Kauno technologijos universitetas

Informatikos fakultetas

Organizacijose naudojamų asmeninių įrenginių saugos politikos valdymas

Baigiamasis magistro projektas

Andrius Šimkus

Projekto autorius

Prof. Jevgenijus Toldinas

Vadovas

Kaunas, 2022

Kauno technologijos universitetas

Informatikos fakultetas

Organizacijose naudojamų asmeninių įrenginių saugos politikos valdymas

Baigiamasis magistro projektas

Informacijos ir informacinių technologijų sauga (6211BX008)

Andrius Šimkus

Projekto autorius

Prof. Jevgenijus Toldinas

Vadovas

Doc. Gedeiminas Činčikas

Recenzentas

Kaunas, 2022

Kauno technologijos universitetas

Informatikos fakultetas

Andrius Šimkus

Organizacijose naudojamų asmeninių įrenginių saugos politikos valdymas

Akademinio sąžiningumo deklaracija

Patvirtinu, kad:

1. baigiamąjį projektą parengiau savarankiškai ir sąžiningai, nepažeisdama(s) kitų asmenų autoriaus ar kitų teisių, laikydamasi(s) Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo nuostatų, Kauno technologijos universiteto (toliau – Universitetas) intelektinės nuosavybės valdymo ir perdavimo nuostatų bei Universiteto akademinės etikos kodekse nustatytų etikos reikalavimų;

2. baigiamajame projekte visi pateikti duomenys ir tyrimų rezultatai yra teisingi ir gauti teisėtai, nei viena šio projekto dalis nėra plagijuota nuo jokių spausdintinių ar elektroninių šaltinių, visos baigiamojo projekto tekste pateiktos citatos ir nuorodos yra nurodytos literatūros sąraše;

3. įstatymų nenumatytų piniginių sumų už baigiamąjį projektą ar jo dalis niekam nesu mokėjęs (-usi);

4. suprantu, kad išaiškėjus nesąžiningumo ar kitų asmenų teisių pažeidimo faktui, man bus taikomos akademinės nuobaudos pagal Universitete galiojančią tvarką ir būsiu pašalinta(s) iš Universiteto, o baigiamasis projektas gali būti pateiktas Akademinės etikos ir procedūrų kontrolieriaus tarnybai nagrinėjant galimą akademinės etikos pažeidimą.

Andrius Šimkus

Patvirtinta elektroniniu būdu

Šimkus, Andrius. Organizacijose naudojamų asmeninių įrenginių saugos politikos valdymas. Magistro baigiamasis projektas / vadovas Prof. Jevgenijus Toldinas; Kauno technologijos universitetas, informatikos fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Informatikos inžinerija (Informatikos mokslai).

Reikšminiai žodžiai: Asmeniniai įrenginiai, saugos politika, valdymas, Android, išmanaus įrenginio programėlės, leidimai, scenarijų atvejų tyrimas, greitaveikos tyrimas.

Kaunas, 2022. 64 p.

Santrauka

Šiuolaikiniame verslo klimate mobilūs išmanieji įrenginiai tampa neatsiejama kasdienės praktikos verslo dalimi. Išmanieji mobilūs įrenginiai tapo duomenų peržiūros, keitimo, dalijimosi platformomis. Kompanijos visame pasaulyje bando pritaikyti inovatyvias praktikas, skirtas padidinti verslo operacijų kokybę ir našumą. Anksčiau taikyta praktika suteikdavo visas darbui skirtas priemones darbuotojui, tačiau šiomis dienomis interneto ryšį turinčių daiktų kiekis lenkia žmonių skaičių pasaulyje keliais kartais, o išmanųjį įrenginį turi 8 iš 10 žmonių pasaulyje. To pasekoje papildomi įrenginiai darbuotojui sukelia nepatogumus, o verslui papildomas išlaidas. Vis dažniau šiuolaikinio verslo aplinkoje sutinkama praktika, kai darbuotojas darbo tikslais gali naudoti asmeninį įrenginį – nešiojamą kompiuterį, planšetę, išmanųjį telefoną ir kt. Su asmeninių įrenginių funkcijomis darbuotojas jau būna gerai susipažinęs, jo nereikia apmokyti įrenginio valdymo, darbuotojui nereikia fiziškai su savimi turėti kelių įrenginių vienu metu. Ko pasekoje kyla darbuotojo pasitenkinimo lygis, kas daro įtaką produktyvesniam darbui, ir įmonės klientų aptarnavimui, įmonei taupant finansinius išteklius. Tačiau jokia praktika neatneša ir savų trūkumų.

Viename įrenginyje saugant, žiūrint ir keičiantis tiek asmeniniais, tiek įmonės duomenimis iškyla grėsmė nutekėti privatiems įmonės duomenims. Darbuotojai gali jungtis prie nesaugaus tinklo, naudoti įrenginius su nesaugiais nustatymais, ar kenkėjiškais failais. Iškyla problema – kaip užtikrinti įmonės duomenų saugumą darbuotojui naudojant asmeninį mobilųjį įrenginį. Taikant nesaugias praktikas, įmonei ar darbuotojui gresia teisinė atsakomybė už pažeidimus. Kompanijose, kurios disponuoja klientų, finansine ar kita įstatymų ginama informacija, privalo būti aprašyti veiksmai ir procedūros, skirti užtikrinti informacijos konfidencialumui. Tam įmonės sudaro informacinių technologijų saugos politiką. Informacinių technologijų saugos politikos tikslas yra užtikrinti informacijos konfidencialumą, vientisumą ir pasiekiamumą, kai ja disponuoja įmonėje dirbantys asmenys.

Šimkus, Andrius. Security Policy Management for Personal Devices Used in Organizations Master's Final Degree Project / supervisor Prof., Jevgenijus Toldinas; faculty of informatics, Kaunas University of Technology.

Study field and area (study field group): Informatics Engineering (Computing).

Keywords: Personal devices, security policy, management, Android, smartphone applications, permissions, case study, operating speed study.

Kaunas, 2022. 64 p.

Summary

In today’s business climate, mobile smart devices are becoming an integral part of everyday business practices. Smart mobile devices have become platforms for viewing, exchanging and sharing data. Companies around the world are trying to adopt innovative practices to increase the quality and productivity of their business operations. Previous practices provided the employee with all the tools required for the job. However, these days, the number of items with an internet connection exceeds the number of people in the world several times over, and 8 out of 10 people in the world have a smart device. Additional devices cause inconvenience to the employee and additional costs to the business. In the modern business environment, there is an increasing practice where an employee can use a personal device for work purposes - a laptop, a tablet, a smartphone, etc. The employee is already well acquainted with the functions of personal devices, he does not need training in the operation of the device, the employee does not need to physically have several devices with him at the same time. As a result, the level of employee satisfaction increases, which affects more productive work, company‘s customer service, additionaly saving the company‘s financial resources. However, no practice brings its own shortcomings.

Storing, viewing, and exchanging both personal and corporate data on a single device poses an additional risk of leaking private company data. Employees can connect to an insecure network, use devices with insecure settings, or malicious files. The problem is how to ensure the security of company data for an employee using a personal mobile device. Unsafe practices expose the company or employee to legal liability for violations. Companies that have access to customer, financial or other legally protected information must practice actions and procedures to ensure the confidentiality of the information. In regard to this, companies develop information technology security policies. The purpose of the information technology security policy is to ensure the confidentiality, integrity and availability of information when it is available to employees of the company.

Turinys

Lentelių sąrašas

Paveikslų sąrašas

Santrumpų ir terminų sąrašas

Santrumpos:

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

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

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

MIM (angl. Mobile Information Management) – mobilios informacijos valdymas;

NFC (angl. Near Field Communication) – artimojo lauko ryšys;

WIFI – belaidžio interneto ryšio technologija;

WPA (angl. Wi-Fi Protected Access) – belaidžio interneto ryšio šifravimo algoritmas;

GPS (angl. Global Positioning System) – globali padėties nustatymo sistema;

SDK (angl. Software Development Kit) – programinės įrangos vystymo įrankiai;

OS (angl. Operating System) – operacinė sistema;

IMEI (angl. International Mobile Equipment Identity) – unikalus mobilaus įrenginio kodas;

VPN (angl. Virtual Private Network) – virtualus privatus tinklas;

SMS (angl. Short Message Service) – trumpųjų žinučių servisas;

MMS (angl. Multimedia Messaging Service) – vaizdo ir garso žinučių servisas;

WAP (angl. Wireless Application Protocol) – tarptautinis belaidžio ryšio standartas;

JRE (angl. Java Runtime Environment) – java programavimo kalbos aplinka;

JVM (angl. Java Virtual Machine) – java programavimo kalbos virtuali mašina.

Įvadas

Nuo pat XX a. antroje pusėje atsiradusių pirmųjų procesorių, gebančių atlikti įvairius skaičiavimus, žmonės sugalvojo kaip realizuoti šią naują galimybę, išrandant vis tobulesnius įrenginius, leidžiančius keistis vaizdine, garsine, ar tekstine informacija. Per kelis dešimtmečius ši žmonijos dalis patyrė eksponentinę plėtrą ir pritaikymą, dėl šiandieną mums savaime suprantamų priežasčių. Kompiuteriniai įrenginiai palengvino, paspartino ir patobulino visas gyvenimo sritis.
Šiuolaikinėje verslo aplinkoje kompiuteriniai įrenginiai yra nepakeičiama kasdienybės dalis. Mobilūs įrenginiai, nuo pat jų atsiradimo patyrė staigų šių technologijų pritaikymą. Pradinė mobilių įrenginių paskirtis buvo atlikti ir priimti telefono skambučius ar tekstinę informaciją. Nuo tada šie įrenginiai išaugo iki į kišenę telpančių kompiuterių, gebančių atlikti daug resursų reikalaujančius skaičiavimus ir turinčių daugybę smulkių sensorių, pranašesnių nei prieš kelis dešimtmečius egzistavusių kompiuterinių sistemų. Atsiradus planšetiniams kompiuteriams ir išmaniųjų telefonų pardavimams pralenkus personalinių kompiuterių pardavimus keliais kartais, mobilių programėlių paklausa patyrė milžinišką augimą. Mobilių įrenginių galimybėms augant, šie įrenginiai tapo vis labiau patrauklia platforma žmonėms.
Šie pasikeitimai globaliame pasaulyje privertė verslą ieškoti alternatyvų, kaip ne tik pagerinti įmonės našumą, bet ir palengvinti darbą darbuotojams. Dar palyginus visai neseniai atsiradusi debesų kompiuterija į verslo pasaulį atnešė naują konceptą BYOD (angl. Bring Your Own Device). Kaip ir kiekvienas naujas konceptas, šis taip pat turi jam būdingų rizikų ir iššūkių priklausomai nuo įmonės pasirinkto informacinės saugos modelio. Tinkamai suformuluota ir pritaikyta įmonės informacinių technologijų saugos politika tapo ne tik sėkmingos verslo praktikos garantu, bet ir mūsų visų informacijos saugumu.

Magistrinio darbo tikslas: pasiūlyti organizacijose naudojamų asmeninių įrenginių saugos politikos valdymo modelį.

Uždaviniai:

- Atlikti organizacijose naudojamų asmeninių įrenginių ir saugos metodų analizę.
- Išnagrinėti asmeniniams įrenginiams gręsiančias grėsmes.
- Pasiūlyti organizacijose naudojamų asmeninių įrenginių saugos politikos valdymo modelį.
- Pagal pasiūlytą modelį realizuoti prototipą.
- Naudojantis prototipu atlikti eksperimentinį atvejų analizės ir greitaveikos tyrimą ir pateikti rezultatus.

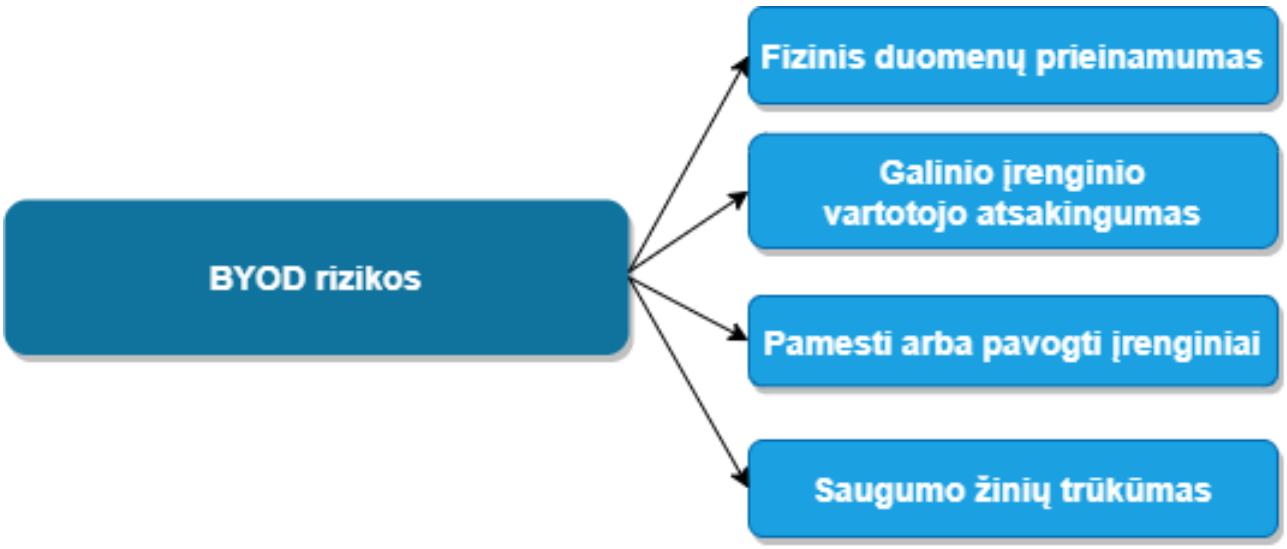
Dokumento struktūra - dokumentą sudaro 3 skyriai ir išvados:

1. Organizacijose naudojamų asmeninių įrenginių saugos analizė (16 psl.).
2. Organizacijose naudojamų asmeninių įrenginių saugos politikos valdymo modelis (15 psl.).
3. Organizacijose naudojamų asmeninių įrenginių saugos politikos valdymo tyrimas (17 psl.).

1. Organizacijose naudojamų asmeninių įrenginių saugos analizė

1.1. Organizacijose naudojamų asmeninių įrenginių konceptas ir problematika

Kylanti pragyvenimo kokybė bei mobilių įrenginių prieinamumas leidžia kiekvienam norinčiam įsigyti ir naudoti mobilų įrenginį. Tačiau tiek įrenginį naudojant asmeniniais, tiek su darbu susijusiais tikslais iškyla grėsmė duomenų konfidencialumui, vientisumui ir prieinamumui. BYOD pakankamai nauja verslo aplinkoje egzistuojanti iniciatyva, leidžianti darbuotojams atsinešti asmeninius įrenginius į darbo vietą. Joje verslas įžvelgia daugelį pranašumų, tačiau kaip ir su kiekviena nauja iniciatyva taip ir su BYOD iškyla naujų galimų rizikų (1 pav.).



1 pav. BYOD rizikos [13]

Organizacijose naudojamų asmeninių įrenginių koncepto problematika

BYOD konceptas pasaulyje yra plačiai taikoma praktika, tačiau didžiausia problema kyla kai reikia užtikrinti įmonės duomenų saugą skirtingiems asmeninių įrenginių tipams, kai juos gali naudoti bet kokių pareigybių darbuotojai. Kokią kontrolės metodiką pasirinkti, įrenginio nustatymų, įrenginiuose esančių programėlių, ar informaciją kurią gauna ir siunčia įrenginys? Taip pat, kaip užtikrinti jog naudojamas kontrolės metodas būtų užtikrinamas, kitaip tariant mobilių asmeninių įrenginių saugumo politikos užtikrinimas?

Fizinis duomenų prieinamumas

Fizinis prieinamumas prie įmonės duomenų reiškia, jog verslas turi užtikrinti neautorizuotų asmenų galimybių pasiekti jautrius įmonės duomenis apribojimą. Naudojant BYOD yra sunkiau užtikrinti šių duomenų saugumą, nei dirbant tik su įrenginiais, skirtais darbo vietai. Jei įrenginys atsiduria ne pas darbuotoją, o tai gali nebūtinai būti vagys ar piktavališkai nusiteikę asmenys, iškyla rizika jautriems duomenims. Aparatinė įranga, operacinės sistemos bei programėlės daro įtaką bendrai BYOD saugai [14].

Pamesti arba pavogti įrenginiai

Kiekvienais metais milijonai asmeninių įrenginių su įmonės duomenimis yra prarandami. Dalis šių įrenginių atsiduria piktavališkai nusiteikusių asmenų rankose. Spėjama, jog 22% įrenginių, kurie yra pagaminti bus pametami, o 50% šių įrenginių niekada nebus sugrąžinti [15]. Dauguma šių įrenginių yra perparduodami siekiant materialinės naudos, o piktavališkai nusiteikę asmenys tokius įrenginius superka ir bando gauti informacijos iš įrenginyje esančių duomenų. BYOD iniciatyvoje svarbu apsisaugoti nuo tokių grėsmių, naudojant tokias saugumo priemones kaip slaptažodžiai, šifravimas, duomenų ištrynimas įrenginio dingimo atveju.

Saugumo žinių trūkumas

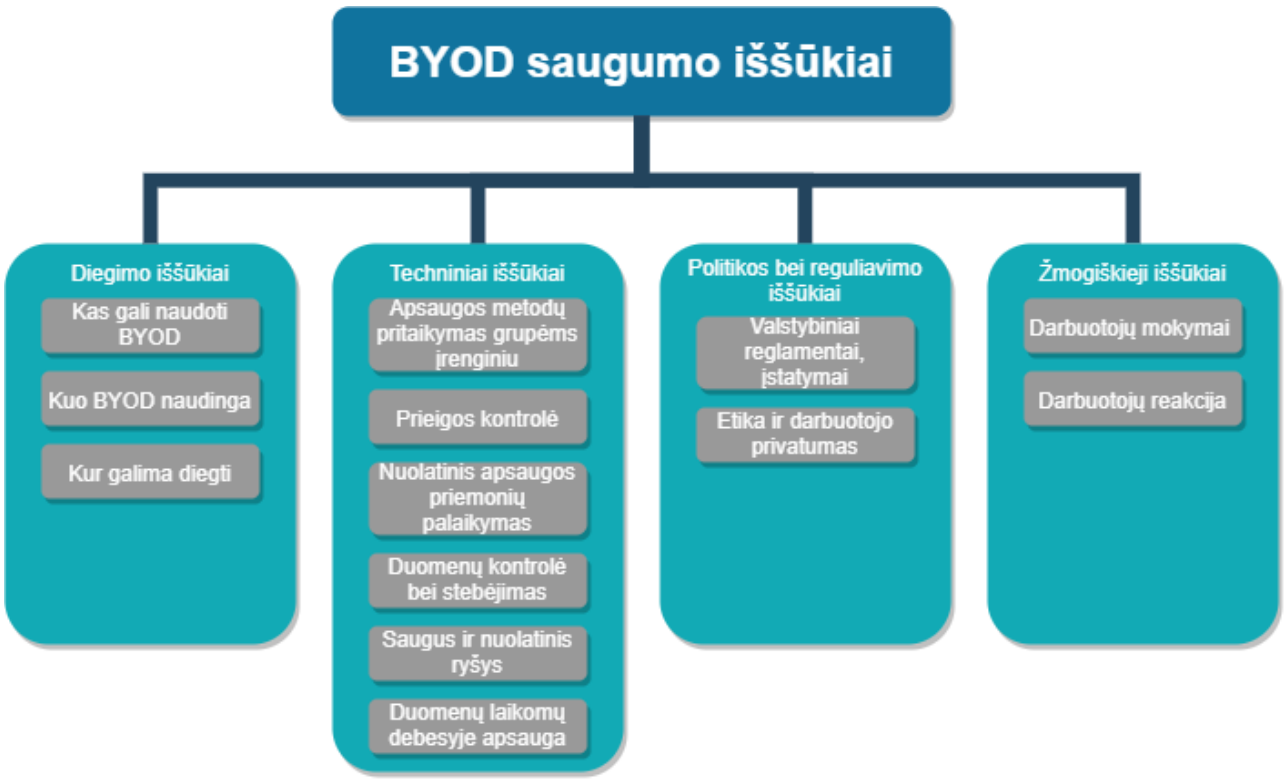
Darbuotojų mokymai reikalauja pastangų bei įmonės resursų. Laikui bėgant darbuotojai yra linkę atlaidžiau žiūrėti į įmonėje taikomą saugumo politiką. Kartais įmonė neskiria pakankamai resursų darbuotojų saugos žinioms gilinti. Nuolatinis darbuotojų švietimas kaip elgtis su įrenginiais ir juose esančia informacija yra neatskiriama BYOD dalis [16].

Galinio įrenginio vartotojo atsakingumas

Naudojant asmeninius mobilius įrenginius darbui atlikti, ant darbuotojo pečių gali kristi daugiau atsakomybės, nes darbuotojas turi atidžiau elgtis su mobiliu įrenginiu. Tai sukelia ir papildomo nerimo įmonei. Tačiau, esant tinkamai saugumo politikai įmonėje, ir tokioms priemonėms kaip debesų kompiuterija galima šią rizika sumažinti [17]. Tačiau įmonės turi imtis reikiamų priemonių, jog IT administratoriai diegtų atnaujintas saugos gaires, o darbuotojai jų laikytųsi.

1.2. Organizacijose naudojamų asmeninių įrenginių apsaugos iššūkiai

Norint įmonėje įvesti BYOD konceptą susiduriama su daugeliu iššūkių. Įmonės saugos politika nustato kokiais įrenginiais bus galima prieiti įmonės duomenis, kokia bus darbuotojų privatumo politika, kiek išteklių galima skirti mokymams bei BYOD palaikymui. Pagrindiniai BYOD apsaugos priemonių iššūkiai versle [1]:



2 pav. Organizacijose naudojamų asmeninių įrenginių saugumo iššūkiai [1]

A. Diegimo iššūkis

Nustatyti kada, kur ir ar reikėtų įmonei toleruoti BYOD iniciatyvą yra vienas iš pirminių iššūkių diegiant saugumo politiką. Norint įveikti šį iššūkį kompanija privalo išanalizuoti skirtingus įmonėje esančius padalinius, juose dirbančius darbuotojus ir jų pareigas. Iššūkis kyla sprendžiant kaip naudojami bendri duomenys, reikalingi keliems darbuotojams ir kaip jie yra prieinami bei keičiami.

B. Techniniai iššūkiai

Prieigos kontrolė. Šis iššūkis gretinamas su prieš tai aprašomu. Kompanijos privalo nustatyti leidimų lygius kiekvienam darbuotojui bandant prieiti prie bendrų įmonės duomenų, naudojant asmeninį įrenginį ir galimai išorinę interneto prieigą [18]. Kiti pasitaikantys iššūkiai: laiko prieigai skirtas limitas, naudotojų skaičius ir kaip šie darbuotojai pasieks norimą informaciją. Prieigos kontrolės iššūkio mastui ir sprendimo būdams daro įtaką įmonės dydis, vieta, industrija ir kt.

Apsaugos metodų pritaikymas grupėms įrenginių. Įrenginių gausa, kuriuos naudoja darbuotojai, apsunkina apsaugos priemones nuo galimų grėsmių. Skirtingi įrenginiai ir operacinės sistemos reiškia, jog reikės įdiegti skirtingas priemones, jog apsauga būtų palaikoma skirtingais įrenginiais. Nuolatinis naujų apsaugos priemonių diegimas ir atnaujinimas plačiam naudojamų įrenginių ratui sukelia papildomus resursų bei personalo išteklius verslui.

Nuolatinis apsaugos priemonių palaikymas. BYOD iniciatyva reikalauja nuolatinio programinio palaikymo. Norint palaikyti siekiamą apsaugos lygmenį organizacijoje reikalingas papildomas personalas patenkinti šią iniciatyvą. Tai reikalauja finansų bei laiko.

Duomenų kontrolė bei stebėjimas. Bendrai naudojami įmonės duomenys yra vienas esminių nerimą keliančių iššūkių verslui [18]. Konfidencialumo ir vientisumo išlaikymas priklauso nuo to ar duomenys yra laikomi ir prieinami tik naudojant mobilius įrenginius. Duomenų stebėjimas yra sudėtingas, nes įmonei sunku užtikrinti, jog duomenys nebus nutekinami.

Saugus ir nuolatinis ryšys. Įmonei kuri naudoja BYOD iniciatyvą nuolatinis ryšys tarp įmonės tinkle esančių duomenų ir asmeniniuose įrenginiuose naudojamo interneto ryšio yra vienas esminių kriterijų norint, jog darbai vyktų sklandžiai [18]. Vieni iš veiksnių yra darbuotojų naudojami vieši, neapsaugoti Wi-Fi prisijungimai bei nežinomi namuose naudojamo interneto apsaugos nustatymai.

Duomenų laikomų debesyje apsauga. Debesų technologija tapo neatskiriama BYOD iniciatyvos dalimi, ji leidžia prieiti prie įmonės duomenų bet kur ir bet kada naudojant interneto prieigą ir pašalinant būtinybę laikyti duomenis kiekviename įrenginyje [19, 21]. Duomenims prieinamiems iš asmeninio įrenginio kyla tokios pačios saugumo spragos kaip ir įrenginiui: laikymas, kontroliavimas bei stebėjimas. Įmonės nepajėgumas kontroliuoti šių duomenų sukelia saugumo spragas [20].

C. Politikos bei reguliavimo iššūkiai

Valstybiniai reglamentai, įstatymai. Skirtingose valstybėse esančios įmonės privalo atsižvelgti į galiojamus valstybinius reglamentus taikant BYOD iniciatyvą. Teisės aktai nustato kokio lygio duomenų kontrolę gali taikyti įmonė, kad nebūtų pažeistos darbuotojų teisės.

Etika ir darbuotojo privatumas. Kai darbuotojas naudoja asmeninį įrenginį darbo tikslais, įmonės privalo atsižvelgti kaip saugumą užtikrinančios priemonės atitinka darbuotojų privatumą užtikrinančius įstatymus. Jautrūs įmonės duomenys turi aukštus sekimo standartus norint užtikrinti, jog duomenys nebūtų nutekinami. Daugumoje valstybių įstatymai nurodo, jog darbuotojai privalo raštiškai sutikti, jog jų įrenginiuose būtų galima įdiegti saugumo priemones ar naudoti asmeniuose įrenginiuose esamus duomenis.

D. Žmogiškieji iššūkiai

Darbuotojų mokymai. Norint taikyti BYOD iniciatyvą nuolatiniai darbuotojų apsaugos politikos taikymo ir užtikrinimo mokymai yra būtini [21]. Kiekvienas darbuotojas privalo žinoti bazinę apsaugos politiką, tačiau tai daryti nuolat yra didelis iššūkis. Pagrindiniai mokymų tikslai yra supažindinti darbuotojus kokie įrenginiai yra priimtini naudojimui, kokios galimos grėsmės kyla naudojant BYOD politiką bei kaip išlaikyti įmonėje naudojamus duomenis saugius.

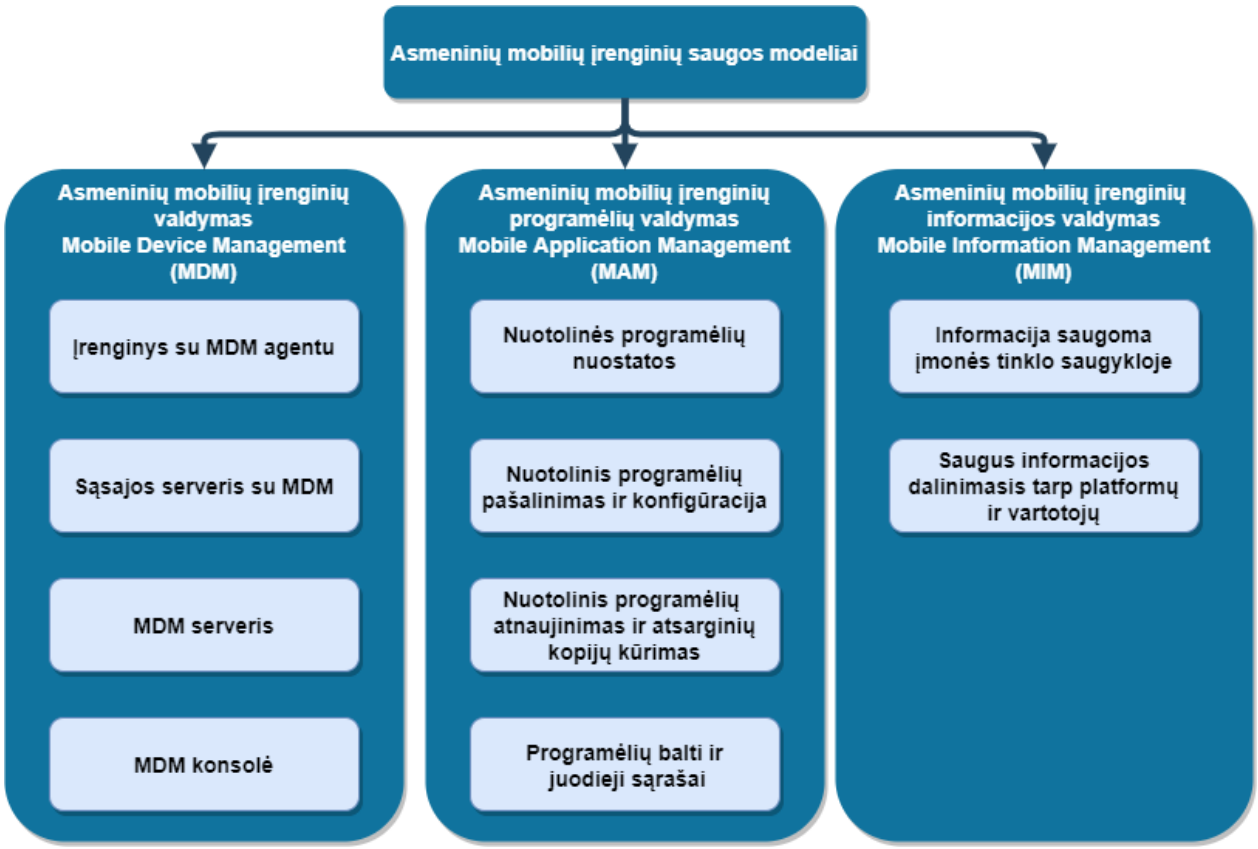
Darbuotojų reakcija. Įmonėje naudojama BYOD politika privalo turėti visiems žinomas gaires ir kas laukia už šių gairių nesilaikymą. Bėgant laikui darbuotojai yra linkę užmiršti įmonėje naudojamos BYOD gairės. O darbuotojams, kurie pažeidžia šias gaires, turi būti taikomos sankcijos.

1.3. Asmeninių mobilių įrenginių apsaugos modeliai

Besivystant informacinėms bei komunikacinėms technologijoms išmaniųjų įrenginių rinka siekia neregėtas aukštumas. Plečiantis mobiliųjų įrenginių galimybėms ir funkcijoms operacinės sistemos tampa vis galingesnės bei vis dažniau naudojamos tiek kasdieninėje tiek verslo aplinkoje. Vis

daugiau darbuotojų pradeda naudoti asmeninius mobilius įrenginius darbui. Literatūroje galima rasti tris asmeniniams įrenginiams, skirtiems naudoti darbo aplinkoje, saugos modelius (3 pav.) [2].

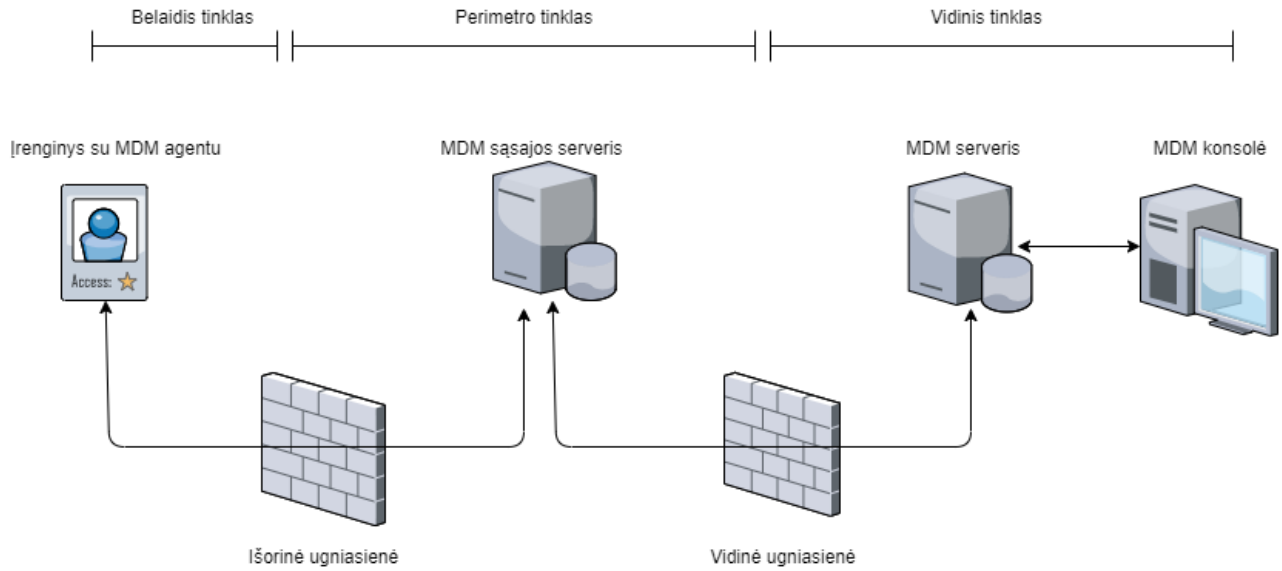
- Mobilių įrenginių valdymas – (angl. Mobile Device Management (MDM));
- Mobilių programėlių valdymas – (angl. Mobile Application Management (MAM));
- Mobilios informacijos valdymas – (angl. Mobile Information Management (MIM)).



3 pav. Organizacijose naudojamų asmeninių įrenginių saugos modeliai [2]

1.4. Asmeninių mobilių įrenginių valdymo modelis (MDM)

MDM modelis naudojamas norint nuotoliniu būdu stebėti įrenginio būklę ir kontroliuoti įrenginio funkcijas. Šio modelio pagrindas sudaromas iš dviejų dalių. MDM agento bei MDM serverio. MDM agentas – programėlė įrašoma į asmeninį įrenginį, kuri siunčia informaciją MDM serveriui (4 pav.) MDM sistemos dažniausiai turi kliento – serverio struktūrą. MDM leidžia pritaikyti tokias saugumo politikas įrenginyje kaip [9]: slaptažodžių naudojimas, pilna duomenų kriptografija, duomenų ištrynimas po nesėkmingų prisijungimo bandymų, naudojimui skirto laiko pasibaigimas ir kt. Įmonė naudojanti MDM gali įjungti ar išjungti mobilaus įrenginio interneto, Bluetooth, kameros, mikrofono ar GPS prieigas. Kokias funkcijas gali palaikyti įrenginys nustato įmonės saugos politika.



4 pav. Paprasta MDM architektūra [8]

MDM architektūra (4 pav.) taip pat leidžia centralizuoti įvairių asmeninių mobilių įrenginių valdymą skirtingoms operacinėms sistemoms kaip Android, iOS, Blackberry OS ar nešiojamų kompiuterių kaip Windows, MAC OS, linux. Naudojant MDM įmonės gali nuspręsti prie kokių duomenų kurie asmeniniai įrenginiai gali turėti prieigą. Norint pritaikyti MDM sustiprinti apsaugą BYOD iniciatyvoje dažnai reikalinga kaupti darbuotojų veiksmų įrašus (angl. Event log) [9]. Darbuotojų veiksmų įrašai įgalina įmonę atlikti saugumo auditą bei gairių laikymąsi. Tai taip pat leidžia sekti naudojamų duomenų srautus ar ryšio gedimus.

1.5. Asmeninių mobilių įrenginių programėlių valdymo modelis (MAM)

MAM yra lankstesnė MDM alternatyva, nes šis metodas reikalauja prižiūrėti tik tam tikras mobiliame įrenginyje esančias programėles [1]. MAM leidžia įmonei pritaikyti mobilių programėlių naudojimo politikas, nustatyti kontrolės taisykles, keisti programėlių nustatymus, atimti prieigą prie tam tikrų programėlių bei pašalinti neautorizuotas programėles. Kitos programėlės esančios už MAM ribų išlieka privačios.

IT sistemų administratoriai naudoja MAM modelį diegiant, šalinant, naujinant, audituojant bei stebint įmonės veiklai skirtas programėles. MAM modelis gali būti apibūdinamas kaip nuotoliniu būdu prieinamos programėlių [2]:

- Nuostatos;
- Diegimas, naujinimas, kopijų kūrimas;
- Baltieji ir juodieji sąrašai;
- Konfigūracija bei šalinimas.

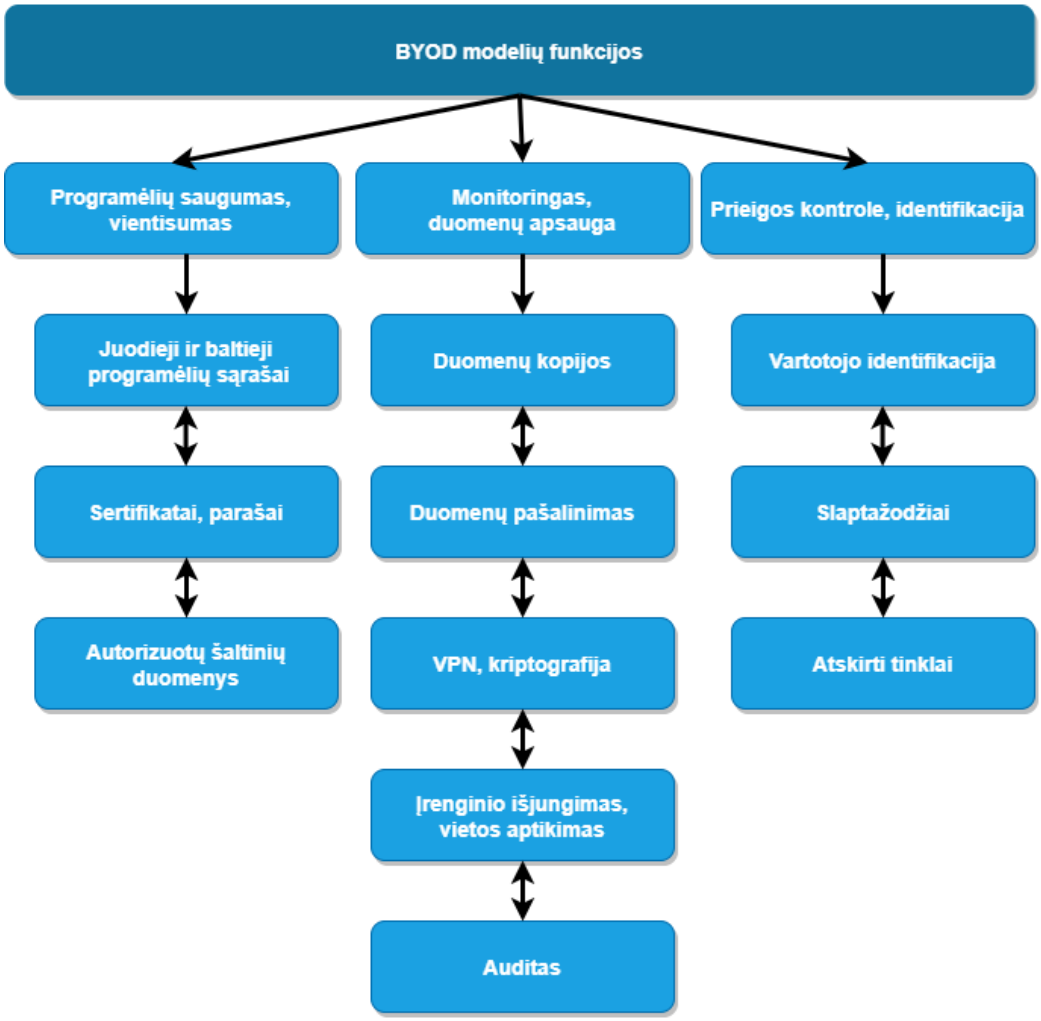
1.6. Asmeninių mobilių įrenginių informacijos valdymo modelis (MIM)

MIM modelyje informacijos valdymas naudojamas sinchronizuojant dokumentus tarp skirtingų platformų bei asmeninių prietaisų serveryje ir užtikrinant saugumo gaires ir procedūras. Šiam metodui užtikrinti naudojama debesų kompiuterijos technologija. Reikalingi duomenys saugomi debesyje. MIM atsakinga tik už informacijos valdymą, tad ji dažniausiai veikia kartu su MDM arba

MAM. MIM leidžia prieiga prie įmonės duomenų tik tam tikriems įrenginiams [2]. Mobilūs prietaisai ar programėlės gali neturėti pakankamai norimos apsaugos, padidinti įmonės duomenų apsaugos lygį, vienas iš sprendimų suteikti apsaugą patiems įmonės duomenims serveryje. Ne visos programėlės kurios turi prieigą prie įmonės duomenų apdoroja šiuos duomenis konteineriuose. MIM yra reikalingas norint apsaugoti duomenis nuo neautorizuotos prieigos, pakeitimo ar ištrynimo.

1.7. Organizacijose naudojamų asmeninių įrenginių funkcijos

MDM, MAM ir MIM modeliai pateikia keletą metodikų kaip gali būti užtikrinamas asmeninių įrenginių duomenų saugumas darbo aplinkoje. Šių metodikų funkcijos gali būti skirstomos apibendrinant į (5 pav.) [23]:



5 pav. Organizacijose naudojamų asmeninių įrenginių modelių: MDM, MAM ir MIM funkcijos

Programėlių saugumo ir vientisumo tikslas yra kiek galima sumažinti programėlių iš nepatikimų šaltinių naudojimą kontroliuojant darbuotojo į įrenginį įrašomas programėles, tai daroma naudojant:

- Juoduosius ir baltuosius sąrašus;
- Parašus, sertifikatus;
- Autorizuotų šaltinių duomenis.

Duomenų monitoringo ir apsaugos tikslas yra apsaugoti įmonės duomenis, tai gali būti atliekama naudojant:

- Kriptografiją ir VPN;
- Duomenų šalinimą;
- Duomenų kopijas;
- Auditą;
- Įrenginio išjungimą ir vietos aptikimą.

Prieigos kontrolė

Identifikacijos ir prieigos kontrolės tikslas yra identifikuoti vartotojus ir asmeninius mobilius įrenginius, vykdyti bei kontroliuoti įmonės duomenų prieinamumo politiką skirtingais lygiais, tai padeda užtikrinti:

- Slaptažodžiai;
- Vartotojo identifikacija;
- Tinklų atskyrimas.

Autentifikavimas

Autentifikavimo procesas suteikia prieigą prie įrenginio ar sistemos tik autorizuotiems asmenims. Autorizacija atliekama naudojant tris technologijas: kas esi, ką žinai arba ką turi. Pirmuoju atveju norint atlikti autentifikaciją surenkami fiziologiniai žmogaus biometriniai duomenys, dažniausiai tai būna pirštų antspaudai, akies rainelė, balsas, veido geometrija ar šių biometrijų kombinacijos. Antruoju atveju naudojama tik tam skirtui asmeniui žinoma informacija kaip slaptažodis ar PIN kodas. Ką turi metodas dažniausiai sutinkamas naudojant žetonus.

5 pav. galima matyti pagrindines funkcijas siekiant apsaugoti BYOD iniciatyvą [23], tačiau šiomis dienomis prižiūrėti mobilius asmeninius įrenginius juose esančias programėles ir informaciją yra be galo sunki užduotis, kai piktavališkai nusiteikę asmenys novatoriškais būdais bando siekti asmeninės naudos [22, 23, 11]. Didelis asmeninių mobilių įrenginių galingumas bei sparta ir kaip niekad plati interneto integracija tapo patraukliu taikiniu nusikaltėliams. Mobilių įrenginių kiekiui pasaulyje augant, laikui bėgant šių grėsmių turėtų daugėti, tolimesni moksliniai tyrimai bei inovacijos kovojant prieš piktavališkai nusiteikiamus asmenis yra būtini.

1.8. Kenkėjiška veikla mobiliuose įrenginiuose

Atakos skirtos mobiliems įrenginiams iš esmės nesiskiria nuo atakų skirtų stacionariems kompiuteriams ar verslams. Didžioji dalis atakų įvykdoma vartotojui neatidžiai įdiegus kenksmingą programėlę ir suteikiant tai programėlei daugiau leidimų pasiekti norimus resursus, negu iš tiesų reikia, ar atliekant kenkėjiškus veiksmus įrenginyje naudojant dar nežinomą spragą operacinėje sistemoje. Programėlės, kurioms yra suteikiama daugiau leidimų nei būtina atlikti pageidaujamoms funkcijoms, gali išnaudoti perteklinę informaciją norint gauti finansinės naudos. Tai galima padaryti ir be vartotojo žinios. Šios grėsmės kyla tiek dėl vartotojo neapdairumo, tiek dėl spragų operacinėse sistemose.

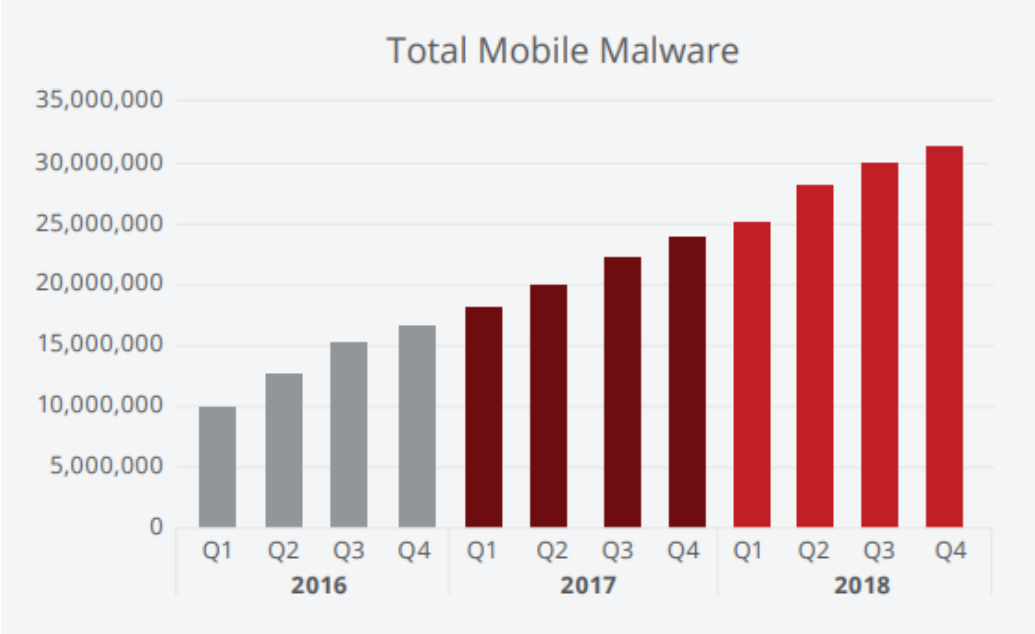
Atsižvelgiant į dviejų populiariausių Android OS ir Iphone operacinių sistemų statistiką, daugiausia piktavališkų programų yra rašoma Android platformai, vien dėl kelis kartus didesnio vartotojų skaičiaus. Symantec, Norton antivirusinės programinės įrangos kūrėjai paskelbė [12], jog iš

mobiliuose įrenginiuose platinamų kenkėjiškų programėlių 30% seka vartotojo buvimo vietą, 28% vagia duomenis iš mobilaus įrenginio, 20% bando parsiųsti failus be vartotojo žinios, 10% bando pakeisti mobilaus įrenginio nustatymus. Didžioji dauguma šių atakų turi finansinio pasipelnymo motyvą. Šiomis dienomis, kai vis daugiau verslui skirtos informacijos laikoma mobiliuose įrenginiuose, kenkėjiškos programėlės kelia vis didesnių neramumų, tad būtina ieškoti būdų kovoti prieš jas.

1 lentelė. Skirtingų tipų kenkėjiškų programėlių veikla

Duomenų pasisavinimas	**Stebėjimas**	**Apsimetimas**	**Finansinė nauda**	**Botnet veikla**
Kontaktai El. laiškai Failai Paskyros Tarptautinis mobilaus įrenginio numeris (IMEI)	Garsas Vaizdas Skambučiai Vieta Žinutės	El. laiškų siuntimas Trumpųjų SMS žinučių peradresavimas Įrašai socialiniuose tinkluose	Išpirka Mokamo tarifo skambučiai Mokamo tarifo SMS/MMS žinutės	Neleidžiami paspaudimai Paskirtytos paslaugos atakos Mokamo tarifo SMS/MMS žinutės

Kalbant mobilių įrenginių saugumo tematika, visų pirma galvojama apie kenkėjiškai nusiteikusius programišius besikėsinančius į programėlių vartotojo asmeninius duomenis ar paslaugų sutrikdymą. Virusai, trojos arkliai bei kitos kenkėjiškos programos padeda programišiams šiuos tikslus pasiekti [22]. Tai pagrindinės priežastys, leidžiančios vykdyti kenkėjišką veiklą, bei taip pat galimybės tirti jas ir ieškoti apsaugos priemonių nuo šios dažnai nelegalios veiklos. Tačiau kyla ir kitų saugumo problemų, kaip vidinės grėsmės. Kai neteisingam programėlių eksploatavimui grėsmę kelia administratoriai ar įmonės darbuotojai nežinodami kaip tinkamai elgtis su jautriais duomenimis ir programėlėmis. Didžiausia problema, tai saugumo gairių neišmanymas bei mokymų trūkumas. Mobilių įrenginių saugumas yra daugiau nei techninis išsilavinimas, tai besitęsiantis procesas apimantis žmones ir jų veiklą.



6 pav. Mobilių įrenginių kenkėjiškų programų statistika, kas ketvirtį metų [30]

Kol internetu besinaudojančių įrenginių skaičius nesustabdomai auga, IT specialistai visame pasaulyje kovoja prieš kenkėjiškus programišius. Debesų technologija priklauso nuo nuolat prieinamos didelės spartos interneto prieigos. Išmanūs telefonai, išmanūs laikrodžiai, daiktų interneto prietaisai, sujungė žmoniją niekad praeityje neregėtais mastais. Kenkėjiškos programos visose formose: šnipinėjimo programos, „phishing“ el. laiškai, trojos arkliai ir kt. [22] kelia grėsmę kasdien. Programėlių patikra prieš įrašymą į mobilų įrenginį gali padėti šių grėsmių išvengti. Kenkėjiškos programos nuolat keičiasi, todėl svarbu apžvelgti kenkėjiškų programėlių klases. Šiandieną dažniausiai pasitaikančios atakos yra prieš bankines sistemas bei kriptovaliutų kasimą naudojant mobilaus įrenginio resursus. Dažniausiai pasitaikančios mobilių įrenginių grėsmės:

1.8.1. Išpirkų programėlės

Tai kenkėjiškos programėlės, kurios pasisavina vartotojo informaciją, ja užšifruoja, ir dažniausiai prašo materialinės naudos, norint gauti raktą informacijos iššifravimui [11]. Apart to, jog informacija esanti įrenginyje yra užšifruojama, vartotojams yra sustabdoma prieiga prie įrenginio uždedant arba pakeičiant prisijungimo slaptažodžius, o bandant šią prieigą atkurti nemokant išpirkos, gręsia duomenų praradimas visam laikui, jei nėra sukurtos duomenų kopijos.

1.8.2. Šnipinėjimo programėlės

Tai tokios programėlės kurių tikslas rinkti informaciją apie vartotojo elgseną, vietą, siunčiamus bei gaunamus duomenis, dažniausiai vartotojui nežinant. Šiomis programėlėmis galima stebėti tiek vartotojo veiklą interneto naršyklėje, tiek skaityti gaunamas bei siunčiamas žinutes, nuotraukas, skambučius, bankinius duomenis [22]. Šie duomenys vėliau parduodami ne etiškoms kompanijoms, siekiančioms įgyti pranašumą prieš konkurentus.

1.8.3. Reklaminės programėlės

Vienas iš dažniausiai pasitaikančių kenkėjiškos veiklos programėlių tipų, dėl tiesioginės naudos programišiams bei nesunkaus pritaikymo ir sunkaus atpažinimo. Reklamos, tai mobilių įrenginių programėlių pagrindinė atlygio priemonė kūrėjams. Dažniausiai tokios programėlės būna nemokamos, o vartotojai pripratę nemokamose paslaugose matyti reklamas, tačiau vartotojai nežino ar šios reklamos, tai atlygis programėlės kūrėjams ar piktavalių programišių pasipelnymo būdas. Praktikoje žinoma atvejų, kai šios programėlės įrašomos dar gamykloje, prieš išleidžiant mobilius įrenginius į rinką. Vartotojai, turintys šias programėles įrenginyje, mato nuolat ekrane pasirodančias reklamas, o tai ypatingai sunku ištaisyti, jei reklaminės kenkėjiškos programėlės yra įrašomos operacinės sistemos lygmenyje.

1.8.4. Laisvos prieigos prie įrenginio programėlės (angl. root)

Tai tokios programėlės, kuriomis bandoma gauti laisvų teisių administracinę prieigą prie mobilaus įrenginio. Programišiai turintys tokią prieigą prie mobilaus įrenginio gali keisti įrenginio nustatymus, įrašyti, paleisti programėles, keisti gamintojo uždraustas funkcijas [22].

1.8.5. Trojos arkliai

Tai kenkėjiškos programėlės, kurios bando apsimetinėti kitomis dažniausiai plačiai naudojamomis programėlėmis, taip pergudraujant vartotoją jas įrašyti į įrenginį. Įrašant programėlę ir ją paleidus, taip pat paleidžiamas ir kenkėjiškas kodas. Mobiliuose įrenginiuose nauja tendencija tapo

kenkėjiškų programėlių įrašymas po netikrų „phishing“ elektroninių laiškų gavimo iš apsimetamai bankinių įmonių. Taip programišiai bando pasisavinti bankinių prisijungimų bei mokėjimo kortelių duomenis.

1.9. Mobilių įrenginių rinkos pasiskirstymas

Tarptautinio duomenų centro duomenimis (2 lentelė), 87% išmaniųjų telefonų naudoja Android OS, likusieji 13% priklauso Iphone operacinei sistemai (iOS) [6]. Dar prieš dešimtį metų galėjome mobiliuose įrenginiuose pamatyti tokias operacines sistemas kaip Symbian, BlackBerry, Windows Phone, tačiau šiandieną operacinių sistemų paklausa primena monopolį.

2 lentelė. Mobilių įrenginių operacinių sistemų rinkos dalies pasiskirstymas. [6]

Metai	2017	2018	2019	2020	2021
Android	85,1%	85,1%	87%	87%	87,2%
iOS	14,7%	14,9%	13%	13%	12,8%
Kitos	0,2%	0%	0%	0%	0%

Toliau atsižvelgiant į mobilių įrenginių operacinių sistemų statistiką ir ateities prognozę, didžiausias dėmesys šiame darbe skiriamas Android OS.

1.10. Android OS programėlių apsaugos metodai

Norint apsaugoti Android OS naudojančiame mobiliajame įrenginyje esančias programėlės taikomi keletas metodų (3 lentelė):

3 lentelė. Mobilių įrenginių programėlių saugos metodai [3]

Programėlių pasirašymas	**Smėliadėžės**	**Leidimai**
Norint, jog programėlė būtų platinama oficialioje Android parduotuvėje, kiekviena programėlė turi būti pasirašoma	Smėliadėžės suteikia galimybę riboti programėlių prieigą prie mobiliame įrenginyje esančių duomenų	Kiekvienai programėlei kūrėjai turi aprašyti priskiriamus leidimus naudoti įrenginyje esančius duomenis. Šiuos leidimus vartotojas prieš įrašant programėlę turi patvirtinti.

1.10.1. Android OS programėlių karkasas ir pasirašymas

Nuo pat Android OS išleidimo 2008 m. ši operacinė sistema, tolygiai integravosi į mobilių prietaisų gamybos, vartotojų, ir programinės įrangos kūrėjų rinką. Jau 2015 m. ši operacinė sistema turėjo 83,1% rinkos, šiandieną šis skaičius siekia virš 87% (lentelė 1). Šie skaičiai lemia, kodėl ši operacinė sistema sulaukia daugiausia dėmesio ir piktavališkai nusiteikusių programišių.

Rašant programą Android OS sugeneruojama keletas APK variantų (debug, debug analigned, release, release signed, release unsigned). Debug versija ir release versija dauguma atvejų, dvejetainiais failais, resursais, manifest failais, tačiau išleista programa su sertifikatu arba be jo. Programa su parašu turės kelis papildomus failus (manifest.mf, cert.mf, cert.rsa) META-INF direktorijoje įrodančius sertifikatą. Tačiau programa be parašo negali būti instaliuota įrenginiuose naudojančiuose Android OS, nebent vartotojas turi specialią teisių (root) prieigą prie įrenginio.

Android programėlės gali būti rašomos Java, Kotlin, C++ kalbomis. Android SDK (angl. Software Development Kit), sukompiliuoja parašytą kodą su visais reikiamais, nurodytais failais į APK archyvo failą su .apk sufiksu. Šiame APK faile yra viskas ko reikia programėlei būti įrašytai įrenginyje. Programėlės rašymo stadijoje, naudojami kūrimo įrankiai taip nustato, kur yra kiti kodo komponentai. Sudedant visus reikiamus failus į APK failų archyvą, programėlės rašymo įrankiai pagal šį pavadinimą sugeneruoja unikalų programėlės numerį, kuris vėliau naudojamas atskirti programėlę tarp kitų sistemoje ir Android programėlių parduotuvėje. Kiekviena programėlė paleidžiama savo atskiroje virtualioje smėliadėžėje (angl. Sandbox), ši smėliadėžė yra sukuriama norint apsaugoti įrenginį nuo galimai piktavališkos programėlės.

Android OS – tai mobiliesiems įrenginiams skirta, atviro kodo, Google kompanijos kuriama Linux OS paremta operacinė sistema. Tai pilnai sukomplektuotas programinės įrangos dėklas (4 lentelė).

4 lentelė. Android programinės įrangos architektūra [4]

Programos			
Programų karkasas			
Bibliotekos			Programų vykdymo aplinka
Atvaizdavimo bibliotekos	Medijų karkasas	SQLite	Pagrindinės JAVA bibliotekos
OpenGL	FreeType	Webkit	Dalvik virtuali mašina
SGL	SSL	libb	
Linux OS			

Programinės Android OS įrangos kūrimo rinkinys, leidžiantis kurti programėles, yra Android SDK (angl. Software Development Kit). Šis rinkinys apima projektų kodą, kūrimo įrankius, bibliotekas, emuliatorius, reikalingus Android programėlėms kurti. Android OS programėlės kuriamos naudojant Java programavimo kalbą. Programėlės vykdomos specialiai šiam tikslui sukurtos dalvik virtualios mašinos (Dalvik Virtual Machine), veikiančios aukščiau Linux OS branduolio. Nepaisant modifikuoto Linux OS branduolio norint paspartinti Android OS spartumą bei efektyvumą mobiliuose įrenginiuose, ši sistema turi keletą bibliotekų ir tvarkyklių, kurios buvo modifikuotos arba visiškai pakeistos. Android OS pateikiama su keletu bazinių programų kaip kalendorius, kontaktai ir kt., kurias vartotojas gali valdyti iš karto įsijungus įrenginiui.

Programų karkasas (angl. Application Framework) (5 lentelė) pateikiamas su sąsajomis, funkcijomis ir sisteminėmis bibliotekomis, reikalingomis funkcionalioms programėlėms kurti. Jis sudarytas iš veiklų valdytojo (angl. Activity Manager) reglamentuojančio programėlių gyvavimo ciklą, turinio administratorių (angl. Content Providers), leidžiančių programėlių prieigą prie įrenginyje esančių duomenų arba leidžiančio dalytis savo duomenimis. Vaizdų sistemos (angl. Viev System), leidžiančios kurti programėlių vartotojo sąsajas, išteklių valdytojo (angl. Reource Manager), užtikrinančio prieigą prie išteklių, pranešimo valdytojo (angl. Notification Manager), užtikrinančio galimą prieigą prie išteklių, pranešimų valdytojo, įgalinančio programėles rodyti paskirtus pranešimus vartotojui.

5 lentelė. Programėlių karkaso architektūra [4]

Programėlių karkasas		
Veiklų valdytojas	Turinio administratoriai	Vaizdų sistema
Išteklių valdytojas	Pranešimų valdytojas	

Programėlių rašytojai, turi galimybę naudotis įrenginyje esančia aparatine įranga. Įranga leidžia gauti informaciją apie įrenginio buvimo vietą, paleisti paslaugas įrenginio fone, nustatyti įspėjamuosius pranešimus bei signalus būsenos juostoje [4]. Šis programėlių karkasas programėlių rašytojams suteikia visas galimybes kurti naujas ar papildyti bazines programėles. Visos Android OS programėlės yra parašytos naudojant Java programavimo kalbą, leidžiančią nesunkiai panaudoti vienai kitos komponentus.

Android OS integruota specialiai šiai operacinei sistemai pritaikytų C/C++ bibliotekų. Dėl galimų licenzijavimo konfliktų buvo priimtas sprendimas Android OS įdiegti nuosavą C biblioteką (bionic) ir sukurti specialią Java programėlių vykdymo aplinką, Dalvik virtualią mašiną. Pagrindinis kriterijus kuriant Android OS buvo infrastruktūros optimizavimas, kadangi mobilaus įrenginio fiziniai ištekliai riboti. Android OS naudoja specialią programos valdymo aplinką (angl. Android Runtime), susidedančią iš pagrindinių Java bibliotekų ir dalvik virtualios mašinos. Remdamasi Linux OS branduoliu ši aplinka veikia virš jos ir užtikrina sąveiką su žemo lygio technine įranga ir valdo programėlių atmintį bei procesų gyvavimo trukmę.

1.10.2. Smėliadėžė

Android OS paremta Linux operacine baze suteikia galimybę izoliuoti veikiančią programėlę nuo aplinkos, paleidžiant ją atskiroje virtualios mašinos smėliadėžėje. Tam atlikti Android priskiria unikalų numerį kiekvienai programėlei (UID) ir paleidžia ją atskirai, neleidžiant dalintis duomenimis su kitomis programėlėmis. OS branduolys (angl. Kernel) užtikrina reikiamą saugumą tarp programėlių ir komandų vykdymo branduolio lygmenyje. Standartiniame scenarijuje, programėlės negali komunikuoti viena su kita, ir turi ribotą prieigą prie OS. Kadangi programėlės smėliadėžė yra branduolio lygmenyje, šis apsaugos metodas gali apimti tiek mašininį Android OS kodą, tiek įrenginyje paleidžiamas programėles. Visi komponentai, esantys aukščiau branduolio lygmens, įskaitant, programėlių karkasą, operacinės sistemos bibliotekas, programėlių vykdymo aplinką paleidžiami šioje smėliadėžėje.

1.11. Baltojo ir juodojo programėlių sąrašų parametrai

Vienas iš atsineštinių mobilių įrenginių saugos politikos nuostatų yra leidžiamų ir draudžiamų įrenginyje vykdyti programėlių sąrašo sudarymas. Pagal NIST programėlių sąrašai gali būti taikomi atsižvelgiant į keletą faktorių [25]:

Kelias iki failo. Tai dažniausiai taikomas faktorius, leidžiantis vykdyti programėles, esančias tik tam tikroje direktorijoje. Tačiau naudojant kaip vienintelį faktorių, jis gan silpnas, nes patalpinus bet kokį failą į šią kategoriją, galimas saugumo pažeidimas. Dažniausiai tokioms direktorijoms yra taikomos prieigos kontrolės, leidžiančios tik autorizuotam administratoriui pridėti ar pakeisti ten esančius failus, taip sustiprinant apsaugą. Naudojant kelią iki failo galima sutaupyti resursų, jog nereikėtų nurodinėti kelio iki kiekvieno failo atsiradus naujai programėlei ar atnaujinimui.

Failo vardas. Šis faktorius per daug abstraktus bandant naudoti kaip vienetinį, nes piktavaliui išsiaiškinus kokios programėlės leidžiamos vykdyti įrenginyje, jis programėlę gali pavadinti tokiu pat vardu ir bandyti ją paleisti iš kitos direktorijos.

Failo dydis. Šis faktorius taip pat dažniausiai naudojamas kartu su kitais. Sekant failo dydį bandoma priimti išvadą, jog ta pati programa turinti papildomo kenkėjiško kodo turėtų užimti daugiau vietos. Tačiau piktavaliai gali sukurti programėlę naudojančią tiek pat atminties kaip ir pirminė. Kiti faktoriai, kaip parašai ar maišos funkcijos suteikia daug patikimesnį identifikavimą ir turėtų būti naudojami vietoj šio.

Skaitmeniniai parašai, leidėjai. Dauguma programėlių šiomis dienomis turi skaitmeninius parašus. Kai kurios operacinės sistemos neleidžia vykdyti programėlių jei jos nėra pasirašytos. Skaitmeninis parašas failui suteikia unikalią reikšmę, jog būtų galima patikrinti ar šis failas yra teisėtas ir nebuvo pakeistas. Tačiau programėlėms be skaitmeninio parašo šis faktorius negali būti taikomas, tad negali būti naudojamas kaip vienetinis. Kai kurie baltieji programėlių sąrašai gali būti taikomi atsižvelgiant į programėlių kūrėjo identifikavimą, pasikliaujant, jog kiekviena šio kūrėjo programėle galima pasitikėti [25]. Naudojant šį metodą išliktų galimybė vykdyti senesnės versijos programėles su žinomomis saugumo spragomis. Tačiau vienas iš pagrindinių privalumų naudojant programėlių leidėjus yra tai, jog baltąjį sąrašą reikia atnaujinti tik norint pridėti naują leidėją arba kai leidėjas atnaujina savo parašą.

Kriptografinė maiša. Kriptografinė maiša failui suteikia unikalią bei patikimą reikšmę, kol naudojama stipri kriptografija ir reikšmė susieta su patikimu failu jau žinoma. Kriptografinė maiša yra tiksli neatsižvelgiant į tai, kokioje direktorijoje yra šis failas, koks yra failo vardas, dydis ar skaitmeninis parašas. Tačiau atnaujinus programėlę maišos reikšmė pasikeičia, tad ji turi būti iš naujo pridėta į baltąjį sąrašą, dažniausiai atsižvelgiant į skaitmeninį parašą. Tačiau norint, jog būtų palaikomas aukšto lygio saugumas, senų versijų failai su žinomomis saugumo spragomis ir susietomis maišos reikšmėmis turi būti naikinami iš baltojo sąrašo.

Faktorių parinkimas sudarant programėlių baltuosius sąrašus, susijęs su balansu tarp apsaugos, priežiūros bei lengvo naudojimo. Paprastesni faktoriai, kaip failo vardas, dydis ar direktorija negali būti naudojami kaip vienetiniai, nebent įvedamos griežtos prieigos kontrolės. Faktorių kombinavimas su skaitmeniniais parašais ir kriptografine maiša baltajam sąrašui suteikia didžiausią apsaugą.

Mobiliajame įrenginyje esančias programėles ketinama skirstyti į juodą bei baltą sąrašus.

Programėlių apsaugos režimai

Dauguma programėlių sąrašų technologijų naudoja vieną iš dviejų operacinių režimų:

- Auditavimas – duomenys apie programėles esančias sąrašuose yra kaupiami registre, tačiau programėlės leidžiamos vykdyti;
- Vykdymas - tai režimas kurio metu programėles, esančias sąraše, leidžia vykdyti arba blokuoja, priklausomai nuo įmonės politikos:

Programėlės versija

Norint naudoti mobilų įrenginį darbo tikslais yra patikrinamos visos programėlės įrenginyje. Taip pat ir jų versija. Visos mobiliame įrenginyje naudojamos programėlės turi būti aptinkamos oficialioje android programėlių parduotuvėje. Mobiliame įrenginyje negali būti trečių šalių programėlių. Jei tokių programėlių aptinkama, dirbti su mobiliuoju įrenginiu neleidžiama. Kiekvienos programėlės versija patikrinama su oficialios android programėlių parduotuvės versija, jei versija nėra naujausia, klientas gauna pranešimą, apie būtiną programėlės atnaujinimą.

Programėlės parašas

Programėles pridėti į juodą arba baltą sąrašus galima naudojant parašus. Taip atsirastų galimybė leisti įrenginyje naudoti net ir senesnės versijos programėles, jei jos buvo sukurtos patikimo autoriaus arba atvirkščiai blokuoti visas nepatikimų autorių programėles.

Prototipe siūloma kurti auditavimo režimu, pagal numatytus saugos lygius atsižvelgiant į programėlių kategorijas ir jų prašomus leidimus. Darbuotojas atlikęs autentifikaciją atliktų Android įrenginio skenavimą ir gautų rezultatų išklotinę, leidžiančią naudotis įrenginiu arba neleidžiančią, su tolimesniais veiksmais norint tenkinti įmonės saugumo politiką.

1.11.1. Leidimai

Modernūs mobilieji įrenginiai paleidžiamų programėlių saugumą užtikrina taikydami smėliadėžes. Tačiau parduotuvėse daugelis programėlių prašo, jog joms būtų suteikta daugiau leidimų, nei būtina atlikti savo funkcijas [7]. Tačiau perteklinis leidimų prašymas, ne visada reiškia tikslingą duomenų kaupimą - tai gali būti spraga programuotojo žiniose, kaip naudojami programėlėms skirti leidimai. Kartais, programėlių kūrėjams lengviau, paprašyti perteklinio kiekio leidimų, jog programėlės turėtų mažiau galimybių neveikti. Dėl to didėja tikimybė leidimus panaudoti piktavališkai.

Plačiau tai aptariama 2.5 skyriuje.

1.12. Rinkoje egzistuojančių MDM platformų funkcionalumas

Mobilių įrenginių valdymo rinka nenustos augti. Rinkoje egzistuoja daugelis įmonių, siūlančių mobilių įrenginių valdymo technologijas. Rinkoje pirmaujančių produktų funkcionalumas aprašytas 6 lentelėje.

6 lentelė. Rinkoje lyderiaujančių atsineštinių mobilių įrenginių p.į. palyginimas

Funkcija	**Citrix**	**Airwatch**	**Mobile iron**	**Seven principles**
IMEI būsena	✓	✓	✓	✓
Baterijos būsena	✓	✓	✓	✓
GPS vieta	✓	✓	✓	✓
OS versija	✓	✓	✓	✓
Įrenginio gamintojas ir modelis	✓	✓	✓	✓
Tinklo informacija	✓	✓	✓	✓
Vartotojų grupių administravimas	✓	✓	✓	✓
Kiosk režimas	✓	✓	✓	✓
Konteinerizacija	✓	✓	✓	✓

Funkcija	Citrix	Airwatch	Mobile iron	Seven principles
Slaptažodis	✓	✓	✓	✓
Įrenginio užrakinimas	✓	✓	✓	✓
Įrenginio atkūrimas	✓	✓	✓	✓
Šifravimas	✓	✓	✓	✓
Kenkėjiškų programų aptikimas			✓	✓
Root/nulaužto įrenginio aptikimas	✓	✓	✓	✓
Atskiras VPN programėlei			✓	
Duomenų pašalinimas	✓	✓	✓	✓
Kelių žingsnių autentifikacija	✓	✓	✓	
Programėlių įrašymas	✓	✓	✓	✓
Juodasis/baltasis sąrašas	✓	✓	✓	✓
Programėlės naudojimosi įrašai	✓	✓	✓	
Nuotolinė prieiga	✓	✓	✓	✓
Pranešimai	✓	✓	✓	✓

6 lentelėje buvo nagrinėta Android OS MAM skirti sprendimai. Visa populiariausia programinė įranga mobilių įrenginių programėlių valdymui gali pasiūlyti įvairių operacijų palaikymą bei pagrindines funkcijas kaip IMEI būsenos peržiūrą, reikalingą įsitikinti jog įrenginys priklauso atitinkamam asmeniui, operacinės sistemos būseną, reikalingą, jog dažniausiai norint asmeniniame įrenginyje dirbti su įmonės duomenimis, būtų užtikrintas sklandus darbas su programėlėmis bei saugumas, nuotolinį mobilaus įrenginio užrakinimą ar duomenų pašalinimą, skirtą apsaugoti duomenis dingus įrenginiui. Taip pat visos nagrinėtos programinės įrangos siūlo duomenų atkūrimą ir duomenų šifravimą. Šifravimo algoritmai: Airwarch: AES 256, SHA 512, TLSv1, RSA 1024; Mobile ironL SHA 256, AES 256, RSA 2048; Citrix: AES-256. Android OS MAM skirti sprendimai siūlo konteinerizaciją, atskiriant vykdomąją vietą nuo likusio mobilaus įrenginio. Visos programinės įrangos gali pasiūlyti nuotolinį programėlių įrašymą ir pašalinimą bei juodą ir baltą programėlių sąrašus, reikalingus norint leisti ar blokuoti pagal įmonės saugos politiką nepageidaujamas programėles. Citrix programinė įranga ir Airwatch programinė įranga negali pasiūlyti integruoto kenkėjiškų programėlių aptikimo, vienintelė iš visų nagrinėtų programų, Mobile Iron programinė įranga, gali pasiūlyti VPN atskiroms programėlėms. Beveik visos gali pasiūlyti kelių žingsnių autentifikaciją saugumo sustiprinimui ir nuotolinę prieigą prie įrenginio.

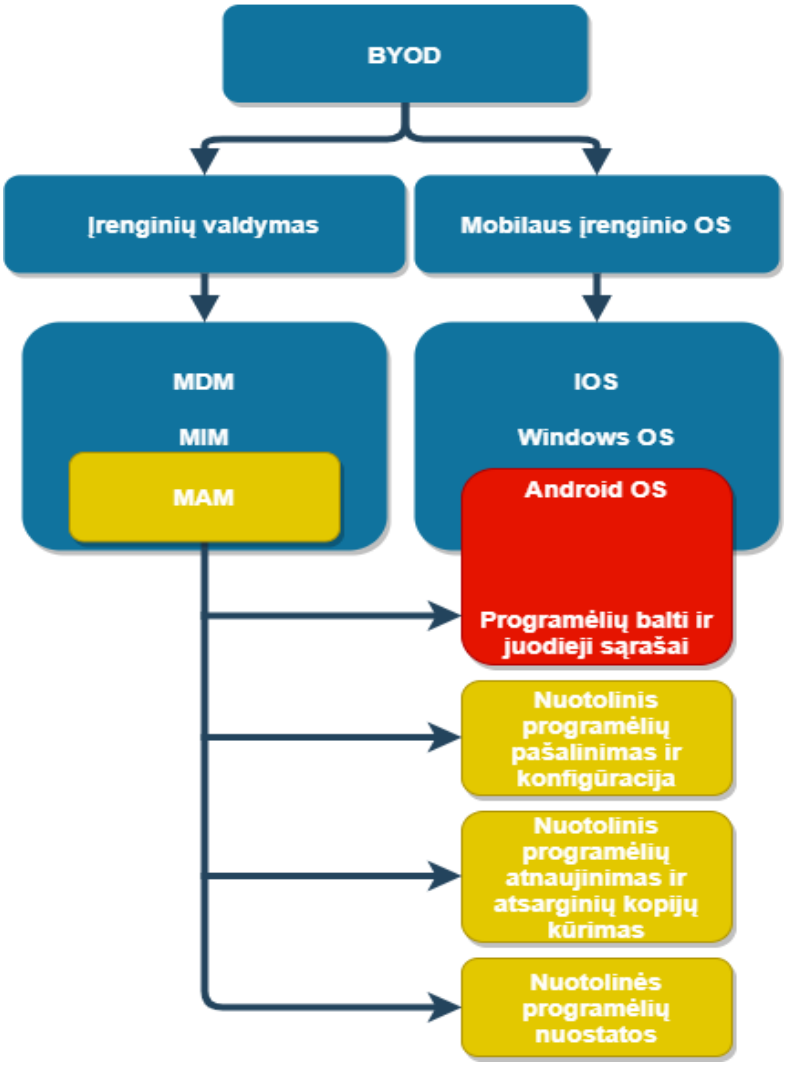
1.13. Analizės išvados

1. Darbe buvo išanalizuotas organizacijose naudojamų asmeninių įrenginių konceptas, kylančios grėsmės ir saugumą užtikrinantys diegimo, techniniai, politikos, reguliavimo bei žmogiškieji iššūkiai bandant įvesti šią praktiką.
2. Buvo išanalizuoti trys asmeninių įrenginių organizacijose saugumo modeliai: mobilių įrenginių valdymas (MDM), mobilių programėlių valdymas (MAM), mobilios informacijos valdymas (MIM), šių modelių gairės. Taip pat kokia kenkėjiška veikla gali kelti grėsmę BYOD konceptui.
3. Buvo išanalizuoti Android OS apsaugos modeliai: OS karkasas, smėliadėžė ir leidimai.

4. Buvo palyginti rinkoje egzistuojantys organizacijose naudojamų asmeninių įrenginių saugos politikos valdymo sprendimai.

2. Organizacijose naudojamų asmeninių įrenginių saugos politikos valdymo modelis

BYOD iniciatyvoje dalyvauja daugybė mobiliųjų įrenginių su skirtingomis operacinėmis sistemomis (Android OS, Iphone OS, Windows OS) bei šiems įrenginiams galimų taikyti skirtingų apsaugos valdymo sprendimų (MDM, MAM, MIM). 1.9 skyriuje minima, jog didžiąją mobilių įrenginių rinkos dalį užima Android OS, tad šio darbo metu nuspręsta pasirinkti šią operacinę sistemą ir MAM (angl. Mobile Application Management) įrenginių valdymo sprendimą.



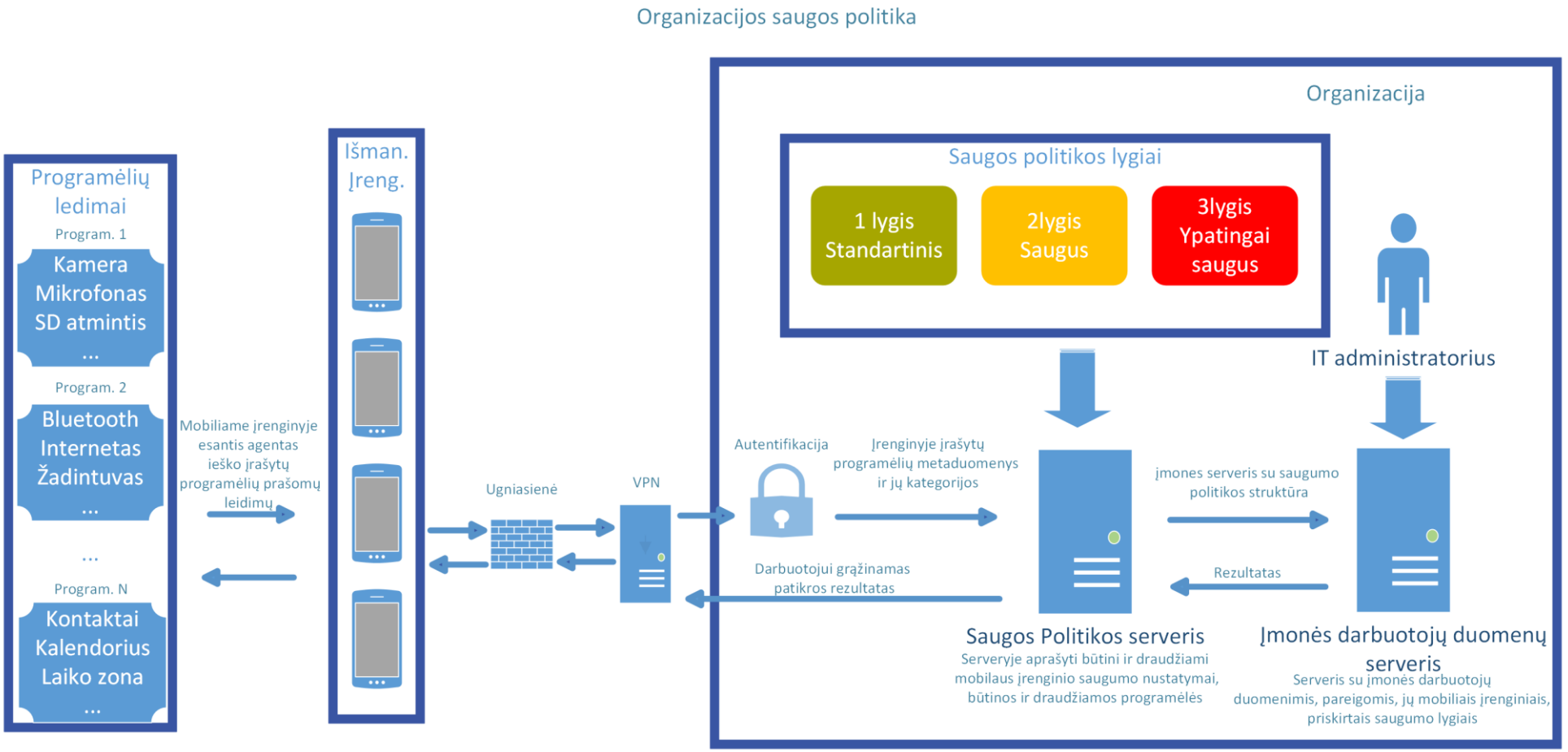
7 pav. Mobilių įrenginių valdymo modelis

Kenkėjiškų programų skaičiui bei įvairovei augant kasdien antikenkėjiškų programų kūrėjai ir programišiai bando surasti naujų būdų įveikti vienas kitą. Gynyba nuo piktavališkų programėlių, blokuojant žinomas kenkėjiškas programėles vadinamas juoduoju sąrašu (angl. Blacklisting), tačiau naudojant šį apsaugos metodą reikalinga kenkėjiškų programėlių duomenų bazė arba metodika šį sąrašą sudaryti. Šis metodas, taip pat, neapgina nuo dar nežinomo kenkėjiško kodo varianto ar nulinės dienos (angl. zero-day attack) atakų. Valdžios institucijos bei korporacijos yra pagrindinis piktavališkai nusiteikusių asmenų taikinys, siekiant pasisavinti slaptą ar jautrią visuomenei informaciją. Kai per daugelį metų operacinės sistemos tapo vis atsparesnės įsilaužimams, atakos pakrypo nuo operacinių sistemų link programėlių, taip pagrindiniu vektoriumi į tinklo vidų tapo individualūs asmenys įrenginiuose, turintys tam tikras programėles. Programėlių baltieji sąrašai

(angl. Whitelisting) yra kitas apsaugos prieš piktavalius metodas. Naudojant šį metodą sukuriamas programėlių, kurias gali paleisti atitinkamas įrenginys, visos kitos programėlės yra automatiškai blokuojamos. Tarkime, jei asmuo gauna phishing el. laišką su piktavališku adresu, kurį atidarius į įrenginį būtų įrašomas kenkėjiškas kodas, ar atidaro failą, kuris išnaudoją failo tipo spragą ir automatiškai bando vykdyti kenkėjišką kodą, piktavališki ketinimai būtų nevaisingi, nes programėlės nebūtų baltuose sąrašuose. Baltieji programėlių sąrašai apsunkina užpuolikų bandymus patekti į tinklą ar įrenginį, nes jie turi išnaudoti vienos iš baltuosiuose sąrašuose esančios programėlės trūkumus ar sukompromituoti patį baltąjį sąrašą. Net jei leidžiama vykdyti įrenginyje programėlė būtų išnaudota, tolimesni piktavališki veiksmai gali būti toliau blokuojami baltuoju sąrašu. Baltieji sąrašai neturėtų pakeisti tradicinės apsaugos programinės įrangos, tačiau tai galėtų būti vienas iš papildomų sluoksnių apsaugai nuo piktavalių. Norint jog programėlių baltieji sąrašai būtų efektyvūs reikia [24]:

- Esant normaliems nustatymams bet koks vykdomas kodas turi būti blokuojamas, jei jo nėra baltajame sąraše.
- Vartotojai negali paleisti programėlių iš direktorijų, kuriose jie gali saugoti failus.
- Vartotojai negali turėti administratoriaus teisių.

Šiame darbe pasiūlytą mobilių įrenginių apsaugos modelį sudarys išmanieji mobilūs įrenginiai, kurie priklausys kiekvienam darbuotojui ir bus registruojami įmonės DB, šie įrenginiai turės įdiegtą saugumo politikos patikros klientą, kuris patikrins įrenginyje esančias programėles, kokiai kategorijai jos priklauso, kokių leidimų reikalauja programėlės ir šį sąrašą grąžins įmonės saugos politikos serveriui. Serveris nuskaitys gautus duomenis, ir pagal darbuotojo pareigybes ir priskirtą saugumo lygį tikrins ar naudojamas įrenginys tenkina įmonės saugos politiką ir grąžins rezultatus atgal į mobilų įrenginį. Sekančiuose skyriuose aptarsime šiuos žingsnius plačiau.



8 pav. Mobilių įrenginių apsaugos politikos modelis

2.1. Saugumo politikų sudarymas

Saugumo politikos tikslas ir nauda

Įmonėje privalo būti vykdoma saugi BYOD politika norint užtikrinti nežalingą prieigą prie įmonės duomenų. Mobilūs įrenginiai nėra pririšti prie vietos, jais galima naudotis iš bet kurios pasaulio vietos, tad dažnu atveju mobilūs įrenginiai reikalauja sustiprintos apsaugos, nes į juos gali kėsintis papildomos grėsmės nuo kurių apsaugo tradicinės apsaugos priemonės įmonės fizinės infrastruktūros vietose ir tinkluose. Saugumo politika yra sudaroma norint užtikrinti maksimalų privatumą ir konfidencialumą bei sumažinti galimas rizikas tyčiniams ar netyčiniams pažeidimams. Ši saugumo politika apima reikiamas procedūras, praktikas, draudimus kiekvienam įmonės darbuotojui, kuris turi pagrįstą tikslą disponuoti įmonės duomenimis. Ši saugumo politika taikoma visiems asmeniniams įrenginiams, išmaniesiems telefonams, planšetėms, kompiuteriams su Android OS, kurie nori disponuoti įmonės duomenimis.

Ši politika skirta įvairioms grėsmėms arba sąsajomis su įmonės naudojamais duomenimis:

7 lentelė. Galimos mobiliu įrenginiu disponuojančiu informacija grėsmės

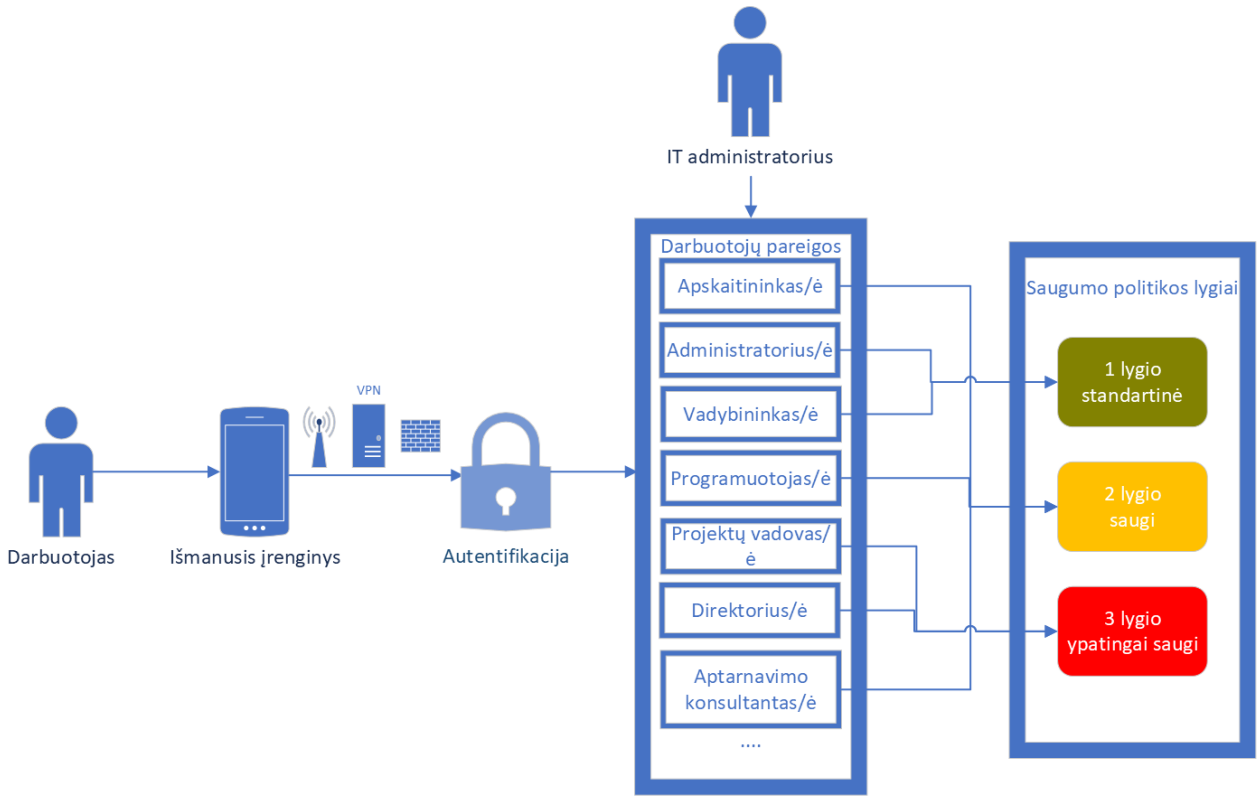
Grėsmė	**Aprašymas**
Praradimas	Mobilaus įrenginio pametimas.
Vagystės	Mobilaus įrenginio vagystė.
Kenkėjiškos programos	Virusai, trojanai, kirminai, šnipinėjimo programos.
Atsakomybė	Apginti tiek įmonės darbuotojų, tiek įmonės interesus, esant įvairių tapatybės, vagystės ir privatumo įstatymų nesilaikymo.
Informacijos nutekėjimas	Privačių įmonės duomenų nutekėjimas, tai informacija neadresuotiems asmenims.
Darbuotojų žinių stoka	Nepakankamas darbuotojų švietimas įrenginių ir duomenų apsaugai.

2.2. Darbuotojų grupių administravimas

Saugumo politika įtraukia visus įmonėje dirbančius darbuotojus, įskaitant akcininkus, savanorius, laisvai samdomus darbuotojus, naudojančius asmeninius mobilius įrenginius pasiekti, įrašyti, atkurti ar kitaip perteikti bet kokius su įmone ar jos darbuotojais susijusius duomenis. Visi su įmonės duomenimis dirbantys asmenys yra suskirstomi į tris saugumo lygius, pagal jų užimamas pareigas ir atsakomybes.

Norint naudoti asmeninį išmanųjį telefoną disponuojant privačiais darbovietei priklausančiais duomenimis, visų pirma, reikia įvertinti su kokiais duomenimis darbuotojas gali dirbti. Duomenys skirti marketingo tikslams ar darbuotojų dienotvarkės gal ir nėra tokie jautrūs įmonei, tačiau apskaitos, klientų, finansiniai duomenys, yra labai jautrūs ir netgi gali būti ginami įstatymų. Žemesnio lygio darbuotojo, priklausomai nuo jo pareigybių, įmonei jautri informacija gali niekad nepasiekti, tad jam nebus pasiūlyta taikyti tokio pat lygio saugos politiką, kaip su asmens duomenimis dirbančiam žmogiškųjų išteklių darbuotojui, buhalteriams ar vadovams.

Šiame darbe pasiūlyta sudaryti metodiką pagal kurią įrenginys pagal darbuotojo užimamas pareigas bus priskiriamas vienai iš 3 saugumo lygių politikai.



9 pav. Darbuotojų grupių pagal pareigybes sudarymas

Darbuotojas naudodamas išmanųjį mobilų įrenginį, interneto prieigą ir virtualų privatų tinklą, jungiasi prie įmonės saugumo patikros serverio, atlikdamas autentifikaciją iš anksto jam suteiktais prisijungimo duomenimis. Šiuos duomenis IT administratorius jau būna priskyręs prie pareigybių grupės DB saugos politikoje, kurios atitinkamai priklauso priskirtam saugumo lygiui.

8 lentelė. Pasiūlyti saugumo lygiai

Saugumo lygis - pavadinimas	**Darbuotojų pareigos**
1 lygio – standartinė.	Administratoriai, vadybininkai, reklamos specialistai, ...
2 lygio – saugi.	Viešųjų ryšių specialistai, žmogiškųjų išteklių specialistai, pardavimų specialistai, klientų aptarnavimo specialistai, ...
3 lygio – ypatingai saugi.	Akcininkai, apskaitininkai, direktoriai, padalinių vadovai, komandų vadovai, IT administratoriai, ...

2.3. Programėlių leidimai

Mobilios programėles leidimai klasifikuojami į [26]:

Įprastuosius - tai tokie leidimai, kurių gaunami duomenys nepriklauso programėlės vidinėms funkcijoms, tačiau nekeliančių didelio pavojaus vartotojo privatumui. Jei šie leidimai nurodomi Manifest faile, sistema juos suteikia automatiškai be vartotojo žinios. Kadangi šie leidimai, pagal Android politiką neypatingi, vartotojai negali jų atšaukti įrašius programėlę.

Pavojingi - priešingai nei įprastieji, šie leidimai įspėja vartotojq, jog bus naudojami privatūs ar kitų programėlių duomenys. Šie leidimai yra parodomi vartotojui prieš įdiegiant programėlę ir

suteikiami tik vartotojui tą leidus. Vartotojui nesuteikus tokios prieigos programėlė neįrašoma. Vartotojas šiuos leidimus gali atšaukti netgi po programėlės įrašymo.

Pasirašomieji - sistemoje šie leidimai yra suteikiami tik tokioms programėlėms, kurios pasirašomos naudojant ta patį sertifikato raktą kaip ir programėlės apibrėžiančios leidimus. Tarpusavyje duomenimis komunikuojančios programėlės privalo turėti tokį pat raktą. Programėlės sukurtos nepriklausomų kūrėjų gali naudoti ne visus šiai kategorijai priklausančius leidimus. Šiame darbe išrinkti tik tie leidimai kuriuos gali naudoti trečių šalių programėlės.

Specialūs - taip pat yra 2 leidimai priskiriami itin pavojingiems, dėl šių leidimų prieinamos informacijos jautrumo. Leidimas gali būti suteikiamas Manifest faile, prieš suteikiant šį leidimą vartotojui pateikiama, informacija dėl šio suteikto leidimo galimybių bei grėsmių. Trečių šalių programėlės šių leidimų naudoti negali.

Leidimų sąrašą sudaro programėlės kūrėjas atsižvelgiant į programėlės funkcionalumą, visus leidimus nurodydamas ANDROID MANIFEST faile.

Šiame darbe pasiūlytas leidimų grupavimas pagal jų funkcijas į Lx grupes (9 lentelė):

L1 – Leidimai susiję su mobilaus įrenginio užrakto nustatymais, ekrano ir darbuotojo sąveika, įrenginio įjungimu.

L2 – Leidimai turintys prieigos (angl. access) teises. Programėlės turinčios šiuos leidimus gali gauti prieigą prie įrenginio vietos nustatymų, tinklo būsenos, perspėjimų politikos.

L3 – Leidimai turintys įrenginio nustatymų pakeitimo (angl. change) teises. Programos su šiomis teisėmis gali keisti mobilaus įrenginio tinklo nustatymus, atidaryti portus, keisti garso nustatymus, įrenginio sinchronizaciją.

L4 – Leidimai turintys skaitymo (angl. read) teises. Programėlės gali skaityti įrenginio sinchronizavimo nustatymus ir rezultatus.

L5 – Leidimai galintys nustatyti (angl. set) žadintuvo, laiko zonos, ekrano užsklandos nustatymus.

L6 – Leidimai galintys paprašyti baterijos optimizavimo bei programėlių paketų (trump. APK) įrašymo į įrenginį, įrašyti greituosius priėjimus.

L7 – Leidimai leidžiantys programėlėms ieškoti ir suporuoti bluetooth įrenginius, naudoti infraraudonųjų spindulių įrangą bei valdyti vibravimo nustatymus, bluetooth ryšį, netolimų elektromagnetinių bangų ryšį (angl. Near Field Communication).

L8 – Leidimai leidžiantys išskleisti įrenginio statuso lauką, peržiūrėti paketo dydį, užbaigti įrenginio RAM atmintyje sulaikytas programėles, pertvarkyti užduotis.

L9 – Leidimai galintys gauti informaciją apie įrenginio vietą.

L10 – Leidimai turintys skaitymo (angl. read) teises. Programėlės gali perskaityti mobilaus įrenginio kalendoriaus įrašus, įrenginio būseną, adresų knygos numerius, išorinę atmintį, trumpąsias žinutes, skambučių žurnalą, ir kontaktus.

L11 – Leidimai turintys rašymo teises. Programėlės gali įrašyti kalendoriaus, adresų, skambučių žurnalo, balso žinučių ir išorinės atminties, bluetooth nustatymus.

L12 – Leidimai susiję su įrenginio fiziniais davikliais ir būsena. Programėlės, turinčios šiuos leidimus, gali įrašyti įrenginiu garsą, naudoti kamerą, įrenginiu nustatyti asmens kūno duomenis bei fizinę veiklą, aptikti aplinkinius įrenginius.

L13 – Leidimų grupė susijusi su žinutėmis, ir leidžianti priimti trumpąsias SMS, MMS, WAP žinutes.

L14 – Leidimų grupė susijusi su komunikacija. Programėlės, turinčios šiuos leidimus, gali rinkti, skambinti, atsiliepti, peradresuoti skambučius, siųsti trumpąsias SMS žinutes.

L15 – Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti baterijos nustatymus, įrenginio prieinamumo funkcijas.

L16 – Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti automatinio užbaigimo, nenaudojamo įrenginio ekrano, ekrano atvaizdavimu, gaunamais duomenimis, spausdinimu, ekrano dalinimusi, balso valdymu.

L17 – Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti perspėjimais, ekrano užsklandomis, ištrinti laikinos talpyklos failus, virtualios realybės funkcijomis.

L18 – Leidimų grupė leidžianti programėlėms prašyti įrašyti paketus, valdyti dokumentus, išorinę įrenginio atmintį, įrenginio naudojimo informaciją, valdyti mediją.

L19 – Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti, NFC funkcijomis, virtualiu privačiu tinklu.

L20 – Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti įrenginio nustatymais, admin teisėmis bei tikrinti įrenginio identifikaciją.

L21 – Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti skambučiais, žinutėmis, balso paštu, operatoriaus paslaugomis.

9 lentelė. Android OS suteikiami leidimai [26]

Įprastieji leidimai	**Pavojingi leidimai**	**Pasirašomieji leidimai**	**Specialūs leidimai**
L1 USE_FINGERPRINT; DISABLE_KEYGUARD; WAKE_LOCK; RECEIVE_BOOT_COMPLETED; USE_BIOMETRIC; USE_FULLSCREEN_INTENT;	L9 ACCESS_FINE_LOCATION; ACCESS_COARSE_LOCATION; ACCESS_BACKGROUND_LOCATION; ACCESS_MEDIA_LOCATION;	L15 BIND_ACCESSIBILITY_SERVICE; BATTERY_STATS; BIND_QUICK_ACCESS_WALLET_STATS;	SYSTEM_ALERT_WINDOW; WRITE_SETTINGS;
L2 ACCESS_LOCATION_EXTRA_COMMANDS; ACCESS_NETWORK_ST	L10 READ_CALENDAR; READ_PHONE_STATE; READ_PHONE_NUMBE	L16 BIND_AUTOFILL_SERVICE; BIND_CHOOSER_TARG	

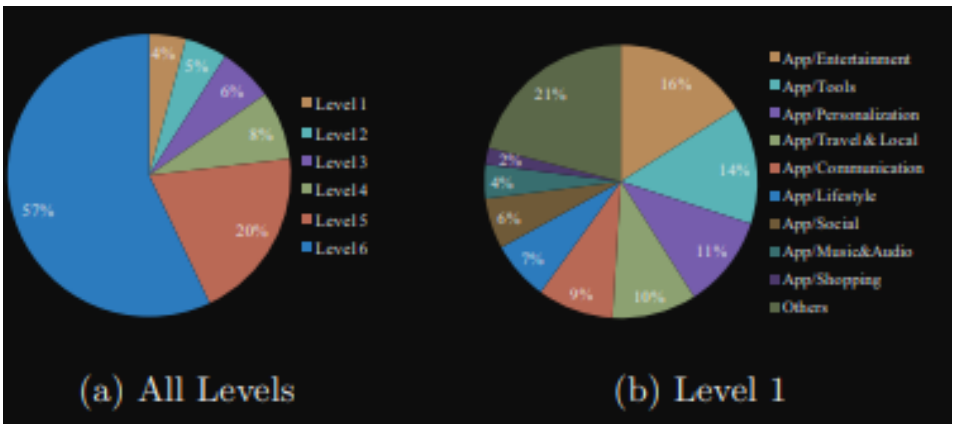
Įprastieji leidimai	Pavojingi leidimai	Pasirašomieji leidimai	Specialūs leidimai
ATE; ACCESS_NOTIFICATION_POLICY; ACCESS_WIFI_STATE;	RS; READ_EXTERNAL_STORAGE; READ_SMS; READ_CALL_LOG; READ_CONTACTS; READ_MEDIA_AUDIO; READ_MEDIA_VIDEO; READ_MEDIA_IMAGE; GET_ACCOUNTS;	ET_SERVICE; BIND_DREAM_SERVICE; BIND_INPUT_METHOD; BIND_MIDI_DEVICE_SERVICE; BIND_PRINT_SERVICE; BIND_SCREENING_SERVICE; BIND_TEXT_SERVICE; BIND_VOICE_INTERACTION; CHANGE_CONFIGURATION;	
L3 CHANGE_NETWORK_STATE; CHANGE_WIFI_MULTICAST_STATE; CHANGE_WIFI_STATE; WRITE_SYNC_SETTINGS; MODIFY_AUDIO_SETTINGS; INTERNET;	L11 WRITE_CALENDAR; WRITE_CONTACTS; WRITE_EXTERNAL_STORAGE; WRITE_CALL_LOG; ADD_VOICEMAIL; NEARBY_WIFI_DEVICES; POST_NOTIFICATION; BLUETOOTH_ADVERTISE ; BLUETOOTH_CONNECT; BLUETOOTH_SCAN;	L17 CLEAR_APP_CACHE; SYSTEM_ALERT_WINDOW; BIND_NOTIFICATION_LISTENER_SERVICE; BIND_WALLPAPER; BIND_TV_INPUT; DELETE_CACHE_FILES; BIND_VR_LISTENER_SERVICE;	
L4 READ_SYNC_SETTINGS; READ_SYNC_STATS;	L12 RECORD_AUDIO; CAMERA; BODY_SENSORS; ACTIVITY_RECOGNITION; UWB_RANGING;	L18 REQUEST_INSTALL_PACKAGES; MANAGE_DOCUMENTS; LOADER_USAGE_STATS; MANAGE_EXTERNAL_STORAGE; MANAGE_MEDIA;	
L5 SET_ALARM; SET_TIME_ZONE; SET_WALLPAPER; SET_WALLPAPER_HINTS; VIBRATE;	L13 RECEIVE_SMS; RECEIVE_WAP_PUSH; RECEIVE_MMS;	L19 BIND_CONDITION_PROVI;DER_SERVICE; BIND_VPN_SERVICE; BIND_NFC_SERVICE;	
L6 REQUEST_IGNORE_BATTERY_OPTIMIZATIONS;	L14 CALL_PHONE; ANSWER_PHONE_CALLS;	L20 BIND_DEVICE_ADMIN; USE_ICC_AUTH_WITH_DE;	

Įprastieji leidimai	Pavojingi leidimai	Pasirašomieji leidimai	Specialūs leidimai
REQUEST_INSTALL_PACKAGES; INSTALL_SHORTCUT; FOREGROUND_SERVICE; QUERY_ALL_PACKAGES;	SEND_SMS; PROCESS_OUTGOING_CALLS; ACCEPT_HANDOVER;	VICE_IDENTIFIER; WRITE_SETTINGS;	
L7 BLUETOOTH_ADMIN; BROADCAST_STICKY; TRANSMIT_IR; NFC; BLUETOOTH; NFC_PREFERRED_PAYMENT_INFO; HIGH_SAMPLING_RATE_SENSOSRS; NFC_TRANSACTION_EVENT;		L21 READ_VOICEMAIL; WRITE_VOICEMAIL; BIND_VISUAL_VOICEMAIL_SERVICE; BIND_INCALL_SERVICE; BIND_CARRIER_SERVICES; BIND_TELECOM_CONNECTION_SERVICE;	
L8 EXPAND_STATUS_BAR; GET_PACKAGE_SIZE; KILL_BACKGROUND_PROCESSES; REORDER_TASKS; UNINSTALL_SHORTCUT; CALL_COMPANION_APP; REQUEST_COMPANION_RUN_IN_BACKGROUND; REQUEST_PASSWORD_COMPLEXITY;			

2.4. Programėlių kategorijos

Saugos politikoje kiekvienam saugumo lygiui priskirtos draudžiamų programėlių kategorijos.

Pagal tyrime [27] gautus rezultatus, kuriame buvo ištirtos 170,753 programėlės iš „Google Play“ programėlių parduotuvės, diagramoje a matome visas programėles suklasifikuotas pagal saugumo lygį nuo kenkėjiškiausių (1 lygio) iki saugiausių (6 lygio), diagramoje b matome nesaugiausio pagal kenkėjiškumą programėlių kategorijų pasiskirstymą, iš kurių eilės tvarka sudaro Pramogos (angl. Entertainment) 16%, Įrankiai (angl. Tools) 14%, Personalizacija (angl. Personalization) 11%, Kelionės ir gidai (angl. Travel and Local) 10%, Komunikacija (angl. Communication) 9%, Gyvensena (angl. Lifestyle) 7%, Socialinės (angl. Social) 6%, Muzika ir įrašai (angl. Music and Audio) 4%, Apsipirkimas (angl. Shopping) 2% ir kitos (angl. Others) 21%. Stiprėjant įmonės saugos politikos lygiui daugėja ir draudžiamų kategorijų kiekis.



10 pav. GooglePlay parduotuvėje esančiose kategorijose randamų pažeidžiamumų skaičius [27]

Prototipe pasiūlyta sudaryti įrenginyje esančių nesisteminių programėlių sąrašą. Kiekviena programėlė turi jai unikalų paketo identifikatorių, dažniausiai atrodantį taip - COM.xxxx.xxxx..

Kiekviena programėlė parduotuvėje turi unikalų Android programėlių parduotuvės adresą (angl. URL). Konkrečiai programėlei URL sudaromas sekančiai:

10 lentelė. URL sudarymas muzikos leistuvei Spotify

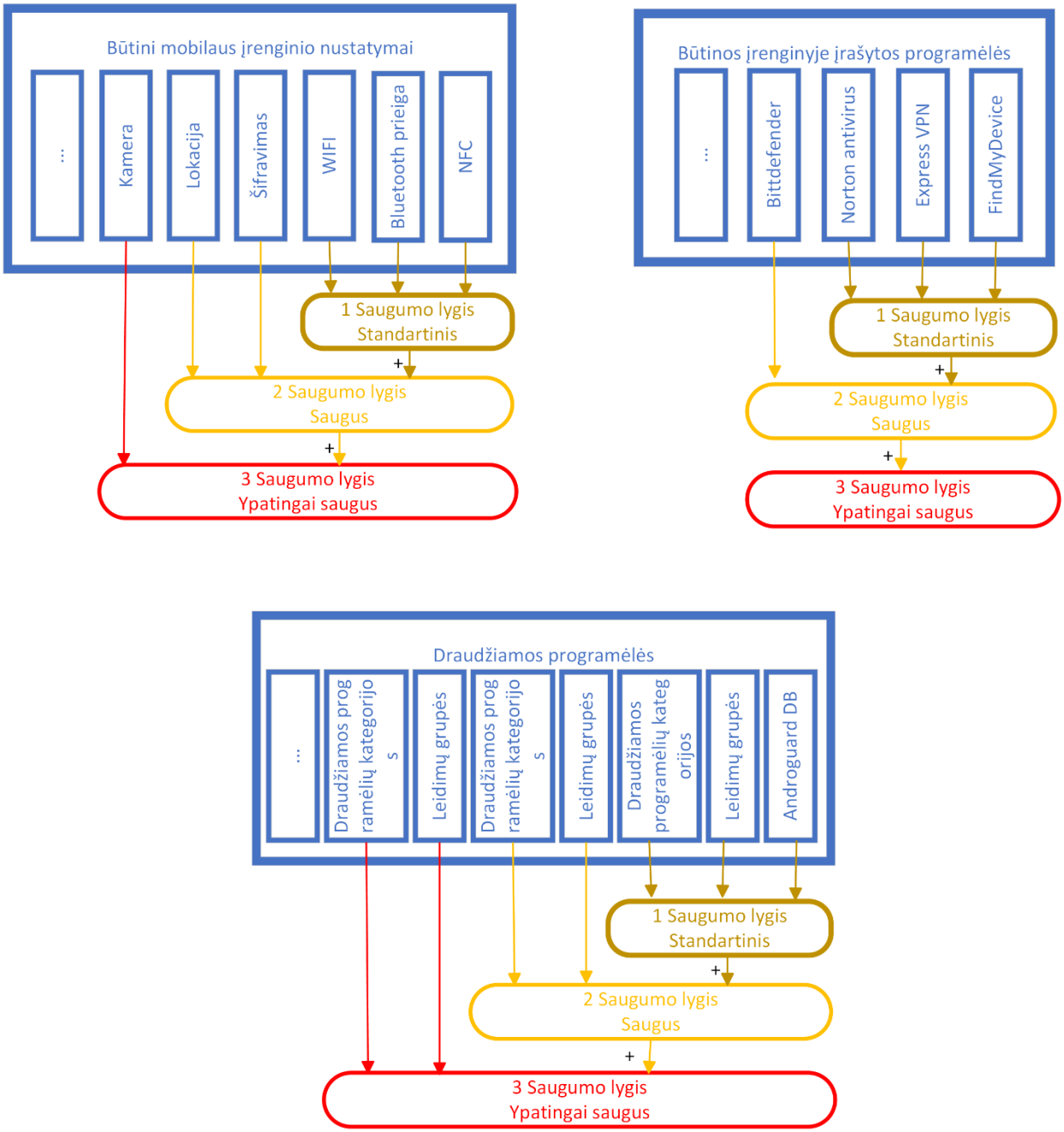
Saugus (SSL) kliento ir serverio komunikacijos protokolas	**Nekintanti domeno konstanta**	**Kintanti URL dalis (paketo identifikatorius)**
https://	play.google.com/store/apps/details?id=	com.spotify.music

Išgavus įrenginyje esančių programėlių sąrašą ir žinant programėlės URL, sudaroma užklausa norint nustatyti jai priklausančią kategoriją. Tam naudojama JSOUP JAVA biblioteka, skirta darbui su HTML duomenimis. Sudarant HTTP užklausą, pagal HTML DOM struktūrą ir pagal CSSQuerry užklausą galima surasti kokiai kategorijai yra priskirta programėlė. Ši informacija naudojama generuoti įrenginio ataskaitai.

```
class="hrTbp R8zArc">Spotify AB</a></span><span class="T32cc UAO9ie"><a itemprop="genre" href="/store/apps/category/MUSIC_AND_AUDIO"
```

11 pav. Muzikos programėlės Spotify HTML kodo vieta, kur randama kategorija

2.5. Saugos politikos lygių sudarymas



12 pav. Saugumo politikos lygių sudarymas

Įmonės saugumo politika sudaroma iš būtinų mobilaus įrenginio nustatymų, draudžiamų ir būtinų įrenginyje esančių programėlių bei darbuotojų ir jų pareigybių. Kiekvieno saugumo lygio politikos taisyklės aprašytos sekančiame poskyryje.

Konkrečių pareigybių darbuotojas priklausantis (8 lentelė) nurodytam saugumo lygiui kartu su asmeniniu darbe naudojamu įrenginiu privalo užtikrinti toliau nurodytas, jam konkrečias saugumo

taisykles. Griežtėjant saugumo lygiui, griežtėja ir prieš tai buvusiame saugumo lygyje esančios arba pritaikomos papildomos taisyklės.

11 lentelė. Saugumo politikos lygiai ir taisyklės

Saugumo lygis	Taisyklės
1.	1. Pirmo saugos lygio taisyklės 1.1. Įrenginys ketinantis naudotis įmonės duomenimis privalo būti įtrauktas į IT skyriaus patvirtintų mobilių įrenginių sąrašą. 1.2. Mobilus įrenginys turi naudoti Express VPN p.į., esant būtinybei jungtis prie įmonės vidinio tinklo. 1.3. Asmuo prieš pradėdamas darbą su mobiliu įrenginiu privalo autentifikuotis įmonės suteiktais prisijungimo duomenimis ir sugeneruoti patikros rezultatų ataskaitą. 1.4. Naudojama WIFI prieiga turi naudoti WEP, WPA 1/2/3 saugumo protokolą. 1.5. Mobilus įrenginys turi turėti ekrano užraktą – piršto antspaudą/veido bruožų patikrą/tiesių seką/skaitmenis. 1.6. Nesijungti prie žiniatinklio svetainių neturinčių SSL/TLS sertifikato. 1.7. Mobiliame įrenginyje turi veikti automatinio užsirakinimo funkcija. 1.8. Mobilus įrenginys negali būti nulaužtas (angl. Jailbreak.) ir veikti Root teisėmis. 1.9. Įrenginyje privalo būti įrašyta „Avast antivirus“ antivirusinė p. į. 1.10. Programėlių valdymo politika neleidžia darbo metu turėti šių kategorijų programėlių: 1.10.1. Pramogos 1.11. Mobiliajame įrenginyje esančioms programėlėms neleidžiama naudoti šių grupių leidimų (lentelė 8): 1.11.1. L20 - Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti įrenginio nustatymais, admin teisėmis bei tikrinti įrenginio identifikaciją. 1.11.2. L21 - Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti skambučiais, žinutėmis, balso paštu, operatoriaus paslaugomis.
2.	1. Antro saugos lygio taisyklės 1.1. Įrenginys ketinantis naudotis įmonės duomenimis privalo būti įtrauktas į IT skyriaus patvirtintų mobilių įrenginių sąrašą. 1.2. Mobilus įrenginys turi naudoti Express VPN p.į., esant būtinybei jungtis prie įmonės vidinio tinklo. 1.3. Asmuo prieš pradėdamas darbą su mobiliu įrenginiu privalo autentifikuotis įmonės suteiktais prisijungimo duomenimis ir sugeneruoti patikros rezultatų ataskaitą. 1.4. Naudojama WIFI prieiga turi naudoti WPA 2/3 saugumo protokolą. 1.5. Įrenginys turi turėti ekrano užraktą įvedant 6 skirtingus skaitmenis, arba 8 simbolių žodį su didžiąja raide, skaitmeniu ir neraidiniu simboliu/piršto antspaudą/veido bruožų patikrą. 1.6. Mobiliame įrenginyje turi veikti automatinio užsirakinimo funkcija. 1.7. Mobilus įrenginys negali būti nulaužtas (angl. Jailbreak.) ir veikti Root teisėmis. 1.8. Mobilus įrenginys turi turėti įjungtą įrenginio disko šifravimo funkciją. 1.9. Mobiliu įrenginiu neskenuoti greitos prieigos (QR) kodų. 1.10. Leisti naudoti GPS lokaciją tik navigacijos kategorijai priklausančioms programėlėms. 1.11. Nesijungti prie žiniatinklio svetainių neturinčių SSL/TLS sertifikato. 1.12. Bluetooth prieigos nustatymus pakeisti į privačius. 1.13. Įrenginyje turi būti įrašyta ir nuolatos veikti Bittdefender p. į. 1.14. Įrenginyje privalo būti įrašyta „Avast antivirus“ p. į. 1.15. Įrenginyje privalo būti įrašyta fizinės įrenginio paieškos vietos p.į „FindMyDevice“. 1.16. Programėlių valdymo politika leidžia darbo metu turėti šių kategorijų programėles: 1.16.1. Pramogos

Saugumo lygis	Taisyklės
	1.16.2. Įrankiai 1.16.3. Personalizacija 1.16.4. Kelionės ir gidai 1.17. Mobiliajame įrenginyje esančioms programėlėms neleidžiama naudoti šių grupių leidimų (lentelė 8): 1.17.1. L3 – Leidimai turintys įrenginio nustatymų pakeitimo (angl. change) teises. Programos su šiomis teisėmis gali keisti mobilaus įrenginio tinklo nustatymus, atidaryti portus, keisti garso nustatymus, įrenginio sinchronizaciją. 1.17.2. L13 – Leidimų grupė susijusi su žinutėmis, ir leidžianti priimti trumpąsias SMS, MMS, WAP žinutes. 1.17.3. L14 – Leidimų grupė susijusi su komunikacija. Programėlės turinčios šiuos leidimus gali rinkti, skambinti, atsiliepti, peradresuoti skambučius, siųsti trumpąsias SMS žinutes. 1.17.4. L18 - Leidimų grupė leidžianti programėlėms prašyti įrašyti paketus, valdyti dokumentus. 1.17.5. L20 - Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti įrenginio nustatymais, admin teisėmis bei tikrinti įrenginio identifikaciją. 1.17.6. L21 - Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti skambučiais, žinutėmis, balso paštu, operatoriaus paslaugomis.
3.	1. Trečio saugos lygio taisyklės 1.1. Įrenginys ketinantis naudotis įmonės duomenimis privalo būti įtrauktas į IT skyriaus patvirtintų mobilių įrenginių sąrašą. 1.2. Mobilus įrenginys turi naudoti Express VPN p.į., esant būtinybei jungtis prie įmonės vidinio tinklo. 1.3. Neaktyvi kamera. 1.4. Asmuo prieš pradėdamas darbą su mobiliu įrenginiu privalo autentifikuotis įmonės suteiktais prisijungimo duomenimis ir sugeneruoti patikros rezultatų ataskaitą. 1.5. Naudojama WIFI prieiga turi naudoti WPA 2/3 saugumo protokolą. 1.6. Įrenginys turi turėti ekrano užraktą įvedant 10 simbolių žodį su didžiąja raide, skaitmeniu ir neraidiniu simboliu/piršto antspaudą. 1.7. Mobilus įrenginys turi turėti įjungtą irenginio disko šifravimo funkciją. 1.8. Įrenginyje negali būti įrašyta jokių su žaidimais susijusių programėlių. 1.9. Mobiliu įrenginiu neskenuoti greitos prieigos (QR) kodų. 1.10. Mobiliame įrenginyje turi veikti automatinio užsirakinimo funkcija. 1.11. Mobilus įrenginys negali būti nulaužtas (angl. Jailbreak.) ir veikti Root teisėmis. 1.12. Nesijungti prie žiniatinklio svetainių neturinčių SSL/TLS sertifikato. 1.13. Vietos nustatymus laikyti išjungtus, nebent to reikalauja specifinė su darbu susijusi funkcija. 1.14. Suaktyvinti NFC technologiją įrenginyje tik norimai užduočiai atlikti, ir po atlikimo šią technologiją laikyti išjungtą. 1.15. Bluetooth prieigos nustatymus pakeisti į privačius. 1.16. Leisti naudoti GPS lokaciją tik navigacijos kategorijai priklausančioms programėlėms. 1.17. Įrenginyje turi būti įrašyta ir nuolatos veikti Bittdefender p. į. 1.18. Įrenginyje privalo būti įrašyta „Avast antivirus“ p. į. 1.19. Įrenginyje privalo būti įrašyta fizinės įrenginio paieškos vietos p.į „FindMyDevice“. 1.20. Programėlių valdymo politika leidžia darbo metu turėti šių kategorijų programėles: 1.20.1. Pramogos 1.20.2. Įrankiai 1.20.3. Personalizacija 1.20.4. Kelionės ir gidai

Saugumo lygis	Taisyklės
	1.20.5. Komunikacija 1.20.6. Gyvensena 1.20.7. Socialinės 1.21. Mobiliajame įrenginyje esančioms programėlėms neleidžiama naudoti šių grupių leidimų (lentelė 8): 1.21.1. L3 – Leidimai turintys įrenginio nustatymų pakeitimo (angl. change) teises. Programos su šiomis teisėmis gali keisti mobilaus įrenginio tinklo nustatymus, atidaryti portus, keisti garso nustatymus, įrenginio sinchronizaciją. 1.21.2. L7 – Leidimai leidžiantys programėlėms ieškoti ir suporuoti bluetooth įrenginius, naudoti infraroudonųjų spindulių įrengą bei valdyti vibravimo nustatymus, bluetooth ryšį, netolimų elektromagnetinių bangų ryšį (angl. Near Field Communication). 1.21.3. L9 – Leidimai galintys gauti informaciją apie įrenginio tikslią ar abstrakčią vietą. 1.21.4. L10 – Leidimai turintys skaitymo (angl. read) teises. Programėlės gali perskaityti mobilaus įrenginio kalendoriaus įrašus, įrenginio būseną, adresų knygos numerius, išorinę atmintį, trumpąsias žinutes, skambučių žurnalą, ir kontaktus. 1.21.5. L13 – Leidimų grupė susijusi su žinutėmis, ir leidžianti priimti trumpąsias SMS, MMS, WAP žinutes. 1.21.6. L14 – Leidimų grupė susijusi su komunikacija. Programėlės turinčios šiuos leidimus gali rinkti, skambinti, atsiliepti, peradresuoti skambučius, siųsti trumpąsias SMS žinutes. 1.21.7. L16 - Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti automatinio užbaigimo, nenaudojamo įrenginio ekrano, ekrano atvaizdavimu, gaunamais duomenimis, spausdinimu, ekrano dalinimusi, balso valdymu. 1.21.8. L18 - Leidimų grupė leidžianti programėlėms prašyti įrašyti paketus, valdyti dokumentus. 1.21.9. L19 - Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti, NFC funkcijomis, virtualiu privačiu tinklu. 1.21.10. L20 - Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti įrenginio nustatymais, admin teisėmis bei tikrinti įrenginio identifikaciją. 1.21.11. L21 - Leidimų grupė leidžianti programėlėms per telefono sistemines funkcijas manipuliuoti skambučiais, žinutėmis, balso paštu, operatoriaus paslaugomis.

2.6. Įrenginiuose naudojamų programėlių klasifikavimas

Jeigu telefone įrašytai programėlei nėra galimybės būti priskirtai jokiai kategorijai, programėlė negali būti įrašyta į įrenginį darbo metu. Norint turėti šią programėlę įrenginyje, reikia perduoti šią programėlę įmonės IT saugos departamentui, kur atsakingi asmenys peržiūrės programėlę nuodugniai, ir šiai programėlei esant saugiai, patalpins programėlės versiją į leidžiamų įrenginiuose programėlių sąrašą.

Įrenginyje darbo metu neleidžiama turėti programėlių kurios neatitinka saugumo politikoje aprašytų taisyklių.

Atlikus mobilaus įrenginio programėlių tikrinimą ir konkrečiai programėlei neatitikus duomenų bazėje nurodytų leidimų grupės, ši programėlė bus patalpinama į neleistinų programėlių sąrašą. Esant būtinybei naudoti programėlę darbo tikslais reikia taip pat kreiptis į IT saugos departamentą ir

prašyti patalpinti šią programėlę į baltąjį sąrašą. Įrenginyje galima blokuoti ir visas konkrečiai kategorijai priklausančias programėles.

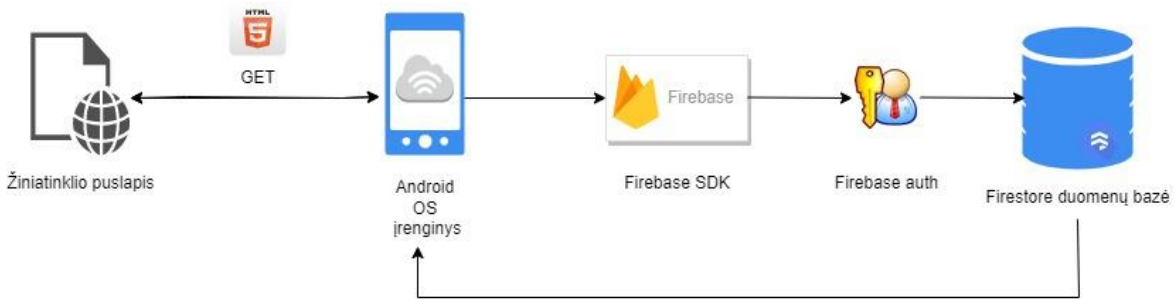
2.7. Išvados

1. Prototipo modelio siūlomoje stadijoje pasirinktas vienas iš BYOD iniciatyvos variacijos modelis – programėlių skirstymas į baltuosius ir juoduosius sąrašus pagal programėlės kategoriją ir programėlės prašomus suteikti leidimus.
2. Buvo aprašytas saugumo politikos tikslas ir nauda, ir pasiūlytas mobilių įrenginių apsaugos politikos modelis.
3. Buvo pasiūlyta kaip vykdyti darbuotojų grupių administravimą, kaip sudaryti saugumo politikos lygius, atsižvelgiant į šaltinius ir ten aprašytus pavojus duomenims, buvo priimtas sprendimas grupuoti programėlių prašomus leidimus ir programėlių kategorijų tipus, pagal grėsmę, juos priskiriant draudžiamų veiksmų sąrašui įmonės saugos politikoje.
4. Šiame skyriuje buvo aprašyti veiksmai kurie privalo būti užtikrinti norint tenkinti 3 skirtingus įmonės saugumo politikos lygius.

3. Organizacijose naudojamų asmeninių įrenginių saugos politikos valdymo tyrimas

Tyrimo dalies prototipas bus realizuotas naudojant Java programavimo kalbą ir Android Studio p.į.

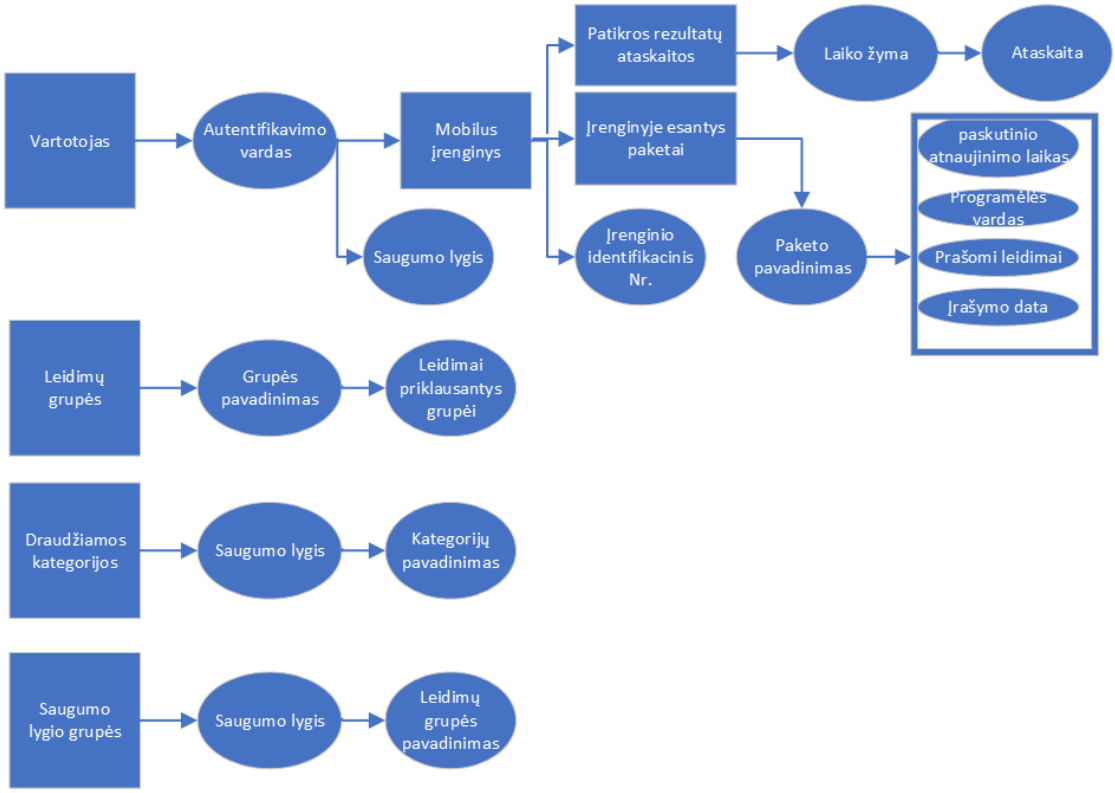
Prototipo architektūra bus realizuojama (13 pav.) naudojant Android įrenginio emuliatorių, skirtą sukurti virtualų įrenginio atvaizdą skirtą prototipo testavimui, žiniatinklio puslapį skirtą ieškoti ir išgauti duomenims naudojant CSSquery užklausas ir parsisiunčiant bei apdirbant duomenis pagal HTML DOM formatą. Firebase SDK p.į. kuri bus naudojama kaip duomenų bazė sudarant duomenų bazės saugumo politikos struktūrą, ir kaip darbuotojos modulis.



13 pav. Numatoma prototipo architektūra

3.1. Saugumo politikos duomenų struktūra

Šiame prototipe yra naudojama ne reliatacinė, dokumentų rinkinių tipo duomenų bazė (14 pav). Duomenų bazė sudaryta iš keturių pagrindinių kolekcijų. Vartotojo kolekcijoje saugomas dokumentas su prisijungimo prie programėlės darbuotojo vardu, pavarde, pareigybėmis, kuriame yra dokumentas su darbuotojui priskirtu saugumo lygiu. Šis dokumentas turi darbuotojo naudojamų mobilių įrenginių kolekciją, kurioje yra dokumentas su mobilaus įrenginio IMEI numeriu, patikros rezultatais ir įrenginyje esančių paketų kolekcijomis. Ataskaitų kolekcijoje saugomas dokumentas su laiko žyma ir įrenginio patikros metu sugeneruota ataskaita. Įrenginio paketų kolekcijoje saugomi dokumentai su mobiliame įrenginyje esančiais paketais. Antrą pagrindinę leidimų grupės kolekciją sudaro dokumentas su grupės pavadinimu ir jai priklausančių leidimų sąrašu. Trečią pagrindinę kolekciją sudaro draudžiamos programėlių kategorijos, kurioje yra saugumo lygio dokumentai su programėlių kategorijų pavadinimais. Ketvirtąją kolekciją sudaro saugumo lygio grupės, kurią sudaro saugumo lygio dokumentai ir juose priskirti leidimų grupių pavadinimai.



14 pav. Dokumentų rinkinių ir saugomų duomenų struktūra

12 lentelė. Kolekcija „vartotojas“

Prisijungimo vardas	**Darbuotojo vardas**	**Darbuotojo pavardė**	**Darbuotojo pareigybės**	**Priskirtas saugumo lygis**	**Kolekcija: mobilus įrenginys**
PetrasPetraitis@email.com	Petras	Petraitis	buhalteris	2	Kolekcija: mobilus įrenginys
..	...	...	...	...	Kolekcija: mobilus įrenginys
Jonasjonaitis@email.com	Jonas	Jonaitis	vadybininkas	1	Kolekcija: mobilus įrenginys

13 lentelė. Kolekcija „mobilus įrenginys“

Įrenginio pavadinimas	**IMEI**	**Kolekcija: ataskaitos**	**Kolekcija: įrenginyje esantys paketai**
LG-H873	154686568...	Kolekcija: ataskaitos	Kolekcija: įrenginyje esantys paketai
..	...	...	...
Samsung A52	254852123...	Kolekcija: ataskaitos	Kolekcija: įrenginyje esantys paketai

14 lentelė. Kolekcija „draudžiamos kategorijos“

Saugumo lygis	**Kategorija Nr. 1**	**Kategorija Nr. 2**	**Kategorija Nr. 3**	**Kategorija Nr. 4**	**Kategorija Nr. ...**
1	Pramogos	-	-	-	-
..	...	...	...	...	...

3	Pramogos	Įrankiai	Personalizacija	Kelionės ir gidai	...

15 lentelė. Kolekcija „ataskatos“

Laiko žyma	**Ataskaita**
Patikros data	Ataskaitos turinys
..	...
Patikros data	Ataskaitos turinys

16 lentelė. Kolekcija „leidimų grupės“

Leidimų grupė	**Leidimo Nr. 1 pavadinimas**	**Leidimo Nr. 2 pavadinimas**	**Leidimo Nr. 3 pavadinimas**	**Leidimo Nr. 4 pavadinimas**	**Leidimo Nr. ... pavad.**
L1	android.permission.USE_FINGERPRINT	android.peramission.DISABLE_KEYGUARD	android.permission.WAKE_LOCK	android.permission.RECEIVE_BOOT_COMPLETED	...
..	...	...	...	...	...
L21	android.permission.READ_VOICEMAIL	android.permission.WRITE_VOICEMAIL	android.permission.BIND_INCALL_SERVICE	android.permission.BIND_CARRIER_SERVICES	....

17 lentelė. Kolekcija „saugumo lygis“

Saugumo lygis	**Leidimų grupė Nr. 1**	**Leidimų grupė Nr. 2**	**Leidimų grupė Nr. 3**	**Leidimų grupė Nr. 4**	**Leidimų grupė Nr. ...**
1	L20	L21	-	-	-
2	L3	L13	L14	L18	...
3	L3	L7	L9	L10	...

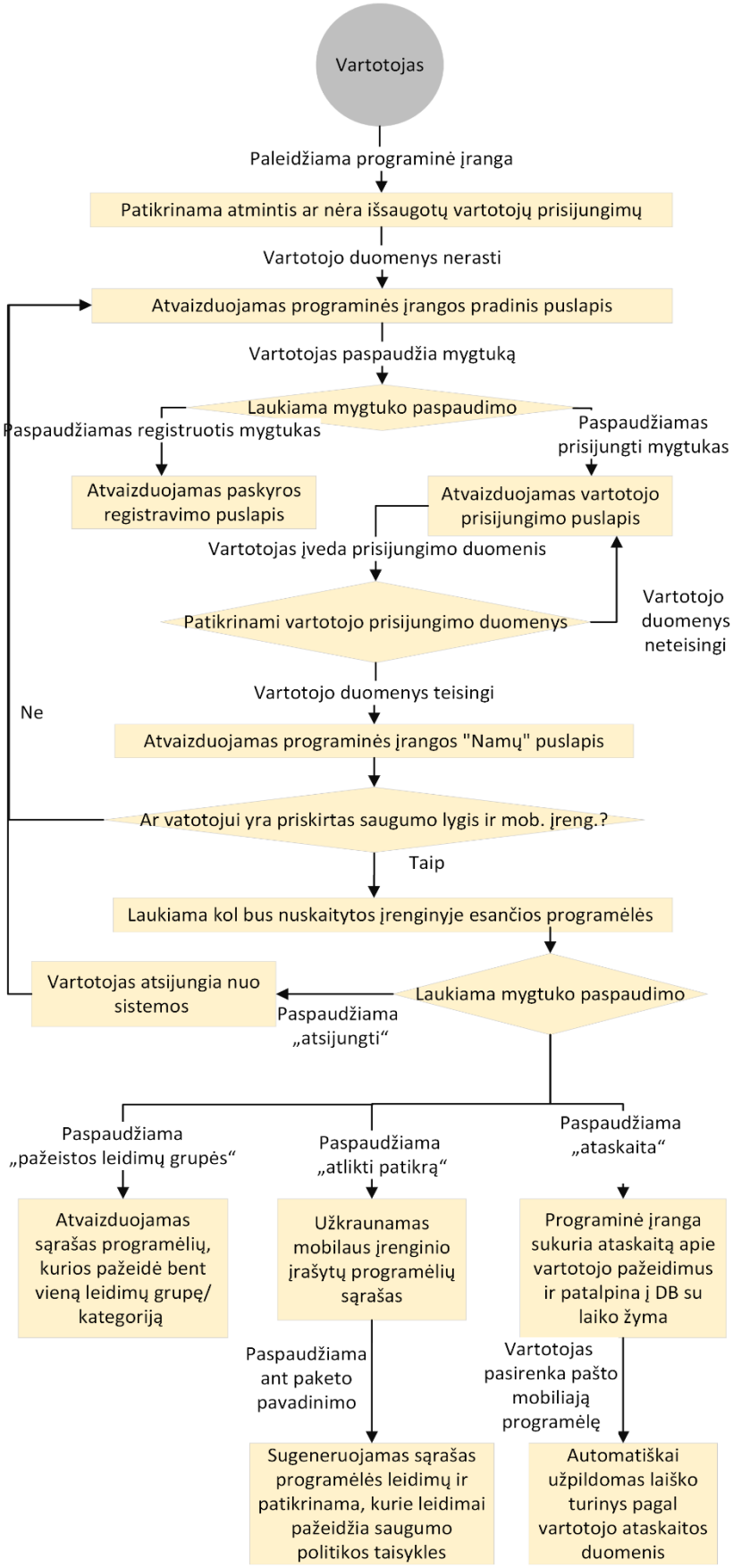
18 lentelė. Kolekcija „įrenginyje esantys paketai“

Laiko žyma	**Paketo pavadinimas**	**Kategorija**	**Prašomas leidimas**	**Prašomas leidimas ...**
Patikros data	Viber	Social	android.permission.WAKE_LOCK	...
..	...	...	...	...
Patikros data	Whatsapp	Social	android.permission.INTERNET	...

3.2. Realizuoto prototipo algoritmas

Toliau matome prototipo veikimo algoritmo schemą (15 pav.). Darbuotojui paleidus programinę įrangą patikrinama ar nėra atmintyje išsaugotų prisijungimo duomenų. Duomenų neradus, atvaizduojamas pradinis programinės įrangos puslapis. Darbuotojui paspaudus prisijungimo mygtuką vyksta nukreipimas į langą su autentifikavimosi duomenimis. Šių duomenų neturint vartotojas gali pasirinkti registracijos mygtuką ir susikurti paskyrą. Suvedus duomenis į prisijungimo laukus ir paspaudus mygtuką prisijungti, tikrinama ar darbuotojui su šiais duomenimis, administratorius DB saugumo politikos taisyklėse yra priskyręs saugumo lygį.

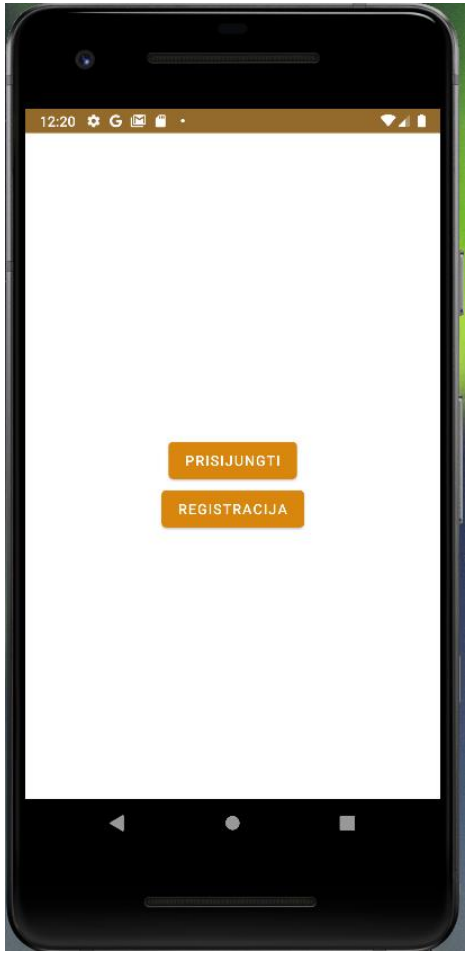
Saugumo lygiui nesant, darbuotojas grąžinamas į pradinį programėlės langą. Saugumo lygiui esant, tikrinama ar mobilaus įrenginio IMEI egzistuoja DB ir yra priskirtas šiam darbuotojui. Toliau darbuotoją pasitinka pagrindinis programėlės ekranas. Laukiama, kol programinė įranga nuskaitys įrenginyje esančias programėles ir pasirodys pranešimas „programinė įranga tinkama darbui“. Pagrindiniame ekrane darbuotojas turi pasirinkimą spaudžiant mygtuką „atlikti patikrą“, sąraše atvaizduoti įrenginyje esančius paketus, pasirinkus vieną iš jų atsiranda langas su šio paketo prašomais leidimais ir kurie leidimai pažeidžia saugumo politikos taisykles. Kitas mygtukas pagrindiniame ekrane „pažeistos leidimų grupės“, kuris grąžina visą sąrašą programėlių kurios pažeidžia draudžiamas leidimų grupes. Kitas mygtukas pagrindiniame ekrane „ataskaita“, sugeneruoja automatinę ataskaitą su paketais, kurie pažeidžia saugumo politikoje draudžiamas programėlių kategorijas, ir paketais kurių prašomi leidimai pažeidžia įmonės saugos politikoje draudžiamas leidimų grupes. Pagrindiniame ekrane paspaudus mygtuką „atsijungti“ vartotojas atsijungia nuo sistemos ir yra grąžinamas į pradinį ekraną.



15 pav. Organizacijose naudojamų asmeninių įrenginių saugos politiko valdymo diagrama

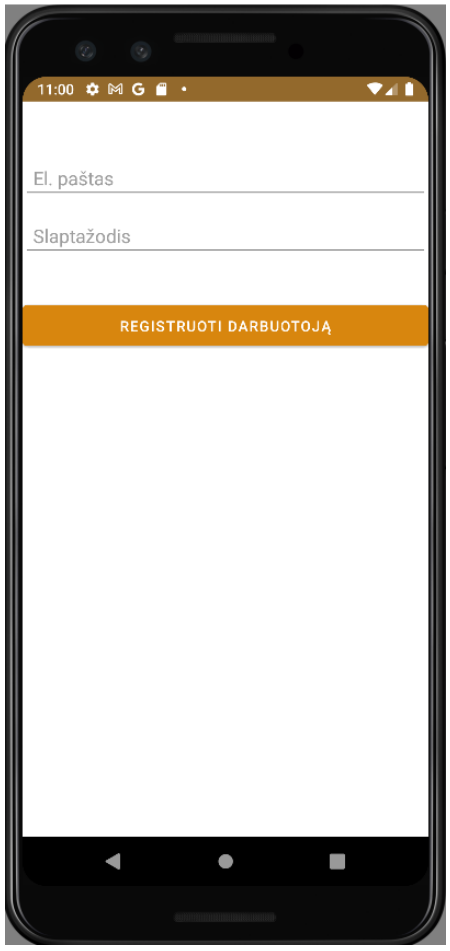
3.3. Realizuotas prototipas

Šiame prototipe buvo realizuotas mobiliame įrenginyje esančių trečių šalių programėlių tikrintojas, patikrinantis įrenginyje esančias programėles ir jų prašomus leidimus. Buvo realizuotas būdas išgauti įrenginyje esančių programėlių kategorijas naudojant oficialią „Google play“ programėlių parduotuvę. Prototipe buvo naudojama Firebase SDK ir FireStore duomenų bazė, atsakinga už vartotojų autentifikaciją, įrenginio registraciją, ir programėlių patikrinimo politikos realizaciją. Paleidus prototipą startuoja paleidimo langas (13 pav.) su prisijungimu darbuotojo duomenimis (14 pav.) arba naujo darbuotojo registracija (15 pav.). Atlikus autentifikaciją startuoja pagrindinis ekranas (16 pav.), kurio viršutinėje dalyje matome prisijungusį darbuotoją, jam priskirtą saugumo lygį bei draudžiamas leidimų grupes. Turime galimybę pasirinkti patikros atlikimo funkciją (17 pav.), kuri grąžina įrenginyje įrašytus paketus. Iš sąrašo galime pasirinkti ir individualiai peržiūrėti kiekvieno paketo leidimus ir saugumo politikos pažeidimus (20 pav.). Funkcija „pažeistos leidimų grupės“ ekrane atvaizduoja įrenginyje įrašytų paketų sąrašą ir kurios leidimų grupės yra pažeidžiamos (18 pav.). Pagrindiniame ekrane, taip pat yra funkcija „Ataskaita“, kuri automatiškai sugeneruoja tekstinę ataskaitą, patalpina į duomenų bazę su laiko žyma ir tolimesne galimybe ją persiųsti elektroniniu paštu (19 pav.). Ataskaitoje pateikiami programėlių paketų pavadinimai, saugumo politiką neatitinkantys leidimai, leidimų grupės, programėlių kategorijos, su tolimesniais veiksmais darbui su įrenginiu.

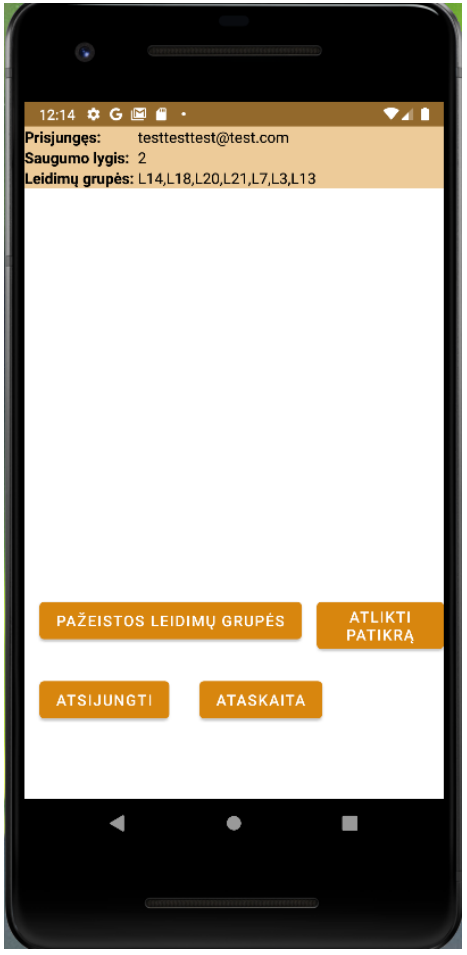


16 pav. Prisijungimo langas

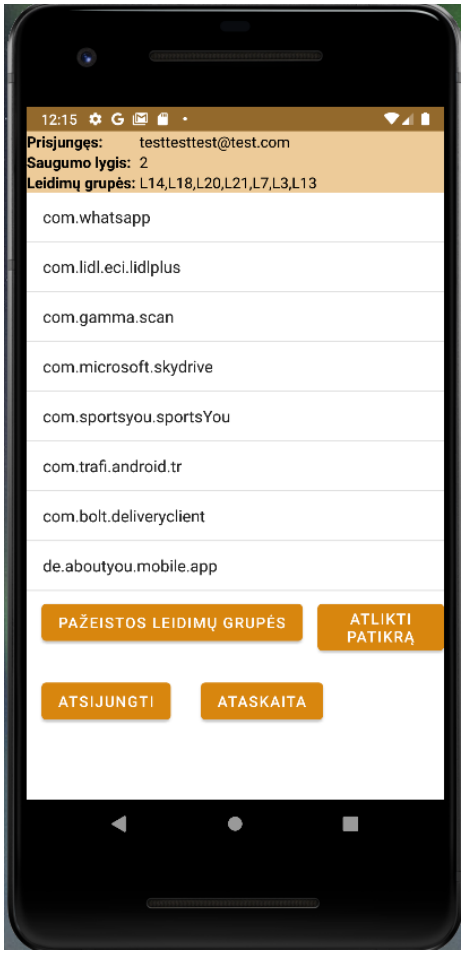
17 pav. Autentifikacijos langas



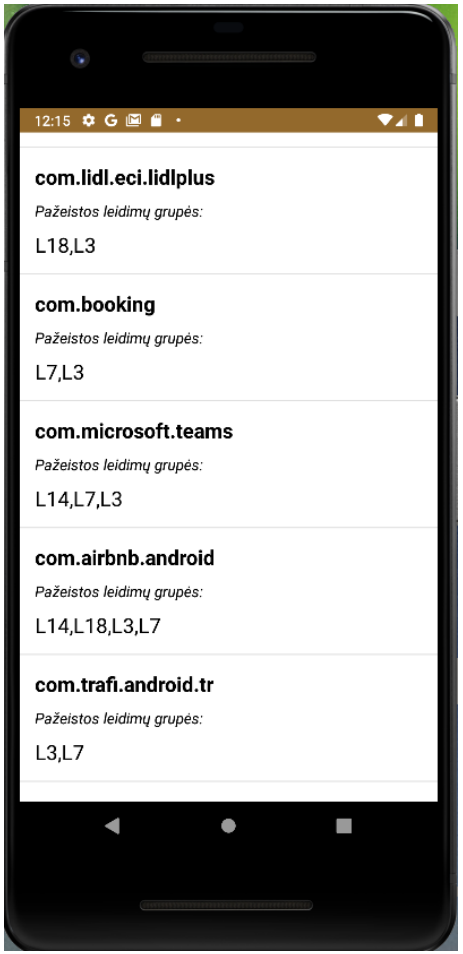
18 pav. Registracijos langas



19 pav. Pagrindinis ekranas

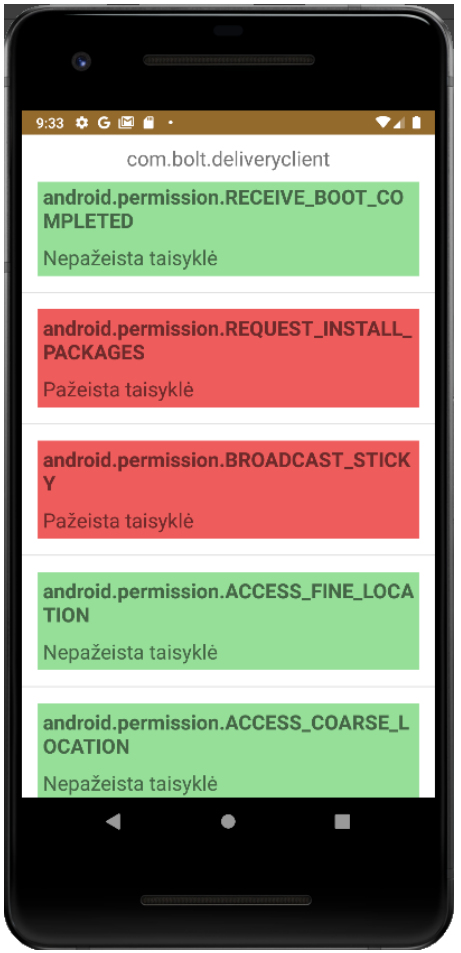


20 pav. Įrenginio paketų atvaizdavimas



21 pav. Funkcija „ATLIKTI PATIKRĄ“

22 pav. Ataskaitos generavimas ir siuntimas el. paštu



23 pav. Individualių paketų peržiūra

3.4. Eksperimentinio tyrimo dalis

3.4.1. Eksperimentinio atvejų analizės tyrimo aprašymas

Organizacijose naudojamų asmeninių mobilių įrenginių saugos valdymo prototipu buvo atliktas tyrimas, kurio metu naudota ši programinė ir aparatinė įranga:

19 lentelė. Aparatinė įranga

Nešiojamas kompiuteris „HP Envy 17“	
Procesorius	Intel(R) Core(TM) i7-4710MQ CPU @ 2.50GHz 2.50 GHz
Operatyvioji atmintis	16 GB
Kietasis diskas	256 GB, ADATA SSD
Grafinė plokštė	NVDIA GeForce 710M, 2GB
Tinklo plokštė	Intel(R) wireless-N 7260
Operacinė sistema	Windows 10 64-bit
Mobilusis įrenginys „LG G6“	
Procesorius	Qualcomm Snapdragon 821 (2x2.35 GHz & 2x1.6 GHz)
Operatyvioji atmintis	4 GB
Kietasis diskas	16 GB
Grafinė plokštė	Adreno 530
Tinklo plokštė	Wi-Fi 802.11 a/b/g/n/ac
Operacinė sistema	Android 9

20 lentelė. Programinė įranga.

Android studio Arctic Fox | 2020.3.1 Patch 3	
Versija	Build #AI-203.7717.56.2031.7784292, built on October 1, 2021
JRE	11.0.10+0-b96-7249189 amd64
JVM	OpenJDK 64-Bit Server VM by Oracle Corporation
Virtualūs įrenginiai	
Google Pixel 2	Google Play Intel Atom (x86) 1080 x 1920, 42 dpi Android 10

Tyrimo metu iškelti tikslai:

1. Ištirti skirtingus atvejų scenarijus, kuriuose naudojami mobilūs įrenginiai su skirtingais įrenginio nustatymais, nekintančia, nei juodajame, nei baltajame sąrašuose nesančių programėlių aibe ir skirtingais darbuotojui priskirtais saugumo lygiais.
2. Ištirti prototipo greitaveiką pradedant darbą su programėle ir atliekant įrenginio saugos politikos patikrą.

Tyrimo eksperimentinis atvejo analizės scenarijus

Tyrimo eksperimentinėje dalyje buvo pasirinkta ištirti 5 scenarijų tyrimo atvejus su mobiliais Android įrenginiais. Kiekviename įrenginyje yra skirtinga aibė nustatymų ir skirtingi šiame darbe pasiūlyti saugumo lygio nustatymai, tačiau visi įrenginiai turi vienodą aibę įrašytų programėlių paketų.

Tiriamų programėlių aibė susidaro iš (14 lentelė): LidlPlus programėlės, kuri prašo 18 leidimų ir tenkina 1 saugumo lygį, OneDrive programėlės, kuri prašo 22 leidimų ir tenkina 1 saugumo lygį, Trafi programėlės, kuri prašo 11 leidimų ir tenkina 1 saugumo lygį, Bolt programėlės, kuri prašo 13 leidimų ir tenkina 1 saugumo lygį, Booking programėlės, kuri prašo 21 leidimų ir tenkina 1 saugumo lygį, Teams programėlės, kuri prašo 33 leidimų ir tenkina 1 ir 2 saugumo lygį, AboutYou programėlės, kuri prašo 7 leidimų ir tenkina 1 ir 2 saugumo lygį, SportstYou programėlės, kuri prašo 10 leidimų ir tenkina 1 ir 2 saugumo lygį, Qr Code Scanner programėlės, kuri prašo 11 leidimų ir tenkina 1 ir 2 saugumo lygį.

21 lentelė. Tiriami paketai įrenginiuose

Programėlė/ Programėlės paketas	**Prašomi leidimai**	**Patenkinamas saugumo lygis**
Lidl Plus/ Com.lidl.eci.lidlplus	android.permission.FOREGROUND_SERVICE;;android.permission.WRITE_INTERNAL_STORAGE;;android.permission.VIBRATE;;android.permission.SYSTEM_ALERT_WINDOW;;android.permission.RECEIVE_BOOT_COMPLETED;android.permission.WRITE_EXTERNAL_STORAGE;;android.permission.REQUEST_INSTALL_PACKAES;;android.permission.ACCESS_FINE_LOCATION;;ndroid.permission.ACCESS_COARSE_LOCATION;android.permission.CHANGE_WIFI_STATE;android.permission.USE_BIOMETRIC;android.permission.ACCESS_NETWORK_STATE;;android.permission.WAKE_LOCK;;android.permission.USE_FINGERPRINT;;android.permission.ACCESS_WIFI_STATE;;android.permission.CAMERA;;android.permission.READ_EXTERNAL_STORAGE;android.permission.READ_PHONE_STATE;	1
OneDrive/ com.microsoft.skydrive	android.permission.GET_ACCOUNTS;android.permission.ACCESS_MEDIA_LOCATION;android.permission.READ_SYNC_SETTINGS;android.permission.AUTHENTICATE_ACCOUNTS;android.permission.FOREGROUND_SERVICE;android.permission.VIBRATE;android.permission.RECEIVE_BOOT_COMPLETED;android.permission.WRITE_EXTERNAL_STORAGE;android.permission.READ_SYNC_STATS;android.permission.WRITE_SYNC_SETTINGS;android.permission.INTERNET;android.permission.USE_CREDENTIALS;android.permission.USE_BIOMETRIC;android.permission.ACCESS_NETWORK_STATE;android.permission.WAKE_LOCK;android.permission.GET_ACCOUNTS_PRIVILEGED;android.permission.USE_FINGERPRINT;android.permission.CAMERA;android.permission.READ_EXTERNAL_STORAGE;android.permission.WRITE_SETTINGS;android.permission.MANAGE_ACCOUNTS;android.permission.READ_PHONE_STATE	1
Trafi/ com.trafi.android.tr	android.permission.ACCESS_FINE_LOCATION;android.permission.FOREGROUND_SERVICE;android.permission.ACCESS_NETWORK_STATE;android.permission.VIBRATE;android.permission.CHANGE_NETWORK_STATE;android.permission.WAKE_LOCK;android.permission.CAMERA;android.permission.NFC;android.permission.RECEIVE_BOOT_COMPLETED;android.permission.READ_EXTERNAL_STORAGE;android.permission.WRITE_EXTERNAL_STORAGE	1
Bolt/ com.bolt.deli	android.permission.FOREGROUND_SERVICE;android.permission.QUERY_ALL_PACKAGES;android.permission.VIBRATE;android.permission.SYSTEM_ALERT_WINDOW;android.permission.RECEIVE_BOOT_COMPLETED;android.p	1

Programėlė/ Programėlės paketas	**Prašomi leidimai**	**Patenkinamas saugumo lygis**
veryclient	ermission.REQUEST_INSTALL_PACKAGES;android.permission.BROADCAST_STICKY;android.permission.ACCESS_FINE_LOCATION;android.permission.ACCESS_COARSE_LOCATION;android.permission.ACCESS_NETWORK_STATE;android.permission.WAKE_LOCK;android.permission.ACCESS_WIFI_STATE;android.permission.READ_EXTERNAL_STORAGE	
Booking/ com.booking	android.permission.READ_SYNC_SETTINGS;android.permission.GET_ACCOUNTS;android.permission.AUTHENTICATE_ACCOUNTS;android.permission.WRITE_CALENDAR;android.permission.READ_CALENDAR;android.permission.NFC;android.permission.RECEIVE_BOOT_COMPLETED;android.permission.RECORD_AUDIO;android.permission.WRITE_EXTERNAL_STORAGE;android.permission.WRITE_SYNC_SETTINGS;android.permission.ACCESS_FINE_LOCATION;android.permission.ACCESS_COARSE_LOCATION;android.permission.USE_CREDENTIALS;android.permission.ACCESS_NETWORK_STATE;android.permission.WAKE_LOCK;android.permission.ACCESS_WIFI_STATE;ndroid.permission.CAMERA;android.permission.READ_EXTERNAL_STORAGE;android.permission.MANAGE_ACCOUNTS;android.permission.HIGH_SAMPLING_RATE_SENSORS;android.permission.READ_PHONE_STATE	1
Teams/ com.microsoft.teams	android.permission.READ_CONTACTS;android.permission.GET_ACCOUNTS;android.permission.CALL_PHONE;android.permission.FOREGROUND_SERVICE;android.permission.AUTHENTICATE_ACCOUNTS;android.permission.BLUETOOTH_ADMIN;android.permission.SYSTEM_ALERT_WINDOW;android.permission.RECEIVE_BOOT_COMPLETED;android.permission.WRITE_EXTERNAL_STORAGE;android.permission.ACCESS_FINE_LOCATION;android.permission.ACCESS_COARSE_LOCATION;android.permission.MANAGE_OWN_CALLS;android.permission.ACCESS_NETWORK_STATE;android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS;android.permission.WAKE_LOCK;android.permission.ACCESS_WIFI_STATE;android.permission.USE_FINGERPRINT;android.permission.WRITE_CONTACTS;android.permission.MANAGE_ACCOUNTS;android.permission.READ_APP_BADGE;android.permission.ACCESS_BACKGROUND_LOCATION;android.permission.QUERY_ALL_PACKAGES;android.permission.VIBRATE;android.permission.RECORD_VIDEO;android.permission.RECORD_AUDIO;android.permission.USE_CREDENTIALS;android.permission.USE_BIOMETRIC;android.permission.CHANGE_NETWORK_STATE;android.permission.USE_FULL_SCREEN_INTENT;android.permission.CAMERA;android.permission.MODIFY_AUDIO_SETTINGS;android.permission.READ_EXTERNAL_STORAGE;android.permission.BLUETOOTH	1
AboutYou/ De.aboutyou.mobile.app	android.permission.SCHEDULE_EXACT_ALARM;ndroid.permission.ACCESS_NETWORK_STATE;android.permission.VIBRATE;android.permission.WAKE_LOCK;android.permission.USE_FULL_SCREEN_INTENT;android.permission.RECEIVE_BOOT_COMPLETED;android.permission.READ_PHONE_STATE	1,2
SportsYou/ Com.sportysyou.sportsYou	android.permission.DOWNLOAD_WITHOUT_NOTIFICATION;ndroid.permission.INTERNET;android.permission.FOREGROUND_SERVICE;;android.permission.ACCESS_NETWORK_STATE;android.permission.WAKE_LOCK;android.permission.ACCESS_WIFI_STATE;android.permission.READ_EXTERNAL_STORAGE;android.permission.RECEIVE_BOOT_COMPLETED;android.permission.WRITE_EXTERNAL_STORAGE;android.permission.READ_PHONE_STATE	1,2
Qr Code Scanner/ com.gamma.scan	android.permission.FLASHLIGHT;android.permission.CHANGE_WIFI_STATE;android.permission.INTERNET;android.permission.ACCESS_NETWORK_STATE;android.permission.CHANGE_WIFI_MULTICAST_STATE;android.permission.VIBRATE;android.permission.WAKE_LOCK;android.permission.ACCESS_WIFI_STATE;android.permission.READ_EXTERNAL_STORAGE;android.permission.RECEIVE_BOOT_COMPLETED;android.permission.WRITE_EXTERNAL_STORAGE	1
AirBnB	android.permission.READ_CONTACTS;android.permission.GET_ACCOUNTS;	1

Programėlė/ Programėlės paketas	Prašomi leidimai	Patenkinamas saugumo lygis
Com.airbnb.android	android.permission.ACCESS_MEDIA_LOCATION;android.permission.CALL_PHONE;android.permission.FOREGOUND_SERVICE;android.permission.RECEIVE_BOOT_COMPLETED;android.permission.WRITE_EXTERNAL_STORAGE;android.permission.ACCESS_FINE_LOCATION;ndroid.permission.ACCESS_COARSE_LOCATION;android.permission.MANAGE_OWN_CALLS;android.permission.ACCESS_NETWORKSTATE;android.permission.WAKE_LOCK;android.permission.ACCESS_WIFI_STATE;android.permission.READ_SETTINGS;android.permission.READ_APP_BADGE;android.permission.VIBRATE;android.permission.RECORD_AUDIO;android.permission.REQUEST_INSTALL_PACKAGES;android.permission.CHANGE_WIFI_STATE;android.permission.USE_CREDENTIALS;android.permission.CHANGE_NETWORK_STATE;android.permission.CAMERA_AUDIO_SETTINGS;android.permission.BLUETOOTH;ndroid.permission.READ_EXTERNAL_STORAGE;android.permission.READ_PHONE_STATE;android.permission.WRITE_SETTINGS	

Toliau tiriami 5 atvejų tyrimo scenarijai (15 lentelė) su taikoma skirtingo lygmens saugumo politika, skirtingais įrenginio nustatymais. Visi įrenginiai turi vienodą aibę įrašytų paketų (14 lentelė). Atvejuose naudojami skirtingos iš anksto patvirtintos papildomai įdiegtos programėlės.

22 lentelė. Tiriami įrenginių atvejų analizės scenarijai

Atvejo Nr./ saugumo lygis	Įrenginio nustatymai	Baltajame sąraše esančios papildomai įdiegtos programėlės	Draudžiamos programėlių kategorijos
1/ 1 lygis	Suaktyvinta kamera Suaktyvintas NFC Suaktyvintas Bluetooth Suaktyvintas ekrano užraktas Suaktyvintas disko šifravimas Aktyvus WIFI WPA3 Suaktyvintas GPS	Avast antivirus Express VPN FindMyDevice	Pramogos
2/ 2 lygis	Suaktyvinta kamera Deaktyvuotas NFC Suaktyvintas Bluetooth Suaktyvintas ekrano užraktas Suaktyvintas disko šifravimas Aktyvus WIFI WPA3 Suaktyvintas GPS	Bittdefender FindMyDevice Express VPN	Pramogos Įrankiai Personalizacija Kelionės ir gidai
3/ 2 lygis	Deaktyvuota kamera Suaktyvintas NFC Deaktyvuotas Bluetooth Suaktyvintas ekrano užraktas Deaktyvuotas disko šifravimas Aktyvus WIFI WPA3 Suaktyvintas GPS	Avast antivirus FindMyDevice	Pramogos Įrankiai Personalizacija Kelionės ir gidai
4/ 3 lygis	Deaktyvuota kamera Suaktyvintas NFC Suaktyvintas Bluetooth Suaktyvintas ekrano užraktas	Bittdefender Express VPN FindMyDevice	Pramogos Įrankiai Personalizacija Kelionės ir gidai

Atvejo Nr./ saugumo lygis	**Įrenginio nustatymai**	**Baltajame sąraše esančios papildomai įdiegtos programėlės**	**Draudžiamos programėlių kategorijos**
	Deaktyvuotas disko šifravimas Aktyvus WIFI WPA3 Suaktyvintas GPS		Komunikacija Gyvensena Socialinės
5/ 3 lygis	Deaktyvuota kamera Deaktyvuotas NFC Deaktyvuotas Bluetooth Suaktyvintas ekrano užraktas Suaktyvintas disko šifravimas Aktyvus WIFI WPA3 Suaktyvintas GPS	Bittdefender Express VPN FindMyDevice	Pramogos Įrankiai Personalizacija Kelionės ir gidai Komunikacija Gyvensena Socialinės

1 atvejo tyrimo rezultatai:

Įrenginio nustatymai tenkina 1 lygio saugos politikos mobilaus įrenginio nustatymų taisykles.

Papildomai įdiegtos programėlės tenkina 1 lygio saugos politikos taisykles.

Iš įdiegtų programėlių aibės joks paketas nepažeidžia 1 lygio draudžiamų kategorijų saugos politikos taisyklių.

Įdiegtos programėlės nepažeidė jokių 1 lygio saugos politikos draudžiamų leidimų grupių.

2 atvejo tyrimo rezultatai:

Įrenginio nustatymai tenkina 2 lygio mobilaus įrenginio nustatymų saugos politikos taisykles.

Papildomai įdiegtos programėlės tenkina 2 lygio saugos politikos taisykles.

Iš įdiegtų programėlių aibės, paketas: com.gamma.scan pažeidė kategoriją: įrankiai.

8 įdiegtos programėlės pažeidė 22 draudžiamų grupių leidimus.

3 atvejo tyrimo rezultatai:

Įrenginio nustatymai tenkina 2 lygio mobilaus įrenginio nustatymų saugos politikos taisykles.

Įrenginyje nėra papildomai įdiegtos Express VPN ir bittdefender programėlės.

Iš įdiegtų programėlių aibės, paketas: com.gamma.scan pažeidė kategoriją: įrankiai.

8 įdiegtos programėlės pažeidė 22 draudžiamų grupių leidimus.

4 atvejo tyrimo rezultatai:

Įrenginio nustatymuose yra aktyvūs 3 lygio politikos taisyklėse draudžiami NFC ir Bluetooth ryšys.

Papildomai įdiegtos programėlės tenkina 3 lygio saugos politikos taisykles.

Iš įdiegtų programėlių aibės, paketas: com.whatsapp pažeidė kategoriją: komunikacija, paketas: com.gamma.scan pažeidė kategoriją: įrankiai., paketas: com.sportsyou.sportsYou pažeidė kategoriją: sportas.

10 įdiegtų programėlių pažeidė 83 draudžiamų grupių leidimus.

5 atvejo tyrimo rezultatai:

Įrenginio nustatymai tenkina 3 lygio mobilaus įrenginio nustatymų saugos politikos taisykles.

Papildomai įdiegtos programėlės tenkina 3 lygio saugos politikos taisykles.

Iš įdiegtų programėlių aibės, paketas: com.whatsapp pažeidė kategoriją: komunikacija, paketas: com.gamma.scan pažeidė kategoriją įrankiai, paketas: com.sportsyou.sportsYou pažeidė kategoriją: sportas.

10 įdiegtų programėlių pažeidė 83 draudžiamų grupių leidimus.

Iš šiame tyrime sudarytų 5 scenarijų tik vienas įrenginys yra tinkamas darbui, neatliekant jokių papildomų veiksmų su įrenginiu.

3.4.2. Prototipo greitaveikos tyrimas

Šio tyrimo metu buvo naudojamas Android OS įrenginys (12 lentelė), turintis skirtingą kiekį programėlių iš „Google Play“ parduotuvės.

Viso bus sudaryti 9 skirtingi atvejų tyrimo scenarijai:

Įrenginys turintis 65 atsitiktinai atrinktas programėles iš „Google Play“ parduotuvės, su kuriomis bus matuojamas greitaveikos laikas, nuo vartotojo prisijungimo prie sistemos, iki laiko, kol bus nuskaitomos visos įrenginyje įrašytos programėlės ir patikrinamos su duomenų bazėje užduotomis taisyklėmis. Šis veiksmas bus atliekamas su vienoda aibe programėlių, trimis skirtingais vartotojo saugumo lygiais.

Įrenginys turintis 45 atsitiktinai atrinktas programėles iš „Google Play“ parduotuvės, su kuriomis bus matuojamas greitaveikos laikas, nuo vartotojo prisijungimo prie sistemos, iki laiko, kol bus nuskaitomos visos įrenginyje įrašytos programėlės, patikrinamos su duomenų bazėje užduotomis taisyklėmis. Šis veiksmas bus atliekamas su vienoda aibe programėlių, trimis skirtingais vartotojo saugumo lygiais.

Įrenginys turintis 20 atsitiktinai atrinktas programėles iš „Google Play“ parduotuvės, su kuriomis bus matuojamas greitaveikos laikas, nuo vartotojo prisijungimo prie sistemos, iki laiko, kol bus nuskaitomos visos įrenginyje įrašytos programėlės, patikrinamos su duomenų bazėje užduotomis taisyklėmis. Šis veiksmas bus atliekamas su vienoda aibe programėlių, trimis skirtingais vartotojo saugumo lygiais.

Šis veiksmas bus žymimas kaip greitaveika (16 lentelė).

23 lentelė. Greitaveikos tyrimo atvejo analizės scenarijai ir rezultatai

Įrenginys	**Įrenginyje įrašytų programėlių skaičius, vnt.**	**Darbuotojo saugumo politikos lygis**	**Greitaveika, s**
LG G6	65	1	41,23
LG G6	65	2	41,59
LG G6	65	3	41,92
LG G6	45	1	30,98
LG G6	45	2	31,41
LG G6	45	3	31,56
LG G6	20	1	17,21
LG G6	20	2	17,56
LG G6	20	3	17,86

Įrenginio greitaveikos tyrimo metu buvo nustatyta jog:

Įrenginyje turint 65 programėles ir darbuotojui taikant: 1 šiame darbe pasiūlytą saugos lygį veikimo greitis yra 41,23 sekundės.

Įrenginyje turint 65 programėles ir darbuotojui taikant 2 šiame darbe pasiūlytą saugos lygį veikimo greitis yra 41,59 sekundės.

Įrenginyje turint 65 programėles ir darbuotojui taikant 3 šiame darbe pasiūlytą saugos lygį veikimo greitis yra 41,92 sekundės.

Įrenginyje turint 45 programėles ir darbuotojui taikant:1 šiame darbe pasiūlytą saugos lygį veikimo greitis yra 30,98 sekundės.

Įrenginyje turint 45 programėles ir darbuotojui taikant 2 šiame darbe pasiūlytą saugos lygį veikimo greitis yra 31,41 sekundės.

Įrenginyje turint 45 programėles ir darbuotojui taikant 3 šiame darbe pasiūlytą saugos lygį veikimo greitis yra 31,56 sekundės.

Įrenginyje turint 20 programėlių ir darbuotojui taikant:1 šiame darbe pasiūlytą saugos lygį veikimo greitis yra 17,21 sekundės.

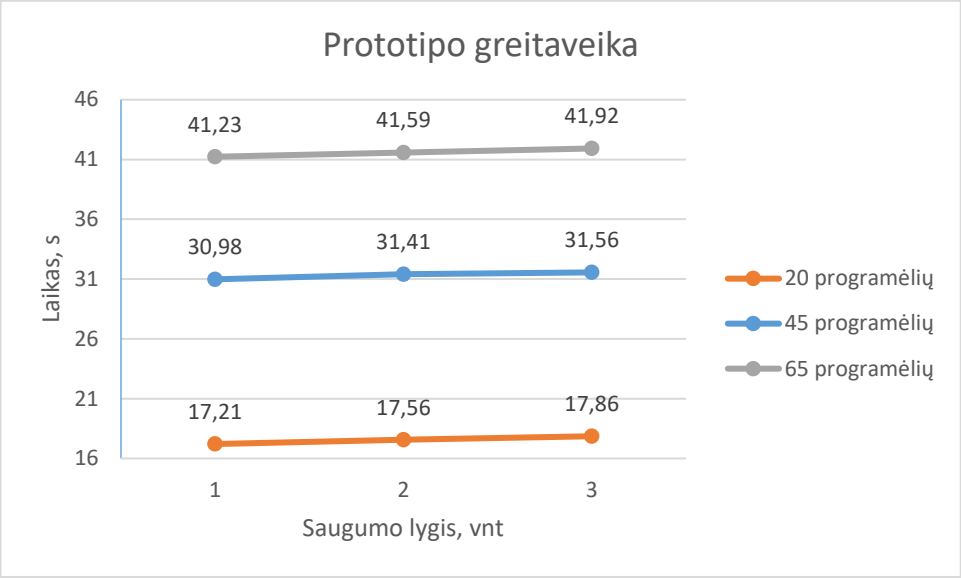
Įrenginyje turint 20 programėlių ir darbuotojui taikant 2 šiame darbe pasiūlytą saugos lygį veikimo greitis yra 17,56 sekundės.

Įrenginyje turint 20 programėlių ir darbuotojui taikant 3 šiame darbe pasiūlytą saugos lygį veikimo greitis yra 17,86 sekundės.

Įrenginyje turint 65 programėles veikimo greitis vidutiniškai yra 41,58 sekundės ir neženkliai priklauso nuo darbuotojui priskirto saugumo lygio.

Įrenginyje turint 45 programėles veikimo greitis vidutiniškai yra 31,31 sekundės ir neženkliai priklauso nuo darbuotojui priskirto saugumo lygio.

Įrenginyje turint 20 programėlių veikimo greitis vidutiniškai yra 17,54 sekundės ir neženkliai priklauso nuo darbuotojui priskirto saugumo lygio.



24 pav. Prototipo greitaveikos grafikas

Nors tiek didėjant programėlių skaičiui įrenginyje, tiek didėjant saugumo lygiui, programėlės rezultatų pateikimo greitis mažėja, tačiau galime teigti, jog greitaveikai nedaro reikšmingos įtakos, saugumo politikos lygis, tačiau didelę įtaką daro mobiliame įrenginyje esančių programėlių kiekis. Nevertinus tinklo greičio, vidutiniškai vieną programėlę patikrinti užtrunka $\frac{7}{10}$ sekundės. Surasti programėlės prašomus leidimus daug laiko neužtrunka, tačiau gavus įrenginyje esančių paketų sąrašą, prototipo kodo metodas kiekvienam paketui siunčia query užklausą surasti individualios programėlės kategorijai. Šis veiksmas užtrunka didžiausią laiko tarpsnį mobilaus įrenginio patikroje.

3.5. Išvados

1. Organizacijose naudojamų asmeninių įrenginių saugos politikos valdymo prototipo dalyje buvo:
   1.1. Aprašyta naudojamos duomenų bazės ir saugumo politikos struktūra.
   1.2. Buvo aprašytas realizuoto prototipo veikimo algoritmas.
   1.3. Atvaizduoti prototipo funkciniai langai.

2. Organizacijose naudojamų asmeninių įrenginių saugos politikos tyrimo dalyje buvo:
   2.1. Ištirti 5 skirtingi atvejų analizės scenarijai, kuriuose naudojami mobilūs įrenginiai su skirtingais įrenginio nustatymais, nekintančia, nei juodajame, nei baltajame sąrašuose nesančių programėlių aibe ir skirtingais darbuotojui priskirtais saugumo lygiais (22 lentelė).
   2.2. Aprašytos atvejų analizės scenarijuose naudojamos programėlės, jų prašomi leidimai ir kokį saugumo lygį tenkina kiekviena programėlė. (21 lentelė).
   2.3. Atvejų analizės scenarijų metu buvo rasta, jog atvejis:
      2.3.1. Nr. 1 tenkina įmonės saugos politiką;
      2.3.2. Nr. 2 netenkina įmonės saugos politikos. Iš atvejų analizėje aprašytos aibės programėlių, 8 netenkina įmonės saugos politikos;

2.3.3. Nr. 3 netenkina įmonės saugos politikos. Iš atvejų analizėje aprašytos aibės programėlių, 8 netenkina įmonės saugos politikos. Iš papildomai įdiegtų programėlių 2 netenkina įmonės saugos politikos;

2.3.4. Nr. 4 netenkina įmonės saugos politikos. 2 mobilaus įrenginio nustatymai ir 10 iš atvejų analizėje aprašytos aibės programėlių, netenkina įmonės saugos politikos. Iš papildomai įdiegtų programėlių 2 netenkina įmonės saugos politikos;

2.3.5. Nr. 5 netenkina įmonės saugos politikos. Iš atvejų analizėje aprašytos aibės programėlių, 10 netenkina įmonės saugos politikos.

2.4. Ištirta prototipo greitaveika pradedant darbą su programėle ir tikrinant įrenginyje esančias programėles. Šio tyrimo metu buvo sudaryti 9 skirtingi scenarijai su 65, 45 ir 20 mobiliame įrenginyje esančių programėlių ir skirtingais įrenginiui taikomais saugumo lygiais. Buvo nustatyta, jog greitaveikai nedaro reikšmingos įtakos, saugumo politikos lygis, tačiau didelę įtaką daro mobiliame įrenginyje esančių programėlių kiekis. Nevertinus tinklo duomenų kaitos greičio, vidutiniškai vieną programėlę patikrinti užtrunka $\frac{7}{10}$ sekundės.

Išvados

1. Magistrinio darbo analizės dalyje buvo nustatyta, jog organizacijose naudojami asmeniniai įrenginiai susiduria su vis didėjančiais diegimo, techniniais, politiniais ir reguliavimo iššūkiais.
2. Buvo išanalizuoti trys asmeninių mobilių įrenginių saugos modeliai – įrenginių, programėlių ir informacijos, nustatyta plačiausiai pasaulyje mobiliuose įrenginiuose naudojama operacinė sistema Android, kurią naudojant buvo realizuotas prototipas ir atliktas tyrimas.
3. Nustatyta jog tiek asmeninių, tiek neasmeninių mobilių įrenginių saugumui gresia tos pačios kenkėjiškos grėsmės.
4. Buvo nustatyta, jog rinkoje egzistuojantys organizacijose naudojamų asmeninių įrenginių sprendimai taikosi į tinklo nustatymus, programėlių kontrolę, įrenginio nustatymus, siunčiamų ir gaunamų duomenų stebėjimą bei valdymą, geolokacijos stebėjimą, vartotojų grupių administravimą, autentifikaciją ir disko šifravimą.
5. Operacinė sistema Android naudoja daugelį vartotojo saugumą užtikrinančių metodų, iš kurių vienas plačiausiai pritaikytų – mobilios programėlės prašomi leidimai. Android OS leidimai buvo suskirstyti į grupes, pagal grėsmę įmonės duomenims.
6. Rasta jog trys labiausiai pažeidžiamos programėlių kategorijos yra: pramogos (angl. Entertainment), įrankiai (angl. Tools) ir personalizacija (angl. personalization).
7. Eksperimentinėje dalyje buvo atlikti du tyrimai: (1) Įrenginių atvejų analizės tyrimas su 5 scenarijais; (2) Prototipo greitaveikos tyrimas su 9 scenarijais.
8. Įrenginių atvejų analizės tyrimo dalyje iš 5 tirtų scenarijų buvo nustatyta, jog didėjant įrenginiui taikomam saugos politikos lygiui didėja ir rastų pažeidimų skaičius:
    - Įrenginys, kuriame taikomas 1 saugos politikos lygis, tenkina visus 148 programėlių prašomus leidimus;
    - Įrenginys, kuriame taikomas 2 saugos politikos lygis, tenkina tik 126 iš 148 programėlių prašomų leidimų;
    - Įrenginys, kuriame taikomas 3 saugos politikos lygis, tenkina tik 65 iš 148 programėlių prašomų leidimų.
9. Įrenginių atvejų analizės tyrimo dalyje iš 5 tirtų scenarijų buvo nustatyta, jog didėjant įrenginiui taikomam saugos politikos lygiui didėja ir paketų skaičius, kurie pažeidžia saugumo politikoje aprašytas programėlės kategorijos taisykles:
    - Įrenginyje, kuriame taikomas 1 saugos politikos lygis, iš įrašytos aibės programėlių visos tenkina įmonės saugos politikoje draudžiamas programėlių kategorijas;
    - Įrenginyje, kuriame taikomas 2 saugos politikos lygis, iš įrašytos aibės programėlių 1 paketas pažeidžia įmonės saugos politikoje draudžiamas programėlių kategorijas;
    - Įrenginyje, kuriame taikomas 3 saugos politikos lygis, iš įrašytos aibės programėlių 3 paketai pažeidžia įmonės saugos politikoje draudžiamas programėlių kategorijas.
10. Prototipo greitaveikos tyrimo dalyje buvo nustatyta, jog atliekant mobilaus įrenginio patikrą su 20 programėlių vidutinis patikros laikas yra 17,54 sekundės, su 45 programėlėmis vidutinis patikros laikas yra 31,31 sekundės, su 65 programėlėmis vidutinis patikros laikas yra 41,58 sekundės. Nustatyta, jog įrenginiui taikomas įmonės saugumo politikos lygmuo neturi reikšmingos įtakos greitaveikai ir svyruoja $\frac{1}{2}$ sekundės dalies, vidutiniškai vieną programėlę patikrinti užtrunka $\frac{7}{10}$ sekundės dalies.

Literatūros sąrašas

1. Downer, Kathleen, and Maumita Bhattacharya. “BYOD Security: A New Business Challenge.” In 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), 1128–33. Chengdu, China: IEEE, 2015. https://doi.org/10.1109/SmartCity.2015.221.
2. Eslahi, Meisam, Maryam Var Naseri, H. Hashim, N.M. Tahir, and Ezril Hisham Mat Saad. “BYOD: Current State and Security Challenges.” In 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), 189–92. Penang, Malaysia: IEEE, 2014. https://doi.org/10.1109/ISCAIE.2014.7010235.
3. Morolong, Mamoqenelo, Attlee Gamundani, and Fungai Bhunu Shava. “Review of Sensitive Data Leakage through Android Applications in a Bring Your Own Device (BYOD) Workplace.” In 2019 IST-Africa Week Conference (IST-Africa), 1–8. Nairobi, Kenya: IEEE, 2019. https://doi.org/10.23919/ISTAFRICA.2019.8764833.
4. N. Sarafinienė, I. Lagzdinytė, D. Matulis, G. Vilutis, R. Zakarevičius, Operacinių sistemų architektūros. 2012. Kaunas. KTU leidykla Technologija. [ISBN 978-609-02-0521-1]
5. Shinde, Supriya S., and Santosh S. Sambare. “Enhancement on Privacy Permission Management for Android Apps.” In 2015 Global Conference on Communication Technologies (GCCT), 838–42. Thuckalay, Kanya kumari district, India: IEEE, 2015. https://doi.org/10.1109/GCCT.2015.7342779.
6. https://www.idc.com/promo/smartphone-market-share/os
7. Felt, Adrienne Porter, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. “Android Permissions Demystified.” In Proceedings of the 18th ACM Conference on Computer and Communications Security - CCS ’11, 627. Chicago, Illinois, USA: ACM Press, 2011. https://doi.org/10.1145/2046707.2046779.
8. Tse, Daniel, Lu Wang, and Yuxi Li. “Mobility Management for Enterprises in BYOD Deployment.” In 2016 IEEE Trustcom/BigDataSE/ISPA, 638–45. Tianjin, China: IEEE, 2016. https://doi.org/10.1109/TrustCom.2016.0120.
9. Al Harthy, khoula, Nazaraf Shah, and Arun Shankarappa. “Intelligent Risk Management Framework for BYOD.” In 2018 IEEE 15th International Conference on E-Business Engineering (ICEBE), 289–93. Xi’an: IEEE, 2018. https://doi.org/10.1109/ICEBE.2018.00055.
10. Ali, Sara, Muhammad Nauman Qureshi, and Abdul Ghafoor Abbasi. “Analysis of BYOD Security Frameworks.” In 2015 Conference on Information Assurance and Cyber Security (CIACS), 56–61. Rawalpindi, Pakistan: IEEE, 2015. https://doi.org/10.1109/CIACS.2015.7395567.
11. M. Bartock, M. Souppaya, J. Cichonski, M. Smith, G. Witte, K. Scarfone, Guide for Cybersecurity Event Recovery, NIST Special Publication (SP), National Institute of Standards and Technology, Gaithersburg, Maryland, 2016. https://doi.org/10.6028/NIST.SP.800-184
12. Symantec, Internet security threat report volume 19,", 2014, Symantec, Mountain View.
13. Uddin Sharif, Md Haris, Ripon Datta, Siva N Sankarasetty, Hari Garikapati, Mounicasri Valavala, and Suchit Maraboyina. “BRING YOUR OWN DEVICE (BYOD) PROGRAM.” International Journal of Engineering Applied Sciences and Technology 04, no. 04, 2019: 36–40. https://doi.org/10.33564/IJEAST.2019.v04i04.006.

14. Souppaya, Murugiah P, and Karen A Scarfone. “Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.” National Institute of Standards and Technology, July 2016. https://doi.org/10.6028/NIST.SP.800-46r2.
15. Kumar, Laxman. “Bring Your Own Device or Bring Your Own Distraction.” International Journal of School and Cognitive Psychology 03, no. 01 (2016). https://doi.org/10.4172/2469-9837.1000170.
16. Souppaya, Murugiah P, and Karen A Scarfone. “User’s Guide to Telework and Bring Your Own Device (BYOD) Security.” National Institute of Standards and Technology, July 2016. https://doi.org/10.6028/NIST.SP.800-114r1.
17. Sharif, Haris Uddin, and Ripon Datta. “SOFTWARE AS A SERVICE HAS STRONG CLOUD SECURITY”. International Journal of Research in Engineering and Management vol 1, no. 2 (2019): psl. 18-27.
18. Kim, Kyong-jin, and Seng-phil Hong. “Study on Enhancing Vulnerability Evaluations for BYOD Security.” International Journal of Security and Its Applications 8, no. 4 (July 31, 2014): 229–38. https://doi.org/10.14257/ijsia.2014.8.4.20.
19. Samaras, Vasileios, Semir Daskapan, Rizwan Ahmad, and Sayan Kumar Ray. “An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD.” In 2014 Australasian Telecommunication Networks and Applications Conference (ATNAC), 129–34. Southbank, Australia: IEEE, 2014. https://doi.org/10.1109/ATNAC.2014.7020886.
20. Leavitt, Neal. “Today’s Mobile Security Requires a New Approach.” Technology news, computer 46, no. 11, 2013, psl. 16–19. https://doi.org/10.1109/MC.2013.400.
21. Selviandro, Nungki, Gede Wisudiawan, Shinta Puspitasari, and Monterico Adrian. “Preliminary Study for Determining Bring Your Own Device Implementation Framework Based on Organizational Culture Analysis Enhanced by Cloud Management Control.” In 2015 3rd International Conference on Information and Communication Technology (ICoICT), 113–18. Nusa Dua, Bali, Indonesia: IEEE, 2015. https://doi.org/10.1109/ICoICT.2015.7231407.
22. La Polla, Mariantonietta, Fabio Martinelli, and Daniele Sgandurra. “A Survey on Security for Mobile Devices.” IEEE Communications Surveys & Tutorials 15, no. 1 (2013): 446–71. https://doi.org/10.1109/SURV.2012.013012.00028.
23. Rhee, Keunwoo, Dongho Won, Sang-Woon Jang, Sooyoung Chae, and Sangwoo Park. “Threat Modeling of a Mobile Device Management System for Secure Smart Work.” Electronic Commerce Research 13, no. 3 (September 2013): 243–56. https://doi.org/10.1007/s10660-013-9121-4.
24. National Security Agency, System and Network Analysis Center “Application Whitelisting Using Software Restriction Policies,” V 1.1, 2010.
25. Sedgewick, Adam, Murugiah P. Souppaya, and Karen A. Scarfone. “Guide to Application Whitelisting.” National Institute of Standards and Technology, October 2015. https://doi.org/10.6028/NIST.SP.800-167.
26. https://developer.android.com/reference/android/Manifest.permission#ACCOUNT_MANAGER
27. Zhu, Hengshu, Hui Xiong, Yong Ge, and Enhong Chen. “Mobile App Recommendations with Security and Privacy Awareness.” In Proceedings of the 20th ACM SIGKDD International

Conference on Knowledge Discovery and Data Mining, 951–60. New York New York USA: ACM, 2017. https://doi.org/10.1145/2623330.2623705.

28. https://support.google.com/googleplay/android-developer/answer/9859673?hl=en
29. https://developer.android.com/reference/android/R.attr
30. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf

Priedai

1 priedas. Automatiškai generuojama ataskaita

1 saugumo lygis

Įrenginyje rasti paketai, kurie pažeidžia saugumo politikos leidimų grupes

---

Rastų pažeidimų skaičius: 0

Įrenginyje rasti paketai, kurie pažeidžia saugumo politikos programėlių kategorijas

---

Rastų pažeidimų skaičius: 0

Įrenginyje rasti paketai, kurie pažeidžia saugumo politikos leidimų grupes

---

2 saugumo lygis

Įrenginyje rasti paketai, kurie pažeidžia saugumo politikos leidimų grupes

---

Paketas: com.whatsapp Pažeidė grupę taisyklių: L14 Pažeista taisyklė: android.permission.CALL_PHONE

Paketas: com.whatsapp Pažeidė grupę taisyklių: L13 Pažeista taisyklė: android.permission.RECEIVE_SMS

Paketas: com.whatsapp Pažeidė grupę taisyklių: L14 Pažeista taisyklė: android.permission.SEND_SMS

Paketas: com.whatsapp Pažeidė grupę taisyklių: L14 Pažeista taisyklė: android.permission.ANSWER_PHONE_CALLS

Paketas: com.whatsapp Pažeidė grupę taisyklių: L18 Pažeista taisyklė: android.permission.REQUEST_INSTALL_PACKAGES

Paketas: com.whatsapp Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.WRITE_SYNC_SETTINGS

Paketas: com.whatsapp Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_WIFI_STATE

Paketas: com.whatsapp Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_NETWORK_STATE

Paketas: com.lidl.eci.lidlplus Pažeidė grupę taisyklių: L18 Pažeista taisyklė: android.permission.REQUEST_INSTALL_PACKAGES

Paketas: com.lidl.eci.lidlplus Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_WIFI_STATE

Paketas: com.gamma.scan Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_WIFI_STATE

Paketas: com.gamma.scan Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_WIFI_MULTICAST_STATE

Paketas: com.microsoft.skydrive Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.WRITE_SYNC_SETTINGS

Paketas: com.trafi.android.tr Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_NETWORK_STATE

Paketas: com.bolt.deliveryclient Pažeidė grupę taisyklių: L18 Pažeista taisyklė: android.permission.REQUEST_INSTALL_PACKAGES

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L14 Pažeista taisyklė: android.permission.CALL_PHONE

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L18 Pažeista taisyklė: android.permission.REQUEST_INSTALL_PACKAGES

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_WIFI_STATE

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_NETWORK_STATE

Paketas: com.booking Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.WRITE_SYNC_SETTINGS

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L14 Pažeista taisyklė: android.permission.CALL_PHONE

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_NETWORK_STATE

Rastų pažeidimų skaičius: 22

Įrenginyje rasti paketai, kurie pažeidžia saugumo politikos programėlių kategorijas

---

Paketas: com.gamma.scan Pažeidė kategoriją:Tools

Rastų pažeidimų skaičius: 1

3 saugumo lygis

Paketas: com.whatsapp Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_CONTACTS

Paketas: com.whatsapp Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.GET_ACCOUNTS

Paketas: com.whatsapp Pažeidė grupę taisyklių: L14 Pažeista taisyklė: android.permission.CALL_PHONE

Paketas: com.whatsapp Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_PHONE_NUMBERS

Paketas: com.whatsapp Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.NFC

Paketas: com.whatsapp Pažeidė grpę taisyklių: L7 Pažeista taisyklė: android.permission.NFC_PREFERRED_PAYMENT_INFO

Paketas: com.whatsapp Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.NFC_TRANSACTION_EVENT

Paketas: com.whatsapp Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_FINE_LOCATION

Paketas: com.whatsapp Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_COARSE_LOCATION

Paketas: com.whatsapp Pažeidė grupę taisyklių: L13 Pažeista taisyklė: android.permission.RECEIVE_SMS

Paketas: com.whatsapp Pažeidė grupę taisyklių: L14 Pažeista taisyklė: android.permission.SEND_SMS

Paketas: com.whatsapp Pažeidė grupę taisyklių: L14 Pažeista taisyklė: android.permission.ANSWER_PHONE_CALLS

Paketas: com.whatsapp Pažeidė grupę taisyklių: L18 Pažeista taisyklė: android.permission.REQUEST_INSTALL_PACKAGES

Paketas: com.whatsapp Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.BROADCAST_STICKY

Paketas: com.whatsapp Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.WRITE_SYNC_SETTINGS

Paketas: com.whatsapp Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_WIFI_STATE

Paketas: com.whatsapp Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_CALL_LOG

Paketas: com.whatsapp Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_NETWORK_STATE

Paketas: com.whatsapp Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.BLUETOOTH_ADMIN

Paketas: com.whatsapp Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.BLUETOOTH

Paketas: com.whatsapp Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_EXTERNAL_STORAGE

Paketas: com.lidl.eci.lidlplus Pažeidė grupę taisyklių: L18 Pažeista taisyklė: android.permission.REQUEST_INSTALL_PACKAGES

Paketas: com.lidl.eci.lidlplus Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_FINE_LOCATION

Paketas: com.lidl.eci.lidlplus Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_COARSE_LOCATION

Paketas: com.lidl.eci.lidlplus Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_WIFI_STATE

Paketas: com.lidl.eci.lidlplus Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_EXTERNAL_STORAGE

Paketas: com.lidl.eci.lidlplus Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_PHONE_STATE

Paketas: com.gamma.scan Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_WIFI_STATE

Paketas: com.gamma.scan Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_WIFI_MULTICAST_STATE

Paketas: com.gamma.scan Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_EXTERNAL_STORAGE

Paketas: com.microsoft.skydrive Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.GET_ACCOUNTS

Paketas: com.microsoft.skydrive Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_MEDIA_LOCATION

Paketas: com.microsoft.skydrive Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.WRITE_SYNC_SETTINGS

Paketas: com.microsoft.skydrive Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_EXTERNAL_STORAGE

Paketas: com.microsoft.skydrive Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_PHONE_STATE

Paketas: com.sportsyou.sportsYou Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_EXTERNAL_STORAGE

Paketas: com.sportsyou.sportsYou Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_PHONE_STATE

Paketas: com.trafi.android.tr Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_FINE_LOCATION

Paketas: com.trafi.android.tr Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_NETWORK_STATE

Paketas: com.trafi.android.tr Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.NFC

Paketas: com.trafi.android.tr Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.NFC_PREFERRED_PAYMENT_INFO

Paketas: com.trafi.android.tr Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.NFC_TRANSACTION_EVENT

Paketas: com.trafi.android.tr Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_EXTERNAL_STORAGE

Paketas: com.bolt.deliveryclient Pažeidė grupę taisyklių: L18 Pažeista taisyklė: android.permission.REQUEST_INSTALL_PACKAGES

Paketas: com.bolt.deliveryclient Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.BROADCAST_STICKY

Paketas: com.bolt.deliveryclient Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_FINE_LOCATION

Paketas: com.bolt.deliveryclient Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_COARSE_LOCATION

Paketas: com.bolt.deliveryclient Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_EXTERNAL_STORAGE

Paketas: de.aboutyou.mobile.app Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_PHONE_SATE

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_CONTACTS

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.GET_ACCOUNTS

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_MEDIA_LOCATION

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L14 Pažeista taisyklė: android.permission.CALL_PHONE

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_FINE_LOCATION

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_COARSE_LOCATION

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L18 Pažeista taisyklė: android.permission.REQUEST_INSTALL_PACKAGES

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_WIFI_STATE

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_NETWORK_STATE

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.BLUETOOTH_ADMIN

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.BLUETOOTH

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_EXTERNAL_STORAGE

Paketas: com.airbnb.android Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_PHONE_STATE

Paketas: com.booking Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.GET_ACCOUNTS

Paketas: com.booking Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_CALENDA

Paketas: com.booking Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.NFC

Paketas: com.booking Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.NFC_PREFERRED_PAYMENT_INFO

Paketas: com.booking Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.NFC_TRANSACTION_EVENT

Paketas: com.booking Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.WRITE_SYNC_SETTINGS

Paketas: com.booking Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_FINE_LOCATION

Paketas: com.booking Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_COARSE_LOCATION

Paketas: com.booking Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_EXTERNAL_STORAGE

Paketas: com.booking Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_PHONE_STATE

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_CONTACTS

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.GET_ACCOUNTS

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L14 Pažeista taisyklė: android.permission.CALL_PHONE

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.BLUETOOTH_ADMIN

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_FINE_LOCATION

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_COARSE_LOCATION

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L9 Pažeista taisyklė: android.permission.ACCESS_BACKGROUND_LOCATION

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L3 Pažeista taisyklė: android.permission.CHANGE_NETWORK_STATE

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L10 Pažeista taisyklė: android.permission.READ_EXTERNAL_STORAGE

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.BLUETOOTH_ADMIN

Paketas: com.microsoft.teams Pažeidė grupę taisyklių: L7 Pažeista taisyklė: android.permission.BLUETOOTH

Rastų pažeidimų skaičius: 83

Įrenginyje rasti paketai, kurie pažeidžia saugumo politikos programėlių kategorijas

---

Paketas: com.whatsapp Pažeidė kategoriją:Communication

Paketas: com.gamma.scan Pažeidė kategoriją:Tools

Paketas: com.sportsyou.sportsYou Pažeidė kategoriją:Sports

Rastų pažeidimų skaičius: 3

---

2 priedas. „Google Play“ programėlių parduotuvės kategorijos ir aprašymas

Android OS programėlių parduotuvės kategorijos [28]

Kategorija	**Programėlės pavyzdžiai**
Menas ir dizainas (angl. Art and Design)	Eskizų knygos, tapytojų įrankiai, meno ir dizaino įrankiai, spalvinimo knygos
Automobiliai ir mašinos (angl. Auto and Vehicles)	Automobilių pirkimas, automobilių draudimas, automobilių kainų palyginimas, kelių saugumas, automobilių apžvalgos ir naujienos
Grožis (angl. Beauty)	Makiažo vadovėliai, plaukų stilius, grožio apsipirkimas, makiažo simuliatoriai
Knygos ir nuorodos (angl. Books and Reference)	Knygos, žinynai, vadovėliai, žodynai
Verslas (angl. Business)	Dokumentų redaktorius / skaitytuvas, nuotolinis darbalaukis, el. pašto valdymas, darbo paieška
Komiksai (angl. Comics)	Komiksai
Komunikacija (angl. Communications)	Pranešimai, pokalbiai, adresų knygos, naršyklės, skambučių valdymas
Pažintys (angl. Dating)	Piršlybos, santykių kūrimas, susitikimas su naujais žmonėmis
Edukacija (angl. Education)	Egzaminų pasirengimas, studijų priemonės, žodynas, edukaciniai žaidimai, kalbų mokymasis
Pramogos (angl. Entertainment)	Vaizdo transliacija, filmai, interaktyvios pramogos
Renginiai (angl. Events)	Koncertų bilietai, sporto renginių bilietai, bilietų perpardavimas, kino bilietai
Finansai (angl. Finance)	Bankininkystė, mokėjimas, bankomatų ieškikliai, draudimas, mokesčiai, portfelis / prekyba
Maistas ir gėrimai (angl. Food and Drink)	Receptai, restoranai, maisto gidai, vyno degustacija, gėrimų receptai

Kategorija	**Programėlės pavyzdžiai**
Sveikata ir fitnesas (angl. Health and Fitness)	Treniruočių stebėjimas, mitybos patarimai, sveikata, saugumas ir kt.
Namai (angl. House and Home)	Namų ir butų paieška, namų tobulinimas, interjero apdaila, hipotekos, nekilnojamasis turtas
Bibliotekos (angl. Libraries and Demo)	Programinės įrangos bibliotekos, techninės demonstracijos
Gyvensena (angl. Lifestyle)	Stiliaus vadovai, vestuvių ir vakarėlių planavimas
Žemėlapiai ir navigacija (angl. Maps and Navigation)	Navigacijos įrankiai, GPS, žemėlapiai, tranzito įrankiai, viešasis transportas
Medicina (angl. Medical)	Vaistai ir klinikos, sveikatos priežiūros paslaugos, medicinos žurnalai ir naujienos
Muzika ir įrašai (angl. Music and Audio)	Muzikos paslaugos, radijo imtuvai, muzikos grotuvai
Žinios ir žurnalai (angl. News and Magazines)	Laikraščiai, žurnalai, dienoraščiai
Auklėjimas (angl. Parenting)	Nėštumas, kūdikių priežiūra ir stebėsena, vaikų priežiūra
Personalizacija (angl. Personalization)	Pagrindinis ekranas, užrakto ekranas, skambėjimo tonos
Fotografija (angl. Photography)	Fotoaparatai, nuotraukų redagavimo įrankiai, nuotraukų valdymas ir bendrinimas
Produktyvumas (angl. Productivity)	Užrašų knygelė, darbų sąrašas, klaviatūra, spausdinimas, kalendorius, skaičiuotuvas, konvertavimas
Apsipirkimas (angl. Shopping)	Pirkimas internetu, aukcionai, kuponai, kainų palyginimas, maisto produktų sąrašai, produktų apžvalgos
Socialinis (angl. Social)	Socialiniai tinklai
Sportas (angl. Sports)	Sporto naujienos ir komentarai, rezultatų sekimas
Įrankiai (angl. Tools)	Įrankiai, skirti Android įrenginiams
Kelionės ir gidai (angl. Travel and Local)	Kelionės užsakymo įrankiai, dalijimasis pavėžėjimo paslaugomis, taksi, miesto gidai, vietinė verslo informacija, kelionių valdymo įrankiai, kelionių užsakymas
Vaizdo grotuvai ir medijos (angl. Video Players and Editors)	Vaizdo grotuvai, vaizdo įrašų redaktoriai, medijos saugykla
Orai (angl. Weather)	Orų ataskaitos
Žaidimai (angl. Games)	Žaidimai