SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 370

Jednokratna autentikacija zasnovana na znanju korisnika

Kristian Skračić

Zagreb, lipanj 2012.

Sadržaj

Uvod

Većina sustava, neovisno o primjeni, ima potrebu razlikovati korisnike. Ovo se postiže davanjem posebnog identiteta za svakog korisnika sustava. No, sustav mora moći odrediti je li korisnik koji koristi sustav zaista onaj korisnik kojemu pripada taj dodijeljeni identitet. Informacijski sustavi imaju sve veću ulogu u današnjem društvu. Tijekom dana, prosječan korisnik koristi razne usluge interneta kako bi obavljao određene zadatke. Obavlja bankovne transakcije putem internet bankarstva, upravlja elektroničkom poštom, posjećuje razne društvene mreže te druge usluge. Svaki od tih sustava mora zadovoljavati određeni skup sigurnosnih zahtjeva kako bi korisnicima pružao najmanju razinu sigurnosti. Najosnovniji sigurnosni zahtjev predstavlja upravljanje pristupom. Korisnicima se obično dodjeljuju određene funkcionalnosti i mogućnosti ovisno o njihovoj ulozi, identitetu i drugim značajkama. No, prethodno je potrebno autentificirati korisnika kako bi se otkrilo koja prava posjeduje. Autentifikacija korisnika je neophodan dio u osiguravanju osnovnih sigurnosnih zahtjeva.

Autentikacija korisnika je širok pojam koji podrazumijeva niz različitih disciplina. U ovom radu se analiziraju metode autentikacije zasnovane na korisničkom znanju. Radi cjelovitosti, u idućem poglavlju se razmatraju svi mogući načini autentikacije korisnika. U poglavlju 2 se detaljnije opisuje autentikacija temeljena znanjem. To je ujedno i glavna metoda autentikacije korisnika koja će se razmatrati u ovom radu. U sklopu ovog rada predlaže se metoda ocjenjivanja metoda autentikacije temeljene na znanju. Poglavlje 4 opisuje predložene mjere ocjenjivanja te se provodi analiza postojećih metoda autentikacije. Drugi cilj ovog rada je predložiti novu metodu autentikacije korisnika koja se temelji na znanju korisnika. U poglavlju 4 se opisuje predložena metoda autentikacije, dok se u poglavlju 5 opisuju smjernice za daljnja istraživanja.

1. Autentikacija

Autentikacija predstavlja proces ovjere identiteta osobe ili entiteta. Većina informacijskih sustava ima potrebu razlikovati jednog korisnika od drugog. Autentifikacija korisnika je neophodan dio u osiguravanju osnovnih sigurnosnih zahtjeva informacijskih sustava. Najosnovniji sigurnosni zahtjev predstavlja upravljanje pristupom. Korisnicima se obično dodjeljuju određene funkcionalnosti i mogućnosti ovisno o njihovoj ulozi, identitetu i drugim značajkama.

Postupak autentikacije korisnika je složen postupak koji obuhvaća nekoliko znanstvenih područja. Općenito, autentikacija se postiže tako da korisnik predoči neku vrstu faktora kojime dokazuje svoj identitet. Autentikacijski faktori mogu uključivati jednu ili više stvari. Ti faktori se opisuju u nastavku, a više informacije može se pronaći u dodatnoj literaturi pod [1] i [2].

- **Nešto što korisnik zna** – obično se radi o tajnim informacijama koje su poznate samo korisniku i onome tko vrši autentikaciju. Na primjer, lozinka je najčešće ostvarenje ovog faktora. Cilj ovog rada je pregled i analiza postojećih metoda autentifikacije temeljenih na znanju korisnika. U nastavku rada se detaljno opisuju pojedine metode autentikacije zasnovane na znanju korisnika.
- **Nešto što korisnik ima** – podrazumijeva uporabu posebnih uređaja kojima korisnik potvrđuje svoj identitet. Takvi uređaji se obično nazivaju tokenima, te se često koriste u bankarstvu. Glavna značajka je da se korisnik autenticira putem tog uređaja. Točnije, korisnik se autenticira pomoću informacijama koje uređaj proizvodi. Tokeni u bankarstvu obično proizvode jednokratne lozinke kojima se korisnik autentificira. Kreditne kartice koriste kombinaciju ovog i prethodno faktora za autentifikaciju korisnika. Kreditne kartice predstavljaju fizički faktor, dok se PIN (engl. *Personal Identification Number*) lozinka koristi kao faktor znanja.
- **Nešto što korisnik jest** – autentifikacija se oslanja na fizička svojstva korisnika. Na primjer, otisci prstiju, raspoznavanje glasa, uzorak vena u očima, geometrija

ruke te drugo. Ovakav način autentifikacije se naziva biometrija te predstavlja posebnu znanstvenu disciplinu.

1.1. Načini uporabe autentikacijskih faktora

Metodologije provjere identiteta korisnika su brojne i mogu biti jednostavne ili složene. Razina sigurnosti koje pružaju varira ovisno o korištenoj metodi i načinu na koji se koristi. Prethodno navedeni faktori autentikacije korisnika mogu se koristiti zasebno ili međusobno kombinirati. U nastavku se opisuju općeniti oblici kombinacija.

- **Jednostruki faktor** (engl. *Single-factor Authentication*) – Najjednostavnija metoda autentikacije se zasniva na uporabi samo jednog faktora za autentikaciju. Ova metoda autentikacije se oslanja na marljivosti korisnika. Na primjer, kod uporabe tekstualnih lozinki često se pretpostavlja da će korisnik izabrati dobru lozinku te da će ju zapamtiti. Tekstualne lozinke se detaljnije razmatraju u nastavku. Općenito, uporaba jednostrukog faktora se obično koristi kod sustava koji imaju manje sigurnosne zahtjeve.
- **Višestruki faktori** (engl. *Multi-factor Authentication*) – često se naziva i metoda dvostrukog faktora (engl. *Two-factor Authentication*). Iako se teoretski mogu koristiti sva tri faktora za autentikaciju, najčešće se kombinira nešto što korisnika zna i nešto što ima. Zbog većeg troška na opremu, biometrija se obično koristi neovisno od ostale dvije. No, u iznimnim slučajevima moguće je koristiti u kombinaciji s ostalim faktorima. Ova metoda autentikacija pruža veću razinu sigurnosti jer se koristi više faktora. Samim time, napadač mora više koraka poduzeti da zaobiđe pojedini faktor. Ova metoda se koristi u sustavima koji zahtijevaju visoku razinu sigurnosti. Naravno, učinkovitost odabranih faktora ovisi i o cjelovitosti procesa i način kojim se upravlja. Najjednostavniji primjer uporabe višestrukih faktora predstavljaju kreditne kartice. Same kartice predstavljaju nešto što korisnik ima, dok PIN čini nešto što korisnik zna.

1.2. Tehnike, procesi i metode autentikacije

Autentikacija je jedan od najvažnijih koraka u sigurnosti informacijskog sustava. Iz tog razloga razvijen je velik broj raznovrsnih tehnika koje omogućuju autentikaciju korisnika u sustavu. U nastavku poglavlja se opisuju neke konkretne metode autentikacija korisnika.

1.2.1. Zajedničke tajne

Zajedničke tajne predstavljaju osnovni način autentikacije korisnika. Ova tehnika se zasniva na faktoru znanja (nešto što korisnik zna). Točnije, zasniva se na tajnim informacijama koje su poznate samo korisniku i entitetu koji obavlja njegovu autentikaciju. Najpoznatija metoda autentikacije zajedničkim tajnama čini uporaba lozinki. No, u zadnje vrijeme se područje širi te se uvode nove tehnike autentikacije temeljene na zajedničkim tajnama. Točnije, uporaba slikovnih lozinki te činjenica koje su poznate korisniku, a koje se ne odnose samo na lozinke. Zajedničke tajne su glavni oslonac autentikacije putem korisničkog znanja i zato se detaljnije opisuje u poglavlju 2.

1.2.2. Token

Token predstavlja fizički uređaj koji se koristi za autentikaciju korisnika. Pripada faktoru koji obilježuje nešto što korisnik ima. Fizički uređaj se obično predaje korisniku prilikom postupka registracije na sustav. Samim time, troškovi održavanja sustava su viši jer se uređaji moraju dostaviti korisniku i mora se osigurati njezin ispravan rad. Uporaba tokena se ne primjenjuje u autentikaciji korisnika temeljenoj na znanju. No, ne isključuje se njihova zajednička uporaba u sustavima koji zahtijevaju veću razinu sigurnosti. Radi cjelovitosti, u nastavku se opisuju neki primjeri uporabe tokena u autentikaciji korisnika.

- **USB Token** – uređaj koji se je obično veličine standardnog USB uređaja. Na samom uređaju se nalazi programska potpora i svi podatci koji su potrebni da se korisnik autenticira sustavu. Korisnik ne treba instalirati dodatnu programsku potporu kako bi koristio uređaj. Nakon što korisnik priključi USB uređaj u svoje računalo, postupak autentikacije može započeti. Ovisno o razini sigurnosti koja se želi postići, nakon očitavanja USB uređaja, u nekim slučajevima se traži dodatna autentikacija korisnika lozinkom. Ovo je primjer uporabe USB uređaja i dijeljenih tajni za ostvarenje metode autentikacije višestrukim faktorima. Osim lozinke, USB token može sadržavati i digitalni certifikat koji se koriste u PKI (engl. *Public Key*

Infrastructure) okruženjima. Kako se na samom uređaju pohranjuju tajni podatci, postoji opasnost da ti podatci ne dođu u ruke zloćudnih korisnika. Uređaji su smješteni na sklopovlju koje je otporno na izmjene. USB tokeni se smatraju jednostavnim za uporabu obzirom da danas gotovo svako računalo ima USB ulaz. Dodatno, ne zahtijevaju nikakve dodatne uređaje ili programsku potporu za rad, već se sve potrebno nalazi na samom uređaju.

- **Pametne kartice** (engl. *Smart Card*) – predstavljaju kartice na kojima se ugrađuje mikroprocesor, čime se omogućuje pohrana i obrada podataka. Uporaba mikroprocesora omogućuje uporabu otpornijih autentikacijskih metoda. Kartica se očitava pomoću posebnih čitača. Iako se većina čitača za osobna računala može jednostavno priključiti putem USB priključka, većina korisnika nema čitač pametnih kartica. Time se troškovi rada povećavaju s obzirom na to da je potrebno svakom korisniku uz karticu, dostaviti i čitač. Prvi korak autentikacije odvija se lokalno prilikom očitavanja kartice. Čitač potvrđuje je li kartica ispravna i ovaj korak predstavlja prvi faktor autentikacije nečime što korisnik ima. Drugi korak autentikacije obično traži od korisnika unos lozinke ili PIN broja. Pametne kartice se smatraju iznimno sigurnom tehnologijom jer ih se teško može kopirati i otporne su na pokušaje izmjene internih podataka. Kao i USB tokeni, pametne kartice su praktični uređaji koje ne zauzimaju velik prostor kod korisnika prilikom prijenosa. Više informacija može se pronaći u dodatnoj literaturi pod [56].

- **Token za proizvodnju lozinki** – metoda koja se zasniva na korištenju posebnog uređaja koji proizvodi jednokratne lozinke kojima se omogućuje autentikacija korisnika. Uređaj je zadužen za to da se ista lozinka nikad ne iskoristi dva ili više puta za redom. Postupak autentikacije obično nalaže da se korisnik prvo autenticira običnom lozinkom, a zatim jednokratnom lozinkom koju proizvede token. Obzirom da se uređaji lako mogu otuđiti, gotovo uvijek se koriste u kombinaciji s nekim drugim faktorom. Najčešće obična tekstualna lozinka, obzirom da je najjednostavnija. Jednokratnost proizvedenih lozinki je korisno svojstvo pošto onemogućuje ponovnu uporabu nakon otuđivanja. Uređaji svakih 60 do 30 sekundi interno mijenjaju lozinku.

1.2.3. Biometrija

Biometrijske tehnologije provjeravaju korisnikov identitet temeljem njegovih fizioloških ili fizičkih karakteristika. Točnije, pomoću faktora koji opisuje nešto što korisnik jest. Fiziološke značajke podrazumijevaju otisak prstiju, šarenice te struktura lica. Fizikalna svojstva uključuju tijek kretanja korisnika kao što su unos podataka putem tipkovnice ili kretanje miša. Postupak registracije korisnika u biometrijski sustav se naziva upisivanje (engl. *enrollment*). Prilikom upisivanja korisnika, uzimaju se podatci iz jedne ili više fizioloških ili fizičkih svojstava te se pretvaraju u matematički model ili predložak. Tako dobiveni model ili predložak se upisuje u bazu podataka koja se koristi prilikom autentikacije korisnika. Biometrijska autentikacija se obično koristi s drugim faktorima autentikacije kako bi se osigurao najviši stupanj sigurnosti. Trenutno najpopularniji oblici biometrijske autentikacije korisnika je prepoznavanje otiska prstiju i lica korisnika. U nastavku se opisuju neke od poznatijih metoda biometrijske autentikacije, a više informacija može se pronaći u dodatnoj literaturi pod [57], [58] i [59].

- **Prepoznavanje otiska prstiju** – smatra se jednim od najpoznatijih i najpouzdanijih metoda biometrijske autentikacije korisnika. Uporaba otiska prsta je najpreciznija metoda autentikacije korisnika biometrijskim algoritmima. Otisci prstiju smatraju se dovoljno složenim i robusnim za sigurnu autentikaciju korisnika. Popularnost im je toliko porasla u zadnjih nekoliko desetljeća da mnogi proizvođači prijenosnih računala ugrađuju čitaće otiska prsta u svija računala. Njihova uporaba se trenutno razmatra u svrhu autentikacije korisnika u bankovnim sustavima. Time bi se uklonila potreba za kreditnim karticama. Iako svaka biometrijska metoda autentikacije korisnika zahtjeva posebno sklopovlje za očitavanje fizioloških značajki, očitavanje otiska prsta smatra se sklopovski najjednostavnijom metodom. Postupak upisivanja je iznimno jednostavan, a može se obaviti kod organizaciji ili kod korisnika doma. Ipak, za sustave koje zahtijevaju visoku razinu sigurnosti preporuča se postupak upisivanja obaviti u živo. Tehnike prepoznavanja zasnivaju se na prikupljanju informacija o shemi otiska zajedno s velikim brojem jedinstvenih detalja koje se u njima nalaze. Tako prikupljeni podatci su izuzetno gusti, što objašnjava pouzdanost ove metode autentikacije. Sustavi ne pohranjuju slike stvarnih otisaka prstiju već samo podatke koji opisuju detalje otiska.

- **Prepoznavanje lica** – zasniva se na prepoznavanju posebnih značajki ljudskog lica. Prilikom očitavanja značajki proizvodi se dvodimenzionalna slika ljudskog lica. Tako dobivena karta lica se pohranjuje u sustav prilikom upisivanja korisnika. Prilikom autentikacije korisnika, pohranjeni podatci se uspoređuju s podatcima prikupljenim prilikom očitavanja lica. Noviji sustavi rade i trodimenzionalne slike, a razlikuju se po količini detalja koje prikupljaju. No, prepoznavanje lica ima određene nedostatke u odnosu na prepoznavanje otiska prstiju. Slike lica su puno osjetljivije na okolinu u kojoj se korisnik nalazi. Točnije, prilikom očitavanja otiska prsta, okolina se zanemaruje. Prst se prislanja uz površinu za očitavanje i time sprječava utjecaj okoline na prikupljenu sliku. Ljudsko lice nije ravno i zato se ne može prisloniti izravno na čitač. Snimka lica se mora napraviti u kontroliranom okruženju. Na prikupljene detalje može utjecati osvijetljenost slike, pozadinski šum, pozicija lica na slici te druge značajke. U sustavima koji zahtijevaju veću razinu sigurnosti mogu se koristiti više kamera koje očitavaju lice iz različitih kuteva. Dodatno, neki sustavi prate micanje lica kao što je treptanje i micanje usana kako bi se osiguralo da se radi o živoj osobi. U suprotnom bi zlćudni korisnici mogli pomoću slike lica legitimnih korisnika dobiti pristup.
- **Signal mozga** – prema novim istraživanjima poput [52] i [53], moguće je koristiti moždane impulse za autentikaciju korisnika. Naime, dokazano je da svaki mozak na određene podražaje može proizvesti signal koji je jedinstven. Na primjer, ako se korisniku prikaže slika njegovog bicikla iz djetinjstva, mozak će proizvesti signal koji je jedinstven samo za taj podražaj i za tog korisnika. Niti jedan drugi korisnik neće na sliku tog bicikla imati identičan signal.
- **Prepoznavanje pokreta na računalu** – podrazumijeva analizu načina na koji korisnik koristi tastaturu [54] i miš [55] prilikom interakcije s računalom. Potrebno je prikupiti određenu količinu informacija profiliranjem korisnika. Točnije, potrebno je prikupiti podatke o tome kako korisnik inače koristi tastaturu i miše. Pomoću tih informacija se kasnije može napraviti autentikacija.

1.2.4. Jednokratne lozinke koje se ne temelje na sklopovlju

Uporaba sklopovlja za autentikaciju korisnika nije uvijek prihvatljivo s obzirom na dodatan trošak opreme. Kako bi se trošak smanjio, uređaji za proizvodnju jednokratnih lozinki se zamijenio papirnatim ili plastičnim karticama. Točnije, korisnici dobivaju kartice na kojima se nalaze nizovi brojeve ili znakova poredanih u matricama. Prilikom autentikacije sustav od korisnika zahtjeva da upiše znakove koji se nalaze u nasumično odabranom redu ili stupcu matrice na kartici. Trošak uporabe ovakvih kartica je zanemariv u odnosu na trošak uporabe posebnog sklopovlja. Budući da kartice nisu u digitalnom obliku, puno ih je teže otuđiti korisniku. Točnije, samo fizičkim otuđivanjem kartice se može narušiti njezina tajnost. U tom slučaju se lako izdaje nova kartica, obzirom da su troškovi zanemarivi. Kao i kod autentikacije uporabom tokena, ova metoda se obično kombinira s uobičajenim načinom prijave koristeći lozinke.

1.2.5. Izvan pojasna autentikacija

Izvan pojasna autentikacija (engl. *Out-of-Band Authentication*) podrazumijeva bilo koju metodu provjere identiteta korisnika koja za provjeru koristi odvojeni kanal od onoga za izvođenje transakcije. Ovaj oblik autentikacije se često koristio u bankovnim sustavima kod provođenje transakcija većeg iznosa. Na primjer, prilikom prijenosa velike količine sredstava s jednog računa na drugi, djelatnik banke bi telefonskim pozivom potvrdio da vlasnik računa žali odobriti transakciju. Potvrda transakcije se radila u nekoliko koraka. Prvo se korisnika autenticira temeljem njegovo znanja. Na primjer, traži se lozinka ili podatak koji je poznat samo legitimnom korisniku. Osim toga, traži se da potvrdi iznos transakcije.

1.2.6. Analiza IP adrese

Svako računalo na globalnoj mreži Internet ima jedinstvenu IP adresu. Jedan način provjere identiteta korisnika može se zasnivati na provjeri vlasnika IP adrese. No, IP adrese se trenutno ne vežu uz korisnikov identitet jer ih u IPv4 protokolu nema dovoljno kako bi se svakom korisniku dodijelila jedna adresa. Ipak, moguće je neke informacije o korisniku prikupiti analizom IP njegove adrese. Neke organizacije nude programsku

potporu kojom se omogućuje identifikacija određenih značajki IP adrese. Na primjer, okvirna lokacija IP adrese, anonimni proxy poslužitelji, nazivi domena te druge značajke koje se zajedno nazivaju IP inteligencija (engl. *IP Intelligence*). Programska potpora analizira tako prikupljene podatke i provjerava odgovaraju li uobičajenom ponašanju korisnika. Točnije, provjerava se odgovaraju li te značajke korisnikovom profilu ponašanja. Naravno, prethodno je potrebno definirati korisnikov profil kako bi se mogao ispravno provjeriti. Izrada profila se radi analizom korisnikovih sjednica i nakon svake prijave postaje sve precizniji. Ova metoda se često uvodi kao dodatna provjera autentičnosti korisnika, a ne kao primarna metoda autentikacije.

Jedna od najkorisnijih metoda analiza IP adrese je geopozicijsko lociranje korisnika. Određivanje geopozicijske lokacije korisnika se utvrđuje analizom vremena koje je potrebno da se uspostavi komunikacije. Točnije, da mrežni paket stigne s izvorišta do odredišta. Tako dobiveno vrijeme se pretvara u kibernetsku udaljenost. Zatim se ta udaljenost uspoređuje s udaljenostima za poznate lokacije i određuje približna pozicija korisnika. Određivanje lokacije korisnika je korisno onda kada se unaprijed znaju legitimne lokacije na kojima se korisnik smije ili ne smije nalaziti. Na primjer, ako se zaposlenik pokuša prijaviti na sustav s lokacije koja je bitno udaljena od sjedišta organizacije, možda je riječ o računalnom napadu. Naravno, ovakva sigurnosna politika je prihvatljiva samo onda ako ne postoji scenarij u kojemu legitiman korisnik može pristupati sustavu za druge udaljen lokacije.

1.2.7. Uzajamna autentikacija

Većina sustav radi autentikaciju korisnika, ali se sustav ne autenticira korisniku. Uzajamna autentikacija podrazumijeva autentikaciju korisnika sustavu i autentikaciju sustava korisniku. Na taj način obje strane znaju da zaista komuniciraju sa željenim stranama. Potreba za uzajamnom autentikacijom pojavila se zbog sve većeg broja phishing napada [60]. Kada se sustav ne autenticira korisniku, napadač se može korisniku predstaviti kao legitiman servis i tako otuđiti povjerljive informacije. Uzajamna autentikacija se najčešće postiže uporabom digitalnih certifikata. No, zbog česte nepažnje korisnika i ova metoda se može zaobići. Točnije, korisnik mora ručno pregledati certifikat i prihvatiti ga. Kako većina korisnika ne obraća pažnju prilikom prihvaćanja digitalnih certifikata, napadač može podmetnuti vlastiti certifikat i time se predstaviti kao odredišni sustav. Uzajamna autentikacija se detaljnije opisuje u dodatnoj literaturi pod [61].

1.3. Standardi za autentikaciju korisnika

Jedan od vodećih standarda za elektroničku autentikaciju korisnika predstavljaju preporuke organizacije NIST [48]. Te preporuke nadopunjuju prethodno uspostavljene kriterije iz dokumenta za definiranje kvaliteta elektroničke autentikacije korisnika u državnih agencijama. Točnije, dokument pod oznakom OBM M-04-04 [49]. OBM definira željenu razinu osiguranja o grešaka koje mogu nastati prilikom autentikacije korisnika, ovisno o njezinim posljedicama za sustav. Razina osiguranja raste proporcionalno posljedicama u slučaju greške prilikom autentikacije. Dokument OBM M-04-04 definira ukupno pet koraka koje bi agencije trebale poduzeti prilikom odabira metode autentikacije korisnika.

1. Provesti postupak procjene rizika za sustav državne agencije
2. Mapirati prepoznate rizike na odgovarajuće razine osiguranja
3. Odabrati tehnologiju autentikacije temeljem tehničkih preporuka
4. Potvrditi da se implementacijom odabrane tehnologije autentikacije postigao željena razina osiguranja
5. Periodički preispitati čitav informacijski sustav kako bi se utvrdili mogući sigurnosni ispadi ili ranjivosti

NIST preporuke [48] definiraju upute za implementaciju koraka 2 iz OBM metodologije. Nakon što se provede procjena rizika i njihovo mapiranje, potrebno je odabrati odgovarajuće tehnologije koje će zadovoljiti tehničke uvjete za željenu razinu sigurnosti. Točnije, dokument opisuje postupak provjere identiteta i registracije novih korisnika, uporabu tokena za autentikaciju te mehanizme kojima se oni održavaju i upravljaju. Dodatno, definiraju se protokoli za podršku autentikacije korisnika te mehanizmi potvrde autentikacije korisnika. Ovo je korisno ukoliko se rezultat autentikacije treba slati drugim stranama. Navedeni dokumenti razlikuju ukupno četiri razine osiguranja sigurnosti. U nastavku se opisuju okvirne značajke svake razine, a više informacija može se pronaći u izvornim dokumentima pod [48] i [49].

- **Razina 1** – ne obavlja se provjera stvarnog identiteta korisnika. No, mehanizam autentikacije osigurava da se radi o istom korisniku koji je sudjelovao u prethodnim

transakcijama. Omogućuje uporabu velikog broja autentikacijskih tehnologija te omogućuje uporabu tokena koji su namijenjeni u razinama 2, 3 i 4. Uspješna autentikacija korisnika podrazumijeva da će korisnik putem sigurnog autentikacijskog protokola dokazati kako posjeduje i upravlja tokenom. Lozinke i drugi tajni podatci se ne prenose mrežom na razini 1. No, ova razina ne nalaže uporabu kriptografskih metoda za sprječavanje prisluškivanja i pogađanja. Na primjer, dozvoljena je uporaba jednostavnih protokola za razmjenu lozinki (engl. *Challenge-response*). Ukoliko napadač prisluškivanje uspije otkriti poruku protokola, moći će jednostavnim napadom pogađanja otkriti tajnu informaciju. Razina 1 zahtjeva zaštitu informacija za dokazivanje identiteta od napada ponavljanja (engl. *Replay Attack*) te napadima izmjene.

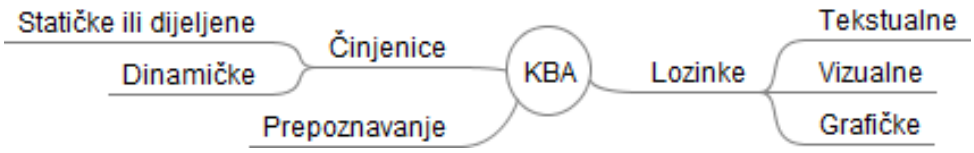
- **Razina 2** – koristi se samo jedan faktor za autentikaciju korisnika. No, na ovoj razini se obavlja provjera stvarnog identiteta. Potrebno je priložiti određene identifikacijske materijale ili informacije. Može se koristiti velik broj autentikacijskih mehanizama i tehnologija. Na primjer, unaprijed dogovorene tajne informacije, tokeni, izvan pojasni (engl. *Out of band*) tokeni i drugo. Također, dozvoljeno je korištenje svih metoda autentikacije s razine 3 i 4. Prilikom autentikacije, od korisnika se zahtjeva da dokaže kako vlada tokenom. Potrebno je onemogućiti napade prisluškivanja, ponavljanja paketa, pogađanja te otimanja sjednice. Također, korišteni protokoli moraju djelomično biti otporni na napade ubacivanja posrednika (engl. *Man-in-the middle*). Prema NIST specifikaciji, protokol je djelomično otporan na napad ubacivanjem posrednika ako se autenticira samo poslužitelj.
- **Razina 3** – podrazumijeva uporabu višestrukih faktora prilikom autentikacije korisnika. Točnije, potrebno je koristiti barem dva faktora za autentikaciju. Na ovoj razini potrebno je detaljnije obraditi priložene identifikacijske materijale. Razina 3 se zasniva na kriptografskim protokolima koji omogućuju da korisnik dokaže kako posjeduje određene tokene. Dozvoljena je uporaba kriptografskih tokena s višestrukim faktorima (engl. *Multi-factor Software Cryptographic Tokens*). Također, dozvoljeno je korištenje svih autentikacijskih mehanizama s razine 4.
- **Razina 4** – najviša razina osiguravanja autentikacije korisnika. Inicijalnu registraciju, odnosno, provjera identifikacijskih materijala se radi u živo. Koriste se isti mehanizmi kao na razini 3. No, dozvoljeno je koristiti isključivo token uređaje

koji zadovoljavaju FIPS (engl. *Federal Information Processing Standard*) 140-2 razinu 2 ili više. Potrebno je spriječiti sve moguće napade na protokole i mehanizme autentikacije korisnika. Na primjer, potrebno je u potpunosti spriječiti napade ubacivanja posrednika.

2. Autentikacija temeljena na korisničkom znanju

Kako je opisano u poglavlju 1, jedan od faktora autentikacije korisnika predstavlja znanje. Cilj ovog rada je analizirati i ocijeniti postojeće metode autentikacije temeljem korisničkog znanja (engl. *KBA – Knowledge-Based Authentication*). Slika 1. prikazuje tipove KBA metode autentikacije kako su definirane u radu pod [62]. U nastavku ovog poglavlja se analiziraju postojeće metode autentikacije temeljene na korisničkom znanju. Trenutno postoje tri različite vrste autentikacije korisničkim znanjem. Točnije, autentikacija korištenjem lozinki, činjenica i prepoznavanjem. U ovom radu se ne razmatra autentikacija prepoznavanjem. U poglavlju 5.2 se predlaže izrada nove metode klasifikacije metoda autentikacije temeljenih na znanju.

Postoje nekoliko definicija koje formalno opisuju KBA metodu autentikacije. No, kako korisničko znanje obuhvaća velik broj različitih metoda, definicije su se mijenjale. Zajedničko svojstvo im je to da korisnik uvijek koristi vlastito znanje kako bi odgovorio na pitanja sustava. Osnovna definicija autentikacije temeljem znanja podrazumijeva verifikaciju temeljem informacija koje je korisnik unaprijed podijelio sa sustavom. Ovo je osnovna definicija autentikacije dijeljenim znanjem. S obzirom na to da se ovom metodom uvijek postavljaju unaprijed dogovorena pitanja, autentikacija dijeljenim znanjem se naziva i statička autentikacija znanjem. Novija definicija autentikacije znanjem proširuje moguće izvore informacija koje se koriste za autentikaciju. Točnije, autenticira se obavlja temeljem referentnih informacija vezanih za korisnika. Uspješna autentikacija ovisi o konzistentnosti informacija koje korisnik unosi prilikom prijave i postojećih informacija u sustavu. Najnovija definicija metode autentikacije temeljem korisničkog znanja podrazumijeva da ne postoji nikakav prethodno uspostavljeni odnos između sustava i korisnika. Ova metoda se naziva dinamička autentikacija korisnika temeljem znanja. Trenutno ne postoji jedinstvena definicija KBA metode autentikacije. Autentikacija temeljem znanja je područje koje se neprestano razvija i čija se definicija često mijenja. Razlog tome je upravo raznolikost metoda uporabe korisničkog znanja za autentikaciju. Ljudski um ima različite sposobnosti i vještine, a ljudi se međusobno razlikuju po onome što znaju i kako razmišljaju. Upravo takva raznolikost daje povoljna svojstva raznim metodama autentikacije koje se temelje na znanju.



Slika 1. KBA metode autentikacije

Organizacija FFIEC (engl. *Federal Financial Institutions Examination Council*) je 2005. godine izdala izvještaj u kojemu si iznesene službene preporuke za autentikaciju korisnika u bankovnim sustavima [2]. Nakon toga, 2011. godine izdano je proširenje na izvještaj iz 2005. godine [30]. U proširenju FFIEC opisuje uporabu KBA metoda autentikacije kod provjere identiteta korisnika u bankovnim sustavima. Prilikom opisivanja pojedinih metoda autentikacije, u izvještaju se koristi nekoliko srodnih pojmova. U ovom radu se isključivo koriste pojmovi statička i dinamička KBA. Ostali postojeći pojmovi ne predstavljaju dodatan grananja već sinonime. Ovo je ujedno dokaz kako postoji potreba za usvajanje formalne terminologije na području autentikacije temeljene znanjem. Radi cjelovitosti, u nastavku se opisuju svi srodni pojmovi. Dodatak izvještaju iz 2005. godine se može pronaći u dodatnoj literaturi pod [31].

- **Statički KBA** (engl. *Static KBA*) – metoda autentikacije temeljena na znanju koja se zasniva na unaprijed dogovorenim tajnim informacijama. Oslanjaju se na informacije koje se prikupljaju nakon što je uspostavljen odnos s korisnikom. Na primjer, korisnika mora odabrati neko tajno pitanje i priložiti vlastiti odgovor. Prilikom autentikacije, korisnik mora ponovno odgovoriti na to pitanje kako bi dokazao svoj identitet.
- **Dinamički KBA** (engl. *Dynamic KBA*) – zasniva se na izmjeni informacija koja nisu unaprijed dogovorena, a na koja samo legitiman korisnik može ispravno odgovoriti u razumnom vremenu. Prilikom prijave, korisnik obično mora unijeti svoje ime i prezime, datum rođenja, mjesto stanovanja te drugo. Ti podatci se koriste kako bi se postavila pitanja na koja može odgovoriti samo onaj korisnik kojemu stvarno pripadaju predani podatci.
- **Izvan lisnička pitanja** (engl. *Out-of-Wallet Questions*) – pojam je nastao ilustracijom načina na koji se pitanja mogu proizvesti prilikom autentikacije. Zamislimo da se skup svih mogućih pitanja i odgovora nalaze u jednom skupu na sustavu. Neka se ovaj skup naziva lisnica. Ako sustav prilikom autentikacije

korisnika postavlja pitanja koja se ne nalaze u njegovoj lisnici, govorimo o izvan lisničkom pitanju. Točnije, radi se o dinamičkom KBA.

- **Dijeljene tajne** (engl. *Shared Secrets*) – označava informaciju koja je poznata samo sustavu koji obavlja autentikaciju i korisniku. Najčešće se pojavljuju u obliku odgovora na pitanja koja sustav postavlja korisniku. Na primjer, sustav pita korisnika koja mu je najdraža boja ili kako se zove grad u kojemu je odrastao. U osnovi, predstavlja statički KBA.
- **Autentikacija pitanjima** (engl. *Challenge Questions*) – pojam koji FFIEC koristi za opisivanje pitanja kojima sustav provjerava identitet korisnika kada on zaboravi lozinku. Radi se o statičkom KBA, odnosno dijeljenim tajnama.
- **Sofisticirana pitanja za provjeru** (engl.*Sophisticated Challenge Questions*) – FFIEC uvodi novi pojam za pitanja koja se odnose na dinamičku KBA.
- **Upitnik identiteta** (engl. *ID Quiz*) – način opisivanja pitanja koja se postavljaju u sklopu autentikacije dinamičkim KBA. Upitnik se sastavlja od pitanja s višestrukim odabirom. Korisnik mora odgovoriti na postavljena pitanja, a sustav ocjenjuje jesu li postavljena pitanja ispravno odgovorena.

2.1. Autentikacija temeljena na lozinkama

Lozinke su najčešće korištena metoda autentikacije korisnika, a zasnivaju se na faktoru korisničkog znanja. Većina sustava koristi tekstualne lozinke za autentikaciju korisnika. Ova metoda je najjednostavnija za implementaciju i održavanje. No, nudi bitno manju razinu sigurnosti. Danas postoji velik broj napada na tekstualne lozinke, a većina njih se može u potpunosti automatizirati.

Obzirom na brojne nedostatke uporabe tekstualnih lozinki za autentikaciju korisnika, razvijene su drugi oblici lozinki. Točnije, razvijene su vizualne i grafičke lozinke. Ljudski um bolje pamti slike nego niz znakova. Dodatno, slike su neovisne o jeziku govora i time se otežava njihovo pogađanje. Također, računala teško raspoznaju slikovne podatke čime se otežava automatizirano pogađanje. Grafičke i vizualne lozinke imaju određene prednosti u odnosu na tekstualne lozinke. No, dijele i neke osnovne mane tekstualnih lozinki. U nastavku se opisuje sve tri metode autentikacije lozinkama.

Neovisno o tipu lozinke, postupak autentikacije lozinkom je identičan. Korisnik dokazuje svoj identitet tako da šalje vlastitu lozinku, a sustav mora prepoznati je li priložena lozinka ispravna. Odnosno, sustav i korisnik moraju podijeliti znanje o tajnoj lozinki kako bi se korisnik uspješno autenticirao. U tu svrhu se obično koristi registracija korisnika. Naime, prilikom postupka otvaranja novog korisničkog računa na sustavu, korisnik odabire lozinku.

2.1.1. Tekstualne lozinke

Tekstualne lozinke podrazumijevaju uporabu tajnog niza znakova koji je poznat samo korisniku i sustavu koji obavlja autentikaciju. Tekstualne lozinke se obično sastavljaju od velikih i mali slova, brojeva, interpunkcijskih znakova te posebnih znakova. Najkvalitetnije lozinke koriste sve skupove navedenih znakova i duljina im je obično 8 do 14 znakova. Dodatno, najbolje lozinke se smatraju one koje su sastavljene nasumičnim odabirom navedenih znakova. No, korisnici često ne odabiru takve lozinke s obzirom na to da se one teško pamte. Puno je jednostavnije zapamtiti riječi specifične za ljudski jezik. Na primjer, lozinka *krevet233!/* se puno lakše pamti nego potpuno nasumična lozinka poput *Sdjf4#qT23%E*.

Autentifikacija korisnika tekstualnom lozinkom smatra se najneprikladnijom metodom provjere identiteta. U psihologiji je poznata činjenica da ljudski um sporo i nepouzdano obrađuje i pamti nasumične nizove znakova. Istraživanja poput [21] i [22] potvrđuju ove činjenice. Dodatno, istraživanje dostupno pod [23] pokazuje kako ljudski lakše pamte nizove znakova ako ih mogu asocirati uz neko poznato značenje ili događaj. Problem u ovoj metodi autentikacije je što ljudi imaju poteškoće s odabirom i pamćenjem kvalitetnih lozinki. Ako su lozinke jednostavne ili imaju neko značenje, mogu se lako napasti brojnim programskim alatima. S druge strane, ako su pre složene i nasumične teško se pamte te ih korisnici često moraju zapisivati. U svakom slučaju, sigurnost sustava se degradira.

Ipak, zbog velike praktičnosti ova metoda se primjenjuje u većini informacijskih sustava. Općenito, autentifikacija korisnika uporabom metode dijeljenog znanja ima velike nedostatke. Na primjer, zloćudni korisnik mora otuđiti dijeljenu informaciju kako bi ukrao identitet legitimnog korisnika. Dodatno, postoje veliki problemi u odabiru kvalitetnih tekstualnih lozinki. Korisnici često iz praktičnih razloga odabiru lozinke koje zloćudni korisnici mogu lako pogoditi. Drugi veliki nedostatak autentifikacijom lozinki je njihova pohrana na sustavu. Naime, kako bi sustav potvrdio identitet korisnika mora pohraniti lozinku radi kasnije usporedbe. Ukoliko sustav pohranjuje lozinke na nesiguran način, vješt napadač moći će otuđiti lozinke korisnika napadom sustava. Time se dokazuje kako sigurnost ove metode autentikacije ne ovisi samo o korisnicima već i o sustavu koji obavlja njihovu autentifikaciju. Kako bi se očuvala tajnost lozinke prilikom njezine pohrane na sustavu, razvijene su metode njezina šifriranja. Točnije, uporabom jednosmjernih funkcija za stvaranje sažetaka (engl. *One-way Hash Function*) pohranjuje se jedinstvena reprezentacija tekstualne lozinke. Tako dobiveni sažetak se pohranjuje na sustavu kako se korisnikova lozinka ne bi mogla očitati. No, kako korisnici često biraju predvidljive lozinke, one se i dalje mogu otkriti pogađanjem. U općem slučaju to su napadi rječnikom (engl. *Dictionary Attack*) i napadi iscrpljivanjem (engl. *Brute Force Attack*).

Resursi koji su potrebni za izvođenje napada grubom silom rastu eksponencijalno s povećanjem veličine lozinke. Dakle, povećavanjem veličine lozinke dva puta potrebno je ostvariti četiri puta više operacija prilikom napada grubom silom. Ipak, zahvaljujući velikoj resursnoj moći današnjih računala, ovaj oblik napada je često uspješan. Pogađanje lozinki je idealan zadatak za paralelna ili raspodijeljena okruženja. Naime, prilikom raspoređivanja zadataka svaki proces dobiva određeni raspon znakova koje treba provjeriti. Prilikom izvođenja, procesi ne moraju međusobno komunicirati niti se usklađivati. Nakon

što završe s obradom, procesi javljaju rezultat izvođenja glavnom procesu koji je zadužen za upravljanje. Takva vrsta zadataka se naziva trivijalno paralelni (engl. *Embarrassingly Parallel*) zadatci. Napad rječnikom označava tehniku pogađanja lozinki pretraživanjem najvjerojatnijih kombinacija znakovnih nizova. Za razliku od napada grubom silom, ne isprobavaju se sve moguće kombinacije. Osnovna razlika je uporaba unaprijed proizvedenog rječnika najvjerojatnijih lozinki. Točnije, rječnik predstavlja iscrpan popis riječi proizvoljne duljine koji se proizveden isključivo s ciljem bržeg pogađanja korisničkih lozinki. Napadi rječnikom su često uspješni jer mnogi korisnici često odabiru lozinke koje su kraće duljine ili se lako predviđaju. Na primjer, često se koriste uobičajene riječi iz rječnika te im se dodaju brojevi vezani uz specifične datume. Više informacija o ovim oblicima napada može se pronaći u dodatnoj literaturi pod [3] i [4].

Jedan od popularnijih načina otežavanja napada rječnikom naziva se *Salt*. Metoda se zasniva na dodavanju nasumičnog niza znakova ispred lozinke prije nego što se proizvede njezin sažetak. Nasumični niz znakova i sažetak se zatim pohranjuju na sustav. Ako napadač uspije očitati sažetak i nasumični niz znakova i dalje može izvesti napad pogađanjem i otkriti stvarnu vrijednost sažetka. No, vrijeme pogađanja se bitno povećava. Ukoliko se koristi napad rječnikom, napadač mora proizvesti novi rječnik tako da svakom unos doda pročitani nasumični niz znakova i proizvede novi sažetak. Kako rječnici obično imaju preko milijun zapisa, ova operacija traje i time produljuje vrijeme napada.

Osim raspodijeljenih sustava, razvijaju se sklopovlja koja su pogodna za izvođenje napada grubom silom. Jedno od tih sklopovlja predstavljaju grafički procesori koji svojom snagom postavljaju sve veće i veće kriterije za duljine lozinki. Zahvaljujući širokoj dostupnosti i prihvatljivoj cijeni, smatraju se najpogodnijim sklopovljem za izvođenje napada grubom silom. Moderni grafički procesori sastoje se od velikog broja procesorskih jezgri koji ih čine pogodnijim za izvođenje paralelnih zadataka. Neki grafički procesori imaju i do 100 procesorskih jedinica, što ih čini znatno pogodnijih za izvođenje paralelnih operacija nego obični procesori. Drugo sklopovlje predstavlja tehnologija FPGA (engl. *Field-Programmable Gate Array*). Pogodni su za izvođenje napada grubom silom zahvaljujući mogućnosti paraleliziranja zadataka. No, ističu se i energetskom učinkovitošću prilikom obavljanja složenih zadataka. Broj procesorskih jedinica u FPGA sklopovima mjeri se i u tisućama. Na primjer, COCACOBANA FPGA grozd koristi napajanje od 600W, a za određene algoritme postiže brzinu od 2.500 umreženih računala. Više o uporabu FPGA sklopova može se pronaći u dodatnoj literaturi pod [5].

2.1.2. Vizualne lozinke

Vizualne lozinke sastavljene su od niza slika koji je poznat samo korisniku i sustavu koji obavlja autentikaciju.

Neki korisnici dobro pamte lica drugih osoba. Jedna od metoda autentikacije vizualnim lozinkama, zasniva se na slikama lica ljudi. Točnije, prilikom registracije korisnik odabire slike lica ljudi koje mu sustav ponudi iz određenog skupa slika. Tako odabrani niz slika lica predstavlja korisnikovu lozinku. Korisnik prilikom prijave mora istim redoslijedom odabrati slike lica kako bi se autenticirao. Primjer sustava koji radi na ovom principu je Passfaces. Prilikom prijave, Passfaces korisniku prikazuje devet slika lica, ali samo jedna od tih lica pripada korisnikovoj lozinki. Korisnik mora odabrati ispravnu sliku, a nakon toga se pojavljuje novih devet lica od kojih opet samo jedna pripada korisnikovoj lozinki. Ovo se ponavlja sve dok korisnik ne označi sve slike koje čine lozinku. Sustav Passfaces koristi ukupno četiri slike lica za stvaranje lozinke. Sustav se temelji na činjenici da ljudi puno lakše pamte slike ljudi nego bilo koje druge vrste slika. Ovo posebno vrijedi ako korisnik može samostalno stvoriti svoju lozinku s vlastitim slikama. Passfaces je detaljnije analiziran u dodanoj literaturi pod [8] i [9].

Slika se mogu proširiti tako da ne uključuju samo lica ljudi, već dodatne svakodnevne objekte, životinje, aute i drugo. Ovakvom izmjenom, korisnik si može zamisliti priču, te ju složiti putem slika. Tako poredane slike čine korisnikovu lozinku. Sustav Story Scheme autenticira korisnike upravo na ovaj način. Ova metoda se detaljnije opisuje u [10].

Jedan od problema vizualnih lozinki je rukovanje slikama na sustavu koji obavlja autentikaciju korisnika. Točnije, potrebno je odrediti način na koji će se korisnikove lozinke pohraniti na sustavi te kako će se provjeriti autentičnost korisnika. Sustav Deja Vu slike grupira u portfeljima. Prilikom registracije, korisnik stvara svoj vlastiti portfelj sa slikama koje bira iz velikog skupa slika. Tako odabrane slike se pohranjuju na sustav. Prilikom prijave, sustav korisniku prikazuje skupa slika od kojih neke pripadaju njegovom portfelju, a neke ne. Korisnik mora odabrati sve slike koje se nalaze u njegovom portfelju. Važno svojstvo Deja Vu sustava je što se ne koriste slike ljudi ili objekata kao u prethodno opisanim sustavima. Koriste se slike zasnovane na radu Andreja Bauera naziva *Gallery of random art [11]*. Riječ je o apstraktnim slikama koje se teško mogu riječima opisati. Kada korisnik radi vlastiti portfelj, sustav putem matematičke formule proizvodi slike koje su jedinstvene za trenutnog korisnika. Matematička formula prima početno sjeme (engl. *Initial*

Seed) pomoću kojeg se izračunavaju boje svakog piksela na slici. Za svakog korisnika se koristi drugačije početno sjeme. Tako proizvedene lozinke su idealne za pohranu. Naime, potrebno je pohraniti samo početno sjeme, a ne čitave slike. Prilikom prijave sustav pomoću početnog sjemena proizvodi slike i tako radi autentikaciju korisnika. više informacija o sustavu Deja Vu može se pronaći u dodatnoj literaturi pod [12].

Jedan od prvih prijedloga implementacije vizualnih lozinki koristio je algoritme za vizualizaciju sažetaka (engl. *HVA – Hash Visualization Algorithm*). Više o tom radu može se pronaći u dodatnoj literaturi pod [6]. Predložena metoda autentikacije se također zasniva na radu Andreja Bauera (*Gallery of random art*) i ima neke sličnosti sa sustavom Deja Vu. Osnova ove metode je implementacija sigurnih algoritama za vizualizaciju sažetaka. Oni na ulaz primaju niz znakova, a na izlazu daju sliku točno određenih dimenzija. HVA algoritmi su vrlo slični jednosmjernim funkcijama u kriptografiji, te imaju slične karakteristike. Točnije, podudaraju se u uvjetima jednosmjernosti i kolizija. Jednosmjernost kod HVA algoritama podrazumijeva da se iz dobivene slike nikako ne može dobiti izvorni niz znakova. Uvjet na kolizije podrazumijeva da ne postoje dva različita niza znakova koji bi proizveli identičnu sliku. Dodatno, uvode se dodatni uvjeti na slike proizvedene HVA algoritmima. Ljudi lako mogu razaznati slike na kojima se pojavljuju geometrijski oblici. Ako HVA algoritam proizvede sliku na kojoj nema geometrijskih oblika ili koja predstavlja bijeli šum (engl. *White noise*) potrebno ju je odbaciti. Prema naputku autora [6], prepoznavanje takvih slika se radi Fourierovim transformacijama.

Slična metoda rukovanja slikama se koristi u sustavu Picture Password [13]. Korisnik bira kategoriju slika pomoću kojih želi složiti svoju lozinku. Na primjer, kategorija slika mogu obuhvaćati životinje, planine, nautika, sport i drugo. Nakon što se odabere kategorija, potrebno je složiti niz slika koje će se koristiti kao lozinka. Svaka slika se preslikava u jedno slovo abecede. No, korisnik ne mora pamtiti tako dobiveni znakova već samo slike koje je odabrao i redosljied biranja. Ovakvo preslikavanje je vrlo slično tekstualnim lozinkama. Ukoliko napadač uspije presresti poruku prijave može otkriti korisnikovu lozinku. Također, kako se proizvedena tekstualna lozinka mora pohraniti na sustavu, ovaj pristup ima iste ranjivosti kao i tekstualne lozinke.

Upravljanje velikom količinom slika opterećuje sustav. Slike zauzimaju puno više prostora od tekstualnih lozinki. Čak i u slučaju kada se slike proizvode matematičkom formulom stvara se opterećenje na sustav. Iako se takve slike lako pohrane, potrebno ih je prilikom

svake prijave proizvesti. Efikasnija metoda autentikacije vizualnim lozinkama podrauzmijeva uporabu samo jedne slike za korisnika. ako na slici postoji velika količina objekata, korisnik može složiti lozinku odabirom nekih objekata sa slike. Na primjer, panoramske slike gradova obično sadrže velik broj objekata. Prilikom registracije korisnik odabire objekte sa slike po volji. Kod prijave korisnik mora iste objekte ponovno odabrati kako bi se autenticirao. Problem kod ovog pristupa je što se svi objekti na slici moraju nekako identificirati. Dodatno, korisnik neće biti u stanju uvijek isti piksel odabrati. Potrebno je osigurati određenu toleranciju na preciznost odabira objekta. Ovaj pristup je pogodan jer olakšava upravljanje slikama. Dodatno, ako slike sadrže dovoljan broj objekata, moguće kombinacije lozinki su daleko veće od tekstualnih. Sustavi Passlogix i Passpoits [14] rade na ovom principu.

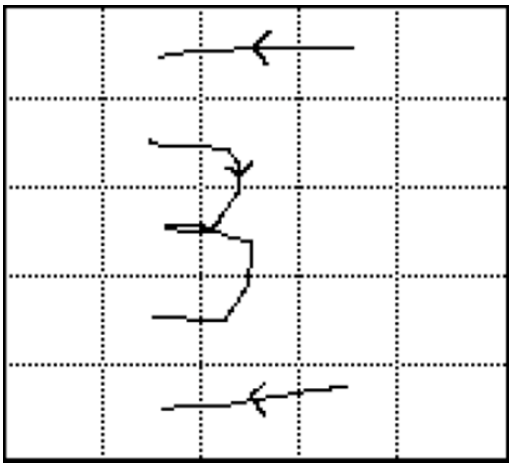
Uporaba tekstualnih lozinki je iznimno rasprostranjena danas, a postoje različite metode kojima se pokušavaju zaštititi. Na primjer, većina sustava ne prikazuje tekstualne lozinke prilikom unosa. Na UNIX/Linux sustavima se obično ne prikazuje ništa, dok se na web formama prikazuju zvjezdice umjesto stvarnih znakova. Takvo skrivanje vizualnih lozinki nije moguće jer se oslanjaju upravo na prepoznavanju slika. Odnosno, korisnik mora vidjeti sliku koja čini njegovu lozinku kako bi ju odabrao. Samim time, vizualne lozinke su ranjive napadima gdje napadač može vidjeti korisnikov ekran. Ovaj problem se zaobilazi dodatnim kombiniranjem slika i njihovih pozicija. Na primjer, sustav proizvede niz slika od kojih samo tri čine korisnikovu lozinku. Korisnik ne odabire slike direktno već se odabir radi indirektno putem određenih okvira. Točnije, korisnik mora okvir pomaknuti na mjesto gdje se nalaze njegove lozinke. Druga metoda je da korisnik mora pozicionirati neki drugi geometrijski lik, recimo pravac, u odnosu na slike koje čine njegovu lozinku. Iako se ovakvim pristupom otežava krađa lozinki gledanjem u korisnikov ekran, bitno se otežava postupak prijave za legitimne korisnike.

Istraživanje dostupno pod [7] pokazalo je kako vizualne lozinke nisu sigurnije od tekstualnih lozinki. Naime, korisnici odabiru mali broj slika (obično 4 ili 5) i time stvaraju lozinke koje se lako pogađaju. Dodatno, pronađen je povezanost kod odabira vizualnih i tekstualnih lozinki. Korisnici koji koriste tekstualne lozinke dulje 4-6 znakova, prilikom odabira vizualne lozinke odabrati će samo 4 slike. Korisnici koji koriste tekstualne lozinke duljine 8-9 znakova obično odaberu 6 slika za svoje vizualne lozinke.

2.1.3. Grafičke lozinke

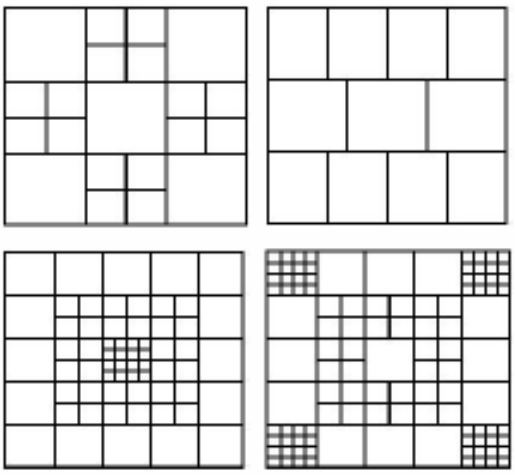
Grafičke lozinke podrazumijevaju uporabu slika koje korisnik samostalno nacrta. Točnije, umjesto da odabire svoju lozinku iz niza ponuđenih slika, korisnik mora nacrtati određenu sliku koja čini njegovu lozinku. Naravno, crtanje slike putem miša ili drugih uređaja za pokazivanje je neprecizno i korisnik neće moći svaki puta reproducirati identičnu sliku. Iz tog razloga se ploha za crtanje dijeli na manja polja, od kojih svako ima određeni indeks. U osnovnom slučaju, takva podjela čini matricu. Slika 2. prikazuje primjer grafičkih lozinki s jednostavnom podjelom plohe na manja polja. Primjer se zasniva na Draw-a-Secret projektu koji je opisan u dodatnoj literaturi pod [15]. Osnovna ideja se zasniva na prepoznavanju polja u kojima korisnik crta svoju sliku. Lozinka se stvar bilježenjem kretanja pokazivača kroz polja prilikom izrade slike. Točnije, polja se bilježe svojim koordinatama u matrici. Na primjer, prvo polje bi bilo (0,1), polje odmah desno bi bilo (0,2), dok bi polje ispod prvog bilo (1,0). Također, posebnim znakom se bilježi i kada je korisnik pustio olovku sa pisanje (engl. *Pen-up Event*). Na primjer, oznaka može biti (xx). Ako je korisnik prvo napravio horizontalnu crtu u gornjem dijelu slike s desna na lijevo (Slika 2.), sustav bi zapamtio koordinate zapisom (0,3), (0,2), (0,1), (xx). Prema ovome, lozinku ne čini slika već niz prolaza kroz određena polja na plohi za crtanje. Samim time slika ne mora biti identična, pa čak niti slična izvornoj kako bi se korisnik autenticirao. Važan korak u Draw-a-Secret metodi autentikacije je uporaba jednosmjernih funkcija za pohranu zapisa lozinke. Tako dobiveni sažetak se pohranjuje na sustavu. Prilikom prijave, korisnik crta svoju lozinku i tako dobiveni zapis koordinata se provodi kroz jednosmjernu funkciju. Dobiveni sažetak se uspoređuje sa s pohranjenim sažetkom, te ukoliko su identični, korisnik je autenticiran. U osnovi, ovom metodom je slična tekstualnim lozinkama obzirom da se za autentikaciju koristi niz znakova. Razlika je u tome što se ovako dobiveni niz znakova lakše pamti obzirom da se stvara crtanjem slike. Pogađanje sažetka stvarne lozinke ovisi o mogućem broju zapisa. Točnije, ovisi o složenosti podjele polja na plohi za crtanje. Ako je ploha podijeljena na matricu malog broja redaka i stupaca, pogađanje zapisa će biti lakše nego kada se koristi veći broj stupaca i redaka. Također, jednostavnost pogađanja ovisi i o složenosti i predvidljivosti slike koju korisnik nacrta. Prema istraživanjima provedenim u [16], [17] i [18] Draw-a-Secret metoda autentikacije ima određene ranjivosti. Točnije, ako korisnik crta znakove koji imaju predvidljive karakteristike i koji su simetrični, napadač bi mogao napraviti rječnik najvjerojatnijih kombinacija. Prema tim primjedbama, Draw-a-Secret metoda autentikacije

je proširena. Točnije, ploha za crtanje se više ne dijeli na jednostavne matrice, nego u puno složenije plohe. Slika 3. prikazuje primjer takvih ploha. Njihovo indeksiranje je znatno složenije i time se zapis koordinata dodatno komplicira. Također, ovakve plohe su manje otporne na greške legitimnih korisnika. prilikom prijave, korisnik mora paziti da ostane u granicama manjih polja kako bi se uspješno autenticirao. Naravno, niti ova metoda ne garantira da će korisnik odabrati kvalitetnu grafičku lozinku. Odnosno, da će maksimalno iskoristiti složenost ploha. Više informacija o ovoj metodi može se pronaći u dodatnoj literaturi pod [19]. Detaljnija analiza vizualnih i grafičkih lozinki može se pronaći u dodatnoj literaturi pod [20].



Slika 2. Primjer grafičke lozinke

Izvor: The Design and Analysis of Graphical Passwords [15]



Slika 3. Primjer složenije podjele plohe za crtanje

Izvor: A multi-grid graphical password scheme [19]

2.2. Statički KBA

Statička KBA podrazumijeva uporabu dijeljenog znanja za autentikaciju korisnika. prilikom registracije, korisnik i sustav međusobno dogovaraju kako će se autentikacija obavljati. Točnije, dijele znanje pomoću kojeg će se korisnik kasnije autenticirati. Prilikom prijave, korisnik predočava informaciju koju je prilikom registracije podijelio sa sustavom. Ukoliko se informacija na sustavu podudara s priloženom informacijom, korisnik je autenticiran. Statička KBA najčešće podrazumijeva postavljanje tajnih pitanja korisniku kako bi se potvrdio njegov identitet. Prilikom registracije, sustav postavlja jedno ili više tajnih pitanja na koja korisnik odgovara. Ovakve metode se obično koriste kao mehanizam prijave kada se izgubi lozinka. Mehanizam se često naziva i rezervna autentikacija (engl. *Fallback Authentication*). Na primjer, korisnik se želi prijaviti na sustav bez lozinke. Sustav mu postavlja pitanja na koja unaprijed zna odgovor. Točnije, sustav postavlja pitanje na koje je korisnik odgovorio prilikom registracije. Pitanja se najčešće odnose na neke privatne informacije koje nisu nužno tajne. Na primjer, pitanja o vlastitoj prošlosti, detalji o obitelji poput majčinog djevojačkog prezimena. Ovaj tip pitanja se u literaturi često nazivaju osobnim pitanjima (engl. *Personal Verification Questions*). U kontekstu rezervne autentikacije korisnika, pretpostavlja se da korisnik nije u stanju zapamtiti proizvoljni niz znakova (ili slika). Inače bi se mogao autenticirati uporabom vlastite lozinke. Prema tome, idealno pitanje za provjeru identiteta korisnika je ono na koje korisnik ne mora pamtiti odgovor. Odnosno da pitanje u potpunosti određuje odgovor koji korisnik mora dati. Ovo metoda prebacuje svu odgovornost s korisnika sustava na razvijatelje sustava. Jedini izbor koji donosi korisnik treba se odnositi na koje pitanje želi odgovoriti. Sve ostale odluke treba donijeti razvijatelj.

Jedno od najvažnijih problema u ovom modelu je kako odabrati pitanja za provjeru identiteta. Postoje različite metode kojima se odabiru pitanja. Jedna od najjednostavnijih metoda je uporaba postojećih podataka u sustavu kako bi se provjerila autentičnost korisnika. Ovo se često koristi u bankama, telekomunikacijskim organizacijama i drugim ustanovama koje imaju određeno količinu informacija o korisniku u vlastitom sustavu. Na primjer, banka može postavljati pitanja koja se odnose na način na koji korisnik koristi svoju kreditnu karticu[1]. Slično tome, telekomunikacijske organizacije mogu postaviti pitanja o telefonskim razgovorima korisnika ili internetskom prometu.

Drugi oblik pitanja se odnosi na osobne informacije o korisniku koje nisu nužno tajne, ali se mogu smatrati privatnima. Na primjer, pitanja o mjestima gdje je korisnik stanovao, majčino djevojačko prezime, ime prve ljubavi te druge privatne informacije. Pitanja o osobnim informacijama nisu jedini tip osobnih pitanja kojima se korisnike može autenticirati. Razvijena je metoda autentikacije koja se zasniva na korisnikovom ukusu. U ovoj metodi korisnik treba odrediti koje od ponuđenih stvari ili ideja odgovaraju vlastitim ukusima. Prilikom prijave, korisnik mora ponovno izraziti svoj ukus o određenoj stvari, a sustav će provjeriti odgovara li odgovor korisniku. Ideja se zasnova na činjenici da je jednostavnije zapamtiti vlastiti ukus nego neki drugi odgovor. Na primjer, korisnik će lako zapamtiti da je ljubitelj mačaka ili da ne voli povrće. Više o ovom istraživanju može se pronaći u dodatnoj literaturi pod [25].

Prema današnjim standardima, postoje strogi uvjeti na tip pitanja koja se mogu postaviti korisniku. Naime, zbog sve veće popularnosti društvenih mreža, privatne informacije se sve lakše mogu dohvatiti. Iznenađujuća većina današnjih studenata i apsolvenata ima

[1] Podiže li sredstva s bankomata ili koristi karticu za plaćanje u dućanu. Dodatno, mogu se postaviti pitanja o lokacijama i iznosima koji su naplaćeni putem kartica ili nekih drugih računa koje korisnik ima u banci.

korisnički račun na društvenim mrežama poput Facebook, MySpace, Twitter, LiveJournal i drugima. Ovo je potvrđeno statistikama dostupnim pod [26]. Društvene mreže omogućuju korisnicima izlaganje osobnih informacija na strukturiran način. Informacija poput datuma rođenja, stupnju obrazovanja, informacije p prijateljima i osobnim događajima te drugih privatnih informacija. Dodatno, pojavom alata poput Maltego [28] i Creepy [29] moguće je potpuno automatizirati prikupljanje privatnih informacija s društvenim mreža i drugih izvora dostupnih putem interneta. Creepy predstavlja alat koji prikuplja geoinformacijske podatke vezane za određenog korisnika analizom njihovih profila na društvenim mrežama. Maltego je alat za automatizirano prikupljanje informacija putem interneta. Iako omogućava otkrivanje različitih tipova informacija, neke transformacije su usmjerene isključivo na informacije o korisnicima. Tako prikupljene informacije mogu napadačima omogućiti pristup računu legitimnog korisnika. Prema istraživanju dostupnom pod [24], oko 12% prikupljenih pitanja mogu se odgovoriti uz pomoć informacija s društvenih mreža. Pitanja vezana uz poštanski broj mjesta stanovanja i datum rođenja pripadaju u tu kategoriju. Odgovori na pitanje obiteljska pitanja, poput majčinog djevojačkog prezimena, se obično ne mogu pronaći na društvenim mrežama. Istraživanje dostupno pod [27] je pokazalo da se i ovakva pitanja mogu otkriti putem javno dostupnih informacija na internetu. Istraživanje dostupno pod [24] identificiralo je nekoliko važnih uvjeta koji se moraju zadovoljiti kako bi se osigurala kvaliteta pitanja za autentikaciju. Ti uvjeti se navode u nastavku.

- **Neprimjenjivost** (engl. *Inapplicable*) – neka sigurnosna pitanja jednostavno nisu primjenjiva na velik dio javnosti. Na primjer, pitanja o fakultetskom obrazovanju su primjenjiva samo na ljude koji su pohađali fakultet. Slično tome, pitanja o bračnim partnerima primjenjiva je samo na ljude koji su bili u braku. Pitanja vezana uz srednje ime korisnika je također neprimjenjivo u nekim slučajevima.
- **Lakoća pamćenja** (engl. *Memorable*) – određena pitanja imaju odgovore koje bi rijetko koji korisnik mogao zapamtiti. Iako je teško odrediti kriterij koji strogo određuje koji odgovori se teško pamte, postoje smjernice. Na primjer, rijetko koji korisnik se sjeća prezimena odgajateljice iz vrtića.
- **Dvosmislenost** (engl. *Ambiguous*) – označava pitanja na koja ne postoje jedinstveni odgovori. Na primjer, ako je potrebno navesti fakultete na koje se korisnik prijavio ali nije upisao, neki korisnici će imati više točnih odgovora. Slično kao pitanje o prezimenu profesorice iz matematike.
- **Pogađanje** (engl. *Guessable*) – neka pitanja imaju odgovore koji se lako mogu pogoditi čak i u slučajevima kada napadač nema nikakvih informacija o korisniku. Na primjer, 30% Amerikanaca ulaze u brak između 25 i 30 godina. Slično tome, 20% Amerikanaca se izjasnilo kako im je Abraham Lincoln najdraži predsjednik.

Takva i druga slična pitanja bi se mogla pogoditi temeljem statističkih podataka o nekoj regiji.

- **Mogućnost napada** (engl. *Attackable*) – ako napadač ima pristup životopisu legitimnog korisnika, znao bi reći naziv firme u kojoj je korisnik dobio prvi posao. Informacije o zaposlenju obično nisu tajne. Drugi oblik pitanja koji se lako mogu napasti su imena članova obitelji.
- **Mogućnost automatiziranog napada** (engl. *Automatically attackable*) – u nekim slučajevima se postupak napada može automatizirati. Na primjer, pitanja o godina završetka studija se može automatski otkriti pretraživanjem korisnikovog profila na društvenim mrežama.

Zbog navedenih nedostataka, ova metoda se u većini slučajeva ne koristi kao primarna metoda autentikacije korisnika. Najčešće se koristi kao rezervni mehanizam prijave kada korisnik zaboravlja lozinku. Ponekad se takvom autentikacijom korisniku ne pruža pristup svim resursima dok se drugim metodama ne provjeri autentičnost. Iako postoje prednosti i nedostatci u ovoj metodi autentikacije, jedan aspekt nije uzet u obzir. Naime, većina istraživanja pretpostavlja da će korisnici prilikom registracije dati ispravan i istinit odgovor na pitanje. Ne razmatra se slučaj kada korisnik kao odgovor unese sasvim nasumičan ili lažan odgovor. Obzirom da se odgovori ne bi smjeli pamtiti u izvornom obliku na sustavu, valjanost odgovora nije važna za ispravnu autentikaciju. Štoviše, ako korisnik koristi lažni odgovor, većina napada pogađanjem i prikupljanjem javnih informacije neće uspjeti.

2.3. Dinamički KBA

Jedna od najvećih zabluda nastaje između statičke i dinamičke metode provjere identiteta. Točnije, o upravljanju pitanjima prilikom statičke, odnosno dinamičke KBA. Zbog slabo usklađene terminologije dolazi do čestog poistovjećivanja tih dviju metoda, iako se one bitno razlikuju. Statička KBA je opisana u prethodnom poglavlju. Zbog raznih nedostataka te metode, cjelokupna metoda autentikacija činjenicama je na lošem glasu. Prema [32], postavljanje istih pitanja prilikom registracije i prijave nije prihvatljiva metoda autentikacije. Postoji velik broj pitanja na koja se odgovori mogu lako pogoditi. U osnovi, uporaba korisnikovih odgovora na pitanja za autentikaciju je lošija metoda od uporabe lozinki. Naime, odgovori na neka pitanja nemaju dovoljno velik broj odgovora. Time se

olakšava njihovo pogađanje. Lošim odabirom pitanja stvara se nova ranjivost na sustavu. Zlćudni korisnici mogu puno lakše pogoditi odgovore na neka pitanja nego što mogu pogoditi lozinke. Dodatno, pohrana korisnikovih odgovora je znatno teža. Ukoliko korisnik kao odgovor unese niz znakova *Zagreb,* je li prilikom autentikacije prihvatljivo uzeti u obzir niz *zagreb*. Razlika je u malom početnom slovu. Ukoliko sustav vrši neki oblik pretvaranja znakovnih nizova prije pohrane[2] se odgovor time se smanjuje abeceda mogućih odgovora i time dodatno olakšava pogađanje. Ipak, ako se umjesto odgovora pohranjuje sažetak, prilikom prijave korisnik mora unijeti identičan odgovor kao prilikom registracije.

Kao i s lozinkama, nedostatak statičke metode KBA je njezina predvidljivost. Naime, korisnik zna što će ga sustav pitati i prije nego što pokrene postupak prijave. Dodatno, korisnik unaprijed zna točan odgovor i može ga odati drugim stranama. Dinamičkom KBA pokušava se dodati nepredvidivost u pitanjima koja se postavljaju korisniku. Naime, korisnik ne zna koje će pitanje sustav postaviti dok ne pokrene postupak prijave. Time se sprječava mogućnost prijenosa odgovora na druge korisnike. Dodatno, dinamički KBA se zasniva na pitanjima koja se teško mogu pogoditi u kratkom vremenu. Točnije, pitanja se proizvode dinamički temeljem dostupnih podataka o korisniku. Snaga ove metode se temelji na činjenici da će legitiman korisnik lako moći odgovoriti na postavljena pitanja, dok će zlćudni korisnik teško moći pogoditi točan odgovor.

Glavni izazov u ovom pristupu je metoda proizvodnje dinamičkih pitanja. Naime, potrebno je na temelju određenih podataka proizvesti pitanje koje će samo legitiman korisnik moći odgovoriti. Dodatno, kod svake iduće prijave sustav mora proizvesti novo pitanje. Postoji nekoliko metoda kojima se osigurava proizvodnju dinamičkih pitanja, a razlikuju se o izvoru podataka. Dinamička pitanja se najčešće proizvode temeljem lokalnih informacija organizacije. Na primjer, pružatelji telefonskih usluga prate velik broj podataka o svim svojim korisnicima. Moguće je proizvesti pitanja koristeći se tim lokalnim podatcima. Primjerice, pitanja se mogu postavljati na temelju plaćenih računa, načinu plaćanja, količini ili tipu poziva (lokalni ili roaming) te drugim podatcima. No, podatci ne moraju nužno biti vezani uz korisnika. Rad pod [33] opisuje dinamičku metodu proizvodnje pitanja koja se zasniva na sjedničkim parametrima prethodne korisnikove sjednice. Točnije, nakon uspješne prijave korisnik otvara sjednicu koja se može sastojati od datuma i

[2] Na primjer, pretvara sva velika slova u mala ili suprotno.

vremena prijave, transakcijskim podatcima[3] te broj sjednice[4]. Naravno, takvi podatci često nisu u obliku koji je namijenjen ljudima te se teško pamte. Dodatno, takvi podatci se rijetko kada prikazuju korisniku prilikom rada već se obavljaju u pozadini. Time se otežava njihovo pogađanje. No, potrebno je osigurati pristup tim podatcima legitimnom korisniku. U tu svrhu se koriste alternativni kanali za komunikaciju s korisnikom. Na primjer, elektronička pošta ili SMS (engl. *Short Message Service*) se koriste kako bi dostavili podatke potrebne za autentikaciju. Ovisno o vremenu kada se podatci šalju, korisnik će moći autentikacijske podatke predati drugoj osobi. Točnije, ako se podatci pošalju odmah nakon odjave korisnika, korisnik sve do iduće prijave može predati podataka nekom drugom korisniku. Također, što dulje podatci borave na mediju nezaštićeni (sandučić elektroničke pošte ili mobitel), to je vjerojatnost njihovog otuđivanja veća.

Većina metoda koristi lokalne podatke ili podatke dostupne putem javnih arhiva (engl. *Public records*). Pitanja dostupna putem javnih arhiva se trebaju pažljivo odabrati. Općeniti odgovori na pitanja poput datuma rođenja ili mjesto boravka mogu biti dostupni i zloćudnim korisnicima. Organizacija IDology [34] izrađuje nekoliko programskih rješenja za autentikaciju korisnika dinamičkim KBA. Koriste javne izvore za stvaranje pitanja. Točnije, sustav koji se koristi za autentikaciju korisnika se zove ExpectID [35]. Prilikom prve prijave, korisnik unos svoje ime i prezime, datum rođenja te mjesto stanovanja. Pomoću tih podataka, korisnik se može jedinstveno identificirati u javnim arhivima te se mogu postavljati pitanja na koja samo stvarni korisnik zna odgovor. U praksi ipak postoji određena opasnost napada, ali je ona znatno manja nego kod statičke KBA. Naime, ukoliko zloćudni korisnik ima pristup istim javnim arhivama kao i sustav, postoji mogućnost da će moći ispravno odgovoriti na pitanja u ime legitimnog korisnika. Trenutno ne postoji rad koji dokazuje ili opovrgava sigurnost i pouzdanost ovog sustava. Prema službenim opisima organizacije IDology, sustav ExpectID koristi velik broj javnih baza podataka[5] pomoću kojih se postavljaju pitanja.

[3] Transakcijski podatci obuhvaćaju različite tipove informacija. Na primjer, podatci o operacijama koje je korisnik obavljao prilikom rada.

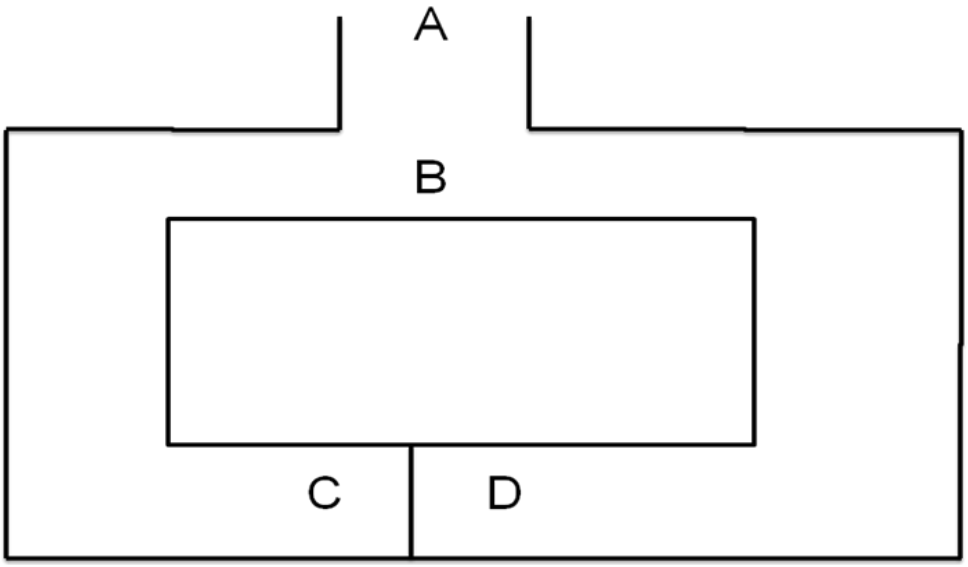
[4] Prilikom prijave na sustav korisnik obično dobiva jedinstveni identifikator kojime se njegovi zahtjevi razlikuju od svih ostalih. Taj identifikator se obično naziva sjednicom.

[5] Prema službenim stranicama, ExpectID pretražuje preko bilijun javnih izvora podataka u potrazi za podatcima o korisniku.

2.4. Dokazi bez poznavanja (engl. Zero-knowledge proofs)

Problem kod uporabe tajnih informacija za autentikaciju je činjenica da ih je potrebno izreći. Prilikom svakog izričaja tajne informacije ona je izložena prisluškivanju. Kako je opisano u prethodnim poglavljima, tajna informacija može biti lozinka, neki odgovor na pitanje, niz slika te drugo. Dokazi bez poznavanja (engl. *Zero-knowledge proofs*) bi trebali jednu stranu u komunikaciji uvjeriti kako druga poznaje određenu tajnu informaciju bez da se ona izreče. Jean-Jacques Quisquater i Louis Guillou su ovu metodu opisali modelom špilje. Slika 4. prikazuje model špilje, a u nastavku je opis. Pretpostavlja se da Peggy želi Viktoru pokazati kako zna tajnu informaciju ali ju ne želi izreći kako ju Viktor ne bi znao. Spilja sa slike ima jedan ulaz i vodi u krug. Između točaka C i D se nalazi pregrada kroz koju nije moguće proći. Samo ako se na pregradu priloži tajna informacija, pregrada se podiže.

1. Viktor stoji na točki A
2. Peggy dolazi do kraja spilje, bilo do točke C ili točke D
3. Nakon što Peggy nestane u spilji, Viktor dolazi do točke B
4. Viktor zahtjeva od Peggy da:
    a. Ili izađe iz spilje kroz stranu C
    b. Ili da izađe iz spilje kroz stranu D
5. Obzirom da Peggy zna tajnu za podizanje pregrade, može napraviti kako Viktor kaže
6. Koraci 1-5 se ponavljaju N puta



Slika 4. Model spilje

Kako bi se teorija dokaza bez poznavanja upotrijebila kod lozinki, stvoreni su ZKPP (engl. *Zero-knowledge password proof*) protokoli. Ovi protokoli se koriste kako bi jednoj strani dokazali kako druga strana poznaje vrijednost neke lozinke, bez da ju izriče. ZKPP protokoli sprečavaju pogađanje tajne informacije te u optimalnom slučaju omogućuje samo jedan pokušaj pogađanja u svakoj iteraciji. Osnova ovih protokola je pretpostavka da obje strane u komunikaciji poznaju određenu tajnu informaciju. Točnije, metoda se zasniva na kriptografiji javnog ključa, ali u ovom slučaju obje strane dijele jedan privatni ključ. Prilikom autentikacije svaka strana dokazuje da pozna tajnu informaciju izvođenjem određenih računskih operacija. Pretpostavka je da se ispravan rezultat može dobiti samo u slučaju kada je poznata tajna informacija. Strogo govoreći, ZKPP se razlikuju od dokaza bez poznavanja po tome što obje strane moraju znati tajnu kako bi se autenticirali. Jedan od prvih ZKPP protokola zvao se EKE (engl. *Encrypted Key Exchange*). Očiti nedostatak u ZKPP protokolima je potreba za inicijalnom razmjenom tajnih informacija. U tu svrhu se obično koristi kriptografija javnog ključa. EKE je detaljno je opisan u dodatnoj literaturi pod [38]. Razvijen je velik broj nadogradnji, alternativa i varijanta ZKPP protokola. Neki standardi se mogu pronaći u dodatnoj literaturi pod [36] i [37].

3. Usporedba tehnika autentifikacije temeljene na korisničkom znanju

U prethodnim poglavljima su opisane postojeće metode autentikacije korisnika temeljem znanja. Postoji velik broj različitih metoda, a svaka od njih ima određene prednosti i nedostatke. Cilj ovog poglavlja je definirati zajedničke mjere ocjenjivanja pouzdanosti metode autentikacije korisnika. Dodatno, pomoću predloženih metoda ocjenjivanja napravit će se usporedba metoda autentikacije korisnika temeljenim na znanju.

3.1. Mjere ocjenjivanja

Prije usporedbe metoda autentikacije korisnika temeljenih na znanju, potrebno je definirati kriterije po kojima će se ocjenjivati. Prije nego što se definiraju kriteriji, potrebno je definirati zahtjeve na sustav autentikacije.

1. **Otpornost na krađu uređaja** – ukoliko se metoda autentikacije korisnika oslanja na uređaj, krađom uređaja zlćudni korisnik ne može oponašati legitimnog korisnika. Ovo svojstvo je bitno kod metoda autentikacije koji koriste faktor posjedovanja. Takve metode autentikacije se obično koriste u kombinaciji s drugim metodama. Naime, ukoliko zlćudni korisnik otuđi uređaj za autentikaciju u većini slučajeva će moći oponašati drugog korisnika. Iz tog razloga se obično koriste dodatne mjere autentikacije poput tekstualnih lozinki.
2. **Otpornost na oponašanje fizičkih ili fizioloških svojstava** – biometrijske metode autentikacije koriste fizička i fiziološka svojstva korisnika kako bi napravili jedinstven otisak korisnika. Metode za autentikaciju korisnika koje se oslanjaju na biometriju moraju osigurati da zlćudni korisnik ne može oponašati neko fizičko ili fiziološko svojstvo drugog korisnika. Ovo se obično postiže dodavanjem raznih provjera prilikom prijave. Na primjer, kod skeniranja otiska ruke se snima korisnikov puls kako bi se osiguralo da se radi o živom korisniku. Prilikom skeniranja lica korisnika promatraju se i dinamička svojstva poput treptanja kako bi se osiguralo da zlćudni korisnik ne koristi sliku drugog korisnika.

3. **Otpornost na pogađanje** – najčešći oblik napada na korisnikov identitet predstavlja pogađanje informacija. Bilo da se radi o tajnim informacijama poput lozinki ili odgovora na pitanja, postoji mogućnost pogađanja. Naravno, pogađanje nikada nije moguće u potpunosti spriječiti. No, moguće ga je bitno otežati. Ukoliko metoda autentikacije sama po sebi ne otežava otuđivanje identiteta pogađanjem, smatra se da nije otporna na pogađanje.
4. **Otpornost na krađu tajnih informacija** – problem u uporabi tajnih informacija za autentikaciju je u činjenici da se prilikom svakog izričaja, odnosno prijave, ta informacija izlaže. Naime, postoje mnogi napadi pomoću kojih se tajne informacije mogu presresti na mreži ili otuđiti s medija za pohranu. Presretanje informacija na mrežnoj razini je rasprostranjen problem, a više detalja se može pronaći u dodatnoj literaturi pod [40], [41], [42], [43], [44] i [45]. Većina korisnika danas može primati poruke elektroničke pošte putem mobilnih uređaja. Postoji velik broj radova koji opisuju nedostatke u pohrani povjerljivih informacija na mobilnim uređajima te način na koji se do tih informacija može doći. Više informacija dostupno je pod [46] i [47].
5. **Otpornost na prisilno otkrivanje** – u većini slučajeva, korisnik unaprijed zna što će sustav od njega tražiti prilikom autentikacije. Odnosno, zna da će morat priložit tajnu informaciji koja se prethodno podijelila. Kada korisnik unaprijed zna odgovor na pitanje koje će se postaviti za provjeru identiteta, može ju pod prisilom otkriti. Otkrivanje te jedne informacije je dovoljno za otuđivanje identiteta korisnika. Otpornost na prisilno otkrivanje podrazumijeva da se napadač nikako ne može autenticirati kao drugi korisnik bez da taj korisnik nije prisutan. Naravno, u ovom zahtjevu se zanemaruje autentikacija pod prisilom. Točnije, zanemaruje se scenarij kada napadač prijeti fizičkom silom korisniku da se prijavi, obzirom da to ulazi u domenu fizičke sigurnosti.

U ovom radu analiziraju se metode autentikacije temeljene na znanju. Time se zahtjevi pod 1 i 2 implicitno zadovoljavaju obzirom da se ne koriste dodatni uređaji niti fizička ili fiziološka svojstva. Iz navedenih zahtjeva izvode se mjere za ocjenjivanje metoda autentikacije temeljenih na znanju. Pretpostavka je da ukoliko metoda sama po sebi zadovoljava sve navedene mjere ocjenjivanja, nije ju moguće zaobići. Točnije, nije moguće otuđiti identitet drugog korisnika. Metoda sama po sebi zadovoljava sve mjere

samo onda ako nisu potrebni dodatnih mehanizmi za zadovoljavanje pojedinih mjera. Na primjer, uporaba tekstualnih lozinki nije otporna na pogađanje. No, dodavanjem CAPTCHA [39] provjera moguće je spriječiti automatizirano pogađanje i time otežati postupak. Dodatno, korištenjem salt vrijednosti kod pohrane lozinki moguće je otežati pogađanje lozinki u slučaju kada napadač ima pristup pozadinskoj bazi podataka. Salt vrijednosti i CAPTCHA provjera predstavljaju dodatne mehanizme kojima se pogađanje tekstualnih lozinki može otežati. Sama po sebi, tekstualna lozinka ne može spriječiti niti otežati pogađanje već mora koristiti te dodatne mehanizme. U nastavku se opisuju prepoznate mjere ocjenjivanja metoda autentikacije korisnika temeljem znanja.

1. **Jednokratnost odgovora** – prilikom svake prijave, korisniku se mora postaviti drugačije pitanje za provjeru identiteta. Ukoliko to nije moguće, odgovor na pitanje mora svaki puta biti različit. Korisnik ne smije znati što će ga sustav pitati prije nego što se pokrene postupak prijave. Ovime se sprječava mogućnost prisilnog otkrivanja tajnih informacija drugim stranama. Naime, ukoliko je zadovoljena jednokratnost, prilikom svake iduće prijave se mijenjaju informacije potrebne za autentikaciju. Korisnik ne zna unaprijed koje pitanje će biti postavljeno i zato ne može otkriti ispravan odgovor drugim stranama čak niti pod prisilom. Dodatno, jednokratnost pitanja gotovo u potpunosti sprječava mogućnost pogađanja. Prilikom autentikacije, korisnik može samo jednom odgovoriti na postavljeno pitanje. Svaki idući puta se postavlja drugačije pitanje koje nije vezano uz prethodno. Svako pitanje mora biti neovisno o prethodnom pitanju. Odnosno, niti korisnik niti napadač ne smiju biti u mogućnosti predvidjeti pitanje koje će se postaviti tokom iduće prijave.
2. **Neovisnost pitanja** – pitanja i odgovori ne smiju otkrivati informacije koje bi se mogle upotrijebiti za lažno predstavljanje. Točnije, ukoliko napadač prisluškivanjem skuplja pitanja i odgovore legitimnog korisnika, neće nikada skupiti dovoljno informacija da se lažno predstavi kao drugi korisnik. Dodatno, čak ako napadač ima pristup korisnikovoj radnoj stanici i može vidjeti sve odgovore koje unosi prilikom prijave, neće se kasnije moći prijaviti kao taj korisnik.
3. **Neovisno o sigurnosti sustava za autentikaciju** – ukoliko napadač dobije ili već ima pristup sustavu koji obavlja autentikaciju i dalje se ne može lažno predstaviti kao drugi korisnik. U slučaju kada se koriste tajne informacije za autentikaciju,

sustav te informacije mora pohraniti u nekom obliku. Ova mjera je zadovoljena samo onda ako metoda autentikacije osigurava identiteta korisnika čak i u slučaju kada napadač ovlada sustavom. Naime, sustav informacijama upravlja na takav način koji napadaču ne dozvoljava otkrivanje uporabu dobivenih informacija za oponašanje korisnika.

3.2. Rezultati usporedbe

U poglavlju 2 su opisane metode autentikacije temeljene na znanju. Prethodno poglavlje opisuje prepoznat zahtjeve i mjere ocjenjivanja koje se koriste za usporedbu metoda. U nastavku su prikazani rezultati usporedbe po definiranim mjerama ocjenjivanja, a Tablica 1. prikazuje sažetak rezultata. Mjere definirane u prethodnom poglavlju predstavljaju svojstva kojima se ocjenjuje potencijal pojedine metode autentikacije. Konkretne implementacije metoda moraju zadovoljiti sve mjere kako bi se u potpunosti uklonila mogućnost otuđivanja identiteta. Kako je konkretnih implementacija metoda previše, u nastavku se analiziraju samo općenite metode. Na primjer, ne analizira se vizualna metoda autentikacije koja se koristi u sustavu Deja Vu (poglavlje 2.1.2), već samo vizualne metode kao jedna od metoda autentikacije korisnika. Ocjenom potencijala želi se istaknuti koje metode ima smisla razvijati a koje ne. Ukoliko neka metoda autentikacije ne zadovoljava niti jednu mjeru, smatra se da niti jedna konkretna izvedba te metode ne može zadovoljiti tu mjeru.

- **Tekstualne lozinke** – uporaba tekstualnih lozinki nije zadovoljila niti jednu mjeru. Autentikacija tekstualnom lozinkom podrazumijeva da će korisnik svaki puta unijeti jednu te istu vrijednost kako bi se prijavio na sustav. Time se narušavaju uvjeti jednokratnosti i neovisnosti. Točnije, jednokratnost je narušena jer korisnik zna unaprijed što je ispravna vrijednost. Neovisnost pitanja je narušena jer ukoliko napadač jednom uspije presresti poruku s lozinkom, može oponašati legitimnog korisnika. Tekstualne lozinke se moraju pohraniti u nekom obliku na sustavu. U suprotnom nije moguće provjeriti je li vrijednost lozinke kojom se korisnik želi prijaviti ista kao i prethodno dogovorena vrijednost. Ukoliko napadač ima pristup pohranjenim vrijednostima može očitati korisnikovu lozinku. Ovo je moguće čak i u slučaju kada je lozinka pohranjena u obliku sažetka. Kako je opisano u poglavlju 2.1.1, pogađanjem se u proizvoljno dugom vremenu može pogoditi velik broj lozinki.

- **Vizualne lozinke** – pružaju nešto veću razinu sigurnosti. Ipak, nisu idealne te ne zadovoljavaju sve mjere ocjenjivanja. U poglavlju 2.1.2 su opisani neki oblici uporabe vizualnih lozinki za autentikaciju korisnika. Uporabom matematičkih algoritama za proizvodnju slika, moguće je napraviti metodu autentikacije u kojoj se odgovori međusobno razlikuju. Naravno, nakon određenog broja prijava, slike će se ponavljati te samim time narušiti jednokratnost. Ipak, ovo ovisi o konkretnoj implementaciji metode. Svojstvo se može narušiti ukoliko je lozinka sastavljena od običnog niza slika koji se kod svake prijave mora reproducirati. Iako se neki odgovori mogu razlikovati, detaljnim prikupljanjem informacija moguće je prikupiti dovoljno informacija za oponašanje korisnika. Ukoliko napadač ima pristup sustavu koji obavlja autentikaciju, može očitati pohranjene vizualne lozinke. Naime, vizualne lozinke se moraju pohraniti u određenom obliku. Bilo da se radi o formuli ili nekim parametrima, odnosno, stvarnim slikama.
- **Grafičke lozinke** – unatoč prividno velikoj razini sigurnosti koju grafičke lozinke pružaju, ne zadovoljavaju niti jednu mjeru ocjenjivanja. Naime, iako se ne koristi strogo tekstualni zapis, korisnik mora uvijek jednu te istu sliku nacrtati kako bi se prijavio. Time se narušava uvjet jednokratnosti. Ukoliko napadač uspije presresti autentikacijski postupak, u većini slučajeva može te informacije iskoristiti za otuđivanje identiteta drugog korisnika. Grafičke lozinke se također moraju u nekom obliku pohraniti na sustavu radi kasnije autentikacije. Kako je opisano u poglavlju 2.1.3, grafičke lozinke se pretvaraju u jedinstven zapis ovisno o poljima po kojima korisnik crta. Taj zapis se obično šifrira putem jednosmjernih funkcija i pohranjuje na sustavu. Iako je izvorni zapis u ovom obliku naizgled teže pogoditi, današnji računalni resursi rastu sve većom brzinom. Držanje tajnih informacija na sustavu nije prihvatljivo ni na koji način.
- **Statička pitanja** – za razliku od autentikacije lozinkama, postoje određene prednosti vezan uz lakoću pamćenja. Kako je opisano u poglavlju 2.2, odgovori na određena pitanja se obično lakše pamte od lozinki. No, statička pitanja se smatraju jednim od najlošijih metoda autentikacije. Za razliku od autentikacije lozinkama gdje postoji samo jedna informacija koja se može iskoristiti za otuđivanje identiteta, u ovoj metodi postoje dvije. Naime, kada napadač može vidi pitanje za provjeru identiteta može pokušati pogoditi odgovor na pitanje. Ukoliko je pitanje općenito ili se može otkriti putem javnih arhiva ili društvenih mreža, napad će biti

uspješan. Dodatno, napadač se može usredotočiti na korisnikov odgovor. Dovoljno je jednom presresti korisnikov odgovor i time otuđiti njegov identiteta. Zbog ovoga se narušava mjera neovisnosti pitanja. Nedostatak statičkih pitanja je identičan lozinkama. Korisnik i sustav moraju unaprijed podijeliti tajne informacije kako bi se kasnije provela autentikacija. Kada se jednom odabere tajno pitanje (ili više njih) nije ih moguće promijeniti. Time se narušava jednokratnost obzirom da korisnik unaprijed zna koja pitanja sustav može postaviti. U ovom slučaju se tajne informacije ponovno nalaze na sustavu. Ukoliko napadač ovlada sustavom, može otuđiti tajne informacije potrebne za oponašanje korisnika.

- **Dinamička pitanja** – kako je opisano u poglavlju 2.3, korisnik i sustav nisu prethodno uspostavili dogovor o tome koje će se informacije koristiti za autentikaciju. Samim time, sustav za autentikaciju bira što će korisnika pitati. Iz toga slijedi da ukoliko sustav proizvoljno odabire pitanja, može se osigurati jednokratnost odgovora. Dodatno, ukoliko su pitanja postavljena tako da odgovor nije uvijek isti, jednokratnost je očuvana čak i onda kada se pitanja ponavljaju. Neovisnost pitanja ovisi o konkretnoj metodi koja se implementira. Naime, potrebno je odabrati pitanja tako da se ni na koji način ne odaju odgovori na druga pitanja. Obzirom da se takva pitanja mogu s lakoćom napraviti, i ova mjera je zadovoljena. U slučaju da napadač ima pristup sustavu za autentikaciju, sigurnost korisnikovog identiteta ovisi o načinu na koji se potvrđuju odgovori. Ukoliko se ispravni odgovori nalaze na ovladanom sustavu za autentikaciju, napadač ih može sakupiti. No, u većini slučajeva se odgovori nalaze u drugim sustavima.
- **ZKPP** – poglavlje 2.4 detaljnije opisuje ZKPP protokole. Zahvaljujući matematičkim svojstvima, prilikom svake autentikacije proizvode se različiti odgovori i time se osigurava njihova jednokratnost. Također, zahvaljujući svojstvima dokaza bez poznavanja, prilikom autentikacije se ne izriču tajne informacije. Jedina mana se nalazi u dijeljenoj tajnoj informaciji koju moraju imati i sustav za autentikaciju i korisnik. Ukoliko napadač ovlada sustavom za autentikaciju može otkriti dijeljeni privatni ključ i time oponašati korisnika.

	Jednokratnost odgovora	Neovisnost pitanja	Neovisnost o sigurnosti sustava za autentikaciju
Tekstualne lozinke	-	-	-
Vizualne lozinke	-	-	-
Grafičke lozinke	-	-	-
Statička pitanja	-	-	-
Dinamička pitanja	+	+	+
ZKPP	+	+	-

Tablica 1. Rezultati usporedbe

4. Prijedlog metoda autentikacije temeljenih na dinamičkim pitanjima

Cilj ovog poglavlja je predložiti konkretnu metodu autentikacije korisnika uporabom dinamičkih pitanja. Prema rezultatima usporedbe metoda autentikacije u poglavlju 3.2., dinamička pitanja imaju najbolji potencijal za osiguravanje identiteta korisnika. U nastavku se opisuju konkretne metode autentikacije temeljene na dinamičkim pitanjima.

Ipak, prije predlaganja nove metode autentikacije potrebno je obrazložiti razlog odabira dinamičkih pitanja. Dodatno, potrebno je odrediti karakteristike pitanja koja će se postavljati. Prema mjerama iz prethodnog poglavlja, najvažnija svojstva koja se odnose na pitanja su njihova jednokratnost i međusobna neovisnost. Jednokratnost je zadovoljena i u slučajevima kada je pitanje isto, ali odgovor različit. Analizom statičkih pitanja u poglavlju 2.2, ustanovilo se da odgovori ne smiju biti pohranjeni na poslužitelju. No, čak i kod dinamičkih pitanja potrebno je odrediti je li korisnikov odgovor ispravan. Odnosno, potrebno je znati ispravan odgovor na pitanje. Drugi problem je utjecaj odgovora na korisnikovu sigurnost identiteta i privatnost. Točnije, odgovor ne bi smio odavati previše informacija o korisniku. Kako bi se ovaj zahtjev zadovoljio, odgovori na pitanja moraju dolaziti iz malog skupa mogućih vrijednosti. Predlaže se uporaba pitanja koja će se moći odgovoriti binarnom logikom, odnosno, pitanja koja se odgovaraju s DA ili NE. Naravno, smanjivanjem prostora mogućih odgovora povećava se vjerojatnost da će zlćudni korisnik pogoditi točan odgovor. Iz tog razloga se koriste mehanizmi iz protokola za dokazivanje bez poznavanja (poglavlje 2.4). Korisniku se postavlja N pitanja u obliku upitnika, gdje N predstavlja broj pitanja koji smanjuje vjerojatnost pogađanja na najmanju moguću razinu. Dodatno, za svaki upitnik je potrebno odrediti najveće moguće vrijeme u kojemu korisnik može odgovarati na pitanja kako bi se otežao pronalazak ispravnih odgovora putem javnih izvora. Pretpostavka je da će se legitiman korisnik s lakoćom prisjetiti ispravnih odgovora, dok zlćudni korisnik neće imati dovoljno vremena pronaći odgovore putem javno dostupnih izvora.

Alternativa ovom pristupu je uporaba uobičajenih odgovora. Time bi se naizgled smanjila mogućnost pogađanja. No, ovo nije nužno istinito. Na primjer, neka se korisnika pita s kojeg broja je zadnji puta uplatio parking za auto s njegovom registracijom[6]. Korisnik će u većini slučajeva odgovoriti s vlastitim brojem. Kada se ta informacije jednom presretne, zloćudni korisnik može na slična pitanja pokušati odgovoriti istim odgovorom. Naime, jednim konkretnim odgovorom se izdala informacija koja se može iskoristiti i nekim daljnjim pitanjima i odgovorima. Zamislimo da je isto pitanje postavljeno na drugačiji način.

- Je li broj telefona s kojeg ste zadnji puta uplatili parking za auto s registracijom X sadržao znamenku 6?
- Je li zbroj zadnja dva broja telefona s kojeg ste zadnji puta uplatili parking za auto s registracijom X jednak 12?

Iz ovih primjera se vidi da se isto pitanje moglo postaviti na velik broj načina. Te da odgovori na ta pitanja ne otkrivaju dovoljno informacija za pogađanje drugih, sličnih, odgovora. Odabir i sastavljanje pitanja je velik dio ove metode autentikacije. Glavni problem se odnosi na domenu odgovora. Naime, za prikazanom primjeru s uplatom parkinga postoje određene zakonitosti i ograničenja koja su specifična za domenu uplate parkinga. Osnovna pretpostavka je da korisnik ima auto te da je barem jednom uplatio parking za svoj auto. Druga zakonitost za domenu uplate parkinga o kojoj treba voditi računa je učestalost promjene broja telefona i registracije automobila. Naime, to nisu značajke koje se često mijenjaju. Većina ljudi imaju isti auto (a time i istu registraciju), što znači da ne nudi velik broj mogućih pitanja. Prethodno navedenim primjerima pitanja se može onemogućiti otkrivanje informacija o odgovoru. No, ukoliko napadač poznaje korisnika, odnosno njegovu registraciju i broj telefona, moći će odgovoriti na ta pitanja. Naravno, ovaj nedostatak se pokriva uvođenjem više pitanja kojima se smanjuje vjerojatnost ovakvog napada. Naime, napadač bi morao znati sve što zna i korisnik kako bi mu otuđio identitet. Prema ovome slijedi da bi pitanja trebala provjeravati znanje korisnika koje je poznato samo njemu. Odnosno, da se provjerava znanje koje niti jedna druga osoba ne može znati. Ovaj zahtjev je nemoguće ostvariti ovim modelom obzirom da i sustavu

[6] Pretpostavlja se da je korisnik prethodno unio registraciju svog automobila u sustav.

koji provjerava odgovor[7] mora znati što je točan odgovor. Prema tome, mehanizam autentikacije znanjem treba otežati napadaču pogađanje točnih odgovora do te mjere da ono postane neisplativo.

Kao što se pogađanje sprječava uporabom dugačkih tekstualnih lozinki. Naime, kvalitetnu lozinku će biti gotovo nemoguće pogoditi u prihvatljivom vremenu[8]. No, ukoliko se ona jednom dozna, moguće je oponašati korisnika. Drugom riječima, dovoljno je otuđiti samo jednu informaciju kako bi se narušio identiteta korisnika. Ovo svojstvo ne vrijedi za autentikaciju dinamičkim pitanjima. Otuđivanjem samo jedne informacije nije moguće narušiti korisnikov identitet. Potrebno je osigurati da količina informacija koju napadač mora o korisniku prikupiti bude u najmanju ruku proporcionalna vremenu koje bi se trebalo utrošiti za pogađanje dugačke i složene tekstualne lozinke. Time bi se opravdala zamjena tekstualnih lozinki ovom metodom autentikacije[9]. Dodatno, ostala povoljna svojstva dinamičkih pitanja koja su navedena u poglavlju 2.3 nadmašuju korisna svojstva lozinki[10].

4.1. Raspodijeljeni izvori pitanja

Osnovni problem svih metoda autentikacije je provjera ispravnosti odgovora. Neovisno o tome provjerava li se ispravnost lozinke, odgovora na dinamičko ili statičko pitanje, podatci o točnom odgovoru moraju biti poznati sustavu koji radi autentikaciju. Samim time se narušava mjera neovisnosti o sigurnosti sustava za autentikaciju. Naime, ukoliko napadač uspije ovladati sustavom na kojemu se nalaze ispravne informacije moći će otkriti tajne informacije za autentikaciju[11]. Kako bi se pružilo rješenje na ovaj problem, predlaže se novi model autentikacije temeljen na dinamičkim pitanjima.

Naime, sustav na koji se korisnik prijavljuje nije zadužen za proizvodnju i provjeru postavljenih pitanja. Tu ulogu preuzimaju drugi sustavi. Drugim riječima, uvodi se nova

---

[7] Sustav za provjeru odgovora i sustav koji obavlja autentikaciju nisu nužno isto. Više u idućem poglavlju.

[8] Na primjer, period od godinu dana. Naravno, pod pretpostavkom da se koriste velik broj računalnih resursa.

[9] Uspoređuje se tekstualnim lozinkama obzirom da je to trenutno najrasprostranjenija metoda autentikacija korisnika temeljem znanja.

[10] Na primjer, kako je opisano u poglavlju 2.1.1, kvalitetne lozinke se teško pamte. No, korisnik bi se trebao s lakoćom prisjetiti pojedinih odgovora na dinamička pitanja. Time se implicitno sprječava mogućnost zapisivanja autentikacijskih informacija ili njihovo odavanje.

[11] Ovo vrijedi i u slučajevima kada se koriste jednosmjerne funkcije, salt vrijednosti i druge kriptografske metode. Naime, pokazalo se te metode zaštite samo otežavaju pronalazak informacija, ne sprječavaju ih.

organizacijska struktura između entiteta koji sudjeluju u postupku autentikacije. Radi preglednosti, u nastavku se opisuje terminologija koja će se koristiti za daljnji opis predložene metode autentikacije.

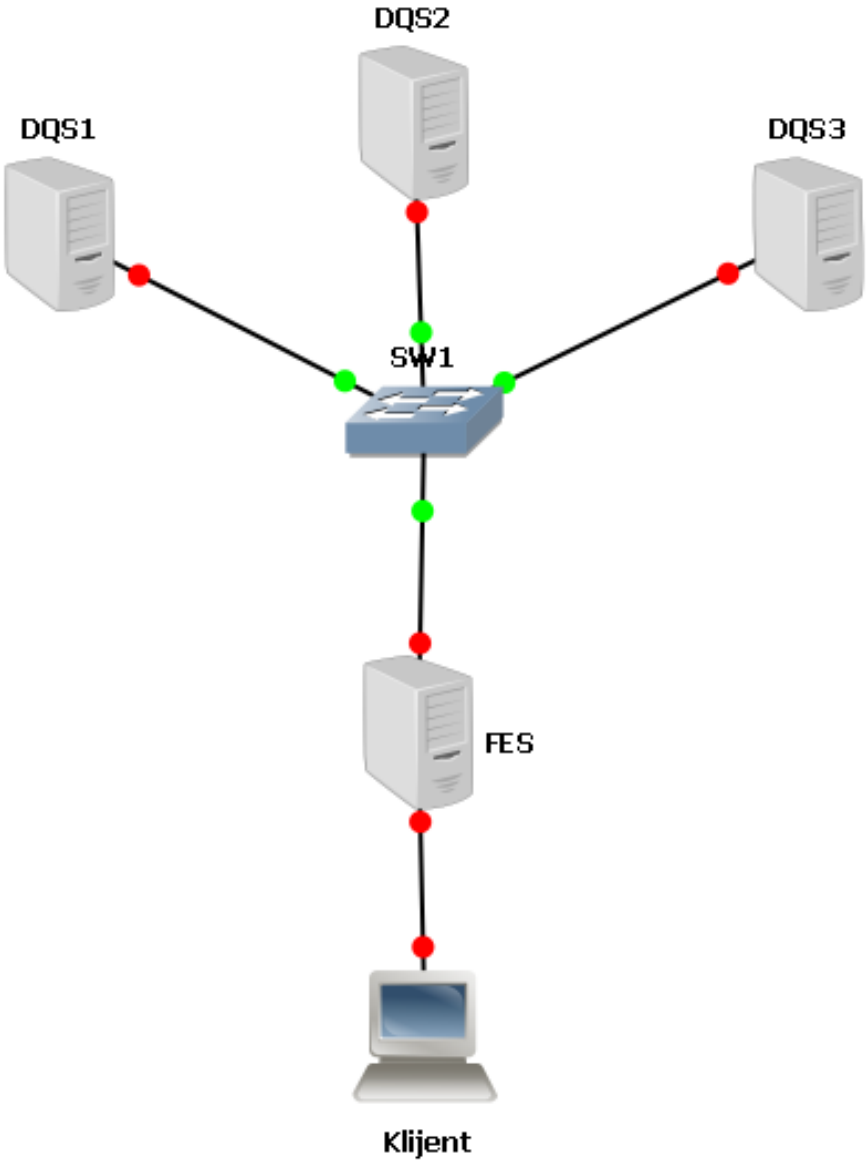
- **Usluga provjere identiteta** (engl. *IVS – Identity Verification Service*) – podrazumijeva postupak proizvodnje pitanja te validacija njihovih odgovora.
- **Korisnik** (engl. *User*) – označava korisnika koji pristupa usluzi i pokušava se autenticirati na sustavu.
- **Pristupni poslužitelj** (engl. *FES – Front-End Server*) – pružatelj usluge na kojemu se nalaze resursi koje korisnik traži. Odnosno, sustav na koji se korisnik želi prijaviti. Prilikom prijave, za svakog korisnika se stvara upitnik koji se sastoji od dinamičkih pitanja. FES ne sudjeluje u sastavljanju pitanja niti u provjeri odgovora. FES traži od DQS sustava sastavljanje pitanja, te im prosljeđuje odgovore na ovjeru.
- **Poslužitelj za dinamičko postavljanje i ovjeru pitanja** (engl. *DQS – Dynamic Question Server*) – podrazumijeva sustav koji je neovisan o svim drugim poslužiteljima, a koji nudi uslugu provjere identiteta (IVS). Točnije, sastavlja pitanja na zahtjev FES poslužitelja, te radi provjeru odgovora i potvrđuje korisnikov identitet.

4.1.1. Opis metode autentikacije korisnika

Korisnik se putem sučelja na FES poslužitelju pokušava prijaviti. Prilikom prijave unosi općenite podatke o sebi. Na primjer, ime i prezime, datum rođenja, adresa stanovanja, broj telefona ili druge informacije. FES poslužitelj traži od svojih DSQ poslužitelja da sastave određen broj pitanja koja se odnose na trenutnog korisnika. DSQ sustavi odgovaraju sa skupom pitanja, koja FES postavlja korisniku u obliku ispita. Nakon što korisnik odgovori na svako pitanje, FES prosljeđuje odgovore na pitanja pojedinim DQS sustavima na provjeru. Ukoliko svaki DQS javi da su odgovori ispravni, korisnik je autenticiran i otvara sjednicu s FES sustavom za daljnji rad. Slika 5. prikazuje opisani model autentikacije korisnika. Model autentikacije se zasniva na pretpostavkama u nastavku.

- FES mora prethodno stupiti u odnos sa svakim pojedinim DQS poslužiteljima koji će se koristiti za autentikaciju korisnika. Naime, svaki sustav koji sadrži određene podatke o svojim korisnicima može postati DQS poslužitelj. Dodatno, tu uslugu može naplaćivati zainteresiranim FES sustavima. Financijske mogućnosti modela se ne razmatraju u ovom radu. Naravno, dva sustava mogu jedan drugome pružati DQS usluge.
- Korišteni DQS mora imati podatke o korisniku koji se pokušava prijaviti. U suprotnome, neće moći proizvesti pitanja koja su karakteristična za tog korisnika.
- Komunikacijski kanal između FES i korisnika mora biti zaštićen. Naime, korisnik prilikom prijave unosi svoje osobne podatke. Iako se ti podatci ne mogu upotrijebiti za otuđivanje identiteta, predstavljaju osobne informacije koje se mogu u drugim pogledima zlouporabiti.
- Potrebno je osigurati komunikacijski kanal između FES i DQS poslužitelja. Naime, FES mora vjerovati rezultatima koje mu DQS pruža. Ukoliko napadač uspije poruku DQS poslužitelja zamijeniti vlastitom, može narušiti integritet postupka i time omogućiti otuđivanje identiteta. Na primjer, ukoliko DQS prilikom ovjere odgovora ustanovi da se ne radi o legitimnom korisniku, šalje negativan odgovor prema FES poslužitelju. Ako zloćudni korisnik uspije presresti DQS poruku i zamijeniti ju vlastitom, može negativnu poruku pretvoriti u pozitivnu i time osigurati pristup. Naravno, obzirom da se koristi više od jednog DQS sustava, napadač mora presresti sve ostale negativne poruke i pretvoriti ih u pozitivne. Time se napad implicitno otežava. Ipak, potrebno je šifrirati poruke il ih digitalno potpisati kako ih napadač ne bi mogao mijenjati. Najjednostavniji način osiguravanja ovog postupka je izmjena javnih ključa između DQS i FES poslužitelja prilikom sklapanja radnog odnosa.
- DQS mora biti u stanju iz vlastite lokalne baze proizvesti pitanja za pojedinog korisnika. Naravno, svaka organizacija ima konačan broj različitih pitanja koja se mogu postavljati. No, odgovori na ta pitanja ne moraju uvijek biti ista. Na primjer, pitanje o iznosu računa za prošli mjesec se mijenja. Kako svaka organizacija može imati specifične podatke o svojim korisnicima, nemoguće je predvidjeti sva moguća pitanja koja se na temelju tih podataka mogu proizvesti. Jedan od mogućih rješenja ovog problema leži u skladištima podataka i predvidljivosti zvjezdastog

modela. Naime, zvjezdasti model predstavlja dominantan standard za oblikovanje skladišta podataka. Zahvaljujući predvidljivosti zvjezdastog modela moguće je unaprijed definirati sve moguće upite koji se nad skladištem mogu napraviti. U tu svrhu se koriste metapodatci koji opisuju moguće operacije i podatke za svako pojedino skladište podataka. Ovaj postupak se koristi u postupku rudarenja podataka (engl. *Data Mining*). Alati za rudarenje podatcima koriste metapodatke kako bi gradili upite nad skladištem podataka i time olakšali njihovu analizu. Isti postupak bi se mogao koristiti i za proizvodnju pitanja. Naime, pitanja bi se mogla definirati putem metapodataka, kao i operacije koje su potrebne za njihovo stvaranje. Metapodatci u skladištima podatka se detaljnije opisuju u radu pod[50], a zvjezdasti model je opisan u [51].



Slika 5. Skica sustava za provjeru identiteta korisnika

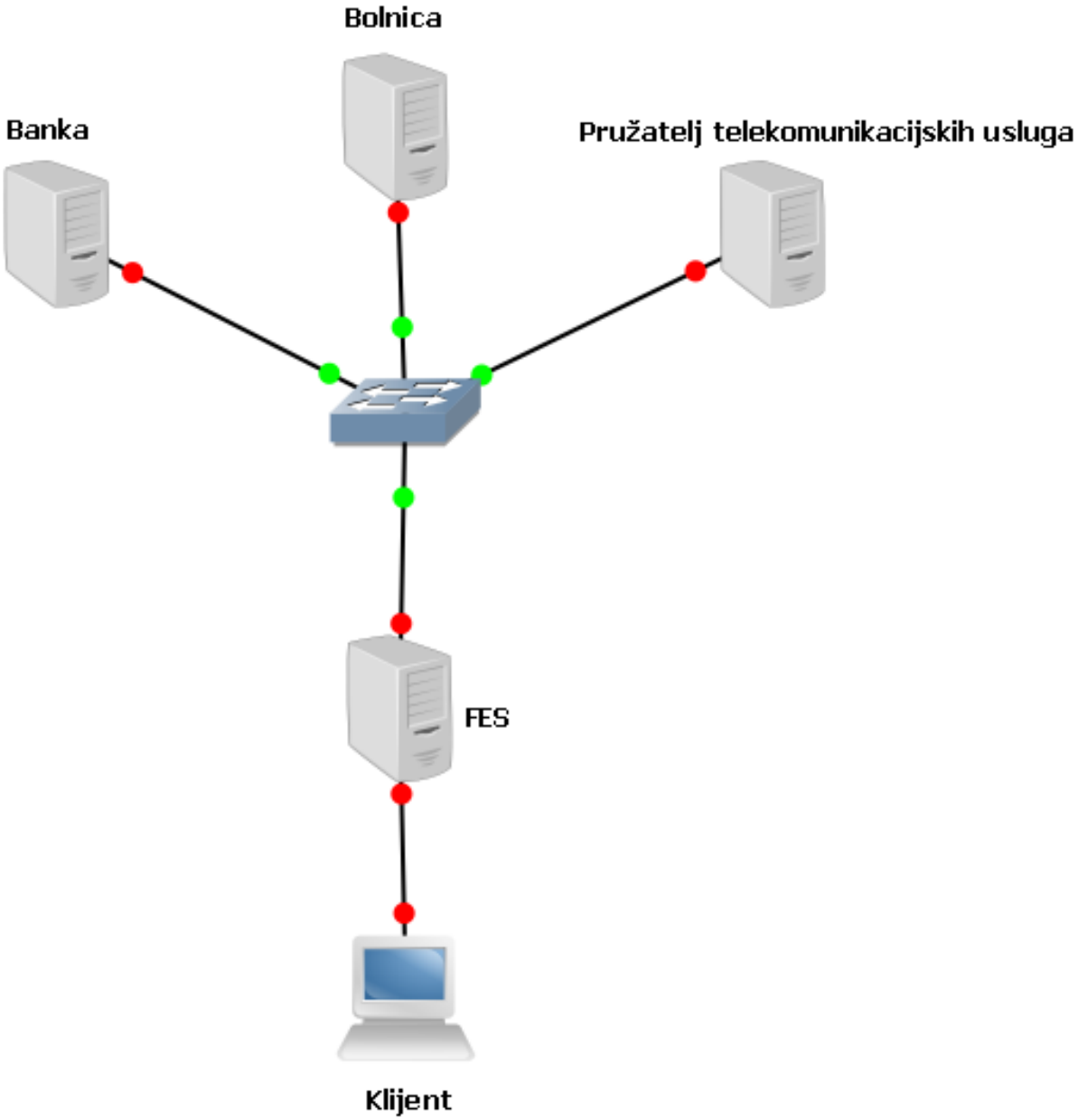
4.1.2. Scenarij autentikacije korisnika

Radni preglednosti, u ovom poglavlju će se opisati stvaran scenarij autentikacije korisnika uporabom predložene metode. Koriste se stvarni DQS poslužitelji kako bi se pokazala proizvodnja stvarnih pitanja. Točnije, u ovom scenariju ulogu DQS poslužitelja imaju banka, bolnica te pružatelj telekomunikacijskih usluga. Pretpostavlja se da svaki od tri navedena sustava ima zapise o korisniku koji se pokušava autenticirati. Slika 6. prikazuje skicu za ovaj scenarij, a u nastavku je opis pojedinih koraka.

1. Korisnik prilikom prijave na FES unosi svoje ime i prezime te OIB.
2. FES od DQS poslužitelja zahtjeva po dva pitanja za trenutnog korisnika te im prosljeđuje njegovom ime, prezime i OIB
3. Banka proizvodi dva pitanja temeljem vlastitih podataka, i odgovore bilježi u privremenoj bazi, zajedno s vremenom kada su se pitanja proizvela. Pitanja su:
    a. Je li Vaša posljednja uplata iznosila više od 500 kuna?
    b. Je li iznos mjesečne naknade za Vaš kredit manji od 300 kuna?
4. Bolnica na isti način proizvodi po dva pitanja i odgovore bilježi u vlastitoj privremenoj bazi.
    a. Je li Vam kod predzadnjeg posjeta izdana uputnica za lijek Sumamed?
    b. Jeste li prilikom zadnje pretrage dali urin na analizu?
5. Pružatelj telekomunikacijskih usluga također proizvodi po dva pitanja, te bilježi odgovore na isti način.
    a. Jeste li za peti mjesec ove godine potrošili više od 300 kuna na podatkovni promet mobitelom?
    b. Jeste li u prethodnih 24 sata obavili poziv prema drugim zemljama?
6. FES dobivena pitanja strukturira u obliku upitnika koji korisnik ispunjava. Za svako pitanje se pamti koji DQS ih je postavio.
7. Korisnik odgovara na sva postavljena pitanja, a FES prosljeđuje odgovore natrag prema pojedinim DSQ poslužiteljima koji su postavili pitanje.
8. Svaki DQS poslužitelj prvo provjerava je li isteklo vrijeme u kojemu je korisnik trebao odgovoriti na pitanja. Ukoliko je vrijeme isteklo, odgovori se zanemaruju i

šalje se odgovarajuća obavijest FES poslužitelju. U suprotnom se dobiveni odgovori uspoređuju s pohranjenim odgovorima. Ako DQS ustanovi da su svi odgovori ispravni, šalje pozitivan odgovor za tog korisnika. U suprotnom se šalje negativan odgovor.

9. FES prikuplja odgovore na pitanja od DSQ poslužitelja te ukoliko su svi odgovori pozitivno ocijenjeni, korisnik je autenticiran.



Slika 6. Skica scenarija za autentikaciju

4.1.3. Nedostatci

Opisani model ima određene nedostatke koje bi zloćudni korisnik mogao iskoristiti. Ukoliko napadač ovlada svakim DQS sustavom, može doznati odgovore na pitanja koja se postavljaju prilikom autentikacije. Naime, opisana metoda proizvodnje pitanja pretpostavlja da će DQS moći potvrditi odgovor na postavljeno pitanje. Samim time se pretpostavlja da će DQS morati zapamtiti ispravan odgovor kada ga postavi. Ako napadač uspije ovladati svakim korištenim DQS sustavom, moći će provjeriti odgovore na pitanja koja su postavljena korisniku. Jedna od metoda kojim se ovo može spriječiti je uporaba protokola koji osigurava tajnost korisničkih identifikatora. Ukoliko napadač ovlada svim DQS sustavima a ne zna korisnički identifikator, neće moći pronaći odgovore na postavljena pitanja. Protokol za upravljanje identifikatorima bi se trebao zasnivati na centraliziranom sustavu. Dodatno, protokol bi morao biti otporan na napade centralnog poslužitelja. Trenutno nije poznat protokol s takvim karakteristikama.

Druga metoda napada predstavlja ubacivanje posrednika (engl. *Man-in-the-middle*) između korisnika i FES poslužitelja. Naime, ukoliko se napadač uspije pozicionirati između korisnika i FES poslužitelja, može presresti korisnikove odgovore i autenticirati se. Slično tome, napadač može phishing napadom prikazati korisniku lažnu stranicu FES poslužitelja. Istovremeno, napadač pokreće postupak autentikacije na stvarnom poslužitelju i dobiva pitanja. Ta pitanja prosljeđuje legitimnom korisniku i čeka da odgovori. Pomoću tih odgovora, napadač se autenticira na sustav kao legitiman korisnik. Naravno, ovo bi se moralo napraviti svaki puta kada napadač želi dobiti pristup. Ako jednom uspije presresti odgovore i autenticirati se, postupak autentikacije neće moći ponoviti istim odgovorima već ponovno mora zavarati korisnika.

Očiti nedostatak ove metode je da se ne može primijeniti za autentikaciju dvaju računala. Naime, korisnik uvijek mora biti čovjek.

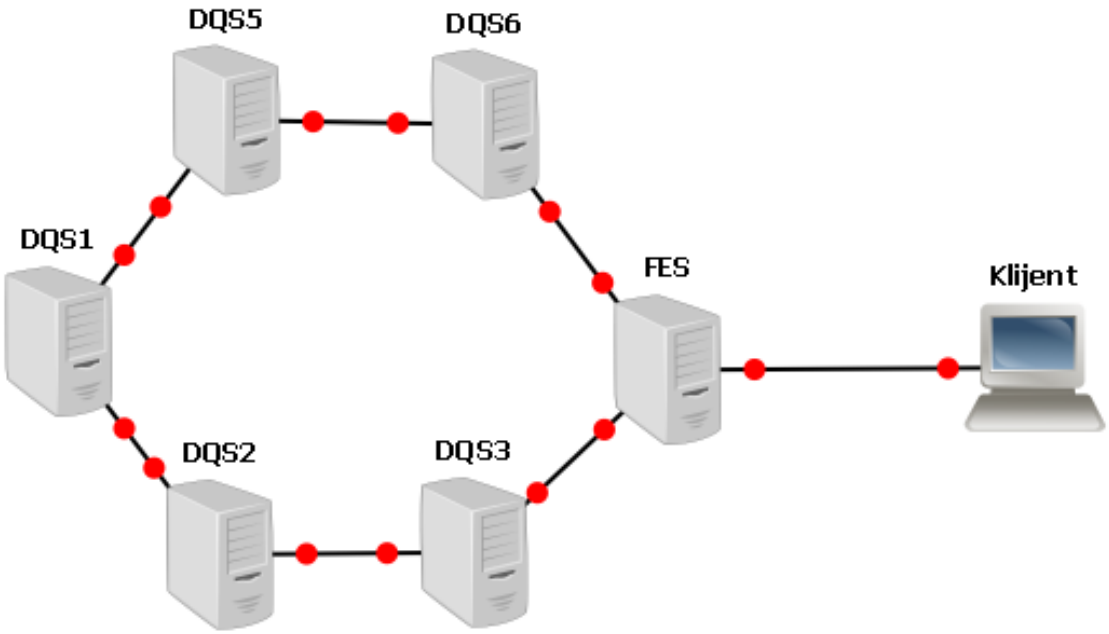
4.2. Poboljšani model zasnovan na Peer-2-Peer mrežama

Predloženi model autentikacije korisnika temeljen na dinamičkim pitanjima nije usko vezan uz metodu ostvarivanja komunikacije između pojedinih FES i DSQ poslužitelja. Napredniji model komuniciranja mogao bi se zasnivati na Peer-2-Peer mrežama. Slika 7. prikazuje ostvarenje u obliku P2P mreže. Svaki čvor u mreži može biti DQS i FES poslužitelj. Na primjer, ako DQS1 želi autenticirati korisnika on postaje trenutni FES poslužitelj te od ostalih čvorova traži IVS uslugu.

U ovom scenariju, upitnik identiteta je moguće izvesti u obliku skupa pitanja koja se prosljeđuju do svakog čvora. FES stvara upitnik u kojemu se nalazi prazan skup pitanja i korisnikovi identifikatori[12]. Tako stvoreni upitnik se prosljeđuje prvom slobodnom čvoru. Na primjer, šalje se čvoru DQS 3 te prosljeđuje dalje dok ne dođe ponovno do FES poslužitelja koji je zatražio pitanja. Svaki čvor pomoću vlastite baze stvara pitanja temeljem identifikatora korisnika. FES upitnik prikazuje korisniku koji odgovara na pitanja. Popunjeni upitnik se ponovno šalje kroz P2P mrežu, a svaki čvor provjerava ispravnost odgovora.

Moguća ranjivost ovog modela predstavljaju lažni DQS poslužitelji. Ukoliko napadač ovlada postojećim DQS poslužiteljima ili uspije vlastito računalo uključiti u P2P mrežu, može pregledavati pitanja i odgovore. Kako bi se to izbjeglo, svaki DQS poslužitelj može svoja pitanja šifrirati javnim ključem FES poslužitelja. Time niti jedan od ostalih DQS poslužitelja ne mogu mijenjati ili pročitati poruku. Dodatno, FES korisnikove odgovore šifrira javnim ključem pojedinog DQS poslužitelja kako bi samo jedan mogao pročitati odgovore. Kao i prethodni model, napad ubacivanjem posrednika između FES poslužitelja i klijenta nije implicitno onemogućena.

[12] Kao i do sada, identifikator može biti ime i prezime, datum rođenja, OIB i drugo.



Slika 7. DSQ u obliku P2P mreže

4.3. Model osobnih poslužitelja informacija

Obzirom na raznovrsnost informacija koje se mogu postavljati prilikom autentikacije korisnika, DQS poslužiteljine moraju nužno biti organizacije. Poželjno je razmotriti mogućnost uporabe drugih korisnika kao izvore pitanja. U takvom scenariju, svaki korisnik bi morao na neki način biti povezan s drugim korisnicima koji mogu potvrditi njegovu autentičnost. Drugi korisnici postavljaju pitanja na koja samo taj korisnik može znati odgovor. Naravno, jedan od zahtjeva je da drugi korisnici budu na raspolaganju kada se pokreće postupak autentikacije. Kako ovo nije uvijek moguće, potrebno je prostor mogućih pitanja ponovno definirati putem meta podataka. Tehničko rješenje bi se moglo ostvariti putem mobilnih uređaja koji danas postaju sve moćniji. Najveća prepreka u ovom modelu je kvaliteta postavljenih pitanja. Također, legitimnost korisnika koji sudjeluju u stvaranju pitanja i ovjeri odgovora.

5. Daljnja istraživanja

Najvažnije svojstvo predložene metode autentikacije korisnika temeljem znanja predstavljaju pitanja koja se postavljaju. Iako se u prethodnom poglavlju istaknulo više različitih problema i izazova, pitanja predstavljaju najveći i najvažniji. Naime, metoda autentikacije se zasniva na pretpostavci da će legitiman korisnik biti u stanju na postavljena pitanja odgovoriti s lakoćom, dok napadač neće. Samim time, potrebno je veliku pažnju posvetiti tipu pitanja koja se postavlja korisniku. U ovom poglavlju se radnju smjernice za daljnja istraživanja vezana za poboljšanje prethodno opisane metode autentikacije korisnika.

5.1. Prepoznavanje kognitivnog stila korisnika

Jedno od mogućih proširenja autentikacije faktorom znanja može biti uporaba kognitivnog stila za identifikaciju korisnika. Kognitivni stil podrazumijeva više različitih tipova znanja koje korisnik imat. Točnije, faktor znanja bi time dobio nove dimenzije. U nastavku se daju smjernice za oblikovanje tih novih dimenzija.

- Nešto što korisnik zna – predstavlja KBA kako je i do sada opisana. Točnije, u ovu skupinu i dalje ulaze sve metode koje su opisane u poglavlju 2.
- Nešto što korisnik može – podrazumijeva podskup znanja koja se odnose na određene vještine i sposobnosti koje korisnik ima. Na primjer, prepoznavanje uzoraka, rješavanje određenih zadataka, audio-vizualne sposobnosti i drugo. Prvo je potrebno odrediti ima li ovaj faktor dovoljno prostora za pouzdanu autentikaciju korisnika. Odnosno, može li se stvoriti dovoljno velika razlika između vještine dvaju korisnika. Naravno, treba razmotriti jednostavnost oponašanja pojedinih vještina.
- Nešto što opisuje kakav je korisnik – faktor koji se odnosi na korisnikovu osobnost. U ovoj kategoriji postoje dva općenita načina na koji se korisnikova osobnost može provjeravati.

- Profiliranje – podrazumijeva postupak prikupljanja određenog broja uzoraka koji se kasnije uspoređuje s korisnikom. Na primjer, stil pisanja ili izražavanja, prevođenje teksta, asocijacije i drugo.
- Ponašanje – odnosi se na promatranje načina na koji korisnik tipka, pomiče miš ili hoda. Ova metoda je iznimno slična faktoru autentikacije koji se odnosi na biometriju. Iz tog razloga se ne razmatra detaljnije obzirom da ne pripada autentikaciji znanjem.

5.2. Nova metoda klasifikacije pitanja

U poglavlju 2 se opisuju različite metode autentikacije temeljene na znanju. Obzirom na velik broj postojećih metoda postoji potreba za njihovom klasifikacijom. Prethodno opisana Slika 1. prikazuje postojeću metodu klasifikacije metoda. U ovom poglavlju se predlaže nova metoda klasifikacije koja se oslanja na pitanja kao glavno sredstvo provjere identiteta. Naime, čak i u slučaju kada koristi autentikacija lozinkom, postavlja se pitanje. Točnije, pitanje je implicitno i traži se prethodno dogovorena lozinka. Dodatno, predlaže se korištenje više različitih dimenzija koje opisuju tipove pitanja. U nastavku se predlažu neke od tih dimenzija.

- Tip pitanja – označava vrstu pitanja koje se postavlja. U općem slučaju razlikuju se dva tipa pitanja. Prvi tip predstavlja umjetno pitanje poput lozinki i neovisno je o samom korisniku. Odnosno, predstavlja pitanje na koje može odgovoriti i računalo. Drugi tip pitanja je ovisan o korisniku i pretpostavlja se da ga u većini slučajeva računalo ne može odgovoriti. Pitanja koja proizvode DSQ poslužitelji pripadaju ovom tipu pitanja. Obzirom da su ovisna o korisniku, pitanja mogu ispitivati bilo koji dio čovjekovog znanja, karaktera, osobnosti i drugo.
- Gdje se nalazi odgovor – obzirom da se u kontekstu autentikacije ispravni odgovori na pitanja moraju negdje pohraniti, potrebno je uvesti dimenziju koja opisuje mjesto pohrane.
- Oblik odgovora – u poglavlju 2 se opisuju razne metode autentikacije korisnika temeljem znanja. Analizom postojećih metoda vidljivo je kako postoje različiti oblici odgovora koje korisnik može dati. Na primjer, lozinke mogu biti tekstualne, vizualne i grafičke. Odnosno, odgovor može biti u obliku teksta ili slike.

- Korisnička akcija – predstavlja radnju koju korisnik mora obaviti kako bi se autenticirao. Na primjer, mora unijeti neki tajni podataka, prepoznati određenu strukturu ili obaviti neku transformaciju.

Zaključak

Autentikacija korisnika je širok pojam koji podrazumijeva niz različitih disciplina. Većina informacijskih sustava ima potrebu razlikovati jednog korisnika od drugog. Autentifikacija korisnika je neophodan dio u osiguravanju osnovnih sigurnosnih zahtjeva informacijskih sustava. U ovom radu su se analizirale metode autentikacije zasnovane na korisničkom znanju. Jedan od ciljeva ovog rada bio je analizirati i ocijeniti postojeće metode autentikacije temeljene na korisničkom znanju (engl. *KBA – Knowledge-Based Authentication*). Kako bi se ostvario ovaj cilj bilo je potrebno definirati zajedničke mjere ocjenjivanja pouzdanosti metode autentikacije korisnika. Definirane mjere, kao i rezultati su prikazani u poglavlju 3. Prema tim rezultatima, dinamička pitanja zadovoljavaju sve postavljene kriterije. Naravno, konkretni rezultat mjerenje može ovisiti o metodi implementacije pojedinih metoda.

Drugi cilj ovog rada bio je predložiti novu metodu autentikacije temeljnu na dinamičkim pitanjima. Dodatno, novo predstavljena metoda dokazuje mjere vrednovanja koje su opisane u poglavlju 3. Odnosno, pokazuje da se konkretnom metodom autentikacije, koja se temelji na dinamičkim pitanjima, može zadovoljiti svi uspostavljeni kriteriji. Kako se radi o novoj metodi autentikacije korisnika, postoje određena pitanja koja trenutno nisu riješena. Na primjer, protokoli razmjene podataka između FES i DQS poslužitelja te metoda proizvodnje dinamičkih pitanja iz različitih izvora informacija.

Kao dodatan doprinos, u poglavlju 5 su opisani daljnji koraci za istraživanje metoda autentikacije temeljene na znanju. Jedno od prepoznatih proširenja autentikacije faktorom znanja može biti uporaba kognitivnog stila za identifikaciju korisnika. Kognitivni stil podrazumijeva više različitih tipova znanja koje korisnik imat. Faktor znanja bi time dobio nove dimenzije. Osim toga, postoji potreba za klasifikacijom pitanja koja se proizvode za autentikaciju dinamičkom KBA metodom.

_____

Kristian Skračić

Literatura

[1] D. Todorov, Mechanics of User Identification and Authentication: Fundamentals of Identity Management, Auerbach Publications, 2007.

[2] Authentication in an Internet Banking Environment, http://www.ffiec.gov/pdf/authentication_guidance.pdf

[3] M. Shema, C. Davis , Anti-Hacker Tool Kit, Third Edition, Chapter 8, Password Cracking / Brute-Force Tools, McGraw-Hill Osborne Media, 2006.

[4] A. Narayanan, V. Shmatikov, Fast dictionary attacks on passwords using time-space tradeoff, Proceedings of the 12th ACM conference on Computer and communications security CCS 05, 2005.

[5] Y. S. Dandass, Using FPGAs to Parallelize Dictionary Attacks for Password Cracking, Proceedings of the 41st Annual Hawaii International Conference on System Sciences HICSS, 2008.

[6] A Perrig, D. Song, Hash visualization: A new technique to improve real-world securiy, In preceedings of the 1999. International Workshop on Cryptographic Technuques and E-Commerce (CryTEC '99)

[7] W. Jansen, Authenticating Mobile Device User through Image Selection, Data Security, svibanj 2004.

[8] K. Renaud, A. De Angeli, My password is here! An investigation into visuo-spatial authentication mechanisms, Interacting with Computers 16, 2004.

[9] Real User Corporation, About Passfaces, http://www.realuser.com/enterprise/about/about_passfaces.htm, 2012.

[10] D. Davis, F. Monrose, M. Reiter, On user choice in graphical password schemes, Proceedings of the 13th USENIX Security Symposium, 2004.

[11] A. Bauer, Gallery of random art, 1998, http://www.random-art.org/about/

[12] R. Dhamija, A. Perrig, Déjà Vu: A user study using images for authentication, Proceedings of the 9th USENIX Security Symposium, 2000.

[13] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, R. Swanstrom, Picture Password: A Visual Login Technique for Mobile Devices, National Institute of Standards and Technology, 2003.

[14] S. Wiedenbeck, J. Waters, C.J. Birget, A. Brodskiy and N. Memon, PassPoints: Design and longitudinal evaluation of a graphical password system, International Journal of Human Computer Studies, 2005.

[15] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin, The Design and Analysis of Graphical Passwords, in Proceedings of the 8th USENIX Security Symposium, USENIX Association, 1999.

[16] D. Nali, J. Thorpe, Analysing user choice in graphical passwords, Tech. Report TR-04-01, School of Computer Science, Carleton University, Canada, 2004.

[17] C. P. van Oorschot, J. Thorpe,On the security of graphical password schemes, Technical Report TR-05-11. Integration and extension of USENIX Security 2004 and ACSAC 2004 papers, 2004.

[18] J. Thorpe, P. Van Oorschot, Graphical dictionaries and the memorable space of graphical passwords, In Proceedings of the 13th UNIX Security Symposium, kolovoz 2004.

[19] K. Chalkias, A. Alexiadis, G. Stephanides, A multi-grid graphical password scheme, In Proceedings of the 6th International Conference on Artificial Intelligence and Digital Communications, Thessaloniki, Greece, 2006.

[20] S. Gkarafli, A.A. Economides, Comparing the Proof by Knowledge Authentication Techniques, International Journal of Computer Science and Security (IJCSS), Volume (4): Issue (2), 2008.

[21] S. K. Card, T. P. Moran, A. Newell, The model human processor, Handbook of Perception and Human Performance, chapter 45. John Wiley and Sons, 1986.

[22] G. A. Miller, The magical number seven, plus or minus two: Some limits on our capacity for processing information, Psychological Review, 1956.

[23] R. John, Anderson and Christian Lebiere, The Atomic Components of Thought, Lawrence Erlbaum Associates, Inc., 1998.

[24] A. Rabkin, Personal knowledge questions for fallback authentication: Security questions in the era of Facebook, Symposium on Usable Privacy and Security (SOUPS) 2008, srpanj 2008.

[25] M. Jakobsson, E. Stolterman, S. Wetzel, L. Yang, Love and authentication, CHI ’08: Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, 197–200, 2008.

[26] Facebook Statistics, http://www.facebook.com/press/info.php?statistics

[27] V. Griffith, M. Jakobsson, Messin’ with Texas: Deriving mothers maiden names using public records, Applied Cryptography and Network Security (ACNS). Springer, 2005.

[28] Maltego, http://www.paterva.com/maltego

[29] Creepy, http://ilektrojohn.github.com/creepy

[30] Press Releases, FFIEC Releases Supplemental Guidance on Internet Banking Authentication, lipanj 2011., http://www.ffiec.gov/press/pr062811.htm

[31] Supplement to Authentication in an Internet Banking Environment, Federal Financial Institutions Examination Council, 2011.

[32] R. Lemos, Are Your "Secret Questions" Too Easily Answered?, Technology Review, MIT, 2009.

[33] A. Alkhalifah, G. D. Skinner, Enhanced Knowledge Based Authentication Using Iterative Session Parameters, Proceedings of World Academy of Science, Engineering and Technology, 2010.

[34] About IDology, http://www.idology.com/about-idology/about-idology

[35] ExpectID, http://www.idology.com/id-verification/id-verification

[36] IEEE P1363.2 Password-based public-key cryptography, 2002.

[37] IETF RFC 2945, The SRP Authentication and Key Exchange System, Stanford University, 2000.

[38] S. M. Bellovin, M. Merritt, Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks, Proceedings of the IEEE Symposium on Research in Security and Privacy, 1992.

[39] S. Shirali-Shahreza, M. Shirali-Shahreza, Categorizing CAPTCHA, Proceedings of the 4th ACM workshop on Security and artificial intelligence, ACM, 2011.

[40] S. Ansari, S. G. Rajeev, H. S. Chandrashekar, Packet sniffing: a brief introduction, Ieee Potentials, Vol. 21., 2002.

[41] X. Yi, Z. Wen, D. Zhang, Sniffing threat and practices in IPv6 networks, Shenyang Jianzhu Daxue Xuebao Ziran Kexue BanJournal of Shenyang Jianzhu University Natural Science, 2006.

[42] K. Tan, D. Kotz, Saluki: A high-performance Wi-Fi sniffing program, Proceedings of the 8th International Symposium on, 2010.

[43] A. Ornaghi, Man in the middle attacks Demos The scenario, Blackhat Conference, 2003.

[44] Z. Trabelsi, K. Shuaib, Man-in-the-middle intrusion detection, Security Systems SymposiumIEEE GlobeCom, 2006.

[45] P. Burkholder, SSL man-in-the-middle attacks, SANS Institue InfoSec Reading, 2003.

[46] Password Keeper, Advanced Password Cracking – Insight Smartphone Forensics : Cracking BlackBerry Backup, Beaver 2010.

[47] I. M. Baggili, Mobile Phone Forensics Tool Testing : A Database Driven Approach, International Journal, 2007.

[48] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, E. A. Nabbus, Electronic Authentication Guideline, NIST Special Publication 800-63-1, 2011.

[49] J. B. Bolten, E-Authentication Guidance for Federal Agencies, OMB M-04-04, 2003.

[50] P. Vassiliadis, DATA WAREHOUSE METADATA, Department of Computer Science, University of Ioannina, 2007.

[51] C. Utley, Designing the Star Schema Database, version 1.1, 2008.

[52] C.N. Gupta, R. Palaniappan, and S. Swaminathan, "On the analysis of various techniques for a novel brain biometric system," International Journal of Medical Engineering and Informatics, vol. 1, issue 2, pp. 266 – 273, 2008.

[53] R. Palaniappan, and D. P. Mandic, "EEG Based Biometric Framework for Automatic Identity Identification," International Journal of VLSI Signal Processing Systems for Signal, Image and Video Technology (special issue on Data Fusion for Medical, Industrial, and Environmental Applications), vol. 49, no.2, pp. 243-250, 2007.

[54] F. Bergadano, D. Gunetti, C. Picardi, User authentication through keystroke dynamics, ACM Transactions on Information and System Security, 2002.

[55] M. Pusara, C. E. Brodley, User re-authentication via mouse movements, Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security , 2004.

[56] H. Y. Chiena, J. K. Jana, Y. M. Tsengb, An Efficient and Practical Solution to Remote Authentication: SmartCard, Computers & Security, Volume 21, Issue 4, 1 2002.

[57] A. K. Hrechak, J. A. McHugh, Automated fingerprintrecognition using structural matching, Pattern Recognition, Volume 23, Issue 8, 1990.

[58] M. A. Turk, Face recognition using eigenfaces, Computer Vision and Pattern Recognition, 1991. Proceedings CVPR '91., 1991.

[59] R. Brunelli, Face recognition: features versus templates, Pattern Analysis and Machine Intelligence, 1993.

[60] R. Dhamija, J. D. Tygar, M. Hearst, Why phishing works, Proceedings of the SIGCHI conference on Human Factors in computing systems, 2006.

[61] M. J. Beller, Fully-fledged two-way public key authentication and key agreement for low-cost terminals, Electronics Letters, 1993.

[62] S. Chokhani, Knowledge Based Authentication (KBA) Metrics, Orion Security Solutions, 2004.

Sažetak

Jednokratna autentikacija zasnovana na znanju korisnika

Nedostatak autentikacije lozinkom je u laganom otimanju tog podatka, prisilom ili prijevarom. U ovom radu su se analizirale metode autentikacije zasnovane na korisničkom znanju. Jedan od ciljeva ovog rada bio je analizirati i ocijeniti postojeće metode autentikacije temeljene na korisničkom znanju (engl. *KBA – Knowledge-Based Authentication*). Kako bi se ostvario ovaj cilj potrebno je definirati zajedničke mjere ocjenjivanja pouzdanosti metode autentikacije korisnika. U radu se definiraju mjere ocjenjivanja te ističu rezultati usporedbe pojedinih metoda autentikacija. Prema tim rezultatima, dinamička pitanja zadovoljavaju sve postavljene kriterije. Iz tog razloga se upravo ova metoda odabire kao osnova za ostvarenje drugog cilja. Naime, drugi cilj ovog rada je predlaganje nove metode autentikacije temeljne na korisničkom znanju.

Ključne riječi: autentikacija korisnika, KBA, Knowledge Based Authentication, statička KBA, dinamički KBA, grafičke lozinke, vizualne lozinke, tekstualne lozinke, ZKPP, dokazi bez poznavanja

Summary

One-time knowledge based chalange response authentication

The lack of password based authentication schemes is in the fact that passwords can be easily stolen. This paper is focused on authentication methods based on user knowledge. One of the objectives of this study was to analyze and evaluate existing methods of user authentication based on knowledge. To achieve this goal it is necessary to define a common measure of reliability in order to evaluate existing authentication methods. This paper defines and uses a set of measures to evaluate existing authentication methods. According to these results, the dynamic question based authentication method meet all the necessary criteria. This is the reason why dynamic questions were chosen to be the basis for achieving the second objective of this paper. The second objective of this paper is to propose a new method of authentication based on user knowledge.

Keywords: user authentication, KBA, Knowledge-Based Authentication, static KBA, KBA dynamic, graphical passwords, passwords, visual, textual passwords, ZKPP, zero knowledge proofs

Privitak

U privitku ovog rada se nalazi CD s dokumentom u PDF obliku, te scenarijima koji prikazuju predloženu metodu autentikacije korisnika. Scenariji su napravljeni pomoću alata GNS3 (*Graphical Network Simulator*).

Instalacija programske podrške

Kako bi se koristio alat GNS3, potrebno je instalirati dodatke u nastavku. Ukoliko se koristi operacijski sustav Windows, moguće je preuzeti all-in-one instalacijsku datoteku koja sadrži sve potrebne dodatke. Datoteku je moguće naći na adresi: http://www.gns3.net/download/

- Dynamips
- Qemu/Pemu
- Putty
- VPCS
- WinPCAP
- Wireshark

Upute za korištenje programske podrške

U direktoriju *Simulacije*, nalaze se scenariji koji su opisani u poglavlju 4. Alat GNS3 koristi datoteke s ekstenzijom *.net* kako bi pohranio trenutnu mrežnu konfiguraciju. Potrebno je željenu *.net* datoteku otvoriti putem GNS3 alata kako bi se prikazao pojedini scenarij.