VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
INFORMATIKOS INSTITUTAS
KOMPIUTERINIO IR DUOMENŲ MODELIAVIMO KATEDRA

Magistro baigiamasis darbas

Išmaniųjų telefonų autentifikacijos panaudojamumo ir saugumo derinimas iš naudotojo potyrių perspektyvos

Atliko:
Paulius Kaminskas parašas

Vadovas:
Doc., Dr. Kristina Lapin

Vilnius
2021

Turinys

Sutartinis terminų žodynas

Panaudojamumas (angl. *usability*) - kiek nustatytomis aplinkybėmis sistema, produktas ar paslauga gali būti panaudota nustatytų naudotojų, kad būtų galima pasiekti nustatytus tikslus efektyviai, tiksliai ir su malonumu [1].

Efektyvumas (angl. *effectiveness*) – pasiekiamų tikslų užbaigtumas ir tikslumas [1].

Našumas (angl. *efficiency*) - pastangų kiekis reikalingas tikslui pasiekti [1].

Naudotojo potyriai (angl. *User Experience*) - naudotojo suvokimas ir reakcija dėl produkto, sistemos ar paslaugos esamo ar numatomo naudojimo [1].

PIN (angl. *Personal Identification Number*) - autentifikacijai skirtas kodas sudarytas vien iš skaitmenų.

Šablonas (angl. *pattern*) - liečiamiems ekranams skirtas autentifikacijos metodas, kuris autentifikuoja naudotoją pagal naudotojo liečiamus ir sujungiamus taškus.

Puolėjas (angl. *attacker*) - žmogus, kuris savo jėgomis, ar naudodamas programinę įrangą, bando autentifikuotis kaip kitas žmogus.

Fišingas (angl. *phishing*) - apgavystės būdas, kuriame aukai nusiunčiamas panašus į tikrą internetinis adresas, bet juo bandoma iš naudotojo išgauti konfidencilius duomenis.

Autentifikacijos metodas (angl. *authentication method*) - naudotojo prašomi atlikti veiksmai, kurie įrodo tariamą tapatybę.

Autentifikacijos sistema (angl. *authentication system*) - autentifikacijos metodo visą veikimą ar veikimo dalį įgyvendinantis programinis komponentas.

Santrauka

Autentifikacijos metoduose sunku suderinti panaudojamumą ir saugumą dėl jų atvirkštinės koreliacijos. Dėl šios priežasties dauguma metodų yra arba patogiai naudojami ir nesaugūs, arba saugūs ir nepatogūs. Šiame darbe įvertinami jau sukurti autentifikacijos metodai išmaniesiems telefonams pagal panaudojamumą ir saugumą. Darbo tikslas yra sukurti autentifikacijos metodą, kuris suderintų panaudojamumą ir saugumą. Buvo įgyvendintas sukurto metodo prototipas, kuris buvo naudotas tyrimuose ir gauti rezultatai parodė, kad metodas atitinka visus svarbiausius panaudojamumo ir saugumo kriterijus, keliamus išmaniųjų telefonų autentifikacijos metodams.

Summary

Balancing Usability and Security of Authentication in Smartphones from User Experience Perspective

There is a very sensitive relation between usability and security of authentication methods. Both usability and security are important to each other. Prioritising on over the other inevitably causes neglect on the other one. If security is neglected becausse of usability the the whole point of authentication is missed, because it does not provide the required security for the used. If the security ir prioritised over the usability, then the method risks being too difficult or complex to use, thus discoraging users from using it, or making user use various shortcuts to make it easier for themselves. These shortcuts used by users often compromise security, so to guarantee security methods must also have high usability. The goals of this work is to identify requirements for good smartphone authentication methods. Then using those requirements to create an authentication method that balances usability and security.

There are no good systems to evaluate usability and security of smartphone authentication methods. For this reason, in this work, requirements were created based on a web authentication evaluation system. They were adapted for issues, unique to smartphones and so 19 criteria for authentication methods was raised. 8 for usability and 11 for security. Using this crieria 6 authentication methods were evaluated. The results were put in a table and the methods were compared with each other. It was discovered, that authentication methods tend to prioritise either usability or security, thus compromising th unprioritised requirements.

In the second chapter of this work, an authentication method was created. It was based on a previous work, that used a grapical password authentication. The second iteration of the authentication methods had some changes done to it, to improve security and usability. During the creation of the second iteration of the authentication methods it was discovered that usability is a very multidisciplinary requirement. It is impacted by human psychology, anatomy and other things, that are normally not often talked about in IT studies. To improve usability developers must look into the studies of other scientific fields, because there is a lot of important information hidden there.

In the third chapter the studies done on the secuond iteration of the authentication method are described. There were two studies to see how resistant graphical password is to being stolen by watching authentication and by recording it. It was discovered that it is very difficult to capture user's password even when authentication is being recorded. To test usability first authentication time was tracked, which relativelly fast, when compared to other methods. Number of errors was also counted to make sure that the method is not too difficult to consistently do correctly. There was not a hig number of errors during the authentication. A survey for the users was also done, and its results are discussed in the third chapter. Users generally enjoyed the method, although they did have some complaints about the images that were chosen for them to use in authentication. Finally, the second iteration of the authentication method is evaluated using the same criteria as all the oher analysed methods and it is revealed that the second iteration does not compromise on any of the most important requirements and strikes a balance between usability and security.

Įvadas

Išmaniųjų telefonų naudotojų kiekis vis auga ir juose saugomi duomenys yra vis jautresni. Tai, kad išmaniesiems telefonams reikia naujų autentifikacijos metodų jau yra gerai žinoma [6]. Buvo bandymų pritaikyti jau žinomus autentifikacijos metodus išmaniesiems telefonams [12] [20], tačiau rezultatai nėra itin geri, nes tuose metoduose prioritzuojamas arba autentifikacijos metodo panaudojamumas, arba saugumas.

Kai prioritizuojamas metodo panaudojamumas, siekiama autentifikaciją padaryti kuo paprastesnę naudotojui ir tai kenkia saugumui. O kai siekiama sukurti saugią autentifikaciją, tuomet ji reikalauja daug naudotojo pastangų. Kompromiso ieškojimas tarp šių dviejų reikalavimų yra sudėtingas dėl kelių priežasčių. Pirma, patikimiausias būdas įvertinti programos panaudojamumą yra naudojant empirinius tyrimus, tačiau tokius bandymus yra sudėtinga padaryti patikimais, ir tai gali daug kainuoti. Antra, koreliacija tarp panaudojamumo ir saugumo yra labai jautri ir šiuo metu mažai suprasta [15].

Šio darbo tikslas yra sukurti išmaniesiems telefonams skirtą autentifikacijos metodą, kuris derintų panaudojamumą ir saugumą. Šiam tikslui pasiekti yra sprendžiami šie uždaviniai:

1. Atlikus literatūros analizę identifikuoti panauojamumo ir saugumo kriterijus išmaniesiems telefonams.

2. Palyginti populiariausių autentifikacijos metodų saugumą ir patogumą naudojantis iškeltais kriterijais.

3. Sukurti autentifikacijos metodą, kuris atitinka išmaniesiems telefonams keliamus panaudojamumo ir saugumo kriterijus.

4. Sukurti autentifikacijos metodo prototipą ir įvertinti jo panaudojamumą bei saugumą.

Pirmame skyriuje tinklo autentifikacijos metodų vertinimui sukurti kriterijai [7] buvo pritaikyti išmaniųjų telefonų panaudojamumo ir saugumo vertinimui. Naudojant šiuos kriterijus įvertinti ir palyginti šiuo metu plačiai naudojami metodai bei grafiniai metodai, kurie taip pat stengiasi suderinti panaudojamumą ir saugumą. Identifikuoti esamų autentifikacijos metodų trūkumai. Antrame skyriuje remiantis mokslo tiriamuoju darbu sukurtas panaudojamumą ir saugumą derinantis autentifikacijos metodas. Šio autentifikacijos metodo prototipas buvo sukurtas naudojant Java programavimo kalbą Android operacinę sistemą naudojantiems išmaniesiems telefonams. Trečiame skyriuje aprašyti atlikti empiriniai panaudojamumo ir saugumo tyrimai, skirti įvertinti sukurtą autentifikacijos metodą. Atlikta apklausa, bei pateikiamas metodo įvertinimas pagal šiame darbe identifikuotus kriterijus. Darbo rezultatas yra sukurtas išmaniesems telefonams skirtas autentifikacijos metodas, kuris suderina panaudojamumą ir saugumą.

1. Esamų autentifikacijos metodų apžvalga

Nėra standartizuoto būdo įvertinti išmaniųjų telefonų panaudojamumą ir saugumą. Siūlomi nauji autentifikacijos metodai dažnai net neturi jokių tyrimų ar įvertinimų [18] [17]. Tie autentifikacijos metodai, kurie turi tyrimų, dažnai tiesiog tiria prioritizuotus metodo bruožas ignoruodami metodo trūkumus [9].

Šiame darbe visi autentifikacijos metodai vertinti naudojant tuos pačius kriterijus. Tačiau, prieš renkantis ar kuriant autentifikacijos metodų vertinimo sistemą pirmiausia reikia suprasti koks ryšys sieja panaudojamumą ir saugumą.

1.1. Ryšys tarp panaudojamumo ir saugumo

Ryšys tarp panaudojamumo ir saugumo yra labai sudėtingas [3]. Didinant saugumą yra tendencija panaudojamumui kristi, nes saugumas naudotojui trukdo naudotis sistema. Dėl saugumo reikalavimų griežtinimo kyla tikimybė, kad naudotojai bandys gerinti panaudojamumą apeidami saugumą. Todėl planuojant saugumą reikia apgalvoti ir panaudojamumą.

Kompromiso ieškojimas tarp saugumo ir patogumo yra sunkiai randamas. Viena iš priežasčių yra mažas tyrimų kiekis tarp šio ryšio. Taip yra todėl, kad sistemos naudojimo patogumas yra sunkiai apibrėžiamas ir nustatomas dalykas. Be to praktiškai kiekvienas sprendimas ar pakeitimas turi įtakos ir saugumui, ir patogumui. Negalima keisti vieno be kito.

Atrodytų, kad saugumo reikalavimus yra lengva nustatyti, bet tai netiesa. Dažniausiai sunku įvertinti galimą padaryti žalą arba ji stipriai keičiasi tarp naudotojų. Pavyzdžiui, vieni žmonės plančetėse saugo svarbius banko ir asmeninius duomenis, kiti jas naudoja tik žaisti žaidimams. Akivaizdu, kad abiem atvejams yra skirtingi saugumo reikalavimai. Bet koki tie reikalavimai? Negalima visiems atvejams dėti pačių sudėtingiausių saugumo reikalavimų, nes tai stipriai sumažina panaudojamumą be naudos.

1.2. Kriterijai

Nėra sukurtos geros sistemos išmaniųjų telefonų autentifikacijos metodų vertinimui. Dėl šios priežastis šiame darbe autentifikacijos metodai bus vertinami naudojantis sistema, kuri buvo skirta interneto tinklo autentifikacijai [7], bet pritaikyta išmaniesiems telefonams. Nors minėtame darbe kriterijai skirtstomi į tris grupes: panaudojamumą, saugumą ir įgyvendinamumą, šiame darbe apie įgyvendinamumą nekalbėsime, nes daug diskutuojamų metodų nekalba apie tai, kaip jie turėtų būti įgyvendinti „po gaubtu“, todėl reikėtų spekuliuoti, ir todėl, nes įgyvendinimas neturi įtakos naudotojų potyriams, o tai ir yra šio darbo tikslas.

Kiekvienas kriterijus turi aprašymą ir jam priskiriamas kodas, kad juos būtų galima lengviau paminėti tekste. Neįmonama turėti metodo, kuris atitiktų visus šiuos kriterijus ir šių kriterijų svarba gali kisti priklausomai nuo reikalavimų. Šiame darbe kriterijai pritaikyti išmaniųjų telefonų autentifikacijai.

Panaudojamumo kriterijai:

P1 Lengvai atsimenamas (angl. *Memorywise-Effortless*) - metodo veikimas ir naudotojui reikalingas slaptažodis turi būti lengvai atsimenami arba intuityvūs;

P2 Keičiamo dydžio naudotojams (angl. *Scalable-for-Users*) - jei yra šimtai naudotojų paskyrų, tai neturi jokios įtakos individualiam naudotojui. Kintantis kiekis naudotojų neturi turėti jokios įtakos patiems naudotojams;

P3 Nereikalauja papildomų daiktų (angl. *Nothing-to-Carry*) - naudotojui nereikia su savimi nešiotis jokių fizinių daiktų, kurie būtų reikalingi autentifikacijai;

P4 Nereikia didelių pastangų įvedimui (angl. *Physically-Effortless*) - naudotojui neturi reikėti atlikti daug ar sudėtingų veiksmų, nes tai trukdo pasiekti norimus tikslius per toleruotiną laiką;

P5 Lengvai išmokstamas (angl. *Easy-to-Learn*) - autentifikacijos metodas turi būti lengvai ir greitai išmokstamas, nes tai užtrikrina naudotojų norą mokytis jiems nežinomą autentifikacijos;

P6 Efektyvus naudojimas (angl. *Efficient-to-Use*) - autentifikacijos metodas turi leisti naudotojui autentifikuotis per priimtinai trumpą laiką. Naujo slaptažodžio ar rakto susikūrimas gali būti ilgesnis už autentifikacijos laiką, bet proto ribose;

P7 Retos klaidos (angl. *Infrequent-Errors*) - teisingas naudotojas turi sugebėti dažniausiai autentifikuotis be didelių problemų. Tai reiškia, kad autentifikacijos metodas turi būti patikimas ir ne per daug sudėtingas;

P8 Lengvai atstatomas po praradimo (angl. *Easy-Recovery-from-Loss*) - naujo slaptažodžio sukūrimas ir pamiršto slaptažodžio atstatymas turi būti aiškus, paprastas ir greitas.

Saugumo kriterijai:

S1 Apsaugo nuo gyvo nužiūrėjimo (angl. *Resilient-to-Physical-Observation*) - fiziškai šalia esantis puolėjas matydamas autentifikaciją negali sugebėti jos atkartoti, net jei ją mato kelis kartus. Šis kriterijus yra ypač aktualus išmaniesiems telefonams, nes jie dažnai naudojami viešose erdvėse, kur yra didelė tikimybė, kad autentifikacija bus pamatyta;

S2 Apsaugo nuo tikslinio apsimetinėjimo (angl. *Resilient-to-Targeted-Impersonation*) - puolėjas, kuris gerai pažįsta naudotoją negali sugebėti juo apsimesti autentifikacijos metu;

S3 Apsaugo nuo limituoto spėliojimo (angl. *Resilient-to-Throttled-Guessing*) - autentifikacijos metodas negali būti greitai atspėtas naudojant automatizuotas spėliojimo priemones. Spėliojimų kiekį gali varžyti autentifikacijos metodo duodamas spėjimų kiekis;

S4 Apsaugo nuo nelimituoto spėliojimo (angl. *Resilient-to-Unthrottled-Guessing*) - autentifikacijos metodas turi apsaugoti nuo automatizuoto nelimituoto spėliojimo. Metodas laikomas dalinai tenkinantis šią salygą, jei jis yra sunkiau atspėjamas nei tipinis PIN kodas, nes tada sunku didinti spėliojimo mastą ir spėliojimas tampa mažai efektyvus;

S5 Apsaugo nuo vidinio nužiūrėjimo (angl. *Resilient-to-Internal-Observation*) - tuo atveju, jei autentifikacijos įrenginyje yra virusas, ar ryšys yra stebimas, autentifikacijos metodas turi būti apsaugotas nuo kopijavimo;

S6 Apsaugo nuo informacijos nutekėjimo iš kitų sistemų (angl. *Resilient-to-Leaks-from-Other-Verifiers*) - jei viena autentifikacijos metodą naudojanti sistema yra sukompromituota, tai neturi duoti puolėjams pranašumo kitose sistemose;

S7 Apsaugo nuo fišingo (angl. *Resilient-to-Phishing*) - puolėjas neturi galėti gauti autentifikacijai skirtų duomenų apsimesdamas tikra autentifikacijos sistema;

S8 Apsaugo nuo vagysčių (angl. *Resilient-to-Theft*) - jei autentifikacijai naudojamas fizinis daiktas, jo turėjimas puolėjui neturi garantuoti autentifikacijos;

S9 Nepriklausomas nuo papildomų asmenų (angl. *No-Trusted-Third-Party*) - autentifikacijos metodas neturi priklausyti nuo papildomų sistemų, kurių sukompromitavimas padarytų autentifikaciją nepatikima, ir pažeistų naudotojo saugumą ir/arba privatumą;

S10 Reikalauja aiškaus sutikimo (angl. *Requiring-Explicit-Consent*) - autentifikacija negali būti pradedama be naudotojo sutikimo (pavyzdžiui, jei naudotojas turi autentifikacijai skirtą kortelę, jam nežinant nuo jos neturi būti galima nuskaityti duomenų imituojant autentifikaciją);

S11 Nesusiejamas (angl. *Unlinkable*) - jei kelios autentifikacijos sistemos dalinasi duomenimis, metodas neturi joms duoti galimybės žinoti, ar jose autentifikuojasi tas pats naudotojas.

1.3. Šiuo metu naudojami populiariausi autentifikacijos metodai

Išmanieji telefonai turi tris dažniausiai naudojamus autentifiacijos metodus: tekstinį slaptažodį, PIN kodą ir šabloną. Nors šie metodai jau yra reliatyviai gerai ištirti, ir jų privalumai bei trūkumai jau yra aiškiai nusakyti, šiame darbe, kaip ir kiti metodai, jie buvo išanalizuoti naudojant tuos pačius panaudojamumo ir saugumo kriterijus.

1.3.1. Tekstiniai slaptažodžiai

1 pav. Tekstinio slaptažodžio autentifikacijos įgyvendinimas Android 10 operacinėje sistemoje

Tai geriausiai žinomas ir labiausiai naudojamas autentifikavimo metodas. Dažniausiai naudojamas kompiuteriuose ir kituose įrenginiuose, kurie turi fizines klaviatūras, dėl patogaus ir greito įvedimo. Išmaniuose telefonuose ir įrenginiuose su liečiamais ekranais šis metodas irgi naudojamas, bet rečiau. Taip yra todėl, nes sudėtinga įgyvendinti lengvai naudojamą ir pilną klaviatūrą ant liečiamo ekrano. Šio autentifikacijos metodo įgyvendinimas pavaizduotas 1 paveikslėlyje. Dažniausiai kyla problemos, kai bandoma sutalpinti visus klavišus į nedidelį ekraną ir tai priverčia klavišus būti ypač mažus ir todėl sunkiai naudojamus. Yra metodai kaip gestūrinis rašymas, kur pirštu braukoma per klaviatūrą ir atleidžiama tik tada, kai pirštu paliečiamos visos žodžio raidės, bet toks rašymas nėra populiarus. Be to šis metodas labai pasikliauja žodyno pagalba, kad galėtų atspėti norimą žodį ir tai kelia problemas, nes ne visos kalbos palaikomos, o ir slaptažodžiai nėra paprasti žodžiai.

Panaudojamumas

P1 Dalinai lengvai atsimenamas. Kuo griežtesni slaptažodžio reikalavimai, tuo sunkiau jį atsiminti;

P2 Naudotojų kiekis šiam autentifikacijos metodui įtakos neturi;

P3 Šis metodas nereikalauja papildomų fizinių daiktų;

P4 Tekstinio slaptažodžio įvedimas liečiamu išmaniojo telefono ekranu yra nepatogus. Kad ekrane tilptų pilna klaviatūra, jos klavišų dydis privalo būti labai mažas. Tai stipriai apsunkina įvedimą;

P5 Lengvai išmokstamas. Daugeliui žmonių jau gerai žinomas;

P6 Neefektyvus naudojimas. Maži klavišai apsunkina įvedimą. Kai kuriems specialiems simboliams reikia iki trijų paspaudimų, kad jie būtų įvesti. Įvedimas dažniausiai užtrunka virš 20 sekundžių [16];

P7 Klaidos dalinai retos [16]. Jei slaptažodis slepiamas žvaigždutėmis, padarytos klaidos negali būti pastebėtos ir slaptažodį reikia rašyti iš naujo;

P8 Lengvai atstatomas po praradimo, nes teužtenka susikurti naują tekstinį slaptažodį;

1 lentelė. Tekstinių slaptažodžių variacijų kiekis. Skaičiavimams buvo naudota anglų kalbos abėcėlė, kuri turi 26 raides

Simbolių kiekis	Tik mažosios raidės	Mažosios ir didžiosios raidės
4	456976	7311616
5	11881376	380204032
6	308915776	19770609664
7	8031810176	1028071702528
8	208827064576	53459728531456
9	5429503678976	2779905883635712
10	141167095653376	144555105949057024

Saugumas

S1 Dalinai apsaugo nuo gyvo nužiūrėjimo. Papildomas funkcionalumas kaip paspaustos raidės parodymas padidinant paspaustą klavišą bei paskutinio įvesto slaptažoždio simbolio parodymas laukelyje palengvina nužiūrėjimą. Pirštų riebalų žymės ant ekrano taip pat gali padėti atspėti slaptažodį. Maždaug kas penktas slaptažodžio įvedimas buvo sėkmingai nužiūrėtas [16];

S2 Dalinai apsaugo nuo tikslinio apsimetinėjimo. Jei reikalaujama specialiųjų simbolių, tikslinis apsimetinėjimas tampa daug sudėtingesnis;

S3 Apsaugo nuo limituoto spėliojimo;

S4 Dalinai apsaugo nuo nelimituoto spėliojimo. 1 lentelėje parodyti galimi tekstinių slaptažodžių kiekiai atsižvelgiant į slaptažodžio ilgi, bei leistinus simboius. Galimų kombinacijų kiekis yra milžiniškas, ir jis dar didesnis, jei slaptažodyje leidžiami skaitmenys, bei specialieji simboliai. Tačiau didelis kiekis kombinacijų negarantuoja apsaugos nuo tekstinio slaptažodžio atspėjimo. Yra dažnai naudojamų slaptažodžių sąrašai, kurie stipriai padidina atspėjimo tikimybę. Ši problema ypač didelė, jei nėra griežtų slaptažodžio reikalavimų. Be to, nors kombinacijų kiekis ir yra didelis, dauguma tekstinių slaptažodžių tėra atsitiktinis tekstinių simbolių kratinys, kurį naudotojui būtų sunku atsiminti, todėl didžioji dalis tekstinių slaptažodžių nėra praktiški;

S5 Neapsaugo nuo vidinio nužiūrėjimo, nes matomi spaudžiami mygtukai;

S6 Apsaugo nuo informacijos nutekėjimo iš kitų sistemų. Tekstiniai slaptažodžiai yra užkoduojami juos saugant sistemoje;

S7 Neapsaugo nuo fišingo, nes tekstinį slaptažodį tarpininkui lengva nuskaityti;

S8 Apsaugo nuo vagysčių, nes tekstiniam slaptažodžiui nereikia jokių papildomų daiktų, o į tekstiniu slaptažodžiu apsaugotą telefoną be autorizacijos sunku patekti;

S9 Nepriklausomas nuo papildomų asmenų, nes tekstiniių slaptažodžių sistemos yra paprastos ir joms nereikia papildomų asmenų;

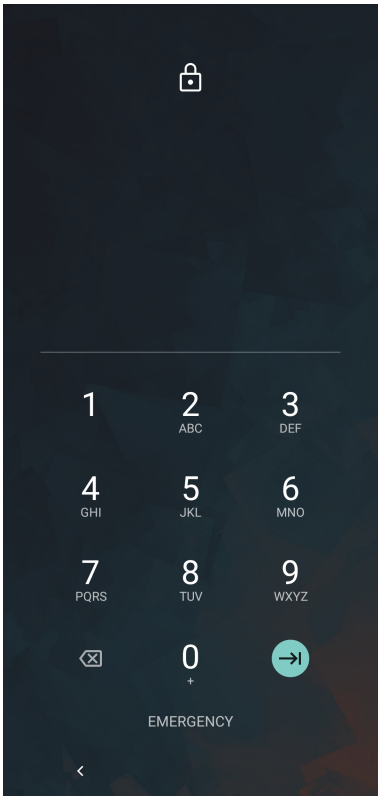
S10 Reikalauja aiškaus sutikimo, nes neįmanoma netyčia autentifikuotis tekstiniu slaptažodžiu;

S11 Nesusiejamas, nes negalima pasakyti ar tas pats žmogus naudoja du duotus tekstinius slaptažodžius;

1.3.2. PIN

PIN kodai yra gerai žinomas autentifikacijos metodas. Šio metodo įgyvendinamas Android išmaniuosiuose telefonuose pavaizduotas 2 paveikslėlyje. Dažniausiai PIN kodą sudaro keturi skaitmenys, bet Azijos šalyse populiarėja šešių skaitmenų PIN kodai. Iš pirmo žvilgsnio jie gali pasirodyti saugūs, nes yra 10 tūkst. keturių skaitmenų išdėstymo kompinacijų. Šešiaženklių skaitemnų PIN kodai atrodo dar saugesni turėdami 1 milijoną skirtingų kombinacijų. Tai suteikia įspūdį, kad kodo atspėjimo tikimybė atitinkamai yra viena iš tūkstančio ir viena iš milijono. Deja naudojai turi tendenciją susikurti lengvai atspėjamas kombinacijas. 10 dažniausiai naudojamų PIN kodų sudaro 14% procentų visų naudotojų sugalvotų keturženklių PIN kodų, o kinų sugalvoti PIN

kodai yra dar lengviau atspėjami: 10 dažniausiai naudojamų PIN kodų sudaro 25% visų naudojamų PIN kodų.



2 pav. PIN autentifikacijos įgyvendinimas Android 10 operacinėje sistemoje

Panaudojamumas

P1 Dalinai lengvai atsimenamas. Žmonėms dažnai reikia atsiminti kelis skirtingus PIN kodus, todėl jie gali maišytis. Keturiems skaitmenims sunku duoti asociacijas, ypač jei skaičiai yra automatiškai sugeneruoti. Jei PIN nėra dažnai naudojami, jie pamirštami;

P2 Naudotojų kiekis šiam autentifikacijos metodui įtakos neturi;

P3 Šis metodas nereikalauja papildomų fizinių daiktų;

P4 Labai lengvas įvedimas. Tereikia 4-5 paspaudimų. PIN kodo mygtukai dažniausiai yra dideli ir visada toje pačioje ekrano dalyje, todėl nereiia nieko naujo ieškoti prieš kiekvieną autentifikaciją;

P5 Lengvai išmokstamas. Dauguma žmonių su šiuo metodu jau gerai pažįstami;

P6 Efektyvus naudojimas. PIN kodą galima įvesti greitai ir lengvai;

P7 Retos klaidos, nes mygtukai dideli, ir visada tose pačiose vietose. Net jei klaida ir įvyksta, tai nekelia didelių problemų;

P8 Lengvai atstatomas po praradimo, tereikia susikurti naują PIN kodą;

2 lentelė. PIN variacijų kiekis.

PIN skaitmenų kiekis	PIN variacijų kiekis
4	10000
6	1000000

Saugumas

S1 Neapsaugo nuo gyvo nužiūrėjimo. Android 10 operacinėje sistemoje paspaustas skaičius netgi nušvinta taip labai palengvindamas nužiūrėjimą puolėjui;

S2 Dalinai apsaugo nuo tikslinio apsimetinėjimo. Jei naudotojai gali patys rinktis norimą PIN kodą, jie turi tendenciją rinktis atspėjamas kombinacijas [21];

S3 Dalinai apsaugo nuo limituoto spėliojimo. Galimų kombinacijų kiekis parodytas 2 lentelėje. Jei naudotojai patys susikūrė PIN kodą, didelė tikimybė, kad jis gali būti atspėtas [21]. Jei PIN buvo sugeneruotas sistemos, reikės daug spėjimų, kad jis būtų atspėtas;

S4 Dalinai apsaugo nuo nelimituoto spėliojimo. Vieną PIN kodą automatizacijos pagalba galima gan greitai rasti, bet jei reikia rasti daug PIN kodų, spėliojimas yra neefektyvus;

S5 Neapsaugo nuo vidinio nužiūrėjimo, nes PIN kodo įvedimas yra aiškiai rodomas ekrane;

S6 Apsaugo nuo informacijos nutekėjimo iš kitų sistemų, nes PIN kodai gali būti saugomi užkoduoti;

S7 Neapsaugo nuo fišingo, nes PIN kodą lengva nuskaityti tarpiniam asmeniui;

S8 Apsaugo nuo vagysčių, nes PIN kodas nereikalauja papildomų daiktų, o turint PIN kodu apsaugotą telefoną, sunku į jį patekti, nežinant teisingo PIN kodo;

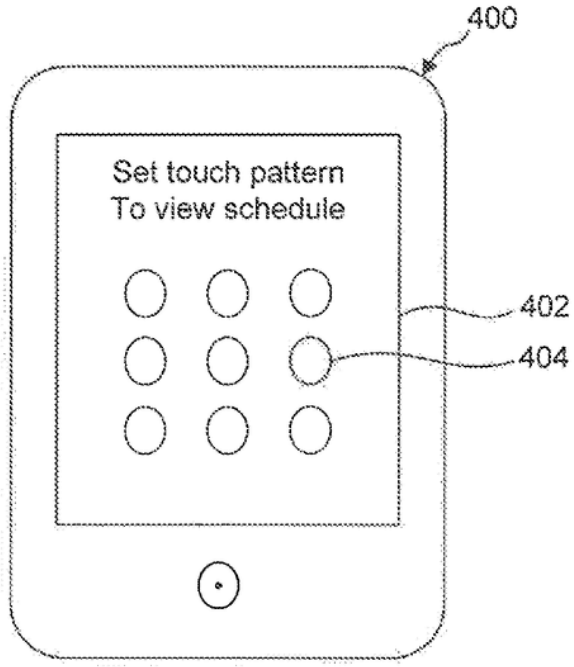
S9 Nepriklausomas nuo papildomų asmenų. Metodo įgyvendinimas yra paprastas ir nereikalauja papildomų asmenų;

S10 Reikalauja aiškaus sutikimo. Negalima to nenorint netyčia autentifikuotis su PIN kodu;

S11 Nesusiejamas. Neįmanoma pasakyti ar du PIN kodai priklauso tam pačiam žmogui;

1.3.3. Šablonai

Šablono autentifikavimo metodas buvo pirmą kartą įgyvendintas Android išmaniuosiuose telefonuose. Google kompanija šį metodą užpatentavo 2010-aisiais metais patente „Tiesioginiai, gestais pagrįsti veiksmai iš įrenginio užrakinimo ekrano“ (angl. „Direct, gesture-based actions from device's lock screen“) ir jo išradėjais paskyrė James B. Miller ir Jean-Michel Trivi [10]. Patente kalbama apie tai, kaip naudotojas gali naudoti kelis skirtingus šablonus, kurie ne tik atrakintų įrenginį, bet ir paleistų kokią nors programą ar atliktų kitą papildomą veiksmą. Be to autoriai siūlo įgyvendinimą, kur šablonas gali būti piešiamas bet kuriuoje ekrano dalyje, o atskaitos taškui naudoti pirmo prisilietimo su ekranu tašką. Šios papildomos funkcijos nėra dažnai naudojamos ir šiais laikais šablonas brėžiamas ant devynių pažymėtų taškų ir naudojamas tik įrenginio atrakinimui. Implementacijos pavyzdys pavaizduotas 3 pav.



3 pav. Šablonas telefono ekrane [10]

Panaudojamumas

P1 Lengvai atsimenamas, nes tereikia atsiminti vieną paprastą paveikslėlį ir piešimo kryptį;

P2 Naudotojų kiekis šiam autentifikacijos metodui įtakos neturi;

P3 Šis metodas nereikalauja papildomų fizinių daiktų;

P4 Lengvai įvedamas. Autentifikacijai reikia pirštu priliesti ekraną, atlikti kelis pabraukimus ir tada patraukti pirštą nuo ekrano. Nors braukimas per ekraną yra kiek sudėtingesnis veiksmas už spustelėjimą, bet daugumai žmonių šis veiksmas vis tiek yra labai lengvai atliekamas;

P5 Lengvai išmokstamas. Metodas yra intuityvus ir daugeliui žmonių jau gerai pažįstamas;

P6 Efektyvus naudojimas. Paveikslėlį galima greitai ir lengvai įvesti;

P7 Retos klaidos. Net jei klaida ir įvyksta, ją lengva ištaisyti iš naujo autententifikuojantis;

P8 Lengvai atstatomas po praradimo. Tereikia susikurti naują šabloną;

3 lentelė. Šablono kombinacijų kiekis

Šablono ilgis	Šablono kombinacijų kiekis
4	1624
5	7152
6	26016
7	72912
8	140704
9	140704
Viso	389112

Saugumas

S1 Neapsaugo nuo gyvo nužiūrėjimo [2]. Autetitifikacijos šablonas taip pat patikimai gali būti atspėtas nužiūrint ant ekrano esančias pirštų riebalų dėmes paliktas po autentifikacijos [5]. Riebalų žymės nuo ekrano gali būti nuskaitytos net jei telefonas buvo įdėtas į kišenę.;

S2 Apsaugo nuo tikslinio apsimetinėjimo;

S3 Dalinai apsaugo nuo limituoto spėliojimo. Dažniausiai naudotojams leidžiama bandyti autentifikuotis penkis kartus, po kurių pradedamas priverstinis laukimas. Naudotojai turi stiprią tendenciją rinktis labai panašius šablonus, dešimt populiariausių šablonų yra naudojami 30% naudotojų, iš kurių patį populiariausią šabloną naudoja 9% naudotojų [4];

S4 Dalinai apsaugo nuo nelimituoto spėliojimo (angl. Resilient-to-Unthrottled-Guessing). Šablonų galimų kombinacijų kiekį galima matyti 3 lentelėje. Kombinacijų kiekis yra mažesnis, nei gali pasirodyti iš pirmo žvilgsnio, nes braukiant liniją tarp dviejų taškų automatiškai pasirenkami visi taškai ant tos linijos. Kombinacijų kiekis viršija keturių skaitmenų PIN kodą tik tada, jei pasirenkama virš penkių taškų;

S5 Neapsaugo nuo vidinio nužiūrėjimo. Autentifikacijos metu įvedamas šablonas yra aiškiai matomas;

S6 Apsaugo nuo informacijos nutekėjimo iš kitų sistemų. Šablono autentifikacijos metodo sistema yra paprasta ir nepriklauso nuo papildomų sistemų;

S7 Neapsaugo nuo fišingo. Lengva imituoti tikrą šablono įvedimo laukelį ir taip gauti naudotojo šabloną;

S8 Apsaugo nuo vagysčių, nes nereikalauja papildomų daiktų, o šablonu apsaugotas telefonas vagies rankose yra sunkiai įveikiamas;

S9 Nepriklausomas nuo papildomų asmenų. Šio metodo įgyvendinimas yra paprastas ir nereikalauja papildomų asmenų;

S10 Reikalauja aiškaus sutikimo. Su šablonu naudotojas negali netyčia autentifikuotis;

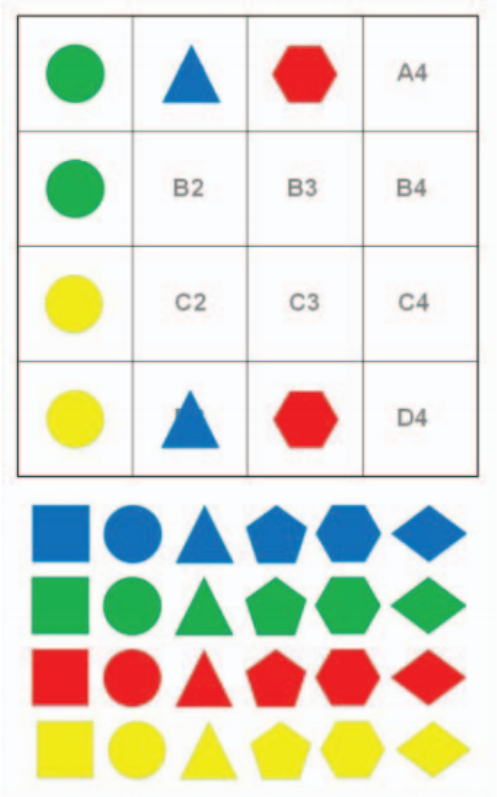
S11 Nesusiejamas. Negalima pasakyti ar du šablonai yra naudojami to pačio asmens;

1.4. Grafiniai autentifikacijos metodai

Grafiniai autentifikacijos metodai yra gerai žinomi dėl dviejų savo bruožų: panaudojamumo ir atsimenamumo [19]. Grafiniai autentifikacijos metodai turi pranašumą prieš kitus metodus dėl žmogaus psichologijos. Žmonės geriau atsimena vaizdus, nei garsus, žodžius ar kitus dalykus, kurie gali būti panaudoti autentifikacijai.

Tačiau grafiniai autentifikacijos metodai turi ir savų trūkumų. Vienas didžiausių yra galimybė autentifikaciją nužiūrėti ir atkartoti puolėjui [11]. Kadangi grafiniai autentifikacijos metodai yra pagrįsti vaizdu, sunku paslėpti įvedamą slaptažodį stipriai neapsunkinant įvedimo tikram naudotojui. Ši problema yra itin aktuali išmaniųjų telefonų autentifikacijai, nes jie dažnai naudojami viešose erdvėse.

1.4.1. Skinerio grafinis slaptažodis



4 pav. Skinnerio grafinio slaptažodžio pavyzdys

G. Skineris atkreipė dėmesį į tai, kad vis daugiau mokymo įstaigų tikisi iš vaikų atsinešti savo įrenginius mokymosi tikslams [17]. Jis taip pat atkreipė dėmesį, kad kuo daugiau slaptažodžių žmonės turi atsiminti, tuo labiau jie linkę slaptažodžius supaprastinti, ar net užsirašyti. Šios problemos sprendimui jis pasitelkė žmonių tendenciją lengviau atsiminti vaizdus, nei žodžius ir sukūrė grafinės autentifikaicjos metodą, kuris pavaizduotas 4 pav. Jame naudotojui reikia atsiminti bent jau aštuonių spalvotų figūrų išsidėstymą 4x4 matricoje.

Panaudojamumas

P1 Dalinai lengvai atsimenamas. Vienas šio metodų prioritetų buvo lengvas atsimenamumas. Jokių tyrimų patikrinti ar tai pasiekti pavyko nebuvo daryta. Pagal reikalavimus naudotojas turi atsiminti aštuonis paveikslėlius ir jų vietas. Reikia atsiminti ne tik formas, bet ir spalvas, nes kiekviena forma gali būti keturių spalvų. Tai gali kelti nepatogumų atsimenant.

P2 Naudotojų kiekis šiam autentifikacijos metodui įtakos neturi;

P3 Šis metodas nereikalauja papildomų fizinių daiktų;

P4 Grafinio slaptažodžio įvedimas yra dalinai lengvas. Šio metodo įvedimo būdas nėra aprašytas, bet galima spėti, kad jis tikriausiai veikia figūros palietimu, nubraukimu iki reikiamo langelio ir paleidimu taip įvedant vieną simbolį. Galima daryti prielaidą, kad autentifikacijai reikia aštuonių braukimų;

P5 Metodas lengvai suprantamas ir išmokstamas. Kadangi metodas neturi raidžių, o susideda tik iš spalvotų figūrų ir yra grafinis, galima spėti, kad jis nėra sunkiai išmokstamas;

P6 Dalinai efektyvus naudojimas. Slaptažodžio kūrimui ir autentifikacijai greičiausiai reikia aštuonių braukimų per ekraną. Kadangi figūros ekrane visada būna tose pačiose vietose, jų ieškojimas neužtrunka;

P7 Mažai klaidų. Šis metodas nebuvo tirtas patikrinti kaip dažnai naudotojai daro klaidas įvedimo metu, bet tai, kad įvedimo metu slaptažodis yra matomas leidžia spręsti, kad klaidos būtų retos;

P8 Slaptažodžio atstatymas nėra sunkus. Tereikia susikurti naują slaptažodį;

Saugumas

S1 Visai neapsaugo nuo nužiūrėjimo, bet sunkų slaptažodį gali būti sunku atsiminti, jei jis matomas tik kartą;

S2 Apsaugo nuo tikslinio atspėjimo. Nėra tyrimų kokius tokio tipo slaptažodžius žmonės yra linkę kurtis, todėl spėliojami jie gali būti tik iš eilės;

S3 Apsaugo nuo limituoto spėliojimo. Šis metodas turi labai daug galimų slaptažodžio kombinacijų;

S4 Apsaugo nuo nelimituoto spėliojimo;

S5 Neapsaugo nuo vidinio nužiūrėjimo. Slaptažodis yra rodomas įvedimo metu;

S6 Apsaugo nuo informacijos nutekėjimo iš kitų sistemų, nes šį slaptažodį galima saugoti užkoduotą;

S7 Neapsaugo nuo fišingo. Puolėjas gali lengvai suimituoti autentifikacijos sistemą ir pavogti slaptažodį;

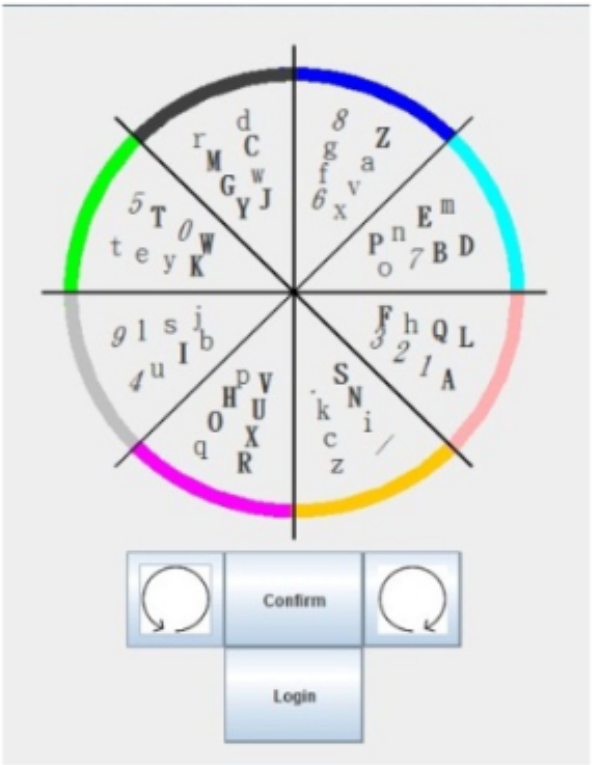
S8 Apsaugo nuo vagysčių, nes šiam metodui nereikia jokių papildomų fizinių daiktų;

S9 Nepriklausomas nuo papildomų asmenų. Šio metodo įgyvendinimas yra paprastas ir nereikalauja papildomų asmenų;

S10 Reikalauja aiškaus sutikimo. Šio metodu negalima netyčia autentifikuotis;

S11 Nesusiejamas. Neįmanoma pasakyti ar du grafinius slaptažodžius susikūrė tas pats žmogus;

1.4.2. Skritulio principu paremtas grafinis slaptažodis



5 pav. Skritulio pagrindu paremto autentifikacijos metodo prisijungimo langas

Atsižvelgiant į tai, kad naudotojai jau yra pažįstami su tekstiniais slaptažodžiais ir remiantis panašiais darbais buvo sukurtas skritulio formos, spalvomis pagrįsto, nuo nužiūrėjimo apsaugančio grafinio slaptažodžio schema [9]. Ši schema ekrane piešiama skritulio pavidalu, kuris suskirstytas į aštuonias lygias dalis. Jos įgyvendinimą galima išvysti 5 paveikslėlyje. Kiekvienoje dalyje įrašyta po aštuonis simbolius (skaitmenis, didžiąsias/mažąsias raides, specialiuosius simbolius). Šį skritulį supa žiedas padalintas į aštuonias lygias dalis, kurios nudažytos skirtingomis spalvomis. Žiedas pasuktas taip, kad virš kiekvienos skirtulio dalies su simboiais būtų vis kitokia spalva. Naudotojui duodami trys mygtukai: skritulį su simboliais pasukantis pagal laikrodžio rodyklę, skritulį su simboliais pasukantis prieš laikrodžio rodyklę, ir įvedimo mygtukas, kuris pasirenka, kad žiedas suorientuotas teisingai ir turėtų būti įvestas simbolis. Naudotojas atsimena vieną spalvą, kuri tampa raktine. Paspaudžiant įvedimo mygtuką, pasirenkama viena skirtulio skirtis. Per petį žiūrintis žmogus nežino naudotojo pasirinktos spalvos, todėl turi sekti visas aštuonias, kas vienam žmogui yra praktiškai neįmanoma. Net jei puolėjas ir sugebėtų sužiūrėti visas aštuonias sritis, tai neduotų jam daug naudos, nes kiekvieną kartą simboliai skirstomi vis kitokiomis aštuoniomis grupėmis.

Panaudojamumas

P1 Atsimenamumas dalinai lengvas. Jis toks pats, kaip tekstinio slaptažodžio, tik papildomai dar reikia atsiminti vieną iš aštuonių spalvų;

P2 Naudotojų kiekis šiam autentifikacijos metodui įtakos neturi;

P3 Nereikalauja papildomų daiktų;

P4 Įvedimas sunkus, nes reikalauja daug paspaudimų. Šiame metode slaptažodžio įvedimui naudojami trys mygtukai. Kadangi yra aštuonios sritys, kurias galima pasirinkti vieno simbolio įvedimui vidutiniškai reikia atlikti tris paspaudimus. Jei slaptažodžio ilgis yra 6, tada tokio slaptažodžio įvedimui vidutiniškai reikės atlikti 18 paspaudimų (geriausiu atveju šešis paspaudimus, blogiausiu - 30);

P5 Lengvai išmokstamas;

P6 Naudojimas nėra efektyvus. Net trumpo slaptažodžio įvedimui reikia atlikti daug paspaudimų. Kita problema, kuri prailgina autentifikacijos laiką yra didelis kiekis atvaizduotų simbolių. Tarp visų jų gali būti sunku rasti reikiamą sekantį slaptažodžio simbolį. Autoriai stengėsi šia problemą taisyti skirtingų grupių simbolius atvaizduodami skirtingais šriftais, bet vargu ar šis sprendimas labai padeda situacijai;

P7 Retos klaidos. Jos gali pasitaikyti nebent sumaišant tam tikrus simbolius dėl skirtingų šriftų, pavyzdžiui, „l“ ir „1“. Tokios klaidos su metodo naudojimo patirtimi neturėtų kartotis;

P8 Lengvas pamiršto slaptažodžio atstatymas. Jei šis slaptažodis pamirštamas, jo atstatymas neturėtų skirtis nuo tekstinio slaptažodžio pamiršimo;

4 lentelė. Skritulio autentifikacijos metodo variacijų kiekis.

Simbolių kiekis	Galimų kombinacijų kiekis
4	4096
5	32768
6	262144
7	2097152
8	16777216

Saugumas

S1 Šis metodas apsaugo nuo gyvo nužiūrėjimo, net jei puolėjas autentifikacijos procesą mato kelis kartus ar naudoja kamerą. Taip yra todėl, nes simboliai nėra išdėstomi tokiomis pačiomis grupėmis kiekvieną kartą, bet yra išmaišomi. Puolėjas gali nebent nužiūrėti įvedamų simbolių kiekį;

S2 Dalinai pažeidžiamas nuo tikslinio apsimetinėjimo. Tikslinis apsimetinėjimas gali įvykti, jei naudotojas susikuria labai paptastą slaptažodį. Spalva gali būti atspėjama, jei naudotojas naudoja sabo mėgstamiausią spalvą, arba ji šiaip atspėjama;

S3 Apsaugo nuo limituoto spėliojimo. Galimų kombinacijų kiekį galima matyti 4-oje lentelėje. Kadangi reikia rinktis vieną skritulio sritį iš aštuonių, tikimybė, kad bus atspėta teisinga sritis, yra viena iš aštuonių. Tokiam spėliojimo tipui trukdo tai, kad simboliai neišdėstomi tokiomis pačiomis grupėmis, todėl aštuonios progos spėti dar nereiškia, kad bus atspėtas vieno simbolio slaptažodis. Kitas būdas spėlioti yra naudojant simbolius, bet tada tikimybė atspėti prilygsta tekstiniam slaptažodžiui, kuris yra sunkiai atspėjamas;

S4 Apsaugo nuo nelimituoto spėliojimo. Jeigu spėliojama naudojant tekstą, tada atspėjimo tikimybė maža. Jei spėliojama naudojant sritis, negalima užtikrinti, kad bus išbandytos visos galimos kombinacijos;

S5 Iš principo apsaugo nuo vidinio nužiūrėjimo, bet galima atrinkti visas galimas tekstinio slaptažodžio kombinacijas iš naudotojo pasirinktų skritulio sričių. Kadangi vienoje srityje yra atvaizduoti aštuoni simboliai, kiekvienas slaptažodžio simbolis galimų slaptažodžių kiekį padidina aštuonis kartus (pavyzdžiui, jei slaptažodį sudaro šeši simboliai, puolėjas žino visas galimas tekstinio slaptažodžio kombinacijas, kurių yra 48).;

S6 Apsaugo nuo informacijos nutekėjimo iš kitų sistemų. Šį slaptažodį galima saugoti užkoduotą;

S7 Dalinai apsaugo nuo fišingo. Puolėjas gali priversti naudotoją autentifikuotis apsimesdamas autentifikacijos sistema, bet tai nereiškia, kad slaptažodis bus pavogtas. Puolėjas tik turės galimų tekstinių slaptažodžių sąrašą, kaip ir S5;

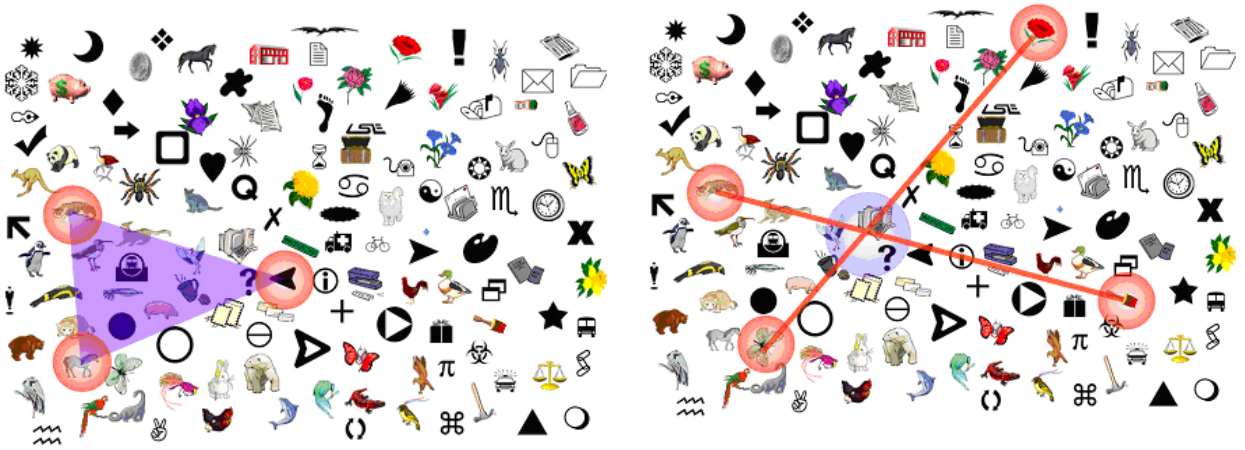
S8 Apsaugo nuo vagysčių, nes šiam metodui nereikia jokių papildomų fizinių daiktų;

S9 Nepriklausomas nuo papildomų asmenų. Šio metodo įgyvendinimas yra paprastas ir nereikalauja papildomų asmenų;

S10 Reikalauja aiškaus sutikimo. Šiuo metodu negalima autentifikuotis netyčia;

S11 Nesusiejamas. Negalima pasakyti ar tas pats žmogus susikūrė du atskirus slaptažodžius;

1.4.3. Dideliu paveikslėlių kiekiu paremta autentifikacija



(a) Raktinis paveikslėlis trikampio plote

(b) Raktinis paveikslėlis susikirtimo taške tarp keturių pasirinktų paveikslėlių

6 pav. Dideliu paveikslėlių kiekiu pagrįsta autentifikacija

Grafiniai slaptažodžiai lengviau atsimenami už tekstinius, bet jie turi didelį trūkumą, kad juos lengva nužiūrėti. Šią problemą galima spręsti vienu metu ekrane atvaizduojant daug paveikslėlių [18]. Šiame darbe autoriai siūlo kelis būdus, kaip galima įvesti grafinį slaptažodį jo neatskleidžiant šalia stovintiems žmonėms. Visi siūlomi metodai prasideda taip pačiai: iš šimtų galimų paveikslėlių naudotojas išsirenka maždaug dešimt, kuriuos naudotojas turi atsimnti. Tada autentifikacijos metu naudotojai ekrane atvaizduojama apie šimtas paveikslėlių, ir kurių keli yra naudotojo pasirinkti registracijos metu. Tada, priklausomai nuo metodo, naudotojas turi pavyzdžiui paspausti ant trikampio, kurio kampus sudaro jo pasirinkti paveikslėliai, kaip parodyta 6a paveikslėlyje. Kiti

variantai yra pastumti eilutį paveikslėlių taip, kad pasirinkti paveikslėliai būtų toje pačioje tiesėje, arba paspausti maždaug toje vietoje, kur susikerta nubrėžtos tiesės tarp keturių atsimintų paveikslėlių, kaip pavaizduota 6b paveikslėlyje. Kad būtų galima sumažinti puolėjo galimybę atspėti slaptažodį, autoriai siūlo šiuos veiksmus pakartoti apie dešimt kartų.

Panaudojamumas

P1 Dalinai lengvas atsimenamumas. Autoriai rekomenduoja naudotojui atsiminti dešimt paveikslėlių iš galimų tūkstančių. Dešimt atsitiktinių paveikslėlių gali būti sunkuko atsiminti, ypač kai toks didelis kiekis kitų galimų paveikslėlių, kurie gali maišytis;

P2 Naudotojų kiekis šiam autentifikacijos metodui įtakos neturi;

P3 Nereikalauja papildomų daiktų;

P4 Sunkus įvedimas. Autoriai duoda kelis galimus variantus kaip slaptažodis gali būti įvedamas ir rekomenduoja naudotojui įvedimą atlikti apie dešimt kartų. Visų pirma dideliame kiekyje paveikslėlių gali būti sunku rasti naudotojui reikiamus paveikslėlius, ypač jei naudojamas mažas ekranas. Kai naudotojas randa jam reikiamus paveikslėlius, jam dar reikia sugebėti ant jų paspausti, kas gali kelti problemų, kai reikiami paveikslėliai yra tokio mažo dydžio. Paskutinis keblumų keliantis dalykas yra neaiškiai nustatyta paklaida, pavyzdžiui, trikampio atveju visas paveikslėlis turi patekti į pasirinkto paveikslėlio plotą ar tik kažkokia jo dalis, kokio dydžio gali būti brėžiamas didžiausias priimtinas trikampis?;

P5 Išmokimui gali kelti problemų anksčiau paminėtos problemos, kaip neaiškios paklaidos. Nepaisant to, šio autentifikacijos metodo principas yra lengvai suprantamas;

P6 Autoriai rekomenduoja autentifikaciją atlikti apie dešimt kartų. Atsižvelgiant į laiką, kuris turėtų būti užtrunkamas ieškant paveikslėlių, autentifikacija šiuo metodu užtrunka ilgai;

P7 Klaidos dalinai retos. Klaidų kiekis priklauso nuo to, koks tikslumas nustatytas metodo įgyvendinimo metu. Atsižvelgiant į tai, kad paveikslėliai gali būti panašūs ir maišytis galima spėti, kad klaidų pasitaiko;

P8 Slaptažodžio atstatymas užtrunka dalinai ilgai. Galima spėti, kad iš tūkstančio galimų paveikslėlių išsirinkti ir atsiminti dešimt paveikslėlių yra laiko reikalaujantis procesas;

Saugumas

S1 Apsaugo nuo gyvo nužiūrėjimo, net jei puolėjas autentifikaciją mato kelis kartus. Dalinai apsaugo ir nuo to, jei autentifikacija yra nufilmuojama;

S2 Apsaugo nuo tikslinio apsimetinėjimo. Neužtenka pažinot žmogaus, kad būtų galima atspėti, kokius paveikslėlius jis pasirinko;

S3 Apsaugo nuo limituoto spėliojimo. Galima spėti, kad maža tikimybė, jog naudotojas atspės teisingus paveikslėlius 10 kartų iš eilės, ko reikalauja autoriai;

S4 Apsaugo nuo nelimituoto spėliojimo. Maža tikimybė atspėti visus 10 paveikslėlių, iš galimų 1000;

S5 Dalinai apsaugo nuo vidinio nužiūrėjimo. Matant ekraną, ne visada aišku, kuris paveikslėlis ekrane buvo pasirinktas;

S6 Apsaugo nuo informacijos nutekėjimo iš kitų sistemų. Raktinius paveislėlius galima saugoti užmaskuotus;

S7 Dalinai apsaugo nuo fišingo. Visai sunku suimituoti šį autentifikacijos metodą, nes puolėjas negali pasakyti, kuriuos paveiklėlius jam reikia parodyti naudotojui. Puolėjas būdamas tarpininku tarp naudotojo ir autentifikacijos sistemos dalinai gali sužinoti kokius raktinius paveikslėlius pasirinko naudotojas;

S8 Apsaugo nuo vagysčių. Šis metodas nepasikliauja jokiais fiziniais daiktais. Vagiui būtų labai sunku patekti į pavogtą šiuo autentifikacijos metodu apsaugotą išmanųjį telefoną;

S9 Nepriklausomas nuo papildomų asmenų. Metodo įgyvendinimas yra paprastas ir nereikalauja papildomų asmenų;

S10 Reikalauja aiškaus sutikimo. Šiuo metodu negalima autentifkuotis netyčia;

S11 Nesusiejamas. Neįmanoma pasakyti ar raktinius paveikslėlius pasirinko tas pats žmogus;

1.5. Metodų tarpusavio palyginimas

Apibendrintas autentifikacijos metodų vertinimas pagal nurodytus panaudojamumo ir saugumo kriterijus pavaizduotas 5 lentelėje. Paryškinti kriterijai yra ypaš aktualūs išmaniesiems telefonams. Autentifikaciją turimą sugebėti įvykdyti greitai ir efektyviai. Tai yra reikalinga todėl, nes naudotojai turi dažnai atlikti išmaniojo telefono autentifikaciją. Kas trečias darbuotojas pažymėjo, kad saugumas jam kėlė problemų [15]. Jei naudotojai taip jaučiasi tai yra didelė problema. Visų pirma, kenčia produktyvumas. Antra, naudotojai pradeda ieškoti būdų, kaip autentifikaciją palengvinti ir jie yra pasiruošę dėl panaudojamumo paaukoti saugumą. Trečia, išmaniųjų telefonų atveju, jie gali tiesiog atsisakyti sunkiai naudojamo autentifikacijos metodo. Kitas išmaniųjų telefonų autentifikacijai itin svarus kriterijus yra apsauga nuo nužiūrimumo per petį. Išmanieji telefonai dažnai naudojami viešose erdvėse, kur didelė tikimybė autentifikacijai būti pamatytai. Puolėjui neturi užtekti pažiūrėti, kaip autentifikuojasi naudotojas, kad autentifikaciją jis galėtų suimituoti.

Stebint 5 lentelę, galima pamatyti, kad kai kurie metodai rinkosi prioritizuoti panaudojamumą, o kiti - saugumą. Jei kuriamas naujas autentifikacijos metodas, jis turi panaudojamumu bent jau varžytis su tekstiniu slaptažodžiu ar PIN kodu, antraip naudotojai nesirinks naujo ir nepatogaus metodo, o rinksis patogius, jau gerai žinomus metodus.

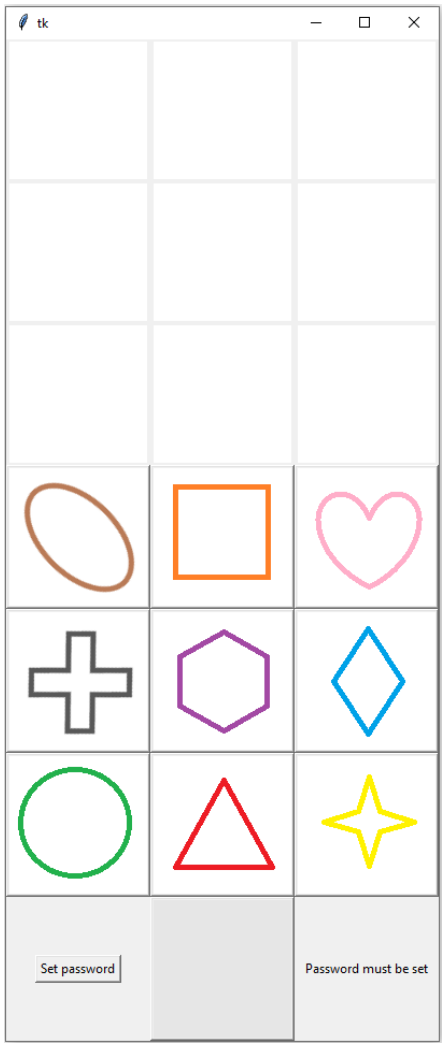
5 lentelė. Esamų autentifikacijos metodų tarpusavio palyginimas.
Žalia spalva pažymėti pilnai tenkinami kriterijai, geltona - dalinai tenkinami, raudona - netenkinami kriterijai.
Paryškinti kriterijai yra itin aktualūs išmaniesiems telefonams.

	Tekstinis slaptažodis	PIN kodas	Šablonas	Skinerio slaptažodis	Skirtulinis slaptažodis	Metodas su daug paveikslėlių
P1 Lengvai atsimenamas						
P2 Keičiamo dydžio naudotojams						
P3 Nereikalauja papildomų daiktų						
P4 Nereikia didelių pastangų įvedimui						
P5 Lengvai išmokstamas						
P6 Efektyvus naudojimas						
P7 Retos klaidos						
P8 Lengvai atstatomas po praradimo						
S1 Apsaugo nuo gyvo nužiūrėjimo						
S2 Apsaugo nuo tikslinio apsimetinėjimo						
S3 Apsaugo nuo limituoto spėliojimo						
S4 Apsaugo nuo nelimituoto spėliojimo						
S5 Apsaugo nuo vidinio nužiūrėjimo						
S6 Apsaugo nuo informacijos nutekėjimo iš kitų sistemų						
S7 Apsaugo nuo fišingo						
S8 Apsaugo nuo vagysčių						
S9 Nepriklausomas nuo papildomų asmenų						
S10 Reikalauja aiškaus sutikimo						
S11 Nesusiejamas						

2. Autentifikacijos metodo kūrimas

Šiame skyriuje aptariama pirmoji kuriamo grafinio autentifikacijos metodo iteracija. Ji įvertinta naudojant pirmame skyriuje iškeltus kriterijus. Tada aptariami pirmosios iteracijos trūkumai. Skyriuje toliau pasakojama apie antros grafinio autentifikacijos metodo iteracijos kūrimą, kodėl buvo atlikti tam tikri pakeitimai.

2.1. Pirmoji autentifikacijos metodo iteracija



7 pav. Originalaus grafinio autentifikacijos metodo prototipas

Pirmoji grafinio autentifikacijos metodo iteracija yra pavaizduota 7 paveikslėlyje. Šio metodo veikimas yra labai paprastas: kiekvienas iš devynių apačioje esančių paveikslėlių yra paspaudžiamas po kartą, ir tada spaudžamas mygtukas slaptažodžiui įvesti. Autentifikacijai reikia dešimties paspaudimų. Po kiekvieno paspaudimo, paspaustas paveiksėlis atsirasdavo atitinkame langelyje viršuje. Atsiradimo tvarka yra iš kairės į dešinę, iš viršaus į apačią. Dėl viršutinių devynių langelių įvedamas grafinis slaptažodis yra matomas realiu laiku. Viršutiniai devyni langeliai skirti naudoti tik tol, kol naudotojas pratinasi prie šio autentifikacijos metodo. Kai naudotojas jau turi patirties su šiuo autentifikacijos metodo, viršutiniai devyni langeliai turi būti panaikinti, kad aplinkiniai naudotojai nematytų vedamo grafinio slaptažodžio.

Nors naudotojas ir turi įvesti visus devynis paveislėlius, jam nereikia atsiminti visų devynių pozicijų. Devyni paveikslėliai naudojami tam, kad suklaidintų puolėjus, kurie gali stebėti autentifikaciją gyvai. Naudotojui reikia atsiminti bent jau keturis paveikslėlius ir jų pozicijas 3x3 matricoje.

2.1.1. Pirmosios metodo iteracijos vertinimas pagal kriterijus

Panaudojamumas

P1 Lengvai atsimenamas. Grafiniai metodai yra lengvai atsimenami, nes jie nepriklauso nuo kalbos. Be to žmonės yra gerai prisitaikę matyti ir suprasti vaizdus (iš visų penkių juslių, rega ir vaizdų suvokimas užima didžiausią smegenų sritį);

P2 Metodas nuo naudotojų kiekio nepriklauo;

P3 Nereikalauja papildomų daiktų. Šiam metodui nereikia jokių papildomų daiktų, kad būtų galima autentifikuotis;

P4 Šio metodo įvedimas yra dalinai lengvas. Reikia dešimties paspaudimų ant didelių mygtukų;

P5 Lengvai išmokstamas. Šis metodas yra intuityvus ir jam nereikia mokytis jokio sudėtingo veikimo;

P6 Efektyvus naudojimas. Šiuo metodu galima greitai autentifikuotis, nes nereikia daug sudėtingų veiksmų;

P7 Retos klaidos. Mygtukai dideli ir juos lengva paspausti;

P8 Lengvai atstatomas po praradimo. Tereikia susikurti naują grafinį slaptažodį;

Saugumas

S1 Neapsaugo nuo gyvo nužiūrėjimo. Slaptažodis aiškiai rodomas įvedimo metu. Vargu ar užtektų slaptažodį pamatyti kartą, kad jis būtų atsimintas, bet kelių kartų gali užtekti;

S2 Apsaugo nuo tikslinio apsimetinėjimo. Jai puolėjas pažįsta naudotoją, tai jam neduoda jokių žinių apie naudotojo pasirinktą grafinį slaptažodį;

S3 Apsaugo nuo limituoto spėliojimo. Naudotojui draudžiama spėlioti kiek jis nori kartų. Maža tikimybė, kad slaptažodis bus atspėtas iš pirmų kelių kartų;

S4 Dalinai apsaugo nuo nelimituoto spėliojimo. Pilnai neapsaugo, tačiau iš saugumo pusės šis metodas panašus į PIN kodą ir skeuoti mases naudotojų neatneštų daug naudos;

S5 Neapsaugo nuo vidinio nužiūrėjimo. Slaptažodis rodomas įvedimo metu;

S6 Apsaugo nuo informacijos nutekėjimo iš kitų sistemų. Šį grafinį slaptažodį galima saugoti užkoduotą;

S7 Neapsaugo nuo fišingo. Puolėjui būtų lengva suimituoti autentifikacijos sistemą. Jei puolėjas yra įsiterpęs tarp naudotojo ir autentifikacijos sistemos, jam labai legva nužiūrėti slaptažodį;

S8 Apsaugo nuo vagysčių. Šis metodas nepriklauso nuo fizinių daiktų. Jei vagis turi šiuo metodu apsaugotą išmanųjį telefoną, jam būtų labai sunku į telefoną patekti;

S9 Nepriklausomas nuo papildomų asmenų. Šio grafinio autentifikacijos metodo įgyvendinimas yra paprastas ir jam nereikia jokių papildomų asmenų;

S10 Reikalauja aiškaus sutikimo. Šiuo autentifikacijos metodu negalima autentifikuotis netyčia;

S11 Nesusiejamas. Neįmanoma pasakyti ar du grafiniai slaptažodžai priklauso tam pačiam žmogui;

2.1.2. Pirmosios grafinio autentifikacijos metodo iteracijos trūkumai

Mokomoji metodo versija, kuri vedamą grafinį slaptažodį atvaizduoja viršutiniuose devyniuose langeliuose visiškai neapsaugo nuo slaptažodžio nužiūrėjimo. Vargu ar ta versija naudotojams padeda suprasti šį autentifikacijos metodą. Jeigu naudotojas nesivargina šios versijos pasikeisti į standartinę, tai kelia didelių saugumo problemų. Geriau naudotojui net neduoti galimybės padaryti tokios klaidos.

Naudotojas turi susigalvoti grafinį slaptažodį naudodamas tik devynius paveikslėlius. Tai yra sudėtinga, nes iš tokio mažo paveikslėlių kiekio naudotojui gali būti sunku sugalvoti tokias asociacijas galvoje, kurios padėtų atsiminti slaptažodį. Be to, naudotojui gali kilti problemų skiriant spalvas tarp devynių duotų figūrų, ar kilt kitų nesklandumų. Naudotojui reikia suteikti laisvę duodant rinktis iš daugiau paveikslėlių.

Autentifikacijos metu, paspaudus devynis paveikslėlius tada dar reikia paspausti mygtuką, kuriuo patvirtinama, kad slaptažodis buvo suvestas. Tai yra nereikalingas veiksmas, nes ir taip aišku, kad kai visi paveikslėliai paspausti, grafinis slaptažodis jau suvestas. Vienas sutaupytas paspaudimas pagerina autentifikacijos metodo panaudojamumą, nes metodo panaudojamumas tampa kiek paprastesnis.

2.2. Antroji grafinio autentifikacijos metodo iteracija

Atsižvlegiant į pirmosios grafinio autentifikacijos metodo iteracijos trūkumas buvo sukurta antroji iteracija. Ji pritaikyta išmaniesiems telefonams ir ja stengiamasi išspręsti pirmojoje iteracijose kilusias problemas.

2.2.1. Metode naudojamų paveikslėlių kūrimas

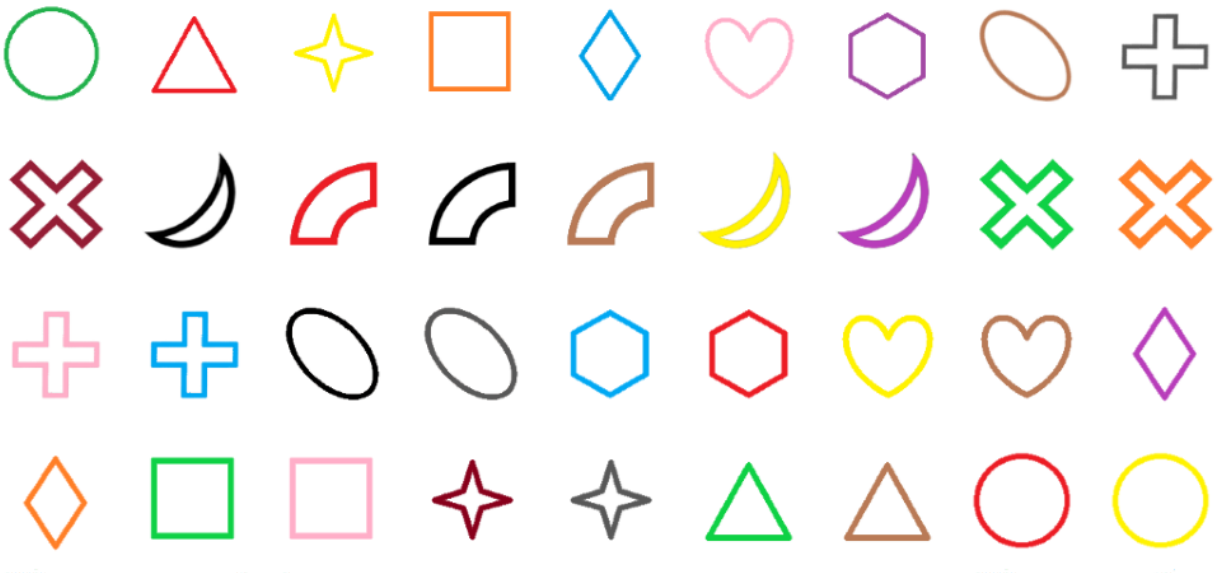
Atpažinimas ir atsiminimas

Atpažinimas yra pranašesnis už atsiminimą [13]. Priminimai žmonėms labai padeda. Todėl kartais kuriant slaptažodį naudotojams ir yra siūloma susikurti slaptažodžio priminimą. Užtenka trumpo komentaro, kad būtų atsimintas net ir sudėtingas slaptažodis.

Viena iš priežasčių, kodėl antros iteracijos registracijos metu naudotojui siūloma rinktis iš didelio kiekio paveikslėlių jam patinkančius devynis, kurie bus naudojami autentifikacjia yra noras išnaudoti žmogaus savybę atpažinti jau jam pažįstamus dalykus. Naudotojas gali pamiršti savo susigalvotą slaptažodį, bet pamatęs siūlomus, jam galimus paveikslėlius, jis gauna priminimą, kurio gali užtekti, kad būtų atsimintas slaptažodis.

Daug paveikslėlių taip pat skatina naudotojui nenaudoti tokio pačio slaptažodžio, nes kiekvieno slaptažodžio įvedimo metu yra priminimas apie tai, koks yra naudotojo grafinis slaptažodis. Be to, skirtingi paveikslėliai užtrikrina, kad naudotojas nemaišys kelių slaptažodžių ir iš kart žinos kurį grafinį slaptažodį jam reikia suvesti.

Formos



8 pav. Metode naudotų paveikslėlių rinkinys

Metodo kūrimui buvo pasirinktos abstrakčios, lengvai atpažįstamos formos. Jeigu formos sudėtingesnės, jas tampa sunkiau greitai atpažinti. Kadangi vienas iš panaudojamumo kriterijų yra autenifikacijos greitis, lengvai atpažįstamas figūras naudojantis grafinis slaptažodis turėtų būti greičiau įvedamas už sudėtingas formas naudojantų metodą.

Paprastos formos taip pat turi didelį pranašumą mažuose ekranuose, pavyzdžiui, tokiuose, kokius naudoja išmanieji telefonai. Sutraukus sudėtingus paveikslėlius į mažus dydžius, juos tampa labai sunku atskirti. Ši problema kyla ir toliaregiams žmonėms, kurie nori autentifkuotis be akinių. Paprastos figūros šios problemos neturi, nes jose nėra jokių detalių, kurios pranyksta sutraukiant paveikslėlio dydį.

Pasirinktos formos yra tuščiavidurės, kad būtų aiškiau matomas formos siluetas. Jei forma būtų pilnavidurė, ji tiesiog atrodytų kaip spalvota dėmė. Ši problema būtų ypač akivaizdi, jei sutraukiamas formų dydis.

Šiam metodui buvo pasirinkta dvyllika paprastų formų. Šios formos pavaizduotos 8 paveikslėlyje. Kiekviena forma kartojasi po tris kartus, vis kitomis spalvomis, kad naudotojas turėtų didesnį pasirinkimą.

Spalvos

Nėra specifinių spalvų, kurios būtų tinkamiausios visiems žmonėms. Kiekvienas žmogus turi savų mėgstamų ir nemėgstamų spalvų. Dėl šios priežasties naudotojams būtinai turi būti suteikiamas pasirinkimas.

Svarbiausias dalykas, kuris žmonėms padeda skirti spalvas, yra kontrastas [8]. Kontrastas yra ypač reikalingas, kai bandoma autentifikuotis saulėtą dieną ir todėl telefono ekranas gali būti sunkiai matomas. Dėl šios priežasties paveikslėlių fonas buvo pasirinktas baltas, o spalvos - tamsios.

Paveikslėlių kūrimui buvo pasirinkta 11 tamsių spalvų, taip užtikrinant naudotojo pasirinkimo laisvę.

Nebuvo sukurta po paveikslėlį kiekvienai galimai formos ir spalvos kombinacijai. Jei tai būtų buvę padaryta, tada naudotojas turėtų rinktis iš 132 skirtingų paveikslėlių. Per didelis paveikslėlių pasirinkimas keltų problemų, nes tarp jų visų užtruktų rasti naudotojui reikiamus paveikslėlius registracijos metu. Be to, naudotojai galimai pradėtų daryti lengvai pamirštamus slaptažodžius, kurie susideda, pavyzdžiui, iš tos pačios spalvos. Tokius slaptažodžius taip pat būtų lengviau atspėti puolėjui. Sukurti paveikslėliai parodyti 8 paveikslėlyje.

2.2.2. Antrosios iteracijosgrafinio autentifikacijos metodo veikimas

Antrosios grafinio autentifikacijos metodo ieracijos veikimas yra labai panašus į pirmosios iteracijos. Tačiau yra ir atskirti pranašumai, kurie antrą iteraciją daro geresne. Pirmasis pranašumas yra naudotojui siūlomas didesnis paveikslėlių kiekis, kuriuos naudojant sukuriamas gafinis slaptažodis. Naudotojas registracijos metu užtrunka ilgiau laiko, nes turi įvertinti visus jam siūlomus paveiksėlius, prieš rinkdamasis savo norimus, bet šis trūkumas yra kompensuojamas tuo, kad naudotojui lengviau sugalvoti jam tinkančius slaptažodžius, kai jis turi teisę rinktis.

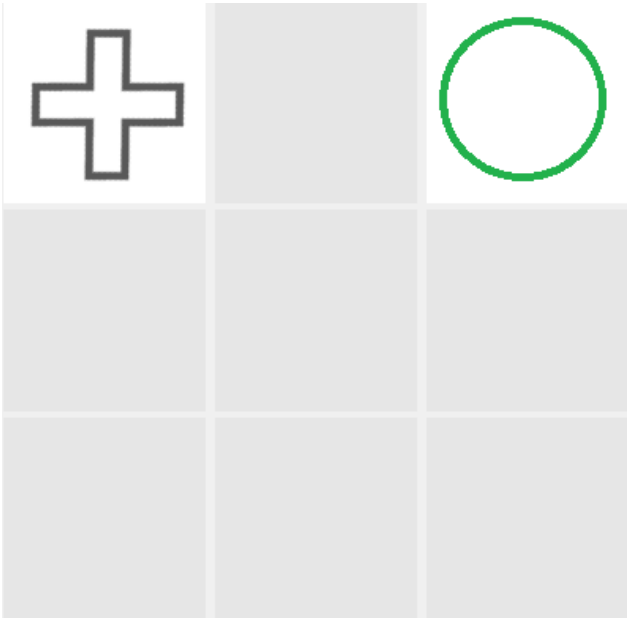
Autentifiacijos metu, anrojoje metodo iteracijoje, kaip ir pirmojoje reikia įvesti kiekvieną iš duodamų devynių paveikslėlių tinkama tvarka. Didžiausias skirtumas tarp iteracijų yra tas, kad metodas buvo supaprastintas neberodant įvestų paveikslėlių. Tai taip pat pagerina is saugumą, nes dėl šios priežasties sunkiau nužiūrėti vedamą slaptažodį. Papildomas privalumas, kad nerodant įvestų paveikslėlių telefono ekrane daugiau vietos, kurią galima išnaudoti darant didesnius paveikslėlių įvedimo mygtukus. Tai yra didelis privalumas išmaniuosiuose telefonuose, nes jie neturi didelių ekranų, todėl kiekvienas ekrane rodomas dalykas turi būti naudingas.

Paskutinis skirtumas, tarp pirmosios ir antrosios autentifikacijos metodo iteracijos yra pašalintas slaptažodžio patvirtinimo mygtukas. Šis mygtukas pirmojoje iteracijoje buvo nereikalingas, nes ir taip akivaizdu, kad slaptažodis yra suvestas, kai paspausti visi galimi mygtukai su paveikslėliais. Pašalinant slaptažodžio patvirtinimo mygtuką buvo atkovota daugiau naudingos ekrano vietos. Antrojoje iteracijoje po paskutinio paspasto mygtuko su paveikslėliu automatiškai patvirtinama, kad naudotojas baigė vesti slaptažodį ir galima pradėti tikrinti, ar jis teisingas.

2.2.3. Grafinio slaptažodžio saugojimas ir tikrinimas

Grafinio autentifikacijos metodo antros iteracijos slaptažodį galima saugoti keturiomis dalimis. Pirma dalis būtų devynių naudotojo pasirinktų paveikslėlių sąrašas. Kai naudotojas pradeda autentifikacijos procesą, jam turėtų būti pateikiami jo pasirinkti devyni paveikslėliai atsitiktine tvarka.

Tada naudotojas pamato jam duodamus paveikslėlius. Prasideda autentifikacijos procesas iš naudotojo pusės. Jis privalo paveikslėlius sudėti tinkama tvarka. Kai jis tą padaro, jam duoti devyni paveikslėliai, jo pasirinkta tvarka persiunčiami autentifikacijai. Šiame žingsnyje galima siųsti ne pačius paveikslėlius, o tik jų ID numerius.



9 pav. Grafinio slaptažodžio pavyzdys

Tada autentifikacijos sistema gauna naudotojo iš eilės sudėtus paveiklėlius. Naudotojas atsiuntė devynis paveikslėlius, net jei jis slaptažodyje jų naudoja mažiau. Dabar kyla uždavinys pašalinti nereikalingus paveikslėlius. Tą galima padaryti naudojant kitą naudotojo slaptažodžio dalį. Ją galima pavadinti „kauke“. Ką ji daro, tai tiesiog pereina per paveikslėlių ID numerius, ir nereikalingose vietose esančių paveikslėlių ID pakeičia į nulį. Taip sekančiame autentifikacijos žingsnyje nesimaišo nereikalingi paveikslėiai. Grafinio slaptažodžio pavyzdys yra duotas 9 paveikslėlyje. Tada tokio paveikslėlio kaukė galėtų būti „101000000“. Tada tuo pačiu metu būtų iteruojama per kaukę ir naudotojo atsiųstą sąrašą. Kiekvienas paveikslėlis, kuris sutaptų su nuliu kaukėje būtų pakeičiamas į nulį.

6 lentelė

Simbolių kiekis	Galimų kombinacijų kiekis
0	QfR5
2	g.4J
4	eD1@

Sekantis žingsnis būtų grafinio slaptažodžio konvertavimas į tekstinį slaptažodį. Tai būtų galima naudojant tam tikrą lentelę, kur kiekvienam paveikslėliui yra priskirta po kelis tekstinius simbolius. Kaip pavyzdį naudokime tą patį grafinį slaptažodį. tarkime ir praėjusio žingsnio gavome tokį apdorotą slaptažodį: „204000000“. Tada konvertavimui užtektų 6 lentelės. Tada į tekstinį formatą apdorotas slaptažodis atrodytų taip: „g.4JQfR5eD1@QfR5QfR5QfR5QfR5QfR5QfR5“.

Tada gautą tekstinį slaptažodį galima užkoduoti naudojant pasirinktą hash algoritmą ir taip jį paslėpti. Nors tokioje autentifikacijos sistemoje ir yra daug žingsnių, jie neturėtų ilgai trukti. Tokioje sistemoje, net jei puolėjas ir gauna visas naudotojo slaptažodžio dalis, jam dar reikės paplūšėti, kad išsiaiškintų naudotojo slaptažodį.

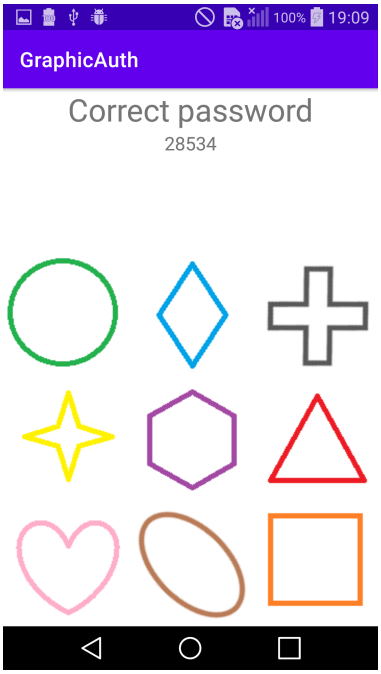
2.3. Prototipo kūrimas

10 pav. Pirmas prototipo langas

Grafinio autentifikacijos metodo prototipas buvo sukurtas Android operacinę sistemą naudojantiems telefonams, nes šiuo metu tai yra plačiausiai naudojama operacinė sistemą. Prototipo kūrimas kitoms išmaniųjų telefonų operacinėms sistemoms stipriai nesikeistų. Naudota Java programavimo kalba, nes tai yra oficiali Android programėlių kūrimo kalba. Prototipo paskirtis yra patikrinti naudotojų potyrius ir gauti jų atsiliepimus, todėl padaryta tik naudotojus liečianti autentifikacijos dalis.

11 pav. Mygtukų dingimas bevedant slaptažodį

Kai prototipas paleidžiamas, naudotojams parodomas 10 paveikslėlyje parodytas langas. Jame prašoma įvesti slaptažodį ir duodamos devynios figūros. Mygtukai su slaptažodžiais piešiami didžiausi, kiek leidžia telefono ekranas. Taip yra todėl, kad tada galima parodyti didesnius paveikslėlius. Be to, lengviau paspausti didelius mygtukus telefono ekrane. Mygtukų briaunos nėra piešiamos, nes jos tik trukdo matyti paveikslėlius ir nesuteikia jokios papildomos naudos.



12 pav. Įvestas teistingas slaptažodis

Kai naudotojas paspaudžia ant mygtuko su atvaizduotu paveiksėliu, paveikslėlis dingsta, kaip pavaizduota 11 paveikslėlyje. Taip yra daroma dėl dviejų priežasčių. Visų pirma, kad jei yra šalia esančių žmonių, jiem būtų sunkiau pamatyti, kuris paveikslėlis buvo pasirinktas. Antra, kad jau naudotojo pasirinkti paveikslėliai jam nesimaišytų ir jis matytų tik jam vis dar galimus pasirinkti paveikslėlius.

Kai naudotojas paspaudžia paskutinį paveikslėlį jam parodomas 12 paveikslėlyje parodytas langas. Visų pirma šiame lange pasakoma ar naudotojas suvedė teisingą slaptažodį. Tada parašoma kiek milisekundžių naudotojas užtruko suvesti slaptažodžiui. Tikrame įgyvendiname naudotojas būtų autentifikuotas ir praleistas, bet šis prototipas buvo sukurtas tyrimo tikslams, todėl po slaptažodžio suvedimo iš naujo išmaišomi paveikslėliai ir naudotojas galį vėl vesti slaptažodį. Jei naudotojas dar kartą suveda slaptažodį, jis vėl gauna panašų langą, kuriame pasakyta ar slaptažodis teisingas ir duodami iš naujo išmaišyti paveikslėliai. Laikmatis rodo ne tai, kiek naudotojas užtruko įvesdamas antrą slaptažodį, bet laiką, per kurį naudotojas įvedė abu slaptažodžius. Naudotojas tada gali vesti grafinį slaptažodį kiek panorėjęs kartų.

3. Autentifikacijos metodo tyrimas ir vertinimas

Šiame skyriuje aptariami grafinio autentifikacijos metodo tyrimai. Panaudojamumo ir saugumo vertinimui naudojami šiame darbe iškelti kriterijai bei empiriniai tyrimai. Kiekvieno tyrimo vykdymo tvarka yra aprašyta, pateikiami gauti rezultatai ir tada parašomos išvados.

3.1. Tyrimo aplinka

3.1.1. Technologinė aplinka

- Išmanusis telefonas „LG G Flex 2“. Šis telefonas buvo naudotas atlikti grafinę autentfikaciją. Jo ekrano raiška yra 1080x1920, įstrižainė - 5,5 colio. Tokiame ekrane mygtukų briaunų ilgiai buvo apie 2cm, todėl kiekvieno mygtuko paviršiaus plotas buvo apie 4cm^2. Šio telefono ekranas yra kiek lenktas, bet tyrimams įtaka buvo minimali. Šiame telefone naudojama 5.1.1 Android operacinės sistemos versija;
- Išmanusis telefonas „Xiaomi Mi A2 Lite“. Šis telefonas buvo naudojamas autentifikacijos filmavimui. Filmuota naudojant šio telefono galinę 12.0 MP kamerą.

3.1.2. Fizinė aplinka

Tyrimai vyko betarpiškai. Dalyviai užduotis atliko gerai apšviestoje uždaroje patalpoje su vienu stebėtoju. Kai buvo tikrinamas autentifikacijos metodo nužiūrimumui patalpoje vinu metu būdavo du dalyviai, vienas iš jų autentifikuodavosi, o kitas stebėdavo autentifikaciją ir bandydavo atsiminti įvedamą slaptažodį. Po to dalyviai apsikeisdavo vietomis. Apklausa taip pat vyko patalpoje esant tik vienam dalyviui ir apklausą vedančiam žmogui.

3.1.3. Tyrimo dalyviai

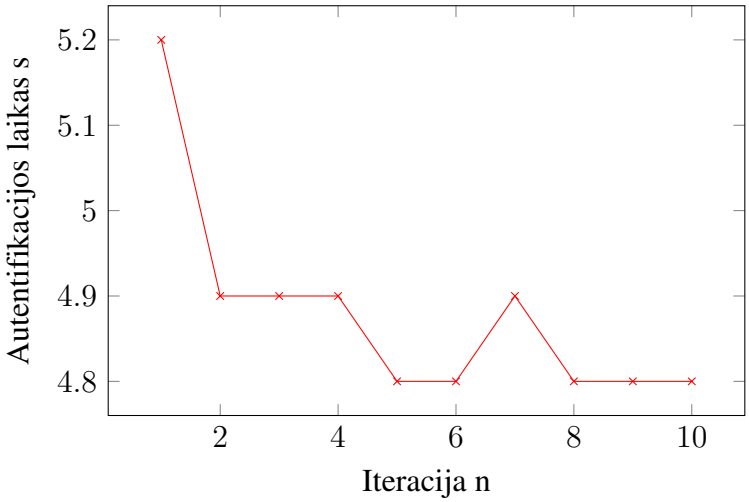
Tyrime dalyvavo 8 savanoriai. Gal iš pirmo karto atrodo, kad dalyvių kiekis yra mažas, bet panaudojamumo ir panašiems tyrimams būtų užtekę ir penkių žmonių [14]. Iš tų dalyvių penki buvo vyrai, o likusios trys - moterys. Dalyvių amžiaus intervalas 24-54 m. Visi dalyviai turėjo asmeninius išmaniuosius telefonus, todėl jie jau buvo gerai susipažinę su išmaniųjų telefonų veikimu. 4 dalyviai savo telefonus buvo užrakinę šablonais, 1 - PIN kodu, 3 - nebuvo nustatę jokio autentifikacijos metodo. Visi dalyviai buvo supažindinti su tyrimų ir apklausos paskirtimi ir davė žodinį sutikimą dalyvauti.

3.2. Panaudojamumo tyrimai

3.2.1. Autentifikacijos trukmė

Autentifikacijos laikas yra labai svarbus autentifikacijos metodo rodiklis. Jis ypač aktualus išmaniųjų telefonų autentifikacijai, nes juose reikalaujama dažnai autentifikuotis. Taip pat svarbu tirti per kiek laiko autentifikuojasi pradedantysis naudotojas, o ne patyręs. Tai svarbu, nes jei pradedantysis naudotojas nesugebės greitai autentifikuotis iš pirmų kelių kartų, jis metodo nenaudos ir rinksis kitą metodą, kuris yra greitas net naudojamas pradedančiojo.

13 pav. Autentifikacijos trukmė



Įvertinti autentifikacijos trukmei dalyvių pirma buvo paprašyta susigalvoti penkių simbolių grafinį slaptažodį. Prieš matuojant naudotojų autentifikacijos laiką naudotojams buvo leista suvesti savo slaptažodį kelis kartus, kad būtų patikrinta, ar naudotojai supranta autentifikacijos metodo veikimą. Tada kiekvieno nauotojo buvo paprašyta pasirinktą slaptažodį įvesti 30 kartų iš eilės. Prieš kiekvieną įvedimą grafinio slaptažodžio įvedimo mygtukai buvo išdėstyti atsitiktine tvarka. Šie trisdešimt slaptažodžio įvedimų buvo suskirstyti iteracijomis po tris. Visų aštuonių dalyvių vidutinio įvedimo laikas atvazduotas kreivėje 13.

Autentifikacijos trukmės grafike matosi, kad pirma iteracija truko kiek ilgiau, o likusios iteracijos užtruko maždaug tiek pat laiko. Vidutinė autentifikacijos trukmė buvo apie 5s. Palyginus su tekstinio slaptažodžio auetntifikacijos laiku, kuris dažniausiai trunka virš 20s [16], tai yra labai geras laikas. Dalyviai nesitikėjo, kad pavyks taip greitai autentifikuotis ir užtikrino, kad tokia autentifikacijos trukmė jiems priimtina.

3.2.2. Klaidų kiekis

Klaidų kiekis yra svarbus kriterijus. Dažnas klaidų kiekis prailgina autentifikacijos laiką ir mažina naudotojo pasitenkinimą naudojant autentifikacijos metodą. Dėl šių priežasčių metodas turi būti toks, kuriame klaidos būtų retos, o jeigu jos ir pasitaiko, padaryta žala turėtų būti minimali.

Autentifikacijos metu daromų klaidų kiekis buvo skaičiuotas tuo pačiu metu, kaip ir autentifikacijos laikas. 8 dalyviai iš viso atliko 240 autentifikacijų. Jas darydami jie padarė 9 klaidas. Tai reiškia 3,75% autentifikacijų buvo klaidingos.

Galima spėti, kad klaidų pasitaikė kiek daugiau, nei pasitaikytų įprastame autentifikacijos metodo naudojime, nes dalyviai buvo nepatyrę autentifikacijos metodo naudotojai. Jie taip pat skubėjo kuo greičiau autentifikuotis, nes žinojo, kad jų autentifikacijos laikas yra matuojamas. Po šio tyrimo dalyviai sakė, kad klaidų kiekis jiems buvo priimtinas.

3.3. Saugumo tyrimai

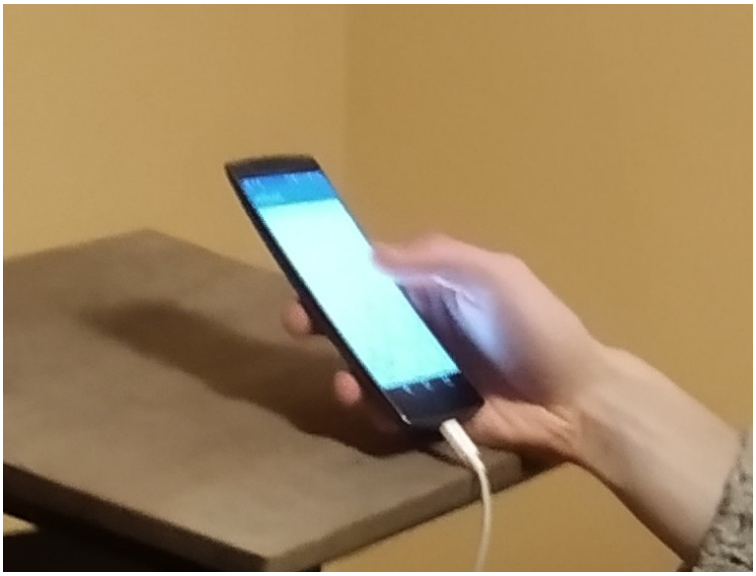
3.3.1. Nužiūrimumas

Ar autentifikaciją lengva nužiūrėti ir vėliau atkartoti šalia esančiam žmogui yra labai rūpimas klausimas išmaniųjų telefonų autentifikacijos metodų kūrėjams. Išmanieji telefonai dažnai naudojami viešose erdvėse, kitų žmonių akivaizduoje, todėl naudotojui paslėpti autentifikavimosi praktiškai neįmanoma. Pats autentifikacijos metodas turi užtikrinti, kad jis nėra lengvai nužiūrimas aplinkinių žmonių.

Tyimo pradžioje dalyviai buvo suskirstyti poromis. Tada vienas iš dviejų dalyvių atsistodavo, kur manė, kad gerai matys slaptažodį, o kitas dalyvis du kartus suvesdavo savo sugalvotą penkių paveikslėlių slaptažodį. Tada stebėtojas gaudavo tris spėjimus atspėti įvestam slaptažodžiui. Po trijų spėjimų partneriai apsikeisdavo rolėmis ir eksperimentas buvo kartojamas.

Kiekvienas iš aštuonių dalyvių gavo po tris spėjimus, todėl iš viso buvo atlikta 24 spėjimai. Nei vienas spėjimas nabuvo sėkmingas. Dalyviai pasakė, kad per kelias sekundes, kurių reikėjo suvesti slaptažodžiui, jie nespėjo sužiūrėti visų spaudžiamų paveikslėlių. Atspėti slaptažodį jiems kliudė ne atmintis, bet nesugebėjimas sužiūrėti spaudomų mygtukų.

3.3.2. Filmavimas



14 pav. Autentifikacijos filmavimas už 2 metrų

Viešose erdvėse, kuriose dažnai naudojami išmanieji telefonai, dažnai yra apsauginių vaizdo stebėjimo kamerų. Tai kelia pavojų, kad slatažodis gali būti nufilmuotas. Tai leistų stebėti įrašą ir išsiaiškinti kaip buvo daroma autentifikacija. Pavojų kelia ne tik apsauginės kameros, bet ir šalia esantys žmonės, kurie autentifikaciją gali nufilmuoti savo telefonais.

Patikrinti grafinio autentifikacijos metodo filmavimo pažeidžiamumui buvo atliktas tyrimas, kurio metu autentifikacija buvo nufilmuota aštuonis kartus. Filmuojama buvo iš abiejų naudotojo pusių po keturis kartus. Filmavimas taip pat buvo daromas iš dviejų skirtingų atstumų: dviejų metrų ir trijų metrų. Kiekvienoje pusėje buvo filmuota iš dviejų skirtingų kampų. Vienas kampas buvo labiau naudotojui iš šono, o kitas - labiau naudotojui už nugaros.

Tyrimo rezultatas nustebino, nes nepavyko sėkmingai nufilmuoti nei vienos autentifikacijos. Filmavimo metu ekranas tiesiog atrodė baltas, kaip pavaizduota 14 paveikslėlyje. Taip tikriausiai nutiko dėl autentifikacijai naudotų paveikslėlių, kurie buvo tuščiaviduriai. Jei būtų buvę naudoti kiti paveikslėliai, kamera juos tikriausiai būtų mačiusi. Kiti galimi paaiškinimai yra nepakankamai gera kamera, arba netinkamas apšvietimas.

3.4. Apklausos analizė

Po tyrimų visi aįtuoni dalyviai dalyvavo apklausoje. Apklausoje buvo užduodami atviri ir uždari klausimai apie jų bandytą grafinės autentifikacijos metodą. Apklausos metu dalyviai buvo apklausti individualiai, kad neturėtų vieni kitiems įtakos.

3.4.1. Paveikslėlių vertinimas

Dažniausias nusiskundimas su duotais paveikslėliais susikurti slaptažodžiui buvo tas, kad sunku sugalvoti atsimenamas asociacijas tokioms abstrakčioms figūroms. Nors paveikslėlių kiekis ir yra visai didelis, dalyviams užtruko sugalvoti slaptažodį, kurį jie manė galės ilgai atsiminti. Tokius nusiskundimus galima paaiškinti tuo, kad naudotojai dar nėra pratę prie naujo grafinės autentifikacijos metodo.

Apklausos dalyviai dar turėjo problemų su kai kuriomis spalvomis. Jiems kilo sunkumų norint atskirti juodą ovalą, nuo tamsiai pilko ovalo. Kitas duotas pavyzdys buvo sunkiai skiriamos tamsiai raudona ir tamsiai pilka keturkampės žvaigždutės. Paskutinis su spalvomis duotas nusiskundimas buvo tas, kad nėra pakankamai didelio kontrasto tarp geltonų formų ir balto fono.

Visas šias problemas galima spręsti nesirenkant naudoti figūrų kurios kelia sunkumus. Tai geras sprendimas, kai iš duotų figūrų reikia susigalvoti tik vieną slaptažodį. Jei iš šių 36 figūrų reikia sugalvoti tris slaptažodžius ar daugiau, tai jau kelia sunkumų, nes sunku susikurti tiek slaptažodžių nekartojant jau kituose slaptažodžiuose pasirinktų figūrų.

3.4.2. Slaptažodžių kūrimo pastebėjimai

Vienas iš autentifikacijos puolimo būdų yra spėti dažniausiai naudojamus slaptažodžius. Pavyzdžiui šablono autentifikacijai toks puolimas yra itin pavojingas, nes pats populiariausias šablonas yra naudojamas 9% visų naudotojų [4]. Labai svarbu išsiaiškinti ką naudotojai galvoja kurdamiesi grafinius slaptažodžius, kad būtų galima suprasti ir galimai išvengti tokio puolimo tipo.

Visi dalyviai apklausos metu buvo paklausti kokį grafinį slaptažodį jie susikūrė tyrimo metu, ir kokios buvo jų priežastys. Pirmas dažniausiai naudotojų paminėtas dalykas buvo tai, kad kurdamiesi slaptažodį jie didesnį dėmesį skyrė figūrai, o ne jos spalvai. Tai būtų galima paaiškinti tuo, kad figūros yra tuščiavidurės, todėl jų forma yra aiškiai matoma, o spalva - prasčiau.

Kitas pastebėtas naudotojų slaptažodžių bruožas buvo paveikslėlių grupavimas. Naudotojai rinkdamiesi slaptažodžius dažnai dėdavo tokias pačias, skirtingų spalvų figūras vieną prie kitos. Jeigu grafinis slaptažodis būdavo sudarytas iš penkių paveikslėlių, tada didelė tikimybė, kad į jį įėjo tik trys skirtingos formos. Dvi formos pasikartojo po du kartus. Šie pastebėjimai slaptažodžio atspėjimo tikimybės labai nedidina, bet parodo, kad yra tam tikri bendri grafinių slaptažodžių

bruožai, kurie kartojasi tarp naudotojų.

3.5. Sukurto autentifikacijos metodo vertinimo apibendrinimas

Panaudojamumas

P1 Lengvai atsimenamas. Šis autentifikacijos metodas išnaudoja žmogaus bruožą lengviau atsiminti vaizdus, nei kokią kitą informaciją;

P2 Keičiamo dydžio naudotojams. Naudotojų kiekis individualiam naudotojui įtakos neturi;

P3 Nereikalauja papildomų daiktų;

P4 Nereikia didelių pastangų įvedimui. Tik reikia paspausti devynis didelius mygtukus;

P5 Lengvai išmokstamas. Slaptažodis nereikalauja jokių specifinių žinių, kaip kalba, raštas, ar skaičiavimas. Jis yra vaizdinis ir intuityvus;

P6 Efektyvus naudojimas. Šiuo metodu galima labai greitai autentifikuotis;

P7 Retos klaidos. Viena iš to priežasčių yra dideli mygtukai, į kuriuos lengva pataikyti;

P8 Lengvai atstatomas po praradimo. Tereikia susikurti naują grafinį slaptažodį.

Saugumas

S1 Apsaugo nuo gyvo nužiūrėjimo. Tyrimo metu įrodyta, kad įprastomis sąlygomis šis metodas apsaugo nuo gyvo nužiūrėjimo;

S2 Apsaugo nuo tikslinio apsimetinėjimo. Naudotojo pažinojimas puolėjui neduoda didesnės tikimybės atspėti jo grafinio slaptažodžio;

S3 Apsaugo nuo limituoto spėliojimo. Grafinis slaptažodis turi užtenkamai galimų kombinacijų, kad apsaugotų nuo atspėjimo iš kelių bandymų;

S4 Dalinai apsaugo nuo nelimituoto spėliojimo. Jei naudojamas penkių paveikslėlių grafinis slaptažodis, jis turi daugiau kombinacijų, nei PIN kodas, todėl automatizuotas spėliojimas efektyvus tik pavieniams asmenims, o ne masėms;

S5 Neapsaugo nuo vidinio nužiūrėjimo. Įvedimo metu virusas gali nuskaityti slaptažodį ir jį atkartoti;

S6 Apsaugo nuo informacijos nutekėjimo iš kitų sistemų. Grafinį slaptažodį galima saugoti užkoduotą;

S7 Dalinai apsaugo nuo fišingo. Kad būtų galima suimituoti autentifikacijos sistemą, reikia žinoti naudotoju pasirinktus devynis paveikslėlius, kuriuos jis naudoja grafinio slaptažodžio įvedimui. Jei puolėjas yra įsiterpęs tarp naudotojo ir autentifikacijos sistemos, jis gali nuskaityti grafinį slaptažodį;

S8 Apsaugo nuo vagysčių. Šis metodas nereikalauja fizinių daiktų. Jei puolėjas turi šiuo grafiniu autentifikacijos metodu apsaugotą telefoną, į jį lengvai nepateks;

S9 Nepriklausomas nuo papildomų asmenų. Šio autentifikacijos metodo sistema yra paprasta ir nereikalauja papildomų asmenų;

S10 Reikalauja aiškaus sutikimo. Šiuo metodu negalima netyčia autentifikuotis;

S11 Nesusiejamas. Neįmanoma pasakyti ar du grafiniai slatažodžiai priklauso tam pačiam žmogui.

Išvados ir rekomendacijos

Palyginus jau sukurtus autentifikacijos metodus iškeltais panaudojamumo ir saugumo sričių kriterijais nustatyta, kad tiek tekstiniai, tiek netekstiniai metodai turi tiek panaudojamumo, tiek saugumo problemų. Nors tekstiniai metodai buvo kuriami prioritizuojant saugumą, tačiau ir jiems buvo rastos saugumo spragos. Netekstiniai autentifikacijos metodai buvo kuriami derinant panaudojamumą ir saugumą, tačiau juose taip pat nustatytos spragos. Gestų šablonas ir Skinerio autentifikacijos turi saugumo spragų, o like du netekstiniai metodai turi panaudojamumo spragų.

Kuriant autentifikacijos metodą buvo nustatyta, kad įmanoma suderinti panaudojamumo ir saugumo aspektus viename metode. Projektavimo gairės yra pateiktos žemiau esančiose rekomendacijose.

Metodo vertinimo metu rasta, kad sukurtam autentifikacijai metodui duoti paveikslėliai turi privalumą, nes jie sunkiai užfiksuojami filmuojant kamera ir nužiūrint iš šono. Taip pat metodas suteikia greitą įvedimą ir apsaugo naudotoją nuo klaidų.

Kuriant naujus autentifikacijos metodus siūloma atsižvelgti į šias rekomendacijas:

1. Kuriant autentifikacijos metodą siūloma vadovautis pirmame skyriuje identifikuotais kriterijais;
2. Grafiniame autentifikacijoje naudoti tuščiavidures figūras;
3. Vartotojui patogiau įvesti slaptažodį naudojant mažesnę elementų aibę, bet kuriant slaptažodį leisti šią aibę pasirinkti iš didesnio elementų kiekio.

Ateities tyrimų planas

Apklausos dalyviai paminėjo, kad abstrakčius paveikslėlius nėra taip lengva atsiminti. Ateities tyrimų metu būtų galima įvertinti koki būtų galimi paveikslėliai, kuriuos naudotojai lengviau atsimintų. Tačiau kuriant naujus paveikslėlius reikėtų atsižvelgti ir į slaptažodžio nužiūrimumą bei tai, kad paveikslėliai būtų lengvai skiriami tarpusavyje.

Ryšys tarp panaudojamumo ir saugumo yra labai jautrus. Trūksta tyrimų, kurie įvertintų, kokią įtaką panaudojamumui ir saugumui turi iš pirmo įspūdžio smulkūs pasirinkimai, pavyzdžiui, skirtumas tarp paspaudimo ir braukimo. Tokie tyrimai padėtų kurti ne tik geresnius autentifikacijos metodus, bet ir patogesnes išmaniųjų telefonų programėles.

Išmanieji telefonai greitai tobulėja. Šiuo metu ypač plinta telefonai turintys sulenkiamus ekranus. Taip pat daugėja telefonų, turinčių kelis ekranus. Reikia tyrimų, kaip toki nauji funkcionalumai keičia panaudojamumą bei saugumą.

Literatūros šaltiniai

[1] ISO 9241-210 (2011) Ergonomics of human-system interaction—Part 210: Human-centred design for interactive systems, ISO 9241-210: 2011 (E), 2011. International organization for standardization.

[2] Cain A.A., Chiu L., Santiago F., Still J.D. (2016) Swipe Authentication: Exploring Over-the-Shoulder Attack Performance. In: Nicholson D. (eds) Advances in Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing, vol 501. Springer, Cham. https://doi.org/10.1007/978-3-319-41932-9_27.

[3] Majed Alshamari. A review of gaps between usability and security/privacy. *International Journal of Communications, Network and System Sciences*, 09:413--429, 01 2016.

[4] Panagiotis Andriotis, George Oikonomou, Alexios Mylonas, and Theo Tryfonas. A study on usability and security features of the android pattern lock screen. *Information and Computer Security*, 24, 01 2015.

[5] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies*, WOOT'10, page 1–7, USA, 2010. USENIX Association.

[6] Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Asaf Ben-Oved, and Sebastian Möller. On the need for different security methods on mobile phones. MobileHCI '11, page 465–473, New York, NY, USA, 2011. Association for Computing Machinery.

[7] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553--567, 2012.

[8] Bethany Cartwright. The designer's guide to color theory, color wheels, and color schemes. https://blog.hubspot.com/marketing/color-theory-design, 2020. Accessed: 2021-01-02.

[9] Y. Chen, W. Ku, Y. Yeh, and D. Liao. A simple text-based shoulder surfing resistant graphical password scheme. In *2013 International Symposium on Next-Generation Electronics*, pages 161--164, 2013.

[10] Jean-Michel Trivi James B. Miller. Direct, gesture-based actions from device's lock screen, U.S. Patent US8136053B1, 2010.

[11] A. V. D. M. Kayem. Graphical passwords -- a discussion. In *2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 596--600, 2016.

[12] T. Kwon and J. Hong. Analysis and improvement of a pin-entry method resilient to shoulder-surfing and recording attacks. *IEEE Transactions on Information Forensics and Security*, 10(2):278--292, 2015.

[13] Geoffrey R. Loftus. Comparisons of recognition and recall in a continuous memory task. *Journal of Experimental Psychology*, pages 220--226.

[14] Jakob Nielsen. How many test users in a usability study? https://www.nngroup.com/articles/how-many-test-users/, 2012. Accessed: 2021-01-02.

[15] Gerald V. Post and Albert Kagan. Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, 26(3):229 -- 237, 2007.

[16] Florian Schaub, Ruben Deyhle, and Michael Weber. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia*, MUM '12, New York, NY, USA, 2012. Association for Computing Machinery.

[17] G. Skinner. Cyber security for younger demographics: A graphic based authentication and authorisation framework. In *2016 IEEE Region 10 Conference (TENCON)*, pages 2487--2490, 2016.

[18] Leonardo Sobrado and Jean-Camille Birget. Graphical passwords. https://rutgersscholar.libraries.rutgers.edu/volume04/sobrbirg/sobrbirg.htm, 2002. Accessed: 2020-12-21.

[19] Xiaoyuan Suo, Ying Zhu, and G. Owen. Graphical passwords: A survey. pages 463--472, 01 2005.

[20] Desney S. Tan, Pedram Keyani, and Mary Czerwinski. Spy-resistant keyboard: More secure password entry on public touch screen displays. In *Proceedings of the 17th Australia Conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future*, OZCHI '05, page 1–10, Narrabundah, AUS, 2005. Computer-Human Interaction Special Interest Group (CHISIG) of Australia.

[21] Ding Wang, Qianchen Gu, and Ping Wang. Understanding human-chosen pins: Characteristics, distribution and security. 02 2017.