VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ STUDIJŲ PROGRAMA

Apsaugos nuo duomenų vagysčių modeliai mobiliesiems įrenginiams

Usable Anti-Phishing Design Patterns for Mobile Devices

Magistro baigiamasis darbas

Atliko: Arminas Marozas

Darbo vadovė: doc. dr. Kristina Lapin

Recenzentas: doc. dr. Vytautas Čyras

Vilnius – 2025

Turinys

Santrauka

Mobiliųjų telefonų populiarumas nesustojamai auga ir žmonės nebegali įsivaizduoti savo gyvenimo be šio įrenginio. Kiekvieną dieną yra atliekami nesuskaičiuojami kiekiai operacijų ir duomenų pasidalinimų, todėl atsiranda ir sukčių, kurie šią informaciją nori pasisavinti. Jie pasitelkia ne tik elektroninius laiškus, žinutes ar skambučius, bet ir kenkėjiškas programėles. Technologinis progresas šias priemones padarė dar pavojingesnėmis. Internete surinkę informaciją apie žmonių elgseną jie duomenų viliojimo priemones padaro dar labiau efektyvesnėmis, todėl apsaugos modelių kūrimo svarba dar labiau padidėja.

Šis darbas aptaria mobiliųjų telefonų mažumą, apribojimus, ribotus resursus bei operacinių sistemų ypatumus. Taip pat atsižvelgia į žmogiškąjį faktorių, vartotojų elgsenos subtilybes, jų įpročius, prarastą budrumą, patogumų siekimą ir emocionalumą. Be to dar aprašomos statinės, euristinės priemonės, automatinių modelių trūkumai bei vartotojo sąsają keičiančių modelių panaudojamumo ir saugumo vertinimas. Prastas tokių modelių projektavimas yra opi problema, kurią reikia spręsti, kad vartotojas neliktų apgautas. Atlikti suasmenintų apsaugos ženklų modelio patobulinimai, tokie kaip garsinės bei vaizdinės reikmenos pasirinkimas bei įkėlimas į duomenų bazę, kurie pagerina efektyvumą prieš duomenų vagystes ir skatina vartotojų budrumą.

Raktiniai žodžiai: duomenų vagystė, duomenų apsauga, vartotojo sąsaja, žmogiškasis faktorius, vartotojo įpročiai, apsaugos priemonės, suasmeninti apsaugos ženklai.

Summary

The popularity of mobile phones is rapidly increasing and society is no longer able to imagine their lives without it. An incredible amount of operations and data transfers occur every day, which also results in many scammers, who want to intercept it. Not only do they use emails, messages and calls, but malicious applications as well. The progress of technology made them even more dangerous. Since the information they can gather from the Internet about the people increased the effectivness of their methods, it is imperative that defense mechanisms are created.

This work talks about the phone's small size, limitations, restricted resources and the way operating systems manage them. In addition to that, the human factor, users's behaviour, their habits and the loss of focus are taken into the consideration. Moreover, it includes static, heuristic defensive measures, the disadvantages of automatic ones and usability and security evalution of user interface changing methods. The inferior design leads to more people being affected by the attacks. The improvements, such as an inclusion of sound recordings, pictures and the possibility to save them in the database, increased personal security signs method's level of proficiency in defending against the phishing and promoted people's awareness.

Key words: phishing, data protection, user interface, awareness, human factor, habits, defense mechanisms, personal security signs.

Įvadas

Žmonės, pasitelkdami išmaniuosius įrenginius ir internetą, atranda vis daugiau informacijos, o prieiga prie banko duomenų bei slaptažodžiais apsaugotų paskyrų tapo lengvesnė. Ši tendencija atvėrė terpę plisti ir sukčiams, kurie skaitmeninėmis technologijomis sėkmingai šias detales išgauna. Per pastarąjį laikotarpį smarkiai padaugėjo didelę įtaką turėjusių išpuolių. Tai ypač pastebima po „COVID“ pandemijos [GRC+23]. Nepakako ir plačiai taikomų saugumo įrankių, tokių kaip ugniasienės ar tapatybės patvirtinimo priemonės. Šiose situacijose didžiulė problema yra ir patys nukentėję vartotojai [NB23]. Dauguma jų nelabai nori skaityti saugumo patarimų ar prisiminti ilgų slaptažodžių. Panašus rezultatas pastebimas ir su privatumo politika bei sąlygomis. Nedaugelis į jas iš tiesų įsigilina. Ilgainiui yra prarandamas budrumas ir suabejojama apgavimo tikimybe. Tokiomis aplinkybėmis žmogus yra labiau linkęs patikėti netikru elektroniniu laišku.

Šiuo darbu siekiama pagerinti jau esamas ir taikomas apsisaugojimo priemones nuo duomenų vagysčių. Išnaudodami žmonių trūkumus, sukčiai puolimais siekia prieiti prie jautrios informacijos. Jie, pavyzdžiui, elektroniniu paštu arba žinute atsiunčia nuorodą, kuri nukreipia į pažįstamą, bet šiuo atveju netikrą, prisijungimo puslapį. Per daugelį metų išpuoliai tapo asmeniškesni ir tobulesni. Į juos jau yra įtraukiamos klonuotos asmens tapatybės nustatymo priemonės, netikros programos, puslapiai ar net „QR“ kodai [BA20].

Aktualumas

Duomenys viliojami nuo seno. Pirmieji atvejai užfiksuoti ankstyvaisiais 2003 metais. Sėkmingų pažeidimų padaugėjo, nors žmonės turėjo laiko ištobulinti apsisaugojimo priemonę [AZ21]. Tai parodo, jog šioje srityje vis dar egzistuoja pažangos potencialas. Nors universalaus sprendimo pasiekti beveik neįmanoma, net ir dalinis atsparumo ir yra reikšminga žmonėms suvokti geriau.

Aukomis tampa ne tik pavieniai asmenys. Finansinę bei reputacinę žalą patiria ir kompanijos bei organizacijos [FSM+19]. Vien 2022 metais buvo atrasta daugiau nei milijonas netikrų puslapių. Bent vienas darbuotojas pabando prie vieno iš jų prisijungti. Žmonės retai tinkamai įvertina potencialias grėsmes. Įmonėms nepavyksta efektyviai jų šviesti, nepaisant prieinamų resursų.

Puolimų gausa parodo jų atnešamą naudą. Sunku pagauti žmogų, kuris nusikalto elektroninėje erdvėje, o panaikinti žalą – dar sunkiau. Kuriami modeliai apsaugo privačius duomenis ir visuomenės gerbūvį.

Naujumas

Saugumo užtikrinimas yra svarbi tema. Kiekvienais metais atsiranda didžiulis kiekis išradingų būdų apkvailinti vartotoją. Apsisaugojimo priemonės turi būti nuolat kuriamos ir tobulinamos, kad puolimai taptų pasenę ir neveiksmingi [ZRM+23].

Yra aktualu užtikrinti mobiliųjų telefonų atsparumą įvairioms grėsmėms. Pirmiausia tai įrenginys su mažesniu ekranu. Dėl šios priežasties yra sunkiau pamatyti, kad elektroninis laiškas ar žinutė yra žalingi. Tai dabartinių vartotojo sąsajų pasekmė. Daugybė įtraukiančių apsaugų atbaido vartotoją, dėl to jos yra paprastesnės. Antra, telefonai vis dar turi mažesnį atminties kiekį bei kitokį resursų valdymą nei asmeniniai kompiuteriai. Ne visos apsaugos technikos gali būti pritaikytos. Vis daugiau asmenų telefone naršo internetiniuose puslapiuose, taiko debesijos sprendimus, įsidiegia programas ir kitas priemones. Atsparumas ženkliai pagerėtų trečiųjų šalių karkasams patikrinus nuorodas ir turinį, dirbtiniam intelektui atpažinus žinutes [MSS19], vartotojams suteikus mokymus [KMI+13] ir įdiegus vartotojos sąsajos pakeitimus. Tačiau turi būti rastas balansas tarp panaudojamumo ir saugumo, kurį net su tokia daugybe priemonių yra sunku užtikrinti.

Šiame darbe vertinami vartotojo sąsają keičiantys duomenų vagysčių apsaugos modeliai, tokie kaip suasmeninti apsaugos ženklai, suasmeninti pranešimai bei būsenos juosta. Šie modeliai vartotojui padeda atpažinti, ar jo naudojama programa yra kenkėjiška. Tokio tipo modeliai pasirinkti siekiant sustiprinti žmogiškojo faktoriaus atsparumą. Atliekama kiekvieno modelio panaudojamumo ir saugumo analizė, kuri parodo modelių trūkumus bei privalumus.

Problema

Nepaisant technologinės pažangos, žmonės vis tiek tampa duomenų vagysčių aukomis. Prastai suprojektuotos vartotojo sąsajos neleidžia vartotojui tinkamai įvertinti ekrane matomo vaizdo. Mobiliųjų telefonų mažumas ir riboti resursai trukdo automatiniems modeliams efektyviai veikti, dėl to reikia surasti tokį, kuris skatintų vartotojų budrumą ir padėtų atpažinti kenkėjiškas programas. Tai pasiekiama keičiant vartotojo sąsajos elementus ir įtraukiant naudotoją.

Darbo tikslas

Šio darbo tikslas yra sukurti projektavimo rekomendacijas mobilių įrenginių vartotojų sąsajų kūrėjams ir jas iliustruojantį prototipą, skirtus pagerinti esamų apsaugos modelių, padedančių naudotojams atpažinti kenkėjiškas programas, efektyvumą. Rekomendacijos ir prototipas formuoja siūlomą naudotojų apsaugos nuo duomenų vagysčių modelį. Keliama hipotezė, kad įtraukus papildomus jutiklius, tokius kaip garsas, nuėmus kognityvinę naštą daugiau atsakomybės

perkeliant paslaugos tiekėjui bei leidžiant vartotojui keisti rodomus pranešimus arba ženklus pagal savo poreikius pagerėtų efektyvumas.

Uždaviniai

1. Identifikuoti esamų mobiliųjų telefonų problemas, jų vartotojų sąsajų pažeidžiamumus, vartotojų elgsenos ypatybes, sukčių taktikas bei esamų apsaugos modelių tipus ir veikimo principus.
2. Atlikti vartotojo sąsają keičiančių modelių, tokių kaip suasmeninti apsaugos ženklai, apsaugos pranešimai bei būsenos juosta, panaudojamumo ir saugumo analizę.
3. Suformuluoti patobulinto apsaugos modelio rekomendacijas.
4. Pagrįsti rekomendacijų tinkamumą įgyvendinus jas detaliajame prototipe ir atlikus testavimus su tikrais vartotojais.

1. Telefonų pažeidžiamumo, vartotojų elgsenos ir apsaugos modelių apžvalga

Šaltinių analizė yra padalinta į keletą poskyrių. Pirmajame yra nagrinėjama, kodėl telefonuose lengviau pavogti duomenis nei kompiuteriuose, ir kodėl ne visos naudojamos apsisaugojimo priemonės jiems tinka. Antrajame atkreipiamas dėmesys į skirtingų operacinių sistemų spragas, kurias išnaudoja puolėjai. Taip pat paminima, kaip kitos sistemos jas užtaiso. Trečiajame skyriuje analizuojama, kokios vartotojo savybės prisideda prie sėkmingų duomenų vagysčių, ir kokia jų įtaka naudojamų apsaugos modelių efektyvumui. Ketvirtajame skyriuje žiūrima, kaip į silpnąsias vartotojo savybes reaguoja piktavaliai asmenys (toliau – sukčiai), ir kaip jie šias savybes panaudoja naujoms viliojimo priemonėms kurti. Galiausiai aptariamos šiuo metu egzistuojančios apsisaugojimo priemonės. Trumpai aprašomas jų veikimo principas, kokiais programiniais įrankiais užtikrinamas informacinis saugumas, ir kokios yra rekomendacijos naujai priemonei.

1.1. Mobiliųjų telefonų pažeidžiamumas

Mobiliosios technologinės priemonės vis labiau įsitvirtina kasdienybėje. Nemaža dalis žmonių prie jų praleidžia ištisas valandas: naršo internete, skaito naujienas, bendrauja ir žaidžia žaidimus. Ilgą laiką šios veiklos buvo atliekamos tik kompiuteriais, kurie dėl savo didumo buvo pastatomi vienoje vietoje ir nejudinami. Internetas ir šių įrenginių prieinamumas plačiajai visuomenei skatino duomenų apsikeitimus ir elektroninę prekybą. Technologijoms tobulėjant atsirado mobilieji telefonai. Mažas dydis ir patogumas nešiotis lėmė jų patrauklumą. Jais daromos nuotraukos, skambinama, ir ilgainiui tapo įmanoma prisijungti prie interneto. Šiuo metu bankinės operacijos, prisijungimai prie paskyrų, internetinių puslapių tikrinimai šiuose įrenginiuose vyksta nesustodami [KJ+19] [WPL20], o jų kiekis kiekvienais metais sparčiai auga.

Finansinių operacijų internete populiarumas lėmė atsiradimą ir tų, kurie nori duomenis perimti. Prarasti finansiniai ištekliai, reputacinė žala ir tapatybės vagystė – tai tik keletas tokių veiksmų padarinių pavyzdžių. Pradėtos kurti apsisaugojimo priemonės, kad kiekvieno vartotojo duomenys išliktų saugūs. Didėjantis mobiliųjų telefonų vartotojų skaičius lemia padažnėjusias duomenų vagystes, o kartu su tuo ir aukštesnį duomenų apsaugos poreikį [GDJ18] [KJ+19] [WPL20] [SAP+21] [PTM+22] [GSB21] [VA16].

Mobilieji telefonai apsunkina apsisaugojimo priemonių kūrimą. Jie technologiškai skiriasi nuo kompiuterių, sparčiau vystosi ir vartotojai jiems kelia kitokius reikalavimus. Šie įrenginiai yra maži, ir pasižymi ekranu, į kurį žmogui žiūrėti yra mažiau patogu. Be to, jiems prieinamas ribotas resursų kiekis, todėl reikalinga geresnė optimizacija [GDJ18] [KJ+19] [ND19] [SAP+21] [CPS16] [VA16]. Taip pat, mobiliuosius telefonus būtina dažniau atnaujinti, nes jie neretai veikia

neapsaugotoje oro uostų ir kavinių tinklo aplinkoje. Šių įrenginių vartotojams būdingas saugumo nuvertinimas, nes dažnas renkasi spartesnį duomenų užkrovimą bei prisijungimą.

Ilgą laiką apsaugos priemonės buvo kuriamos tik kompiuteriams, o mobiliesiems telefonams dažnai skiriama per mažai dėmesio. Dėl esminių skirtumų tarp šių įrenginių, kompiuteriams sukurti sprendimai dažnai tiesiogiai negali būti pritaikomi telefonams [GDJ18] [PTM+22] [CPS16] [VA16]. Automatiškai neatitikimų ieškančios programos greičiau iškrautų bateriją, pasiimtų visus reikalingus įrenginio išteklius, ir trukdytų vartotojui naudotis įrenginiu. Tai pasireikštų nuolatinėmis įspėjamosiomis žinutėmis ir stringančiomis programomis. Programuotojai buvo priversi keisti elementų išdėstymą ekrane dėl mažesnio įrenginio ekrano. Noras parodyti tik svarbiausią informaciją lėmė paprastesnių vartotojo sąsajų, kurias sukčiams paprasčiau atkartoti, atsiradimą.

Kartu keitėsi ir vartotojų įpročiai. Net mažiau technologiškai išprusę asmenys galėjo pradėti naudotis telefonu. Taip nutiko dėl paprastesnio paruošimo naudotis, lengvesnio valdymo pirštu bei mažesnio ekrane rodomo informacijos kiekio. Tokia tendencija pastebėta pandemijos metu, kai žmonės turėjo daugiau laiko mobiliuosius įrenginius išbandyti.

Telefonas buvo kurtas su mintimi, kad našumas yra svarbiausias. Tai greičiausiai vartotojo pamatoma ir įvertinama įrenginio charakteristika. Greitas duomenų ir puslapių užkrovimas bei momentinė reakcija yra labai vertinami. Tai ypač svarbu laikais, kai įrenginį galima panaudoti ne tik skambučiams. Tam, kad šie tikslai būtų įgyvendinti kažkas turėjo būti paaukota. Kūrėjai nusprendė nevarginti apsauginiais prašymais, kad nesumenkintų vartotojų potyrių, nors apsaugos priemonės ir mokymai yra ypač svarbūs šių laikų kontekste. Viena iš tokio aplaidumo pasekmių yra tokia, kad internetinis puslapis, kompiuteryje rodomas kaip užblokuotas, bus atidarytas mobiliojo telefono naršyklėse [WLD+15]. Šiuose įrenginiuose jų funkcijos buvo supaprastintos, kas neigiamai paveikė panaudojamumą. Siekiant sutaupyti vietą atsisakyta kelių langų atidarymo vienu metu, plėtinių palaikymo ir lankstesnio sausainių (angl. *cookies*) valdymo [WLD+15]. Tokiu būdu sumažėjo iššokančių langų bei naršyklės juostos elementų skaičius, ekranas tapo vientisesnis ir mažiau reikalavo nustatymų. Navigacija taip pat buvo supaprastinta. Vartotojui nebereikia praeiti per tiek daug sąveikos lygių [VA16].

Kompiuterių naršyklės išliko galingesnės. Jose galima peržiūrėti visą internetinį adresą, elektroninio pašto siuntėjo duomenis bei detalią antraštės informaciją [SAP+21]. Telefone ši informacija nėra parodoma arba jos nesimato. Vartotojui reikia paspausti daugiau mygtukų, kad, pavyzdžiui, išsiaiškintų daugiau apie siųstą elektroninį laišką [VA16]. Tai reikalauja daugiau pastangų ir laiko. Prie to prisidėjo ir kintantis atvaizdavimo dizainas. Interaktyvios nuorodos nebėra pabraukiamos, o mygtukus pakeitė piktogramos. Tokią raidą lėmė žmonių įpročiai ir įgyjami gebėjimai. Technologijų veikimo principas tampa savaime suprantamas. Tačiau šis

progresas privedė prie sumažėjusio budrumo ir pastabumo. Vartotojai nepamato, kad elektroninis laiškas išsiųstas iš netikro pašto adreso. Atliekami veiksmai patapo greiti ir neapgalvoti. Toks elgesys padidina duomenų vagysčių sėkmės tikimybę [VA16]. Reklamuojamas pagerintas naujų telefonų saugumas sukuria iliuziją, kad atakos nėra įmanomos. Žmonės nebeatkreipia dėmesio į įvairaus tipo įspėjamuosius pranešimus, nes sumažėjo dėmesio išlaikymo trukmė.

Dizaino pritaikymas mobiliesiems telefonams sukūrė keletą specifinių problemų. Viena tokių yra labai arti vienas kito esantys klaviatūros elementai. Sukčiai nuspėja paspaudžiamus mygtukus stebėdami vartotojų akių judesius [KJ+19]. Kita bėda yra išimti statuso laukai bei sutrumpintos nuorodos, kad ekrane būtų daugiau vietos. Vartotojui tampa sunkiau įvertinti atidaromo puslapio teisėtumą [WLD+15]. Programėlės bei internetiniai puslapiai tapo paprastesni, sukčiams lengva apsimesti viena iš jų, atkartojus matomą vaizdą [MC+16], o vartotojas, matydamas pažįstamą prisijungimo langą, suveda savo prisijungimo duomenis, kuriuos netikra programa pasisavina. Prie problemos prisideda ir greitas programėlių perjunginėjimas – nukenčia pastabumas, kai peržiūrėjus informaciją vienoje, greitai perjungiama kita [GDJ18] [WPL20].

Modernizacija ir paprastinimas ne visur matomas. Operacinių sistemų išvaizda nuo pat sukūrimo pradžios radikaliai nesikeitė [VA16]. Žmonės vis labiau pripranta prie įrenginio naudojimo, bet tai skatina budrumo praradimą. Dažnas elementų išdėstymo keitimas padėtų, bet sukeltų nepasitenkinimą dėl padidėjusio nepatogumo. Tai sukelia iššūkį rasti pastabumą skatinantį sprendimą, kuris išlaikytų vartotojui priimtiną paprastumą.

Apibendrinant, mobiliųjų telefonų saugumas yra kaip niekad svarbus dėl jų populiarumo ir pažeidžiamumo. Šiems įrenginiams reikalingas atskiras dėmesys, nes:

- didėja jų populiarumas;
- atsisakyta daug funkcijų siekiant sutaupyti ekrano vietą;
- automatinės apsisaugojimo priemonės eikvoja ribotus resursus ir trukdo naudotis įrenginiu;
- žmonės priprato prie naudojimo, todėl veiksmai tapo greiti ir neapgalvoti;
- paprastesnę vartotojo sąsają lengviau atkartoti.

1.2. Mobiliųjų telefonų operacinių sistemų spragos

Operacinė sistema užtikrina sąveiką tarp techninių įrenginio komponentų, programų ir vartotojo sąsajos. Ji yra atsakinga už duomenų valdymą, taikomųjų programų paleidimą bei resursų paskirstymą. Mobiliuosiuose telefonuose šis procesas dažniau vyksta tuomet, kai programa perkeliama į foną, arba kai kitai programai pritrūksta darbinės atminties. Duomenų apsaugos uždavinys šiuose įrenginiuose pasunkėja ir dėl griežto sistemos prieigų valdymo [GSB21]. Tokia savybė stiprina vartotojo privatumą, bet sudaro sąlygas kenkėjiškoms programos pasislėpti nuo automatinių aptikimo priemonių. Tokios programos apsimeta tvarkingomis, paprašo

leidimų valdyti duomenis, ir neteisėtai juos pasisavina. Jų žalą bei veikimo principą yra sunku aptikti dėl izoliuotos programos aplinkos. Kadangi operacinės sistemos tai įgyvendina nevienodai, sukčiai pasinaudoja šiais skirtumais savo tikslams pasiekti. Šiuo metu didžiausią rinkos dalį užima „Android“ ir „iOS“ operacinės sistemos [ND19] [HA+21].

Kiekviena jų turi savą kodo tvarkymo politiką. Pirmosios pirminis kodas yra atviras visiems (angl: *open source*) [GSB21]. Tai palengvina sisteminių spragų radimą bei skatina visuomenės įsitraukimą į jų šalinimą. Sudaroma galimybė teikti pasiūlymus ir inicijuoti pakeitimus. Tačiau atsiranda žmonių, kurie apie rastus trūkumus nepraneša ir juos išnaudoja savo tikslams. Nepatikimos pigių telefonu kompanijos tuo pasinaudoja. Jos pakeičia sistemą taip, kad gautų naudotojo jautrius duomenis. Tokiu atveju net garso įrašymo programėlė teikia informaciją trečiųjų šalių serveriams [WPL20]. „iOS“ operacinė sistema neturi atviro pirminio kodo. „Apple“ kontroliuoja techninę ir programinę įrangą bei duomenų šifravimą [GSB21] [HA+21]. Tai sumažina nežinomų pakeitimų grėsmę, bet potencialūs pažeidimai ilgiau išlieka nepastebėti. Vartotojai negali pagal save pasikeisti sistemos išvaizdos, o švaresnis ir nekintantis dizainas dar labiau sumažina budrumą. Sukčiai panaudoja iššokančius langus, kurie atrodo kaip sisteminiai.

Skirtingas programėlių platinimas taip pat turi įtakos saugumui. „Android“ programų kūrėjams savo kūrinį leidžiama įkelti bet kur [GSB21]. Jiems nereikia jokio sertifikato ar patvirtinimo. Tai vis dar išlieka opi problema, nors „Google“ šią politiką griežtina. Plinta daug netikrų programų, kai jų sklaida yra neprižiūrima. „iOS“ programų kūrėjams programą leidžiama įkelti tik į oficialią platformą [GSB21]. Programuotojams reikia prisiregistruoti, gauti licenciją, patvirtinimą bei įrodyti tapatybę. Taip stabdomas netikrų programų plitimas, tačiau vartotojai pradeda per daug pasitikėti parsisiųstų programų saugumu. Patikrą praeina ir žinomą prekės ženklą imituojančios programos, ir tos, kurios duomenų vagystes pradeda vėliau.

Kita išryškėjanti problema yra susijusi su prieigos leidimų suteikimu. Operacinės sistemos draudžia programoms be vartotojo leidimo panaudoti tam tikrą telefono funkcionalumą, pavyzdžiui, įrenginio koordinačių gavimą. Kenksmingos programėlės priverčia vartotoją suteikti prieigą prie tokios informacijos. „Android“ visų reikalingų leidimų prašo iškart. Žmonės, norėdami kuo greičiau pradėti naudotis programėle, juos suteikia nežinodami ir net negalvodami, kokiu tikslu jie bus panaudoti. „iOS“ leidimų paprašo tik tada, kai ši informacija reikalinga [GSB21]. Šitaip siekiama suteikti vartotojui aiškumo dėl leidimo paskirties, tačiau pasitaiko atvejų, kai prieiga prie, pavyzdžiui, nuotraukų galerijos, suteikiama impulsyviai ir neapgalvotai.

Sukčiai puolimuose pritaiko ir resursų valdymo niuansus. „Android“ telefone kenksmingos programėlės fone stebi, kada naudotojas nori atidaryti kurią nors programą, ir tada atidaro blogąją [GDJ18] [MC+16] [GSB21]. „iOS“ sistema automatiškai valdo foninius procesus, paskirsto sistemos resursus bei pristabdo ilgesnį laiką nepanaudojamas programėles. Tačiau tai neapsaugo

sistemos nuo pavojų. Jeigu vartotojas paspaudžia ant netinkamos nuorodos, abiejų sistemų telefonuose įdiegiamas kenkėjiškas kodas. Jis gauna prieigą nuskaityti bei įrašyti bet kokią programinę įrangą. Tokie virusai paskleidžia save per lokalų tinklą, atidaro netikrus dialogus tikrų programų veikimo metu, ir perskaito slaptažodžius [HA+21]. Vartotojas pagalvoja, kad iššokęs ir prisijungimo duomenų reikalaujantis langas yra dalis naudojamos programos, nors jį atidarė piktybinė programa [GDJ18] [MC+16]. Kai kuriais atvejais programos vartotojus ragina pasidalinti pasiekimais socialiniuose tinkluose, o nusprendus tai padaryti, atveria netikrus jų puslapius [GDJ18]. Tam, kad tokių sumažėtų tokių incidentų, organizuojami vartotojų mokymai.

Apibendrinant, operacinė sistema yra svarbi mobiliojo telefono dalis. Ji yra dažnai atnaujinama ir tobulinama, tačiau pasitiko spragų, kurias sukčiai išnaudoja savo tikslams pasiekti. Kiekvienai jų yra būdingos tam tikros savybės. Vienos jų panaudojamos duomenų vagysčių išpuoliuose, kitos – veikia kaip apsaugos priemonės, neleidžiančios joms įvykti:

- izoliuoti programų katalogai didina vartotojų privatumą, tačiau apsunkina kenkėjiškų programų aptikimą;
- „Android“ kodas yra atviras visiems, kas skatina visuomenės įsitraukimą, tačiau pigių telefonų kompanijos tuo pasinaudoja įdiegdamos kenkėjiškas programas;
- „iOS“ kodas nėra visiems prieinamas, kas sumažina nežinomų pakeitimų grėsmę, bet potencialūs pažeidimai ilgiau lieka nepastebėti;
- „Android“ programas leidžiama platinti visur, kas didina kenkėjiškų programų skaičių;
- „iOS“ programos įkeliamos tik į vieną platformą, kas sukuria saugumo iliuziją;
- vartotojai neapdariai suteikia programoms leidimus prieiti prie, pavyzdžiui, nuotraukų galerijos;
- „Android“ kenkėjiška programa atsidaro, kai būdama fone pamato tinkamą momentą;
- paspaustos nuorodos įrašo programinę įrangą, atidaro netikras programėles, dialogus ar internetinius puslapius, kurie atrodo patikimi, bet siunčia įrašytus duomenis į trečiųjų šalių serverius.

1.3. Mobiliųjų telefonų vartotojų elgsena

Prisitaikymas prie vartotojo elgsenos ypatumų yra didžiausias šiai dienai žinomas iššūkis [WPL20]. Sunku užtikrinti geras žinias apie saugumą, tinkamą reakciją į atėjusį pranešimą, ar išmokyti nepaspausti ant neaiškios nuorodos. Didžioji dalis visuomenės dar nėra pakankamai technologiškai išprusę, kad iškart atpažintų, jog kažkas ekrane atrodo negerai [ND19] [CPS16]. Žmonės dažnai nepaiso saugumo reikalavimų dėl prastų projektinių sprendimų. Jie išjungia apsaugines programas, duoda konfidencialią informaciją kitiems, siunčiasi programas iš neoficialių vietų bei jungiasi prie nesaugių interneto tinklų [WPL20]. Vartotojai tikisi automatinio

saugumo užtikrinimo, nenori atlikti daug veiksmų, duoda pirmenybę patogumui, nesitiki duomenų vagystės bei nemato apsaugos veiksmų tikslo [P16].

Vartotojo reakciją į duomenų vagystės bandymą lemia ir jo charakteris. Nervingi žmonės dažnai jaučia negatyvias emocijas, dėl ko dažniau tampa aukomis. Taip atsitinka, kai elektroninis laiškas yra gąsdinantis, atkreipiantis dėmesį į jų baimes ir nerimą [GDJ18] [LPS21]. Emocionalesni ar stresą patiriantys asmenys dažniau pasiduoda įtikinėjimams, nes šie jausmai iššaukia neapgalvotą sprendimų priėmimą [LPS21]. Prie lengviau pasiduodančių priskiriami ir ekstravertai, nes jie labiau pasitiki kitais [LPS21].

Socialinis statusas irgi daro įtaką vartotojo elgsenai. Požiūrį į apsaugos priemones formuoja ekonomika, kultūra, pajamos bei aplaidumas [ND19] [PTM+22]. Žmonės, ypač paaugliai, turi prastas saugumo elektroninėje erdvėje žinias [GDJ18] [PTM+22]. Nuolatinis mokymas užtikrina gebėjimą atpažinti net pačias naujausias duomenų vagysčių technikas. Tai gelbėja asmenį nuo finansinės ir reputacinės žalos.

Greitas gyvenimo būdas mažina vartotojo budrumą. Žmonės yra nuolatos apsupti didžiuliu ir besikeičiančiu informacijos kiekiu. Jiems vis sunkiau išlaikyti dėmesį ilgesniam laikui [ND19]. Valgydami klausosi pokalbių, eidami – muzikos, o gyvą komunikaciją pakeitė skaitmenine dėl efektyvumo. Telefonas nukreipia dėmesį, mažina koncentraciją bei didina neapgalvotų veiksmų tikimybę. Dėl to neįvertinama atėjusios žinutės svarba, paspaudžiama atsitiktinė nuoroda, ir patikima atėjusiu piktybiniu elektroniniu laišku.

Pripratimas prie pažįstamos vartotojo sąsajos mažina pastabumą. Nors žinomas išdėstymas mažina kognityvinę apkrovą bei pagreitina išmokimą, tas pats vaizdas, elementai, teksto dydžiai ilgainiui sukelia šalutinį poveikį [VA16]. Veiksmai atliekami greičiau nei apie juos spėjama pagalvoti, o tuo pasinaudoja kenkėjiškos programos, kurių vartotojo sąsaja tik šiek tiek skiriasi nuo vartotojams priimtinos [WLD+15].

Vartotojai ignoruoja įspėjamuosius pranešimus [GDJ18] [VA16]. Šiais laikais jų yra tiek daug, kad neįmanoma į visus reaguoti. Dažniausiai praleidžiami ne laiku arba įkyriai rodomi pranešimai bei reklamos. Dėl šios tendencijos retkarčiais pasitaikanti svarbesnė informacija irgi yra nepaisoma, net jeigu žmogui rūpi saugumas [ND19].

Naudotojai labiausiai vertina patogumą bei įpročius. Dauguma žmonių atsikėlę pirmiausia tikrina naujienas ir atėjusias žinutes. Net 72 procentai asmenų, ryte atėję į darbą, telefone tikrina elektroninį paštą [CM+21]. Po „COVID-19" pandemijos padaugėjo elektroninių nusikaltimų. Sukčiai išnaudoja tai, kad žmonės vis daugiau laiko praleidžia internete [LPS21]. Naršymas jame tapo toks įprastas, kad yra įgyjamas saugumo jausmas, suabejojama duomenų vagystės tikimybe ar jos sėkme. Dėl greitumo ir patogumo vartotojai susikuria paprastus slaptažodžius. Rankinis jų įrašymas vargina, dėl to dažnas susigundo paspausti ant vienu mygtuko paspaudimu kažkur

nuvedančios nuorodos [WLD+15]. Prie problemos masto prisideda ir prastas sąsajų projektavimas. Norėdamas pamatyti visą elektroninio laiško informaciją, vartotojas turi toli naviguoti. Kūrėjai turėtų atkreipti į tai dėmesį.

Apibendrinant, jeigu norime kurti saugias programėles, turime suprasti žmogaus požiūrį į privatumą ir saugumą [WPL20]. Projektuotojai turėtų atsižvelgti į vartotojų žmogiškumą, įpročius ir norus. Kiekvienas asmuo prioretizuoja patogumą ir tikisi, kad viskas bus pasiekta greitai ir be trikdžių. Dažnai pasirodantys pranešimai ar reikalavimai apkartina naudojimo potyrius. Šiomis žiniomis pasinaudoję sukčiai atlieka duomenų vagystes. Jų sėkmę lemia žmogaus:

- charakterio savybės, tokios kaip nervingumas ir emocionalumas;
- socialinis statusas, kuris lemia požiūrį į saugumą;
- greitas gyvenimo būdas, kuris didina neapgalvotų veiksmų tikimybę;
- pripratimas prie vartotojo sąsajų, kas mažina kognityvinę apkrovą, bet ir budrumą;
- įspėjamųjų pranešimų vengimas, kas įvyksta dėl jų įkyrumo;
- įpročiai, kai vis daugiau laiko praleidžiama internete.

1.4. Mobiliųjų telefonų duomenų viliojimo principai

Sukčiai pasitelkia žinias apie mobiliųjų telefonų problemas ir žmonių psichologines subtilybes kurdami naujas duomenų viliojimo technikas. Tai nėra vienintelė priežastis, lemianti šių modelių sėkmę, tačiau tai padidina jų efektyvumą. Su duomenų vagystėmis labiausiai asocijuojasi elektroniniai laiškai, skambučiai, ar žinutės, skirtos jautriai informacijai išgauti, tačiau mobiliųjų telefonų rinkoje dominuoja kenkėjiškos programos [GDJ18] [MC+16] [CPS16].

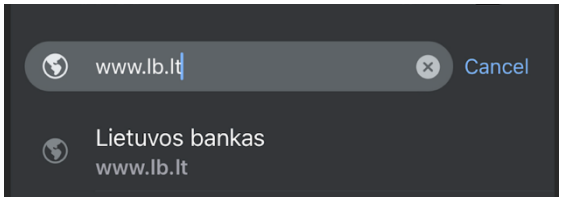
Įdiegta piktybinė programėlė pridaro daug žalos. Vartotojui suteikus leidimą, ji prieina prie įvairaus pobūdžio informacijos: buvimo vietos, žinučių, kontaktų ar nuotraukų [GDJ18] [CPS16]. Sukčiai tikisi, kad vartotojas leis prieiti skubotai ir neapgalvojęs pasekmių. Labiausiai tikėtina, jog tokį tikslą turės programėlės, parsiųstos iš neoficialios svetainės, ar įdiegtos po neaiškios nuorodos paspaudimo. Po tokių veiksmų mobiliajame telefone atsiranda ne tik naudinga apsimetinėjanti programėlė, bet kartu ir įvairūs papildiniai, kurie siekia priėjimo prie duomenų ar išnaudoti įrenginį. Vartotojui nežinant plėtiniai gaunami kartu su, pavyzdžiui, reklamuojamu žaidimu. Vienas iš pavyzdžių yra kriptovaliutų kasimo įrankiai, kurie naudoja įrenginio resursus ir neigiamai veikia vartotojo patirtį [WPL20]. Kitas pavyzdys – virusai. Jų tikslas yra išnaudoti operacinę sistemą ir pamėginti apgauti žmogų. Jie stebi, kada vartotojas mėgina atidaryti tikrąją programą, ir tuo momentu inicijuoja netikros programos atidarymą. Taip pat matydami, kokios programos yra atvertos, generuoja iššokančius langus, kurie prašo prisijungti. Taip prisijungimo duomenys atiduodami kitiems asmenims [WLD+15] [CPS16]. Jie taip pat sugeba užsiregistruoti sistemoje kaip visai kito pobūdžio programos. Įdiegtas žaidimas pasirodo kaip socialinis tinklas

[WLD+15]. Tokias programas sunku sugauti, nes negalima tiksliai pasakyti, kur iškeliauja inicijuota užklausa programą atidarius.

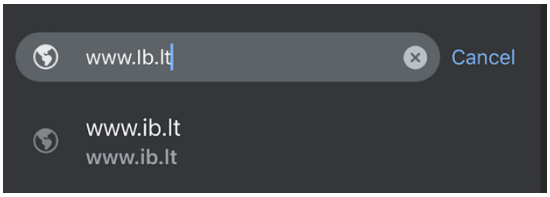
Daugiausiai pasitikėdami kenkėjiškomis programomis, sukčiai vis dar pasitelkia elektroninius laiškus bei žinutes duomenimis išvilioti. Ilgainiui šių laiškų rašymo būdas bei kokybė pagerėjo. Šiais laikais dauguma žmonių turi skaitmeninį pėdsaką (angl. *digital footprint*), kuris susidaro naudojantis internetu ar įrenginiais. Sukčiai išsiaiškina apie vartotojų įpročius bei elgseną įvertinę socialinius tinklus bei straipsnius. Surinkus didelį kiekį informacijos apie tikslinį asmenį, netikri elektroniniai laiškai tampa itin asmeniški ir įtikinami. Dirbtinis intelektas šią situaciją dar labiau pablogino, nes tapo lengviau rinkti, apibendrinti ir pasitelkti informaciją. Laiškuose pradėtas naudoti ir prekės ženklo panašumas. Pamatęs figūruojančią žinomos kompanijos, socialinio tinklo ar banko ženklą, žmogus pirmiausia pagalvoja, jog laiškas yra tikras. Prie žinučių įtikinamumo prisideda ir apeliavimas į baimes bei patriotizmą. Šis būdas buvo pasitelktas „COVID-19" pandemijos metu, kai žmonės nežinojo, kuo pasitikėti. Sukčiai pasinaudoja ir nerimu, kurį sukelia potenciali karo grėsmė. Efektui sustiprinti įdedami ir įvairūs paveiksliukai bei simboliai, kad būtų sumažinamas dėmesys [SAP+21]. Naudojamos ir piktogramos, kurios asocijuojamos su teisėtų siuntėju. Taip padidėja šansas, kad žmogus patikės laiške esančiu turiniu [VA16]. Tai ypač koreliuoja su tuo, kad dėl budrumo stokos, ar įgytų įpročių, vartotojai neįvertina klastos. Laiškuose aprašoma plačiai žinoma bėda, vyrauja skatinimas, naudojami plačiai žinomi adresai, valstybinių įstaigų šriftai ir fonai, kurie asocijuojami su patikimu [SAP+21]. Nors dauguma elektroninių laiškų programų naudoja piktybinių laiškų aptikimo priemones, jos neapsaugo nuo visų su tuo susijusių pavojų. Dėl šios priežasties programų kūrėjai turėtų projektuoti taip, kad vartotojas aiškiai atpažintų, jog atidarė patikimą programą. Tokia priemonė būtų ypač svarbi situacijose, kai vartotojai, patikėję gautu elektroniniu laišku, paspaustų ant pateiktos nuorodos ir įsidiegtų kenkėjišką programą.

Greito atsakymo (angl. *quick response* arba *QR*) kodai taip pat paverčiami puolimo įrankiais. Jie yra pakankamai lengvai sukuriami, patogūs, veikia be prieigos prie interneto, ir jais pasitiki, nes didžiosios kompanijos juos pasitelkia. Sukčiai į šiuos kodus prideda kenkėjiškas nuorodas, su jais inicijuoja automatinį programos įrašymą, ar sukuria užklausą perversti pinigus, o iš anksto nuspėti, ką šis kodas padarys, nėra įmanoma [SS+20].

Sukčiai išnaudoja ir internetines nuorodas. Siekdami suklaidinti vartotoją, jie apkeičia vizualiai vienodai atrodančias raides. Pavyzdžiui, l ir L yra labai panašios, ir tai klaidina vartotoją [WLD+15]. www.lb.lt (**Error! Reference source not found.** pav.) ir www.Ib.lt (***Error! Reference source not found.*** pav.) yra lengvai sumaišomos ir šituo yra dažnai pasinaudojama. Dėl riboto matomų nuorodų ilgio tai dar sunkiau pastebėti. Vartotojas mato tik nuorodos pradžią, o sukeistos raidės dažniausiai būna jos gale [WLD+15].



1 pav. Nuoroda su mažąja L raide



2 pav. Nuoroda su didžiąja i raide

Apibendrinant, sukčiai pasitelkia žinias apie operacinių sistemų spragas ir žmonių psichologiją. Jie jas panaudoja kurdami įvairius duomenų viliojimo modelius:

- įdiegiamos kenkėjiškos programos, virusai, plėtiniai;
- siunčiami suasmeninti elektroniniai laiškai bei žinutės;
- sukuriami kenkėjiški greito atsakymo kodai;
- išnaudojamos vizualiai panašios raidės nuorodose.

1.5. Mobiliųjų telefonų apsaugojimo priemonės

Mobiliesiems telefonams apsaugoti pasitelkiamos įvairios priemonės. Vienos naudoja dirbtinį intelektą bei kitas automatines priemones, kad aptiktų kenkėjiškas programas bei netikrus puslapius, kitos vertina ekrane esančią informaciją, internetinį adresą, laiško stilistiką bei elementų išdėstymą. Prie apsaugos prisideda ir vartotojų mokymai bei atidumo stiprinimas pasitelkiant informatyvius pranešimus ir kitus vartotojo sąsają papildančius elementus. Kartu su technologijų tobulėjimu auga ir sukčių žinios, todėl apsisaugojimo metodikos turi būti nuolatos gerinamos.

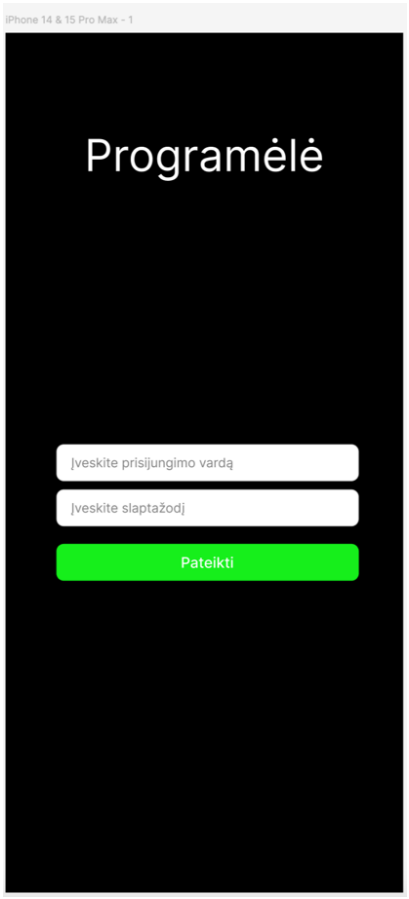
Vieną kategoriją sudaro statinės aptikimo priemonės [CPS16] [WLD+15]. Jos naudoja nustatytas taisykles ir kriterijus, kad aptiktų ir užblokuotų vykstančius puolimus. Puslapių adresų talpinimas į duomenų bazę yra vienas tokių modelių. Jis yra labiausiai paplitęs ir naudojamas su įvairias įrankiais ir įskiepiais [CPS16] [WLD+15]. Vartotojas yra įspėjamas arba prieiga yra užblokuojama, kai paieškos laukelyje įvestas ir patikrintas internetinis adresas yra piktybinių arba netikrų nuorodų sąraše. Šio modelio esminis trūkumas – nuolatinis poreikis šį sąrašą pildyti, kad informacija išliktų aktuali ir nepasentų. Kasdien sukuriami tūkstančiai internetinių puslapių, iš kurių dalis yra netikri ir piktybiniai. Būtina šiuos puslapius aptikti, patirti jų poveikį, apie juos pranešti ir rankiniu būdu įtraukti į sąrašą, todėl šis modelis nėra veiksmingas prieš nulinės dienos puolimus, kai puslapis tik ką atsirado [GDJ18] [CPS16]. „PhishTank“ yra vienas iš šią metodiką naudojančių įrankių. Tai puslapis, kuriame tokios svetainės fiksuojamos. Jame taip pat yra pateikiamos instrukcijos programuotojams, kaip šią sukauptą informaciją panaudoti programėlėse, kuriose ypač svarbus apsisaugojimas nuo duomenų vagysčių [GDJ18] [CPS16].

Kita kategorija – euristinės aptikimo priemonės [CPS16] [WLD+15]. Jos fokusuojasi į ženklus bei iš patirties atpažįstamus elementus ir reiškinius. Analizuojamos internetinės nuorodos,

laiškai, ekrane matomas skaitmeninis turinys bei išgautas kodas. Jų tikslas – atrasti bendrus duomenų vagystėms būdingus bruožus. Naudojant šį būdą bandoma aptikti gramatikos klaidas, keistai išdėstytus sakinius, neteisingai vartojamas frazes ar raktinius žodžius, kurie dažnai pasitaiko elektroniniuose laiškuose ar puslapiuose. Žiūrima, ar nėra užsimenama apie pinigus, neprašoma bankinių duomenų, neskubinami veiksmai. Tikrinama, ar laiško siuntėjas nefigūravo duomenų viliojimo skandale, ar puslapis patalpintas patikimuose serveriuose ir kaip svetainę vertina paieškos varikliai. Nuskenavus „HTML“ kodą tikrinamas domeno amžius, puslapio reitingas, prisijungimo formos apsaugos lygis, ar nėra paslėptų duomenų vagystės elementų, neaiškių peradresavimų bei kitų įtartinų vietų [CPS16]. Mobiliuosiuose telefonuose šį būdą patogu taikyti dėl mažo ekrano dydžio, paprastų vartotojo sąsajų, aiškiai matomų nuotraukų ir pavadinimų [WLD+15]. Šio modelio minusas – gerai situaciją išmanantys sukčiai problemines vietas užgožia įvairiais tekstais, nuorodomis bei padidintomis nuotraukomis, o ieškomais raktiniais žodžiais manipuliuoja pasitelkdami žinomų kompanijų logotipus ir prekės ženklus [WLD+15]. „MobiFish“ yra vienas iš tokią metodiką naudojančių įrankių. Jis pirmiausia patikrina, ar internetinė nuoroda nėra „IP“ adresas, o vėliau matomas nuotraukas paverčia tekstu siekdamas nustatyti, ar domeno pavadinimas nuorodoje atitinka sugeneruotą prekės ženklo tekstą [CPS16] [WLD+15]. Kitos šio įrankio dalys tikrina naudotojo „ID“, paleidimo laiką, užklausas į serverį bei bandomų pridėti programų pavadinimų sutapimą [CPS16] [WLD+15]. Kitas tokio pobūdžio įrankis yra „GoldPhish“, bet jis naudojamas kompiuterių naršyklėse [WLD+15].

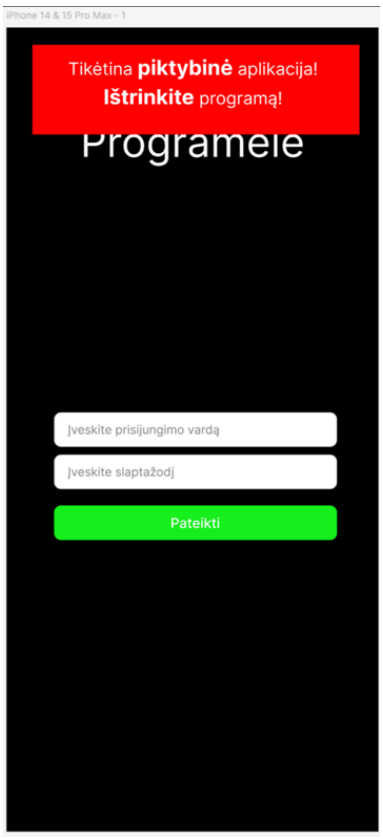
Trečia kategorija – vartotojo sąsają keičiančios priemonės. Jos pasitelkia vaizdo modifikacijas siekdamos padėti vartotojams pastebėti puolimus, pristabdyti automatinę elgseną bei atbaidyti sukčius nuo programėlių ar internetinių puslapių imitavimo. Viena iš tokių priemonių yra asmeniniai apsaugos ženklai [MC+16]. Registracijos metu pasirenkama nuotrauka, kuri yra išsaugojama tik tai programai prieinamame kataloge. Matydamas ją prisijungimo metu, vartotojas yra užtikrintas, kad tai tikrai ta programa, kurios jam reikia. Pirmajame paveikslėlyje (3 pav.) rodomas paprastos programėlės prisijungimo langas, kuriame matoma ekrano viduryje esanti žvaigždė. Šis vartotojo pasirinktas indikatorius yra visada parodomas. Antrojoje nuotraukoje (4 pav.) ši žvaigždė nematoma, o tai rodo, jog tai netinkama programa. Tai žinodamas vartotojas neapsigauna ir sužino apie įrenginyje vykstančią neleistiną veiklą. Ši priemonė ne tik gerina pastabumą, bet ir yra lengvai įtraukiama į programėlę. Šis modelis leidžia išvengti operacinės sistemos spragos, kuri leidžia stebėti vartotojo veiksmus, ir atidaryti kitas programėles jam nežinant [MC+16] [WLD+15]. Nors jis yra veiksmingas, pasitaiko asmenų, kurie netinkamai įvertina situaciją galvodami apie interneto arba naršyklės problemas, kai pasirinkta nuotrauka nėra parodoma, arba tų, kurie pasirenka pačią pirmą nuotrauką, kad procesas būtų greitesnis [MC+16].

3 pav. Rodomas asmeninis ženklas



4 pav. Nerodomas asmeninis ženklas

Kita priemonė – suasmeninti apsaugos pranešimai. Žmonės ignoruoja svarbius pranešimus, nes juose rodoma per daug teksto, ir jie per dažnai ir netinkamu laiku rodomi. Norint to išvengti, būtina sudaryti galimybę koreguoti pranešimų parametrus. Labai gerai vertinamas informacijos kiekio bei rodymo dažnumo keitimas: geriausi pranešimai yra trumpi, su dideliu šriftu bei su paryškintomis svarbiausiomis vietomis. Vartotojai yra labiau linkę atlikti reikalingus veiksmus, kai pranešime matomos instrukcijos [ND19]. Jų budrumų skatina ir įtraukiamos spalvos, kurios kiekvienam vartotojui turi specifinę reikšmę [ND19]. Pavyzdžiui, raudonos spalvos pranešimas simbolizuotų pavojų ir skubą (5 pav.).



5 pav. Raudonas pranešimas su trumpu tekstu, instrukcija bei paryškintais svarbiausias žodžiais

Dar viena vartotojo sąsają keičianti priemonė – būsenos juosta (6 pav.). Joje atvaizduojamas programos pavadinimas bei kūrėjas. Prie šitos priemonės priskiriami ir kiti vizualiniai pakeitimai, įrodantys programos autentiškumą, tokie kaip vandens ženklas ar piktograma (7 pav.) [CPS16]. Matydamas šią informaciją vartotojas įvertina, kokią programą yra atsidaręs. Tačiau šis modelis turi keletą trūkumų. Pirmasis, kuris sutvarkomas leidus nustatymuose ją išjungti, yra tai, kad ši juosta užima dalį ir taip mažo mobiliojo telefono ekrano. Antras – jis reikalauja operacinės sistemos pakeitimo, atskiros programos arba dažno rodomos informacijos kaitaliojimo, kas neigiamai paveikia panaudojamumą.

6 pav. Būsenos juosta

7 pav. Vandens ženklas

Egzistuoja įvairios kitos priemonės, išbandančios skirtingas metodikas. Vienos jų yra paprastesnės, kitos panaudoja sudėtingesnes atpažinimo taktikas:

1. Patikimų veiksmų grandinės (angl. *Trusted Activity Chains*) – programuotojas nurodo, kurie veiksmai yra leidžiami, ir kurių negalima nutraukti [WLD+15].
2. Hou ir Yang apsaugos schema – į „iOS“ užkraunama apsaugos priemonė, kuri įspėja vartotoją, kai jis bando įvesti duomenis į programą, esančią nepatikimųjų sąraše [WLD+15].
3. „PhishZoo“ – profiliuoja patikimų puslapių išvaizdą užkoduodama matomus turinio elementus, kurie vėliau yra lyginami su ekrane pateikiamu puslapiu [WLD+15].
4. „SpoofGuard“ – išsaugoja nuorodas, nuotraukas bei domeno pavadinimus, kuriuos vėliau tikrina su ekrane esančiu puslapiu [WLD+15].
5. „VeriUI“ – prie įvestų prisijungimo duomenų prikabina sertifikatą, kuriame pateikiama informacija apie įrenginį. Iškodavus šią informaciją tikrinama, ar telefonas yra patikimųjų sąraše [WLD+15] [GDJ18].
6. Prisijungimo duomenų saugojimas „SIM“ kortelėje, bet vartotojas turi prisiminti joje patalpintą kodą [GDJ18].
7. „QR“ kodo pagrindu veikiantys prisijungimo modeliai. Informacija atkoduojama ir pateikiama „QR“ kodo pavidalu siejant ją su įrenginyje esančiu kodu [SS+20] [CPS16].
8. „MPShield“ – tarpinis serveris, kuris tikrina paketus, analizuoja užklausas bei ištraukia nuorodas [CPS16].
9. „AntiPhish“ – išmeta apsaugos pranešimą kiekvieną kartą vartotojui vedant jautrią informaciją [WLD+15].

Apsaugos modeliai bei įrankiai sukuriami pirmiausia sugalvojus idėją. Teoriškai įvertinamas jos veiksmingumas, ar įmanoma ją įgyvendinti, ir ar tai verta daryti. Šios idėjos vėliau tampa patikimais ir efektyviais apsaugos modeliais:

1. Išsiunčiamų užklausų tikrinimas pirmiausia panaudojus netikrus duomenis. Tai nusakytų, ar naudojamas teisingas serveris [ND19] [CPS16] [WLD+15] [GDJ18].
2. Nuolatinis programų pavadinimų, piktogramų bei nuotraukų stebėjimas. Vienintelis trūkumas – bankai dažnai turi panašius pavadinimus bei nuotraukas, kas klaidintų atpažinimo priemonę [CPS16] [KS+19].
3. Periodiškas ekrano nuotraukų siuntimas ir neatitikimų ieškojimas. Reikėtų laikyti kelis programėlės vaizdo variantus, nes ne visi vartotojai ją atsinaujina. Programos versijai pasikeitus, dažnai pasikeičia ir vartotojo sąsajos elementai [KJ+19].
4. Draudžiami daugiafunkciniai veiksmai. Nebeliktų užslėpto programų veikimo, tačiau vartotojas nebegautų pranešimų iš, pavyzdžiui, socialinių tinklų, jeigu paleistų programą, kurioje šis veikimas yra uždraustas [KJ+19].

5. Valstybinių nuorodų pritaikymas. Adresai, kurie baigiasi valstybių kodais, žmonėms atrodo patikimesni [ND19].
6. Patikimesnis „QR“ kodų generavimas. Vienas iš pavyzdžių yra jų kūrimas su parašu, kad žmonės atpažintų jų autentiškumą [SS+20].
7. Kreipti dėmesį į socialinio pobūdžio puolimus projektuojant modelius bei programas [WPL20] [LPS21].
8. Emocionalesnių įspėjamųjų pranešimų naudojimas. Tokie pranešimai skatina žmonių pastabumą [SAP+21].
9. Daugelio apsaugos sluoksnių pridėjimas. Pavyzdžiui, pradžioje leisti paprastesnį prisijungimą, o vėliau prašyti tapatybės patvirtinimo [PGS+22].
10. Saugos kodų pasitelkimas. Tai modelis, leidžiantis atskirti kompiuterį nuo žmogaus. Duodama atlikti užduotis, kuri yra lengva žmonėms, bet sudėtinga mašinoms [PGS+22].
11. Vienkartinių slaptažodžių naudojimas. Žmonės dažnai susikuria labai paprastus, todėl šitas modelis, kai slaptažodis sukuriamas sistemos, sumažintų šį žmogiškąjį faktorių [PGS+22].
12. Veido ar piršto antspaudų atpažinimo dažnesnis naudojimas [PGS+22].
13. Didinti žmonių supratimą. Jų mokymas nekreipti dėmesio į keistas žinutes, dažnai atsinaujinti programinę įrangą, įsijungti antivirusinę, nepasitikėti viešaisiais interneto tinklais, naudoti daugiafunkcinį prisijungimą ir išlikti budriems.

Apibendrinant, apsisaugoti nuo duomenų vagysčių yra labai svarbu. Tam pasitelkiamos įvairios priemonės, tokios kaip:

- statiniai modeliai, kurie grupuoja puslapius ir programėlės pagal nustatytus kriterijus. Šie sąrašai turi būti nuolatos papildomi, bet yra dažnai naudojami žmonėms įspėti. Vienas iš pavyzdžių yra „PhishTank“ puslapis, kuriame talpinami netikrų svetainių adresai;
- euristiniai modeliai, kurie ieško puolimams būdingų bruožų vertindami elektroninių laiškų, programėlių bei puslapių turinį. Nors pažangūs sukčiai moka šias priemones apeiti, dažnai randamos pamirštos paslėpti vietos. Vienas iš pavyzdžių yra „MobiFish“ įrankis, kuris tikrina puslapių kodą, internetinį adresą bei matomą programėlių vaizdą;
- vartotojo sąsają keičiantys modeliai, kurie modifikuodami elementus skatina vartotojų budrumą bei atgraso sukčius nuo imitavimo. Šiai kategorijai priklauso suasmeninti apsaugos indikatoriai, pranešimai bei būsenos juosta;
- kiti modeliai, kurie panaudoja įvairesnes apsaugos taktikas. Jie analizuoja užklaustas, koduoja matomą vaizdą, kiekvieną kartą įspėją vartotoją ar nurodo leidžiamus veiksmus. Tarp tokių yra „SpoofGuard“, „VeriUI“ ar „MPShield“;

- potencialios idėjos, kurios pagerintų apsaugą. Jos apima nuolatinį programų stebėjimą, nuotraukų siuntimą, patikimesnį kodų generavimą, didesnį žmonių mokymą ar veikimo draudimą.

1.6. Mobiliųjų telefonų apžvalgos apibendrinimas

Mobiliųjų telefonų apsauga nuo duomenų vagysčių išlieka aktuali problema. Sukčiai ne tik siunčia elektroninius laiškus ir žinutes, bet ir panaudoja kenkėjiškas programas, virusus, plėtinius, vienodas raides nuorodose bei greito atsakymo kodus. Jie pasitelkia žinias apie vartotojo charakterį, įpročius, statusą, propaguojamą greitą gyvenimo būdą, pripratimą prie vartotojo sąsajų bei polinkį į įspėjamųjų pranešimų vengimą. Didėjantis mobiliųjų įrenginių populiarumas atkreipė sukčių dėmesį, bet lengvai atkartojama vartotojo sąsaja, mažiau funkcijų siekiant sutaupyti ekrano vietą bei ribotas resursų kiekis neleidžia iki šiol sukurtoms apsaugos priemonėms efektyviai veikti. Norėdami sustiprinti vartotojų privatumą, operacinių sistemų kūrėjai izoliavo programų katalogus bei įvedė leidimų suteikimo sistemą, tačiau tai apsunkino kenkėjiškų programų aptikimą, o vartotojai dažnai leidimus suteikia neapgalvoję. Kenkėjiška programinė įranga atidaro netikras programas, dialogus, puslapius bei siunčia duomenis į trečiųjų šalių serverius. Į vartotojo įrenginį ji patenka paspaudus ant neaiškios nuorodos, parsisiuntus iš neoficialių šaltinių, arba įrašius teisėta apsimetančią programą. Duomenų vagystėms aptikti pasitelkiami statiniai, euristiniai, vartotojo sąsają keičiantys bei įvairūs kitas technikas išbandantys modeliai.

2. Telefonų apsaugos modelių vertinimas ir sprendimo formavimas

Principinio sprendimo gavimas yra padalintas į keletą poskyrių. Pirmajame aptariamos apsaugos modelių vertinimo priežastys bei eiga, pristatomi nagrinėjami modeliai bei paaiškinama, kaip jų analizė padeda formuoti patobulintą sprendimą. Antrajame nagrinėjamas apsaugos modelių panaudojamumas, pateikiami šio rodiklio ir vertinamų savybių apibrėžimai bei kiekvienos jų vertinimo skalė. Taip pat aptariama panaudojamumo vertinimo reikšmė bei jo indėlis į tolesnio sprendimo gavimą. Trečiajame dėmesys sutelkiamas į modelių saugumą, aprašomi šio rodiklio savybių apibrėžimai, jų svarba bei aptariami duomenų saugumo modeliai. Galiausiai kitame poskyryje pateikiami modelių patobulinimo pasiūlymai, skirti rastų trūkumų šalinimui ir vertintų kriterijų gerinimui.

2.1. Mobiliųjų telefonų apsaugos sprendimo rengimo eiga

Apsaugos nuo duomenų vagysčių principinio sprendimo kūrimas prasideda nuo išsamaus esamų modelių vertinimo. Šie modeliai yra analizuojami remiantis panaudojamumo ir saugumo kriterijais, parinktais iš pripažintų standartų ir metodinių karkasų. Panaudojamumas vertinamas pagal tokius požymius kaip masteliavimas, prisimenamumas, atstatomumas, pabaigtumas, proceso laikas, matomų elementų ar reikalingų atlikti veiksmų kiekis, padaromų klaidų vidurkis bei papildomų įrenginių reikalingumas [BJ+12]. Saugumas – pagal atsparumą išoriniam stebėjimui, apsimetinėjimui, spėliojimui, vidiniam stebėjimui, trečiųjų šalių ir leidimų reikalingumą [BJ+12] bei „KVP trikampio“ informacijos saugumo reikalavimų užtikrinimą [CM+23].

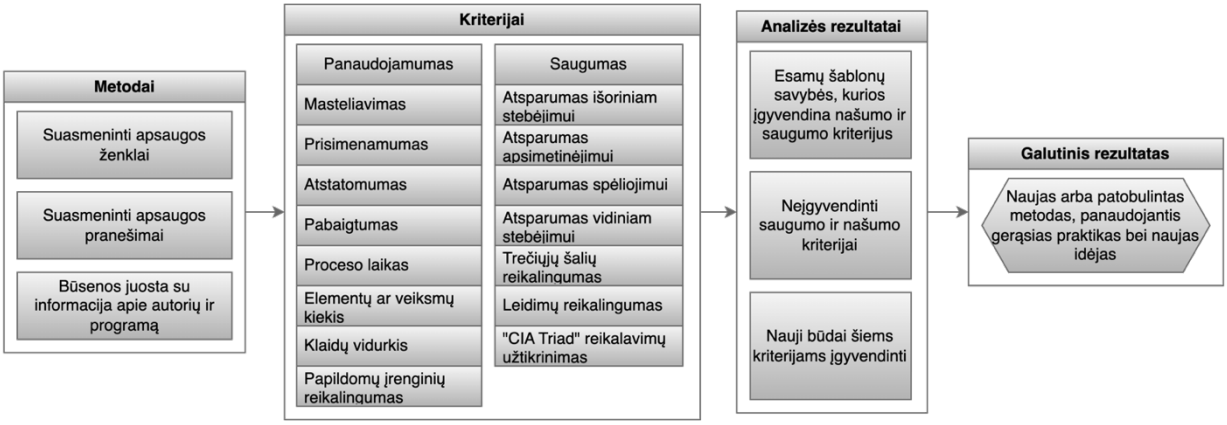
Požymio reikšmės išvedamos iš modelių testavimą aprašiusių straipsnių medžiagos. Dažniausiai paimami statistiniai duomenys, tokie kaip dalyvių skaičius ir užduoties laikas. Jeigu iš esamos informacijos savybės reikšmės nustatyti neįmanoma, ji gaunama pasitelkus įvairius skaičiavimus, modelius, ar atsižvelgiant į modelio veikimo principą. Klaidų vidurkis, pavyzdžiui, išskaičiuojamas iš reikalingų atlikti veiksmų kiekio bei puolimą nepastebėjusių žmonių procento.

Mobiliuosiuose telefonuose naudojami kelių tipų modeliai. Vieni yra automatiniai, kurie darbą atlieka fone ir nereikalauja vartotojo įsikišimo. Jų veikimas panašus į antivirusinės, kai potencialios grėsmės yra surandamos ir pašalinamos, arba ugniasienės, kai užkertamas kelias šių grėsmių kilimui. Tokiu būdu vartotojo veikla nėra petraukiama, o duomenų sauga – užtikrinama. Kiti modeliai – keičiantys vartotojo sąsają. Jie geriausiai veikia tais atvejais, kai automatinės priemonės negali teikti visapusiškos apsaugos dėl ribotų resursų, izoliuotų programų katalogų bei ribojamos veiklos siekiant sutaupyti baterijos energiją. Šie modeliai, tikslingai pateikdami ekrane informaciją, didina vartotojų kritinį mąstymą ir skatina duomenų vagysčių atpažinimą. Jų pasitelkiamos spalvingos žinutės ar garso signalai nereikalauja nei daug resursų, bei specifinės

prieigos prie duomenų. Pasirinktos vertinti būtent šio tipo priemonės, nes jos tiesiogiai daro įtaką žmogiškajam faktoriui:

- **suasmeninti apsaugos ženklai** – matydamas registracijos metu pasirinktą nuotrauką, vartotojas įvertina atidarytos programėlės autentiškumą;
- **suasmeninti apsaugos pranešimai** – matydamas ryškias ir aiškias žinutes, kurias pritaikė pagal savo norus, vartotojas supranta apie įrenginyje vykstančias duomenų pasisavinimo veikas;
- **būsenos juosta** – matydamas juostą ar vandens ženklą su programos pavadinimu ir autoriaus vardu, vartotojas supranta atidarytos programos tikrumą.

Apibendrinant, vertinimo metu nustatomi modelių privalumai ir trūkumai (8 pav.). Patobulintas sprendimas gaunamas apjungiant gerąsias praktikas ir užpildant surastas problemines vietas. Vėliau pateikti pasiūlymai yra įgyvendinami ir patvirtinami testavimo su realiais vartotojais metu.



8 pav. Principinio sprendimo gavimo planas

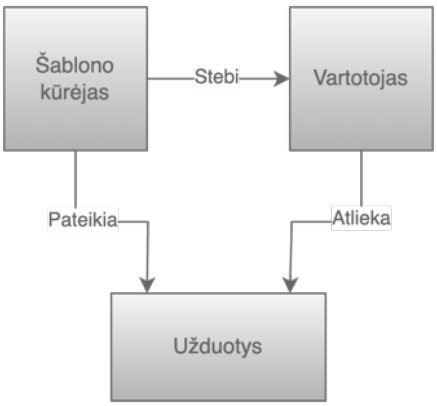
2.2. Mobiliųjų telefonų apsaugos modelių panaudojamumo vertinimas

Panaudojamumas yra savybė, nusakanti vartotojo gebėjimą veiksmingai, našiai ir su pasitenkinimu pasiekti užsibrėžtą tikslą naudojantis sistema [ISO-9241-11:2018]. Veiksmingumas apibrėžia užduoties įvykdymo užbaigtumą ir tikslumą, našumas – įdėtas pastangas, o pasitenkinimas – vartotojo patirtį, susijusią su naudojimosi malonumu, patogumu ir teigiamu požiūriu. Žmonės nelinkę rinktis alternatyvių, naudojimąsi apsunkinančių, neaiškių ir daug naujovių turinčių programų [LT+16]. Blogai suprojektuota, pakitusi, neintuityvi sistema vartotojui sukelia negatyvias emocijas. Panašiai kaip pasikeitęs maisto parduotuvės išplanavimas, kuris trikdo ir verčia daugiau laiko skirti norimos prekės paieškai. Tinkama sistema skatina saugią vartotojų elgseną, o netinkamas dizainas ir prasta vartotojo sąsajos struktūra lemia nesaugias

praktikas, atsirandančias dėl painiavos ar noro apeiti sudėtingus procesus. Vartotojas vengia įsijungti programą, kuri reikalauja daug specifinių veiksmų ir atidarinėja daugybę sunkiai uždaromų reklaminių langų. Panašiai vertinami ir apsaugos modeliai, kurių sėkmę lemia ne tik gynybinis jų efektyvumas, bet ir kokia patogi jų integracija į jau esamą sistemą, ar yra lengvai suprantami bei ar nekelia naudojimosi sunkumų. Nors paprasta vartotojo sąsaja yra svarbi projektavimo siekiamybė, programa pirmiausia turi atitikti vartotojo poreikius. Dėl to tam tikrais atvejais didesnis elementų kiekis ekrane bei sudėtingesnė sąveikos struktūra yra neišvengiami. Bet kuriuo atveju, kiekvienas mygtukas, žodis, iššokantis langas turi būti aiškūs bei dalis tvarkingai sudėliotų ir atliekamų veiksmų visumos.

Programuotojo ir vartotojo perspektyvos dažnai skiriasi. Pirmieji supranta programos veikimo principą, o pastarieji atlieka veiksmus remdamiesi asmenine patirtimi. Pasitaiko vartotojų, kurie rodomą klaidą įvertina kaip sistemos trikdį, o ne vykstančią duomenų vagystę. Siekiant nustatyti rizikingas situacijas, potencialius iššūkius bei mąstysenos subtilybes, modelis testuojamas su realiais vartotojais, kurie atlieka užduotis skirtingose situacijose (9 pav.). Suasmenintų apsaugos ženklų, pavyzdžiui, testavimo metu vieniems buvo pateikta teisinga nuotrauka, kitiems – neteisinga, o tretiems ji rodoma nebuvo. Surinkta informacija fiksuojant metrikas, tokias kaip paspaudimų skaičius ar atlikimo trukmė, bei renkant žmonių nuomonę, padeda atsakyti į įvairius tyrimo klausimus:

- Ar pasiekė galutinį tikslą?
- Kiek laiko užtruko jį pasiekti?
- Kur dažniausiai strigo?
- Ar buvo patenkinti programos veikimu?
- Ar betikslis spaudinėjimas nereiškė programos neveiksnumo?
- Ar užduoties atlikimo tvarka buvo aiški?
- Kada lengviausia pastebėti vykstantį puolimą?
- Ar atliko teisingus veiksmus?
- Ar vėliau pakartoję užduotis žinojo, ką daryti?



9 pav. Informacijos rinkimo eiga

Tinkamas panaudojamumo savybių įgyvendinimas pagerina žmogaus ir programos santykį. Patenkinti vartotojai yra labiau linkę toliau naudotis sistema. Jeigu veiksmingas apsaugos modelis yra nepatogus ir įkyrus, žmonės grįžta prie senų, nesaugių įpročių. Tačiau kokybiškai atliktas panaudojamumo sprendimas ne tik suteikia konkurencinį pranašumą, kai naudodamiesi kitomis programomis žmonės tikisi to paties patogumo ir lengvumo, bet ir skatina dažnesnį apsaugos modelių taikymą. Tai lemia tokios bendros panaudojamumo savybės:

- **našumas** *(angl. efficiency)* – vertinamas pagal užduoties atlikimo greitį. Vienas iš vertinimo modelių – lyginti su laiku, per kurį užduotį atlieka sistemą išmanantis žmogus. Tikslas – sumažinti atotrūkį tarp patyrusio ir paprasto vartotojo rezultatų;
- **veiksmingumas** (angl. *effectivness*) – vertinamas pagal vartotojo sugebėjimą savarankiškai atlikti užduotį. Tikslas – suprasti, ar vartotojo sąsaja yra pakankamai tiksli ir aiški;
- **malonumas naudotis** (angl. *satisfaction*) – vertinamas pagal vartotojų atsakymus į klausimus apie patirtį naudojantis sistema. Šį rodiklį sunku objektyviai įvertinti, nes kiekvienas žmogus turi savus lūkesčius. Tikslas – išsiaiškinti, ar programa yra lengvai suprantama ir patogi;
- **išmokstamumas** (angl. *learnability*) – vertinamas stebint, ar pakartotinai atlikus užduotį sumažėja atliktų klaidų kiekis ir strumpėja užduoties atlikimo laikas. Tikslas – suprasti, ar programa yra lengvai perprantama ir greitai įsisavinama;
- **prisimenamumas** (angl. *memorability*) – vertinamas stebint, kaip greitai po tam tikro laiko vartotojas grįžta prie anksčiau pasiekto sugebėjimo lygio. Tikslas – suprasti, ar vartotojo sąsaja yra intuityvi ir įsimenama.

Kadangi bendros panaudojamumo savybės yra sunkiai pamatuojamos ir įvertinamos, pasitelkiamos ir kitos, labiau analitinės savybės [BJ+12]:

- **papildomų įrenginių reikalingumas** (angl. *nothing-to-carry*) – nusako, ar modelio veikimui reikalingas kitas prietaisas ar programa. Turėtų pakakti vieno įrenginio ir jį naudojančio

vartotojo. Pavyzdžiui, sprendimo patogumą sumažintų reikalavimas vartotojui nešiotis kodų generatorių autentifikacijai atlikti;

- **padaromų klaidų vidurkis** (angl. *infrequent-errors*) – iš veiksmų kiekio ir puolimo nepastebėjusių žmonių procento išskaičiuojamas įvertis. Pagal jį daromos išvados apie apsaugos modelio bei rodomų ekrane elementų aiškumą. Daugybė pridaromų klaidų simbolizuoja apie prastą modelio dizainą, kuris kelia vartotojų nepasitenkinimą;
- **matomų elementų ar reikalingų atlikti veiksmų kiekis** (angl. *physically-efortless*) – nusako, kiek vartotojui reikia padaryti veiksmų, kad praeitų pro modelio apsaugą, arba kiek vaizdinių elementų jis turi peržiūrėti, kad suprastų vykstančius procesus. Mažai pastangų iš vartotojo reikalaujanti programa yra labiausiai priimtina. Ji neturėtų varginti dažnai iššokančiais langais, ar nenatūralia veiksmų virtine;
- **proceso laikas** (angl. *efficient-to-use*) – nusako, kiek laiko vartotojas truko atlikti modelio prašomus veiksmus. Turėtų būti sudarytos sąlygos vartotojui greitai priimti sprendimą po informacijos perskaitymo, kad integracija būtų natūrali ir organiška;
- **prisimenamumas** (angl. *memorywise-effortless*) – nusako, kiek procentų žmonių, po pertraukos pakartojusių veiksmus, išvengė ir pastebėjo vykstančią duomenų vagystę. Jeigu bendras skaičius yra 10 procentų didesnis, tai šio rodiklio reikšmė yra aukšta, jeigu 10 procentų mažesnis – žema, o kitu atveju – vidutinė, nes pokytis nėra didelis;
- **masteliavimas** (angl. *scalable-for-users*) – nusako, ar modelį įmanoma pritaikyti prie daugiau įrenginių ar paskyrų. Vartotojas jaučia didesnę kognityvinę naštą, jeigu turi atlikti tuos pačius veiksmus atskirai prisijungdamas. Rodiklio reikšmė yra aukšta, jeigu modelis persikelia į kitas paskyras ar įrenginius, o žema, kai to padaryti nėra įmanoma;
- **atstatomumas** (angl. *easy-recovery-from-loss*) – nusako, ar sistema greitai atsistato po įvykusios klaidos ar pamiršto prisijungimo, ir kaip modelis leidžia tai įgyvendinti. Rodiklio reikšmė yra aukšta, jeigu vartotojui įmanoma sekti atsistatymo instrukciją, o žema, kai jos nėra arba ji yra neaiški;
- **pabaigtumas** (angl. *successful-completion*) – nurodo, ar modelis yra intuityvus ir suprantamas, jeigu vartotojui pavyko užbaigti užduotį sėkmingai. Šis rodiklio reikšmė yra testavimo metu užduotį padariusių žmonių skaičius.

Panaudojamumo vertinimas sudaro vaizdą apie šiuo metu rinkoje esančią apsaugos modelių situaciją. Jis parodo, ar verta toliau gilintis į šią sritį, ar yra kur ją tobulinti, kurios vietos džiugino, o kurios kelia vartotojams daugiausiai sunkumų, yra neaiškios ir skatina atmetimo reakciją. Tai padeda rasti atsakymus į keletą klausimų:

- Kokios idėjos buvo išbandytos modeliuose?
- Kokias panaudojamumo savybes šie modeliai geriausiai įgyvendina?

- Kurios panaudojamumo savybės yra praleidžiamos?
- Kokios matomos vartotojų elgsenos tendencijos?
- Ar įmanoma pagerinti savybių reikšmes?
- Ar įmanoma įgyvendinti pamirštas savybes?

Kiekvienas vartotojo sąsają keičiantis modelis vertinamas pagal panaudojamumo metrikas. Pirmasis vertinamas modelis – suasmeninti apsaugos ženklai:

- **papildomų įrenginių reikalingumas** – modelyje naudojamą nuotrauką vartotojas pasirenka iš mobiliajame telefone esančios galerijos [MC+16]. Dėl šios priežasties joks kitas įrenginys nėra reikalingas;
- **matomų elementų ar reikalingų atlikti veiksmų kiekis** – registracijos metu vartotojas atlieka penkis veiksmus: suveda prisijungimo vardą ir slaptažodį, paspaudžia nuotraukos pasirinkimo mygtuką, išsirenka paveikslėlį ir galiausia užbaigia procesą. Prisijungimo metu – tris: patikrina rodomą nuotrauką, suveda duomenis ir prisijungia. Laikant, kad nebuvo atlikta jokių nuotraukos keitimų ar blogai suvestų prisijungimo duomenų, gaunamas atliekamų veiksmų vidurkis yra (3 + 5) / 2 = 4;
- **padaromų klaidų vidurkis** – šio rodiklio reikšmė išskaičiuojama iš atliekamų veiksmų kiekio, kas šiuo atveju yra 4, ir duomenų vagystės nepastebėjusių žmonių kiekio vidurkio. Tikimybė padaryti klaidą kiekviename žingsnyje yra vienoda, todėl klaidų vidurkis yra (1 + 2 + 3 + 4) / 4 = 2,5 klaidos. Kadangi pusė dalyvių neatpažino vykstančio puolimo, šis rodiklis krenta iki 2,5 * 0,5 = 1,75 klaidų;
- **proceso laikas** – prisijungimo lange vartotojai truko apie 14 sekundžių o registracijos – 46 [MC+16]. Paskaičiuotas proceso laiko vidurkis yra (46 + 14) / 2 = 30 sekundžių;
- **masteliavimas** – pasirinkta nuotrauka sisteminiu lygiu nėra susiejama su konkrečiu vartotoju. Pasirinkimas yra išsaugomas vartotojo įrenginyje, gyvuoja atmintyje ir yra rodomas prisijungimo metu. Ne savo įrenginyje prie programos bandantis prisijungti žmogus matytų kitą nuotrauką. Dėl šios priežasties masteliavimas yra vidutinis;
- **prisimenamumas** – po keturių dienų kartodami užduotį 54 procentai dalyvių nepastebėjo vykstančio puolimo [MC+16]. Įvertis sumažėjo 4 procentais, todėl prisimenamumo reikšmė yra vidutinė;
- **atstatomumas** – pasirinkta nuotrauka yra išsaugoma programos dokumentų kataloge. Nėra būdo prie jos prieiti ar pakeisti iš išorės, todėl po kurio laiko programą įsijungęs ir pasirinkimą pamiršęs vartotojas negalėtų būti užtikrintas dėl programos saugumo. Dėl šios priežasties atstatomumas yra žemas;
- **pabaigtumas** – iš 276 užduotį atlikusių žmonių 221, apie 80 procentų, ją sėkmingai užbaigė [MC+16].

Kitas modelis – suasmentinti apsaugos pranešimai:

- **papildomų įrenginių reikalingumas** – nors kitas prietaisas šiam modeliui nėra reikalingas, norint visapusiškai išnaudoti modelio galimybes turėtų būti įdiegta kita programa arba atlikti operacinės sistemos pakeitimai;
- **matomų elementų ar reikalingų atlikti veiksmų kiekis –** vienas nuspalvintas sakinys yra labiausiai priimtinas, nes žmonėms patraukliausios trumpos, specifiškai nuspalvintos ir instruktuojančios žinutės [ND19];
- **padaromų klaidų vidurkis** – iš dviejų testavime dalyvavusių grupių vidutiniškai (16 + 11) / 2 = 13,5 procentai žmonių praignoravo pranešimus [ND19]. Jeigu jų kokybė būtų pagerinta, pastabumo rodikliai išaugtų 13,4 procentais, nes primenantys pranešimai paskatina įsitraukimą 17,1 procentais, o prašantys atnaujinti programinę įrangą – 9,7 procentais [PX+16]. Iš 206 dalyvių suklydo 13,6% * 206 = 27,81 ≈ 28 žmonės [ND19]. Pagerinus situaciją 13,4 procentais, klaidų vidurkis sumažėtų iki 24. Tokiu atveju pranešimus perskaitytų 206 – 24 = 182 žmonės, kas sudaro apie 88,35 procentus;
- **proceso laikas** – pranešimo parodymas ir jo perskaitymas tetrunka keletą sekundžių. Į šį vertinimą neįskaičiuota informacijos rinkimo trukmė;
- **masteliavimas** – šio rodiklio reikšmė yra aukšta, kadangi pranešimai rodomi nepaisant paskyros ar naudojamos programos. Jeigu vartotojas panaudotų kitą įrenginį, reikėtų įsikelti pasirinkimus į už pranešimų rodymą atsakingą programą;
- **prisimenamumas** – modelis nereikalauja iš vartotojo nieko prisiminti, kadangi yra informacinio pobūdžio.
- **atstatomumas** – vartotojui reikėtų atstatyti nebent tik pasirinktus pranešimų rodymo nustatymus, kurie niekur nesaugomi, dėl to atstatomumas vidutinis.

Trečias modelis – būsenos juosta:

- **papildomų įrenginių reikalingumas** – vartotojas turėtų įsidiegti už būsenos juostos rodymą atsakingą programą, o kiti prietaisai nėra reikalingi;
- **matomų elementų ar reikalingų atlikti veiksmų kiekis** – taupant ekrano vietą rodomas trumpas sakinys su programos pavadinimu ir kūrėju, arba programos statusą simbolizuojanti spalva [FE-17] [WLD+15];
- **padaromų klaidų vidurkis** – 76 procentai dalyvių pastebėjo kenkėjišką programą [FE-17] [WLD+15]. Imant logišką 100 žmonių imtį, gaunamas 24 klaidų vidurkis;
- **proceso laikas** – nekreipiant dėmesio į rodomos informacijos surinkimo trukmę, būsenos juostą parodyti ir pamatyti tetrunka keletą sekundžių;

- **masteliavimas** – būsenos juosta matoma visose programose, nes už jos parodymą atsakinga kita programa arba operacinė sistema. Šio rodiklio reikšmė yra vidutinė, nes vartotojas turi sutikti su šios informacijos rinkimu ir rodymu;
- **prisimenamumas** – informacinio pobūdžio modelis nereikalauja nieko prisiminti;
- **atstatomumas** – informacinio pobūdžio modelis nereikalauja nieko atstatyti.

Apibendrinant, apsaugos modelis turi užtikrinti tinkamą programos panaudojamumą. Blogai suprojektuotas įrankis skatina atmetimo reakciją ir priveda vartotoją prie nesaugių įrenginio naudojimo praktikų. Nepasitenkinimas kyla dėl per didelių reikalavimų ir įkyriai mėtomų pranešimų. Norėdami suprasti vartotojų mąstyseną, programuotojai atlieka modelių testavimą su realiais asmenimis. Tokiu būdu surandamos neaiškios bei optimizacijos reikalaujančios programos vietos. Vartotojo sąsają keičiantys modeliai buvo vertinami pagal nustatytas panaudojamumo savybes. Ši analizė parodė modelių trūkumus ir privalumus. Kiekvienas analizuotas modelis yra pakankamai patogus vartotojui (1 lentelė). Bent pusė dalyvių sugebėjo pastebėti vykstantį puolimą, nei vienam nereikėjo papildomo prietaiso, o ir procesas truko neilgai. Dėl savo informacinio pobūdžio suasmeninti apsaugos pranešimai bei būsenos juosta priklauso nuo kitos programos ar operacinės sistemos pakeitimų, bet tai padaro šiuos modelius veiksnius daugybėje programų. Suasmeninti apsaugos ženklai reikalauja daugiau vartotojo veiksmų, vyksta prisijungimo metu, dėl to turi mažesnius rodiklius, kurie galėtų būti patobulinti.

1 lentelė Modelių panaudojamumo vertinimas

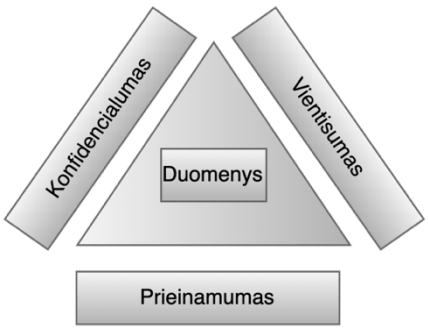
Modeliai / Savybės	Reikalingi papildomi įrenginiai?	Matomų elementų ar veiksmų kiekis?	Padaromų klaidų vidurkis	Proceso laikas	Masteliavimas	Prisime-namumas	Atstatomumas
Suasmeninti apsaugos ženklai	Ne	4 veiksmai	1,75 klaidos. ≈ 80% pastebėjo problemą.	≈ 30 sekundžių	**Vidutinis**	**Vidutinis**	**Žemas**
Suasmeninti apsaugos pranešimai	**Reikalinga kita programa**	1 nuspalvintas sakinys	24 klaidos. ≈ 88,35% pastebėjo puolimą.	Keletas sekundžių	Aukštas	Nereika-lauja	Nereikalauja
Būsenos juosta	**Reikalinga kita programa**	1 sakinys, 1 spalva	24 klaidos. 76% pastebėjo puolimą.	Keletas sekundžių	Vidutinis	Nereika-lauja	Vidutinis

2.3. Mobiliųjų telefonų apsaugos modelių saugumo vertinimas

Informacinių technologijų srityje duomenų apsauga yra kritiškai svarbi. Sukčiai kėsinasi į įmonių komercines paslaptis, klientų duomenis ir žmonių asmeninę informaciją siekdami finansinės naudos ar pridaryti žalos. Saugumo sistemos turi užtikrinti informacijos integralumą, užfiksuoti pakeitimo legalumą, neleisti neteisėtos prieigos, atlaikyti bandymą programas sutrikdyti ar sunaikinti, o kiekvienas apsisaugojimo modelis turi būti pakankamai veiksmingas, kad vartotojo duomenys išliktų saugūs. Žmonės dalinasi informacija ir internete atlieka atsiskaitymus, todėl jų prisijungimo duomenys yra pažeidžiami. Vis dėlto, efektyvumo stiprinimas dažnai turi neigiamos įtakos panaudojamumui: programa tampa nepatogi, įkyri ir vartotojui nemaloni. Iš kitos pusės, naudotojui patrauklus, bet apsaugos neužtikrinantis modelis praranda praktinę vertę. Dėl šios priežasties modelių saugumo analizė yra būtina siekiant surasti tobulinamas sritis bei jas suderinti su panaudojamumu.

Informacijos saugumo principus aprašo įvairūs aukšto lygio modeliai. Jais remiantis sprendžiama, ar sistema yra atspari įvairiems pavojams. Bent vieno modelio savybes išlaikantis apsaugos modelis didina savo pagrįstumą. Vienas iš tokių modelių – KVP trikampis (angl. *CIA Triad*) [CM+23] (10 pav.). Šis modelis pasirinktas kaip viena modelio vertinimo savybė, nes jis labiau orientuotas į duomenų apsaugą, o ne procesą, kurį labiau pabrėžia kiti modeliai. Jis atskiria tris idėjas, apibūdinančias sistemos atsparumą iškilusioms grėsmėms:

- **konfidencialumas** (angl. *confidentiality*) – duomenų slaptumo ir privatumo užtikrinimas, kad jais dalintųsi tik įgalioti asmenys;
- **vientisumas** (angl. *integrity*) – duomenų patikimumo ir nepakeičiamumo užtikrinimas, kad jie išliktų tikslūs ir teisingi;
- **prieinamumas** (angl. *availability*) – duomenų pasiekiamumo užtikrinimas, kad prie jų bet kuriuo metu prieitų tik suinteresuoti asmenys.



10 pav. KVP trikampis

Kitas modelis – AKAIAP (angl. *STRIDE*) [LC+20] (11 pav.). Jis įvertina tikėtinas grėsmes, kurios neužtikrina norimos saugumo savybės:

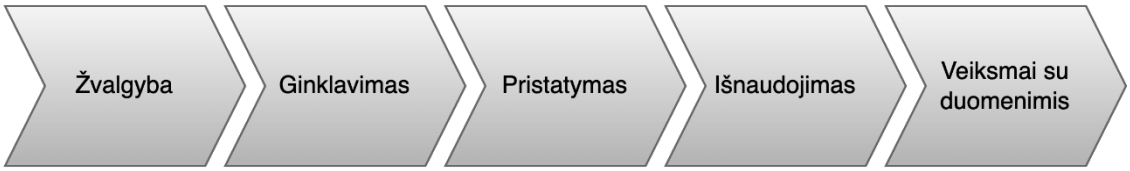
- **apsimetimas** (angl. *spoofing*) – apsimetimas kitu asmeniu ar patikima sistema, kuris pažeidžia autentiškumo užtikrinimo principą;
- **klastojimas** (angl. *tampering*) – neįgaliotas duomenų pakeitimas, kuris pažeidžia integralumo principą;
- **atsisakymas** (angl. *repudiation*) – neleistinų veiksmų atlikimo neigimas arba atsakomybės perkėlimas kitam asmeniui;
- **informacijos atskleidimas** (angl. *information disclosure*) – neleistinas priėjimas prie duomenų, kuris pažeidžia konfidencialumą;
- aptarnavimo perkrova (angl. *denial of service*) – resursų išnaudojimas, sutrikdantis programos veikimą bei uždarantis prieigą prie duomenų;
- **privilegijų pakeitimas** (angl. *elevation of privilege*) – neteisėtas leidimų suteikimas, kuris sugadina autorizacijos principą.

11 pav. AKAIAP modelis

Dar vienas informacijos saugumo modelis – grandinės nutraukimo (angl. *Kill Chain*) [KSS+18] (12 pav.). Jis nusako, kokių žingsnių sutrikdymas lemtų duomenų vagystės nesėkmę:

- **žvalgyba** (angl. *reconnaissance*) – renkama informacija apie potencialią auką: elektroninis paštas, pageidavimai, įpročiai bei naudojamos programos;
- **ginklavimas** (angl. *weaponization*) – sukuriama duomenų viliojimo priemonė: netikra programa, įtikinamas elektroninis laiškas, žinutė;
- **pristatymas** (angl. *delivery*) – pateikiama sukurta duomenų viliojimo priemonė: išsiunčiamas elektroninis laiškas, įdiegiama kenkėjiška programa;
- **išnaudojimas** (angl. *exploitation*) – laukiama vartotojo veiksmų: paspaudimo ant pateiktos nuorodos, prisijungimo duomenų įvedimo;

- **veiksmai su duomenimis** (angl. *actions on objectives*) – atliekama duomenų vagystė, paskyros sukompromitavimas.



12 pav. Grandinės nutraukimo modelis

Apsaugos modelių saugumas vertinamas pagal stiprumo ir veiksnumo savybes [BJ+12]:

- **atsparumas išoriniam stebėjimui** (angl. *resilient-to-physical-observation*) – atsparumas nuo sukčiaus, pažiūrėjusio kelis kartus, gebėjimo atkartoti vartotojo veiksmus. Rodiklio reikšmė yra laikoma aukšta, kai vaizdo pamatymas neleidžia sukčiui jokiomis priemonės įveikti apsaugos modelio, vidutinė, kai tam tikrais atvejais tai palengvintų modelio apėjimą, o žema, kai tai neišvengiamai lemtų modelio nesėkmę;
- **atsparumas apsimetinėjimui** (angl. *resilient-to-targeted-observation*) – atsparumas nuo sukčiaus, gerai pažįstančio auką, gebėjimo su žinoma informacija apeiti sistemą. Rodiklio reikšmė yra aukšta, kai aukos pažinojimas leidžia prieit prie duomenų, o žema – kai žinios neturėtų jokios įtakos;
- **atsparumas spėliojimui** (angl. *resilient-to-guessing*) **–** atsparumas nuo sukčiaus gebėjimo spėliojimu apeiti modelio apsaugas. Rodiklio reikšmė yra aukšta, kai spėliojimas nėra įmanomas, vidutinė, kai prie tam tikrų sąlygų spėliojimas padėtų, o žema, kai spėliojimas ilgainiui privestų prie modelio nulaužimo;
- **atsparumas vidiniam stebėjimui** (angl. *resilient-to-internal-observation*) – atsparumas nuo įdiegto viruso, tikrinančio vartotojo veiksmus. Rodiklio reikšmė yra aukšta, kai virusas pridarytų žalos, o žema, kai modelio saugumui jis įtakos neturėtų.
- **trečiųjų šalių reikalingumas** (angl. *no-trusted-third-party*) – nusako, ar modelio efektyvumui užtikrinti reikalingas informacijos siuntimas interneto ryšiu į atskirą serverį, kurį sukčiai galėtų sukompromituoti;
- **leidimų suteikimo reikalingumas** (angl. *requiring-explicit-consent*) **–** nusako, ar vartotojas turi lesti apsaugos modeliui atlikti darbą;

Kiekvienas vartotojo sąsają keičiantis modelis vertinamas pagal šias savybes. Pirmasis modelis – suasmeninti apsaugos ženklai:

- **atsparumas išoriniam stebėjimui** – sukčius galėtų pamatyti vartotojo pasirinktą nuotrauką ir ją panaudoti kenkėjiškoje programoje, tačiau tam reikalinga prieiga prie nuotraukų galerijos

arba gebėjimas matytą vaizdą atkurti. Šio modelio atsparumas išoriniam stebėjimui yra vidutinis, nes reikalingos specifinės sąlygos apeiti modelį;

- **atsparumas apsimetinėjimui** – žinodamas vartotojo technologinį išsilavinimą sukčius turėtų suvokimą apie tikėtiną reakciją į nuotraukos nebuvimą: ar toks atvejis būtų palaikytas kaip programos klaida ar bandymas pavogti duomenis. Taip pat sukčius galėtų nuspėti, kokią nuotrauką vartotojas rinksis. Šio modelio atsparumas apsimetinėjimui yra aukštas, kadangi modelis prisijungimo neapsaugo, o tik parodo, ar programa yra kenkėjiška;
- **atsparumas spėliojimui** – išlieka tikimybė, kad taupydamas laiką vartotojas pasirinks pirmą pasitaikiusią nuotrauką galerijoje. Panašiai kaip su paprastesnių slaptažodžių kūrimu. Šio modelio atsparumas yra aukštas, nes bet kokiu atveju nuotrauką reikia išgauti;
- **atsparumas vidiniam stebėjimui** – šio modelio tikslas yra įrodyti programos teisėtumą, todėl vartotojas įvertina rodomą ar nerodomą nuotrauką net tokiu atveju, kai virusas paleidžia kenkėjišką programą. Dėl šios priežasties atsparumas vidiniam stebėjimui yra aukštas;
- **trečiųjų šalių reikalingumas** – vartotojo pasirinkta nuotrauka yra išsaugoma programėlės kataloge, kadangi dėl prisijungimo saugojimo nėra galimybės ją susieti su konkrečiu vartotoju. Dėl šios priežasties trečiųjų šalių modeliui nereikia;
- **leidimų suteikimo reikalingumas** – norėdamas pasirinkti nuotrauką, vartotojas turi suteikti programai leidimą prieiti prie nuotraukų galerijos. Šis faktas stipriai pagerina programos saugumą, nes kitos programos to padaryti negali, nebent vartotojas leidimą suteikė ir joms;
- **KVP trikampis** – pasirinkta nuotrauka saugiais perdavimo kanalais turi būti patalpinta apsaugotoje saugykloje, kad būtų išsaugotas konfidencialumas. Ji turi būti užkoduotas kriptografinėmis priemonėmis, kad būtų užtikrintas integralumas. Nuotrauka turi būti lengvai pasiekiama ir greitai užkraunama, kad nebūtų pažeistas prieinamumas.

Kitas modelis – suasmeninti apsaugos pranešimai:

- **atsparumas išoriniam stebėjimui** – pritaikyti pranešimai vartotojui parodomi, kad įspėtų apie tikėtiną kenkėjišką programą arba reikalingus atlikti veiksmus, apsaugojančius nuo potencialios duomenų vagystės. Už jų rodymą atsakinga kita programa arba operacinė sistema, dėl to gavęs prieigą prie įrenginio sukčius pakeistų nebent tik pranešimų rodymo dažnumą. Toks scenarijus paliktų duomenis nepakitusius, bet padidėja šansai, jog vartotojas kitą kartą neatliks prašomų apsaugos veiksmų. Kadangi tai įspėjamojo pobūdžio modelis, o ne papildomas apsaugos sluoksnis, atsparumas išoriniam stebėjimui yra aukštas;
- **atsparumas apsimetinėjimui** – aukos pažinojimas suteiktų žinių apie vartotojui svarbius pranešimus ir kokios žinutes atkreipia jo dėmesį. Kadangi modelis yra įspėjamojo pobūdžio, atsparumas apsimetinėjimui yra aukštas;

- **atsparumas spėliojimui** – rodomi pranešimai nesuteikia prieigos prie duomenų, o tik įspėja vartotoją. Jeigu nebus vertinama tai, kad šis modelis netrukdo vartotojui prisijungti, tai atsparumas spėliojimui yra aukštas;
- **atsparumas vidiniam stebėjimui** – įrenginyje įdiegtas virusas, išsiaiškinęs kokia programa naudojama pranešimams gauti, galėtų ją apeiti ir pakeitęs pranešimų sudėtį, išjungęs apsimetinėjimo atvejus fiksuojančias priemones suklaidintų vartotoją. Prisijungdamas prie kenkėjiškos programos vartotojas negautų pranešimo, todėl apsauga vidiniam stebėjimui yra vidutinė;
- **trečiųjų šalių reikalingumas** – už pranešimų rodymą atsakinga operacinė sistema arba programa. Pastaroji veiktų su priemonėmis, kurios ieško virusų bei ar nepasitaikė neleistinų programos pakeitimų. Ši programinė įranga įdiegiama atskirai;
- **leidimų suteikimo reikalingumas** – kad būtų užtikrinta teisinga informacija apie įvykius sistemoje, vartotojas turi suteikti leidimą rodyti pranešimus, tikrinti programas bei programai sklandžiai veikti įrenginio fone;
- **KVP trikampis** – vartotojo pasirinkimai turi būti saugomi privačiame įrenginio kataloge, kad būtų užtikrintas konfidencialumas. Tokiu būdu išsaugomas ir šios informacijos integralumas, nes sukčiai negalėtų pakeisti nei norimos gauti informacijos, nei rodymo dažnumo. Prieinamumui užtikrinti reikėtų turėti pirminius nustatymus pasirinkimų neužkrovimo atvejui bei uždėti limitus, kad informacija nebūtų rodoma per dažnai.

Galiausiai – būsenos juosta:

- **atsparumas išoriniam stebėjimui** – vartotojui rodoma informacija apie naudojamą programą. Tai pamatęs sukčius neturėtų būdo šias žinias pritaikyti priėjimui prie duomenų. Kadangi tai yra informacinio pobūdžio modelis, atsparumas išoriniam stebėjimui yra aukštas;
- **atsparumas apsimetinėjimui** – pažinodamas auką ar bandydamas ja apsimesti sukčius neprieitų prie jokių duomenų, nes tai yra informacinio pobūdžio modelis. Dėl šios priežasties atsparumas apsimetinėjimui yra aukštas;
- **atsparumas spėliojimui** – sukčiui nėra ko spėlioti, kad prieitų prie duomenų, nes tai informacinio pobūdžio modelis. Dėl to atsparumas spėliojimui yra aukštas;
- **atsparumas vidiniam stebėjimui** – jeigu įdiegtas virusas sukompromituotų arba išjungtų programą, kuri teikia informaciją būsenos juostai, tada vartotojas būtų suklaidintas. Nors modelis yra informacinio pobūdžio, pakeista rodoma informacija pridarytų žalos. Dėl šios priežasties atsparumas vidiniam stebėjimui yra vidutinis;
- **trečiųjų šalių reikalingumas** – būsenos juostoje turėtų būti atvaizduota teisinga informacija, kurią tiektų operacinė sistema arba kita programa;

- **leidimų suteikimo reikalingumas** – būsenos juostai informaciją teikiančiai programai vartotojas turėtų suteikti leidimą tikrinti programas, pasiekti jų pavadinimą bei savininko vardą.
- **KVP trikampis** – būsenos juostoje turėtų būti rodoma mažiau jautri informacija, kad būtų užtikrintas konfidencialumas. Pavyzdžiui, neturėtų būti rodoma programos savininko elektroninis paštas. Siekiant užtikrinti integralumą, reikėtų apsaugoti programą nuo tikėtino rodomos informacijos pakeitimo. Prieinamumui užtikrinti padėtų parodomas rodiklis, jeigu informacija vis dar kraunama dėl trikdžių.

Apibendrinant, svarbu užtikrinti duomenų saugumą mobiliuosiuose telefonuose. Vis daugiau žmonių duomenimis dalinasi internetinėje erdvėje. Apsaugos modeliai neturi trikdyti panaudojamumo įkyriais pranešimais bei prašymais, tačiau jų gynybinis efektyvumas dėl to negali nukentėti. KVP trikampis, AKAIAP bei grandinės nutraukimas yra aukšto lygio informacijos saugumo modeliai. Pirmasis nusako, kas turi būti užtikrinta, kad duomenis būtų galima laikyti saugiais, antrasis įvertina grėsmes, o trečiasis – duomenų vagysčių žingsnius. Prie saugumo užtikrinimo prisideda ir vartotojo sąsają keičiantys modeliai. Jie buvo vertinami pagal nustatytas saugumo savybes. Kiekvienas analizuotas modelis yra saugus savame kontekste (2 lentelė). Suasmeninti pranešimai bei būsenos juosta yra informacinio pobūdžio modeliai, kurių nulaužimas neduotų tiesioginės prieigos prie duomenų, tačiau pakeista žinutė suklaidintų vartotoją ir privestų prie neteisingo matomo vaizdo interpretavimo. Nepaisant to, atsparumas stebėjimams ir klastojimams yra aukštas. Suasmeninti apsaugos pranešimai turi daugiau sluoksnių ir prašo iš vartotojo atlikti daugiau veiksmų bei stabdo programos veikimą iki kol jie bus įgyvendinti. Skirtingai nei kiti, šiam modeliui nereikia atskirų programų, kurios irgi savo ruožtu yra pažeidžiamos. Jo atsparumas daugumai grėsmių yra aukštas, nebent sukčius gauna prieigą prie pasirinktos nuotraukas. Taip vartotojas būtų apgautas šią nuotrauką panaudojus kenkėjiškoje programoje.

2 lentelė Modelių saugumo vertinimas

Modelis/ Savybės	Atsparumas išoriniam stebėjimui	Atsparumas apsimetinė-jimui	Atsparumas spelioji-mui	Atsparumas vidiniam stebėji-mui	Trečiųjų šalių reikalingumas	Leidimų suteikimo reikalingumas	Ar atspari pagal KVP trikampį?
Suasmeninti apsaugos ženklai	**Vidutinis**	**Aukštas**	**Vidutinis**	**Aukštas**	Nereikia	Leidimo prieiti prie nuotraukų galerijos	Saugyklos, kriptografijos, atsarginės priemonės, jeigu neužkrauna nuotraukos
Suasmeninti apsaugos pranešimai	Aukštas	Aukštas	Aukštas	Vidutinis	**Reikia operacinės sistemos pakeitimų arba programos**	Reikia leidimo rodyti pranešimus, tikrinti programas	Saugyklos, pirminių nustatymų, limitų
Būsenos juosta	Aukštas	Aukštas	Aukštas	Vidutinis	**Reikia operacinės sistemos pakeitimų arba programos**	Leidimų rodyti juostą, tikrinti programas, paimti programos pavadinimą bei savininką	Nerodyti jautrios informacijos, neleisti pakeisti informacijos, užtikrinti, kad krovimo metu, tai indikuotų

2.4. Mobiliųjų telefonų apsaugos modelių patobulinimų pasiūlymai

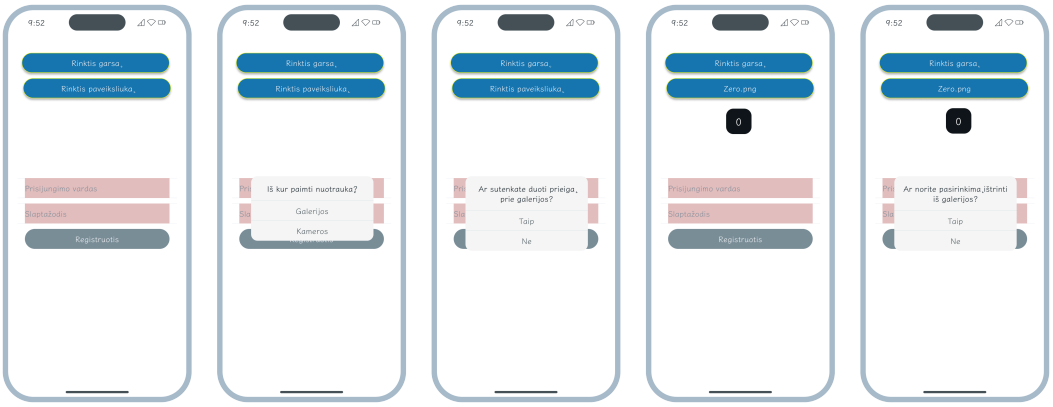
Po atliktos analizės pateikiamos modelių pagerinimo rekomendacijos. Suasmeninti apsaugos pranešimai ir būsenos juosta priklauso nuo kitos programos, nereikalauja daug veiksmų iš vartotojo ir yra informacinio pobūdžio. Jie neįgyvendina dalies panaudojamumo kriterijų, tokių kaip prisimenamumas, o saugumo rodikliai daugiausiai priklauso nuo nesukompromituotų informaciją teikiančių programų. Asmeniniai apsaugos ženklai, tuo tarpu, veikia savarankiškai, yra pritaikomi prie esamų sistemų, nerenka informacijos iš išorinių šaltinių, ir dėl to yra lengvai išplečiamas. Nors 80 procentų dalyvių pastebėjo vykstančią duomenų vagystę, modelio prisimenamumo ir atstatomumo rodikliai nėra idealūs, o atsparumas išoriniam stebėjimui bei spėliojimui turėtų būti padidintas. Pateikiami suasmenintų apsaugos ženklų patobulinimai, kurie pagerintų panaudojamumo ir saugumo savybių įverčius:

- **kartu su nuotrauka leidžiama pasirinkti garsinio formato rinkmeną** - papildomų jutiklių pajungimas skatina vartotojus labiau įsitraukti ir atkreipti dėmesį. Išgirstas garsas reikalauja mažiau kognityvinių sugebėjimų ir dėl keliamos asociacijos priverčia greičiau priimti sprendimą [RZG24]. Tokia taktika naudojama pagerinti pardavimus internetinėse parduotuvėse bei paskatinti emocinį prieraišumą žaidimuose. Šis pakeitimas sumažintų padaromų klaidų vidurkį, nes vartotojas lengviau suprastų įsijungtos programos tinkamumą. Taip pat maždaug penktadalis gyventojų turi garsinę atmintį. 22,4 procentai viename tyrime dalyvavusių studentų pasisakė geriau prisimenantys garsu pateikiamą informaciją [MMS+21], o kitas tyrimas atskleidė, kad taip yra 24 procentams žmonių [IS+21]. Be to, apie 285 milijonai visuomenės narių turi su matymu susijusių problemų [JS+21]. Daroma prielaida, kad garsinės rinkmenos pasirinkimas pagerintų padaromų klaidų vidurkį bei prisimenamumą;
- **vartotojo informavimas trumpomis, spalvotomis žinutėmis** – iš suasmenintų pranešimų ir būsenos juostos analizės žinoma, kad vartotojams labai padeda trumpi informaciniai pranešimai [ND19], o iš suasmenintų apsaugos ženklų – kad dalis asmenų neužkrautą nuotrauką palaikė serverio klaida [MC+16]. Vartotojų informavimas apie jų veiksmų sėkmę arba serverio klaidas užtikrintų KVP trikampio prieinamumo reikalavimus, kai nepasiekiamumo atveju rodoma numatyta reikšmė, o žmogus supranta, kas su sistema vyksta [CM+23];
- **suteikiama galimybė padarytos nuotraukos nesaugoti galerijoje** – suasmenintų apsaugos ženklų analizė atskleidė, kad sukčiams gavus prieigą prie nuotraukų galerijos, sumažėja šio modelio suteikiamas saugumas. Tiesioginis multimedijos elementų talpinimas dokumentų kataloge šią problemą panaikintų. Tai pasiekiama leidus nuotrauką iškart padaryti su kamera, o garsinį failą – mikrofonu. Be to, vartotojo informavimas apie vienkartinę prieigą prie nuotraukų galerijos sustiprintų pasitikėjimą;

- **pasirinktos rinkmenos saugojimas duomenų bazėje** – suasmenintų apsaugos ženklų modelio atveju išsirinkta nuotrauka yra talpinama vartotojo įrenginyje. Kiekvienai naudojamai paskyrai rodomas tas pats paveikslėlis, nes procesas vykdomas prisijungimo metu, kas neleidžia jo susieti su konkrečiu vartotoju. Taip pat paėmus kitą įrenginį reikia pasirinkti kitą nuotrauką, nes praeitas pasirinkimas yra nepasiekiamas. Suteikus galimybę multimedijos elementus išsaugoti duomenų bazėje po sėkmingo prisijungimo, kitame įrenginyje vartotojas galėtų šias rinkmenas parsisiųsti ir pernaudoti. Nors tam įgyvendinti reikėtų saugaus komunikacijos protokolo, duomenų bazės bei kartais kito įrenginio, būtų pagerintas prisimenamumas, nes vartotojas prisimintų rodomo paveikslėlio tinkamumą pasižiūrėjęs į jį kitame įrenginyje. Be to, dalį atsakomybės prisiima paslaugos tiekėjas, kuris saugumo naštą nuima nuo vartotojo. Tokiu būdu saugumas nenukentės, o konfidencialumas ir integralumas bus užtikrintas;
- **vartotojo įtraukimas su patvirtinimo mygtuku ir didesniu nuotraukų rodymu** – didelė dalis žmonių telefonu naudojasi išjungę garsą [CJT15]. Kol vartotojas neišklausė pasirinkto garsinio failo, tol būtų neleidžiama jam prisijungti. Taip pat leidimas pasirinkti keletą nuotraukų padidintų saugumą. Tokiu atveju sukčiams reikėtų žinoti keletą nuotraukų, o matydamas bent vieną teisingą vartotojas suprastų paleistos programos kilmę. Siekiama išsiaiškinti, ar tokie prašymai nekeltų nepasitenkinimo;
- **leidimas pasikeisti rodomus elementus** – didesnės laisvės davimas vartotojui didina pasitenkinimą sistemos vartojimu [ND19]. Leidžiama pasikeisti rodomą nuotrauką ar girdimą garsą, kad vartotojui nereikėtų perdiegti programos.

Pateikti pasiūlymai yra įtraukiami į suasmenintų apsaugos ženklų modelį. Registracijos metu vartotojui leidžiama pasirinkti nuotrauką bei įrašyti garsą. Garsinė rinkmena pasirenkama iš jau egzistuojančių arba įrašoma mikrofonu (13 pav.). Vartotojui suteikus leidimą tai padaryti, pateikiamas informacinis pranešimas apie vykstantį garso įrašymą. Vėliau, po prisijungimo, suteikiama galimybė šį garsą išsaugoti duomenų bazėje. Nuotrauką, kurią irgi galima išsaugoti, taip pat galima pasirinkti iš jau esamų įrenginyje arba padaryti su kamera (14 pav.). Šie multimedijos elementai prisijungimo metu yra parodomi vartotojui (15 pav.). Paprašoma įsijungti garsą ir išklausyti grotą rinkmeną dar kartą. Testavimo metu su realiais vartotojais sprendžiama, kuriuos patobulinimus palikti, o kurie kelia neigiamas emocijas.

13 pav. Garsinės rinkmenos pasirinkimas



14 pav. Paveikslėliuko pasirinkimas

15 pav. Prisijungimo metu rodomas paveiksliukas ir grojamas garsas

Apibendrinant, pasirinkti gerinti suasmeninti apsaugos ženklai, kadangi jie nepriklauso nuo kitų programų. Prie jo veikimo pridedamas garsinės rinkmenos naudojimas, dažnesnis vartotojo informavimas žinutėmis, padarytų nuotraukų ir įrašyto garso saugojimas tik programos dokumentų kataloge, galimybė jas įkelti į duomenų bazę, vartotojo įtraukimas prašymu įsijungti garsą ar pasirinkti daugiau nuotraukų bei leidimas pakeisti rodomus elementus. Šiais pakeitimais siekiama pagerinti atsparumą išoriniam stebėjimui bei spėliojimui, padidinti atstatomumą bei prisimenamumą, ir sumažinti padaromų klaidų vidurkį.

2.5. Mobiliųjų telefonų apsaugos modelių analizės apibendrinimas

Principinis sprendimas gautas įgyvendinus apsaugos modelių panaudojamumo ir saugumo analizę. Šis vertinimas yra svarbus, nes neefektyvus modelis priveda prie reputacinės ir finansinės žalos, o blogai suprojektuotas – padaro programą įkyria ir nemalonia naudotis. Pasirinkti vertinti vartotojo sąsają keičiantys modeliai, nes jie skatina vartotojų pastabumą bei nepasiduoda įrenginio resursų ir izoliuotos aplinkos limitavimui. Pirmasis vertintas suasmenintų apsaugos ženklų modelis nereikalauja papildomų įrenginių, trunka tik apie 30 sekundžių, turi tik 4 veiksmus, tik penktadalis asmenų nepastebėjo problemų, bet masteliavimas bei prisimenamumas yra vidutiniai, o atstatomumas – žemas. Jo atsparumas apsimetinėjimui bei vidiniam stebėjimui yra aukštas, bet išoriniam stebėjimui ir spėliojimui – vidutinis. Jam reikia suteikti prieigą prie nuotraukų galerijos bei saugyklos, tačiau trečiosios šalys nėra reikalingos. Antrasis vertintas suasmenintų pranešimų modelis reikalauja atskiros, informaciją teikiančios programos, labiausiai priimtinas su vienu nuspalvintu sakiniu, tik apie dešimtadalį žmonių rodomos žinutės neįvertino, tetrunka keletą sekundžių ir yra panaudojamas daugybėje programų, tačiau nereikalauja prisimenamumo ir atstatomumo, nes yra informacinio pobūdžio. Jo atsparumas išoriniam stebėjimui, apsimetinėjimui, spėliojimui yra aukštas, bet efektyvumas sumažėja pakeitus nustatymus. Jam reikia atskiros programos arba operacinės sistemos pakeitimų, leidimo rodyti pranešimus ir skenuoti programas bei rodymo limitų. Trečiasis vertintas būsenos juostos modelis yra labai panašus. Jam taip pat reikalinga atskira programa, geriausiai veikia kaip vienas sakinys ar spalva, tetrunka keletą sekundžių bei nereikalauja prisimenamumo. Su šiuo modeliu tik ketvirtadalis žmonių nepastebėjo problemų, o jo masteliavimas ir atstatomumas yra vidutiniai. Būsenos juostos atsparumas stebėjimui, apsimetinėjimui bei spėliojimui yra aukštas, bet sutrikdyti programa sukeltų bėdų. Jai reikia informaciją teikiančios programos, leidimo tikrinti aplinką bei užtikrinti, kad nerodytų jautrios informacijos. Kadangi suasmeninti apsaugos ženklai nuo nieko kito nepriklauso, pasirinkta gerinti šio modelio rodikliai įtraukiant garsinę rinkmeną, išsaugojimą duomenų bazėje, prašymu įjungti garsą, keliomis pasirinktinomis nuotraukomis bei leidimu pasikeisti rodomus elementus.

3. Telefonų apsaugos modelio patobulinimų įgyvendinimas ir validavimas

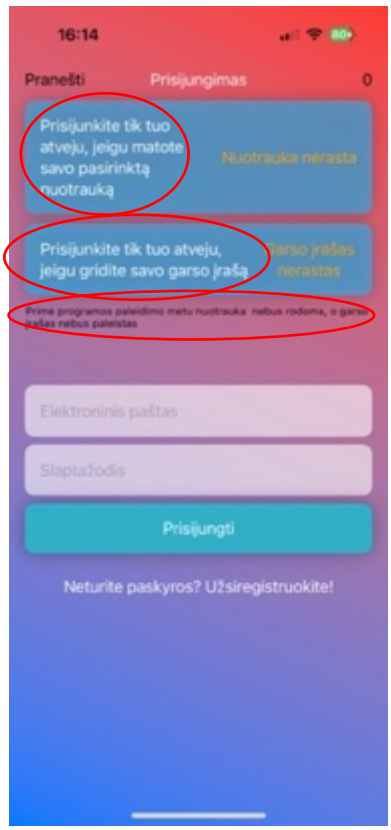
Patobulinimų validacija yra suskirstyta į keletą poskyrių. Pirmajame pateikiama informacija apie padarytą programą ir dalyvius. Antrajame pateikiama informacija apie vartotojams pateiktus scenarijus ir informacijos rinkimo būdus. Galiausiai trečiajame surašomi testavimo rezultatai ir palyginimas su kitais vartotojo sąsają keičiančiais modeliais.

3.1. Apsaugos modelio patobulinimus pritaikanti programa ir dalyviai

Dalyviams buvo pateikta specialiai „iOS“ operacinei sistemai skirta programėlė. Ji sukurta su „Swift“ programavimo kalba, o vartotojo sąsajai sudėlioti – „SwiftUI“ karkasu. Programinis kodas sudėliotas „MVVM“ architektūros pagrindu. Multimedijos duomenims saugoti pasitelkta „Firebase Storage“ debesijos paslauga, o prisijungimo duomenų tvarkymui – „Firebase Authentication“. Nuotrauka ir garso įrašas yra pirmiausia patalpinami į programos dokumentų katalogą, o į debesį sukeliami tik vartotojui pasirinkus tokį variantą.

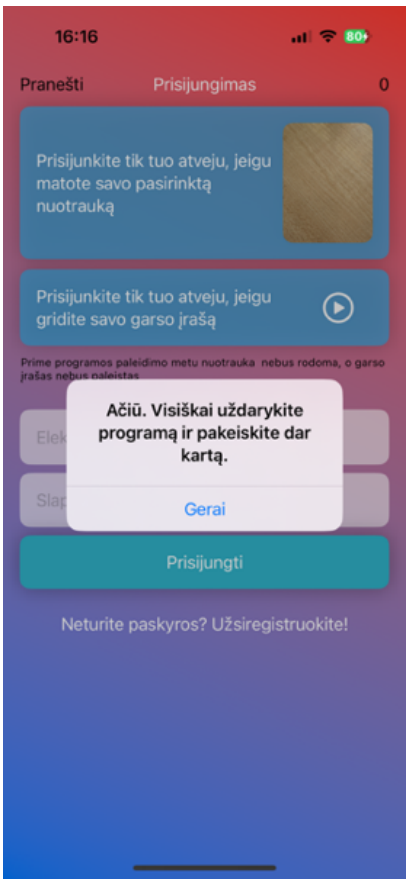
Testavime dalyvavo 6 asmenys, kurie turi skirtingą patirtį bei priklauso skirtingo amžiaus grupėms, siekiant atlikti kokybinį tyrimą. Du iš jų dirba informacinių technologijų srityje, todėl turi aukštesnį supratimą, du iš jų jaunesni, kurie dirba kitose srityse, ir du vyresnio amžiaus, turintys vidutinį technologinį raštingumą. Tokia dalyvių įvairovė leido patikrinti sprendimo tinkamumą įvairaus profilio naudotojams.

Programėlė susideda iš trijų ekranų, kurie turi skirtingą funkcionalumą. Pirmiausia vartotojas mato prisijungimo langą. Jame leidžiama įvesti prisijungimo duomenis bei prisijungti. Vartotojui taip pat pateikiami paaiškinamieji tekstai apie tai, jog turėtų matyti bei girdėti registracijos metu arba vėliau programoje pasirinktą nuotrauką bei garso įrašą, ir kad pirmą kartą įsidiegus programą nieko nematys (16 pav.). Vartotojas paprašomas įsijungti garsą, nes kitu atveju prie programos prisijungti jis negalės (17 pav.). Testavimo tikslais dar pateikiamas ir mygtukas, kurį paspaudus pranešama apie neteisingus veiksmus, tokius kaip netinkamos nuotraukos rodymas (18 pav.). Vartotojui leidžiama pereiti ir į registracijos langą (19 pav.) . Jis panašus į prisijungimo, tačiau čia jau galima pasirinkti arba padaryti nuotrauką (20 pav.) bei pasirinkti arba įrašyti garso įrašą (21 pav.). Po registracijos ir prisijungimo vartotojas yra perkeliamas į pagrindinį puslapį. Jame rodomi telefone bei debesyje išsaugoti multimedijos elementai (22 pav.). Čia vartotojui leidžiama juos pakeisti, parsisiųsti iš debesies, arba į jį įkelti duomenis. Jeigu atliktas veiksmas buvo sėkmingas, išmetamas žalias pranešimas, jeigu ne – raudonas (23 pav.).

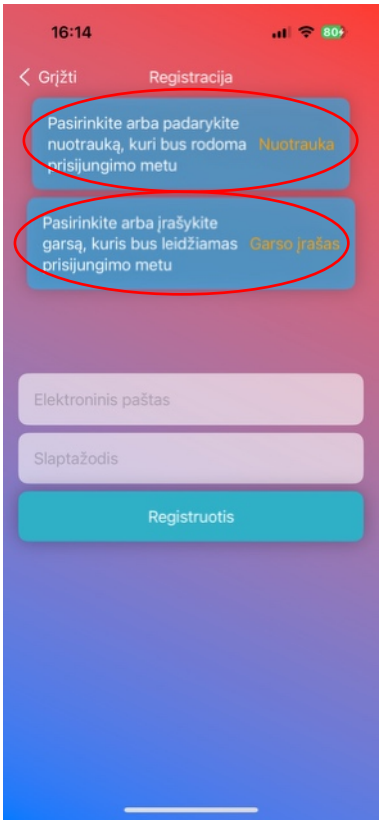


16 pav. Prisijungimo langas su paaiškinimais

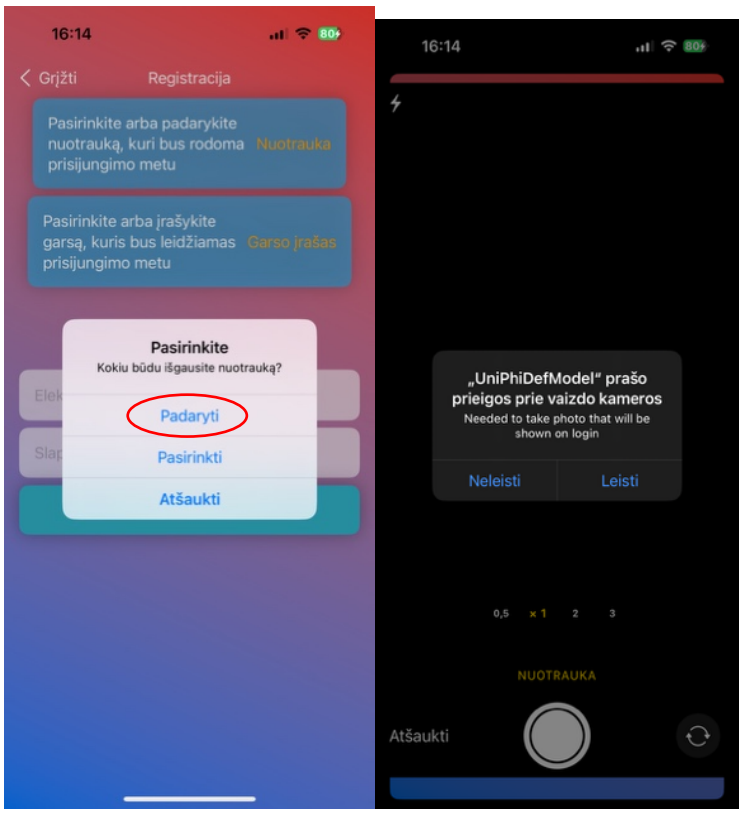
17 pav. Prašoma įjungti garsą ir išklausyti įrašą



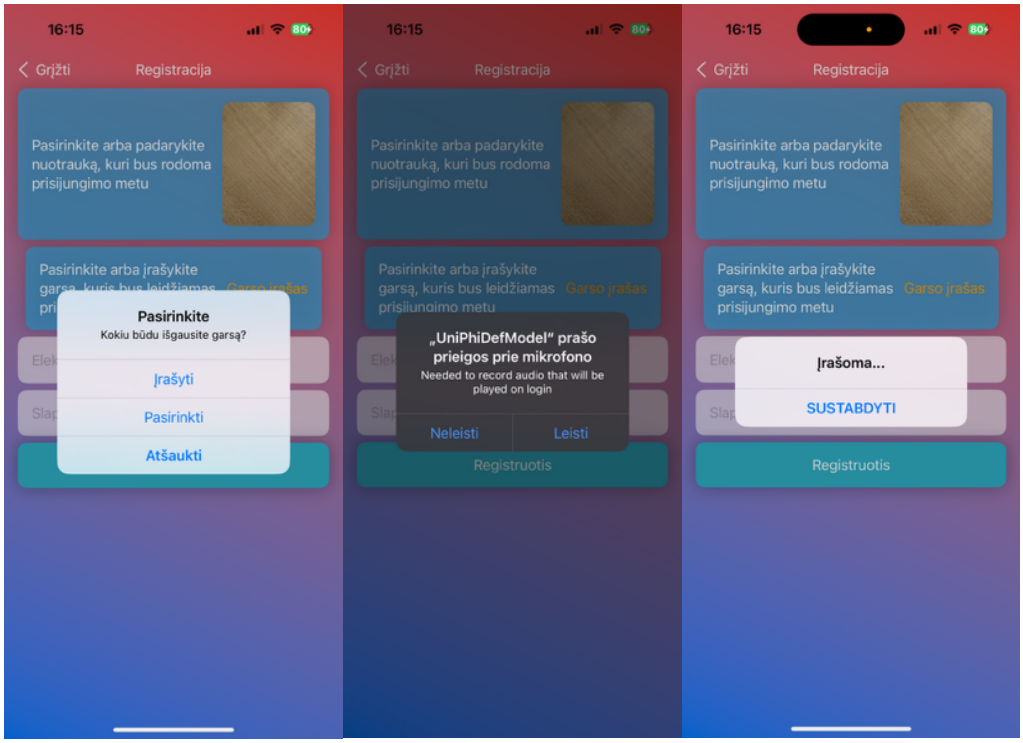
18 pav. Prašoma įjungti programą iš naujo po pranešimo apie neatitikimus



19 pav. Registracijos langas su paaiškinimais

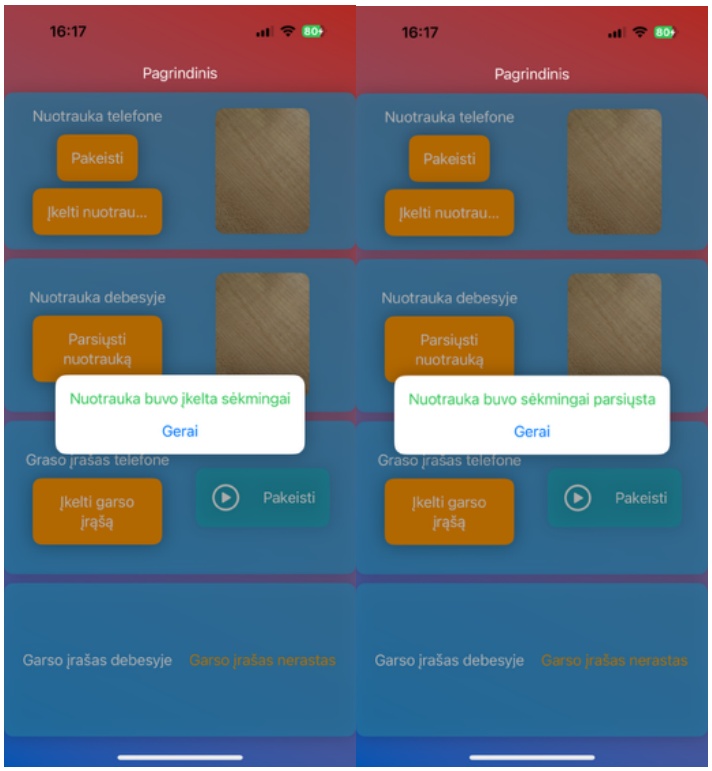


20 pav. Nuotraukos gavimo eiga: pateikiami nuotraukos išgavimo variantai, paspaudus padaryti prašoma leidimo įjungti kamerą



21 pav. Garso įrašymo eiga: rašoma pasirinkti grašo įrašo gavimo būdą, toliau prašoma suteikti mikrofono pasitelkimo leidimą, ir galiausiai informuojama apie įrašymą

22 pav. Pagrindinis puslapis su matomais įrenginyje bei debesyje esamais multimedijos elementais



23 pav. Sėkmingo nuotraukos įkėlimo bei parsisiuntimo pavyzdys

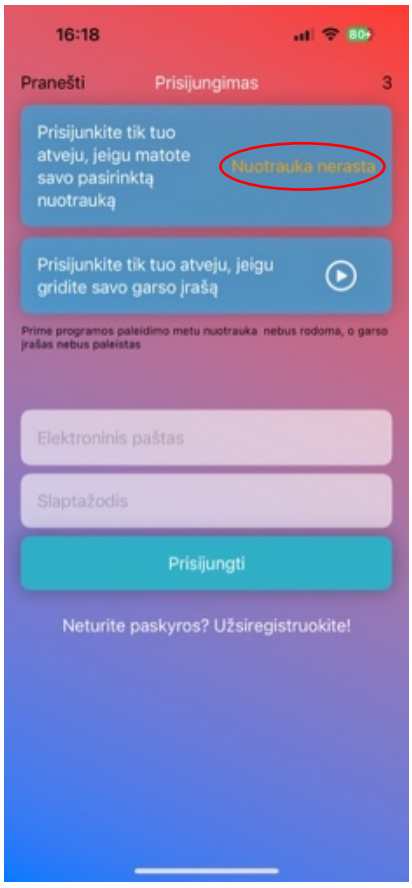
Apibendrinant, modelis ištestuotas pasitelkus realius vartotojus, kuriems buvo duota „iOS“ programėlė. Tyrime dalyvavo 6 įvairią technologinę patirtį turintys asmenys. Jiems buvo leista pasirinkti prisijungimo metu rodomą nuotrauką bei grojamą garsą, pažymėti matomą problemą ir įsikelti multimedijos elementus į debesį.

3.2. Dalyviams pateikti testavimo scenarijai ir informacijos rinkimas

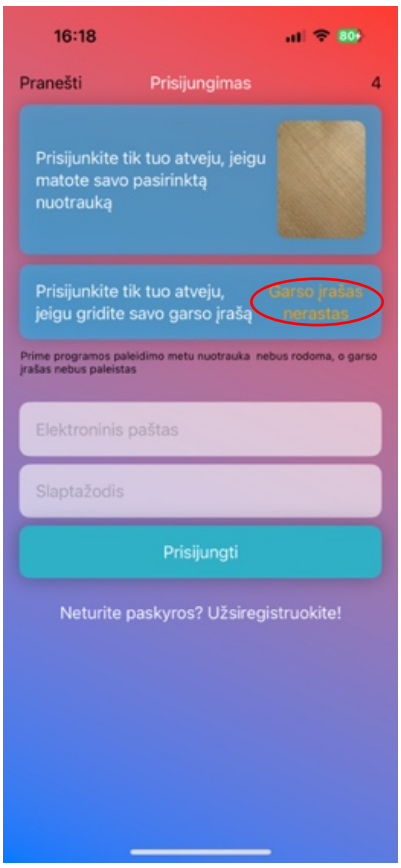
Kiekvieną kartą vartotojui įsijungus programą pateikiami skirtingi scenarijai: rodoma pasirinkta nuotrauka bei grojamas pasirinktas garsas (24 pav.), rodoma netinkama nuotrauka, grojamas netinkamas garsas (25 pav.), nerodoma nuotrauka (26 pav.) ir negrojamas garsas (27 pav.). Tokiu būdu tikrinamas žmogaus pastabumas bei programos dizaino tinkamumas. Vartotojas paprašomas prisijungti, arba paspausti pranešimo mygtuką, jeigu mato neatitikimus. Kartu tikrinami ir kiti veiksmai: ar perskaito žinutes, ar pasirenka elementus registracijos metu, ar supranta, kam reikalingas įrašymas į debesį, ar praverstų didesnis nuotraukų pasirinkimas, ar rinktųsi garso įrašymą, ar suprato tyrimo tikslą, ar tinka prašymas įsijungti garsą, ir ar suprato tyrimo tikslą. Ši informacija leidžia daryti prielaidą apie panaudojamumo bei saugumo balanso pagerėjimą.

24 pav. Rodoma pasirinkta nuotrauka ir grojamas pasirinktas įrašas

25 pav. Rodoma kita nuotrauka, grojamas kitas įrašas

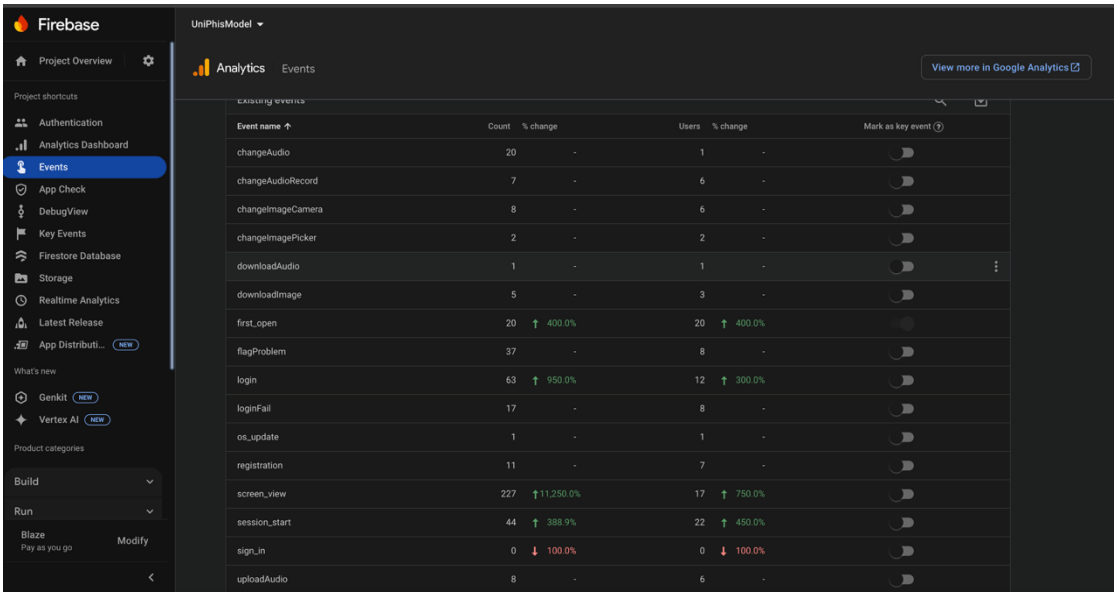


26 pav. Rodoma, kad nuotrauka nerasta



27 pav. Rodoma, kad nėra įrašo

Rezultatams reikalinga informacija buvo renkama įvairias būdais. Vienas iš jų buvo vartotojų elgsenos stebėjimas ir užrašinėjimas. Kitas – vartotojų klausinėjimas apie sistemos naudojimosi patirtį, suvokimą, norus ir pasirinkimus. Galiausiai kiekvienas paspaudimo įvykis buvo registruojamas, kad būtų galima padaryti išvadas (28 pav.).



28 pav. Firebase registruojama vartotojų veikla

Apibendrinant, informacija rezultatams buvo renkama įvairias būdais, o modelio veikimui patikrinti vartotojams pateikiami keli tikėtini kenkėjiškos programos scenarijai. Vartotojų elgsena fiksuojama automatinėmis priemonėmis, apklausomis bei stebėjimu. Prisijungimo metu vartotojui pateikiama teisinga nuotrauka ir tinkamas garsas, jokios nuotraukos, jokio garso, netinkama nuotrauka arba netinkamas garsas. Vartotojo prašoma prisijungti arba užfiksuoti ekrane matomą problemą.

3.3. Modelio patobulinimų testavimo rezultatai

Po tyrimo išryškėjo keletas tendencijų. Didžioji dalis žmonių iš pradžių neskaitė pranešimų, nebandė pasirinkti nei nuotraukos, nei garso, bei nesuprato įkėlimo į debesį prasmės. Dauguma bent vieną kartą prisijungė prie paskyros, nors ekrane matė klaidingus multimedijos elementus (3 lentelė). Po kurio laiko visi suprato tyrimo esmę ir pradėjo atskirinėti, kada to daryti nereikėtų. Visiems tiko nuotraukos bei garso įkėlimo variantai, tačiau keli dalyviai pareiškė, kad garso niekada nejungia, tai tokio varianto nesirinktų (4 lentelė). Didžioji dalis dalyvių buvo nepatenkinti garso įjungimo prašymu (5 lentelė). Visiems pasirodė logiškas leidimas įkelti į debesį, nors iš pradžių nesuprato, kam to reikėtų. Visi po kurio laiko atpažino savo pasirinktus multimedijos elementus ir kai kurie pamėgino juos parsisiųsti iš duomenų bazės. Žmonės tiko kelių nuotraukų pasirinkimas, nes padidėja sugumas, bet kai kuriems to būtų per daug.

3 lentelė Veiksmai su multimedija

Dalyvis/Veiksmas	Registracijos metu pasirinko nuotrauką	Registacijos metu įrašė garsą	Po prisijungimo pasirinko nuotrauką	Po prisijungimo įrašė garsą	Įkėlė multimedijos elementus į debesį
Pirmas	Taip	Taip	Taip	Taip	Taip
Antras	Ne	Ne	Taip	Taip	Taip
Trečias	Taip	Ne	Ne	Ne	Ne
Ketvirtas	Ne	Ne	Taip	Taip	Taip
Penktas	Ne	Ne	Taip	Taip	Taip
Šeštas	Ne	Ne	Ne	Ne	Ne

4 lentelė Pastabumo veiksmai

Dalyvis/Veiksmas	Skaitė informacines žinutes	Prisijungė klaidingu metu	Ilgainiui pradėjo pastebėti neatitikimus	Po kurio laiko atpažino savo įkeltą nuotrauką ar garsą	Parsisiuntė multimedijos elementus iš debesies
Pirmas	Taip	Taip	Taip	Taip	Taip

Antras	Ne	Taip	Taip	Taip	Ne
Trečias	Ne	Ne	Taip	Taip	Ne
Ketvirtas	Taip	Ne	Taip	Taip	Taip
Penktas	Ne	Taip	Taip	Taip	Taip
Šeštas	Ne	Taip	Ne visai	Taip	Ne

5 lentelė Pasirinkimų atsakymai

Dalyvis/Veiksmas	Tinka nuotraukos pasirinkimas	Tinka garso pasirinkimas	Norėtų daugiau nuotraukų	Suvokė įkėlimo į debesį prasmę	Tinka prašymas įjungti garsą
Pirmas	Taip	Taip	Taip	Taip	Ne
Antras	Taip	Taip	Ne	Ne	Taip
Trečias	Taip	Ne	Ne	Ne	Ne
Ketvirtas	Taip	Taip	Ne	Ne	Taip
Penktas	Taip	Ne	Taip	Ne	Ne
Šeštas	Ne	Taip	Ne	Ne	Ne

6 lentelė Patobulinimų panaudojamumo vertinimas

Modelis/Savybės	Papildomi įrenginiai	Matomų elementų ar veiksmų kiekis	Padaromų klaidų vidurkis	Proceso laikas	Masteliavimas	Prisimenamumas	Atstatomumas
Pagerintas modelis	Nereikalingi	8 veiksmai	6 klaidos	40 sekundžių	Aukštas	Aukštas	Aukštas

7 lentelė Patobulinimų saugumo vertinimas

Modelis/Savybės	Atsparumas išoriniam stebėjimui	Atsparumas apsimetinėjimui	Atsparumas spėliojimui	Atsparumas vidiniam stebėjimui	Trečiųjų šalių reikalingumas	Leidimų suteikimo reikalingumas	KVP trikampis?
Pagerintas modelis	Vidutinis	Aukštas	Vidutinis	Aukštas	Reikia	Reikia	Taip

Įvertinus pagerinimus pagal panaudojamumo (6 lentelė) ir saugumo (7 lentelė) savybes galima teigti, jog patobulinimai yra vertingi. Proceso laiko ir klaidų vidurkio padidėjimas yra nežymūs, o masteliavimas, prisimenamumas bei atstatomumas pagerėjo. Saugumo vertinimas nepakito, tik prireikė trečiųjų šalių multimedijos elementams saugoti.

Apibendrinant, didžioji dalis modelio patobulinimų pasiteisino. Nors didžioji dalis dalyvių iš pradžių žinučių neskaitė ir nieko nepasirinko, vėliau pradėjo suprasti nuotraukos ir garso pasirinkimo prasmę. Keletas asmenų prisijungė netinkamu metu, bet ilgainiui pradėjo pastebėti trūkumus. Taip pat su patobulinimais pagerėjo masteliavimas, prisimenamumas ir atstatomumas, nors prireikė trečiųjų šalių įsikišimo. Kiti saugumo rodikliai liko tokie patys.

3.4. Modelio validacijos apibendrinimas ir projektavimo rekomendacijos

Buvo atlikta modelio patobulinimų validacija su realiais vartotojais. Jiems duota iOS operacinei sistemai skirta programėlė. Ją sudarė prisijungimo, registracijos bei pagrindinis langai. Prisijungimo metu vartotojas mato savo pasirinktą nuotrauką, girdi įrašytą garsą ir gali prisijungti, registracijos metu šiuos multimedijos elementus pasirenka ir gali prisiregistruoti, o pagrindinis langas taip pat juos rodo, leidžia įkelti į debesį, parsiųsti bei juos pasikeisti. Kiekvienas veiksmas lydimas prašymu suteikti reikalingus leidimus ir pranešimu apie statusą. Kiekvieną kartą vartotojui jungiantis pateikiamas skirtingas scenarijus: tinkama nuotrauka su tinkamu garsu, netinkama nuotrauka, netinkamas garsas, nerodoma nuotrauka ar nerodomas garsas. Informacija apie veikimą rinkta stebint vartotojo elgseną, fiksuojant paspaudimus bei apklausos būdu. Didžioji dalis iš pradžių neskaitė pranešimų ir nesirinko nuotraukų, bet prisijungę tai pamėgino padaryti. Keletas nesuprato įkėlimo į debesį prasmės ir buvo nepatenkinti prašymu įjungti garsą. Panaudojamumo rodikliai tokie kaip prisimenamumas ir atstatomumas pagerėjo, o saugumo nepakito, nors prisidėjo trečiųjų šalių įsikišimas.

Po validacijos išryškėjo projektavimo rekomendacijos. Aiškus ir nuoseklus informavimas yra labai svarbus vartotojui, kad prašymas atlikti veiksmus būtų lengviau suprantamas. Išvada vedama iš to, kad dalyviai nesuprato įkėlimo į debesį prasmės iki kol tai buvo jiems paaiškinta. Taip pat jutiklių įtraukimas, didesnis lankstumas ir pasirinkimų įvairovė skatina vartotojo įsitraukimą ir pastabumą. Tai galima teigti iš to, nes garsinės rinkmenos ir daugybinių nuotraukų pasirinkimas vertintas teigiamai. Taip pat yra svarbu užtikrinti vartotojo pasirinkimo laisvę, kadangi prašymas įjungti garsą ir išklausyti įrašą buvo priimtas labai skeptiškai, o paskutinis dalyvis susilaikė nuo nuotraukos ir garso įrašo įkėlimo. Galutiniame modelyje leidžiama: pasirinkti daugiau nuotraukų, pasirinkti garsinę rinkmeną, prisijungus pakeisti rodomos multimedijos elementus, juos įkelti į duomenų bazę.

Rezultatai ir išvados

Po atliktos apžvalgos ir įgyvendintų uždavinių pasiekti rezultatai:

1. Atlikus literatūros analizę surinkti apsaugos nuo duomenų vagysčių būdai ir modeliai bei esamų vartotojo sąsajų pažeidžiamumai.
2. Analizuojant literatūrą identifikuoti suasmeninti apsaugos ženklai, pranešimai ir būsenos juostos modeliai įvertinti pagal saugumo ir panaudojamumo kriterijus:
    a. pirmąjį atlikti vartotojai užtruko 30 sekundžių, jam nereikia papildomų įrenginių ir tereikia atlikti keturis veiksmus, bet atstatomumo, prisimenamumo ir masteliavimo vertinimai yra vidutiniai arba žemi;
    b. pirmojo atsparumas vidiniam stebėjimui ir apsimetinėjimui yra aukštas, bet spėliojimui ir išoriniam stebėjimui – vidutinis;
    c. kiti tetrunka kelias sekundes, geriausiai veikia kaip vienas trumpas spalvotas sakinys, ir reikalauja papildomos programos informacijai surinkti;
    d. kitų atsparumas yra aukštas, bet atsparumas vidiniam stebėjimui yra vidutinis;
3. Sukurtos rekomendacijos mobiliąsias vartotojo sąsajas kuriantiems projektuotojams.
4. Sukurtas rekomendacijas iliustruojantis prototipas.

Atlikus tyrimą gautos išvados:

1. Literatūros analizė parodė, kad vartotojų elgsena nulemia duomenų vagystės sėkmę, dėl to budrumo ir pastabumo gerinimas tvarkingai suprojektuotomis programomis ar modeliais priveda prie geresnio apsisaugojimo;
2. Kadangi tik keli straipsniai aptarė vartotojo sąsają keičiančių modelių indėlį į apsaugą prieš duomenų vagystes, todėl nuspręsta šią sritį tirti šiame darbe. Esamų modelių analizė parodė, jog suasmeninti apsaugos ženklai nepriklauso nuo kitų programų, ir turi trūkumų su masteliavimu, prisimenamumu ir atstatomumu, kurių reikšmės galėtų būti pagerinamos įtraukus garsinio formato rinkmeną, galimybę pasikeisti pasirinktus multimedijos elementus ir leidimą įsikelti multimedijos elementus į duomenų bazę.
3. Testavimo dalyviai nepasirinko multimedijos elementų ir klydo atpažindami neatitikimus iki kol neperskaitė ekrane esamų pranešimų. Visi teigiamai vertino garsinio failo pasirinkimą, galimybę pasirinkti daugiau nuotraukų bei įkėlimą į duomenų bazę, nors iš pradžių nesuprato, kam to reikia. Ilgainiui visi pradėjo pastebėti neatitikimus.
4. Patobulinimų testavimas su vartotojais parodė, jog panaudojamumas buvo pagerintas nepažeidžiant saugumo ir budrumą įmanoma pakelti, tačiau vis tiek atsiras žmonių, kurie rinksis patogumą. Todėl modeliai turi būti toliau tobulinami.

Šaltiniai

[AZ21] Alkhalil, Zainab, et al. "Phishing attacks: A recent comprehensive study and a new anatomy." *Frontiers in Computer Science* 3 (2021): 563060. https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

[BA20] Bhardwaj, Akashdeep, et al. "Why is phishing still successful?." *Computer Fraud & Security* 2020.9 (2020): 15-19. https://www.sciencedirect.com/science/article/pii/S1361372320300981

[BJ+12] Bonneau, Joseph, et al. "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes." *2012 IEEE symposium on security and privacy*. IEEE, 2012. https://ieeexplore.ieee.org/abstract/document/6234436?casa_token=NW3wazxVrF4AAAAA:0RM9cro5YnQppjAG0hPziJegq1sL6kHSTJTdk6GQLSgy9IJetxoGV7R4VpuZXYhxLvBqeglU7A

[CJT15] Chang, Yung-Ju, and John C. Tang. "Investigating mobile users' ringer mode usage and attentiveness and responsiveness to communication." *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*. 2015. https://dl.acm.org/doi/abs/10.1145/2785830.2785852

[CM+21] Cooper, Molly, et al. "Heads-up! An alert and warning system for phishing emails." *Organizational Cybersecurity Journal: Practice, Process and People* 1.1 (2021): 47-68. https://www.emerald.com/insight/content/doi/10.1108/OCJ-03-2021-0006/full/html

[CM+23] Chowdhury, MD Minhaz, et al. "Chatgpt: A threat against the cia triad of cyber security." *2023 IEEE International Conference on Electro Information Technology (eIT)*. IEEE, 2023. https://ieeexplore.ieee.org/abstract/document/10187355

[CPS16] Chorghe, Sharvari Prakash, and Narendra Shekokar. "A survey on anti-phishing techniques in mobile phones." *2016 International Conference on Inventive Computation Technologies (ICICT)*. Vol. 2. IEEE, 2016. https://ieeexplore.ieee.org/abstract/document/7824819

[FE-17] Fernandes, Earlence, et al. "Android ui deception revisited: Attacks and defenses." Financial Cryptography and Data Security: 20th International

Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers 20. Springer Berlin Heidelberg, 2017.
https://ics.uci.edu/~alfchen/pubs/earlence_fc16.pdf

[FSM+19] Furnell, Steven, Kieran Millet, and Maria Papadaki. "Fifteen years of phishing: can technology save us?." *Computer Fraud & Security* 2019.7 (2019): 11-16.
https://www.sciencedirect.com/science/article/pii/S1361372319300740

[GDJ18] Goel, Diksha, and Ankit Kumar Jain. "Mobile phishing attacks and defence mechanisms: State of art and open research challenges." *computers & security* 73 (2018): 519-544.
https://www.sciencedirect.com/science/article/pii/S0167404817302717

[GRC+23] Goenka, Richa, Meenu Chawla, and Namita Tiwari. "A comprehensive survey of phishing: mediums, intended targets, attack and defence techniques and a novel taxonomy." *International Journal of Information Security* (2023): 1-30.
https://link.springer.com/article/10.1007/s10207-023-00768-x

[GSB21] Garg, Shivi, and Niyati Baliyan. "Comparative analysis of Android and iOS from security viewpoint." *Computer Science Review* 40 (2021): 100372.
https://www.sciencedirect.com/science/article/abs/pii/S1574013721000125

[HA+21] Husainiamer, Muhammad'Afif, et al. "Mobile malware classification for ios inspired by phylogenetics." *International Journal of Advanced Computer Science and Applications* 12.8 (2021).
Mobile Malware Classification for iOS Inspired by Phylogenetics

[IS+21] Ishartono, Naufal, et al. "Visual, Auditory, and Kinesthetic Students: How They Solve PISA-Oriented Mathematics Problems?." *Journal of Physics: Conference Series*. Vol. 1720. No. 1. IOP Publishing, 2021.
https://iopscience.iop.org/article/10.1088/1742-6596/1720/1/012012/meta

[ISO-9241-11:2018] Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts

Jung, Crescentia, et al. "Communicating visualizations without visuals: Investigation of visualization alternative text for people with visual impairments." *IEEE transactions on visualization and computer graphics* 28.1 (2021): 1095-1105.
https://ieeexplore.ieee.org/abstract/document/9552938

[JJL15] Jansen, Jurjen, and Rutger Leukfeldt. "How people help fraudsters steal their money: An analysis of 600 online banking fraud cases." *2015 workshop on socio-technical aspects in security and trust*. IEEE, 2015. https://ieeexplore.ieee.org/abstract/document/7351973

[KJ+19] Khalid, Javaria, et al. "Anti-phishing models for mobile application development: a review paper." Intelligent Technologies and Applications: First International Conference, INTAP 2018, Bahawalpur, Pakistan, October 23-25, 2018, Revised Selected Papers 1. Springer Singapore, 2019. https://link.springer.com/chapter/10.1007/978-981-13-6052-7_15

[KMI+13] Khonji, Mahmoud, Youssef Iraqi, and Andrew Jones. "Phishing detection: a literature survey." *IEEE Communications Surveys & Tutorials* 15.4 (2013): 2091-2121. https://ieeexplore.ieee.org/abstract/document/6497928

[KSS+18] Khan, Muhammad Salman, Sana Siddiqui, and Ken Ferens. "A cognitive and concurrent cyber kill chain model." *Computer and Network Security Essentials* (2018): 585-602. https://link.springer.com/chapter/10.1007/978-3-319-58424-9_34

[LC+10] Jiang, Li, Hao Chen, and Fei Deng. "A security evaluation method based on STRIDE model for web service." *2010 2nd International Workshop on Intelligent Systems and Applications*. IEEE, 2010 https://ieeexplore.ieee.org/abstract/document/5473445

[LPS21] López-Aguilar, Pablo, and Agusti Solanas. "Human susceptibility to phishing attacks based on personality traits: The role of neuroticism." *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2021. https://ieeexplore.ieee.org/abstract/document/9529789

[LT-16] Laukkanen, Tommi. "Consumer adoption versus rejection decisions in seemingly similar service innovations: The case of the Internet and mobile banking." *Journal of Business Research* 69.7 (2016): 2432-2439. https://www.sciencedirect.com/science/article/pii/S0148296316000266

[MC+16] Marforio, Claudio, et al. "Evaluation of personalized security indicators as an anti-phishing mechanism for smartphone applications." *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 2016. https://dl.acm.org/doi/abs/10.1145/2858036.2858085

[MMS+21] Masela, Maximeliana, and Adaninggar Septi Subekti. "Auditory and kinaesthetic learning styles and L2 achievement: A correlational study." *Englisia: Journal of Language, Education, and Humanities* 8.2 (2021): 41-53. https://jurnal.ar-raniry.ac.id/index.php/englisia/article/view/7529

[MSS19] Mishra, Sandhya, and Devpriya Soni. "SMS phishing and mitigation approaches." *2019 twelfth international conference on contemporary computing (ic3)*. IEEE, 2019. https://ieeexplore.ieee.org/abstract/document/8844920

[NB23] Naqvi, Bilal, et al. "Mitigation strategies against the phishing attacks: A systematic literature review." *Computers & Security* (2023): 103387. https://www.sciencedirect.com/science/article/pii/S0167404823002973?via%3Dihub

[ND19] Ndibwile, Jema David. "Validation Agents and Persuasive Designs for Phishing Detection and Update Compliance on Smartphones." (2019). Validation agents and persuasive designs for phishing detection and update compliance on smarphones

[P16] David Platt - The Joy of UX_ User Experience and Interactive Design for Developers (2016, Addison-Wesley Professional)

[PGS+22] Peter, Geno, Albert Alexander Stonier, and Anli Sherine. "Development of mobile application for e-voting system using 3-step security for preventing phishing attack." *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. IEEE, 2022. https://ieeexplore.ieee.org/abstract/document/9823503

[PTM+22] Panga, Rosemary Cosmas Tlatlaa, Janeth Marwa, and Jema David Ndibwile. "A Game or Notes? The Use of a Customized Mobile Game to Improve Teenagers' Phishing Knowledge, Case of Tanzania." *Journal of Cybersecurity and Privacy* 2.3 (2022): 466-489. https://www.mdpi.com/2624-800X/2/3/24

[PX+16] Pham, Xuan-Lam, et al. "Effects of push notifications on learner engagement in a mobile learning app." *2016 IEEE 16th International Conference on Advanced Learning Technologies (ICALT)*. IEEE, 2016. https://ieeexplore.ieee.org/abstract/document/7756930

[RZG24] Rui, Zhepeng, and Zhenyu Gu. "Use of event-related potentials to assess visual–auditory multisensory information in the decision-making processes related to

fast-consuming behavior." *International Journal of Human–Computer Interaction* 40.22 (2024): 7019-7042. https://www.tandfonline.com/doi/full/10.1080/10447318.2023.2260983

[SAP+21] Szarvák, Anikó, Valéria Póser, and Miklós Kozlovszky. "Simplification on mobile devices reduces personal (cyber) safety." *2021 IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. IEEE, 2021. https://ieeexplore.ieee.org/abstract/document/9465589

[SS+20] Subairu, Sikiru, et al. "A Review of Detection Methodologies for Quick Response code Phishing Attacks." *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. IEEE, 2020. https://ieeexplore.ieee.org/abstract/document/9257687

[VA16] Vishwanath, Arun. "Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks." *Computers in Human Behavior* 63 (2016): 198-207. https://www.sciencedirect.com/science/article/pii/S0747563216303624

[WLD+15] Wu, Longfei, Xiaojiang Du, and Jie Wu. "Effective defense schemes for phishing attacks on mobile computing platforms." *IEEE Transactions on Vehicular Technology* 65.8 (2015): 6678-6691. https://ieeexplore.ieee.org/abstract/document/7222471

[WP+20] Weichbroth, Paweł. "Usability of mobile applications: a systematic literature study." *Ieee Access* 8 (2020): 55563-55577. https://ieeexplore.ieee.org/abstract/document/9042272

[WPL20] Weichbroth, Paweł, and Łukasz Łysik. "Mobile security: Threats and best practices." *Mobile Information Systems* 2020 (2020): 1-15. https://www.hindawi.com/journals/misy/2020/8828078/

[ZRM+23] Zieni, Rasha, Luisa Massari, and Maria Carla Calzarossa. "Phishing or not phishing? A survey on the detection of phishing websites." *IEEE Access* 11 (2023): 18499-18519. https://ieeexplore.ieee.org/abstract/document/10049452