Primerjava varnosti in pomnjenja gesel: ugotavljanje uporabnosti tradicionalne metode in metode igrifikacije

Leon Bošnjak, Viktor Taneski
Fakulteta za elektrotehniko, računalništvo in informatiko, Univerza v Mariboru, Koroška cesta 46, 2000 Maribor
leon.bosnjak@um.si, viktor.taneski@um.si

Izvleček

Besedilna gesla so dandanes še vedno najbolj pogost mehanizem avtentikacije, predvsem zaradi enostavne uporabe in implementacije, ter lažje pomljivosti. Kljub številnim prednostim pa so s postopnim povečanjem procesorske moči računalnikov postala dovzetna za številne napade, zaradi česar se je pojavila potreba po daljših, bolj varnih, ter težje zapomljivih geslih. Posledično so bile raziskane številne alternativne sheme avtentikacije, med drugim tudi grafična gesla. Študija, ki so jo leta 2017 izvedli McLennan in sodelavci, je predstavila novo shemo grafične avtentikacije, imenovano Game Changer Password System (GCPS), v sklopu katere so znaki gesla predstavljeni s položaji igralnih figuric. Čeprav avtorji ocenjujejo uporabnost sheme kot obetavno, rezultati študije ne dosegajo zadostne stopnje veljavnosti, saj ne upoštevajo zahtevane varnosti gesel. Poleg tega so avtorji ugotovili, da je potrebno rezultate primerjati tudi s tradicionalnimi gesli. V tej raziskavi smo preučili pomljivost in čas vnosa besedilnih in GCPS gesel, ter rezultate med obema metodama statistično primerjali. Pokazali smo, da so besedilna gesla boljša tako glede pomljivosti, kot tudi hitrosti vnašanja, kar opravičuje njihovo uveljavljenost kot osnovni mehanizem avtentikacije.

Ključne besede: Gesla igrifikacije, besedilna gesla, pomljivost gesel, varnost gesel, statistična primerjava

Comparison of password security and memorability: assessing the usability of traditional and gamification methods

Abstract

Textual passwords are the most common authentication mechanism due to their ease of use and implementation, as well as high memorability. As the computer processing power continued to increase, textual passwords gradually became less secure, resulting in an increased demand for longer, more secure and harder-to-remember passwords. As a result, other authentication schemes such as graphical passwords have been explored. A study by McLennan *et al.* in 2017 introduced a new authentication scheme called Game Changer Password System (GCPS), which uses game figure positions as password characters. The usability of the scheme was evaluated as promising, however these conclusions suffered from validity threats as the passwords used in the study did not represent secure GCPS passwords. In addition, the proposed scheme was not compared to the traditional passwords. In this study, we examined password recall rates and reaction time (login time), and we compared the results between the textual and GCPS passwords. We conclude that textual passwords are still superior both in terms of memorability and input speed, which justifies their prominence as a primary authentication mechanism.

Keywords: Gamification method passwords, textual passwords, password memorization, password security, statistical comparison

1 UVOD

Besedilna gesla so prevladujoča metoda avtentikacije že od šestdesetih let prejšnjega stoletja, ko se je prvič pojavila potreba po zaščiti občutljivih digitalnih podatkov [8]. Takrat so se uveljavila, ker jih je bilo enostavno implementirati, si jih je bilo mogoče zlahka zapomniti, hkrati pa so zagotavljala tudi zadostno varnost. Ker pa se je moč računalniške obdelave z leti povečevala (v skladu z Moorovim zakonom [7]), je kratka in preprosta gesla postopoma postajalo vse lažje razbiti. Čeprav so strokovnjaki za varnost kot odgovor na vse pogostejše zlorabe podatkov zagovarjali uporabo daljših in bolj zapletenih gesel, je pomnjenje le-teh postala težavna, kar je uporabnike spodbudilo, da se zatečejo k slabim praksam upravljanja z gesli. Žal takšna rešitev ostaja zgolj začasna: ker naj bi se procesorska moč računalnikov še naprej povečala, si bodo uporabniki dolga in zapletena gesla za več storitev, do katerih dostopajo, vedno težje zapomnili.

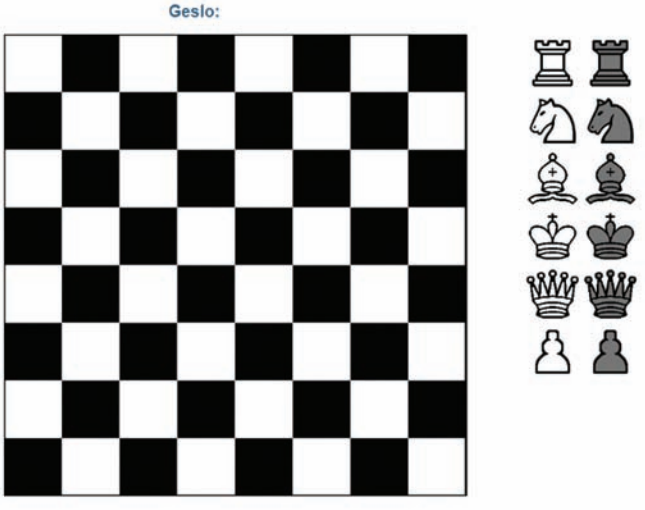
Posledično je bilo na področju informacijske varnosti v zadnjih nekaj desetletij izvedenih veliko raziskav na tematiko alternativnih shem avtentikacije. Čeprav obstoječe raziskave doslej še niso odkrile očitno boljše metode, obstaja nekaj obetavnih alternativ, ki bi lahko v prihodnosti dopolnile ali celo nadomestile besedilna gesla. Na primer, grafična gesla ohranjajo številne prednosti besedilnih gesel, kot sta enostavna uporaba in pomljivost, hkrati pa lahko zaradi svoje razširljivosti znatno povečajo stopnjo varnosti.

Tako kot besedilna gesla, so tudi grafična gesla avtentikacijski mehanizem, ki temelji na znanju. Glavni cilj grafičnih gesel je uporaba slik ali oblik za zamenjavo besedila, saj so številne kognitivne in psihološke študije pokazale, da si ljudje veliko bolje zapomnijo slike kot besede [20]. Najbolj splošno sprejeta teorija, ki pojasnjuje to razliko, je teorija dvojnega kodiranja [10], ki nakazuje, da se verbalni in neverbalni spomini v možganih obdelujejo in predstavljajo drugače. Slike, ki jim je pripisan zaznan pomen na podlagi neposrednega opazovanja, so predstavljene na način, ki ohranja opazovane zaznavne značilnosti. Besedilo je predstavljeno s simboli, ki izražajo asociativno spoznavni pomen. Posledično vsakršna dodatna obdelava, ki je potrebna za verbalni spomin, kognitivno nalogo oteži. Tako si lahko človek zlahka zapomni obraze ljudi, kraje, ki so jih obiskali, ter stvari, ki so jih opazovali dlje časa. Grafična gesla so se skozi čas razvila iz preprostega prepoznavanja obrazov, risb in kognitivnih shem do grafičnih metod igrifikacije [21, 13].

V študiji iz leta 2017 so McLennan in sodelavci [16] predstavili novo shemo grafične avtentikacije, imenovano Game Changer Password System (v nadaljevanju GCPS). Metoda predpostavlja standardno igralno ploščo poljubne namizne igre, na katero mora uporabnik v določenem zaporedju postaviti igralne figurice, pri čemer vsaka pozicija igralne figure na plošči predstavlja znak gesla. Primer metode GCPS je prikazan na sliki 1, kjer je prikazana grafična metoda na osnovi šahovnice.

Rezultati eksperimenta so pokazali, da so si uporabniki v več starostnih skupinah razmeroma enostavno zapomnili GCPS gesla (77 % povprečna natančnost v treh poskusih), čeprav je posamezen vnos trajal razmeroma dolgo (povprečni čas 28 sekund). V sklopu drugega eksperimenta, ki je trajal 10 tednov, so avtorji ugotovili, da se je sposobnost udeležencev, da si zapomnijo svoja gesla, sčasoma povečala (82 % povprečna natančnost), medtem ko so se njihovi reakcijski časi zmanjšali (povprečni čas 11 sekund).

Čeprav so ti rezultati sicer obetavni, na njihovi osnovi ne moremo sklepati o uporabnosti metode GCPS zaradi metodoloških pomanjkljivosti omenjene študije. Varnostna analiza metode GCPS je pokazala, da bi bilo za skladnost s trenutnimi varnostnimi zahtevami potrebno geslo z najmanj 7 znaki [6]. Prav tako v času pisanja tega članka NIST specifikacije določajo minimalno dolžino besedilnega gesla 8 znakov [1]. Ker so bili poskusi izvedeni na dvo- in štirimestnem geslu, so dobljene natančnosti vnosov in



Slika 1: **Grafični prikaz šahovnice pri metodi GCPS.**

reakcijski časi najverjetneje preveč optimistični. Prav tako so avtorji izpostavili, da bi bilo potrebno rezultate primerjati z že uveljavljenimi avtentikacijskimi metodami, kot so na primer tradicionalna gesla.

Namen obstoječe raziskave je razširiti delo [16] ter preučiti, ali so pri avtentikaciji grafična gesla GCPS bolj zapomljiva v primerjavi z besedilnimi gesli. V sklopu izvedenega eksperimenta smo določili varnostne politike, s katerimi smo zagotovili zadostno varnost izbranih gesel.

Raziskovalni vprašanji, na kateri smo odgovarjali, sta:

- Ali so izbrana grafična gesla bolj zapomljiva kot klasična besedilna gesla?
- Ali je čas, potreben za uspešno prijavo, nižji pri grafičnih kot pri besedilnih geslih?

Da bi odgovorili na zadana raziskovalna vprašanja, smo nad vzorcem študentov izvedli pilotno študijo. Eksperiment je potekal v dveh fazah. V prvi fazi so si študenti ustvarili uporabniške račune, ki so bili zaščiteni z obema metodama, torej s klasičnimi besedilnimi gesli, ter grafičnimi gesli GCPS. Po natanko dveh tednih je sledila druga faza raziskave, v kateri so se isti študentje poskusili ponovno prijaviti v uporabniške račune, ki so si jih ustvarili v prvi fazi. Pri tem smo merili število napačnih vnosov gesel, ter hitrost vnosa posameznih gesel.

1.1 Motivacija

Zaradi svoje zasnove grafična gesla (kot je GCPS) ohranjajo številne prednosti klasičnih, besedilnih shem avtentikacije: so relativno enostavna za implementacijo in intuitivna za uporabo, od uporabnika ne zahtevajo, da ima fizične žetone, poleg tega pa njihova izrazito vizualna podoba omogoča, da si je takšna gesla lažje zapomniti in pozneje priklicati na podlagi asociacij. Ker je takšne sheme možno enostavno razširiti, prav tako omogočajo drastično povečanje varnosti, zaradi česar bi takšne sheme lahko v prihodnosti potencialno dopolnile ali celo nadomestile besedilna gesla.

V tej raziskavi nameravamo preučiti predvsem dva ključna vidika uporabnosti: pomljivost in čas vnosa gesel. Izvorna študija je v sklopu izvedenih eksperimentov že preučevala oba vidika [16], vendar avtorji pri tem niso upoštevali takratnih varnostnih zahtev, niti niso svojih rezultatov primerjali z drugimi avtentikacijskimi metodami, kot so predlagali avtorji v [6]. Naša motivacija je razširiti obstoječe študije metode GCPS in rezultate primerjati primerjati s klasičnimi besedilnimi gesli, z namenom, da bi ugotovili, kakšna je izvedljivost in uporabnost metod grafične avtentikacije GCPS v praksi.

1.2 Organizacija članka

V nadaljevanju članka bo sledila predstavitev sorodnih del in izbranih tipov grafičnih gesel. Tretje poglavje povzema glavne metode raziskovanja. Podrobneje bomo predstavili obe raziskovalni vprašanji, postopek raziskovanja in način izvedbe meritev. Četrto poglavje bo predstavilo glavne rezultate, ki jih bomo v petem poglavju podrobneje analizirali. V zadnjem poglavju bomo na kratko povzeli bistvo in rezultate članka, ter predlagali nekaj možnih smernic za nadaljnje delo.

2 SORODNA DELA

Čeprav so gesla še vedno najbolj pogosta metoda avtentikacije [8], so bile njihove številne pomanjkljivosti [22] prvič zaznane že pred več kot štiridesetimi leti, ko sta avtorja Morris in Thompson besedilna gesla označila kot šibko točko varnosti informacijskega sistema [17]. Izvedla sta eksperiment, v katerem sta preučevala tipične navade uporabnikov pri izbiri lastnih gesel. Poročala sta, da so številni uporabniki sistema UNIX izbrali gesla, ki so bila zelo šibka: kratka, vsebovala so samo male črke ali številke, ali pa so se pojavljala v različnih slovarjih. Konec devetdesetih let prejšnjega stoletja sta avtorja Zviran in Haga prišla do podobne ugotovitve [26]. Dvajset let kasneje pa smo s pomočjo sistematičnega pregleda literature s tega področja ugotovili, da se stanje ni bistveno spremenilo, in sicer so uporabniki ter njihova gesla še vedno »Ahilova peta« varnosti informacijskih sistemov [22]. Med identificiranimi težavami so: ponovna uporaba gesel, več različnih gesel, ki si jih je treba zapomniti, šibka gesla, človeške omejitve pri pomljivosti gesel, zapisovanje gesel, ter deljenje osebnih gesel z ostalimi uporabniki sistema. Večina teh težav je tesno povezana s spominskimi omejitvami uporabnikov, ki jim onemogočajo, da bi si zapomnili več kompleksnih gesel za različne uporabniške račune [2]. Posledično so identificirane težave povzročile val raziskav na tematiko alternativnih metod avtentikacije, med katerimi so tudi grafična gesla.

Študija iz leta 2000 [5] uporablja standardno izvedbo predstavitvenega kompleta orodij *Passfaces*, ki od

udeležencev zahteva, da si zapomnijo 4 obraze in pravilno izberejo vse 4: enega v vsaki od 4 mrež z devetimi obrazi. Mreže so na zaslonu prikazane ena za drugo, vrstni red predstavitve ter obrazov v vsaki mreži pa ostaja nespremenjen. Kljub temu je vrstni red obrazov znotraj vsake mreže naključno izbran, prav tako pa nobena mreža ne vsebuje obrazov, ki se pojavijo v drugih mrežah. Avtorji so pri metodi *Passface* poročali o procentualno manj napačnih prijavah kot pri navadnih geslih. Naprednejša študija grafičnih gesel, ki temelji na prepoznavanju obrazov, je bila narejena leta 2004 [9]. Avtorji so raziskovali kako uporabniki izbirajo grafična gesla, ter ali so le-ta dovolj varna. Ugotovili so, da če uporabnike prisilimo, da si izberejo varnejša grafična gesla, s tem negativno vplivamo na njihovo pomljivost, kar nas pripelje nazaj do besedilnih gesel.

Čeprav se prav pomljivost grafičnih gesel pogosto izpostavlja kot njihova glavna prednost pred besedilnimi gesli, so obstoječe študije na to tematiko omejene in ne podajajo prepričljivih dokazov, ki bi podpirali to trditev [21]. V času nastavna prvih grafičnih gesel je bilo le-ta z uporabo tradicionalnih metod napadov (napad z grobo silo ali napad s slovarjem) težje zlomiti, so pa bila dovzetna za druge vrste napadov, kot so napadi z opazovanjem (*angl.* shoulder surfing), analiza vročih točk (*angl.* hotspot analysis), in drugi načini socialnega inženiringa (*angl.* social engineering) [21, 15]. Napad z opazovanjem je ključna pomanjkljivost grafičnih gesel, saj lahko napadalci (zlonamerni ali ne) lažje opazujejo in si zapomnijo grafične konstrukcije kot besedilne [4]. Avtorji v [24] so predlagali določene obrambne tehnike za zaščito pred takšnimi napadi, ki so se v splošnem izkazale kot delujoče, čeprav lahko njihova implementacija zmanjša uporabnost metode. Hkrati so določene grafične sheme gesel občutljive tudi na pomnilniške motnje (*angl.* memory interference), ki nastanejo, ko si morajo uporabniki zapomniti več različnih gesel za številne sisteme (kar je sicer pogost izziv tudi pri besedilnih geslih) [14].

Na splošno je uporabnost grafičnih avtentikacijskih shem vprašljiva. Raziskave kažejo na dejstvo, da sta varnost in uporabnost avtentikacijskih metod pogosto obratno sorazmerni [3]: povečanje varnosti pomeni zmanjšanje uporabnosti in obratno. To velja tudi za grafična gesla [13]. Pri doseganju želenega ravnovesja varnosti in uporabnosti nam lahko v prihodnosti pomaga umetna inteligenca, ter kombinacija različnih avtentikacijskih shem [25].

Osrednji del naše raziskave je študija, ki so jo opravili avtorji v [16]. Študija predstavlja novo avtentikacijsko metodo GCPS, v sklopu katere so znaki gesla grafično predstavljeni s premiki figuric na igralno ploščo. Čeprav to ni prva študija, ki raziskuje uporabnost grafičnih gesel, je prva, ki se osredotoča na GCPS avtentikacijske metode: igro šaha ter igro monopolija. Omenjena študija predstavlja obetavne rezultate, kljub določenim pomanjkljivostim. Nekatere so že identificirali avtorji sami (na primer, predlagani metodi nista bili primerjani z že obstoječimi besedilnimi gesli), nekatere pa so kasneje izpostavili avtorji v [6].

3 METODE RAZISKOVANJA

Ta študija, ki je raziskava v teku, raziskuje predlagano avtentikacijsko metodo GCPS iz [16] in jo primerja s klasičnimi besedilnimi gesli v sklopu klasičnega eksperimenta. Pilotno študijo smo izvedli na vzorcu študentov Fakultete za elektrotehniko, računalništvo in informatiko ter študentov Filozofske fakultete Univerze v Mariboru. Dobljeni rezultati so bili statistično obdelani ter interpretirani v diskusiji na koncu članka.

3.1 Eksperiment

Podatke za analizo smo zbrali s pomočjo eksperimentalne metode, pri čemer smo se zgledovali na eksperi- ment, ki so ga izpeljali avtorji v okviru [16]. Avtorji so izvedli dva eksperimenta. Tekom prvega eksperimenta so si udeleženci ustvarili gesla za dostop do fiktivnega uporabniškega računa. Po preteku 15 - 20 min so se ponovno prijavili v svoj račun z namenom testiranja dolgoročnega spomina. Omenjen eksperiment so avtorji nadgradili v longitudinalni študiji, v sklopu katere so v časovnem obdobju 10 tednov opazovali pomljivost in hitrost vnosa GCPS gesel. Ker nam čas in organizacija študentov nista dopuščala, da bi oba eksperimenta izvedli v polnem obsegu, smo se odločili, da se bomo osredotočili na prvi eksperiment, drugega pa smo izvedli v okrnjenem obsegu. Da bi bili rezultati našega eksperimenta primerljivi s tistimi, ki so jih producirali avtorji v [16], smo eksperiment načrtovali na podoben način. Eksperiment smo nadgradili z dodatno avtentikacijsko metodo, in sicer s klasičnimi besedilnimi gesli, kar nam je omogočilo, da smo lahko obe metodi statistično primerjali in odgovorili na zadana raziskovalna vprašanja.

Glavna cilja eksperimenta sta: ugotoviti, ali so izbrana grafična gesla na podlagi šahovnice bolj zapomljiva kot klasična besedilna gesla, ter ali je čas, potreben za prijavo pri besedilnih geslih krajši kot pri grafičnih.

3.2 Udeleženci

Prve faze eksperimenta se je skupaj udeležilo 110 študentov Univerze v Mariboru. Od tega jih je bilo 75 vpisanih na smer Informatika in tehnologija komuniciranja na Fakulteti za elektrotehniko, računalništvo in informatiko, in 35 na smer Psihologija na Filozofski fakulteti. Od skupno 110 udeležencev je bilo 68 moških in 42 žensk, pri čemer jih je bilo 90 vpisanih v prvi letnik, ter 20 v drugi letnik dodiplomskega študija. Povprečna starost udeležencev je 20,27 let (SD = 1,23). Obe fazi eksperimenta je končalo skupaj 83 udeležencev, ki smo jih upoštevali v končni analizi.

3.3 Izvedba eksperimenta

Udeleženci so dobili dostop do spletne aplikacije, kjer so bili pozvani k ustvarjanju novega uporabniškega računa. Za zaščito računa so morali ustvariti najprej navadno, besedilno geslo in nato še GCPS grafično geslo s premiki šahovskih figuric na šahovnico.

V prvi fazi je bila naloga udeležencev ustvariti besedilno geslo, za katerega so menili, da je dovolj varno, da bi ga sami uporabili kot dejansko geslo. Enako je veljalo tudi za grafična gesla. Takoj po registraciji uporabniških računov so se morali udeleženci dvakrat prijaviti v sistem: z novo ustvarjenim besedilnim in grafičnim geslom (v nadaljevanju bo ta del eksperimenta naslovljen kot »Prijava 1«). Sledil je 15 – 20 minutni odmor (kognitivni psihologi trdijo, da se informacije po največ 20 sekundah shranijo v dolgoročnem spominu), med katerim so udeleženci morali izpolniti demografski vprašalnik, ter vprašalnik o namiznih igrah in geslih. S tem smo zmanjšali verjetnost, da bi med odmorom udeleženci vadili na novo ustvarjena gesla. Po odmoru smo udeležence pozvali, da ponovno vnesejo svoje besedilno ter grafično geslo (v nadaljevanju bo ta del eksperimenta naslovljen kot »Prijava 2«). Pri tem je potrebno poudariti, da udeleženci niso bili vnaprej obveščeni o tem, da se bodo morali v sistem prijaviti večkrat. Udeležencem smo omogočili tri poskuse, da pravilno vnesejo svoje geslo, pri čemer smo za vsakega udeleženca merili reakcijski čas in število potrebnih poskusov do uspešne prijave. Reakcijski časi so bili izmerjeni v sekundah (s), in sicer od začetka tipkanja besedilnega gesla oziroma premikanja igralnih figuric, do pritiska na gumb »Prijava«.

Druga faza eksperimenta je potekala natanko dva tedna po prvi fazi. Udeleženci, ki so sodelovali v prvi fazi, so se morali ponovno prijaviti v sistem, pri čemer so morali vnesti besedilna in grafična gesla, ki so si jih ustvarili v prvi fazi eksperimenta (v nadaljevanju bo ta del eksperimenta naslovljen kot »Prijava 3«). Ponovno smo jim omogočili največ tri poskuse prijave, prav tako smo ponovno merili reakcijski čas ter število potrebnih poskusov do uspešne prijave.

3.4 Pravila pri ustvarjanju gesel

Dosedanje raziskave iz obstoječe literature kažejo, da uporabniki predvidoma izbirajo šibka gesla, ki jih je enostavno ugotoviti ali zlomiti, razen v primerih, ko je določena politika izbiranja gesel [22]. Za ta namen smo določili ustrezno politiko izbiranja gesel tako pri besedilnih kot tudi pri geslih GCPS. Pri določanju le-te smo izhajali iz politike besedilnih gesel, ki je najbolj pogosta v literaturi [11]. Za to politiko smo izračunali ustrezno teoretično entropijo oz. entropijo, kot bi jo imeli, če bi bila izbira znakov v geslu enakomerna. Ustrezno politiko gesel smo za (približno) enako entropijo sestavili tudi pri grafični metodi. Na ta način smo želeli obe metodi primerjati z vidika realnega primera, kjer je izbor gesla prepuščen uporabnikom. S tem jim olajšamo izbiro gesel in skušamo zagotoviti, da je izbrano geslo bolj podobno realnemu geslu, ki bi ga lahko uporabniki uporabili pri ustvarjanju računa na določeni spletni strani ali spletni storitvi.

3.4.1 Besedilna gesla

Ker včasih tudi določena varnostna politika ni zagotovilo, da bodo uporabniki izbrali močno geslo, smo se odločili, da zastavimo varnostno politiko izbiranja besedilnih gesel, ki ne bo prezahtevna za uporabnike. Namreč, če je politika zastavljena prestrogo, lahko deluje tudi kontraproduktivno, saj se uporabniki prej nagibajo k zamenjavi varnosti z lažjo pomljivostjo (»password« lahko postane »Password1!« kar je v osnovi enako (ne)varno). V končni fazi smo se odločili za varnostno politiko, ki vsebuje naslednja pravila:

- Geslo mora imeti vsaj 8 znakov
- Geslo mora vsebovati vsaj eno veliko črko
- Geslo mora vsebovati vsaj eno malo črko

- Geslo mora vsebovati vsaj eno številko
- Geslo mora vsebovati vsaj en poseben znak
- Geslo ne sme biti beseda iz slovarja

3.4.2 Gesla GCPS

Da bi bila izbrana grafična gesla primerljiva z besedilnimi smo morali tudi pri grafičnem načinu avtentikacije določiti politiko izbiranja gesel, ki bo primerljiva tisti iz besedilnih gesel glede na težavnost ter varnost izbranega gesla. Avtorji originalnega članka [16] so v osnovi že določili neko politiko gesel, in sicer: udeležencem je bilo dovoljeno uporabiti le dve ali štiri figurice za izdelavo gesla, posamezna lokacija na šahovnici pa je lahko bila uporabljena le enkrat. Prav tako pravilni vrstni red postavljanja figuric na šahovnici ni bil zahtevan. Te omejitve so se izkazale za premalo striktne, da bi bila ustvarjena gesla dovolj varna pred napadom z grobo silo [6]. V našem eksperimentu smo omenjena pravila nadgradili po predlogih [6]. Ustvarjena gesla GCPS morajo vsebovati:

- Vsaj 5 figuric
- Največ eno belo trdnjavo
- Največ enega belega kralja
- Največ dva bela konja
- Največ dva bela kmeta
- Največ eno vročo pozicijo
- Največ dve manj vroči poziciji

Vroče pozicije smo pridobili iz originalnega članka [16], v katerem je bila izvedena frekvenčna analiza uporabljenih figuric in pozicij na šahovnici. Vrstni red postavljanja figuric na šahovnici lahko pripomore k izbiri močnejšega in bolj varnega gesla [6], zato je bilo uporabnikom naročeno, da naj le to upoštevajo. Prav tako ni bilo nobenih omejitev glede lokacij na šahovnici, kar pomeni, da lahko uporabniki na eno lokacijo postavijo tudi več figuric.

4 REZULTATI

Preverili smo pravilnost vnesenih besedilnih in grafičnih gesel ob prvi prijavi (takoj po prvi registraciji) ter ob drugi in tretji prijavi. V tej sekciji bomo povzeli rezultate naše študije tako, da bomo statistično primerjali rezultate iz obeh faz eksperimenta. V nadaljevanju bomo predstavili še reakcijske čase, oziroma potrebne čase za prijavo v sistem. Kot je bilo že omenjeno, je obe fazi eksperimenta končalo le 83 študentov, kar smo pri obdelavi rezultatov tudi upoštevali.

4.1 Pravilnost vnesenih gesel

Tabela 1 prikazuje število potrebnih poskusov do uspešne prijave za izbrano avtentikacijsko metodo v posamezni fazi eksperimenta. Če spomnimo: »Prijava 1« predstavlja število potrebnih poskusov za prijavo v sistem takoj po ustvarjanju gesel, »Prijava 2« predstavlja število potrebnih poskusov za prijavo v sistem po 10-20 minutnem odmoru in »Prijava 3« predstavlja število potrebnih poskusov za prijavo po dveh tednih, ko je potekala druga faza eksperimenta.

Iz sekcije »Prijava 1« v Tabeli 1 je razvidno, da so se z besedilnim geslom v treh poskusih uspešno prijavili vsi razen enega udeleženca (98,8 %). 74 od 82 (90,2 %) udeležencev je pravilno geslo vneslo že pri prvem poskusu, šest (7,3 %) jih je vneslo pravilno geslo pri drugem poskusu, dva udeleženca (2,4 %) pa sta pravilno geslo uspela vnesti v tretjem poskusu.

Iz iste tabele je razvidno, da je za uspešno prijavo z geslom GCPS v povprečju potrebnih več poskusov. Le 53 od vseh 83 (63,7 %) udeležencev je uspelo vtipkati pravilno geslo v treh poskusih. Od teh 53 se je 45 (84,9 %) uspelo prijaviti v prvem poskusu, le dva udeleženca (3,8 %) sta se uspela prijaviti v dveh poskusih, šest (11,3 %) se je uspelo prijaviti v treh poskusih.

Da smo rezultate lahko primerjali z rezultati iz članka [16] smo analizirali tudi rezultate iz sekcije »Prijava 2«, v sklopu katere so se udeleženci posku-

Tabela 1: **Število prijav v posamezni fazi eksperimenta**

	Prijava 1		**Prijava 2**		**Prijava 3**	
Št. prijav	Besedilna gesla	GCPS	Besedilna gesla	GCPS	Besedilna gesla	GCPS
1	74	45	71	53	43	32
2	6	2	8	3	14	4
3	2	6	2	3	7	4
Neuspešno	1	30	2	24	19	43

šali prijaviti v svoje uporabniške račune po 10-20 minutnem odmoru, podobno kot v [16]. Opazimo lahko, da je v primerjavi s »Prijavo 1« število udeležencev, ki se jim je uspelo prijaviti v treh poskusih ali manj pri besedilnih geslih skoraj enako (81/83 oz. 97,6 %) in celo višje pri GCPS (59/83 oz. 71,1 %). Drugače povedano, 71,1 % udeležencev se je s pomočjo šahovnice uspelo uspešno prijaviti v treh poskusih ali manj, pri čemer se je kar 53 od teh 59 (89,9 %) udeležencev uspešno prijavilo že v prvem poskusu.

Za podrobnejšo analizo smo uporabili neparametrični Wilcoxonov statistični test, saj je Shapiro-Wilk test normalnosti pokazal, da vse razlike med pari naborov podatkov niso v skladu z normalno porazdelitvijo ($p < 0,05$ v vseh primerih).

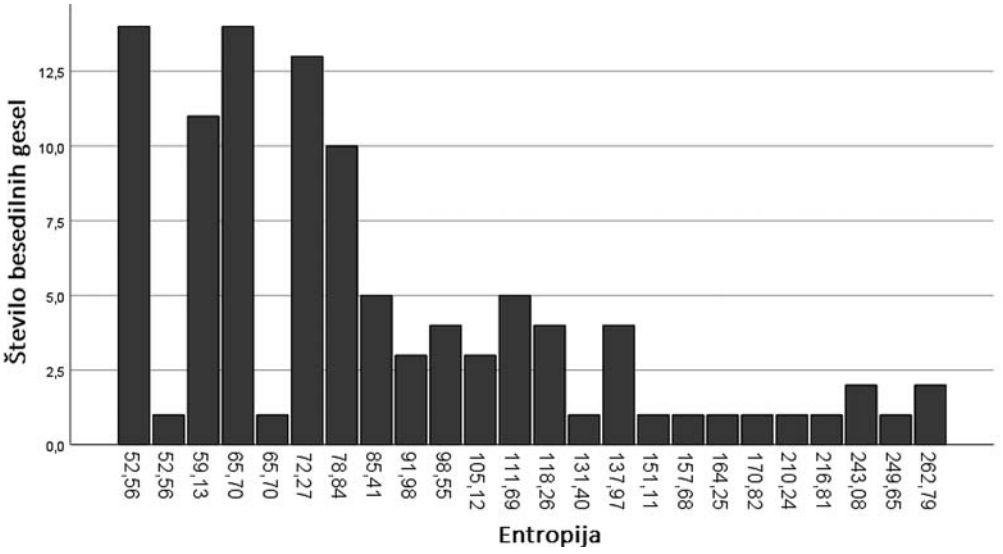
Pri besedilnih geslih Wilcoxonov neparametrični test ni pokazal statistično značilne razlike v številu potrebnih prijav med »Prijavo 1« in »Prijavo 2« ($T = 66$ pri $p = 0,38$). Pri GCPS pa je bila ta razlika signifikantna ($T = 57,5$ pri $p < 0,05$) saj se je več udeležencev uspelo prijaviti že v prvem poskusu.

Po dveh tednih pa se je število potrebnih poskusov za uspešno prijavo pri obeh avtentikacijskih metodah pričakovano povečalo, kot je razvidno iz stolpca »Prijava 3«. Iz zadnjega stolpca v Tabeli 1 je razvidno, da je 64 od vseh 83 (77,1 %) udeležencev uporabilo pravilno besedilno geslo v treh poskusih ali manj, od tega le 43 (67,2 %) v prvem, 14 (21,9 %) v drugem, ter 7 (10,9 %) v tretjem poskusu. Preostalim 19 izmed vseh 83 (22,9 %) udeležencev se ni uspelo prijaviti. Rezultati so bistveno slabši pri metodi GCPS. Le 40 izmed vseh 83 (48,2 %) udeležencev se je uspešno prijavilo v treh poskusih ali manj, od tega 32 (80 %) v prvem, 4 (10 %) v drugem, in 4 (10 %) v zadnjem poskusu. Kar 43 oziroma 51,8 % udeležencev pri prijavi v sistem z grafičnim geslom ni bilo uspešnih. Primerjava med »Prijava 2« in »Prijava 3« pa je tokrat pokazala statistično signifikantno razliko za obe metodi, tako besedilna ($T = 807,5$ pri $p < 0,05$) kot gesla GCPS ($T = 385,5$ pri $p < 0,05$).

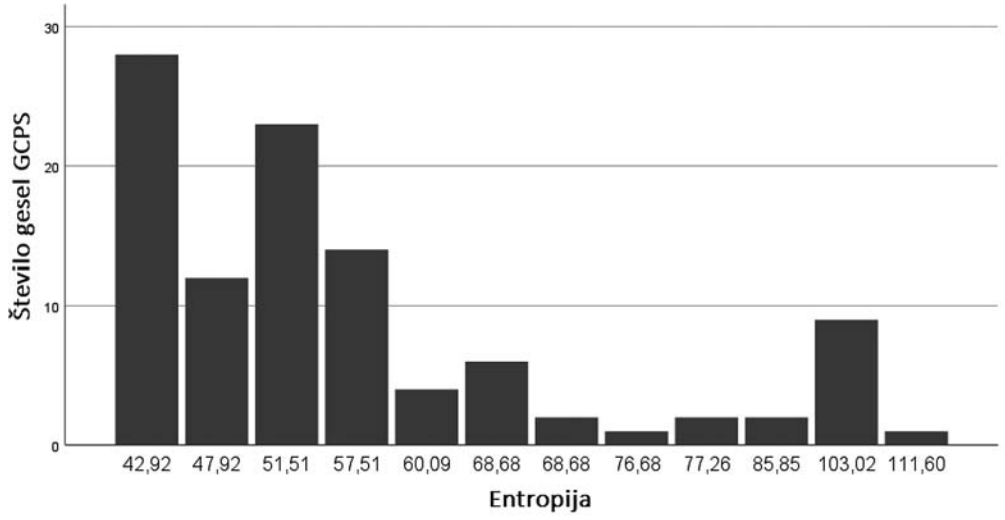
Nadaljnje primerjave obeh metod v različnih fazah so razkrile statistično signifikantne razlike med besedilnimi gesli ter gesli GCPS v vseh treh fazah eksperimenta: $T1 = 841$, $T2 = 676,5$ in $T3 = 905,5$ (pri teh statističnih testih je $p < 0,05$).

Podrobnejša analiza uspešnih prijav nam je pomagala boljše razumeti uporabnost posameznih metod. Pogledali smo, ali obstaja korelacija med številom potrebnih prijav za obe metodi v posameznih fazah eksperimenta. Uporabili smo neparametrični Spearmanov korelacijskih statistični test, saj je Shapiro-Wilk test normalnosti pokazal, da vse razlike med pari naborov podatkov niso v skladu z normalno porazdelitvijo ($p < 0,05$ v vseh primerih). Rezultati so pokazali, da korelacije med številom potrebnih prijav pri obeh metodah v fazah »Prijava 1« ($r = 0,162$, $p = 0,085$) in »Prijava 2« ($r = 0,08$, $p = 0,930$) ni. V zadnji fazi »Prijava 3« pa statistična korelacija ($r = 0,207$, $p < 0,05$) med številom potrebnih prijav pri obeh metodah obstaja.

Da bi dobili boljši vpogled v ustvarjena gesla, smo poleg števila uspešnih prijav in reakcijski čas za do-



Slika 2: **Graf entropije za ustrezno število besedilnih gesel.**



Slika 3: **Graf entropije za ustrezno število gesel GCPS.**

ločeno metodo izračunali tudi entropijo ustvarjenih gesel pri registraciji. Entropija je pomembna, saj nam pove kako nepredvidljivo in neuganljivo je geslo. Dejansko predstavlja verjetnost naključja (kako verjetno je, da bo napadalec izbral prav to geslo) [18]. Čeprav obstajajo boljši načini izračuna moči oz. verjetnosti določenega gesla [23], smo se za potrebe tega eksperimenta odločili za entropijo, saj cilj tega eksperimenta ni analiza moči gesel. Slika 2 in slika 3 prikazujeta grafa entropije za posamezne metode v času registracije (ustvarjanja gesel).

Wilcoxonov neparametrični test je pokazal, da so udeleženci ustvarjali besedilna gesla s signifikantno višjo entropijo (Mdn = 72,3) kot pa gesla GCPS (Mdn = 51,5), T=415, p<0,05.

4.2 Reakcijski čas

Tabela 2 prikazuje potrebne čase za uspešno prijavo za posamezno avtentikacijsko metodo v posamezni fazi eksperimenta. Podobno kot pri Tabeli 1 »Prijava 1« predstavlja čas, potreben za uspešno prijavo v sistem takoj po ustvarjanju gesel, »Prijava 2« predstavlja čas, potreben za uspešno prijavo v sistem po 10-20 minutnem odmoru in »Prijava 3« predstavlja čas, potreben za uspešno prijavo po dveh tednih, ko je potekala druga faza eksperimenta.

Iz zgornje tabele je razvidno, da je povprečni reakcijski čas za besedilna gesla malo daljši v fazi »Prijava 1« (M = 12,98, SD = 19,61) kot pa v fazi »Prijava 2« (M = 11,25, SD = 9,35). Ponovno smo uporabili neparametrični Wilcoxonov statistični test (Shapiro-Wilk test normalnosti je pokazal, da vse razlike med pari naborov podatkov niso v skladu z normalno porazdelitvijo, $p < 0,05$ v vseh primerih), ki ni pokazal statističnih razlik ($T = 1720$ in $p = 0,917$). Pri GCPS smo opazili signifikantno daljši čas v fazi »Prijava 1« (M = 28,49, SD = 16,52) kot pa v fazi »Prijava 2« (M = 20,09, SD = 10,24) ($T = 667$ in $p < 0,05$). Podobno kot pri pravilnosti vnesenih gesel sklepamo, da so udeleženci na začetku potrebovali malo več časa, da se navadijo na svoje geslo.

Tabela 2: **Reakcijski časi (v sekundah) po posameznih fazah**

		Minimum	Maksimum	Povprečje	Std. odklon
Prijava 1	Besedilna gesla	3,70	178,23	12,98	19,61
	GCPS gesla	7,94	86,19	28,49	16,52
Prijava 2	Besedilna gesla	3,83	65,69	11,25	9,35
	GCPS gesla	4,31	58,66	20,09	10,24
Prijava 3	Besedilna gesla	3,79	47,37	13,33	8,72
	GCPS gesla	3,60	77,02	23,1	11,89

V fazi »Prijava 3« se je reakcijski čas povečal tako pri besedilnih (M = 13,33, SD = 8,72) kot tudi pri geslih GCPS (M = 23,1, SD = 11,89). Pri obeh metodah je bila razlika reakcijskega časa med fazami »Prijava 2« in »Prijava 3« signifikantna ($p < 0,05$), in sicer za besedilna gesla je bil T = 2463, za GCPS gesla pa T = 2247.

Očitna razlika med povprečnima časoma, potrebnima za prijavo z geslom GCPS in besedilnim geslom v vseh fazah eksperimenta je bila tudi statistično utemeljena. Rezultati Wilcoxonovih neparametričnih testov so: T1 = 3251, T2 = 3181 in T3 = 3179 za posamezno fazo (pri vseh statističnih testih je $p < 0,05$).

5 RAZPRAVA

Avtorji v [16] poročajo o 77 % skupnem povprečju uspešnih vnosov gesel v treh poskusih. Čeprav bi avtentikacijski sistem v realnem okolju moral zagotavljati višjo pomljivost, so nižje vrednosti pričakovane, saj gre za popolnoma nov sistem, prav tako pa so udeleženci ustvarjali nova gesla ter pred tem niso bili opozorjeni, da si je potrebno novo-ustvarjena gesla zapomniti. V našem eksperimentu je bilo skupno povprečje že tekom registracije še nižje, in sicer 63,7 %, kar pomeni, da so udeleženci potrebovali razmeroma še več poskusov za vnos pravilnega gesla. Pri tem moramo izpostaviti, da je takšno povprečje še vedno obetavno, če upoštevamo dejstvo, da smo v našem eksperimentu implementirali dodatne omejitve. Varnostne politike, ki smo jih določili v sklopu ustvarjanja novih GCPS gesel so ustrezale priporočenim politikam, namenjenim besedilnim geslom. Takšne zahteve v realnosti prinašajo dodatno breme pri ustvarjanju (in kasnejšem pomnjenju) gesla. Namreč, če varnostne politike niso dovolj stroge, si uporabniki lahko ustvarijo tekstovna in grafična gesla, ki ne dosegajo zahtevanega nivoja varnosti.

Za primerjavo, tekstovna gesla so v sklopu prve prijave dosegla kar 98,8 % skupno povprečje uspešnih vnosov. Čeprav se je ta odstotek tekom kasnejših prijav po pričakovanjih zmanjševal, so udeleženci po dveh tednih še vedno dosegali višje skupno povprečje uspešnih vnosov (77,1 %), kot z metodo GCPS takoj po registraciji (63,7 %). Statistična primerjava med obema metodama je pokazala, da je bila razlika v pravilnosti vnosa signifikantna tekom vseh treh prijav.

Analiza reakcijskih časov je razkrila podobne rezultate. Tekom registracije so udeleženci za uspešno prijavo z besedilnim geslom potrebovali v povprečju 15 sekund manj kot z geslom GCPS. Čeprav se je ta razlika v drugi in tretji prijavi zmanjšala za okoli 5 sekund, razlike v reakcijskem času med metodama ostajajo signifikantne. Rezultati nakazujejo, da je potreben kompromis med varnostjo in uporabnostjo večji pri geslih GCPS kot pri besedilnih geslih.

Kot zanimivost lahko izpostavimo še, da je število uspešnih prijav z metodo GCPS v fazi »Prijava 2« manjše kot pa pri »Prijava 1«. Najverjetnejša razlaga predvideva, da so rezultati takšni, ker gre za novo avtentikacijsko metodo, ki ima še dodatne omejitve in bolj strogo varnostno politiko, kot je bila zahtevana v [16]. To lahko dodatno obremeni kognitivni spomin, kar lahko vpliva na čas, ki ga udeleženci potrebujejo, da se navadijo na novo avtentikacijsko metodo, ter novo-ustvarjena gesla. Na večje število napak v »Prijavi 1« je tako najvernetneje vplivalo prav nepoznavanje nove metode.

5.1 Pomljivost izbranih gesel

Odgovor na prvo raziskovalno vprašanje: »Ali so izbrana grafična gesla bolj zapomljiva kot klasična besedilna gesla?« lahko najdemo v podpoglavju 4.1, kjer so statistični testi v vseh fazah eksperimenta pokazali statistične razlike med besedilnimi gesli ter gesli GCPS. V fazi »Prijava 3« je število udeležencev, ki so se v treh poskusih uspešno prijavili z besedilnimi gesli 77,1 %, z gesli GCPS pa le 48,2 %. V splošnem so takšni rezultati podobni rezultatom nekaterih predhodnih študij [13]: grafična gesla so v osnovi manj uporabna kot besedilna, če pa povečamo zahteve po varnih grafičnih geslih, postanejo še manj uporabna. Kako težko je sestaviti geslo GCPS prikazuje tudi izračunana entropija za gesla, ki so si jih udeleženci izbrali ob prvi registraciji v sistem. Rezultati kažejo na to, da so izbrana gesla GCPS manj varna kot pa navadna besedilna gesla, kar je glede na zgoraj povedano tudi pričakovano.

Korelacijska analiza pa je pokazala, da zmožnost pomnjenja besedilnih gesel ne vpliva na zmožnost pomnjenja grafičnih gesel, in obratno. Drugače povedano, če si uporabniki lažje (oz. težje) zapomnijo besedilna gesla, to ne pomeni, da si bodo lažje (oz. težje) zapomnili tudi gesla GCPS. Čeprav lahko iz tabele 1 razberemo, da si uporabniki besedilna gesla v splošnem zapomnijo lažje kot grafična, rezultati korelacijske analize nakazujejo na dejstvo, da je zmožnost pomnenja besedilnih konstruktov neodvisna od zmožnosti pomnjenja grafičnih konstruktov. Pozitivna korelacija, ki smo jo opazili v fazi »Prijava 3«,

je nastala zaradi dvo-tedenskega premora pri obeh metodah; tabela 1 prikazuje, da je v zadnji fazi pomljivost obeh tipov gesel znižana zaradi postopnega propada spomina (t.j. pozabljanje).

Zavedamo se, da je ekološka veljavnost rezultatov omejena, saj študija ne predstavlja realnega primera, v sklopu katerega bi uporabniki vsakodnevno uporabljali svoja gesla. Pričakovano je, da pomljivost postopoma upada s časom, na kar lahko negativno vpliva tudi pogostost vnašanja gesel. Zato so avtorji v [16] izvedli še dodaten eksperiment, v katerem so preučevali pomljivost gesel GCPS v daljšem časovnem obdobju (10 tednov). Izveden eksperiment v tem članku predstavlja osnovo za nadaljnje raziskave na tem področju.

5.2 Reakcijski čas

Odgovor na drugo raziskovalno vprašanje: »Ali je čas, potreben za uspešno prijavo, nižji pri grafičnih kot pri besedilnih geslih?« lahko najdemo v podpoglavju 4.2, kjer so statistični testi pokazali statistično signifikantne razlike med povprečnimi časi, potrebnimi za vnašanje izbranega gesla v vseh fazah. Tudi na tem področju so bila besedilna gesla boljša s povprečnim časom 11,25 sekund v fazi »Prijava 2« v primerjavi s povprečnim časom 20,09 sekund za gesla GCPS.

Rezultati presenetljivo kažejo na dejstvo, da je povprečni čas vnosa GCPS gesla v fazah »Prijava 2« in »Prijava 3« hitrejši kot pa v originalnem članku [16], kar bi lahko nakazovalo na to, da se udeleženci relativno hitro navadijo na tovrstna gesla, ter postopek njihovega vnašanja. S to trditvijo se skladajo tudi rezultati drugega eksperimenta v sklopu študije [16], ki so pokazali, da je bil povprečni reakcijski čas za gesla GCPS približno 11 sekund.

5.3 Omejitve

5.3.1 Vzorec

Vzorec, ki smo ga imeli možnost izbrati za to raziskavo, ter podatki, ki smo jih pridobili in so navedeni v tem članku, morda niso popolnoma reprezentativni, ter ne predstavljajo splošne populacije. Nadalje, primerjavo med dvema metodama avtentikacije (besedilna gesla in GCPS) je potrebno izvesti na bistveno večjem in bolj raznolikem vzorcu (npr. primerjave je možno izvajati med različnimi starostnimi skupinami, študijskimi smermi, študenti z različnimi nivoji informacijske pismenosti, itn.).

5.3.2 Ekološka veljavnost eksperimenta

Gesla, ki so si jih uporabniki izbirali tekom eksperimenta, ne predstavljajo dejanskih gesel, ki bi ščitila realne uporabniške račune, temveč so bila ustvarjena izključno za namen te raziskave. To je sicer pogosta omejitev pri eksperimentih, ki se ukvarjajo z avtentikacijskimi metodami.

V sklopu tovrstnih študij gesel so pomembna vprašanja vezana tudi na ekološko veljavnost. Pri tem nas posebej zanima, ali je izsledke raziskovalne študije mogoče posplošiti iz opazovanega vedenja v laboratoriju na okolja v resničnem življenju [19], oziroma, ali se udeleženci študije obnašajo tako, kot bi se sicer obnašali uporabniki v resničnem življenju. Ekološka veljavnost je v študijah uporabnikov zelo pomembna, saj lahko že same informacije, ki jih uporabnikom podamo v začetni fazi eksperimenta, vplivajo na njihovo vedenje tekom študije. Avtorji v [12] so raziskali vpliv, ki ga zasnove uporabniških študij dejansko imajo na ekološko veljavnost izvedenih eksperimentov. Prišli so do zaključka, da so udeleženci pristranski in da se njihovo vedenje lahko spremeni že samo zaradi seznanjenosti z dejstvom, da sodelujejo v študiji gesel.

Izrazi »eksperiment«, »realistična zasnova« in »resnični podatki« so tesno povezani s kontekstom ekološke veljavnosti. V našem primeru lahko izraz »eksperiment« opredelimo kot laboratorijsko študijo, kjer uporabniki niso v njihovem naravnem okolju, izraz »realistična zasnova« lahko definiramo kot okolje, v katerem se uporabniki ne zavedajo, da jih preučujemo (npr. doma, v službi itd.), izraz »resnični podatki« pa bi lahko predstavljal gesla iz resničnega sveta, ki jih uporabniki uporabljajo v vsakdanjem življenju.

5.3.3 Implementacija grafičnega vmesnika

Pri implementaciji grafične metode avtentikacije, ki temelji na igrifikaciji, smo uporabili enak grafični vmesnik, kot je opisan v izvirnem članku [16], v katerem je bila ta metoda predstavljena. Moramo se zavedati, da kakršnekoli spremembe v implementaciji lahko vplivajo na končne rezultate primerjave, saj uvajanje drastičnih sprememb spreminja dejansko zasnovo grafične metode. Upoštevali smo nekaj nasvetov, ki so jih podali avtorji v [6], saj le-ti predstavljajo zgolj varnostno izboljšavo metode in omogočajo ustvarjanje močnejšega gesla, ne spreminjajo pa izgleda in delovanja same metode. En primer takšne

izboljšave je vrstni red postavljanja figuric na šahovnici, kar avtorji originalne metode niso upoštevali, čeprav vemo, da je vrstni red znakov v besedilnem geslu zelo pomemben, saj je od tega odvisno kako močno bo končno geslo [23]. Zavedamo se, da bi ob drugačnem načinu implementacije grafičnega vmesnika lahko dobili drugačne rezultate, kar je tematika naših nadaljnjih raziskav.

6 ZAKLJUČEK

V tem članku so predstavljeni rezultati raziskave, v kateri smo primerjali navadna besedilna gesla z grafičnimi gesli GCPS, ki so bila predstavljena v [16]. Glavna cilja raziskave sta bila ugotoviti ali so gesla GCPS bolj zapomljiva kot klasična besedilna gesla, ter ali je čas, potreben za prijavo v sistem krajši pri besedilnih geslih, kot pri geslih GCPS.

Pokazali smo, da so besedilna gesla boljša od grafičnih tako glede pomljivosti kot tudi hitrosti vnašanja. Takšni rezultati upravičujejo tudi njihovo razširjenost in vseprisotnost kot najbolj pogosto uporabljen način avtentikacije. GCPS je v obeh eksperimentih konsistentno dosegal slabše rezultate. Kljub temu, da je GCPS bolj kompleksen kot besedilna gesla, pa rezultati kažejo, da se uporabniki hitro naučijo kako sistem uporabljati. Ob tem je povprečni reakcijski čas še vedno hitrejši kot pa pri nekaterih grafičnih metodah avtentikacije [25]. K temu zaključku se nagibajo tudi avtorji v [16] saj je bil povprečni reakcijski čas v drugem eksperimentu celo 11 sekund, kar je skoraj dvakrat hitreje kot pri GCPS shemi, ki smo jo testirali v našem eksperimentu.

V tej raziskavi smo uporabili nadgrajeno GCPS shemo, ki je uvedla varnostne politike za doseganje ustre- znega nivoja varnosti glede na obstoječa priporočila [6]. S tem smo se želeli približati povprečni varnosti politiki, ki je implementirana v okviru besedilnih gesel. Posledično so bili rezultati nekoliko slabši kot pri [16], saj se je število udeležencev, ki so se uspešno prijavili v treh poskusih zmanjšalo. Določanje uravnoteženih varnostnih politik pri GCPS načinu avtentikacije (ter tudi na splošno pri grafičnih geslih) je zahtevno. Z dodatnimi raziskavami bi za gesla, ki temeljijo na namiznih igrah, lahko določili dobro ravnovesje med pomljivostjo in njihovo odpornostjo na surovo silo in napade s slovarjem. Nekateri predlogi so bili podani v [16] in [6], ki so predlagali, da bi od uporabnikov zahtevali, da naj uporablja več kombinacij, več figuric, lokacij, barv in potez. Vpliv tovrstnih varnostnih politik na pomljivost in uporabnost grafičnih gesel ostaja predmet nadaljnjih empiričnih raziskav.

Predstavljeni rezultati v tej raziskavi so preliminarni. V nadaljnjih raziskavah se bomo osredotočili predvsem na vpliv različnih eksperimentalnih skupin na pomljivost in čase vnosov izbranih gesel GCPS, ter na njihovo pomljivost v daljšem časovnem obdobju.

LITERATURA

[1] NIST special publication 800-63B. https://pages.nist.gov/800-63-3/sp800-63b.html. Accessed: 2022-7-10.

[2] Anne Adams and Martina Angela Sasse. Users Are Not the Enemy. *Commun. ACM*, 42(12):40–46, December 1999.

[3] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank 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.

[4] Leon Bosnjak and Bostjan Brumen. Shoulder surfing: From an experimental study to a comparative framework. *CoRR,* abs/1902.02501, 2019.

[5] Sacha Brostoff and M Angela Sasse. Are passfaces more usable than passwords? a field trial investigation. *People and Computers*, pages 1–20, 2000.

[6] Boštjan Brumen. Security analysis of game changer password system. *Int. J. Hum. Comput. Stud.*, 126:44–52, 2019.

[7] Boštjan Brumen and Viktor Taneski. Moore's curse on textual passwords. In *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1360–1365, 2015.

[8] Sadie Creese, Duncan Hodges, Sue Jamison-Powell, and Monica Whitty. Relationships between password choices, perceptions of risk and security expertise. In Louis Marinos and Ioannis Askoxylakis, editors, *Human Aspects of Information Security, Privacy, and Trust*, volume 8030 of *Lecture Notes in Computer Science*, pages 80–89. Springer Berlin Heidelberg, 2013.

[9] Darren Davis, Fabian Monrose, and Michael K Reiter. On user choice in graphical password schemes. *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13, page 11, 2004.*

[10] Dennis J Delprato. Mind and its evolution: A dual coding theoretical approach. *The Psychological Record*, 59:295–300, 2009.

[11] Roberto Dillon, Shailey Chawla, Dayana Hristova, Barbara Göbl, and Suzana Jovicic. Password policies vs. usability: When do users go »bananas«? In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 148–153, 2020.

[12] Sascha Fahl, Marian Harbach, Yasemin Acar, and Matthew Smith. On the ecological validity of a password study. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 13:1–13:13. ACM, 2013.

[13] Haichang Gao, Wei Jia, Fei Ye, and Licheng Ma. A survey on the use of graphical passwords in security. *Journal of Software, 8(7), 2013.*

[14] Haichang Gao, Licheng Ma, Wei Jia, and Fei Ye. Multiple password interference in graphical passwords. *International Journal of Information and Computer Security, 5(1):11–27, 2012.*

[15] Wei Hu, Xiaoping Wu, and Guoheng Wei. The security analysis of graphical passwords. In *2010 International Conference on Communications and Intelligence Information Security*, pages 200–203, 2010.
[16] Conor Mclennan, Philip Manning, and Samantha E. Tuft. An evaluation of the game changer password system: A new approach to password security. *Int. J. Hum. Comput. Stud.*, 100:1–17, 2017.
[17] Robert Morris and Ken Thompson. Password security: A case history. *Commun. ACM*, 22(11):594–597, nov 1979.
[18] Arvind Narayanan and Vitaly Shmatikov. Fast dictionary attacks on passwords using time-space tradeoff. In *Proceedings of the 12th ACM Conference on Computer and Communications Security*, CCS '05, pages 364–372. ACM, 2005.
[19] Mark A. Schmuckler. What is ecological validity? a dimensional analysis. *Infancy*, 2(4):419–436, 2001.
[20] Roger N Shepard. Recognition memory for words, sentences, and pictures. *Journal of Verbal Learning and Verbal Behavior*, 6:156–163, 1967.
[21] Xiaoyuan Suo, Ying Zhu, and G.S. Owen. Graphical passwords: a survey. In *21st Annual Computer Security Applications Conference (ACSAC'05)*, pages 10 pp.–472, 2005.
[22] Viktor Taneski, Marjan Heričko, and Boštjan Brumen. Systematic overview of password security problems. *Acta Polytechnica Hungarica*, 16(3):143–165, 2019.
[23] Viktor Taneski, Marko Kompara, Marjan Heričko, and Boštjan Brumen. Strength analysis of real-life passwords using markov models. *Applied Sciences*, 11(20), 2021.
[24] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, and Jeff Yan. Shoulder surfing defence for recall- based graphical passwords. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, New York, NY, USA, 2011. Association for Computing Machinery.
[25] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu. Captcha as graphical passwords—a new security primitive based on hard ai problems. *IEEE Transactions on Information Forensics and Security*, 9(6):891–904, 2014.
[26] Moshe Zviran and William J. Haga. Password security: An empirical study. *J. Manage. Inf. Syst.*, 15(4):161–185, mar 1999.

▪

Leon Bošnjak je zaposlen kot asistent za področje informatike na Fakulteti za eletrotehniko, računalništvo in informatiko na Univerzi v Mariboru. Leta 2014 je magistriral iz informatike in tehnologij komuniciranja. Leta 2022 pa je uspešno končal doktorski program Računalništvo in informatika. V okviru raziskav se ukvarja z informacijsko varnostjo, bolj specifično z tekstovnimi in grafičnimi gesli, ter drugimi metodami overjanja.

▪

Viktor Taneski je asistent na Fakulteti za elektrotehniko, računalništvo in informatiko na Univerzi v Mariboru. Doktoriral je leta 2019 iz tematike Markovih modelov ter vpliv podatkovnih zbirk za usposabljanje Markovih modelov na dokončno ocenjevanje moči gesel. Njegovo raziskovalno delo je povezano z varnostjo informacijskih sistemov, varnostjo gesel ter s človeškimi vidiki in navadami, povezanimi z ustvarjanjem in uporabo gesel.