimui. Jis turi būti pridedamas prie visų serveriui siunčiamų užklausų.
		Komandų rinkinys	Serveris kartu su sėkmingos registracijos pranešimu mobiliajam įrenginiui gali perduoti konfigūravimo arba valdymo komandas.
	Nesėkminga registracija	**Klaidos kodas**	Sveikasis skaičius, kurio vertė yra lygi 4xx. Klaidos kodas parodo kokia klaida įvyko. Naudojami standartiniai HTTP protokolo klaidų kodai.
		Klaidos žinutė	Grąžinama žinutė su žmogui suprantamu tekstu apibūdinančiu įvykusią klaidą.
Išregistravimas	Sėkmingas išregistravimas	-	Serveris negrąžina jokių papildomų parametrų.
	Nesėkmingas išregistravimas	**Klaidos kodas**	Sveikasis skaičius, kurio vertė yra lygi 4xx. Klaidos kodas parodo kokia klaida įvyko. Naudojami standartiniai HTTP protokolo klaidų kodai.
		Klaidos žinutė	Grąžinama žinutė su žmogui suprantamu tekstu apibūdinančiu įvykusią klaidą.

3.3.2. Įrenginių konfigūravimo ir valdymo mechanizmas



3.5 pav. Mobiliųjų įrenginių konfigūravimo ir valdymo mechanizmas

3.5 pav. yra pavaizduotas mobiliųjų įrenginių konfigūravimo ir valdymo mechanizmas. Komandų perdavimui gali būti inicijuojama nauja sesija arba pratęsiama prieš tai įrenginio registracijai ar pranešimų perdavimui sudaryta sesija. Šis mechanizmas susideda iš 3 etapų.

1. **Etapas: sesijos sudarymas** – šis etapas nėra privalomas, nes komandų perdavimui gali būti pratęsiama sena sesija. Šio etapo tikslas užmegzti ryšį su serveriu.
   0. Sesijos prašymo pranešimas – tai neprivalomas žingsnis, kurio metu serveris klientui išsiunčia pranešimą (pasinaudodamas standartinėmis pranešimų perdavimo paslaugomis), kuriuo prašo klientą sudaryti sujungimą. Šiuo pranešimu nėra perduodami jokie parametrai.
   1. Sesijos inicijavimo užklausa – klientas darydamas užklausą inicijuoja sesiją ir praneša serveriui, kad yra pasiruošęs vykdyti komandas. Kartu su šiuo pranešimu turi būti perduodamas įrenginio autorizacijos žetonas.
2. **Etapas: komandų vykdymas** – šio etapo metu mobilusis įrenginys vykdo komandas, kurias jam atsiuntė serveris. Atlikus užduotas komandas klientas serveriui siunčia atsakymą su gautu rezultatu. Šis etapas prasideda tuomet kai klientas iš serverio gauną pirmąjį pranešimą su konfigūracinėmis arba valdymo komandomis, t.y. atsakymas į sesijos inicijavimo užklausą. Tuo atveju kai sesija yra pratęsiama pirmoji komanda yra perduodama kartu su įrenginio registracijos patvirtinimu ar kaip atsakymas į perduodamą kliento pranešimą.
   2. Atsakymas su komandomis (žr. 3.6 lent.) – komandų vykdymas yra pradedamas kai klientas gauna atsakymą iš serverio, kad sesija buvo sėkmingai užmegzta. Kartu su šiuo pranešimu yra perduodamas klientui skirtų komandų (žr. 3.5 lent.) ir jų identifikatorių rinkinys. Jeigu sesijos užmegzti nepavyko yra grąžinamas klaidos pranešimas.

Užklausa su rezultatais (žr.

   3. 3.7 lent.) – įvykdžius komandas, klientas daro užklausą į serverį, kuria perduoda gautus rezultatus. Kartu su šiuo pranešimu yra perduodami šie parametrai: rezultatų tipai, rezultatų duomenys ir įvykdytų komandų identifikatoriai.

3.5 lentelė Klientui perduodamos komandos

Pasyvios komandos	Aprašymas
Įrenginio informacijos gavimas	Gavęs šią komandą klientas serveriui nusiunčia informaciją apie įrenginį. Tai tokia informacija kaip: įrenginio modelis, gamintojas, operacinė sistema ar jos versija ir pan.
Saugumo politikų atnaujinimas	Šia komanda serveris inicijuoja saugumo politikų atnaujinimą kliente. Saugumo politikos yra perduodamos kartu su komandos pranešimu kaip papildomi duomenys.
Nuotolinis programinės įrangos diegimas/atnaujinimas	Šia komanda yra inicijuojamas nuotolinis programinės įrangos diegimas arba atnaujinimas. Kartu su komandos pranešimu yra perduodama nuoroda į taikomųjų programų serverį iš kurio klientas parsisiunčia programinės įrangos paketą diegimui.
Įrenginio užrakinimas	Ši komanda skirta nuotoliniam mobiliojo įrenginio užrakinimui. Šią komanda gali inicijuoti tik sistemos administratorius.
Įrenginio atminties ištrynimas (gamykliniai nustatymai)	Ši komanda skirta visų įrenginyje esančių duomenų ištrynimui nuotoliniu būdu. Šią komanda gali inicijuoti tik sistemos administratorius.
Sesijos uždarymas	Ši komanda parodo, kad serveris uždaro sesiją ir baigia komunikacijas.

3.6 lentelė Pranešimo, kuriuo yra perduodamos komandos, parametrai

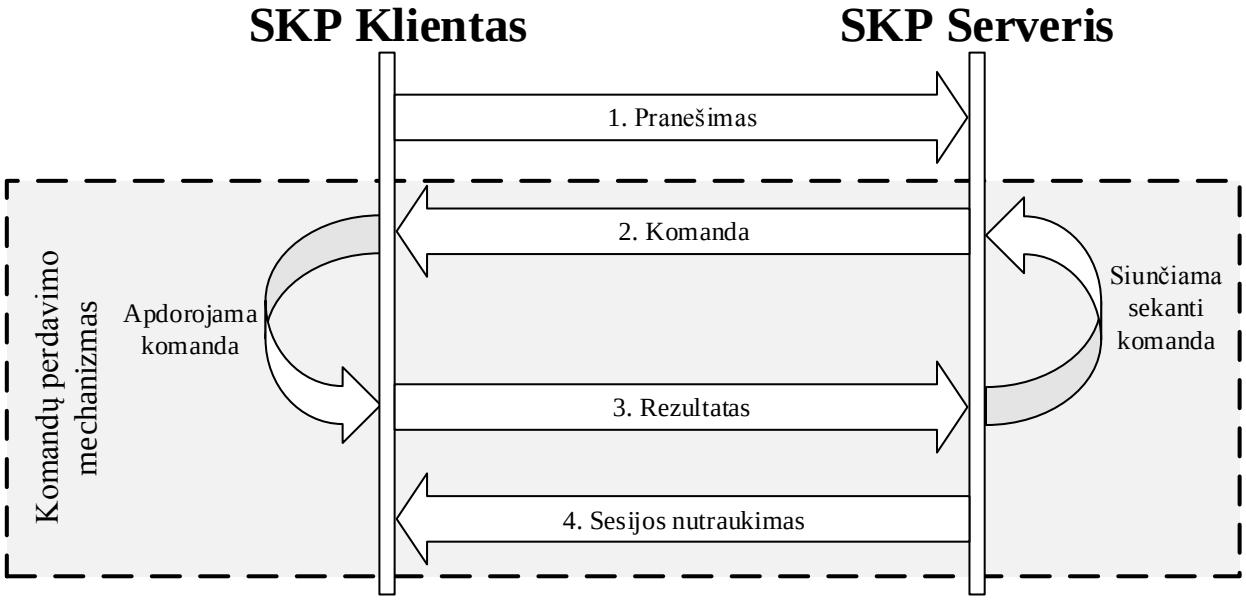
Rezultatas	Parametras	Aprašymas
Sėkminga iniciacija	**Komandų rinkinys**	Masyvas, kuriame yra pateikiamos klientui skirtos komandos ir jų identifikatoriai.
Nesėkminga iniciacija	**Klaidos kodas**	Sveikasis skaičius, kurio vertė yra lygi 4xx. Klaidos kodas parodo kokia klaida įvyko. Naudojami standartiniai HTTP protokolo klaidų kodai.
	Klaidos žinutė	Grąžinama žinutė su žmogui suprantamu tekstu apibūdinančiu įvykusią klaidą.

3.7 lentelė Pranešimo, kuriuo yra perduodami komandų vykdymo rezultatai, parametrai

Parametras	Aprašymas
Autorizacijos žetonas	Įrenginio registracijos metu gautas autorizacijos žetonas skirtas įrenginio identifikacijai..
Komandų vykdymo rezultatas	Masyvas, kuriame yra pateikiami vykdytų komandų identifikatoriai, rezultatų tipai ir rezultatų duomenys

3. **Etapas: sesijos nutraukimas** – sesiją visuomet nutraukia serveris. Sesija yra nutraukiama sesijos nutraukimo pranešimu. Serveris šį pranešimą perduoda kaip atsakymą į kliento siunčiamą komandų vykdymo rezultato užklausą. Taip pat sesija yra laikoma nutraukta jeigu serveris klientui atsako klaidos pranešimu.

3.3.3. Pranešimų perdavimo mechanizmas



3.6 pav. Pranešimų perdavimo mechanizmas

Klientas serveriui taip gali perduoti pranešimus apie mobiliojo įrenginio būsenos ir būklės pokyčius. Šie pranešimai gali būti perduodami neinicijuojant sesijos. Perdavus pranešimą sesija gali būti inicijuojama tuo atveju, jeigu serveris klientui kartu su atsakymų į užklausą atsiunčia komandą(-as). Tokiu atveju tolimesnis sesijos vykdymas yra atliekamas „3.3.2. Įrenginių konfigūravimo ir valdymo mechanizmas“ skyriuje aprašyta tvarka. 3.6 pav. yra pateikiamas pranešimų perdavimo mechanizmas.

Pranešimai (žr. 3.9 lent.) serveriui yra perduodami kaip nepriklausomos užklausos, kurioms nėra reikalinga sesija. Pranešimai gali būti trijų tipų:

1. **Informaciniai pranešimai** – šis pranešimų tipas skirtas įvairių įrenginio parametrų bei įvykių (pvz.: baterijos lygio, būvimo vietos ar programinės įrangos diegimo) perdavimui į serverį.
2. **Klaidų pranešimai** – šis pranešimų tipas skirtas informuoti serverį apie įrenginyje įvykusias klaidas (pvz.: užstrigo programėlė, baigėsi įrenginio atmintis).
3. **Įspėjamieji pranešimai** - šie pranešimai serveriui perduoda įspėjimus apie mobiliajame įrenginyje atliekamus saugumo politiką pažeidžiančius veiksmus (pvz.: keletą kartų neteisingai įvestas PIN kodas ar slaptažodis).

Su pranešimu turi būti perduoti šie parametrai: įrenginio autorizacijos žetonas, pranešimo tipas,

perduodamos informacijos tipas ir pati informacija. Pranešimais perduodami parametrai yra pateikiami 3.8 lentelėje.

3.8 lentelė Pranešimu perduodami parametrai

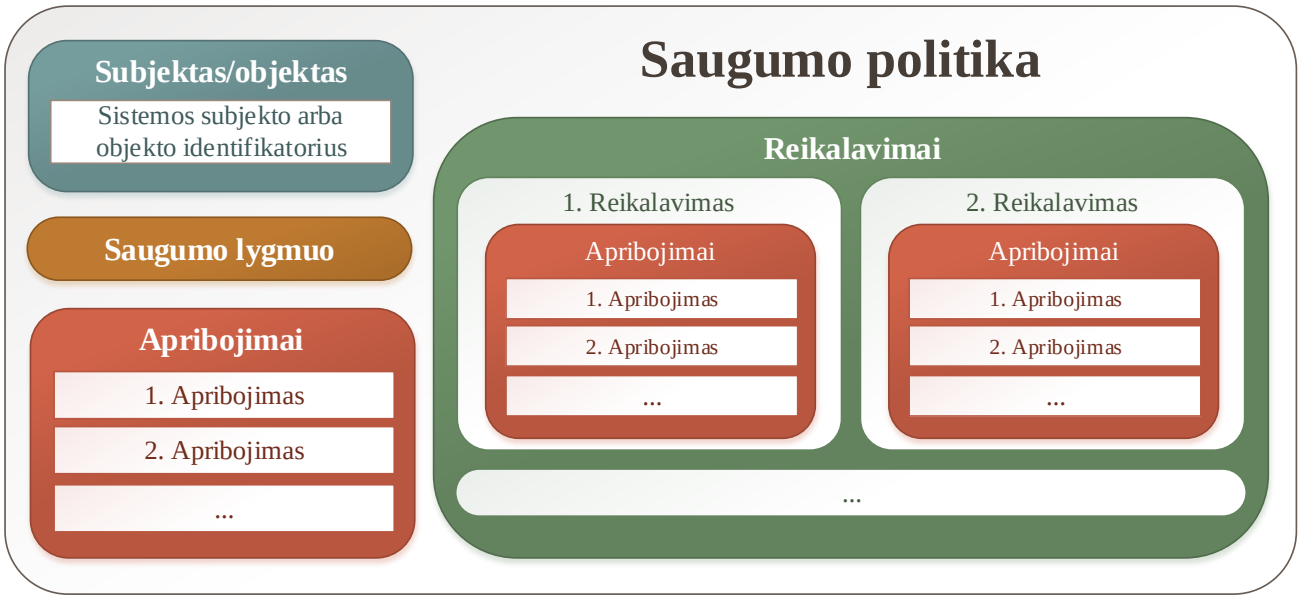
Parametras	Aprašymas
Įrenginio autorizacijos žetonas	Įrenginio registracijos metu gautas autorizacijos žetonas skirtas įrenginio identifikacijai.
Pranešimo tipas	Identifikatorius, kuris nurodo kokio tipo pranešimas yra perduodamas: informacinis, klaidos ar įspėjamasis.
Perduodamos informacijos tipas	Identifikatorius, kuris nurodo koks įvykis ar įrenginio būklės pasikeitimas yra pranešamas. Perduodamos informacijos tipai yra aprašomi 3.9 lentelėje.
Perduodama informacija	Tam tikra informacija apibūdinanti įvykį ar įrenginio būklės pokytį.

3.9 lentelė Pranešimais perduodami informacijos tipai

Pranešimo tipas	Parametro pavadinimas	Aprašymas
Informacinis	Baterijos lygis	Perduodama informacija apie įrenginio baterijos lygį (procentais).
	Pozicija (koordinatės)	Perduodama informacija apie dabartinę įrenginio būvimo vietą (GPS koordinatės).
	„Bluetooth“ veikimo pokytis	Perduodama informacija apie „Bluetooth“ adapterio veikimą, t.y. kada jis buvo įjungtas arba išjungtas, su kokiais įrenginiais buvo susijungęs ir kokius veiksmus atliko.
	„NFC“ veikimo pokytis	Perduodama informacija apie „NFC“ adapterio veikimą, t.y. kada jis buvo įjungtas arba išjungtas ir kokius veiksmus atliko.
	Bevielio tinklo jungties pokytis	Perduodama informacija apie tai prie kokių bevielių tinklų ir kada buvo prisijungęs įrenginys.
	Kameros veikimas	Perduodama informacija apie tai, kada buvo naudojama mobiliojo įrenginio kamera.
	Programinės įrangos diegimas	Pranešama, kad mobiliajame įrenginyje buvo įdiegta programėlė.
	Programinės įrangos ištrynimas	Pranešama, kad mobiliajame įrenginyje buvo ištrinta programėlė.
	Kiti	Realizuojant sistemą gali būti naudojami ne tik šioje lentelėje apibrėžti pranešimų parametrai. Sistemos kūrėjai gali aprašyti ir panaudoti kitokius jų sistemai svarbius mobiliųjų įrenginių parametrus.
Klaidos	Klaidos kodas	Sveikasis skaičius nurodantis klaidos kodą.
	Kontekstinė informacija	Duomenų masyvas, kuriame pateikiama papildoma informacija apie klaidos įvykio aplinkybes. Šis parametras gali būti tuščias.
Įspėjamasis	Įvykio tipas	Sveikasis skaičius nurodantis įspėjamojo pranešimo tipą.
	Kontekstinė informacija	Duomenų masyvas, kuriame pateikiama papildoma informacija apie įvykusio incidento aplinkybes. Šis parametras gali būti tuščias.

3.4. Dinaminis saugumo politikų profiliavimas

Mobiliųjų įrenginių konfigūravimui ir jų saugumo lygio įvertinimui yra naudojamos saugumo politikos. Saugumo politika (žr. 3.7 pav.) tai duomenų struktūra, kuri nurodo tris pagrindinius mobiliųjų įrenginių saugaus konfigūravimo aspektus, t.y. kokiam sistemos subjektui ar objektui yra priskirta saugumo politika, kokie apsaugos mechanizmai turi būti taikomi ir kokioms sąlygoms esant jie turėtų būti taikomi įrenginyje. Kaip matome, saugumo politika yra sudaryta iš keturių komponentų subjektų/objektų identifikatoriaus, saugumo lygmens, apribojimų ir reikalavimų.



3.7 pav. Saugumo politikos struktūra

Saugumo politikos gali būti priskiriamos tiek atskiriems sistemos subjektams (vartotojams), tiek sistemos objektams (mobiliesiems įrenginiams). Bet kuriuo atveju saugumo politikos yra pritaikomos mobiliuosiuose įrenginiuose. Vienas įrenginys gali turėti keletą skirtingų saugumo politikų. Saugumo politikos įrenginyje yra pritaikomos atsižvelgiant į apribojimus ir saugumo lygmenį. Esant kelioms vienu metu galiojančioms saugumo politikoms pritaikoma yra ta, kurios saugumo lygmuo yra aukštesnis, t.y. yra pritaikoma griežtesnė saugumo politika. Sistemoje siūlomi realizuoti saugumo lygmenys ir su jais susiję saugos mechanizmai yra pateikiami 3.10 lentelėje, tačiau realizuojant sistemą gali būti sudaromi ir kitokie saugumo lygmenys bei pasirenkami kitokie saugumo mechanizmai atitinkantys sistemai keliamus reikalavimus.

3.10 lentelė Saugumo lygmenys ir su jais susiję saugos mechanizmai

Privalomas Neprivalomas Nereikalingas	**Saugumo lygmenys**			
Saugumo mechanizmai	**Labai aukštas**	**Aukštas**	**Vidutinis**	**Žemas**
Darbuotojų autentifikavimas				
Prieigos prie įmonės duomenų kontrolė				
Užraktas su slaptažodžiu				
Sudėtingas slaptažodis				
Automatinis užrakinimas	Iš karto	Po 1 min.	Po 1 min.	Po 5 min.
Duomenų šifravimas				
„WiFi“ ryšio apribojimai	WPA2	WPA2	WPA2, WPA	WPA2, WPA
Antivirusinė programinė įranga				
Užtvara				
Įsibrovimo aptikimo programinė įranga				
Automatiniai programinės įrangos atnaujinimai				
Programinės įrangos diegimo ir naudojimo apribojimai				
„Bluetooth“ naudojimas	Išjungtas	Išjungtas	Išjungtas	
„NFC“ naudojimas	Išjungtas	Išjungtas	Išjungtas	
GPS sekimas	Įjungtas	Įjungtas	Įjungtas	
Nuotolinio valdymo funkcijos	Įjungtos	Įjungtos	Įjungtos	Įjungtos

Apribojimai tai saugumo politikos dalis, kuri nurodo kokioms sąlygoms esant ji turėtų būti pritaikoma įrenginyje. Apribojimai gali būti priskiriami visai saugumo politikai, tai reiškia, kad priklausomai nuo šio apribojimo bus pritaikoma arba ne visa saugumo politika. Taip pat apribojimus galima priskirti ir atskiriems saugumo politikos reikalavimams, šiuo atveju apribojimas apspręs ar

turėtų būti pritaikomas būtent šis saugumo politikos elementas. Galimi saugumo politikos apribojimai yra pateikiami 3.11 lentelėje. Atsižvelgdamas į šiuos apribojimus klientas automatiškai perjungia saugumo politikas kintant įrenginio būsenai ar parametrams.

3.11 lentelė Saugumo politikos apribojimai

Apribojimas	Aprašymas	Pavyzdys
Pozicija (GPS koordinatės)	Saugumo politika arba jos reikalavimai apribojami pagal įrenginio buvimo vietą, t.y. saugumo politika įjungiama arba išjungiama kai įrenginys patenka į tam tikrą zoną	Įrenginyje yra išjungiama kamera patekus į įmonės teritoriją.
Laikas	Saugumo politika yra pritaikoma atsižvelgiant į laiką ir datą.	Darbo valandomis įrenginyje yra uždraudžiama naudotis socialinių tinklų programėlėmis, o po darbo jų veikimas vėl aktyvuojamas.
Bevielio ryšio tinklas	Saugumo politika pritaikoma priklausomai nuo to prie kokio bevielio ryšio tinklo yra prisijungiama ir kokį ryšio protokolą šis tinklas naudoja.	Uždrausti prieigą prie įmonės duomenų jeigu yra prisijungta prie viešo „WiFi“ tinklo ir suteikti prieigą jeigu yra prisijungtą prie vidinio įmonės tinklo.
Įrenginio aparatinių funkcijų veikimas	Saugumo politika pritaikoma priklausomai nuo to kokios įrenginio aparatinės funkcijos yra įjungtos (GPS, Bluetooth, NFC ir pan.).	Uždrausti prieigą prie įmonės duomenų jeigu yra įjungtas „Bluetooth“.

Reikalavimai – tai saugumo politikos dalis, kuri aprašo kokios saugumo priemonės turėtų būti pritaikomos įrenginyje. Saugos reikalavimai gali būti dviejų tipų: privalomi ir neprivalomi. Įrenginys įgyja saugaus įrenginio statusą tik tuomet kai yra patenkinami visi privalomi saugumo politikos reikalavimai. Įrenginys gali neatitikti neprivalomų reikalavimų ir vis tiek būti laikomu saugiu, tačiau sistema informuos vartotoją (pateikdama informacinius pranešimus), kad mobilusis įrenginys neatitinka tam tikrų saugumo politikos reikalavimų ir yra siūloma pakeisti tam tikrus įrenginio nustatymus. Galimi saugumo politikos reikalavimai yra pateikiami 3.10 lentelėje. Šiame darbe pateikti tik rekomendaciniai saugumo reikalavimai, realizuojant sistemą, atsižvelgiant į įmonės poreikius, gali būti pasirenkami kitokie saugumo mechanizmai bei sudaromos kitokios saugumo politikos.

3.5. Nuotolinio programinės įrangos diegimo ir atnaujinimo mechanizmas

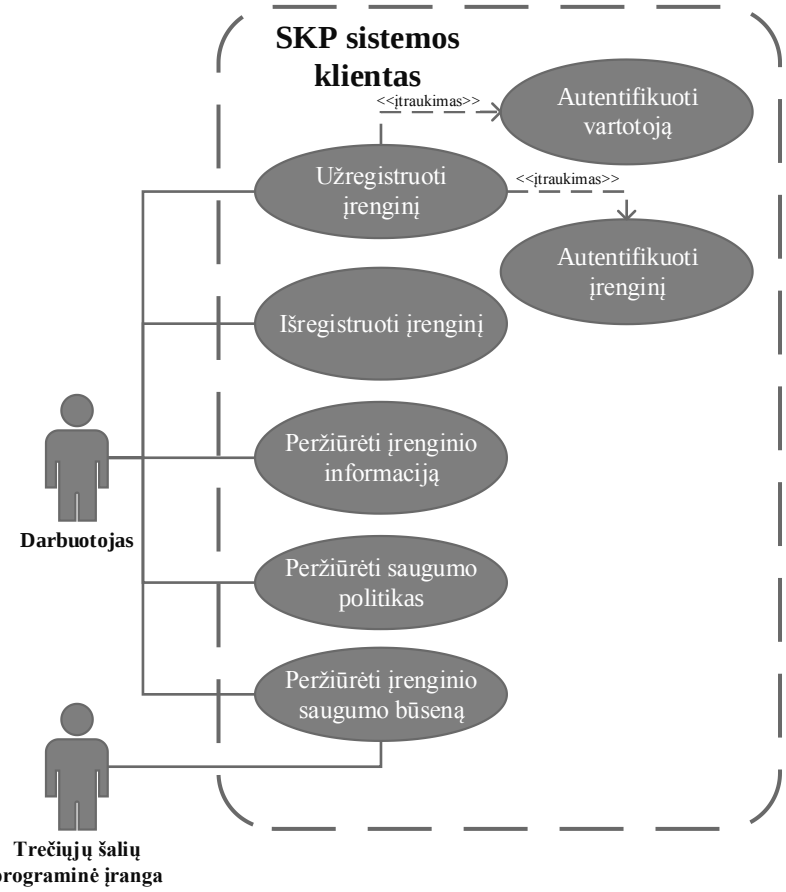
3.8 pav. Nuotolinio programinės įrangos diegimo ir atnaujinimo mechanizmas

Nuotolinis programinės įrangos diegimas arba atnaujinimas yra inicijuojamas valdymo komanda „nuotolinis programinės įrangos diegimas/atnaujinimas“. Serveris klientui kartu su valdymo komanda perduoda URL nuoroda kuri nurodo iš kur reikia atsisiųsti diegiamą programinę

įrangą. Už programinės įrangos diegimą yra atsakingas taikomųjų programų serveris. Šis sistemos komponentas gali būti realizuotas kaip pagrindinio mobiliųjų įrenginių konfigūravimo serverio dalis arba kaip atskiras serveris. Gavęs tokią komandą klientas inicijuoja sujungimą su taikomųjų programų serveriu. Šiam tikslui panaudodamas gautą URL nuorodą, ir iš jo atsisiunčia programinės įrangos paketą. Gavus vartotojo sutikimą parsiųsta programinė įrangą yra įdiegiama. Klientas užfiksuoja, kad programinės įrangos diegimo ar atnaujinimo procesas yra baigtas ir serveriui išsiunčia atsakymą, kad komanda buvo įvykdyta sėkmingai. Jeigu nepavyko parsisiųsti programos diegimo paketo, jos įdiegti ar vartotojas nesuteikė leidimo ją diegti, serveriui yra perduodamas klaidos pranešimas, kuris parodo, kad programinė įranga nebuvo įdiegta. 3.8 pav. yra pateikiamas programinės įrangos diegimo/atnaujinimo procedūros grafikas.

3.6. Saugaus konfigūravimo paramos sistemos modelis

Sistemos darbą geriausiai apibūdina serverio ir kliento panaudos atvejų bei būsenų diagramos (žr. 3.9 pav. – 3.12 pav.).

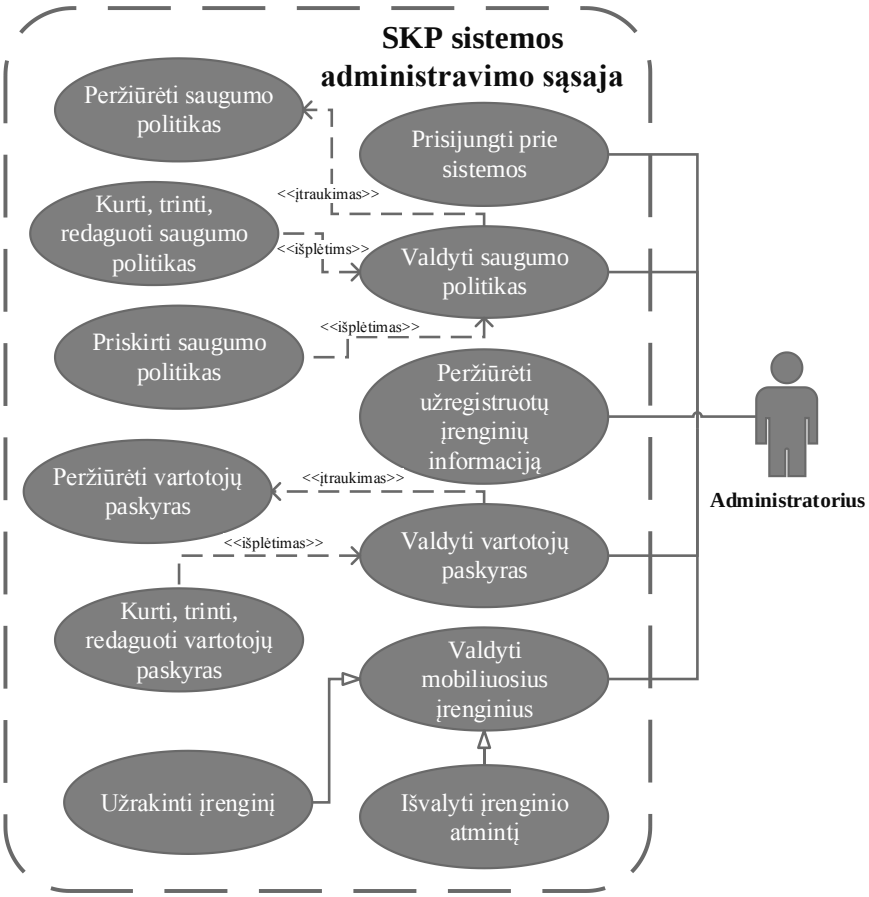


3.9 pav. SKP sistemos kliento programinės įrangos panaudos atvejų diagrama (UML notacija)

3.9 pav. yra pateikta SKP sistemos kliento programinės įrangos panaudos atvejų diagrama. Joje matome, kad klientu gali naudotis dviejų tipų aktoriai: darbuotojai ir trečiųjų šalių programinė įranga. Panaudos atvejai kuriais aktoriai gali sąveikauti su sistema yra aprašomi 3.12 lentelėje.

3.12 lentelė SKP sistemos kliento programinės įrangos panaudos atvejai

Panaudos atvejis:	Užregistruoti įrenginį
Tikslas: užregistruoti mobilųjį įrenginį sistemoje **Aktorius:** darbuotojas **Susiję PA:** • Autentifikuoti vartotoją; • Autentifikuoti įrenginį;	**Aprašymas:** Įmonės darbuotojas, turintis vartotojo paskyrą, gali sistemoje užregistruoti mobilųjį įrenginį. Vykdant įrenginio registraciją yra atliekamas vartotojo ir jo įrenginio autentifikavimas. Įrenginys yra sėkmingai užregistruojamas tuo atveju, jeigu jo nėra užregistravęs kažkuris kitas sistemos vartotojas.
Panaudos atvejis:	Autentifikuoti vartotoją
Tikslas: atpažinti, kad įrenginį registruoja tikras sistemos vartotojas **Aktorius:** darbuotojas **Susiję PA:** • Užregistruoti įrenginį;	**Aprašymas:** Registruojant įrenginį sistema patikrina ar vartotojas bandantis užregistruoti įrenginį yra tikras. Vartotojų autentifikavimui gali būti naudojamas vartotojo vardas ir slaptažodis arba sertifikatai.
Panaudos atvejis:	Autentifikuoti įrenginį
Tikslas: nustatyti ar registruojamas įrenginys yra validus **Aktorius:** darbuotojas **Susiję PA:** • Užregistruoti įrenginį;	**Aprašymas:** Registruojant įrenginį, sistema patikrina ar tai tikras sistemos klientas, ar įrenginys gali būti registruojamas ir ar jis nėra priskirtas kitam įmonės darbuotojui.
Panaudos atvejis:	Išregistruoti įrenginį
Tikslas: išregistruoti mobilųjį įrenginį iš sistemos. **Aktorius:** darbuotojas	**Aprašymas:** Darbuotojas turi galimybę išregistruoti įrenginį iš sistemos. Atlikus išregistravimą klienas mobiliajame įrenginyje nustoja veikti ir įrenginys tampa netinkamu darbui įmonėje.
Panaudos atvejis:	Peržiūrėti įrenginio informaciją
Tikslas: pamatyti įvairią įrenginio techninę ir programinę informaciją **Aktorius:** darbuotojas	**Aprašymas:** Darbuotojas įrenginyje gali matyti įvairius įrenginio parametrus, tokius kaip: įrenginio gamintojas, modelis, operacinės sistemos versija, WiFi ir mobiliojo ryšio tinklų informacija ir kt.
Panaudos atvejis:	Peržiūrėti saugumo politikas
Tikslas: pamatyti įrenginiui priskirtas saugumo politikas **Aktorius:** darbuotojas	**Aprašymas:** Įmonės darbuotojas, turi galimybę peržiūrėti visas jam ir mobiliajam įrenginiui priskirtas saugumo politikas. Taip pat yra atvaizduojama informacija apie šiuo metu galiojančią saugumo politiką..
Panaudos atvejis:	Peržiūrėti įrenginio saugumo būseną
Tikslas: pamatyti ar įrenginys atitinka saugumo politikos keliamus reikalavimus ar ne **Aktorius:** darbuotojas, trečiųjų šalių programinė įranga	**Aprašymas:** Darbuotojas ir trečiųjų šalių programinė įranga turi galimybę matyti ar įrenginys atitinka saugumo politikos keliamus reikalavimus ir yra saugus darbui įmonėje.



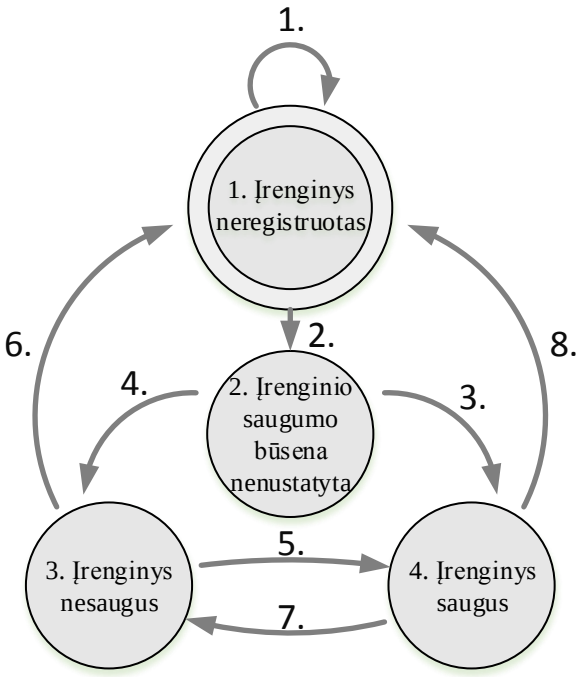
3.10 pav. SKP sistemos administravimo sąsajos panaudos atvejų diagrama (UML notacija).

3.10 pav. yra pateikta SKP sistemos administravimo sąsajos panaudos atvejų diagrama. Joje matome, kad administravimo sąsaja gali naudotis tik vieno tipo aktoriai, administratoriai. Panaudos atvejai kuriais vartotojai gali sąveikauti su sistema yra aprašomi 3.13 lentelėje.

3.13 lentelė SKP sistemos administravimo sąsajos panaudos atvejai

Panaudos atvejis:	Prisijungti prie sistemos
Tikslas: prisijungti prie sistemos	**Aprašymas:** Administratorius norėdamas atlikti kokius nors veiksmus SKP sistemoje privalo prisijungti prie administravimo sąsajos. Prisijungimui yra naudojamas vartotojo vardas ir slaptažodis.
Aktorius: administratorius	
Panaudos atvejis:	Valdyti saugumo politikas
Tikslas: valdyti mobiliesiems įrenginiams priskirtas saugumo politikas	**Aprašymas:** Administratorius prisijungęs prie administravimo sąsajos turi galimybę peržiūrėti, kurti, trinti, redaguoti ir priskirti saugumo politikas.
Aktorius: administratorius	
Susiję PA: • Peržiūrėti saugumo politikas; • Kurti, trinti, redaguoti saugumo politikas; • Priskirti saugumo politikas;	
Panaudos atvejis:	Peržiūrėti saugumo politikas
Tikslas: peržiūrėti sistemoje sukurtas saugumo politikas	**Aprašymas:** Administratorius prisijungęs prie administravimo sąsajos turi galimybę peržiūrėti visas sistemoje sukurtas saugumo politikas, gali peržiūrėti kurios saugumo politikos kuriems vartotojams ir įrenginiams yra priskirtos.
Aktorius: administratorius	
Susiję PA: • Valdyti saugumo politikas;	

Panaudos atvejis:	Kurti, trinti , redaguoti saugumo politikas
Tikslas: sudaryti saugumo politikas	**Aprašymas:** Administratorius prisijungęs prie administravimo sąsajos turi galimybę kurti naujas, trinti ir redaguoti senas saugumo politikas..
Aktorius: administratorius	
Susiję PA: • Valdyti saugumo politikas;	
Panaudos atvejis:	Priskirti saugumo politikas
Tikslas: įmonės darbuotojams ir jų įrenginiams priskirti saugumo politikas	**Aprašymas:** Administratorius prisijungęs prie administravimo sąsajos turi galimybę įmonės darbuotojams ir jų įrenginiams priskirti įvairias saugumo politikas arba jas panaikinti.
Aktorius: administratorius	
Susiję PA: • Valdyti saugumo politikas;	
Panaudos atvejis:	Peržiūrėti užregistruotų įrenginių informaciją
Tikslas: matyti sistemoje registruotų įrenginių informaciją	**Aprašymas:** Administratorius prisijungęs prie administravimo sąsajos turi galimybę peržiūrėti visų sistemoje registruotų įrenginių informaciją. Administravimo sąsajoje matoma tiek bazinė įrenginių informacija (gamintojas, modelis, operacinė sistema), tiek ir įrenginio įvykių bei pozicijos registras, jeigu to reikalauja saugumo politika ir darbuotojas suteikia atitinkamas teisės kliento programinei įrangai.
Aktorius: administratorius	
Panaudos atvejis:	Valdyti vartotojų paskyras
Tikslas: peržiūrėti, kurti, trinti ir redaguoti sistemos vartotojų paskyras	**Aprašymas:** Administratorius prisijungęs prie administravimo sąsajos turi galimybę peržiūrėti visų sistemoje registruotų vartotojų paskyras, jas redaguoti, trinti ir kurti naujas. Administratorius taip pat mato kiek ir kokių įrenginių vartotojas yra užregistravęs sistemoje.
Aktorius: administratorius	
Panaudos atvejis:	Valdyti mobiliuosius įrenginius
Tikslas: įvykdyti nuotolines mobiliųjų įrenginių valdymo komandas	**Aprašymas:** Administratorius prisijungęs prie administravimo sąsajos turi galimybę mobiliuosiuose įrenginiuose įvykdyti nuotolines valdymo komandas. Jis gali atlikti dvi komandas: užrakinti įrenginį arba išvalyti jo atmintį. Šios komandos gali būti vykdomos tik tuo atveju jeigu darbuotojas kliento programinei įrangai suteikiama atitinkamas teises.
Aktorius: administratorius	
Susiję PA: • Užrakinti įrenginį; • Išvalyti įrenginio atmintį;	
Panaudos atvejis:	Užrakinti įrenginį
Tikslas: užrakinti mobilųjį įrenginį nuotoliniu būdu	**Aprašymas:** Administratoriui įvykdžius užrakinimo komandą, mobilusis įrenginys yra užrakinamas ir norint juo naudotis reikia iš naujo suvesti atrakinimo slaptažodį.
Aktorius: administratorius	
Susiję PA: • Valdyti mobiliuosius įrenginius;	
Panaudos atvejis:	Išvalyti įrenginio atmintį
Tikslas: išvalyti visus įrenginyje esančius įmonės duomenis	**Aprašymas:** Administratoriui įvykdžius atminties išvalymo komandą, mobiliajame įrenginyje yra ištrinami visi duomenys ir nustatomi gamykliniai nustatymai.
Aktorius: administratorius	
Susiję PA: • Valdyti mobiliuosius įrenginius;	

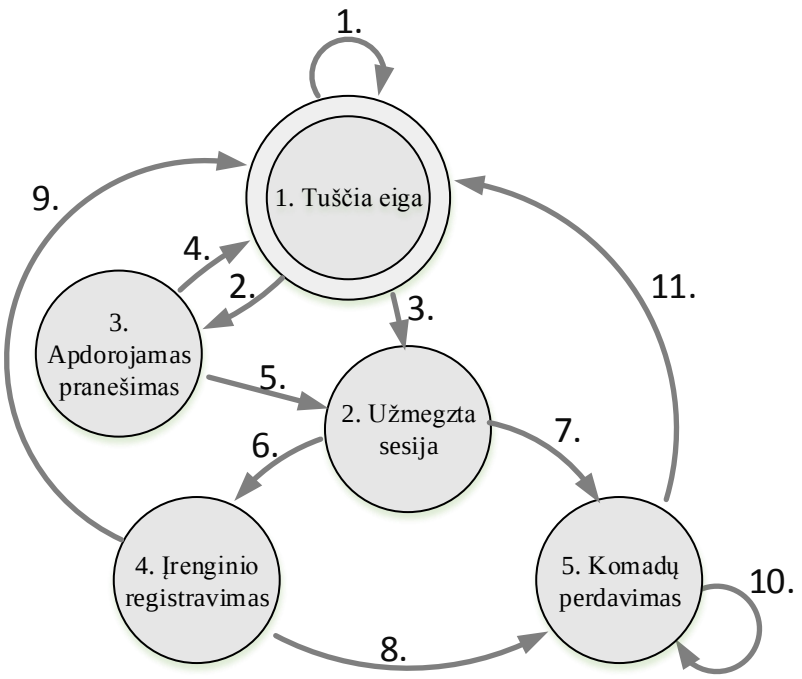


3.11 pav. Mobiliojo įrenginio būsenų diagrama

3.11 pav. matome, kad kliento programinė įranga gali būti vienoje iš 4 būsenų. Pirmoji ir paskutinė būsena – „įrenginys neregistruotas“. Šioje būsenoje įrenginys būna tuo metu kai jis nėra užregistruotas sistemoje ir negali prieiti prie įmonės duomenų bei informacinių resursų. Perėjimai tarp būsenų yra aprašomi 3.14 lentelėje.

3.14 lentelė Mobiliojo įrenginio būsenų diagrama

Pokyčio nr.	Pradinė būsena	Pokytis	Sekanti būsena	Rezultatas
1.	**Įrenginys neregistruotas**	Įrenginio užregistruoti nepavyko.	Įrenginys neregistruotas	Parodomas pranešimas apie įvykusią klaidą.
2.		Įrenginys užregistruotas sėkmingai	Įrenginio saugumo būsena nenustatyta.	Inicijuojamas saugumo politikų atnaujinimas.
3.	**Įrenginio saugumo būsena nenustatyta.**	Patikrintos įrenginio konfigūracijos, jos atitinka saugumo politiką.	Įrenginys saugus	Galimas darbas su įrenginiu.
4.		Patikrintos įrenginio konfigūracijos, jos neatitinka saugumo politiką.	Įrenginys nesaugus	Informuojamas vartotojas, darbas su įrenginius negalimas.
5.	**Įrenginys nesaugus**	Pasikeitė įrenginio konfigūracijos, jos atitinka saugumo politiką.	Įrenginys saugus	Galimas darbas su įrenginiu.
6.		Įrenginys išregistruojamas iš sistemos.	Įrenginys neregistruotas	Darbas su įrenginiu baigtas.
7.	**Įrenginys saugus**	Pasikeitė įrenginio konfigūracijos, jos neatitinka saugumo politiką.	Įrenginys nesaugus	Informuojamas vartotojas, darbas su įrenginius negalimas.
8.		Įrenginys išregistruojamas iš sistemos.	Įrenginys neregistruotas	Darbas su įrenginiu baigtas.



3.12 pav. Serverio būsenų diagrama.

3.12 pav. matome, kad serverio programinė įranga gali būti vienoje iš 5 būsenų. Pirmoji ir paskutinė būsena – „tuščia eiga“. Šioje būsenoje serveris būna tuo metu kai į jį dar nesikreipė klientas ir jis neapdoroja jokių užklausų. Perėjimai tarp serverio būsenų yra aprašomi 3.15 lentelėje.

3.15 lentelė Serverio būsenų perėjimai

Pokyčio nr.	Dabartinė būsena	Pokytis	Sekanti būsena	Rezultatas
1.	**Tuščia eiga**	-	Tuščia eiga	-
2.		Gaunamas pranešimas iš kliento apie jo būsenos pokytį	Apdorojamas pranešimas	Identifikuojamas pranešimą siunčiantis įrenginys ir pranešimas įrašomas į duomenų bazę
3.		Įrenginys bando sudaryti sesiją	Užmegzta sesija	Autentifikuotas ir identifikuotas įrenginys, sudaryta sesija.
4.	**Apdorojamas pranešimas**	Sesija nesudaroma	Tuščia eiga	-
5.		Sudaroma sesija	Užmegzta sesija	Autentifikuotas ir identifikuotas įrenginys, sudaryta sesija.
6.	**Užmegzta sesija**	Sudaroma sesija su klientu	Įrenginio registravimas	Atliekamas įrenginio registravimas į arba išregistravimas iš sistemos.
7.		Perduodamos konfigūracijų ir valdymo komandos klientui	Komandų perdavimas	Konfigūruojamas ir valdomas mobilusis įrenginys.
8.	**Įrenginio registravimas**	Perduodamos konfigūracijų ir valdymo komandos klientui	Komandų perdavimas	Konfigūruojamas ir valdomas mobilusis įrenginys.
9.		Baigtas įrenginio registravimas	Tuščia eiga	-
10.	**Komandų perdavimas**	Perduodama sekanti konfigūravimo ar valdymo komanda	Komandų perdavimas	Konfigūruojamas ir valdomas mobilusis įrenginys.
11		Uždaroma sesija	Tuščia eiga	-

3.7. Asmeninių įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos prototipas

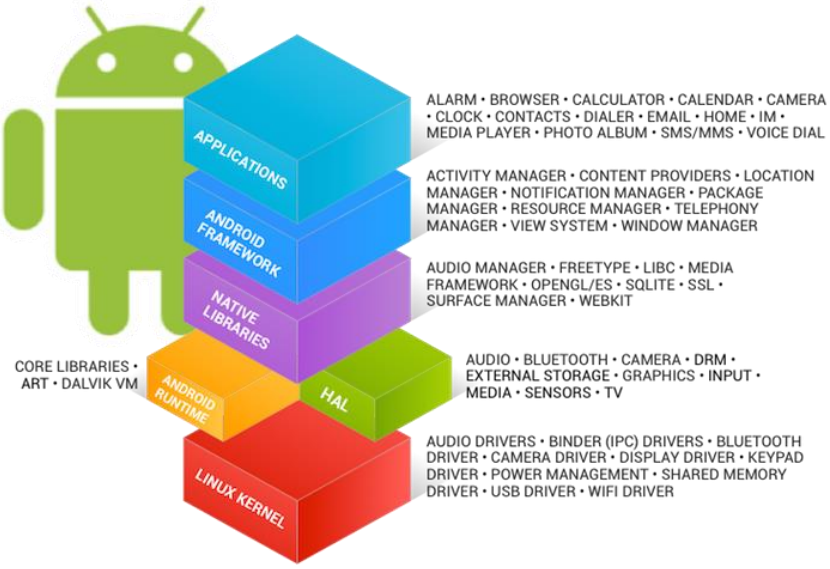
Šiame skyriuje aprašytas asmeninių įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos prototipas. Pateikiama technologijų, kuriomis pasirinkta realizuoti sistemos prototipą apžvalga. Apibrėžiama kokios pasiūlyto sistemos modelio dalys yra realizuotos.

3.7.1. Pasirinktų technologijų apžvalga

Tyrimą nuspręsta atlikti „Android“ operacinės sistemos aplinkoje. Todėl šiai platformai buvo sukurtas kliento programinės įrangos prototipas. Sprendimą įtakojo tai, kad „Android“ nuo 2012 m. yra plačiausiai mobiliuosiuose įrenginiuose naudojama operacinė sistema. Taip pat ši platforma yra atvirojo kodo ir nemokama [17].

„Android“ – tai „Google“ kompanijos vystoma mobiliųjų įrenginių operacinė sistema. Ši sistema sukurta remiantis atvirojo kodo „Linux“ operacinės sistemos pagrindu. Operacinėje sistemoje yra naudojama tiesioginio manipuliavimo grafinė vartotojo sąsaja. Ji leidžia vartotojui įrenginį valdyti gestais: liečiant, braukiant ar spaudžiant ekraną bei naudojantis virtualia klaviatūra. Taip pat vartotojas naudodamasis gestais gali tiesiogiai valdyti programinės įrangos elementus ar objektus, jam nereikia papildomų įrenginių tokių kaip klaviatūra ar kompiuterinė pelė. Tai sukuria natūralią ir intuityvią vartotojo sąsają. Ši operacinė sistema yra pritaikytą įrenginiams su lietimui jautriais ekranais: mobiliesiems telefonams ar planšetiniams kompiuteriams, tačiau gali būti naudojama ir kitur: televizoriuose, automobilių borto kompiuteriuose ar išmaniuosiuose laikrodžiuose.

Programinė įranga naudojama „Android“ operacinėje sistemoje yra kuriama „Java“ programavimo kalba, naudojantis „Android“ programinės įrangos kūrimo įrankių rinkiniu (*angl. Android software development kit*). Šis įrankių rinkinys susideda iš: derinimo programos (*angl. Debugger*), programinės įrangos bibliotekų, „Android“ įrenginių emuliatoriaus, dokumentacijos, programinio kodo pavyzdžių ir pamokų. „Android“ operacinės sistemos architektūra yra pateikiama 3.13 pav. Programinė įranga „Android“ mobiliesiems įrenginiams yra platinama per „Google play“ mobilią parduotuvę.

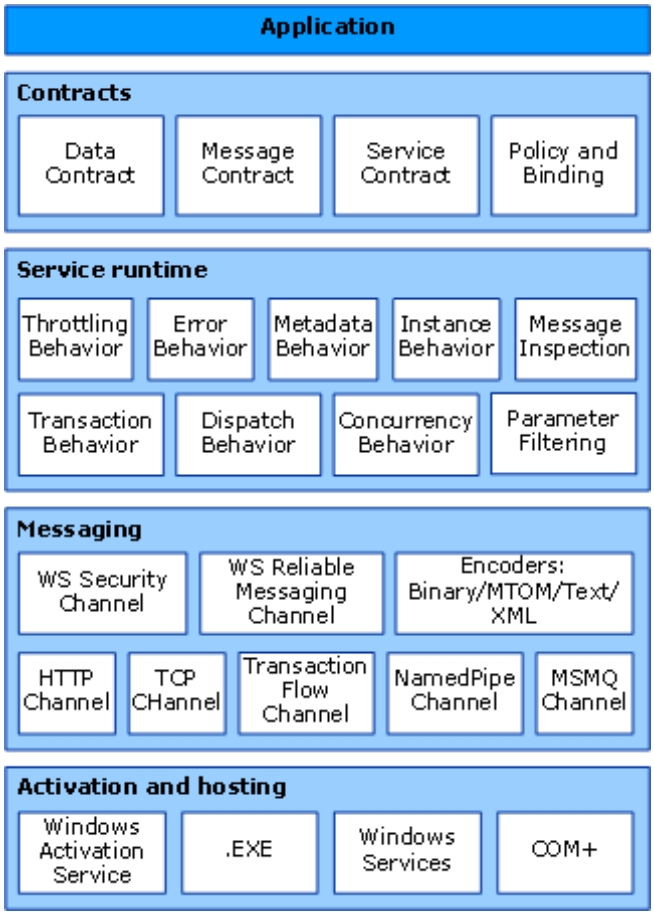


3.13 pav. „Android" operacinės sistemos architektūra [20]

„Android“ operacinei sistemai skirtos kliento mobiliosios programėlės kūrimui buvo naudota „Android Studio“ programinė įranga. „Android Studio“ – tai oficiali, nemokama integruota kūrimo

aplinka (*angl. Integrated development environment*) skirta programinės įrangos „Android“ mobiliajai platformai kūrimui.

Serveryje sistemos žiniatinklio paslaugoms teikti buvo pasirinkta naudoti „Windows Communication Foundation“ (WCF) technologiją, kuri yra „.NET“ programinio karkaso (*angl. Framework*) dalis. Ji susideda iš veikimo aplinkos (*angl. Runtime*) ir rinkinio taikomųjų programų sąsajų (*angl. Application programmin interface API*). WCF architektūra yra pateikiama 3.14 pav.



3.14 pav. WCF architektūra [21]

WCF – tai įrankis, kuris yra dažniausiai naudojamas žiniatinklio paslaugų kūrimui ir diegimui. Ši technologija yra suprojektuota naudojantis žiniatinklio paslaugų architektūros principais, naudoja paskirstytuosius skaičiavimus ir yra orientuota į paslaugų, kurios turi nutolusius vartotojus kūrimą. Vartotojai vienu metu gali naudotis keletu tokių žiniatinklio paslaugų, taip pat viena žiniatinklio paslauga gali būti naudojama kelėtos vartotojų vienu metu. Šia technologija sukurtos žiniatinklio paslaugos dažniausiai turi WSDL (*angl. Web Services Description Language*) kontraktus, kuriuos naudodamas bet kuris WCF klientas gali pasiekti tą paslaugą, nepriklausomai nuo to kokioje platformoje ji yra talpinama. WCF naudoja daugelį žiniatinklio paslaugų standartų, tokius kaip: ŽP-adresavimas, ŽP-patikimi pranešimai ar ŽP-sauga. Nuo 4-osios „.NET“ versijos WCF taip pat naudoja RSS sindikavimo paslaugas (*angl. Syndication Services*), ŽP-aptikimą, maršrutizavimą ir geriau palaiko „REST“ žiniatinklio paslaugas.

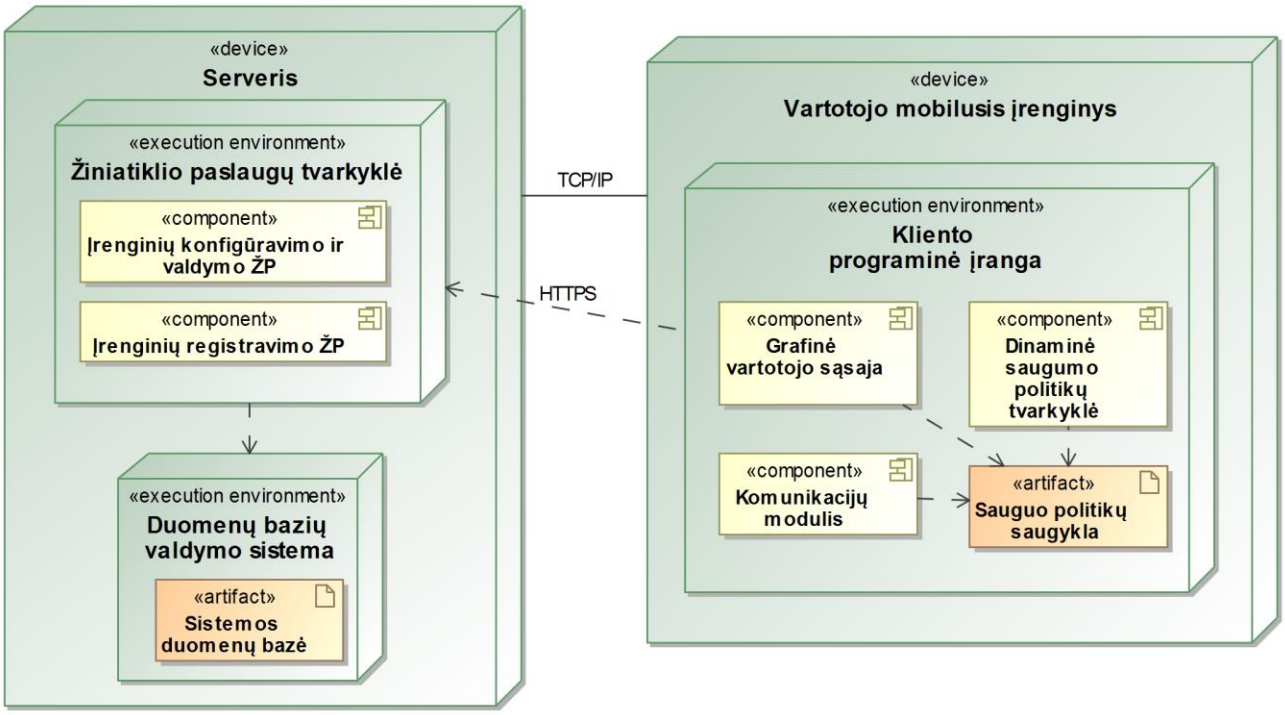
Žiniatinklio paslaugų realizavimui buvo pasirinkta naudoti „Microsoft Visual Studio 2013 Community“ integruotą kūrimo aplinką. Tai nemokama programinė įranga skirta kompiuterinių programų, interneto puslapių ir žiniatinklio paslaugų kūrimui Windows platformai.

3.7.2. Saugaus konfigūravimo paramos sistemos prototipo struktūra

Tyrimo tikslams įgyvendinti sukurtas mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos prototipas. Prototipo struktūra yra pateikiama 3.15 pav. Prototipas susideda iš kliento programinės įrangos ir sistemos žiniatinklio paslaugų apibrėžtų pateiktame sistemos modelyje.

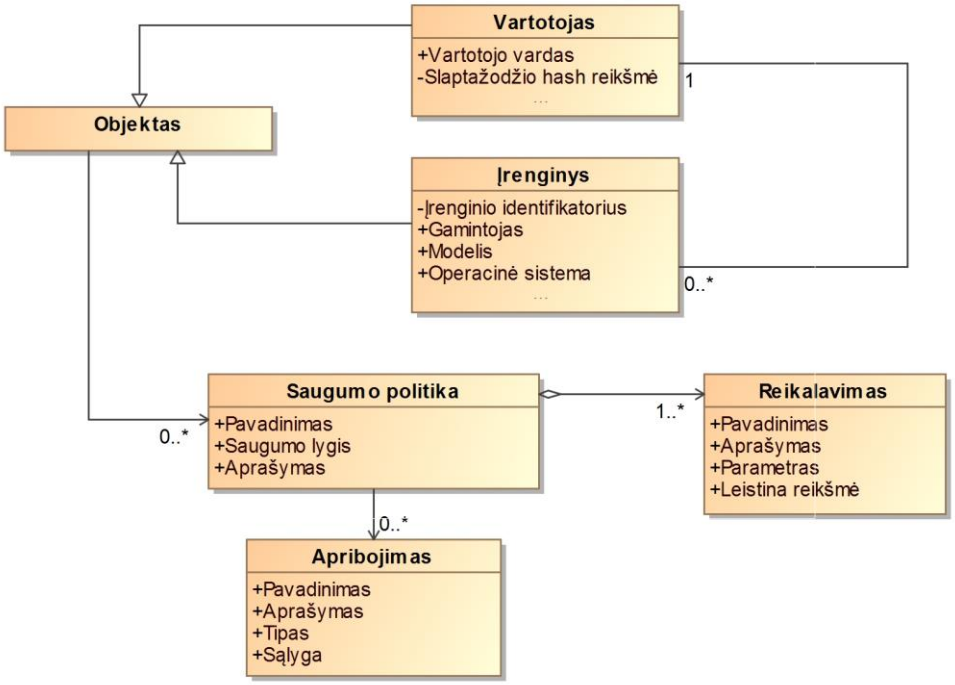
Kliento programinėje įrangoje realizuota vartotojo grafinė sąsaja, komunikacijų modulis, saugumo politikų saugykla ir dinaminė saugumo politikų tvarkyklė. Realizuoti programinės įrangos komponentai yra skirti informacijos apie įrenginį atvaizdavimui, saugumo politikų parsisiuntimui iš serverio, naudojantis žiniatinklio paslaugomis, ir jų pritaikymui įrenginyje. Kliento programinė įranga buvo realizuota „Android“ mobiliųjų įrenginių platformoje.

Sistemos serveryje realizuotos įrenginių konfigūravimo ir valdymo bei registravimo žiniatinklio paslaugos. Pirmoji paslauga skirta saugumo politikų ir valdymo komandų perdavimui iš serverio klientui. Naudojantis antrąja paslauga įrenginiai yra užregistruojami administravimui. Žiniatinklio paslaugos buvo realizuotos naudojantis „Windows Communication Foundation“ technologijomis. Duomenų perdavimui prototipas gali naudoti HTTP ir HTTPS transporto lygmens protokolus bei JSON arba SOAP pranešimų formatus.



3.15 pav. SKP sistemos prototipo struktūra (UML notacija)

3.7.3. Saugaus konfigūravimo paramos sistemos prototipo koncepcinis duomenų modelis



3.16 pav. Sistemos prototipo koncepcinis duomenų modelis (UML notacija)

Koncepcinis mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos prototipo duomenų modelis yra pateiktas 3.16 pav. Šiame modelyje galime matyti, kad sistemos prototipe yra realizuotos šios duomenų esybės: vartotojas, įrenginys, saugumo politikos, reikalavimai ir konfigūracijos.

Saugumo politikos sistemoje yra apibrėžiamos kaip reikalavimų ir apribojimų rinkinys. Jos turi vienkrypčius ryšius tiek su reikalavimų, tiek su apribojimų duomenų esybėmis. Saugumo politikos negali egzistuoti be jokių reikalavimų. Apribojimai nurodo kokioms sąlygoms esant saugumo politika yra aktyvi. Taip pat saugumo politika turi saugumo lygio atributą. Pagal šį atributą kliento programinė įranga nustato kurią iš kelių įrenginyje esančių aktyvių saugumo politikų pritaikyti. Pritaikoma yra ta saugumo politika kuri turi aukščiausią saugumo lygį.

Modelyje matome, kad saugumo politikos sistemoje gali būti priskiriamos tiek sistemos vartotojams tiek atskiriems jų įrenginiams. Priskyrus saugumo politiką vartotojui, ji yra pritaikoma visuose to vartotojo mobiliuosiuose įrenginiuose.

3.7.4. Saugaus konfigūravimo paramos sistemos kliento programinės įrangos prototipas

a) b) c)

d) e)

3.17 pav. Sistemos grafinės vartotojo sąsajos prototipas

Sistemos kliento programinės įrangos prototipas buvo realizuotas kaip „Android“ platformai skirta mobilioji programėlė. Šioje programėlėje yra naudojamas skilčių navigacijos metodas. Programėlėje yra penki langai (žr. 3.17 pav.): įrenginio registravimo (a), įrenginio informacijos (b), saugumo politikų (c), nustatymų (d) ir testavimo langai (e). Langų viršuje (išskyrus įrenginių registravimo langą) visą laiką matome šiuo metu įrenginyje aktyvuotos saugumo politikos pavadinimą ir statusą, t.y. ar įrenginys atitinka saugumo politiką ar ne.

Visų pirma pasileidus mobiliąją programėlę yra atidaromas įrenginio registravimo langas. Šiame lange mobiliojo įrenginio naudotojas privalo pateikti savo autentifikavimosi informaciją (vartotojo vardą ir slaptažodį) ir gali atlikti įrenginio registravimo sistemoje funkciją. Įvykus

sėkmingai įrenginio registracijai yra atidaromas įrenginio informacijos langas. Nesėkmingos įrenginio registracijos atveju vartotojui parodomas klaidos pranešimas.

Įrenginio informacijos lange vartotojui yra pateikiama visa pagrindinė įrenginio informacija. Programėlėje matoma įrenginio informacija yra pateikiama 3.16 lentelėje.

Antrojoje programėlės skiltyje „politikos“ yra atvaizduojamos įrenginiui priskirtos saugumo politikos (politikos pavadinimas, apribojimai ir reikalavimai). Įrenginys vienu metu gali turėti kelias jam priskirtas saugumo politikas. Aktyviomis yra tik tos saugumo politikos, kurių visi apribojimai yra patenkinti. Jeigu įrenginyje vienu metu yra kelios aktyvios saugumo politikos, tuomet jame yra pritaikoma aukščiausią saugumo lygi turinti aktyvi politika. Vienu metu įrenginyje gali būti pritaikoma tik viena saugumo politika. Šiuo metu įrenginyje pritaikyta saugumo politika yra pažymėta varnelės piktograma. Kai kurie saugumo politikoje keliami reikalavimai, kurių pavadinimas arba reikšmė yra nepakankamai informatyvūs, gali turėti papildomą aprašymą. Šią informaciją galima prieiti paspaudus ant atitinkamo saugumo politikos elemento.

Ketvirtajame programėlės lange yra pateikiami nustatymai. Šiame lange vartotojas gali įjungti arba išjungti automatinį įrenginio konfigūravimą bei atlikti įrenginio išregistravimo funkciją.

Paskutinis programėlės langas yra skirtas sistemos eksperimentinio tyrimo atlikimui. Naudojantis šiuo langu galima atlikti įvairias užklausas į serverį. Galima nustatyti šiuos atliekamų užklausų parametrus: perduodamų pranešimų formatą, transporto lygmens protokolą ir saugą, bandomojo vartotojo identifikatorių, užklausų atlikimo dažnį bei iteracijų skaičių. Lango apačioje yra eksperimento progresą atvaizduojanti juosta.

3.16 lentelė Mobiliojoje programėlėje pateikiama įrenginio informacija

Parametras	Apibūdinimas
Gamintojas	Įmonės pagaminusios įrenginį pavadinimas.
Modelis	Įrenginio modelio pavadinimas.
Android versija	Android operacinės sistemos versija.
Serijinis numeris	Įrenginio serijinis numeris.
Įrenginio identifikatorius	Unikali 16 šešioliktainio formato simbolių eilutė, kuri skirta įrenginių identifikavimui.
Mobiliojo ryšio operatorius	Mobiliojo ryšio operatoriaus pavadinimas.
MNC	Mobiliojo ryšio tinklo numeris.
MCC	Mobiliojo ryšio šalies numeris.
IMEI	Tarptautinis mobiliojo ryšio įrangos numeris.
Tarptautinių skambučių informacija	Informacija ar šiuo metu įrenginyje yra įjungta tarptautinių skambučių paslauga.
Paketinis duomenų perdavimas	Informacija ar šiuo metu įrenginyje yra įjungtas paketinis duomenų perdavimas.
Paketinių duomenų perdavimas užsienyje	Informacija ar šiuo metu įrenginyje yra įjungta tarptautinė paketinių duomenų perdavimo paslauga.
Radijo ryšio technologija	Šiuo metu veikianti radijo ryšio technologija.
SSID	Wi-fi tinklo, prie kurio šiuo metu yra prisijungęs įrenginys, pavadinimas.
IP adresas	Šiuo metu įrenginiui priskirtas IP adresas.
Wifi saugos protokolas	Wi-fi tinkle, prie kurio šiuo metu yra prisijungęs įrenginys, naudojamas saugos protokolas.
MAC adresas	Įrenginio MAC adresas.
Bluetooth būsena	Parodo ar įrenginyje yra įjungtos Bluetooth technologijos.
NFC būsena	Parodo ar įrenginyje yra įjungtos NFC technologijos.
Kamera	Parodo ar įrenginyje esanti kamera yra blokuojama.
Šifravimas	Parodo ar įrenginyje yra įjungtas šifravimas.
Slaptažodis įjungtas	Parodo ar įrenginyje yra įjungtas slaptažodis.

3.8. Išvados

1. Pasiūlytas asmeninių mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos modelis skirtas centralizuotam įmonės darbuotojų asmeninių mobiliųjų įrenginių konfigūracijų valdymui ir būklės stebėjimui.
2. SKP sistemos modelis leidžia ne tik stebėti ir įvertinti asmeninių įrenginių saugumo būseną, bet ir esant reikalui pakeisti įrenginio konfigūracijas taip, kad jos atitiktų jam priskirtą saugumo politiką.
3. Modelio ir jo pagrindu realizuotos paramos sistemos prototipo pagrindiniai bruožai paprastumas (klientas – serveris architektūra), dinaminis saugumo politikų profiliavimas ir orientacija į įmonės darbuotojų asmeninius mobiliuosius įrenginius.
4. Remiantis saugaus konfigūravimo paramos sistemos modeliu realizuotas sistemos prototipas, kuris yra skirtas Android platformos pagrindu veikiantiems mobiliesiems įrenginiams.

4. ASMENINIŲ ĮRENGINIŲ, NAUDOJAMŲ ĮMONĖSE, SAUGAUS KONFIGŪRAVIMO PARAMOS SISTEMOS EKSPERIMENTINIS TYRIMAS

Naudojantis 3-iame skyriuje „Asmeninių įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos prototipas“ aprašytu sistemos prototipu buvo atliktas tyrimas. Tyrimo metu naudota techninė įranga:

- Nešiojamasis kompiuteris „DELL Inspiron 17R SE“;
- Nešiojamasis kompiuteris „MacBook Pro“;
- Mobilusis įrenginys „Samsung Galaxy S2“;
- Maršrutizatorius ir Wi-fi prieigos stotelė „D-Link DR-615“.

Detali techninės įrangos specifikacija yra pateikiama 4.1 lentelėje.

Tyrimui naudojama programinė įranga:

- Microsoft Visual Studio 2013 Community;
- Android studio;
- Android SDK;
- SoapUI.

4.1 lentelė Tyrime naudos techninės įrangos detali specifikacija

Nešiojamasis kompiuteris „DELL Inspiron 17R SE“	
Procesorius	Intel Core i7-3630QM, 2,40 GHz
Operatyvioji atmintis	8 GB
Kietasis diskas	Intel SSD, 120 GB
Grafinė plokštė	NVIDIA GeForce GT 650M, 2 GB
Tinklo plokštė	Intel Centrino Wireless-N 2230, a/b/g/n
Operacinė sistema	Windows 7 64-bit
Nešiojamasis kompiuteris „MacBook Pro“	
Procesorius	Intel Core i5, 2,60 GHz
Operatyvioji atmintis	8 GB
Kietasis diskas	Apple SSD, 120 GB
Grafinė plokštė	Intel Iris Graphics 6100, 1,5 GB
Tinklo plokštė	AirPort, a/b/g/n
Operacinė sistema	Mac OS X Yosemite
Mobilusis įrenginys „Samsung Galaxy S2“	
Procesorius	Dual-core 1.2 GHz Cortex-A9
Operatyvioji atmintis	1 GB
Vidinė atmintis	16 GB
Tinklo plokštė	Wi-Fi 802.11 a/b/g/n, dual-band
Operacinė sistema	Android 4.1.2 (Jellybean)
Maršrutizatorius ir Wi-fi prieigos stotelė „D-Link DR-615“	
Standartas	Wi-Fi 802.11 b/g/n
Perdavimo greitis	300 Mb/s
Dažnių juosta	2,4 GHz
Apsaugos protokolas	WPA2

Eksperimentams atlikti buvo naudojamos etaloninės mobiliojo įrenginio saugumo politikos, kurios yra pateikiamos 2 priede.

4.1. Žiniatinklio paslaugų transporto lygmens konfigūracijų tyrimas

4.1 pav. Pirmajame eksperimente naudoto tinklo schema

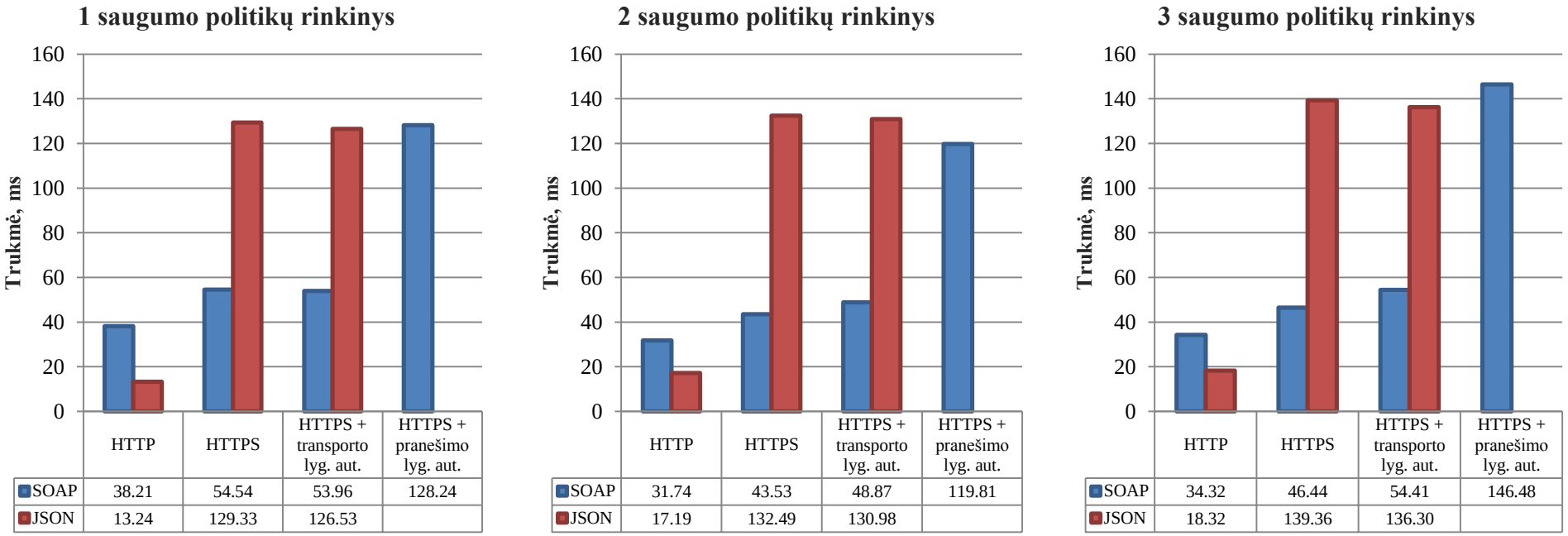
Pirmojo eksperimento metu buvo tiriama transporto lygmens protokolų ir pranešimų formatų naudojimo įtaka atliekamų užklausų greitaveikai. Tyrimas atliekamas naudojant etaloninius saugumo politikų rinkinius. Jo metu naudoti skirtingo dydžio saugumo politikų rinkiniai pateikti 4.2 lentelėje. Mobilusis įrenginys prie serverio (nešiojamojo kompiuterio) jungiasi bevieliu ryšiu. Šiam tikslui naudojama bevielės prieigos stotelė. Tyrimo metu naudoto tinklo schema pateikiama 4.1 pav.. Eksperimento metu iš mobiliojo įrenginio yra atliekamos užklausos į serverį ir matuojami jų įvykdymo laikai. Kiekviename eksperimento etape atliekama po 400 užklausų naudojant skirtingas serverio ir kliento programinės įrangos konfigūracijas. Šios konfigūracijos pateiktos 4.3 lentelėje. Matavimų rezultatai rašomi į tekstinius failus ir vėliau apdorojami kompiuteriu. Tyrimo rezultatai pateikiami grafikų pavidalu (žr. 4.2 pav.– 4.5 pav.).

4.2 lentelė Saugumo politikų rinkinių, naudotų tyrime, parametrai

Rinkinio nr.	Saugumo politikų skaičius	Pranešimo dydis (JSON formatu)	Pranešimo dydis (SOAP formatu)
1.	1	1,12 kB	2,29 kB
2.	3	2,42 kB	4,33 kB
3.	5	4,67 kB	7,88 kB

4.3 lentelė Eksperimentų metu naudotos žiniatinklio paslaugų konfigūracijos

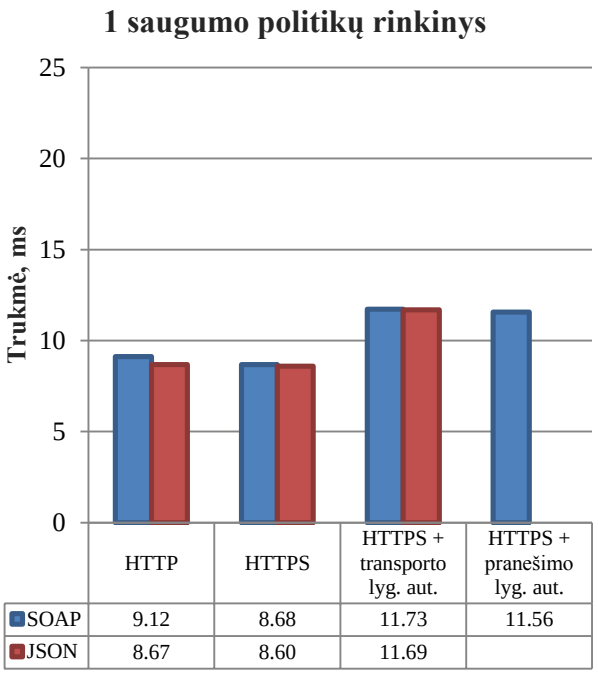
Eksperimento nr.	1.	2.	3.	4.	5.	6.	7.
Transporto protokolas	HTTP	HTTPS	HTTPS	HTTP	HTTPS	HTTPS	HTTPS
Pranešimų formatas	JSON	JSON	JSON	SOAP	SOAP	SOAP	SOAP
Autentifikavimas	-	-	Transporto lygmens	-	-	Transporto lygmens	Pranešimo lygmens

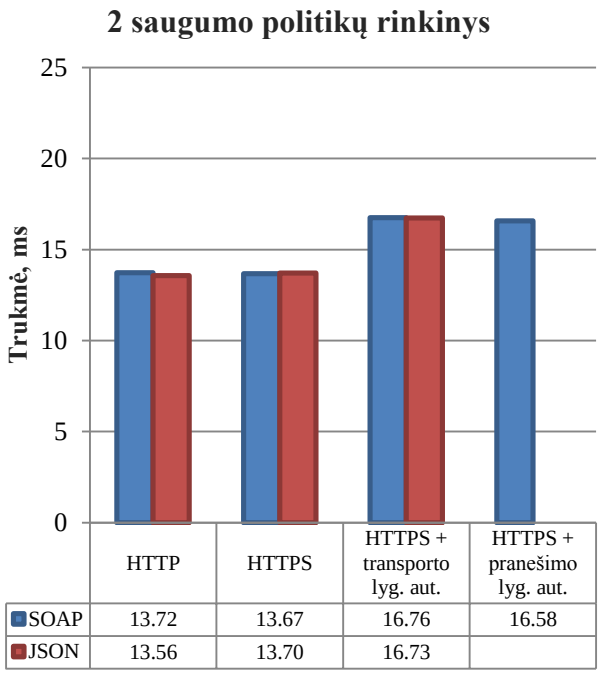


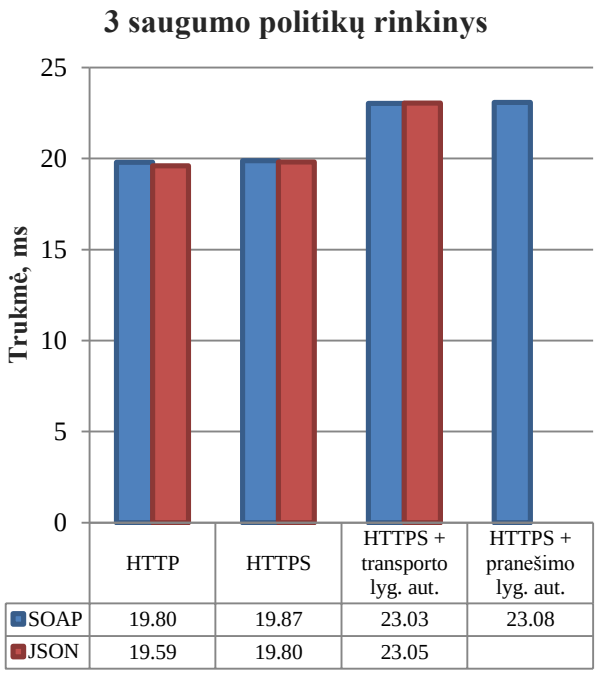
4.2 pav. Užklausų perdavimo tinklu vidutinių trukmių priklausomybė nuo skirtingo perduodamų duomenų kiekio ir žiniatinklio paslaugų konfigūracijų

4.2 pav. yra pateiktos vidutinės pranešimų perdavimo tinklu trukmės esant skirtingiems transporto lygmens protokolų parametrams ir duomenų perdavimo formatams. Kaip matosi iš grafikų didėjant saugumo politikų skaičiui pranešimų perdavimo tinklu trukmės taip pat didėja, tačiau šis pokytis nėra žymus. Didesnę įtaką pranešimų perdavimo tinklu trukmei turi transporto lygmens protokolų konfigūracijos ir perduodamų pranešimų formatas. Iš grafikų matome, kad:

- Tinklu pranešimai greičiausiai perduodami HTTP protokolu, SOAP pranešimai per 31,74 – 38,21 ms, o JSON per 13,24 – 18,32 ms, tačiau šis protokolas nenaudoja jokių saugos priemonių, todėl yra netinkamas naudoti sistemoje;
- SOAP formato pranešimai tinklu lėčiausiai perduodami naudojant HTTPS protokolą su pranešimų lygmens autentifikavimu, pranešimai perduodami per 119,81 – 146,48 ms, tai vidutiniškai 3 kartus lėčiau negu naudojant kitas konfigūracijas;
- Įjungus HTTPS protokolą, pranešimai su JSON duomenimis tinklu yra perduodami žymiai lėčiau, trukmės vidutiniškai padidėja netgi 8 kartus.



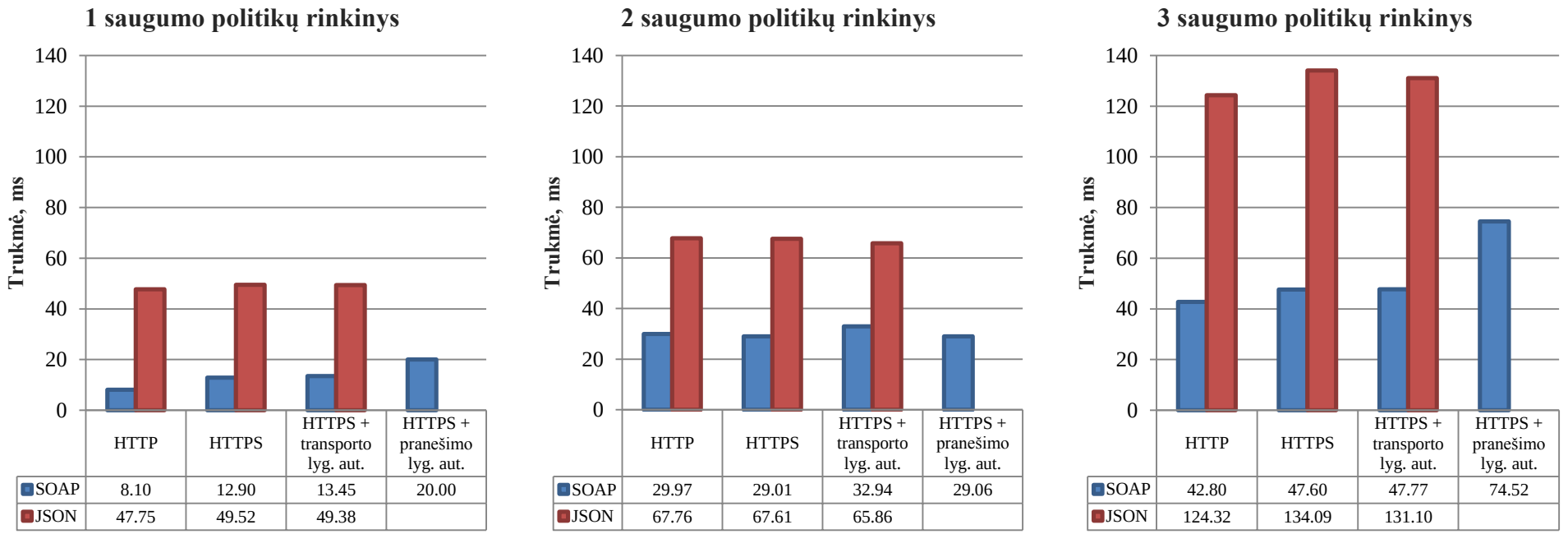




4.3 pav. Užklausų apdorojimo serveryje vidutinių trukmių priklausomybė nuo skirtingo perduodamų duomenų kiekio ir žiniatinklio paslaugų konfigūracijų

Tyrimo metu buvo išmatuota kokiu greičiu serveris apdoroja užklausas (žr. 4.3 pav.). Iš grafikų matome, kad:

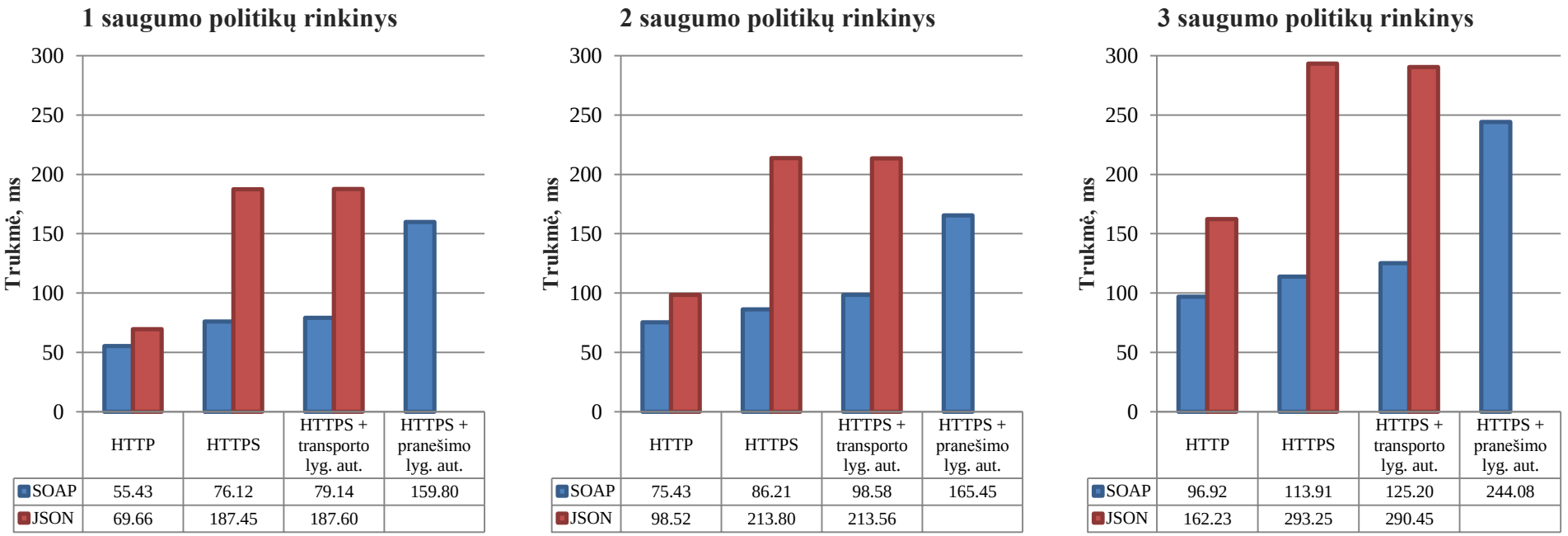
- Didėjant pranešimais perduodamų duomenų kiekiui (skirtingas saugumo politikų skaičius) užklausų apdorojimo trukmė serveryje proporcingai didėja, o šis pokytis nepriklauso nuo naudojamų protokolų ir pranešimų formatų;
- Užklausų apdorojimo trukmė yra beveik tokia pati naudojant tiek JSON, tiek SOAP pranešimų formatus, vidutinis skirtumas 1,0 %;
- Transporto lygmens protokolai užklausų apdorojimo trukmei įtakos neturi;
- Naudojant pranešimų autentifikavimą užklausų apdorojimas serveryje padidėja vidutiniškai 3,07 ms.



4.4 pav. Atsakymų apdorojimo kliente vidutinių trukmių priklausomybė nuo skirtingo perduodamų duomenų kiekio ir žiniatinklio paslaugų konfigūracijų

Eksperimento metu buvo matuojamos ir iš serverio gautų atsakymų apdorojimo trukmės mobiliajame įrenginyje (žr. 4.4 pav.) Išanalizavus rezultatus nustatyta, kad:

- Didėjant pranešimais perduodamų duomenų kiekiui (skirtingas saugumo politikų skaičius) atsakymų apdorojimo trukmė mobiliajame įrenginyje didėja proporcingai pranešimu perduodamų duomenų kiekiui;
- Naudojant SOAP pranešimų formatą, atsakymai mobiliajame įrenginyje yra apdorojamos žymiai greičiau, negu naudojant JSON formatą, apdorojimo trukmės vidutiniškai skiriasi 2,8 karto;
- Transporto lygmens protokolų konfigūracijos turi nedidelę įtaką atsakymų apdorojimo trukmei, didinant saugos priemonių kiekį atsakymų apdorojimo laikas didėja, tačiau šis pokytis nėra toks didelis kaip naudojant skirtingus pranešimų formatus.



4.5 pav. Vidutinių užklausų atlikimo trukmių priklausomybė nuo skirtingo perduodamų duomenų kiekio ir žiniatinklio paslaugų konfigūracijų

Sudėjus pranešimo perdavimo tinklu, jo apdorojimo serveryje ir atsakymo apdorojimo mobiliajame įrenginyje laikus buvo gauta bendra užklausos į serverį atlikimo trukmė (žr. 4.5 pav.). Pagal gautus rezultatus matome, kad:

- Didėjant perduodamų saugumo politikų kiekiui atliekamų užklausų trukmė taip pat proporcingai didėja;
- Greičiausiai užklausos atliekamos naudojant HTTP protokolą, lėčiausiai – HTTPS su pranešimų autentifikavimu;
- Naudojant HTTP protokolą ir SOAP perduodamų pranešimų formatą, užklausos yra atliekamos vidutiniškai 28 % greičiau negu naudojant JSON pranešimų formatą. Naudojant HTTPS protokolą SOAP pranešimai yra perduodami vidutiniškai 2,4 karto greičiau negu JSON.

Pagal gautus rezultatus nustatyta, kad užklausos greičiausiai atliekamos naudojant HTTP protokolą, tačiau jis nėra saugus ir dėl to netinka būti naudojamas sistemoje. Dėl šios priežasties sistemoje siūloma naudoti saugų HTTPS duomenų perdavimo protokolą. Klientų autentifikavimui siūloma pasirinkti transporto lygmens autentifikavimą, kuris yra greitesnis už pranešimo lygmens autentifikavimą. Atsižvelgiant į sistemos greitaveiką duomenų perdavimui patartina naudoti SOAP pranešimų formatą, tačiau norint sumažinti tinklu perduodamų duomenų kiekį (skirtumas apytiksliai du kartai) galima naudoti ir JSON duomenų perdavimo formatą.

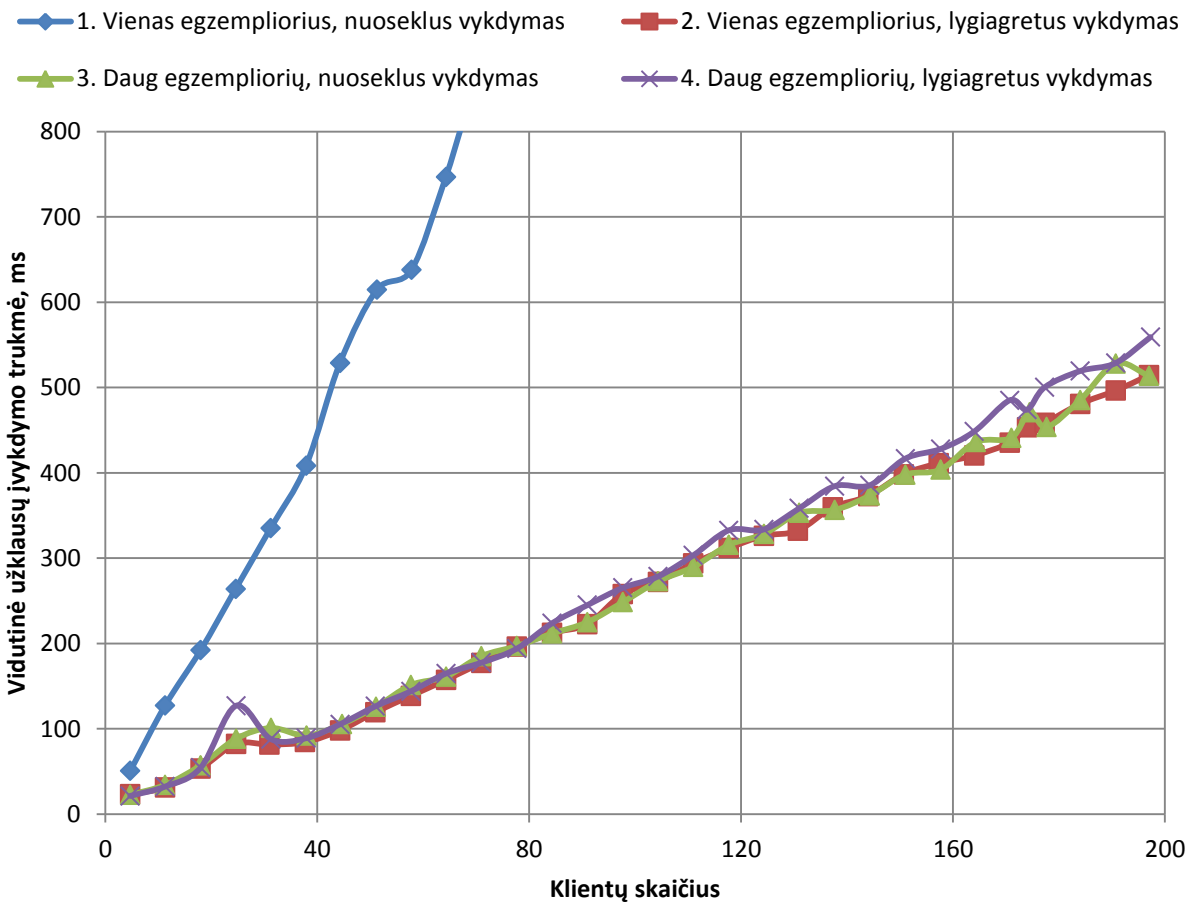
4.2. Žiniatinklio paslaugų egzempliorių ir lygiagretaus vykdymo rėžimų tyrimas

4.6 pav. Antrajame eksperimente naudoto tinklo schema.

Antrojo eksperimento metu buvo tiriama žiniatinklio paslaugų greitaveikos priklausomybė nuo žiniatinklio paslaugų egzempliorių rėžimo (*angl. Instance Type*) ir lygiagretaus užklausų apdorojimo rėžimo (*angl. Concurrency Type*). Eksperimento metu pasinaudojant programa „SoapUI“ buvo imituojama kintanti daugelio vartotojų (mobiliųjų įrenginių) apkrova (nuo 1 iki 200). Tinklo schema naudota antrajame eksperimente pateikta 4.6 paveikslėlyje. Tyrimas buvo atliekamas naudojant etalonines saugumo politikas. Eksperimento metu iš imituojamų vartotojų mobiliųjų įrenginių į serverį yra atliekamos užklausos ir matuojami jų įvykdymo laikai, aptarnaujamų užklausų per sekundę skaičius bei kiti parametrai. Eksperimentas kartojamas keičiant žiniatinklio paslaugų egzempliorių ir lygiagretaus užklausų apdorojimo rėžimus. Tyrime naudotos žiniatinklio paslaugų konfigūracijos yra pateikiamos 4.4 lentelėje. Gauti matavimų rezultatai rašomi į tekstinius failus ir vėliau apdorojami kompiuteriu. Tyrimo rezultatai pateikiami grafikų pavidalu (žr. 4.7 pav., 4.8 pav.).

4.4 lentelė Eksperimentų metu naudotos žiniatinklio paslaugų konfigūracijos

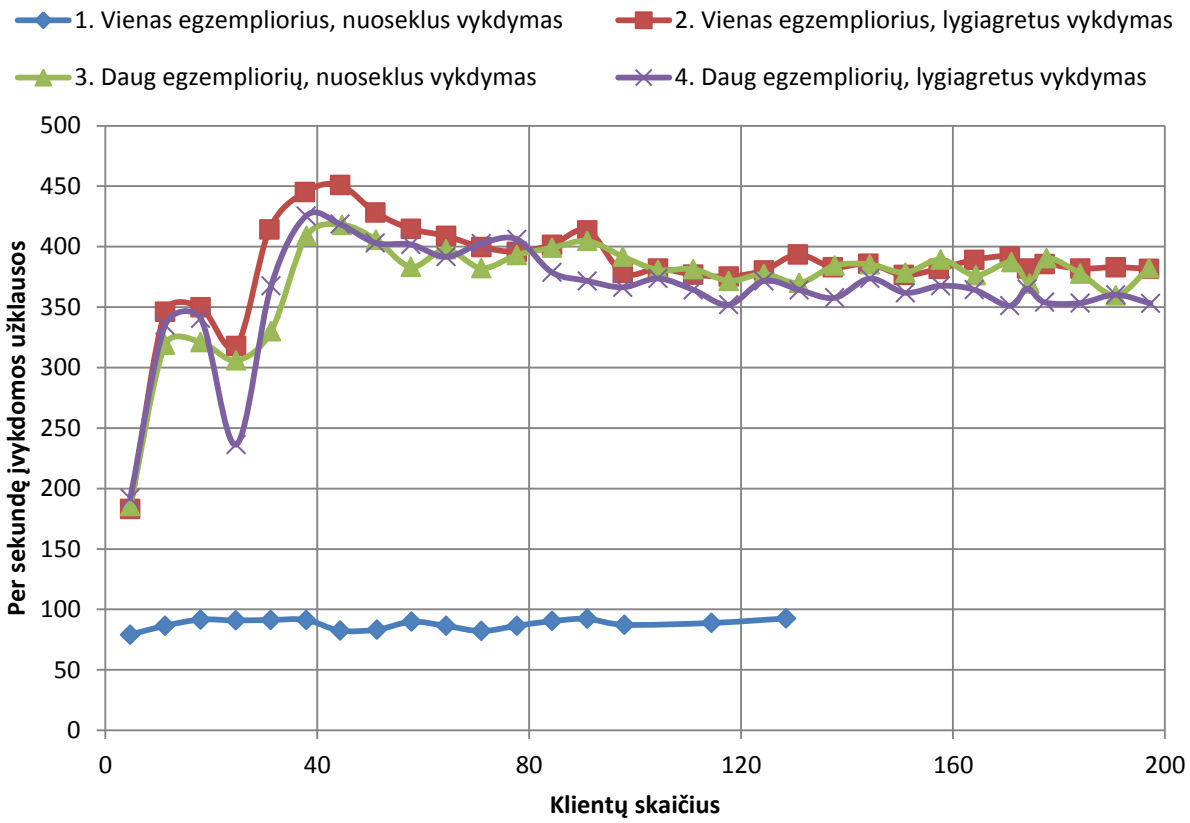
Eksperimento nr.	ŽP lygiagretaus užklausų apdorojimo rėžimas	ŽP egzempliorių rėžimas
1.	Nuoseklus	Vienas egzempliorius visoms užklausoms
2.		Po egzempliorių kiekvienai užklausai
3.	Lygiagretus	Vienas egzempliorius visoms užklausoms
4.		Po egzempliorių kiekvienai užklausai



4.7 pav. Vidutinės užklausų įvykdymo trukmės priklausomybė nuo serverio apkrovos esant įvairiems ŽP egzempliorių ir lygiagretaus užklausų apdorojimo rėžimams

Tyrimo metu buvo išmatuota užklausų įvykdymo vidutinių trukmių priklausomybė nuo sistemos klientų skaičiaus (žr. 4.7 pav.). Pagal gautus rezultatus matome, kad:

- Prasčiausiai pasirodė vieno ŽP egzemplioriaus ir nuoseklaus užklausų apdorojimo konfigūracijų derinys, jis daugiau negu 4 kartus lėtesnis už kitus konfigūracijų derinius.
- Naudojant kitus tris ŽP konfigūracijų derinius gauti labai panašūs rezultatai. Taip yra dėl to, kad visi trys konfigūracijų deriniai užklausų apdorojimui naudoja kelias vykdymo gijas (angl. Multi Thread) vienu metu. Naudojant daugelio ŽP egzempliorių ir nuoseklaus užklausų apdorojimo rėžimus, užklausos taip pat yra apdorojamos skirtingose gijose. Nors ir atrodo, kad tai prieštarauja lygiagretaus ŽP vykdymo konfigūracijai, tačiau taip nėra, nes kiekvienas ŽP egzempliorius yra sukuriamas ir vykdomas atskiroje gijoje. Kadangi kiekvienai užklausai yra sukuriama po naują ŽP egzempliorių, todėl jos visos yra apdorojamos skirtingose gijose [22].
- Iš grafiko matyti, kad greičiausiai ŽP veikia su vieno egzemplioriaus ir lygiagretaus užklausų apdorojimo rėžimų konfigūracijomis. Taip yra dėl to, kad sutaupoma šiek tiek laiko, kuris yra sugaištamas kuriant naujus ŽP egzempliorius.



4.8 pav. Vidutinio užklausų aptarnavimo per sekundę skaičiaus priklausomybė nuo serverio apkrovos ir ŽP konfigūracijų

Eksperimento metų taip pat buvo matuojamas vidutinis aptarnaujamų užklausų per sekundę skaičius (žr. 4.8 pav.). Pagal grafiką matyti, kad:

- Tyrimo pradžioje, iki tam tikros apkrovos (20 vartotojų – pirmajam konfigūracijų deriniui ir 40 vartotojų likusiems konfigūracijų deriniams) aptarnaujamų užklausų skaičius auga. Viršijus šią ribą apdorojamų užklausų skaičius sumažėja ir nusistovi ties pastovia reikšme.
- Skirtingų ŽP konfigūracijų derinių maksimalios užklausų apdorojimo spartos yra:
- Pirmasis derinys: maksimali sparta – 93 užklausos/s, esant didesnėms apkrovoms - 88 užklausos/s.
- Antrasis derinys: maksimali sparta - 451 užklausa/s, esant didesnėms apkrovoms - 383 užklausos/s.
- Trečiasis derinys: maksimali sparta - 418 užklausų/s, esant didesnėms apkrovoms - 380 užklausų/s.
- Ketvirtasis derinys: maksimali užklausų apdorojimo sparta - 425 užklausos/s, esant didesnėms apkrovoms - 362 užklausos/s.

Pagal gautus tyrimo rezultatus nustatyta, kad greičiausiai ŽP veikia naudojant vieno egzemplioriaus ir lygiagretaus užklausų apdorojimo rėžimus, tačiau greičio pranašumas prieš daugelio egzempliorių rėžimą nėra didelis.

4.3. Eksperimentinio tyrimo rezultatų apibendrinimas

- Atliekant pirmąją tyrimo dalį buvo išmatuotos pranešimų perdavimo tinklu, užklausų apdorojimo serveryje, atsakymų apdorojimo mobiliajame įrenginyje ir bendros užklausų atlikimo trukmės esant įvairioms žiniatinklio paslaugų konfigūracijoms;
- Išmatuotos pranešimų perdavimo tinklu trukmės:
  - Tinklu pranešimai greičiausiai perduodami naudojant HTTP protokolą;
  - Naudojant SOAP pranešimų formatą kartu su HTTPS protokolu ir pranešimų lygmens autentifikavimu, pranešimai perduodami per 119,81 – 146,48 ms, tai vidutiniškai 3 kartus lėčiau negu naudojant kitas konfigūracijas;
  - Naudojant JSON duomenų perdavimo formatą matomas ryškus užklausų perdavimo sulėtėjimas įjungus HTTPS protokolą, trukmės vidutiniškai padidėja netgi 8 kartus.
- Išmatavus užklausų apdorojimo serveryje trukmes nustatyta, kad:
  - Didėjant pranešimais perduodamų duomenų kiekiui užklausų apdorojimo trukmė serveryje proporcingai didėja, o šis pokytis nepriklauso nuo naudojamų protokolų ir pranešimų formatų;
  - Užklausų apdorojimo trukmė yra beveik tokia pati tiek naudojant JSON, tiek SOAP pranešimų formatus, vidutinis skirtumas 1,0 %;
  - Transporto lygmens protokolai užklausų apdorojimo trukmei įtakos neturi;
  - Užklausų apdorojimo trukmei įtakos turi pranešimų autentifikavimas, su juo užklausos apdorojamos vidutiniškai 3,07 ms lėčiau.
- Išmatavus atsakymų apdorojimo mobiliajame įrenginyje trukmes nustatyta:
  - Didėjant pranešimais perduodamų duomenų kiekiui, atsakymų apdorojimo trukmė mobiliajame įrenginyje didėja;
  - Naudojant SOAP pranešimų formatą, atsakymai mobiliajame įrenginyje yra apdorojami daug greičiau negu naudojant JSON formatą, apdorojimo trukmės vidutiniškai skiriasi 2,8 karto.
- Apskaičiavus bendras užklausų įvykdymo trukmes nustatyta, kad:
  - Greičiausiai užklausos atliekamos naudojant HTTP protokolą, lėčiausiai – HTTPS su įjungtu autentifikavimu;
  - Naudojant HTTP protokolą ir SOAP perduodamų pranešimų formatą, užklausos yra atliekamos vidutiniškai 28 % greičiau negu naudojant JSON pranešimų formatą. Naudojant HTTPS protokolą SOAP pranešimai yra perduodami vidutiniškai 2,4 karto greičiau negu JSON.
- Išmatavus vidutinių užklausų įvykdymo trukmių priklausomybes nuo serverio apkrovos esant įvairioms ŽP konfigūracijoms nustatyta:
  - Vieno ŽP egzemplioriaus ir nuoseklaus užklausų apdorojimo konfigūracijų derinys yra daugiau negu 4 kartus lėtesnis už kitus konfigūracijų derinius;
  - Naudojant kitus tris ŽP konfigūracijų derinius gauti labai panašūs rezultatai;
  - Greičiausiai ŽP veikia su vieno egzemplioriaus ir lygiagretaus užklausų apdorojimo rėžimų konfigūracijomis.
- Išmatuota vidutinio užklausų aptarnavimo per sekundę skaičiaus priklausomybė nuo serverio apkrovos ir ŽP konfigūracijų:
  - Tyrimo pradžioje, iki 20 vartotojų apkrovos – pirmajam konfigūracijų deriniui ir 40 vartotojų apkrovos likusiems konfigūracijų deriniams, aptarnaujamų užklausų

skaičius auga. Viršijus šią ribą apdorojamų užklausų skaičius ima mažėti ir nusistovi ties pastovia reikšme.
    - Skirtingų ŽP konfigūracijų derinių maksimalios užklausų apdorojimo spartos yra:
        - Vienas ŽP egzempliorius ir nuoseklus vykdymas: maksimali sparta – 93 užklausos/s, esant didesnėms apkrovoms - 88 užklausos/s;
        - Vienas ŽP egzempliorius ir lygiagretus vykdymas: maksimali sparta - 451 užklausa/s, esant didesnėms apkrovoms - 383 užklausos/s;
        - Po ŽP egzempliorių kiekvienai užklausai ir nuoseklus vykdymas: maksimali sparta - 418 užklausų/s, esant didesnėms apkrovoms - 380 užklausų/s;
        - Po ŽP egzempliorių kiekvienai užklausai ir lygiagretus vykdymas: maksimali sparta - 425 užklausos/s, esant didesnėms apkrovoms - 362 užklausos/s.
- Sistemoje siūloma naudoti šias žiniatinklio paslaugų konfigūracijas:
    - Vieno ŽP egzemplioriaus ir nuoseklaus užklausų apdorojimo rėžimus;
    - Saugų HTTPS duomenų perdavimo protokolą;
    - Transporto lygmens klientų autentifikavimą;
    - Siekiant didžiausios greitaveikos sistemoje patartina naudoti SOAP pranešimų formatą, tačiau norint sumažinti tinklu perduodamų duomenų kiekį galima naudoti ir JSON formatą.

5. IŠVADOS

1. Šiuo metu pasaulyje labai plačiai plinta asmeninių įrenginių naudojimo įmonėse tendencija. Nors mobilieji įrenginiai ir padidina darbo efektyvumą bei jo kokybę, tačiau kartu atneša ir papildomas saugumo grėsmes įmonėms.
2. Neteisingas mobiliųjų įrenginių naudojimas ir konfigūravimas atveria kelią įvairioms saugumo grėsmėms ir atakoms. Tai tokios grėsmės kaip: kenkėjiškos programėlės, socialinė inžinerija, komunikacijų perėmimas ar konfidencialių įmonės duomenų praradimas ir nutekinimas.
3. Norint apsaugoti įmonės duomenis nuo konfidencialumo ir vientisumo pažeidimų yra būtina sudaryti mobiliųjų įrenginių saugumo politiką ir ją įgyvendinti pasinaudojant organizacinėmis ir techninėmis priemonėmis.
4. Įmonės saugumo politikos įgyvendinimą ir kontrolę, darbuotojų asmeniniuose mobiliuosiuose įrenginiuose, leistų užtikrinti saugaus konfigūravimo paramos sistema, kuri suteiktų nuotolinio mobiliųjų įrenginių konfigūravimo ir priežiūros funkcijas.
5. Pasiūlytas asmeninių mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos modelis skirtas centralizuotam įmonės darbuotojų mobiliųjų įrenginių konfigūracijų valdymui ir būklės stebėjimui.
6. Saugaus konfigūravimo paramos sistema leidžia ne tik stebėti ir įvertinti asmeninių įrenginių saugumo būseną, bet ir esant reikalui pakeisti įrenginio konfigūracijas taip, kad jos atitiktų jam priskirtą saugumo politiką.
7. Atlikus eksperimentinį tyrimą nustatyta:
    a. Greičiausiai pranešimai tinklu perduodami naudojant HTTP protokolą, lėčiausiai – HTTPS su įjungtu pranešimų autentifikavimu;
    b. Užklausų apdorojimo trukmė serveryje yra beveik tokia pati naudojant tiek JSON, tiek SOAP pranešimų formatus, vidutinis skirtumas 1%;
    c. Naudojant klientų autentifikavimą, užklausos serveryje yra apdorojamos vidutiniškai 3,07 ms lėčiau;
    d. Naudojant SOAP pranešimų formatą, atsakymai gauti iš serverio mobiliajame įrenginyje yra apdorojami vidutiniškai 2,8 kartus greičiau negu naudojant JSON formatą;
    e. Transporto lygmens protokolų konfigūracijos turi nedidelę įtaką atsakymų apdorojimo trukmei mobiliajame įrenginyje;
    f. Didėjant perduodamų saugumo politikų kiekiui atliekamų užklausų trukmė taip pat proporcingai didėja;
    g. Naudojant HTTP protokolą ir SOAP perduodamų pranešimų formatą, užklausos yra atliekamos vidutiniškai 28 % greičiau negu naudojant JSON pranešimų formatą. Naudojant HTTPS protokolą SOAP pranešimai yra perduodami vidutiniškai 2,4 karto greičiau negu JSON;
    h. Daugiausiai užklausų sistema gali aptarnauti naudodama vieno ŽP egzemplioriaus ir lygiagretaus užklausų vykdymo rėžimus. Maksimali užklausų apdorojimo sparta - 451 užklausa/s. Esant didesnėms apkrovoms - 383 užklausos/s;
    i. Naudojant daugelio ŽP egzempliorių rėžimą maksimali apdorojamų užklausų sparta svyruoja nuo 425 iki 418 užklausų/s. Esant didesnėms apkrovoms nuo 362 iki 380 užklausų/s;

8. Sistemoje siūloma naudoti šias žiniatinklio paslaugų konfigūracijas:
    a. Daugelio žiniatinklio paslaugos egzempliorių ir nuoseklaus užklausų apdorojimo rėžimus;
    b. Saugų HTTPS duomenų perdavimo protokolą;
    c. Transporto lygmens pranešimų autentifikavimą;
    d. Siekiant didžiausios greitaveikos sistemoje patartina naudoti SOAP pranešimų formatą, tačiau norint sumažinti tinklu perduodamų duomenų kiekį galima naudoti ir JSON formatą.

6. LITERATŪROS SĄRAŠAS

[1] M. Landman, „Managing smart phone security risks,“ įtraukta *InfoSecCD '10 2010 Information Security Curriculum Development Conference*, New York, 2010.

[2] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck ir C. Wolf, „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.

[3] 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.

[4] 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.

[5] A. B. Garba, J. Armarego ir D. Murray, „BRING YOUR OWN DEVICE ORGANISATIONAL INFORMATION SECURITY AND PRIVACY,“ *ARPN Journal of Engineering and Applied Sciences*, t. 10, nr. 3, pp. 1279-1287, 2015.

[6] A. Greenberg, „iOS 7 Bug Lets Anyone Bypass iPhone's Lockscreen To Hijack Photos, Email, Or Twitter,“ 19 9 2013. [Tinkle]. Available: http://www.forbes.com/sites/andygreenberg/2013/09/19/ios-7-bug-lets-anyone-bypass-iphones-lockscreen-to-hijack-photos-email-or-twitter/. [Kreiptasi 23 11 2013].

[7] Kaspersky Lab, „IT SECURITY RISKS SURVEY 2014: A BUSINESS APPROACH TO MANAGING DATA SECURITY THREATS,“ Kaspersky Lab, 2014.

[8] A. Venčkauskas ir E. Kazanavičius, Informacinių technologijų saugos metodai, mokomoji knyga, Kaunas: UAB “TEV”, 2011.

[9] G. Russello, M. Conti, B. Crispo ir E. Fernandes, „MOSES: Supporting Operation Modes on Smartphones,“ įtraukta *SACMAT '12 Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, New York, 2012.

[10] Trend Micro, „Enterprise Readiness of Consumer Mobile Platforms,“ Trend Micro, 2012.

[11] Trend Micro, „Security in Evolving Mobile Platforms,“ Trend Micro, 2012.

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

[13] T. Zhao, G. Zhang ir L. Zhang, „An Overview of Mobile Devices Security Issues and Countermeasures,“ įtraukta *Wireless Communication and Sensor Network (WCSN), International Conference*, Wuhan, 2014.

[14] K. Kostiainen, E. Reshetova, J.-E. Ekberg ir N. Asokan, „Old, New, Borrowed, Blue – A Perspective on the Evolutionof Mobile Platform Security Architectures,“ įtraukta *CODASPY '11*

Proceedings of the first ACM conference on Data and application security and privacy, New York, 2011.

[15] G. Russello, et al., „DEMO: Demonstrating the Effectiveness of MOSES for Separation of Execution Modes," įtraukta *CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security*, New York, 2012.

[16] J. Shin, Y. Chung, K. S. Ko ir Y. I. Eom, „Design and implementation of the Management Agent for Mobile Devices based on OMA DM," įtraukta *ICUIMC '08 Proceedings of the 2nd international conference on Ubiquitous information management and communication*, New York, 2008.

[17] Y. Sun, Y. Wang ir X. Wang, „Mobile Security Apps: Loyal Gaurds or Hypercritical Thieves?," įtraukta *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), International Conference*, Guangdong, 2014.

[18] A. Distefano, A. Grillo, A. Lentini ir G. F. Italiano, „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.

[19] Open Mobile Allience, „OMA Device Management V1.2," 28 1 2011. [Tinkle]. Available: http://technical.openmobilealliance.org/Technical/release_program/dm_v1_2.aspx. [Kreiptasi 9 7 2014].

[20] „Android" operacinės sistemos architektūra. Paveiksliukas., [Tinkle]. Available: http://source.android.com/images/android_framework_details.png.

[21] „WCF" architektūra. Paveiksliukas., [Tinkle]. Available: http://i.msdn.microsoft.com/dynimg/IC5864.gif.

[22] Microsoft, „Developer network," [Tinkle]. Available: https://msdn.microsoft.com/en-us. [Kreiptasi 9 5 2015].

7. PRIEDAI

Visi magistrinio darbo priedai, kaip ir pats darbas elektroniniame formate, yra į rašyti į kompaktinę plokštelę, kuri pateikti priede 6.2. Priedus sudaro:

1. Konferencijoje „Informacinės technologijos 2015“ pristatytas straipsnis magistrinio darbo tematika;
2. Eksperimente naudotos etaloninės saugumo politikos;
3. Kompaktinė plokštelė su visais duomenimis ir dokumentais.

7.1. Straipsnis

ASMENINIŲ MOBILIŲJŲ ĮRENGINIŲ, NAUDOJAMŲ ĮMONĖSE, SAUGAUS KONFIGŪRAVIMO PARAMOS (SKP) SISTEMA

Vladas Drejeris

Kauno technologijos universitetas, Kompiuterių katedra, Studentų g. 50, Kaunas, Lietuva, vladas.drejeris@ktu.edu

Santrauka. Šiais laikais vis labiau plinta asmeninių mobiliųjų įrenginių naudojimo įmonėse tendencija, dar vadinama „atsinešk savo įrenginį" (angl. *Bring your own device*). Asmeninių mobiliųjų įrenginių naudojimas įmonėse darbuotojams suteikia daug privalumų, tačiau kartu įmonei sukelia papildomų saugumų problemų. Darbuotojai dažnai piktnaudžiauja mobiliaisiais įrenginiais, jungiasi prie atvirų viešųjų belaidžio ryšio tinklų ir naudoja netinkamai sukonfigūruotus įrenginius. Dėl to jie gali būti pažeidžiami virusų, piktavališkų programėlių, programišių atakų ar tiesiog pametami. Įvykus saugumo pažeidimui, įmonė rizikuoja prarasti konfidencialią informaciją, esančią mobiliajame įrenginyje. Viena iš priemonių įmonės darbuotojų kontrolei ir mobiliųjų įrenginių saugos užtikrinimui yra centralizuota mobiliųjų įrenginių valdymo sistema. Šiame darbe pateikiamas mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos modelis.

Raktiniai žodžiai: mobilieji įrenginiai, mobiliųjų įrenginių sauga, saugumo politika.

1 Įvadas

Šiuolaikiniai mobilieji įrenginiai pasiekė tokius skaičiavimų ir atminties kiekius, kurie prieš keletą metų buvo prieinami tik personaliniams ar nešiojamiesiems kompiuteriams. Dėl šio technologinio proveržio mobilieji įrenginiai vartotojams suteikia labai plačias galimybes tiek asmeniniam naudojimui, tiek darbui. Šiandien daugelyje įmonių šie įrenginiai tapo neatsiejama IT (informacinių technologijų) infrastruktūros dalimi.

Dabar beveik kiekvienas asmuo turi nuosavus mobiliuosius įrenginius, todėl pasaulyje ėmė sparčiai plisti tokių įrenginių naudojimo įmonėse tendencija, dar vadinama „atsinešk savo įrenginį" (angl. *Bring your own device*). Asmeninių įrenginių naudojimas įmonėje darbuotojui suteikia labai daug privalumų, tačiau kartu tai sukelia papildomų saugumo problemų įmonei. Įvykus saugumo pažeidimui mobiliajame įrenginyje kyla papildomas pavojus įmonės IT infrastruktūrai ir konfidencialiai informacijai. Įmonėse saugumui užtikrinti būtina sudaryti mobiliųjų įrenginių saugumo politiką ir įdiegti įvairias saugos priemones.

Darbo tikslas – sukurti paprastos asmeninių mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos modelį. Paprastumas traktuojamas kaip galimybė naudoti sistemą mažose verslo įmonėse su ribotais techniniais ištekliais. Modelio tyrimui atlikti realizuoti sistemos prototipą, skirtą centralizuotam įmonės darbuotojų asmeninių mobiliųjų įrenginių konfigūracijų valdymui ir būklės stebėjimui. Ištirti sistemos prototipą JSON (angl. *Java Script Object Notation*) ir SOAP (angl. *Simple Object Access Protocol*) pranešimų apsikeitimui HTTP ir HTTPS protokolais su ir be transporto lygmens autentifikavimo.

2 Mobiliųjų įrenginių saugumo grėsmės

Virusai – tai viena iš grėsmių, su kuriomis susiduria mobilieji įrenginiai, tačiau daug didesnį pavojų jiems kelia kenkėjiškas programinis kodas ir netinkamai veikiančios programėlės. Taip yra dėl to, kad standartinės apsaugos priemonės, kurios dažniausiai yra orientuotos į apsaugą nuo virusų, nepadeda apsisaugoti nuo šių grėsmių. Be to, įmonėms didelę grėsmę kelia netyčinis arba piktavališkas darbuotojų piktnaudžiavimas mobiliaisiais įrenginiais. Mobilieji įrenginiai naudojami nesilaikant įmonės saugumo politikos. Jais jungiamasi prie nesaugių viešų belaidės interneto prieigos taškų. Įrenginiai, kuriuose yra konfidencialių įmonės duomenų, gali būti pametami ar net pavagiami. Dažniausiai nuo šių pavojų neapsaugo ir vartotojų autentifikavimas ar duomenų šifravimas. Taip pat įmonėse sudėtinga kontroliuoti mobiliųjų įrenginių saugą dėl to, kad jose nėra naudojami nuotoliniai mobiliųjų įrenginių audito ir kontrolės įrankiai [4, 3].

3 Esamų mobiliųjų įrenginių konfigūravimo ir valdymo sistemų analizė

„Samsung Knox" – tai mobiliųjų įrenginių saugos sprendimas, skirtas atvirojo kodo „Android" operacinei sistemai. Jis užtikrina įrenginių saugumą operacinės sistemos lygmenyje naudodamas trijų dalių apsaugą, t. y. platformos apsaugą, programinės įrangos apsaugą ir mobiliųjų įrenginių valdymą. Saugumo mechanizmų realizavimui „Samsung Knox" naudoja modifikuotą „Android" operacinės sistemos versiją, todėl ši sistema veikia tik „Samsung" įmonės gaminamuose įrenginiuose [7].

„VMware" įmonės siūlomas mobiliųjų įrenginių saugumo sprendimas verslui – „Airwatch". Ši sistema skirta kovoti su mobiliųjų įrenginių keliamais sunkumais. Šiam tikslui ji suteikia efektyvų būdą valdyti visus įrenginius vienoje centralizuotoje administracinėje konsolėje. „Airwatch" leidžia lengvai įtraukti įrenginius į

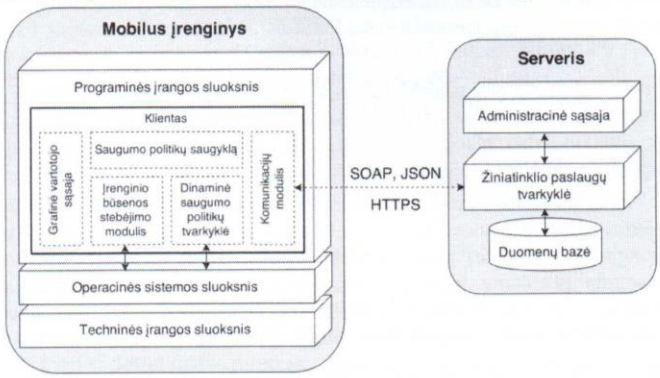
verslo aplinką, juos konfigūruoti ir atnaujinti nuotoliniu būdu. Ši sistema yra multiplatformė ir gali būti įdiegta tiek debesyje, tiek įmonės viduje [1].

Naudodamasis „MobileIron" platforma įmonės IT administratorius gali kontroliuoti mobiliųjų įrenginių ir jų programinės įrangos gyvavimo ciklą nuo pat įrenginio registracijos iki pašalinimo. Platforma sudaryta iš trijų pagrindinių komponentų: branduolio (angl. *Core*) – tai sąsaja, skirta mobiliųjų įrenginių, programėlių ir duomenų politikoms nustatyti, sargybinio (angl. *Sentry*) – tai išmanūs vartai, skirti mobilių duomenų kontrolei ir apsaugai, kliento (angl. *Client*) – tai programinė įranga, diegiama į mobiliuosius įrenginius, skirta konfigūracinių ir saugumo politikos įgyvendinimui. Ši sistema gali būti įdiegta debesyje arba įmonės viduje [5].

„BlackBerry verslo paslauga" (angl. *Enterprise Service*) – tai populiariausia mobiliųjų įrenginių konfigūravimo ir valdymo sistema tarp vyriausybinių organizacijų visame pasaulyje. Ši paslauga suteikia įrenginių, programėlių ir saugos valdymą vienoje centralizuotoje administravimo konsolėje. Taip pat ji suteikia galimybę atskirti asmenines ir darbui skirtas mobiliojo įrenginio funkcijas su saugios darbo vietos (angl. *Secure Work Space*) paslauga. Ši paslauga vartotojams suteikia galimybę atskirti socialinių tinklų duomenis, elektroninį paštą ir programinę įrangą, taip suteikiant aukštą kontrolės lygį ir apsaugą nuo duomenų praradimo [2].

4 SKP sistemos modelis

Mobiliųjų įrenginių saugaus konfigūravimo paramos sistema yra klientas – serveris architektūros tipo. Kiekviena sistemos dalis sudaryta iš komponentų, atliekančių tam tikras funkcijas (1 pav.).



1 pav. SKP sistemos architektūra

Komunikacijų modulis naudoja serverio teikiamas žiniatinklio paslaugas vartotojų ir įrenginių autentifikavimui, saugumo politikų ir komandų parsisiuntimui bei įrenginio audito pranešimų perdavimui.

Dinaminė saugumo politikų tvarkyklė yra atsakinga už saugumo politikos pritaikymą įrenginyje, atsižvelgiant į kontekstinę informaciją. Be to, šis modulis vartotojui arba trečiųjų šalių programinei įrangai gali pateikti įrenginio saugumo būseną, t. y. ar įrenginys atitinka aktyvią saugumo politiką.

Saugumo politikų saugykla – tai duomenų bazė, kurioje laikomos įrenginio saugumo politikos.

Įrenginio būsenos stebėjimo modulis atsakingas už mobiliojo įrenginio būsenos sekimą (laiko, pozicijos, aparatinių komponentų veikimo ir pan.) ir įvykių, įvykstančių įrenginyje, registravimą.

Administracinė sąsaja administratoriui suteikia galimybę valdyti vartotojų paskyras ir saugumo politikas, peržiūrėti mobiliųjų įrenginių informaciją ir atlikti nuotolinio įrenginių valdymo komandas.

Žiniatinklio paslaugų tvarkyklė – šiame komponente realizuojamos sistemoje naudojamos žiniatinklio paslaugos.

Duomenų bazė – šiame komponente saugomi visi sistemos duomenys.

4.1 Dinaminis saugumo politikų profiliavimas

Mobiliųjų įrenginių saugumo lygio ir konfigūracijų įvertinimui naudojamos saugumo politikos. Saugumo politika sudaryta iš keturių komponentų: sistemos subjekto / objekto identifikatoriaus, saugumo lygmens, apribojimų ir reikalavimų. Saugumo politikos gali būti priskiriamos tiek atskiriems sistemos subjektams (vartotojams), tiek objektams (mobiliesiems įrenginiams). Vienu metu įrenginyje gali būti keletas skirtingų saugumo politikų. Saugumo politikos įrenginyje dinamiškai pritaikomos atsižvelgiant į apribojimus [6] ir saugumo lygmenį. Esant kelioms vienu metu galiojančioms saugumo politikoms pritaikoma ta, kurios saugumo lygmuo yra aukštesnis, tai reiškia, pritaikoma griežtesnė saugumo politika.

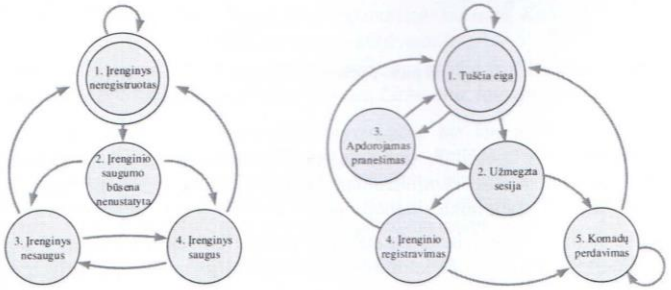
Apribojimai – tai saugumo politikos dalis, nurodanti, kokioms sąlygoms esant ji turėtų būti pritaikoma įrenginyje. Apribojimai gali būti priskiriami visai saugumo politikai arba atskiriems reikalavimams. Modelyje apibrėžiami šie apribojimai: įrenginio pozicija, laikas, data ir įrenginio aparatinių funkcijų veikimas.

Reikalavimai – tai saugumo politikos dalis, aprašanti, kokios saugumo priemonės turėtų būti

pritaikomos įrenginyje. Saugos reikalavimai gali būti dviejų tipų: privalomi ir neprivalomi. Įrenginys įgyja saugaus įrenginio statusą tik tuo atveju, jeigu yra patenkinami visi privalomi saugumo politikos reikalavimai. Saugumo politikoms gali būti priskiriami tokie saugumo reikalavimai kaip: slaptažodžių naudojimas ir sudėtingumas, automatinis užrakinimas, duomenų šifravimas, aparatinių funkcijų naudojimas („Wi-fi", „Bluetooth", „NFC" (angl. *Near Field Communication*), „GPS" (globali padėties nustatymo sistema), kamera) ir programinės įrangos naudojimas (privalomas arba draudžiamas).

4.2 Sistemos veikimas

Sistemos darbą geriausiai apibūdina serverio ir vartotojo mobiliojo įrenginio būsenų diagramos.



a) b)

2 pav. a) Vartotojo mobilaus įrenginio būsenų diagrama, b) serverio būsenų diagrama

Mobilusis įrenginys gali įgyti vieną iš keturių būsenų (žr. 2 pav. a). Visi sistemoje neregistruoti įrenginiai yra 1-ojoje būsenoje. Po sėkmingo įrenginio autentifikavimo ir registracijos sistemoje jis įgyja 2-ąją būseną. Šioje būsenoje įrenginys būna tol, kol iš serverio parsiunčiamos saugumo politikos. Gavus saugumo politikas, jos pritaikomos įrenginyje ir jis įgyja 3-iąją arba 4-ąją būseną. Pasikeitus įrenginio konfigūracijoms, jo būsena gali kisti tarp 3-iosios ir 4-osios būsenų, priklausomai nuo to, ar jos atitinka saugumo politiką ar ne. Baigus darbą įrenginys yra išregistruojamas iš sistemos ir vėl pereina į 1-ąją būseną.

SKP sistemos serveris gali įgyti vieną iš 5 būsenų (žr. 2 pav. b). Visų pirma serveris yra 1-ojoje būsenoje. Tuomet sistemos klientas gali užmegzti sesiją su serveriu ir jis pereis į 2-ąją būseną. Taip pat klientas gali į serverį perduoti pranešimą ir serveris iš 1-osios būsenos pereis į 3-iąją. Apdorojus pranešimą, esant reikalui, serveris gali užmegzti sesiją su klientu ir pereiti į 2-ąją būseną arba grįžti į 1-ąją būseną. Iš 2-osios būsenos serveris gali pereiti į 4-ąją arba 5-ąją būsenas. Į 4-ąją būseną serveris pereina, kai atliekama mobiliojo įrenginio registracija sistemoje, o į 5-ąją, kai užregistruotam įrenginiui perduodamos konfigūravimo ir valdymo komandos. Serveriui esant šioje būsenoje vyksta komunikacijos su klientu, baigus komunikacijas su klientu serveris vėl pereina į 1-ąją būseną.

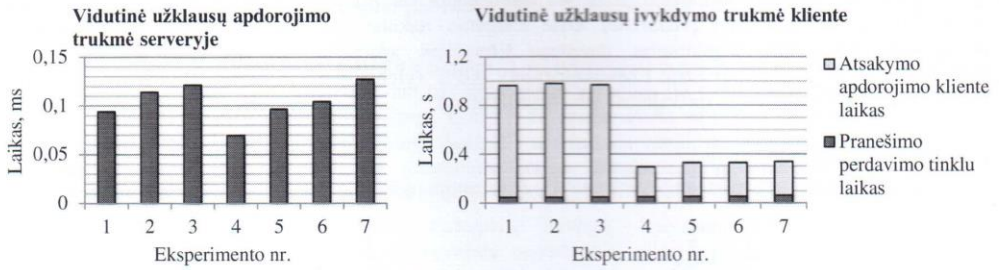
5 Eksperimentinis tyrimas

Tyrimui atlikti naudojama techninė įranga: nešiojamasis kompiuteris „DELL Inspiron 17R SE" (Intel Core i7 2,40 GHz, 8 GB RAM, Intel Centrino Wireless-N a/b/g/n, Windows 7 64-bit), mobilusis įrenginys „Samsung Galaxy S2" (Dual-core 1.2 GHz Cortex-A9, 1 GB RAM, Wi-Fi 802.11 a/b/g/n, Android 4.1.2) ir belaidės prieigos stotelė „D-link DIR-615" (802.11 b/g/n, 2.4 GHz, 300 Mbps).

Tyrimas atliekamas naudojant etalonines saugumo politikas. Naudojant JSON formatą pranešimas užima 4,27 kB, naudojant SOAP formatą – 8,83 kB. Mobilusis įrenginys prie serverio (nešiojamojo kompiuterio) jungiasi belaidžiu ryšiu. Šiam tikslui naudojama belaidės prieigos stotelė. Kiekvieno eksperimento metu serverio ir kliento programinė įranga naudoja skirtingas konfigūracijas, jos pateiktos 1 lentelėje. Eksperimento metu iš mobiliojo įrenginio atliekamos užklausos į serverį ir matuojami jų įvykdymo laikai. Rezultatai rašomi į tekstinius failus ir vėliau apdorojami kompiuteriu. Tyrimo rezultatai pateikiami grafikų pavidalu (žr. 3 pav.).

1 lentelė. Eksperimentų metu naudotos žiniatinklio paslaugų konfigūracijos

Eksperimento nr.	1.	2.	3.	4.	5.	6.	7.
Transporto protokolas	HTTP	HTTPS	HTTPS	HTTP	HTTPS	HTTPS	HTTPS
Pranešimų formatas	JSON	JSON	JSON	SOAP	SOAP	SOAP	SOAP
Autentifikavimas	-	-	Transporto lygmens	-	-	Transporto lygmens	Pranešimo lygmens



3 pav. Tyrimo rezultatai

6 Išvados

1. Pasiūlytas asmeninių mobiliųjų įrenginių, naudojamų įmonėse, saugaus konfigūravimo paramos sistemos modelis skirtas centralizuotam įmonės darbuotojų asmeninių mobiliųjų įrenginių konfigūracijų valdymui ir būklės stebėjimui.
2. SKP sistemos modelis leidžia ne tik stebėti ir įvertinti asmeninių įrenginių saugumo būseną, bet ir esant reikalui pakeisti įrenginio konfigūracijas taip, kad jos atitiktų jam priskirtą saugumo politiką.
3. Modelio ir jo pagrindu realizuotos paramos sistemos prototipo pagrindiniai bruožai paprastumas (klientas – serveris architektūra), dinaminis saugumo politikų profiliavimas ir orientacija į įmonės darbuotojų asmeninius mobiliuosius įrenginius. Tai išskiria pasiūlytą modelį ir paramos sistemos prototipą tarp žinomų komercinių sistemų, tokių kaip: „Samsung KNOX“, „Airwatch“, „Mobile Iron“ ir daugelio kitų, kurios paremtos sudėtinga architektūra ir debesų kompiuterijos sprendimais.
4. Tyrimo rezultatai rodo, kad SOAP duomenų perdavimo formato naudojimas yra 70 % našesnis negu JSON. Skirtumas tarp HTTP ir HTTPS transporto protokolų naudojimo yra nežymus. Todėl SKP sistemoje pranešimų perdavimui optimalu naudoti SOAP pranešimų formatą, HTTPS perdavimo protokolą ir transporto lygmens autentifikavimą. Naudojant šiuos serverio nustatymus užklausa, etaloninėms saugumo politikoms parsiųsti ir apdoroti, vidutiniškai trunka 0,329 sek.

Literatūros sąrašas

[1] **Airwatch.** Mobile Device Management, [žiūrėta 2015 03 24]. Prieiga internete: http://www.air-watch.com/

[2] **BlackBerry.** Blackberry enterprise portfolio, [žiūrėta 2015 03 24]. Prieiga internete: http://us.blackberry.com/

[3] **Kostiainen K., Reshetova E., Ekberg J.-E., Asokan N.** „Old, New, Borrowed, Blue – A Perspective on the Evolution of Mobile Platform Security Architectures“. CODASPY'11 Proceedings of the first ACM conference on Data and application security and privacy, New York, 2011.

[4] **Landman M.** „Managing smart phone security risks“. InfoSecCD'10 2010 Information Security Curriculum Development Conference, New York, 2010.

[5] **MobileIron.** MobileIron's EMM Tools, [žiūrėta 2015 03 24]. Prieiga internete: https://www.mobileiron.com/

[6] **Russello G., Conti M., Crispo B., Fernandes E.** „MOSES: Supporting Operation Modes on Smartphones“. SACMAT' 12 Proceedings of the 17th ACM symposium on Access Control Models and Technologies, New Tork, 2012.

[7] **Samsung.** White Paper: An Overview of Samsung KNOX, [žiūrėta 2015 03 24]. Prieiga internete: http://www.samsungknox.com/

Employee-owned mobile devices secure configuration support system used in enterprises

More and more employee-owned devices are being used in business. This increasing trend is also known as "Bring your own device". The use of personal mobile devices in enterprises provides many advantages to employees, but at the same time it leads to additional security threats for the company. Employees often misuse mobile devices, connect to the open wireless networks and use devices with unsecure configurations. As a result, these devices can be vulnerable to viruses, malicious applications, hacker attacks or simply be lost. In the event of a security breach company is at a risk of losing confidential information stored on a mobile device. One of the means to control the company's employees and to ensure the safety of mobile devices is a mobile device management system. This work presents the model of the employee-owned mobile devices secure configuration support system used in enterprises.

7.2. Eksperimente naudotų etaloninių saugumo politikų pavyzdžiai

7.2.1. Saugumo politika JSON formatu


```
[
  {
    "Configurations": [
      {
        "Description": "Slaptažodis negali būti trumpesnis negu nurodyta.",
        "Title": "Slaptažodžio ilgis",
        "Type": 0,
        "Value": "6"
      },
      {
        "Description": "Reikalingas sudėtingas slaptažodis.",
        "Title": "Slaptažodžio sudėtingumas",
        "Type": 1,
        "Value": "complex"
      },
      {
        "Description": null,
        "Title": "Slaptažodis būtinas",
        "Type": 2,
        "Value": "1"
      },
      {
        "Description": "Įrenginyje esanti kamera yra išjungta kol galioja ši saugumo politika.",
        "Title": "Kamera išjungta",
        "Type": 3,
        "Value": "1"
      },
      {
        "Description": "Įrenginyje esantys duomenys privalo būti šifruojami.",
        "Title": "Įrenginio šifravimas būtinas",
        "Type": 4,
        "Value": "1"
      }
    ],
    "Description": "Ši saugumo politika yra pritaikoma darbuotojui esant darbe.",
    "Requirements": [
      {
        "Description": "Saugumo politika galioja tik darbo dienomis.",
        "Title": "Savaitės dienomis",
        "Type": 0,
        "Value": "Mon,Tue,Wen,Thu,Fri"
      },
      {
        "Description": "Saugumo politika galioja tik darbo valandomis.",
        "Title": "Darbo valandomis",
        "Type": 2,
        "Value": "8:00-17:00"
      },
      {
        "Description": "Saugumo politika galioja tik įmonės teritorijoje.",
        "Title": "Įmonės teritorijoje",
        "Type": 1,
        "Value": "55.387,23.863,1000"
      }
    ],
    "SecurityLevel": 3,
    "Title": "Darbo saugumo politika"
  }
]
```

7.2.2. Saugumo politika SOAP formatu

```
<b:SecurityPolicy>
  <b:Configurations>
    <b:Configuration>
      <b:Description>Slaptažodis negali būti trumpesnis negu nurodyta.</b:Description>
      <b:Title>Slaptažodžio ilgis</b:Title>
      <b:Type>0</b:Type>
      <b:Value>6</b:Value>
    </b:Configuration>
    <b:Configuration>
      <b:Description> Reikalingas sudėtingas slaptažodis.</b:Description>
      <b:Title>Slaptažodžio sudėtingumas</b:Title>
      <b:Type>1</b:Type>
      <b:Value>complex</b:Value>
    </b:Configuration>
    <b:Configuration>
      <b:Description i:nil="true"/>
      <b:Title>Slaptažodis būtinas</b:Title>
      <b:Type>2</b:Type>
      <b:Value>1</b:Value>
    </b:Configuration>
    <b:Configuration>
      <b:Description>Įrenginyje esanti kamera yra išjungta kol galioja ši saugumo politika.</b:Description>
      <b:Title>Kamera išjungta</b:Title>
      <b:Type>3</b:Type>
      <b:Value>1</b:Value>
    </b:Configuration>
    <b:Configuration>
      <b:Description>Įrenginyje esantys duomenys privalo būti šifruojami.</b:Description>
      <b:Title>Įrenginio šifravimas būtinas</b:Title>
      <b:Type>4</b:Type>
      <b:Value>1</b:Value>
    </b:Configuration>
  </b:Configurations>
  <b:Description>Ši saugumo politika yra pritaikoma darbuotojui esant darbe.</b:Description>
  <b:Requirements>
    <b:Requirement>
      <b:Description>Saugumo politika galioja tik darbo dienomis.</b:Description>
      <b:Title>Savaitės dienomis</b:Title>
      <b:Type>0</b:Type>
      <b:Value>Mon,Tue,Wen,Thu,Fri</b:Value>
    </b:Requirement>
    <b:Requirement>
      <b:Description>Saugumo politika galioja tik darbo valandomis.</b:Description>
      <b:Title>Darbo valandomis</b:Title>
      <b:Type>2</b:Type>
      <b:Value>8:00-17:00</b:Value>
    </b:Requirement>
    <b:Requirement>
      <b:Description>Saugumo politika galioja tik įmonės teritorijoje.</b:Description>
      <b:Title>Įmonės teritorijoje</b:Title>
      <b:Type>1</b:Type>
      <b:Value>55.387,23.863,1000</b:Value>
    </b:Requirement>
  </b:Requirements>
  <b:SecurityLevel>3</b:SecurityLevel>
  <b:Title>Darbo saugumo politika</b:Title>
</b:SecurityPolicy>
```

7.3. Eksperimento duomenys ir dokumentai

VIETA KOMPAKTINEI PLOKŠTELEI