CARNET

Višefaktorska autentifikacija

CERT.hr-PUBDOC-2018-12-370

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

U raznim fizičkim i elektroničkim sustavima često je potrebno osigurati da samo određeni ljudi smiju pristupiti odgovarajućim resursima. Primjerice:

- vlasnik stana želi osigurati da samo on može ući u svoj stan,
- banka želi osigurati da samo vlasnik računa može pristupiti novcima na tom računu,
- korisnik e-pošte želi osigurati da samo on može pristupiti svojim porukama.

Općenito, taj se postupak naziva **kontrola pristupa (eng. *access control*)**. Kontrolu pristupa moguće je podijeliti na tri temeljna postupka:

- identifikacija,
- autentifikacija
- i autorizacija.

Ta tri postupka najbolje je objasniti kroz primjer. Uzmimo za primjer korisnika, Ivana Horvata, koji pokušava pristupiti svojem računu e-pošte. U prvom koraku, Ivan se spaja na sustav e-pošte te upisuje svoje korisničko ime (npr. *ivan.horvat*) ili svoju adresu e-pošte (*ivan.horvat@carnet.hr*). Ovaj se korak naziva **identifikacija** – u njemu **korisnik izjavljuje tko je on**. Kada bi samo ovaj korak bio dovoljan za uspješnu prijavu, ne bi bilo nikakve sigurnosti – napadač bi mogao upisati bilo koje korisničko ime i tako nedozvoljeno pristupiti tuđem računu.

Zato, u narednom koraku sustav traži od korisnika da upiše lozinku kako bi **dokazao svoj identitet**. Drugim riječima, sustav traži nekakvu potvrdu da je korisnik koji pristupa računalu zaista Ivan Horvat. Taj se postupak naziva **autentifikacija**. Navedeni dokaz identiteta nikada nije savršen – u ovom primjeru, napadač može nekako saznati lozinku Ivana Horvata i lažno se predstaviti u njegovo ime. No u svakom slučaju, ovaj postupak daje neku razinu vjerodostojnosti tvrdnji da je korisnik za računalom zaista Ivan Horvat.

Nakon upisivanja lozinke, kada je sustav uvjeren da je korisnik zaista Ivan Horvat, potrebno je odlučiti što Ivan Horvat zapravo smije. U ovom slučaju, Ivan Horvat će dobiti pristup računu e-pošte s adresom *ivan.horvat@carnet.hr*, tj. dobit će mogućnost čitanja poruka pristiglih na tu adresu te slanja poruka s te adrese. Naravno, Ivan Horvat neće dobiti pristup računu bilo kojeg drugog korisnika. Ovaj se postupak naziva **autorizacija**.

Kao i mnoge stvari u današnjem svijetu, i ovaj postupak kontrole pristupa je često automatiziran, tj. provodi ga računalni sustav. U tom kontekstu, osmišljanje i implementacija sigurnog postupka autentifikacije je posebno velik izazov. Cilj ovog dokumenta je objasniti kako postići izrazito visoku razinu sigurnosti autentifikacije kroz tzv. **višefaktorsku autentifikaciju**.

2 Autentifikacijski faktori

Ključ razumijevanja višefaktorske autentifikacije je razumijevanje tzv. autentifikacijskih faktora te njihovih prednosti i mana. Autentifikacijski faktor je **skup metoda za autentifikaciju koje dijele neke zajedničke odlike**. Metode autentifikacije se obično grupiraju u sljedeća tri autentifikacijska faktora:

- **„nešto što osoba zna“** (eng. *something you **know***),
- **„nešto što osoba posjeduje“** (eng. *something you **have***),
- **„nešto što osoba je**“ (eng. *something you **are***).

U ovom će poglavlju biti predstavljen svaki od navedenih autentifikacijskih faktora, uključujući konkretne metode autentifikacije te njihove prednosti i mane.

2.1 Nešto što osoba zna (eng. *something you know*)

Sigurnost autentifikacijskog faktora „nešto što osoba zna“ temelji se na nekoj **tajnoj informaciji** koju **samo odgovarajući korisnik** zna. Ta tajna informacija je najčešće lozinka ili PIN. Postupak autentifikacije je prilično jednostavan – korisnik sustavu predaje lozinku, PIN ili ekvivalentu informaciju te time dokazuje svoj identitet. Kada bi se napadač htio lažno predstaviti kao neka druga osoba, on to u načelu ne može, jer ne zna njegovu lozinku/PIN.

U kontekstu računalnih sustava, metode ovog faktora je često jednostavno i jeftino implementirati jer nije potrebna nikakva posebna oprema ni sa strane korisnika, ni u drugim dijelovima sustava. Zato je ovaj faktor često korišten za autentifikaciju na računala i na mrežne usluge kao što su e-pošta i razne web aplikacije. Nažalost, iako je ovaj faktor jeftino implementirati te u teoriji on može biti prilično siguran, u stvarnosti, njegova sigurnost često nije zadovoljavajuća.

Jedan od razloga je sljedeći – kada korisnici sami smišljaju lozinke, PIN-ove i slično, oni to obično rade **na izrazito predvidljiv način**. Napadači mogu koristiti tu predvidljivost da pogode žrtvinu lozinku ili PIN.

Istraživanja o najčešće korištenim lozinkama mogu dočarati koliki je ovo zaista problem. Analiza tvrtke *SplashData* pokazuje da je najčešće korištena lozinka „123456“ te da nju koristi **skoro 4% korisnika** (1). Drugim riječima, ako se napadač pokušava lažno predstaviti i unese lozinku „123456“, to će mu uspjeti za svakog 25. korisnika. U navedenoj je analizi moguće vidjeti da ostale najčešće lozinke uključuju „password“, „12345678“ i „qwerty“ te da **preko 10% korisnika koristi neku od 25 najčešće korištenih lozinki** (1).

Kod pogađanja lozinki, napadači ne koriste samo informacije o najčešće korištenim lozinkama, već i o **najčešćim načinima kako korisnici smišljaju lozinke**. Primjerice, ako sustav traži da lozinke sadržavaju velika slova, mala slova i brojeve te da lozinke moraju biti izmijenjene svaka 3 mjeseca, to se naizgled čini prilično sigurno. No i u takvim slučajevima su korisnici predvidljivi, pa će na temelju prethodno navedenih zahtjeva doći do lozinke kao što je „Jesen2018“. Napadači koriste ovakvu predvidljivost korisnika uz

alate za automatizirano, uzastopno isprobavanje lozinki i na taj način neovlašteno dobivaju pristup tuđim korisničkim računima.

Kao odgovor na ovakvu predvidljivost, oprezniji korisnici znaju osmisliti prilično složene i nepredvidljive lozinke ili čak koriste nasumično generirane lozinke. U jednu ruku, to je odlično – sada je lozinka složena i nepredvidljiva te ju napadač neće moći pogoditi. No s druge strane, takvu lozinku je prilično teško zapamtiti. Zbog lozinki koje je teško pamtiti korisnici često rade druge kompromise – **lozinku zapisuju** negdje i/ili **koriste istu lozinku** na više mjesta.

Zapisivanje lozinke nije dobro, no u praksi, ono samo po sebi obično ne uzrokuje toliku štetu, jer ako je napadač nekako došao do zapisane lozinke, on obično već ima pristup žrtvinom računalu ili nekom zaštićenom prostoru.

Korištenje iste lozinke na više mjesta je vjerojatno najveći od do sada navedenih problema (2). U tom slučaju, dovoljno je da napadač jednom kompromitira tu zajedničku lozinku i imat će pristup svim servisima za koje je ta lozinka korištena. Koliko god ta zajednička lozinka bila složena, i koliko god korisnik brinuo o njenoj sigurnosti (nigdje ju ne zapisuje, ne dijeli ju ni s kim), ona će i dalje često završiti u napadačevim rukama **zbog nemara pružatelja usluga**. Već godinama se redovito događaju napadi na sustave raznih pružatelja usluga u kojima napadači dolaze do podataka korisnika. Osim što ti korisnički podaci uključuju osobne informacije, oni često uključuju i **slabo zaštićeni ili potpuno nezaštićeni zapis lozinke**. Ovakve kompromitacije su izrazito ozbiljan i učestali problem – na web stranici *Have I Been Pwned* je za sada dokumentirano preko 300 takvih slučajeva za koje se javno zna (3). Sveukupni broj je zasigurno i veći. Nisu samo mali, nepoznati servisi bili nemarni – pokazalo se da čak i neke od najvećih tvrtki nisu brinule o sigurnom zapisivanju lozinke, primjerice:

- U lipnju 2011. godine, kompromitirani su sustavi tvrtke ***Sony*** vezani za web stranice na domenama *sonypictures.com*, *sonybmg.nl* i *sonybmg.be*. Ukradeni su podaci o korisnicima (navodno preko milijun korisničkih računa) koji su sadržavali lozinke u potpuno nezaštićenom (eng. *plain text*) obliku. Dio korisničkih podataka je i javno objavljen. (4)

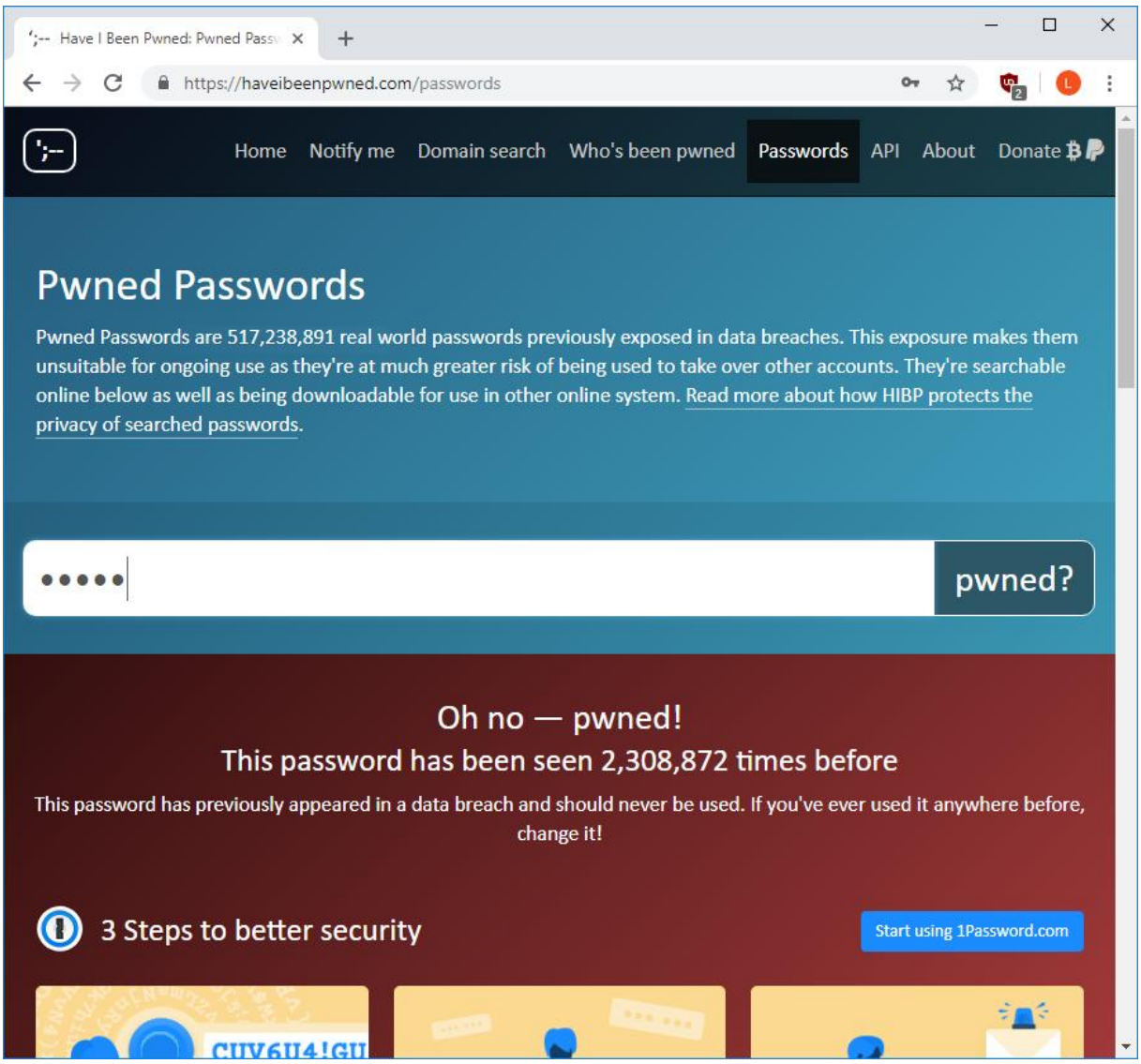
- U svibnju 2012. godine, kompromitirani su sustavi web stranice ***LinkedIn*** te su ukradeni (i kasnije prodavani) podaci od 117 milijuna korisnika, uključujući slabo zaštićene zapise lozinki. (5)

- U srpnju 2012. godine kompromitirani su sustavi servisa ***Yahoo! Voices*** te su, između ostaloga, javno objavljene potpuno nezaštićene (eng. *plain text*) lozinke od preko 450.000 korisnika. (6)

- U listopadu 2013. godine kompromitirani su sustavi tvrtke ***Adobe*** te su javno objavljeni podaci od preko 150 milijuna korisnika. Ti podaci su uključivali slabo zaštićene zapise lozinki te potpuno nezaštićene (eng. *plain text*) podsjetnike za lozinku (eng. *password hint*). (7)

Prethodno spomenuta web stranica *Have I Been Pwned* pruža korisnu uslugu za krajnje korisnike – na ovoj poveznici moguće je upisati neku lozinku i provjeriti je li se ona pojavila u nekome od do sada javno objavljenih skupova kompromitiranih podataka. Na

slici 1 prikazan je primjer korištenja navedene usluge – upisana je lozinka „12345“ za koju web stranica kaže da je viđena preko 2 milijuna puta u javno objavljenim skupovima kompromitiranih podataka.



Slika 1 – provjera pojavljivanja lozinke u javno objavljenim skupovima kompromitiranih podataka na servisu *Have I Been Pwned*

Osim lozinki, u ovom faktoru se često koriste i PIN-ovi. PIN-ovi su u srži isti kao lozinke, samo se češće koriste u fizičkim sustavima gdje je praktičnije unijeti kratki broj putem numeričke tipkovnice te gdje je broj ponovnih pokušaja unosa strogo ograničen. Prethodno opisani problemi s lozinkama prisutni su i kod PIN-ova. Istraživanje iz 2012. godine analiziralo je kompromitirane, javno objavljene lozinke te je izdvojilo sve lozinke koje su se sastojale od četiri znamenke pod pretpostavkom da će one otkriti nešto o načinu kako ljudi biraju PIN-ove (8). Pokazalo se da su i u ovom slučaju korisnici predvidljivi – među najčešćim četveroznamenkastim brojevima su bili 1234, 0000 i 1111, a uz takve brojčane uzorke, često su se pojavljivali brojevi koji su odgovarali nekoj godini u 20. stoljeću (npr. 1980) ili nekom datumu (npr. 3012) (8).

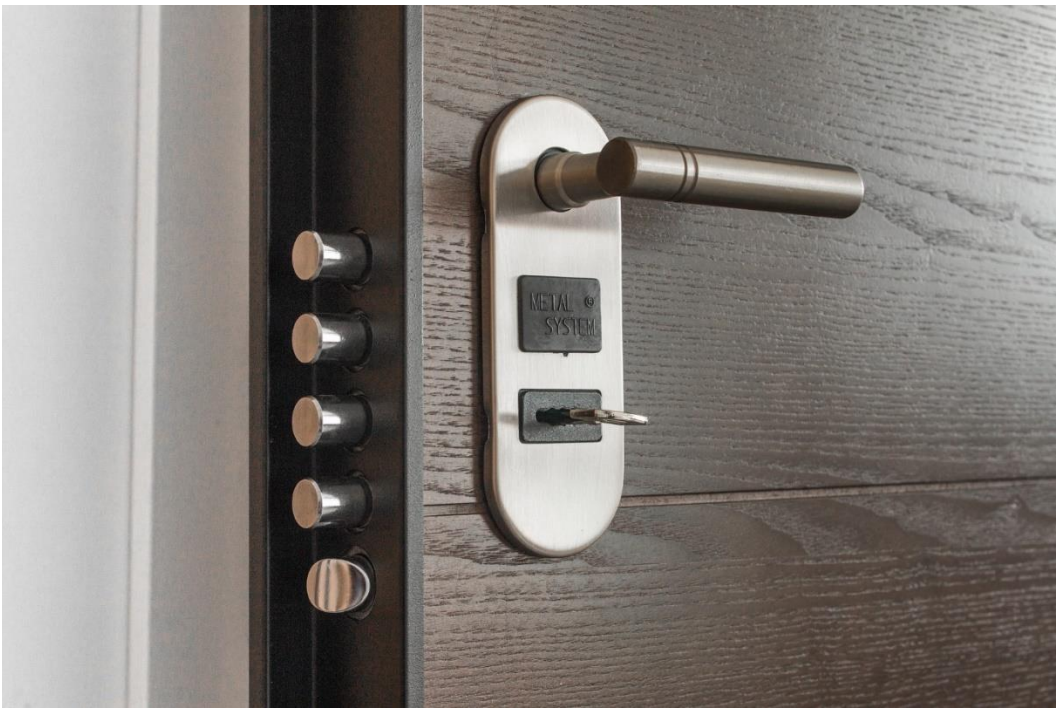
Jedna stvar koju treba uzeti u obzir kod ovog autentifikacijskog faktora je da korisnik može zaboraviti svoju lozinku ili PIN. U takvim slučajevima, poželjno je korisniku omogućiti autentifikaciju na neki drugi način. Jedno često rješenje za takve slučajeve je korištenje tzv. **sigurnosnog pitanja**. U tom rješenju, kod prve prijave u sustav, tj. uspostave identiteta u njemu, korisnik odabire pitanje na koje samo on zna odgovor, primjerice „Koje je ime Vašeg prvog kućnog ljubimca?“, te se zatim odgovor na to pitanje koristi kao tajna informacija za ovaj alternativni način autentifikacije. Metoda autentifikacije putem takvog sigurnosnog pitanja također spada u ovaj autentifikacijski faktor te sa sobom nosi i prethodno opisane rizike – isto kako napadač može pogoditi lozinku/PIN, tako može pogoditi i odgovor na sigurnosno pitanje. Upravo zato je tajnost odgovora na sigurnosno pitanje jednako bitna kao i tajnost same lozinke/PIN-a.

2.2 Nešto što osoba posjeduje (eng. *something you have*)

Sigurnost metoda autentifikacijskog faktora „nešto što osoba posjeduje“ temelji se na nekom **objektu kojega samo odgovarajući korisnik posjeduje**. Ovaj faktor moguće je implementirati na razne načine, no općenito, kada je potrebna autentifikacija:

- legitiman korisnik može se autentificirati pomoću navedenog objekta kojega samo on posjeduje,
- a napadač koji se pokušava lažno predstaviti ne može se autentificirati upravo zato što ne posjeduje navedeni objekt.

Vjerojatno najpoznatija metoda ovog autentifikacijskog faktora je korištenje **ključa i brave**, primjerice na vratima neke zaštićene prostorije kao što je prikazano na slici 2. U tom slučaju, ključ je objekt kojega samo legitiman korisnik posjeduje, a brava je izrađena tako da ju isključivo taj ključ može otključati.



Slika 2 – primjer ključa koji otključava bravu na vratima

Osim metoda koje koriste ključ i bravu, česte su i autentifikacijske metode koje koriste neki oblik **kartice** te odgovarajući čitač kartica. Autentifikacija pomoću kartica može biti izvedena na razne načine – od jednostavnijih, ali nesigurnijih načina, do složenijih i sigurnijih načina.

U jednostavnijoj varijanti, kartica je zapravo samo **specijalizirani uređaj za pohranu podataka**. Podaci povezani s korisnikom zapisani su na karticu na magnetskoj traci ili u čipu koje zatim specijalizirani čitač može pročitati. Primjer kartice s magnetskom trakom te odgovarajućeg čitača prikazan je na slici 3. Primjer kartice s memorijskim čipom kojega je moguće očitati na daljinu RFID tehnologijom (skraćeno od eng. ***R**adio-**f**requency **id**entification*) te odgovarajućeg čitača prikazan je na slici 4. Uz kartice, postoje i razne značke, privjesci te slični uređaji koji su zapravo funkcionalno isti kao i prethodno opisane

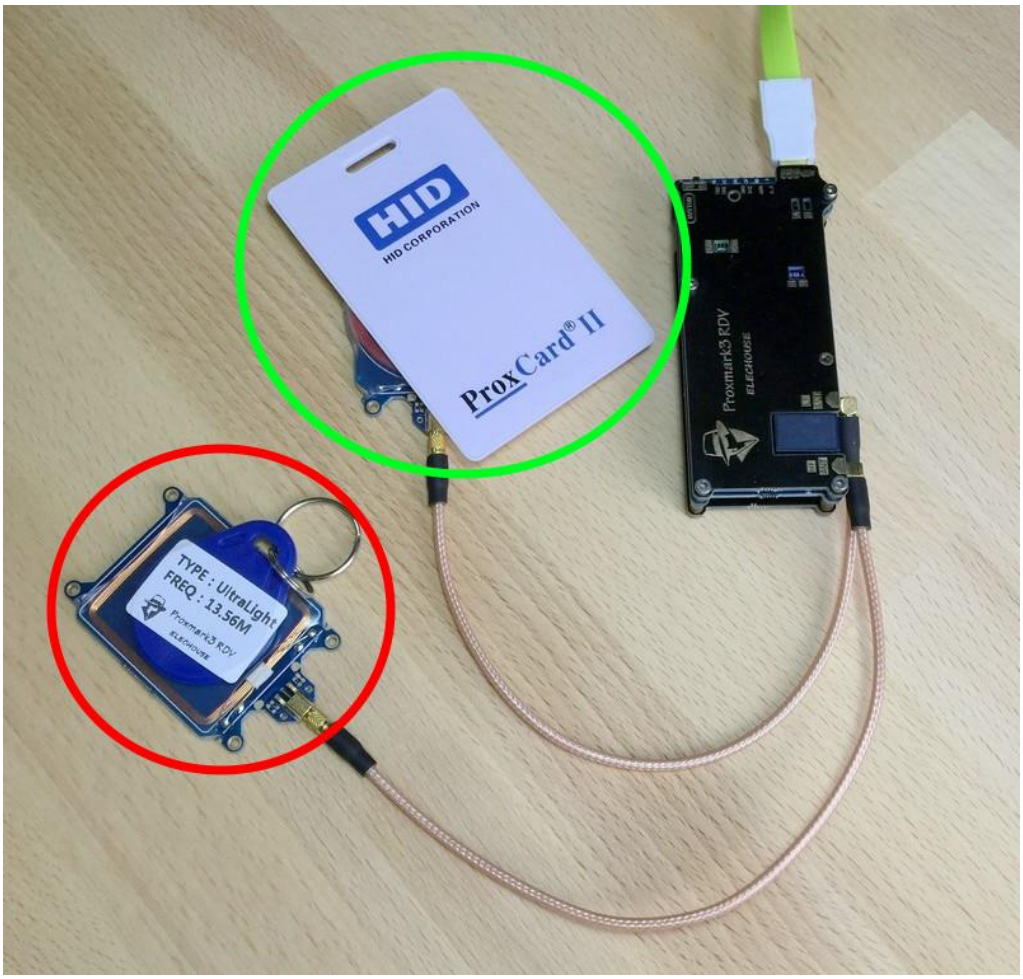
kartice, samo u drugačijem fizičkom obliku. Na slici 5 prikazan je primjer privjeska koji koristi RFID tehnologiju te odgovarajućeg čitača – prikazani je privjesak zapravo funkcionalno isti kao i RFID kartica na slici 4, samo u drugačijem fizičkom obliku.

Slika 3 – primjer kartice s magnetskom trakom te odgovarajućeg čitača (izvor)

Slika 4 – primjer RFID kartice te odgovarajućeg čitača (izvor)

Slika 5 – primjer RFID privjeska te odgovarajućeg čitača (izvor)

Prethodno navedene kartice i ostali uređaji jeftiniji su za izradu, no ujedno su i **nesigurniji** jer su široko dostupni alati pomoću kojih je moguće napraviti funkcionalnu kopiju takve kartice/uređaja. Taj postupak izrade funkcionalne kopije naziva se i **kloniranje** kartice/uređaja. Kao primjer, na slici 6 prikazan je postupak kloniranja RFID privjeska. Nakon kloniranja privjeska (označenog crvenom bojom) prikazanom će karticom (označenom zelenom bojom) biti moguće otključati sva vrata koja otključava i privjesak.



Slika 6 – primjer kloniranja RFID privjeska; nakon kloniranja privjeska (označenog crvenom bojom) prikazanom će karticom (označenom zelenom bojom) biti moguće otključati sva vrata koja otključava i privjesak (izvor)

Sigurnija, ali složenija i skuplja varijanta kartica su tzv. **pametne kartice (eng. *smart cards*)**. One na sebi imaju čip koji je zapravo malo **računalo**. U njihovom slučaju, autentifikacija se ne svodi samo na očitavanje podataka, već se ona temelji na nekom sigurnom kriptografskom protokolu. Konkretnije, pametne kartice imaju vlastiti digitalni certifikat kojim mogu osigurati komunikaciju te dokazati identitet korisnika.

Široko korišteni primjer pametnih kartica su moderne bankovne kartice. Primjer bankovne kartice koja je ujedno i pametna kartica prikazan je na slici 7. Moguće je prepoznati da se radi o pametnoj kartici po kontaktima ugrađenog računala (označeni crveno na slici 7). Uz bankovne kartice, još jedan primjer pametnih kartica su elektroničke osobne iskaznice Republike Hrvatske. Primjer elektroničke osobne iskaznice prikazan je na slici 8.

Slika 7 – primjer bankovne kartice koja je ujedno i pametna kartica (kontakti ugrađenog računala označeni su crveno)

Slika 8 – primjer elektroničke osobne iskaznice Republike Hrvatske (izvor)

Pametne kartice mogu se koristiti priključivanjem na čitač (prikazano na slici 9), a neke se mogu koristiti čak i beskontaktno (prikazano na slici 10). No u oba slučaja, one su pažljivo oblikovane i izrađene tako da tako da ih napadač ne može klonirati ni izvući bilo kakve osjetljive informacije iz njih.

Slika 9 – korištenje pametne kartice priključivanjem na čitač (izvor)

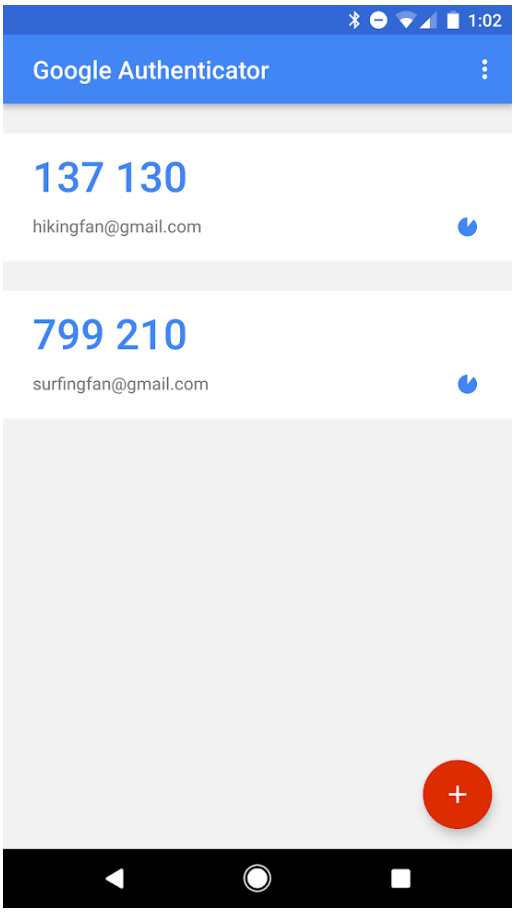
Slika 10 – beskontaktno korištenje pametne kartice (izvor)

Uz pametne kartice, postoje i uređaji koji funkcioniraju na gotovo isti način, samo što imaju drugačiji fizički oblik i priključak. Primjerice, postoje uređaji s USB priključkom koji su funkcionalno gotovo isti kao i pametne kartice. Takve uređaje je moguće izravno koristiti na bilo kojem računalu s USB priključkom bez ikakvog dodatnog čitača. Primjer jednog takvog uređaja prikazan je na slici 11.

Slika 11 – uređaj s USB priključkom koji je funkcionalno gotovo isti kao i pametna kartica (izvor)

Ovom autentifikacijskom faktoru također pripadaju i metode koje koriste **sigurnosni token za generiranje jednokratne lozinke**. Takav sigurnosni token može biti izveden fizički, kao samostalni uređaj, ili softverski, primjerice kao aplikacija na pametnom telefonu. Na slici 12 prikazan je primjer sigurnosnog tokena za generiranje jednokratne lozinke u obliku samostalnog uređaja, a na slici 13 prikazan je primjer sigurnosnog tokena za generiranje jednokratne lozinke u obliku aplikacije za pametni telefon.

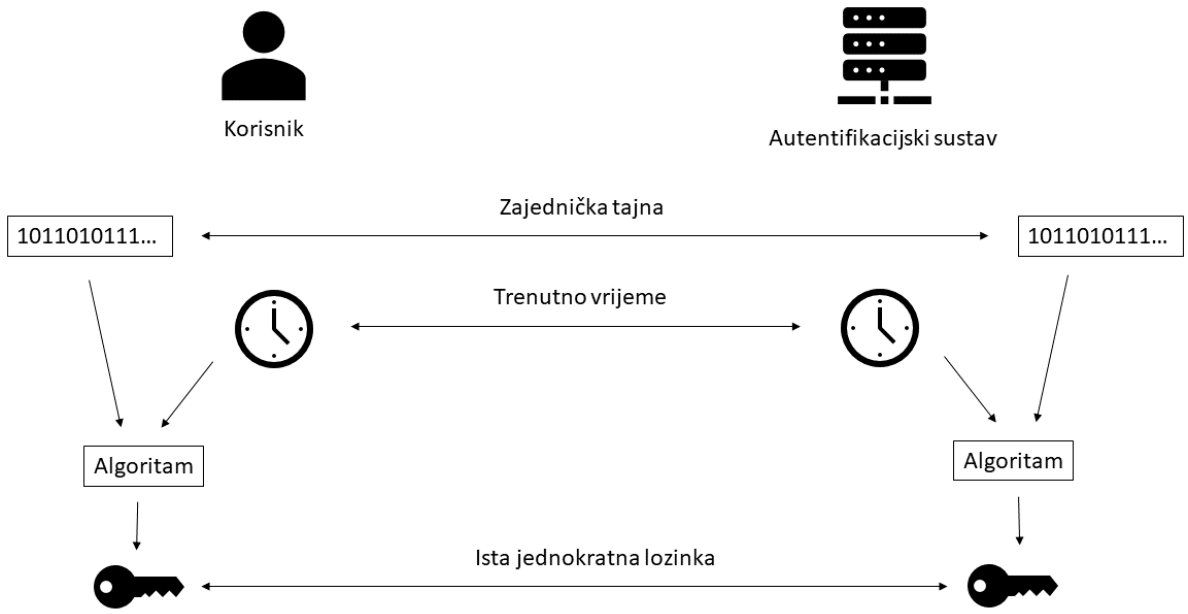
Slika 12 – sigurnosni token za generiranje jednokratne lozinke u obliku samostalnog uređaja; na zaslonu je prikazana trenutna jednokratna lozinka (izvor)



Slika 13 – sigurnosni token za generiranje jednokratne lozinke u obliku aplikacije za pametni telefon; na zaslonu su prikazane trenutne jednokratne lozinke za dva različita računa e-pošte (izvor)

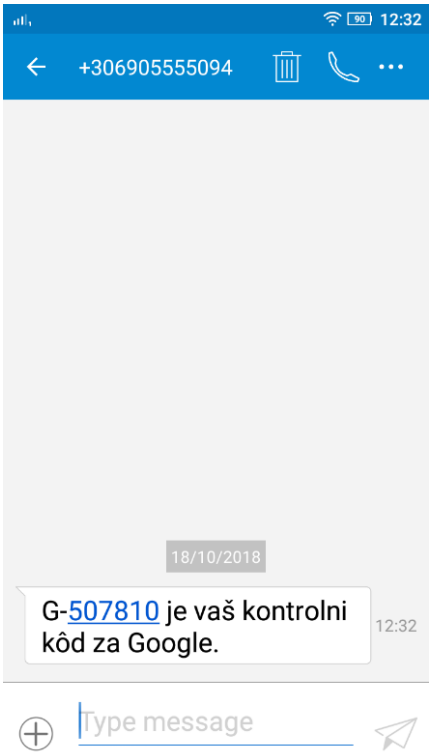
Kao što i ime kaže, svrha ovakvih sigurnosnih tokena je **generiranje jednokratne lozinke** pomoću koje se zatim provodi autentifikacija. Unatoč tome što se autentifikacija u konačnici provodi lozinkom, ova metoda ne spada u faktor „nešto što osoba zna“, jer ovo nije vrsta lozinke koju korisnik ikako može znati ili pamtiti – ova lozinka se redovito mijenja, a generira ju sigurnosni token pomoću kriptografskog algoritma. Zato se sigurnost ove metode temelji na tome da samo legitimni korisnik posjeduje odgovarajući sigurnosni token (u obliku samostalnog uređaja ili pametnog telefona) i time ova metoda spada u faktor „nešto što osoba posjeduje“.

Kako bi generirali jednokratnu lozinku, prethodno opisani sigurnosni tokeni se oslanjaju na tajnu informaciju (u pravilu jedan veliki, nasumični broj) koju znaju samo oni i sustav kojemu se autentificiraju (npr. sustav banke). Konkretno, sigurnosni tokeni generiraju jednokratne lozinke pomoću navedene tajne i trenutnog vremena – na taj način mogu generirati novu, naizgled nasumičnu lozinku svake minute. Kako sustav kojemu se korisnik autentificira pomoću ovakvog sigurnosnog tokena također zna tu tajnu, i on može pomoću tajne i trenutnog vremena generirati istu jednokratnu lozinku te provjeriti podudara li se ona s predanom lozinkom. Na slici 14 prikazan je dijagram navedenog postupka generiranja jednokratne lozinke. Sigurnosni tokeni za generiranje jednokratne lozinke često koriste standardizirani algoritam za prethodno navedeni postupak zvan *Time-Based One-Time Password Algorithm*, skraćeno TOTP (9).



Slika 14 – generiranje jednokratne lozinke na temelju zajedničke tajne i trenutnog vremena

Jedna relativno jednostavna metoda ovog faktora je **slanje tajnog koda** korisniku putem SMS poruke ili poziva na njegov mobitel. Sustav kojemu se korisnik autentificira šalje taj tajni kod, korisnik ga prima putem svog mobitela te unosi prilikom autentifikacije. Slično kao i sigurnosni token u obliku aplikacije na pametnom telefonu, i u ovoj metodi je „nešto što osoba posjeduje“ njen mobitel. Na slici 15 prikazan je primjer SMS poruke s tajnim kodom za autentifikaciju kojega je u ovom slučaju poslao servis *Gmail*.



Slika 15 – primjer SMS poruke s tajnim kodom za autentifikaciju koji je u ovom slučaju poslao servis *Gmail*

Jedan općeniti rizik metoda ovog autentifikacijskog faktora je **krađa** objekta kojega bi samo legitimni korisnik trebao posjedovati. U slučaju da napadač uspije ukrasti, ili čak i na kratko pristupiti navedenom objektu, to znači da se on može i lažno predstaviti u ime korisnika.

Većina ostalih sigurnosnih rizika ovog autentifikacijskog faktora svojstvena je konkretnoj metodi autentifikacije. Primjerice, u slučaju prethodno opisanih jednostavnijih, ali nesigurnijih kartica koje se udaljeno očitavaju RFID tehnologijom, napadači ne moraju nužno ukrasti karticu, već ju mogu udaljeno klonirati s udaljenosti od otprilike jednog metra (10).

U slučaju korištenja sigurnosnih tokena koji generiraju jednokratne lozinke ili kod slanja tajnog koda na mobitel, napadač može doći do jednokratne lozinke/tajnog koda kroz *phishing* napad (11). Uz to, u slučaju kada se jednokratna lozinka generira na mobitelu, odnosno kada se tajni kod prima na mobitelu, napadač kompromitacijom mobitela može doći do jednokratne lozinke/tajnog koda.

Metoda u kojoj korisnik prima tajni kod putem SMS-a ili poziva na mobitel također je ranjiva na tzv. *SIM swap* napade. U *SIM swap* napadima, napadač preuzme kontrolu nad brojem telefona žrtve, pa na temelju toga može i primiti tajni kod putem SMS-a odnosno poziva (12). U *SIM swap* napadima, napadač ne napada žrtvu izravno, već napada pružatelja mobilnih usluga, te pomoću socijalnog inženjeringa ili podmićivanja zaposlenika uspijeva preuzeti kontrolu nad tuđim brojem telefona (12).

Među najsigurnijim rješenjima ovog autentifikacijskog faktora su pametne kartice i ekvivalentni uređaji (13; 14). Dobra implementacija ovakvog rješenja trebala bi biti imuna na *phishing* napade (13; 14).

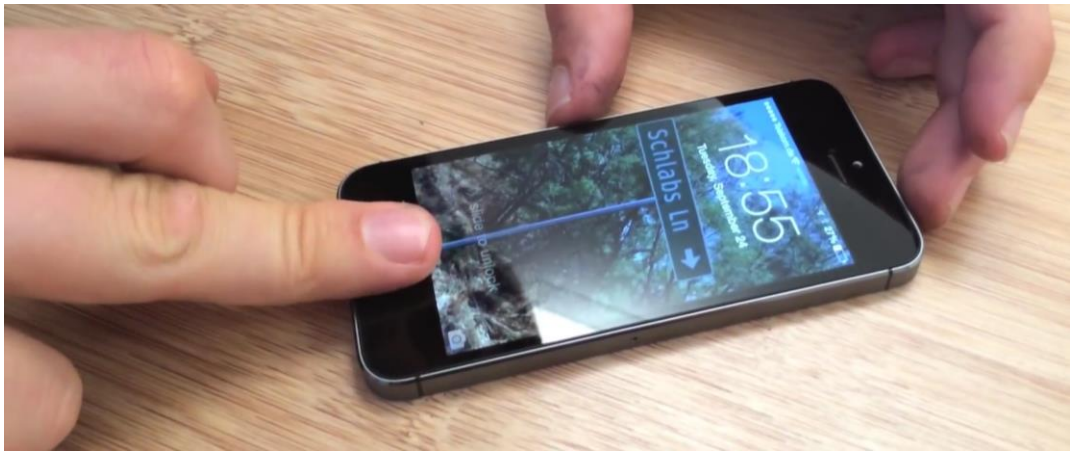
U slučaju prethodnog autentifikacijskog faktora („nešto što osoba zna“) korisnik može zaboraviti tajnu informaciju na koju se oslanja metoda autentifikacija. Slično tome, u slučaju ovog faktora („nešto što osoba posjeduje“) korisnik može izgubiti objekt (karticu, privjesak, mobitel...) na kojega se oslanja metode autentifikacije. I u ovom je slučaju potrebno uzeti to u obzir te je zato često poželjno korisniku omogućiti alternativnu metodu autentifikacije.

2.3 Nešto što osoba je (eng. *something you are*)

Sigurnost metoda autentifikacijskog faktora „nešto što osoba je“ temelji se na nekom **obilježju koje samo odgovarajući korisnik ima**. Primjerice, kao navedeno obilježje mogu se koristiti otisci prstiju, uzorci na šarenici ili mrežnici oka, karakteristike glasa, oblik lica, uzorci krvnih žila na dlanu i slično. Navedena obilježja su jedinstvena svakoj osobi te se ne mijenjaju, pa su zato pogodna korištenju za autentifikaciju. Kako se ovakva autentifikacija temelji na mjerenju nekih bioloških karakteristika korisnika, ona se naziva i **biometrijska autentifikacija**.

Nekada je bilo skupo implementirati gotovo bilo kakvu metodu biometrijske autentifikacije, no s vremenom, cijena implementacije je pala, pa se danas razne metode ovog faktora mogu koristiti čak i na pametnim telefonima.

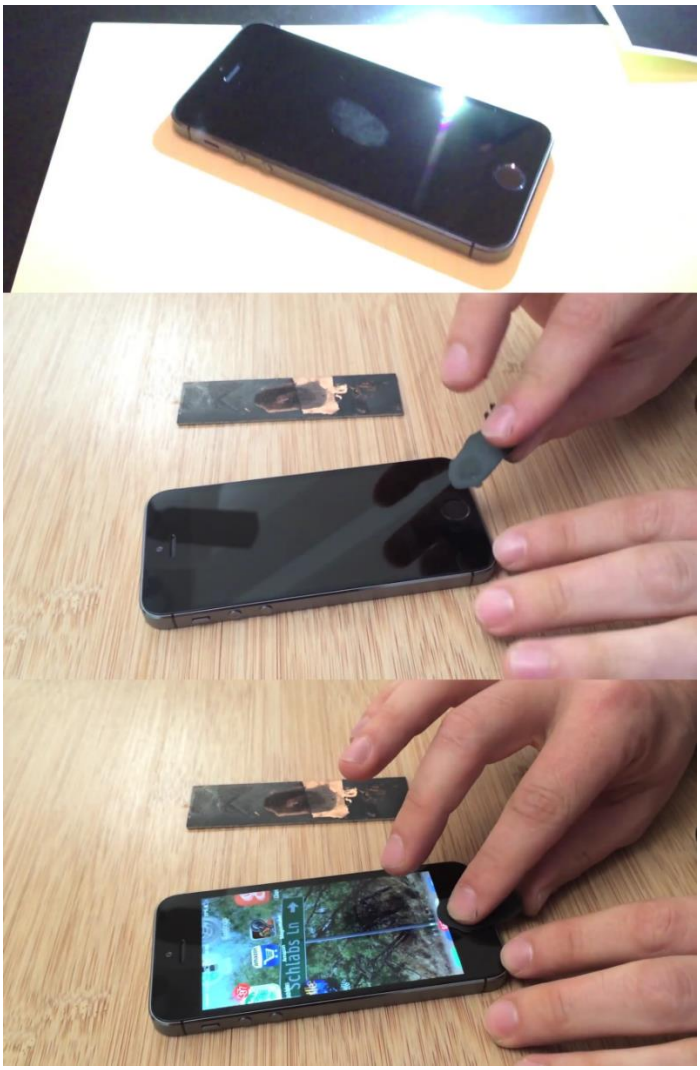
Jedna česta metoda ovog autentifikacijska faktora oslanja se na očitavanje **otiska prsta**. Razne oblike čitača otisaka prstiju danas je jeftino implementirati, pa je ova metoda sve češće dostupna na pametnim telefonima i prijenosnim računalima. Slika 16 prikazuje primjer otključavanja pametnog telefona očitanjem otiska prsta.



Slika 16 – otključavanje pametnog telefona očitanjem otiska prsta (izvor)

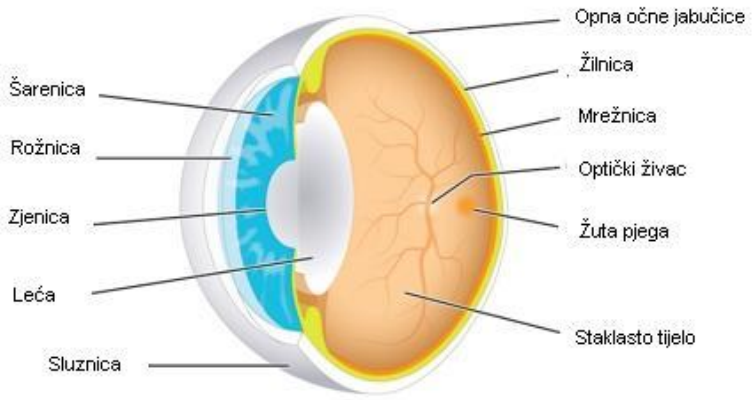
Autentifikacija temeljena na otisku prsta je prilično **praktična, ali ne i izrazito sigurna**. Kroz svakodnevne radnje ostavljamo otiske svojih prstiju na raznim predmetima. Između ostaloga, otiske ostavljamo i na pametnim telefonima i prijenosnim računalima koje pokušavamo zaštititi upravo tim otiskom.

Pokazalo se da može biti prilično jeftino i jednostavno na temelju tako ostavljenog otiska prsta izraditi umjetni vrh prsta **s istim otiskom** (15). S takvim umjetnim vrhom prsta je zatim moguće uspješno se autentificirati na sustav koji očekuje stvarni prst od legitimnog korisnika (15). Za stvaranje takvog umjetnog vrha prsta može biti dovoljna fotografija otiska prsta ostavljenog na nekoj površini u kombinaciji s jeftinim materijalima i alatima (15). Na slici 17 prikazan je primjer ovog postupka. Otisak prsta ostavljen na pametnom telefonu je fotografiran te je na temelju fotografije izrađen umjetni vrh prsta. Taj umjetni vrh prsta zatim može otključati pametni telefon – jednako kao i stvarni prst koji se inače koristi za otključavanje (15). Drugim riječima, pametni telefon kojega bi trebao samo vlasnik moći otključati svojim prstom sada je moguće otključati pomoću navedenog umjetnog vrha prsta.



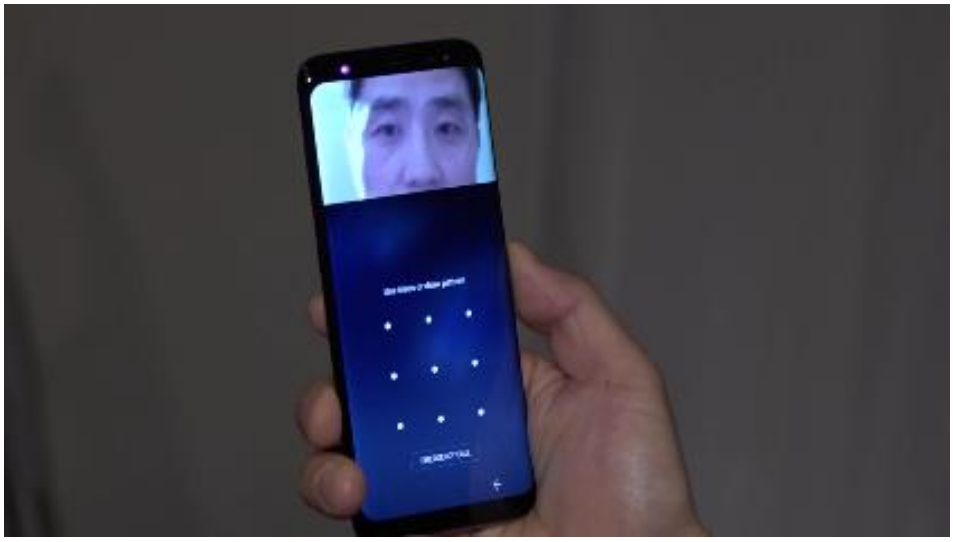
Slika 17 – otisak prsta ostavljen na pametnom telefonu je fotografiran te je na temelju fotografije izrađen umjetni vrh prsta koji zatim može otključati pametni telefon (izvor)

Osim uzoraka na otisku prsta, metode ovog faktora mogu koristiti i uzorke na **šarenici oka** ili uzorke na **mrežnici oka**. Na slici 18 prikazano je ljudsko oko s označenom šarenicom i mrežnicom. Iako se u obje metode očitavaju uzorci dijela oka, očitavanje uzoraka šarenice i uzoraka mrežnice je prilično različito.



Slika 18 – ljudsko oko s označenim dijelovima (izvor)

Očitanje uzoraka **šarenice** oka slično je fotografiranju očiju korisnika fotoaparatom koji podržava snimanje dijela infracrvenog spektra (16), primjerice u kontekstu funkcionalnosti za noćno snimanje. Na tako snimljenoj fotografiji zatim je moguće vidjeti i izolirati složeni uzorak šarenice korisnika. Slično kao i kod očitanja otiska prsta, sklopovlje za očitanje uzoraka šarenice oka postalo je dovoljno jeftino da se već sada nalazi i na nekim pametnim telefonima. Pametni telefoni očitavaju uzorke šarenice oka s oko 30 centimetara udaljenosti (17), dok moćniji uređaji mogu očitati uzorke šarenice sa čak 12 metara (18). Na slici 19 prikazano je otključavanje pametnog telefona očitanjem uzoraka šarenice oka.

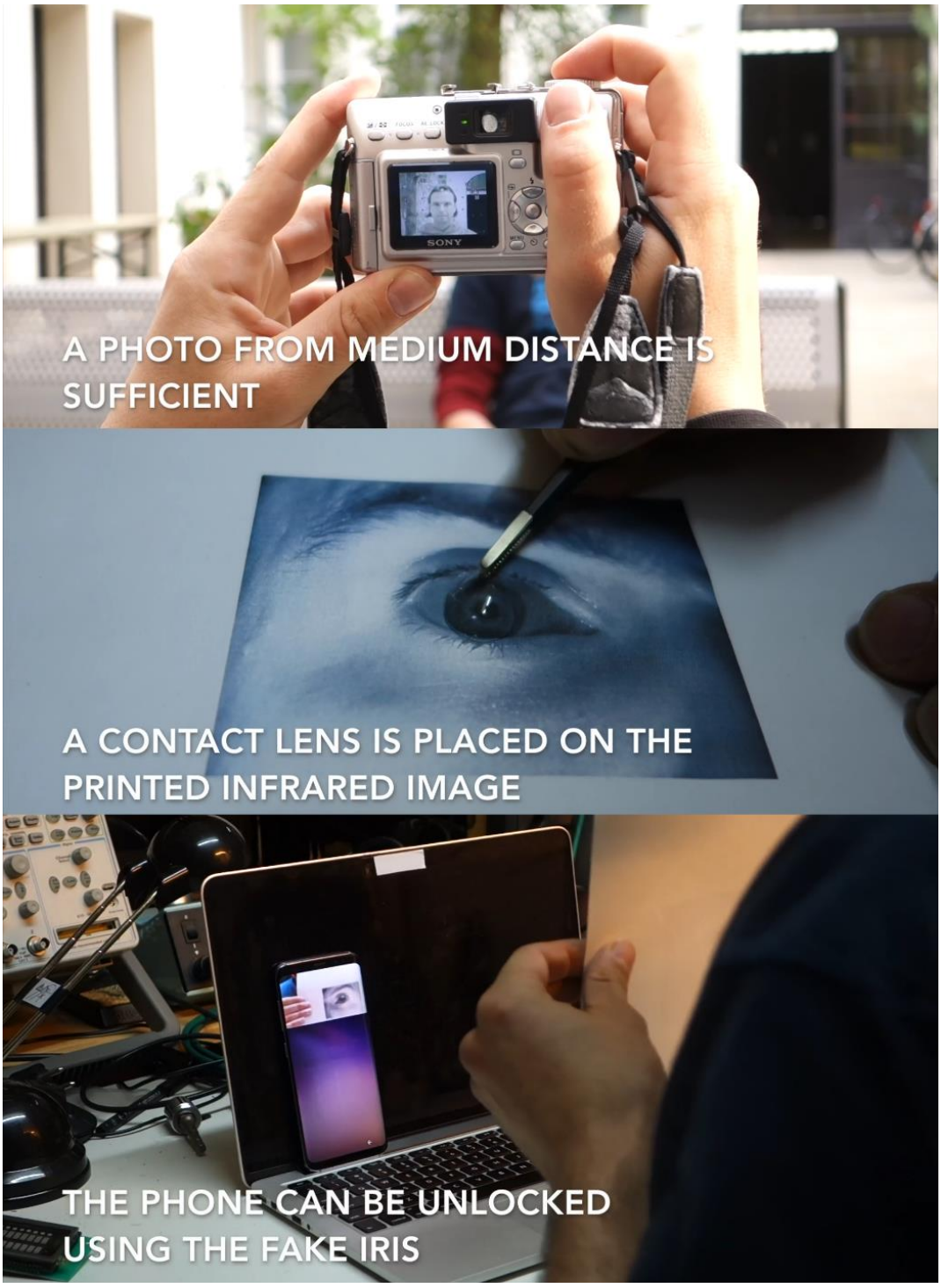


Slika 19 – otključavanje pametnog telefona očitanjem uzoraka šarenice oka (izvor)

Velika udaljenost s koje je moguće očitati uzorke šarenice oka ujedno je i **slabost iz perspektive sigurnosti**. Pokazano je kako je moguće:

- fotografirati šarenicu korisnika s udaljenosti od nekoliko metara (fotoaparatom koji podržava noćno snimanje),
- ispisati tu fotografiju
- te zatim uz pomoć ispisane fotografije i kontaktne leće uspješno prevariti neke sustave za autentifikaciju temeljene na ovoj metodi (19).

Na slici 20 prikazan je primjer prethodno navedenog postupka kojim je uspješno prevaren autentifikacijski sustav pametnog telefona.



Slika 20 – izrada lažne šarenice oka kojom je uspješno prevaren autentifikacijski sustav pametnog telefona (izvor)

Za razliku od očitanja uzoraka šarenice oka, implementacija autentifikacijske očitanjem uzoraka **mrežnice** oka je **skupa**, no ujedno i **prilično sigurna** (20; 21). Zato se ova metoda koristi gotovo isključivo u vojsci, obavještajnim agencijama i sličnim okruženjima (20; 21). Očitanje uzoraka mrežnice oka moguće je samo s visoko specijaliziranom opremom te s kratkih udaljenosti (20). Primjer autentifikacije očitanjem uzoraka mrežnice oka prikazan je na slici 21.

Slika 21 – autentifikacija očitanjem uzoraka mrežnice oka (izvor)

Neke metode ovog faktora oslanjaju se na očitanje **oblika lica** korisnika. Za očitanje oblika lica korisnika, jednostavnije i nesigurnije izvedbe koriste uobičajene kamere za fotografiranje lica (22), dok se složenije i sigurnije izvedbe oslanjaju na posebne kamere koje snimaju i dio infracrvenog spektra te podatke o dubini (23). Slično kao i kod metoda koje očitavaju otiske prsta i uzorke šarenice, metode autentifikacije koje očitavaju oblik lica danas se pojavljuju i na pametnim telefonima te prijenosnim računalima. Na slici 22 prikazano je otključavanje pametnog telefona očitanjem oblika lica.

Slika 22 – otključavanje pametnog telefona očitanjem oblika lica (izvor)

Jednostavnije izvedbe ovih metoda moguće je prevariti već fotografijom lica korisnika. Drugim riječima, umjesto lica korisnika, za uspješnu autentifikaciju može biti dovoljno staviti fotografiju korisnika ispred čitača.

Primjer takvog načina prevare autentifikacijskog sustava prikazan je na slici 23. U navedenom primjeru, za prevaru sustava bio je potreban samo jedan dodatni, sporedni pametni telefon. Prvo, sporednim pametnim telefonom je fotografirano lice legitimnog korisnika. Zatim, umjesto lica legitimnog korisnika, pred zaštićeni pametni telefon stavljen je zaslon sporednog pametnog telefona na kojemu je prikazana fotografija lica. U

konačnici, na taj način je umjesto lica legitimnog korisnika, zaštićeni pametni telefon otključan običnom fotografijom.

Slika 23 – jednostavniji autentifikacijski sustav temeljen na očitanju oblika lica prevaren pomoću fotografije korisnika (izvor)

Složenije sustave čiji čitači snimaju dio infracrvenog spektra te podatke o dubini obično nije moguće prevariti samo fotografijom korisnika. No pokazalo se da je s više truda, konkretnije pomoću 3D ispisane maske koja sliči licu korisnika, moguće prevariti i neke od takvih sustava (24). Na slici 24 prikazan je primjer maske koja može prevariti jedan ovakav autentifikacijski sustav – istraživači tvrde da je izrada maske koštala oko 200 američkih dolara te da je masku moguće izraditi na temelju fotografija legitimnog korisnika (24).

Slika 24 – složeniji autentifikacijski sustav temeljen na očitanju oblika lica prevaren pomoću maske lica korisnika (izvor)

Općenito, jedna prednost ovog autentifikacijskog faktora nad prethodno opisanim faktorima je to što korisnik u pravilu **ne može „zaboraviti“ ili „izgubiti“** svoj otisak prsta, svoje uzorke šarenice oka ili neko drugo takvo obilježje. Zato, za krajnjeg korisnika, metode ovog autentifikacijskog faktora mogu biti **jednostavnije** od pamćenja i unosa lozinke ili od nošenja i korištenja kartice.

No iz perspektive samog sustava, očitanje otiska prsta, uzoraka šarenica oka ili slično znatno je složenije od unosa lozinke ili komunikacije s pametnom karticom. Zato, **može se dogoditi i da legitimnom korisniku autentifikacija ne radi** zbog nekog vanjskog faktora, primjerice zbog lošeg osvjetljenja kod očitanja šarenice oka ili zbog malih nečistoća na vrhovima prstiju kod očitanja otiska prsta.

Što se tiče sigurnosne perspektive, do sada je kroz poglavlje demonstrirano kako je **mnoge metode ovog faktora moguće prevariti** umjetnim prstom, lažnom šarenicom oka, maskom lica korisnika i slično. Preduvjet takvih prevara bio je da napadač nekako **snimi traženo obilježe žrtve** – primjerice da nekako prikupi žrtvin otisak prsta ili snimi uzorke šarenice njenog oka.

Uzimajući to u obzir, činjenica da se obilježja korisnika koje ove metode koriste (otisak prsta, uzorak šarenice...) **ne mogu promijeniti** predstavlja izrazito ozbiljan sigurnosni problem. Kako bi demonstrirali ovu slabost na primjeru, članovi njemačke organizacije sigurnosnih stručnjaka *Chaos Computer Club* su u 92. izdanju njihovog časopisa *Die Datenschleuder* **objavili snimku otiska prsta tadašnjeg njemačkog ministra unutarnjih poslova, Wolfganga Schäubla** (25). Time se postavlja izrazito konkretno pitanje – što to znači za njega i za sigurnost sustava koji se temelje na očitanju njegovog otiska prsta? Nadalje, što ovo znači općenito za sigurnost bilo kojeg sustava autentifikacije koji se temelji na očitanju ovakvog nepromjenjivog obilježja? Na slici 25 prikazana je stranica iz časopisa *Die Datenschleuder* u kojoj je navedena snimka otiska prsta objavljena kao dio „albuma biometrijskih podataka“ njemačkih službenika (25).

Slika 25 – snimka otiska prsta bivšeg njemačkog ministra unutarnjih poslova, Wolfganga Schäubla, objavljena kao dio „albuma biometrijskih podataka" njemačkih službenika u 92. izdanju časopisa *Die Datenschleuder* (izvor)

Jasno je da otisak prsta može biti kompromitiran, slično kao što lozinka ili kartica mogu biti kompromitirani. U slučaju prethodnih faktora, kompromitirana lozinka može se zamijeniti drugom te se isto tako kompromitirana kartica može zamijeniti. No otisak prsta, uzorci šarenice oka i slično **ne mogu se zamijeniti**, tako da u slučaju njihove kompromitacije, **napadač njihove važeće snimke ima zauvijek**. Žrtva zato više ne može biti sigurna kada želi koristiti kompromitirano obilježje za autentifikaciju. Uz to, za razliku od prethodnih faktora kod kojih korisnik može koristiti različitu lozinku odnosno karticu za različite sustave – s obilježjima kao što su uzorci šarenica očiju ili oblik lica, **korisnik je prisiljen koristiti isto obilježje za sve sustave**.

3 Višefaktorska autentifikacija

Kada su jasne prednosti i mane pojedinih autentifikacijskih faktora, koncept višefaktorske autentifikacije postaje prilično intuitivan. Kao što niz primjera iz prethodnog poglavlja pokazuje, svaka metoda autentifikacije ima neke slabosti. Bitno je primijetiti da **metode iz istog autentifikacijskog faktora imaju i slične slabosti**. Primjerice, do lozinka, PIN-ova i odgovora na sigurnosna pitanja napadači mogu doći *phishing* napadom. Ključ, karticu i privjesak moguće je ukrasti. Uzorke šarenice oka, oblik lica i karakteristike glasa napadač može snimiti ako je u blizini korisnika.

3.1 Jednofaktorska autentifikacija

Ako za određenu svrhu ni jedna metoda autentifikacije sama po sebi nije dovoljno sigurna, **kako onda smisleno podići razinu sigurnosti?**

Recimo da je za ulazak u neku zaštićenu prostoriju do sada bio potreban samo ključ. No, to se više ne smatra dovoljno sigurnim, jer postoji realna opasnost da napadač **ukrade ključ** od nekog korisnika. Koje je rješenje? Možda da korisnik za ulazak u navedenu prostoriju prvo mora otvoriti jedna vrata ključem, a zatim druga, dodatna vrata RFID privjeskom? Ne, takvim pristup **nije** riješen problem, jer napadač koji može **ukrasti ključ isto tako** može **ukrasti i privjesak**.

Sličan problem bio bi sljedeći – recimo da je za prijavu na račun e-pošte do sada korisnik morao samo upisati lozinku. No opet, to se ne smatra dovoljno sigurnim, jer postoji realna opasnost da napadač nekako **dođe do lozinke** korisnika, primjerice ***phishing* napadom**. Je li dobro rješenje da korisnik sada, uz lozinku, za prijavu na račun e-pošte mora unijeti i odgovor na sigurnosno pitanje? I u ovom slučaju, ovime **nije** riješen problem, jer napadač koji može ***phishing* napadom doći do lozinke**, **isto tako** može doći i do **odgovora na sigurnosno pitanje**.

U navedenim rješenjima bi se umjesto jedne, koristile dvije metode autentifikacije – zašto onda cjelokupni sustav nije postao znatno sigurniji? Problem u oba rješenja bio je to što su obje korištene metode autentifikacije (ključ i privjesak odnosno lozinka i sigurnosno pitanje) bile **iz istog autentifikacijskog faktora** i zato su imale **iste slabosti**. Drugim riječima, u oba primjera korištena je tzv. **jednofaktorska autentifikacija**.

Autentifikacija je **jednofaktorska** kada je za uspješnu autentifikaciju dovoljno da se korisnik autentificira jednom ili više metoda **iz istog autentifikacijskog faktora**. Kada se koristi samo jedna metoda autentifikacije, primjerice kada je potreban samo ključ ili samo lozinka, to je jednofaktorska autentifikacija. No ključno je razumjeti da čak i kada se zahtijeva **više metoda** autentifikacije, primjerice i ključ i privjesak, ako su sve te metode **iz istog faktora**, to je i dalje **jednofaktorska** autentifikacija.

3.2 Višefaktorska autentifikacija

Koje je onda rješenje za višu razine sigurnosti prilikom autentifikacije? Kada se korištenje jedne metode autentifikacije ne smatra dovoljno sigurnim, bolji pristup od jednofaktorske autentifikacije je **višefaktorska autentifikacija**. Autentifikacija je **višefaktorska** kada je

za uspješnu autentifikaciju potrebno da se korisnik autentificira pomoću **više metoda** iz **različitih** autentifikacijskih faktora.

Primjerice, ako za prijavu na račun e-pošte korisnik treba unijeti **lozinku** i priključiti pametnu **karticu** na odgovarajući čitač, to se smatra višefaktorskom autentifikacijom. U ovom slučaju koriste se dvije metode autentifikacije (lozinka i kartica) iz dva različita faktora („nešto što osoba zna“ i „nešto što osoba posjeduje“). Ovakva višefaktorska autentifikacija u kojoj se koriste metode iz točno **dva** različita faktora naziva se i **dvofaktorska autentifikacija**.

U ovom primjeru, napadač koji *phishing* napadom može doći do lozinke korisnika sada mora i nekako fizički ukrasti njegovu karticu. Dodavanje metode autentifikacije iz **drugog** faktora može spriječiti cijele kategorije napada, primjerice *phishing* napade u ovom slučaju (13).

Ako za podizanje novca s bankomata korisnik treba priključiti karticu na bankomat, upisati PIN te prisloniti prst kako bi se očitao otisak, to je također primjer višefaktorske autentifikacije. Sada se koriste tri metode autentifikacije (PIN, kartica, otisak prsta) iz sva tri faktora („nešto što osoba zna“, „nešto što osoba posjeduje“, „nešto što osoba je“). Ovakva višefaktorska autentifikacija u kojoj se koriste metode iz sva tri faktora naziva se i **trofaktorska autentifikacija**.

Ključno je razumjeti da je autentifikacija višefaktorska samo ako se korisnik **mora** uspješno autentificirati kroz više metoda iz više faktora. Primjerice, autentifikacija je višefaktorska ako korisnik mora unijeti ispravnu lozinku te zatim mora priključiti ispravnu karticu. Ako za uspješnu autentifikaciju korisnik može birati samo jednu metodu – ili unos lozinke ili korištenje kartice – to **nije** višefaktorska autentifikacija.

Također, potrebno je imati na umu da, iako metode iz istog autentifikacijskog faktora imaju slične prednosti i mane, to ne znači da su sve metode iz istog faktora jednako sigurne. Primjerice, kao što je opisano u prethodnom poglavlju, metode faktora „nešto što osoba posjeduje“ u kojima uređaj generira jednokratnu lozinku su ranjive na *phishing* napade, dok metode s uređajima koji funkcioniraju kao pametne kartice nisu (11) (13) (14). Zato je, uz korištenje metoda iz različitih faktora, potrebno obratiti i pažnju na to koje se konkretne metode koriste.

3.3 Primjeri višefaktorske autentifikacije

Primjer višefaktorske autentifikacije s kojim su se gotovi svi susreli je korištenje **bankovne kartice** i **PIN-a** za kartično plaćanje ili podizanje gotovine na bankomatu. Bankovna kartica je „nešto što osoba posjeduje“, dok je PIN „nešto što osoba zna“. Primjer višefaktorske autentifikacije prilikom kartičnog plaćanja prikazan je na slici 26.

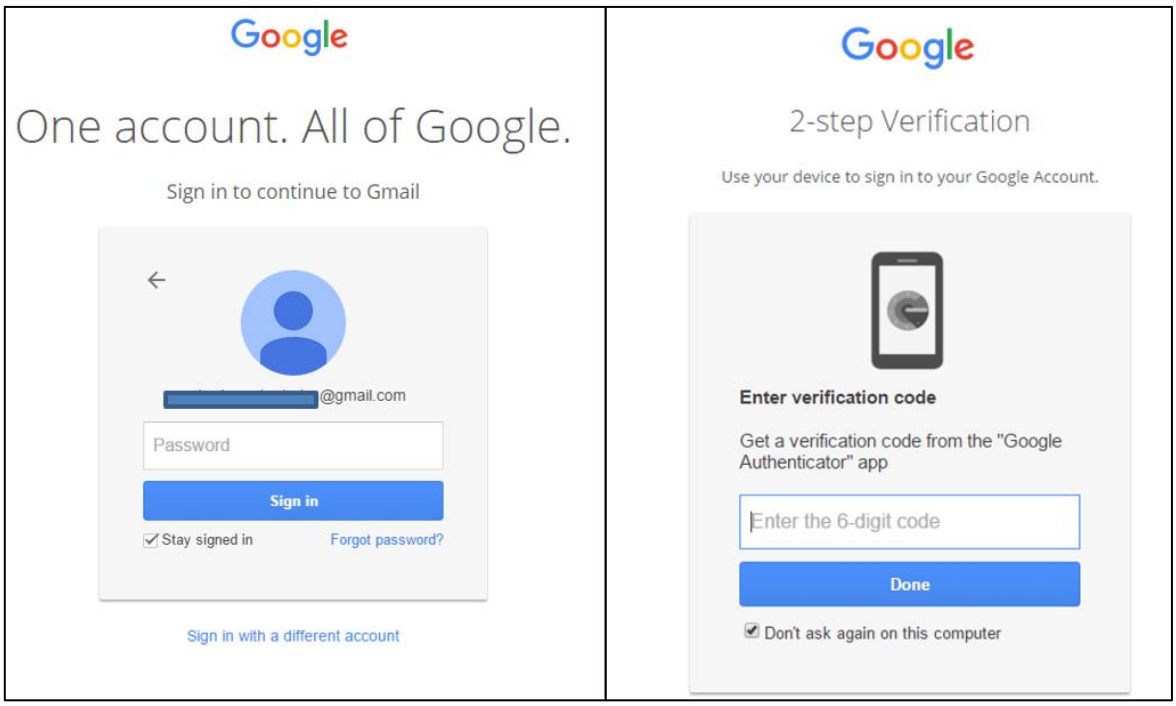
Slika 26 – višefaktorska autentifikacija bankovnom karticom i PIN-om prilikom kartičnog plaćanja

U posljednjih nekoliko godina, višefaktorska autentifikacija postala je dostupna i za razne usluge na internetu. Danas, gotovo sve popularne usluge e-pošte (*Gmail*, *Yahoo mail*, *Outlook.com*...), društvene mreže (*Facebook*, *Twitter*, *LinkedIn*...) te brojne druge usluge (npr. *Amazon*, *Dropbox*, *Paypal*...) pružaju mogućnost višefaktorske autentifikacije (26).

Na navedenim uslugama najčešće je dostupna dvofaktorska autentifikacija kojom se uz lozinku traži i tajni kod poslan putem SMS-a ili jednokratna lozinka generirana pomoću aplikacije na mobitelu. Uz to, sve više usluga podržava još sigurniji pristup – korištenje lozinke u kombinaciji s pametnom karticom ili sličnim uređajem. Jedan često korišteni standard za takvu autentifikaciju je U2F (27).

Na slici 27 prikazan je primjer dvofaktorske autentifikacije za uslugu e-pošte *Gmail*. Prilikom prijave, prvo je potrebno upisati lozinku za svoj korisnički račun, a zatim je potrebno upisati jednokratnu lozinku koju je generirala aplikacija na pametnom telefonu.

Upute kako uključiti i koristiti višefaktorsku autentifikaciju za često korištene usluge na internetu dostupne su ovdje i ovdje.



Slika 27 – primjer prijave na uslugu e-pošte *Gmail* dvofaktorskom autentifikacijom (izvor)

Trofaktorska autentifikacija se koristi prilično rijetko jer dvofaktorska autentifikacija obično predstavlja bolji omjer sigurnosti i lakoće korištenja. Unatoč tome, kroz posebne uređaje i standarde kao što je U2F, oprezniji korisnici mogu već danas koristiti trofaktorsku autentifikaciju za neke usluge na internetu.

Primjerice, na uslugama koje podržavaju U2F standard moguće je, uz lozinku, koristiti uređaj koji ima čitač otiska prsta i funkcionalnost sličnu pametnoj kartici. Primjer takvog uređaja prikazan je na slici 28. Na slici 29 prikazano je kako takva trofaktorska autentifikacija izgleda – korisnik unosi lozinku („nešto što osoba zna“), priključuje svoj uređaj („nešto što osoba posjeduje“) te na njemu očitava svoj otisak prsta („nešto što osoba je“). Svo troje – korisnikova lozinka, korisnikov uređaj, korisnikov otisak prsta – potrebno je za uspješnu autentifikaciju.

Slika 28 – uređaj kompatibilan s U2F standardom koji ujedno ima i čitač otiska prsta (izvor)

Slika 29 – trofaktorska autentifikacija kombinacijom lozinke i uređaja kompatibilnog s U2F standardnom koji ima čitač otiska prsta (izvor)

4 Zaključak

Korištenje samo jedne metode autentifikacije često nije dovoljno sigurno. U takvim slučajevima, ispravno rješenje je korištenje **višefaktorske autentifikacije**. Ključno je razumjeti da je autentifikacija višefaktorska isključivo:

1. ako se koristi više metoda autentifikacije **iz više različitih faktora**

2. i ako se korisnik **mora** autentificirati metodama iz **svakog** od korištenih faktora.

Zahtijevanje **i lozinke i kartice** je **višefaktorska autentifikacija**. Zahtijevanje i lozinke i PIN-a **nije** višefaktorska autentifikacija. Zahtijevanje **ili** lozinke **ili** kartice **nije** višefaktorska autentifikacija.

Višefaktorska autentifikacija nije nedavna pojava – prije više od 50 godina, na prvim je bankomatima bilo moguće podizati gotovinu pomoću posebnih čekova („nešto što osoba posjeduje“) i PIN-a („nešto što osoba zna“) (28). Na slici 30 prikazan je prvi bankomat kao primjer višefaktorske autentifikacije iz 1967. godine.

Slika 30 – prvi bankomat, primjer višefaktorske autentifikacije iz 1967. godine (izvor)

Već neko vrijeme, gotovo sve usluge gdje je sigurnost bitna pružaju mogućnost ili čak zahtijevaju korištenje višefaktorske autentifikacije. Danas obično nije pitanje podržava li neka usluga višefaktorsku autentifikaciju, već želi li ju korisnik koristiti. Što se tiče usluga na internetu, široko korišteni standardi kao što su TOTP i U2F osiguravaju da korisnik može koristiti istu aplikaciju odnosno isti uređaj za višefaktorsku autentifikaciju na niz različitih servisa.

U konačnici, **autentifikacija je izrazito bitan dio sigurnosti** sveukupnog sustava te višefaktorski pristup može sigurnost autentifikacije podići na izrazito visoku razinu. No bitno je razumjeti kako **sigurna autentifikacija ne znači da je cijeli sustav siguran**. Autentifikacija je samo jedna karika u lancu sigurnosti – ako je ona dovoljno sigurna, napadači će usmjeriti napade na neki drugi dio sustava. Primjerice, sigurna autentifikacija je bespomoćna protiv nekih oblika zlonamjernog softvera (29) ili protiv legitimnog korisnika koji je odlučio sabotirati sustav. Zato je kod evaluacije sigurnosti uvijek bitno imati na umu pregled cijelog sustava.

5 Literatura

1. **Morgan.** Announcing our Worst Passwords of 2016. [Mrežno] 2017. [Citirano: 15. listopada 2018.] https://www.teamsid.com/worst-passwords-2016/.
2. **Hunt, Troy.** What do Sony and Yahoo! have in common? Passwords! [Mrežno] 12. srpnja 2012. [Citirano: 24. listopada 2018.] https://www.troyhunt.com/what-do-sony-and-yahoo-have-in-common/.
3. —. Have I Been Pwned: Pwned websites. [Mrežno] [Citirano: 24. listopada 2018.] https://haveibeenpwned.com/PwnedWebsites.
4. **Bright, Peter.** Sony hacked yet again, plaintext passwords, e-mails, DOB posted. *Ars Technica.* [Mrežno] 3. lipnja 2011. [Citirano: 24. listopada 2018.] https://arstechnica.com/tech-policy/2011/06/sony-hacked-yet-again-plaintext-passwords-posted/.
5. **Franceschi-Bicchierai, Lorenzo.** Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords. *Motherboard.* [Mrežno] 18. svibnja 2016. [Citirano: 24. listopada 2018.] https://motherboard.vice.com/en_us/article/78kk4z/another-day-another-hack-117-million-linkedin-emails-and-password.
6. **Goodin, Dan.** Hackers expose 453,000 credentials allegedly taken from Yahoo service (Updated). *Ars Technica.* [Mrežno] 12. srpnja 2012. [Citirano: 24. listopada 2018.] https://arstechnica.com/information-technology/2012/07/yahoo-service-hacked/.
7. **Ducklin, Paul.** Anatomy of a password disaster – Adobe's giant-sized cryptographic blunder. *Naked Security.* [Mrežno] 4. studenog 2013. [Citirano: 24. listopada 2018.] https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/.
8. **DataGenetics.** PIN number analysis. [Mrežno] [Citirano: 24. listopada 2018.] http://www.datagenetics.com/blog/september32012/.
9. **M'Raihi, David, i dr.** TOTP: Time-Based One-Time Password Algorithm. [Mrežno] svibanj 2011. [Citirano: 20. studenog 2018.] https://tools.ietf.org/html/rfc6238.
10. **Bishop Fox.** RFID Hacking Tools & Downloads. [Mrežno] [Citirano: 4. prosinca 2018.] https://www.bishopfox.com/resources/tools/rfid-hacking/attack-tools/.
11. **Paya, Cem.** Twitter, two-factor authentication and phishing myths (part I). *Random Oracle.* [Mrežno] 5. svibnja 2013. [Citirano: 21. studenog 2018.] https://randomoracle.wordpress.com/2013/05/05/twitter-two-factor-authentication-and-phishing-myths-part-i/.
12. **Krebs, Brian.** Busting SIM Swappers and SIM Swap Myths. *Krebs on Security.* [Mrežno] 7. studenog 2018. [Citirano: 11. prosinca 2018.] https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths/.
13. **Paya, Cem.** Two-factor authentication and phishing: smart cards (part II). *Random Oracle.* [Mrežno] 8. svibnja 2013. [Citirano: 21. studenog 2018.] https://randomoracle.wordpress.com/2013/05/08/twitter-two-factor-authentication-and-phishing-myths-part-ii/.
14. —. TLS client authentication and phishing (part III). *Random Oracle.* [Mrežno] 10. svibnja 2013. [Citirano: 21. studenog 2018.] https://randomoracle.wordpress.com/2013/05/10/tls-client-authentication-and-phishing-part-iii/.
15. **Security Research Labs.** Fingerprints are not fit for secure device unlocking – Security Research Labs. [Mrežno] [Citirano: 22. studenog 2018.] https://srlabs.de/bites/spoofing-fingerprints/.

16. **Trader, John.** Iris Recognition vs. Retina Scanning - What are the Differences? *M2SYS Blog On Biometric Technology.* [Mrežno] [Citirano: 22. studenog 2018.] http://www.m2sys.com/blog/biometric-hardware/iris-recognition-vs-retina-scanning-what-are-the-differences/.
17. **Samsung.** Set Up Galaxy Note8 to Use Iris Security. [Mrežno] [Citirano: 4. prosinca 2018.] https://www.samsung.com/us/support/answer/ANS00077686/.
18. **Meyer, Robinson.** Long-Range Iris Scanning Is Here (and It's Creepy). *The Atlantic.* [Mrežno] 13. svibnja 2015. [Citirano: 4. prosinca 2018.] https://www.theatlantic.com/technology/archive/2015/05/long-range-iris-scanning-is-here/393065/.
19. **46halbe.** CCC | Chaos Computer Clubs breaks iris recognition system of the Samsung Galaxy S8. [Mrežno] 22. svibnja 2017. [Citirano: 22. studenog 2018.] https://www.ccc.de/en/updates/2017/iriden.
20. **Thakkar, Danny.** Retinal vs. Iris Recognition: Your Eyes Can Get You Identified? *Bayometric.* [Mrežno] [Citirano: 4. prosinca 2018.] https://www.bayometric.com/retinal-vs-iris-recognition/.
21. **GlobalSecurity.org.** Biometrics - Retina and Iris Identification. [Mrežno] [Citirano: 4. prosinca 2018.] https://www.globalsecurity.org/security/systems/biometrics-eye_scan.htm.
22. **Heater, Brian.** Don't rely on Face Unlock to keep your phone secure. *TechCrunch.* [Mrežno] 6. rujna 2017. [Citirano: 5. prosinca 2018.] https://techcrunch.com/2017/09/06/dont-rely-on-face-unlock-to-keep-your-phone-secure/.
23. **Apple.** About Face ID advanced technology. [Mrežno] [Citirano: 5. prosinca 2018.] https://support.apple.com/en-au/HT208108.
24. **Bkav.** Bkav's new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions. [Mrežno] 27. studenog 2017. [Citirano: 23. studenog 2018.] http://www.bkav.com/dt/top-news/-/view_content/content/103968/bkav%EF%BF%BDs-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions.
25. **Chaos Computer Club.** Die Datenschleuder: Das wissenschaftliche Fachblatt für den Datenreisenden #92. [Mrežno] ožujak 2008. [Citirano: 5. prosinca 2018.] https://ds.ccc.de/pdfs/ds092.pdf.
26. **Gebhart, Gennie.** The 12 Days of 2FA: How to Enable Two-Factor Authentication For Your Online Accounts. *Electronic Frontier Foundation.* [Mrežno] 8. prosinca 2016. [Citirano: 6. prosinca 2018.] https://www.eff.org/deeplinks/2016/12/12-days-2fa-how-enable-two-factor-authentication-your-online-accounts.
27. **Yubico.** U2F - FIDO Universal 2nd Factor Authentication. [Mrežno] [Citirano: 6. prosinca 2018.] https://www.yubico.com/solutions/fido-u2f/.
28. **Barclays.** From the archives: the ATM is 50. [Mrežno] 27. lipnja 2017. [Citirano: 10. prosinca 2018.] https://home.barclays/news/2017/06/from-the-archives-the-atm-is-50/.
29. **Mushtaq, Atif.** Man in the Browser. *FireEye.* [Mrežno] 18. veljače 2010. [Citirano: 10. prosinca 2018.] https://www.fireeye.com/blog/threat-research/2010/02/man-in-the-browser.html.
30. **Wang, Krystal.** Multi-factor Authentication: Because Phishing Happens. *okta.* [Mrežno] 10. travnja 2018. [Citirano: 2. listopada 2018.] Multi-factor Authentication: Because Phishing Happens.

31. **Sheridan, Kelly.** Phishing Attack Bypasses Two-Factor Authentication. *Dark Reading.* [Mrežno] 10. svibnja 2018. [Citirano: 2. listopada 2018.]
32. **-.** Access Control. *techopedia.* [Mrežno] [Citirano: 2. listopada 2018.] https://www.techopedia.com/definition/5831/access-control.
33. **Gibson, Darril.** Understanding the Three Factors of Authentication. *Pearson IT Certification.* [Mrežno] 6. lipnja 2011. [Citirano: 2. listopada 2018.] http://www.pearsonitcertification.com/articles/article.aspx?p=1718488.
34. **Miessler, Daniel.** Security: Identification, Authentication, and Authorization. [Mrežno] 4. listopada 2005. [Citirano: listopada. 10 2018.] https://danielmiessler.com/blog/security-identification-authentication-and-authorization/.