Povećanje sigurnosti Web aplikacija primjenom dvostrukog faktora autentikacije

Gortan, Ivan

ISTARSKO VELEUČILIŠTE
Pula
Preddiplomski stručni studij

ZAVRŠNI RAD

POVEĆANJE SIGURNOSTI WEB APLIKACIJA PRIMJENOM DVOSTRUKOG FAKTORA AUTENTIFIKACIJE

Ivan Gortan

Pula, 2019.

ISTARSKO VELEUČILIŠTE
Pula
Preddiplomski stručni studij

ZAVRŠNI RAD

POVEĆANJE SIGURNOSTI WEB APLIKACIJA PRIMJENOM DVOSTRUKOG FAKTORA AUTENTIFIKACIJE

Kolegij: Računalne Mreže

Mentor: Pred. Kristijan Matas

Student: Ivan Gortan

Studijski program: Preddiplomski stručni studij Politehnike

Pula, srpanj 2019.

IZJAVA

Kojom izjavljujem da sam završni rad s naslovom Povećanje sigurnosti web aplikacija primjenom dvostrukog faktora autentifikacije izradio samostalno pod mentorstvom Pred. Kristijana Matasa.

U radu sam primijenio metodologiju znanstveno-istraživačkog rada i koristio literaturu koja je navedena na kraju završnog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo u završnom radu na uobičajen, standardan način citirao sam i povezao s fusnotama i korištenim bibliografskim jedinicama. Rad je pisan u duhu hrvatskoga jezika. Suglasan sam s objavom završnog rada na službenim stranicama Fakulteta.

Student

( )

Ivan Gortan.

SADRŽAJ

SAŽETAK

Autentifikacija je proces određivanja identiteta nekog subjekta, najčešće se odnosi na fizičku osobu. U praksi subjekt daje određene podatke po kojima druga strana može utvrditi da je subjekt upravo taj kojim se predstavlja. Autentifikacija s dva faktora je metoda kombiniranja dvije tzv. autentifikacije čimbenika kako bi se povećala sigurnost autentifikacije korisnika. Faktor autentičnosti je definiran kao "nešto što korisnik zna, ima ili je". Nešto što korisnik zna često je tradicionalno korisničko ime i lozinka, a nešto što korisnik ima je nešto što je korisniku u fizičkom posjedu i što korisnik je, je fizička osobina korisnika, kao što su biometrijske osobine. Autentifikacija s dva faktora uvelike povećava sigurnost u usporedbi s metodama koje se sastoje samo od zaporke. S povećanom primjenom pametnih telefona, razvijene su nove prikladne metode provjere autentičnosti i zato su se počele koristiti svestranosti takvih uređaja. Ovaj rad istražuje, raspravlja i uspoređuje različite metode autentifikacijske koje se danas koriste u pametnim telefonima i računalima u smislu sigurnosti i upotrebljivosti.

Ključne riječi: autentifikacija,SMS,faktori,zaporka.2FA

SUMMARY

Authentication is a process of identifying a subject's identity, most often it refers to a physical person. In practice, the subject gives certain information by which the other party can determine that the subject is exactly what it represents. Authentication with two factors is a method of combining two so-called. Authentication of Factors to Increase User Authentication Security. Authentication factor is defined as "something the user knows, has or is". Something the user knows is often a traditional username and password, and something that the user has is something that the user is in a physical possession and what the user is the physical feature of the user, such as biometrics. Authentication with two factors greatly increases security compared to password-only methods. With the arrival of smartphones, new convenient authentication methods have been developed and therefore the versatility of such devices has begun. This paper explores, discusses and compares different authentication methods used today in smartphones and computers for security and usability.

Keywords: authentication, SMS, factors, password.2FA

1.UVOD

1.1. Predmet istraživanja

U ovom završnom radu obrađena je važnost dvofaktorske autentifikacije, te je prikazan način kako taj sustav funkcionirau interakciji sa SMS porukama te suuspoređene negativne i pozitivne strane takvog načina zaštite pristupa podacima.

1.2. Cilj i svrha rada

Cilj rada jest prikazati kako implementirati SMS na web aplikacije u svrhu povećanja sigurnosti primjenom dvofaktorske autentifikacije i uvidjeti koje su prednosti integracije ove metode.Rad daje odgovore na sljedeća pitanja:zašto je važan dvostruki faktor autentifikacije i koju ulogu ima te koje su prednosti i nedostaci te metode?

1.3. Hipoteza

Implementacijom sustava dvostrukog faktora autentifikacije značajno se povećava sigurnost informacijskih sustava te ostalih važnih podataka na mobilnim i web aplikacijama. Dvostruki faktor autentifikacije lako se implementira i jednostavan je za korištenje od strane korisnika.

1.4. Metode rada

Metode rada koje će biti korištene prilikom izrade ovo završnog rada jesu:
Metoda analize i sinteze, statistička metoda, komparativna metoda i metoda dokazivanja.

1.5. Struktura rada

U prvom poglavlju rada opisana je svrha rada te je definirana hipoteza. Drugo poglavlje uvodi u problematiku sigurnosti na internetu, kreće od povijesti razvoja interneta. Zatim su u istom poglavlju navedene statistike vezane uz korištenje interneta te su opisani rizici i kako se oni osiguravaju. Nakon toga dolazi se do glavnog dijela sadržaja, dvostrukog faktora autentifikacije, navode se različiti faktori koji se mogu koristiti za podizanje sigurnosti. U tom poglavlju isto tako navodi se prednost SMS-a te njegova funkcionalnost za implementaciju 2FA. U četvrtom poglavlju opisuje se implementacija 2FA na web stranicama, dok je na samom kraju rada dan zaključak, osvrt na hipotezu te preporuke za daljnja istraživanja.

2. PROBLEMATIKA SIGURNOSTI NA INTERNETU

2.1 Razvoj interneta

Iako su mnoge tehnologije izmijenile način na koji se živi i radi u posljednjem stoljeću, Internet je jedan od najznačajnijih dostignuća koji je omogućio da se velik dio uobičajenih ljudskih aktivnosti izvršava daljinski – putem mreže. Za nastanak i razvoj Interneta može se vezati niz događaja i osoba. Početak razvoja Internetazapočeo je u SAD-u krajem 60-ih godina prošlog stoljeća te su ga onda primarno koristili znanstvenici i istraživači kako bi međusobno komunicirali i dijelili podatke, dok sedanas Internet koristi za znanstvene, edukacijske, komercijalne i još mnoge aktivnosti.[1]

Dana 4. listopada 1957. Sovjetski Savez je u orbitu lansirao prvi satelit Sputnik.Iako tadanije imao neku značajnu svrhu usporedivši s načinima na koji se danas koristi satelitska tehnologija, Sputnik je bio dokaz znanstveno-tehnološke moći i inovacije SSSR-a u odnosu na Sjedinjene Američke Države

Nakon lansiranja Sputnika, Američka vlada je smatrala da treba odgovoriti na ovaj izazov te suse usmjerili na poboljšanje u području znanosti i tehnologije. Unaprijeđen je sustav obrazovanja tako da su obnovljenisadržaji u obrazovnim institucijama te su dodani novi i moderni sadržaji iz područja znanosti, tehnologije i informatike. Korporacije su dobile na raspolaganje državne potpore i ulagale ih u znanstveno istraživanje i razvoj. Vlada je formirala nove agencije, kao što su Nacionalna uprava za aeronautiku i svemir (NASA) i Agencija za napredne istraživačke projekte Ministarstva obrane (ARPA), kako bi razvijali tehnologije kao što su samonavodeće rakete, avioni nevidljivi za radar, snažna računala i sl.

Godine 1962. J.C.R. Licklider, znanstvenik iz M.I.T. predložio je "galaktičku mrežu" u kojoj će računala moći međusobno komunicirati i razmjenjivati podatke. Takva bi mreža omogućila bržu iučinkovitiju komunikaciju.[2]Ta mreža nazvana je kasnije ARPAnet i te je to bila prethodnik Interneta kakvog danas poznajemo.

---

[1] www.history.com/History.com Editors/The Invention of the Internet/02.07.2019
[2] Ibidem

2.1.1. Prvo slanje podataka "Razmjena paketa"

Godine 1965, na M.I.T.-u je razvijen način slanja informacija s jednog računala na drugou obliku malih adresiranih paketa. Paketi informacija se razbijaju u blokove tj. pakete te se multipleksiraju tako da svaki paket može ići vlastitim putanjom od odredišta do destinacije. Takva mreža bila je puno učinkovitija nego dotadašnja telefonska mreža bazirana na preklopnicima koja je za svaku komunikaciju trebala osigurati zasebnu fizičku liniju. Glavna značajka tada nove paketne mreže je omogućila da više korisnika može komunicirati u isto vrijeme preko iste fizičke linije uzmogućnost korištenja redundantnihlinija ukoliko dođe do prekidaneke od linija.

Godine 1969.preko ARPAnet mreže prenesena je prva„poruka" između dva računala. Jedno je računalo bilo u istraživačkom laboratoriju u UCLA-u (University of California, Los Angeles) a drugo je bilo na Stanfordu. Poslanaje poruka - "LOGIN"(prijava) –iako nije bila kompleksna prijenos nije u potpunosti uspio te je Stanfordsko računalo primilo samo prva dva slova te poruke.[3]

2.1.2. Razvoj i širenje internetske mreže

Do kraja 1969. samo su četiri računala bila povezana s ARPAnet mrežom, ali se mreža proširivala tijekom 1970-ih. Godine 1971. u mrežu je dodan ALOHAnet sa Sveučilišta Hawaii, Kako su se i druge institucije spajale u komunikacijsku mrežu kao npr. londonski University College i Royal Radar Establishment u Norveškoj na principu paketne razmjene, potrebno je bilo definirati komunikacijski standardkoji će sva računala integrirati u jednu „globalnu mrežu".

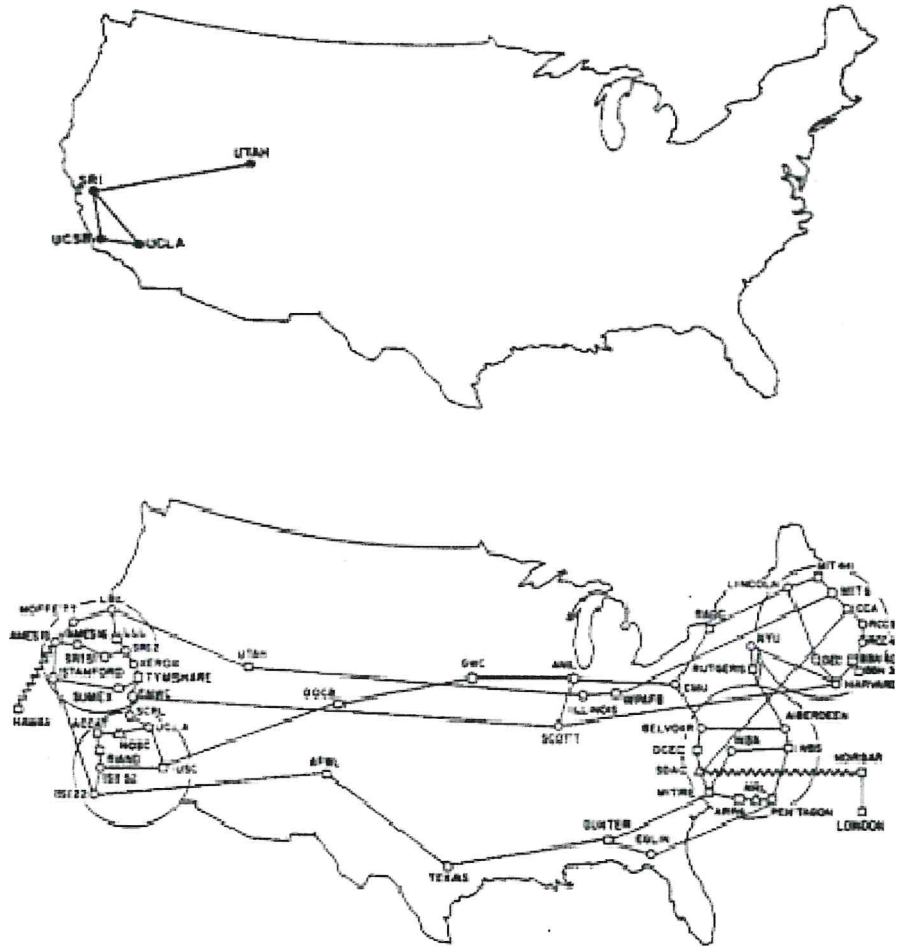
Krajem sedamdesetih godina prošlog stoljeća računalni znanstvenik Vinton Cerf razvio je metodukojom će sva računala na svim svjetskim mini-mrežama moći međusobno komunicirati s velikim postotkom sigurnosti. Protokol je nazvan "Protokol za kontrolu prijenosa" ili TCP – transmission control protocol.

---

[3] www.history.com/History.com Editors/The Invention of the Internet/02.07.2019

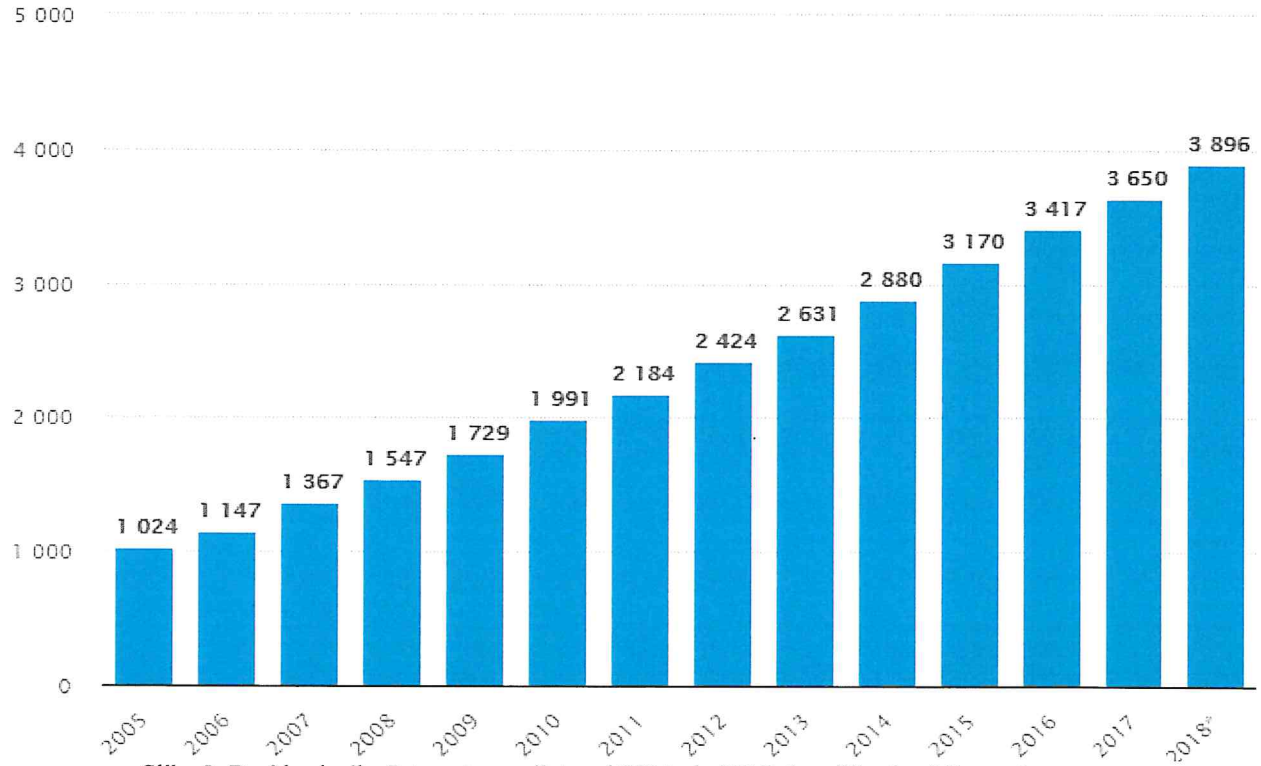
Kasnije je dodatno kombiniran s mrežnim slojem protokola, „Internet Protocol" koji uvodi adresiranje i čime je definiran TCP/IP protokol. TCP/IP protokol omogućio je da Internet preraste uglobalnu mrežu.

1991. godine računalni programer u Švicarskoj, Tim Berners-Lee, predstavio je World Wide Web: uslugu koja je omogućila da svatko na Internetu može objavljivati i pristupati informacijama pa je isti zaslužan za internet kakav danas poznajemo.



Slika 1. ARPAnet umreženja u prosincu 1969. (skica gore) i ARPAnet umreženja u srpnju 1977. (skica dole). Preuzeto s http://theconversation.com/how-the-internet-was-born-from-the-arpanet-to-the-internet-68072 (25.5.2019)

Godine 1992. skupina studenata i istraživača sa Sveučilišta Illinois razvila je preglednik koji su nazvali Mozaik (poznat pod nazivom Netscape). Iste godine Američki kongres je odlučio da se web može koristiti i u komercijalne svrhe. Kao rezultat toga, mnoge su tvrtke počele koristiti servis za postavljanje vlastitih web stranica a stvorila se i mogućnost za razvoj e-commerca te supoduzetnici počeli koristiti Internet za prodaju robe direktno kupcima. Slika 2. daje informacije o ukupnom broju internetskih korisnika u svijetu od 2005. do 2018. godine. Od posljednjeg izvještajnog razdoblja, broj korisnika interneta u svijetu iznosio je 3,9 milijardi, što je povećanje u odnosu na 3,65 milijardi korisnika u prethodnoj godini.[4]

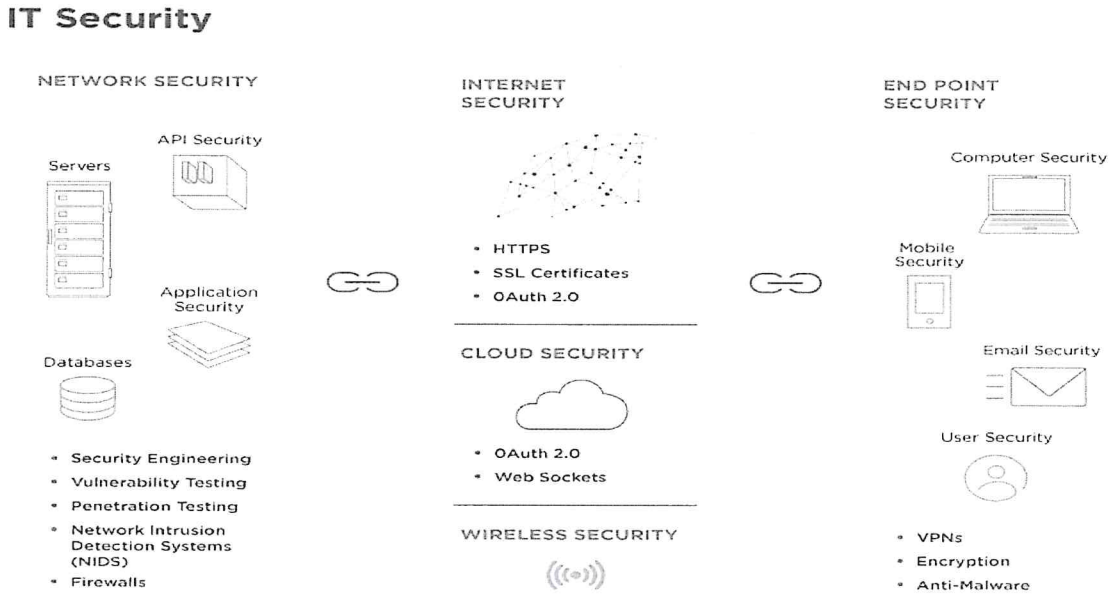


Slika 2. Broj korisnika Interneta u svijetu od 2005. do 2018. (u milijunima).Preuzeto s https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/(25.5.2019)

[4] www.statista.com/Numberofinternetusersworldwide/(25.5.2019)

2.2. Osnovni pojmovi računalne sigurnosti

Masovnim komercijalnim aktivnostima na Internetu raste i broj onih koji pokušavaju zloupotrijebiti takav sustav i samim time stvorila se povećana potreba za IT sigurnošću.



Slika 3. Vrste IT sigurnosti. Preuzeto s https://www.upwork.com/hiring/development/understanding-it-security-and-network-security(14.04.2019)

Korištenjem dodatnih sigurnosnih procedura je dvojako, s jedne strane podižu nivo sigurnosti s time da nisu uvijek pogodne i lake za korištenje radi dodatnih aktivnosti koje treba obaviti. S druge strane ako se želi olakšati korisnicima da koriste tehnologije pa se usmjerava na lakoću korištenja, obično se smanji razina sigurnosti. Time se zapravo u implementaciji sigurnosnih rješenja postavlja pitanje balansa između razine sigurnosti i lakoće korištenja.Resursi koji se štitena internetu jesu informacije. Informacijska sigurnost i sigurnost informacijske tehnologije (IT) se često koriste naizmjenično, ali su to drugačija područja. Kada se govori o informacijskoj sigurnosti, zapravo se podrazumijeva zaštita podataka, bilo da je riječ o digitalnoj ili fizičkoj (npr. papirnati dokumenti). IT sigurnost je specifična po tome štose odnosi samo na sigurnost digitalnih informacija te se odnosi na kompletnu sigurnost računalne infrastrukture.[5]

[5]www.upwork.com/Carey Wodehouse/Inside IT Security/02.07.2019

Tri glavna faktora u kontekstu računalne sigurnosti koje treba osigurati, poznati pod akronimom - CIA:

1. povjerljivost (confidentiality),
2. integritet (integrity)
3. dostupnost (availability)

Povjerljivost je zaštita informacija kod koje je potrebno spriječiti otkrivanje informacija od strane neovlaštenih osoba ili sustava.

Očuvanje integriteta podataka znači da korisnik podatke ne može izmijeniti bez odobrenja.

Kako bi informacijski sustav služio svojoj svrsi, sadržane informacije moraju u svakom trenutku biti dostupne. tj. da je sustav dimenzioniran i kapacitiran prema planu njegove upotrebe[6]

Ove filozofije prenose se u svaki drugi aspekt sigurnosti, bilo da se radi o sigurnosti aplikacije ili bežičnoj sigurnosti.

IT stručnjaci za sigurnost kao što su administratori sustava i administratori mreže, jedni su od najvažnijih članova informatičkog tima. Službenik za sigurnost tvrtke (CISO-Company Information Security Officer) je glavni odgovorni za sigurnost informacijske sigurnosti te osigurava implementaciju sigurnosne politike, redovite provjererazine sigurnosti računalnih sustava. Kroz analizu sigurnosti i ranjivosti mogu se identificirati potencijalni sigurnosni problemite se mogu anticipirati određena rješenja - planovi za zaštitu, otkrivanje i reagiranje.[7]

2.2.1. Načini osiguranja računalne mreže

Sigurnost mreže obuhvaća aktivnosti koje se poduzimaju kako bi se zaštitilo svoju mrežu od neovlaštenog upada, integritet i raspoloživost mreže a za nju su zaduženi mrežni administratori te administratori sustava.

Otkrivanje slabosti u mreži može se postići sigurnosnim inženjeringom:

Praksa zaštite od tih prijetnji izgradnjom mreža kako bi bila sigurna, pouzdana i sigurna od zlonamjernih napada. Sigurnosni inženjeri dizajniraju sustave od temelja. Cilj sigurnosnog

[6] www.cis.hr/Sigurnosna politika/04.10.2019

[7] www.upwork.com/Carey Wodehouse/Inside IT Security/02.08.2019

inženjera je osigurati sustav od probijanja, napada, grešaka i to dizajniranjem, implementacijom i testiranjem kompletnih i sigurnih sustava.[8]

Kao dio sigurnosnog inženjeringa, postoje proaktivne mjere za otkrivanje gdje supotencijalne ranjivosti te kako ih otkloniti:

- Procjena ranjivosti : Inženjeri identificiraju potencijalne scenarije i postavljaju proaktivne planove i rješenja. Uz softver za analizu sigurnosti identificiraju se i rješavaju ranjivosti u računalnoj, mrežnoj ili komunikacijskoj infrastrukturi.
- Testiranje penetracije : To podrazumijeva ispitivanje mreže ili sustava na slabosti, izvješće testiranja mora sadržavati detaljne nalaze. Nađeni rizici ranjivosti i njihov utjecaj na organizaciju moraju se dobro sagledati i analizirati te se zatim donose preporuke i rješenja.[9]

2.2.2. Osiguravanje najslabijih krajnjih točaka jedne mreže

Korisnici su najslabija karika u sigurnosnom lancu mreže. Tzv. socijalnim inženjeringom napadači se lažno predstavljaju i navode korisnike da im daju vjerodajnice ili da instaliraju zlonamjerni softver. Stoga sigurnost korisnika odnosno krajnje točke je jedna od najznačajnijih komponenti sigurnosnog lanca. Tehnologija zaštite krajnjih točaka odnosi se na osiguravanju podataka na mjestu na kojem ulaze i izlaze iz mreže. To je pristup zaštite mreže na razini uređaja koji zahtijeva da bilo koji uređaj koji daljinski pristupa zajedničkoj mreži bude odobren ili da mu bude onemogućen pristup mreži. Obično se to radi o pametnom telefonu, osobnom računalu, bežičnom prodajnom mjestu ili prijenosnom računalu. Svaki uređaj koji se spaja na mrežu predstavlja potencijalnu ulaznu točku za vanjsku prijetnju. Sigurnost krajnjih točaka postavlja pravila za sprečavanje napada, a sigurnosni softver za krajnje točke provodi ta pravila. [10]

---

[8] www.upwork.com/Carey Wodehouse/Inside IT Security/02.08.2019

[9] Kou, W. Networking security and standards. Boston ; Dodrecht ; London : Kluwer Academic Publishers, cop. 1997. Str. 90

[10] Majić, I. Provođenje analize ranjivosti računalnih mreža. (2007) ; Str. 113

2.2.3. Internetska sigurnost i čuvanje protiv cyber kriminala

Internet je dizajniran s ciljem da bude funkcionalan te se u samim počecima razvoja nije toliko posvećivalo zaštiti i sigurnosti, stoga danas Internet ima određene naslijeđene slabosti koje naročito dolaze do izražaja njegovim masovnim korištenjem te načinima za koje sedanas koristi. Prije svega se ovo odnosi na komercijalno poslovanje, prijenos osjetljivih podataka i sl. Internetska sigurnost ili eng. cyber sigurnosti jepodručje u računarstvu koje se bavi zaštitom podataka.

Kako bi se zaštitile informacije u kontekstu povjerljivosti, integriteta i dostupnosti postoji niz standarda i protokolakoji omogućavaju sigurno slanje informacija putem javne mreže odnosno interneta. Također koriste se rješenja za neovlaštene update, antivirusne zaštite te različite metode enkripcijekoja će osigurati da podaci se podaci ne presretnu u tranzitu između računala, preglednika i web-mjesta.

Primjer jesu nadogradnje transparentnog HTTP protokola za pregled web stranica s HTTPS protokolom koji dodaje sloj kriptografske zaštite tzv, Secure Sockets Layer (SSL) ili Transport Layer Security (TLS).[11]

2.2.4. Cloud sustavi i sigurnost

Cloud (oblak) ili računalstvo u oblaku je tehnologija su programi i datoteke spremljeni na internetu (metaforički, "u oblaku"), a ne na osobnom računalu na kojem se radi. Primjerice, cloud computing-u pripada naširoko korištena aplikacija Google docs, s uključenim programom za obradu teksta i mogućnošću pohrane dokumenata na poslužitelj. Jedan od oblik rada u računalnom oblaku je i spremanje datoteka na mrežu. Budući da su ove usluge elektronske pošte smještene na mreži, tim datotekama se može pristupiti s bilo kojeg računala povezanog s internetom.[12]

---

[11] www.upwork.com/Carey Wodehouse/Inside IT Security/02.08.2019

[12] www.poslovni.hr/Ozren Podnar/Samo je nebo granica za cloud – najvažnije o računalstvu u oblacima/02.08.2019

Sve većim oslanjanjem na rad u Cloudu (korištenje e-pošte, pohranu podataka, aplikacije)postavlja zahtjev da sva komunikacija između web-lokacije i cloud-a mora biti sigurna i pouzdana. Uz svu tu povezanost i protok (ponekad osjetljivih) informacija dolazi do novih problema u podruju sigurnosti na internetu: sigurnost računalstva u samom cloud-u gdje ponekad čitavo poslovanje ovisi o sigurnosni nekog udaljenog računalnog sustava.

2.3. Rizici u poslovanju i svakodnevnom korištenju informacijskih tehnologija

Danas u suvremenom dobu nezamislivo je poslovati bez informacijskih tehnologija u svim segmentima proizvodnje, poslovanja i marketinga, jer današnje poslovne organizacije, bile one male ili velike, ne mogu poslovati bez informacijskog sustava koji je zasnovan na informacijsko – komunikacijskim tehnologijama.

Danas su ljudi neprestano u doticaju s informacijskim tehnologijama i njihovim informacijskim sustavima i to je danas neodvojivi čimbenik modernog čovjeka u njegovom svakodnevnom životu bilo kod podizanja ili polaganja gotovine putem bankomata, plaćanjem putem pametnih kartica u fizičkim ili online trgovinama, elektroničke naplate cestarine odnosno ENC, te pri svakom telefonskom razgovoru i u mnogim drugim životnim okolnostima. Razlog njihove primjene je automatizacija koja omogućuje daleko bržu obradu informacija i koja je manje podložna pogreškama te je ekonomski i ekološki prihvatljiva, odnosno radi se o hardveru i softveru koji predstavljaju informacijske tehnologije koje omogućuju prikupljanje, obradu, pohranu i isporuku informacija. Time osigurava poslovnoj organizaciji rast, povećanje prihoda i konkurentnost na tržištu.[13]

Primjena informacijskih tehnologija u sebi sadrži nepoznanice, rizike, nesigurnosti i probleme koji mogu biti uočeni s vremenom. To može biti primjena ne odgovarajućih odluka, metoda, provedba neodgovarajućeg znanja, gubitak podataka, nedovoljna izobrazba korisnika sustava, zlouporaba informacijskih tehnologija radi ostvarivanja neopravdanih ili protupravnih koristi od strane pojedinaca ili organiziranih skupina. To rezultira nezadovoljavajućim poslovnim informacijskim sustavom koji ne udovoljava kritičnim faktorima uspjeha jedne poslovne organizacije. Rizik informacijskih tehnologija nije samo

---

[13]Petrunić, R. Sigurnost elektroničkog poslovanja. Zagreb : Algebra, 2011.Str 46

objektivne prirode već i subjektivne, odnosno rizik može nastati namjerama pojedinaca i skupinama unutar poslovnog informacijskog sustava. Za otklanjanje rizika informacijskih tehnologija potrebno je poznavanje specifičnih metoda i alata kojima se uočava i prepoznaje rizik. Te specifične metode i alati podrazumijevaju pravilnike sigurnosne politike informacijskih sustava i međunarodne standarde sigurnosti čijom se implementacijom osigurava kvalitetno upravljanje informacijskim tehnologijama i sustavima.[14]

2.4. Sigurnosna politika informacijskih sustava

Informacijski sustavi u sebi mogu sadržavati povjerljive podatke kojima se služe korisnici koji imaju ovlasti nad tim podacima i korisnici kojima je omogućeno da koriste podatke informacijskog sustava. To su na primjer: ime identifikacije, lozinka, podaci i obavijesti sustava koji ne smiju biti javno dostupni bez odobrenja ovlaštenih korisnika. Time se provodi sigurnosna politika koja zadovoljava navedene uvjete. Sigurnosna politika predstavlja zaštitu slobode individualnih osoba, ostvaruje i implementira sankcijske mjere sigurnosne kontrole te omogućuje sigurnu razmjenu materijalnih i ljudskih resursa. To znači da sigurnosna politika informacijskih sustava obuhvaća tvrtke, državne institucije, svu računalnu opremu, sve zaposlenike i korisnike sustava. Svi oni imaju zajednički interes da im se osiguraju uvjeti zaštite i sigurnosti informacija, koji su važni za ostvarenje individualnih, tehničkih, organizacijskih, zakonskih i operacijskih ciljeva. [15]

Svrha sigurnosne politike je da omogući upravljanje s rizicima i sigurnošću informacijskih sustava te da definira elemente prihvatljivog i neprihvatljivog načina ponašanja. U suprotnom određuju se sankcije, u koliko se korisnik ne pridržava pravila koje je sigurnosna politika postavila. Da bi se provela mora biti usklađena sa zakonima i propisima od države u kojoj se provodi, te mora biti odobrena i prihvaćena od strane uprave. Korisnici i administratori pojedinog informacijskog sustava moraju biti upoznati sa sigurnosnom politikom i njezinimuvođenjem u sustav. To znači da je potrebna izobrazba svih korisnika i administratora pogotovo kod novih korisnika sustava.

[14]Petrunić, R. Sigurnost elektroničkog poslovanja. Zagreb : Algebra, 2011.Str 52
[15]Ždrnja, B. Sigurnost informacijskih sustava. Zagreb : Algebra, 2010.Str 13

Zaposlene je potrebno također upoznati s osnovnim pravilima za korištenje elektroničke pošte, zaporki i pravilima o čuvanju povjerljivih informacija. Vrlo je važno konstantno obrazovanje i usklađivanje pravila korisnika sustava, te je ustanova obavezna na svojim javnim web stranicama postavljati i ažurirati politiku prihvatljivog korištenja. Ustanova može postavljati i prilagođavati svoja pravila kako bi njihova sigurnosna politika bila usklađena s njihovim uvjetima i poslovanjem. Međutim, ne smije se zanemarivati osnovne principe i pravila „Politike prihvatljivog korištenja". Sigurnosna politika mora omogućiti slobodu korisnika u onoj mjeri koliko je potrebno za obavljanje poslova i ostvarenje cilja informacijskog sustava.[16]

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- Svu računalnu opremu koja se nalazi u prostorima Ustanove
- Administratore informacijskih sustava
- Korisnike, među koje spadaju: zaposlenici, vanjski suradnici, studenti
- Vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera.

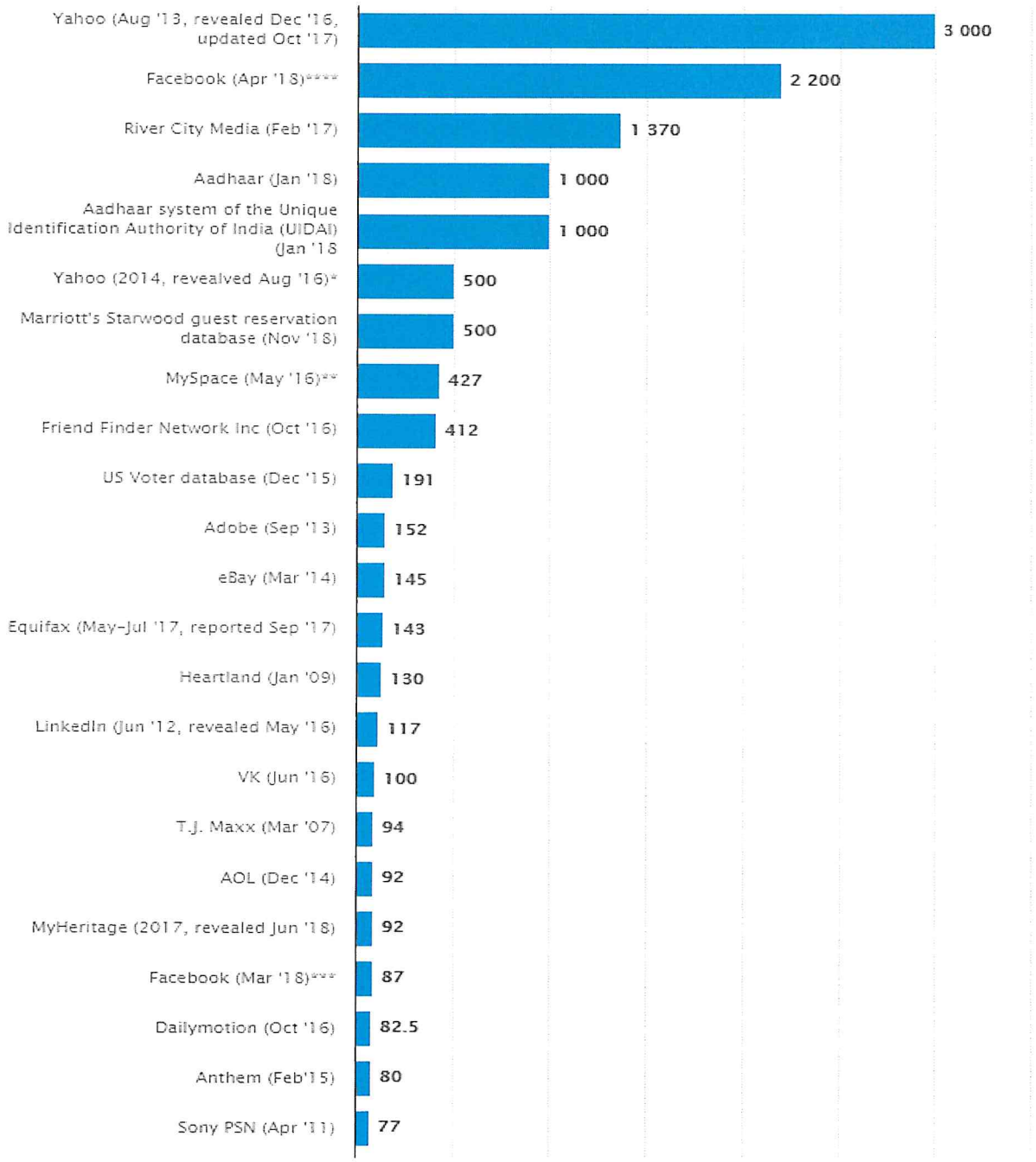
Provođenjem sigurnosne politike informacijskog sustava moraju se znati uloge i zadaci svih sudionika, kako bi se raspodijelili zadaci, obaveze, obrazovanje i formirala tijela za upravljanje sigurnošću.

Slika 4. Primjer javne objave Facebook straniceo sigurnom i efikasnom korištenju iste.Preuzeto s www.facebook.com/security(14.04.2019)

[16] www.cert.hr/sigurnosna_politika_ustanove.pdf/02.09.2019

2.5. Sigurnosni incidenti

Proteklih godina svjedoci smo mnogih pokušaja preuzimanja osjetljivih podataka. Uvijek će biti osoba koje će se pokušati domoći podataka na neautorizirani način. Neke od najvećih napada u povijesti su rezultat nedostatka snažnih mjera kontrola pristupa. Takve vrste kršenja u velikoj mjeri se i dalje šire.



Slika 5. Broj kompromitiranih podataka u odabranim kršenjima podataka od studenog 2018. (u milijunima). Preuzeto s https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide(14.04.2019)

Napad na Deloitte

Napad na Deloitte je objavljen u rujnu 2017. Najbolji je primjer devastacije s kojom se organizacija može suočiti ako ne uspije implementirati snažnu kontrolu pristupa. Deloitte - jedna od "velikih četiri" računovodstvenih tvrtki - doživjela je kršenje koje je rezultiralo neautoriziranom pristupu e-pošti svojih klijenata, uključujući one američkih vladinih agencija i velikih poduzeća. Napadači su pristupili sustavu e-pošte tvrtke putem administrativnog računa - koristeći samo jednu ugroženu lozinku. Sigurnosna industrija brzo je istaknula da račun nije osiguran autentifikacijom pomoću dva faktora.[17]

Yahoo!

Tvrtka za internetske usluge Yahoo! Doživjelaje dva velika napada na podatke njihovihkorisnika te njihovih korisničkih računa tijekom druge polovice 2016. godine. Prvi napad odvio se negdje krajem 2014., a utjecao je na više od 500 milijuna korisničkih računa. Zabilježen je još jedan napad koji se dogodio kolovozu 2013, a napad je prijavljen tek u 2016. godini. Prvobitno se smatralo da je utjecalo na više od 1 milijarde korisničkih računa. Kasnije je u listopadu 2017. potvrđeno da je utjecalo na sve 3 milijarde korisničkih računa. Oba napada smatraju se najvećim otkrivenim napadima u povijesti Interneta. U napadima su ugrožena imena, adrese e-pošte, telefonski brojevi, šifrirana ili nekodirana sigurnosna pitanja i odgovori, datume rođenja i šifrirane zaporke.

LinkedIn

Isto vrijedi i za 2012 godinu i LinkedIn. Napadači su uspjeli probiti sustav, i ugroziti 167 milijuna korisnika. Ukradene lozinke su objavljene na ruskom forumu za ukradene odnosno probijene lozinke nedugo nakon. Lozinke za tisuće računa bile su dostupne online u običnom tekstu. Stručnjaci za sigurnost na internetu rekli su da se lozinke mogu lako dešifrirati jer su napadači brzo preokrenuli proces kodiranja pomoći unaprijed napravljenih lista podudaranja šifriranih i dešifriranih lozinki.

[17] www.htbridge.com/Top 10 Application Security Data Breaches of 2018/02.09.2019

Amnesty International

Jedna skupina napadača probila je metodu zaštite kako bi saznala osobne podatke 1.000 ljudi koje podatke sadrži institucija za ljudska prava, Amnesty Internationala. Ciljali su osobe i zaštićene svjedoke na Bliskom istoku i u Sjevernoj Africi korištenjem lažnih poruka i stranica za prijavu. Cilj napada bio je prevariti žrtve u predaju pristupa svojim Google i Yahoo računima.[18]

eBay

Online tvrtka za aukcije eBay izvijestila je o napadu u koji se desio svibnju 2014.godine. Nakon napada tvrtka je obavijestila da su ugrožena imena, adrese, datumi rođenja i šifrirane lozinke svih svojih 145 milijuna korisnika. Tvrtka je izjavila da su napadači ušli u mrežu tvrtke koristeći vjerodajnice od tri korporativna zaposlenika, te su imali potpuni unutarnji pristup 229 dana, za koje vrijeme su uspjeli doći do baze podataka korisnika. Kompanija je od svojih klijenata tražila da promijene svoje lozinke, ali su rekli da su financijske informacije, kao što su brojevi kreditnih kartica, pohranjene odvojeno i nisu ugrožene. Tvrtka je tada bila kritizirana zbog nedostatka komunikacije koja je informirala svoje korisnike i loše provedbe procesa obnove lozinki.

Uber

Tvrtka Uber je krajem 2016. saznala da su dvojica napadača uspjela dobiti imena, adrese e-pošte i brojeve mobilnih telefona 57 korisnika aplikacije Uber. Također su dobili broj vozačkih dozvola od 600.000 Uberovih vozača. Nijedan drugi podatak, kao što su kreditna kartica ili brojevi socijalnog osiguranja, nisu ukradeni. Napadači su mogli pristupiti Uber-ovom GitHub računu, gdje su pronašli vjerodajnice za korisničko ime i zaporku na Uber-ovom AWS računu. Te vjerodajnice nikada nisu trebale biti na GitHubu. U vrijeme objavljivanja napada, tvrtka je pregovarala o prodaji udjela SoftBanku. Uber je u početku vrijedio 68 milijardi dolara. Do trenutka zaključenja ugovora , njegova je vrijednost pala na 48 milijardi dolara. Ne može se sve to pripisati napadu, ali to je značajan čimbenik pada vrijednosti tvrtke.

[18] www.betanews.com/Web applications leave companies vulnerable to breaches/02.09.2019

Facebook

Facebook, koji se već suočava s pitanjem kako postupa s privatnim informacijama svojih korisnika, je nedavno napadnut te su preuzeti osobni podaci gotovo 50 milijuna korisnika. To je bio najveći napad u povijesti tvrtke. Napadači su iskoristili značajku u Facebookovom kodu kako bi dobili pristup korisničkim računima i potencijalno preuzeli kontrolu nad njima.[19]

Twitter

Twitter je pretrpio zastoj u sigurnosti u svibnju 2012. godine kada je na web-mjestu za razmjenu datoteka „Pastebin" objavljeno gotovo 60.000 korisničkih imena i lozinki. U to vrijeme, Twitter je umanjio značaj incidenta tvrdeći da je većina korisničkih imena i lozinki ili duplikat ili poznati neželjeni računi. Tvrtka je odgovorila tako što je automatski ponovno postavila zaporke legitimnih računa. Nije jasno kako su napadači dobili pristup sustavu Twitter-a kako bi kopirali ove osjetljive podatke.

Sony PS

Ovo se smatra najtežom povredom podataka o sveukupnim podacima u zajednici za igrice. Od više od 77 milijuna računa, 12 milijuna imalo je nešifrirane brojeve kreditnih kartica. Napadači su dobili pristup punim imenima, lozinkama, e-mailovima, kućnim adresama, povijesti kupnje, brojevima kreditnih kartica.[20]

[19] www.htbridge.com/Top 10 Application Security Data Breaches of 2018/02.09.2019

[20] www.arstechnica.com/Bright Peter. Sony hacked yet again, plaintext passwords, e-mails/02.09.2019

3. RJEŠENJA POVEĆANJA SIGURNOSTI

Zaštita podataka je postala moralna i poslovna obaveza, te neophodan postupak pri osmišljavanju i izgradnji informacijskih sustava.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. Kontrolu pristupa moguće je podijeliti na tri temeljna postupka:

- identifikacija,
- autentifikacija
- i autorizacija.

Uzmimo za primjer korisnika, Ivana Horvata, koji pokušava pristupiti svojem računu e-pošte. Ivan se spaja na sustav te upisuje svoje korisničko ime (npr. ivan.horvat) ili svoju adresu epošte (ivan.horvat@carnet.hr). Kada bi samo ovaj korak bio dovoljan za uspješnu prijavu, ne bi bilo nikakve sigurnosti, svatko bi mogao upisati bilo neko korisničko ime i nedozvoljeno pristupiti tuđem računu. Zato 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 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 određenu razinu vjerodostojnosti tvrdnji da je korisnik za računalom zaista Ivan Horvat.

Nakon upisivanja lozinke, kada je sustav uvjeren da je korisnik zaista Ivan Horvat, sustav određuje što Ivan Horvat smije u tom sustavu. U ovom slučaju, Ivan Horvat će dobiti pristup svom računu te ostvariti određena prava u tom sustavu npr. dobit će mogućnost čitanja poruka i pristup određenim dokumentima. Ovaj daljini korak se naziva autorizacija i njime se određuje što autentificirani korisnik može raditi u sustavu odnosno za što je ovlašten.

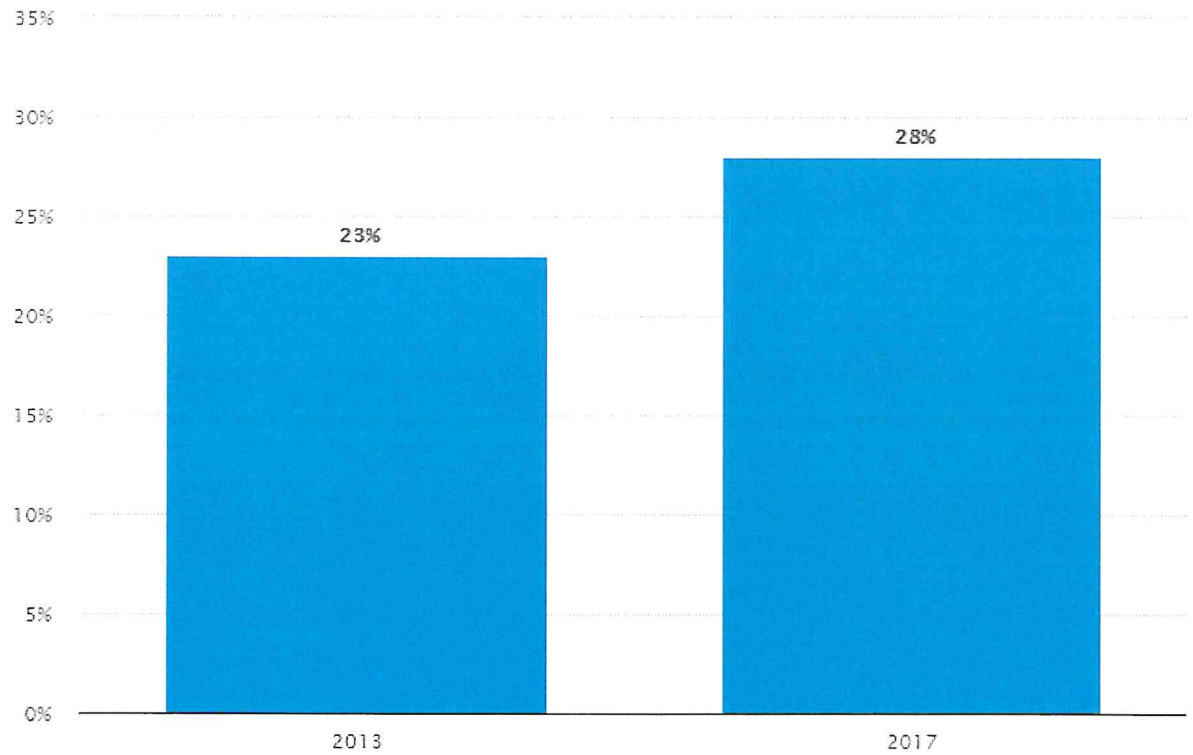
3.1 Autentifikacijski faktori

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“,
- „nešto što osoba posjeduje“,
- „nešto što osoba je“ .

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

Statistika na slici 6. pokazuje udio korisnika interneta u Sjedinjenim Američkim Državama koji koriste autentifikaciju u dva faktora u 2013. i 2017. godini. Tijekom posljednjeg razdoblja istraživanja 28% ispitanika izjavilo je da je koristilo autentifikaciju u dva faktora.



Slika 6. Udio korisnika interneta u Sjedinjenim Američkim Državama koji koriste autentifikaciju s dva faktora u 2013. i 2017. godini. Preuzeto s https://www.statista.com/statistics/789473/us-use-of-two-factor-authentication(25.5.2019)

3.1.1. Lozinka - „nešto što osoba zna“

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 i odvija se na način da korisnik sustavu predaje lozinku, PIN ili ekvivalentu informaciju te time dokazuje svoj identitet. 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.

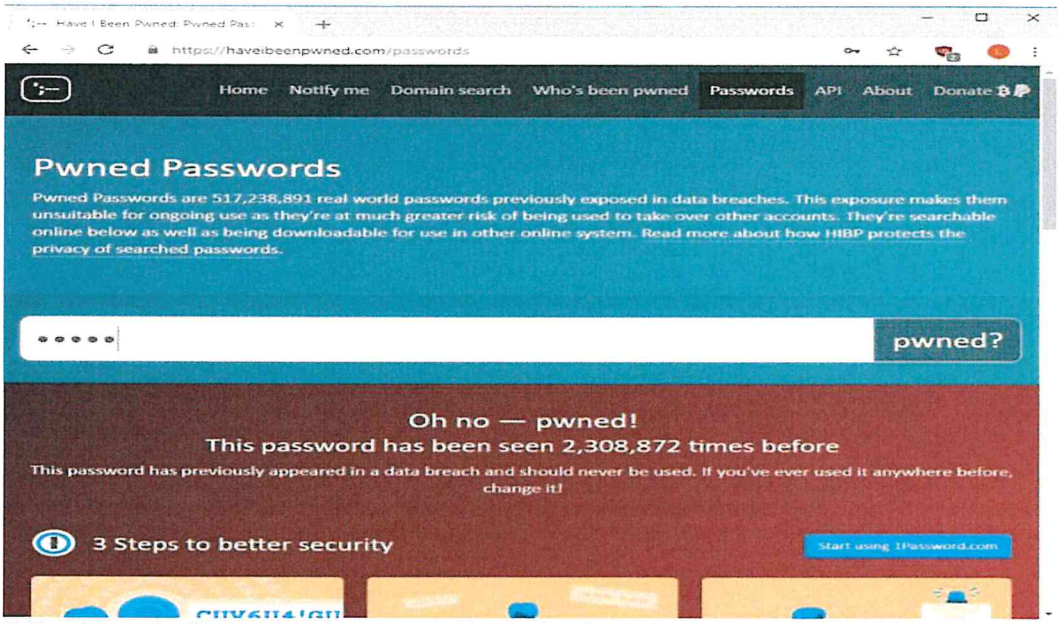
Nažalost, iako je ovaj faktor jeftino implementirati te u teoriji on može biti prilično siguran, u stvarnosti, njegova sigurnost često nije zadovoljavajuća. Jedan od razloga je da korisnici sami smišljaju lozinke, PIN-ove i slično, oni to obično rade na izrazito predvidljiv način. Napadači mogu koristiti tu predvidljivost da pogode korisnikovu 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.[21]

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“ te da preko 10% korisnika koristi neku od 25 najčešće korištenih lozinki.[22]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. No i u takvim slučajevima su korisnici predvidljivi, pa će na temelju prethodno navedenih zahtjeva doći do lozinke kao što je „Jesen2018“. Kao odgovor na ovakvu predvidljivost, oprezniji korisnici znaju osmisliti prilično složene i nepredvidljive lozinke ili čak koriste nasumično generirane lozinke koje se teško zapamte. S druge strane, korištenje iste lozinke na više mjesta je vjerojatno najveći od

[21] www.teamsid.com/Morgan/worst-passwords-2016/Announcing our Worst Passwords of 2016/02.09.2019
[22] Ibiden

do sada navedenih problema. U tom slučaju, dovoljno je da napadač jednom kompromitira tu zajedničku lozinku i imat će pristup svim servisima za koje je ta lozinka korištena.

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.[23] 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 7. upisana je lozinka „12345" za koju web stranica kaže da je viđena preko 2 milijuna puta u javno objavljenim skupovima kompromitiranih podataka. [24]



Slika 7. Provjera pojavljivanja lozinke u javno objavljenim skupovima kompromitiranih podataka na servisu Have I Been Pwned. Preuzeto s www.cert.hr/Višefaktorska autentifikacija/(02.11.2019)

[23] www.troyhunt.com/what-do-sony-and-yahoo-have-in-common/Troy Hunt/What do Sony and Yahoo! have in common? Passwords!/02.10.2019

[24] www.cert.hr/Višefaktorska autentifikacija/02.11.2019

3.1.2. Biometrija – nešto što osoba je

Sigurnost metoda autentifikacijskog faktora „nešto što osoba je" temelji se na nekom obilježju koje samo odgovarajući korisnik ima. Primjerice 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.

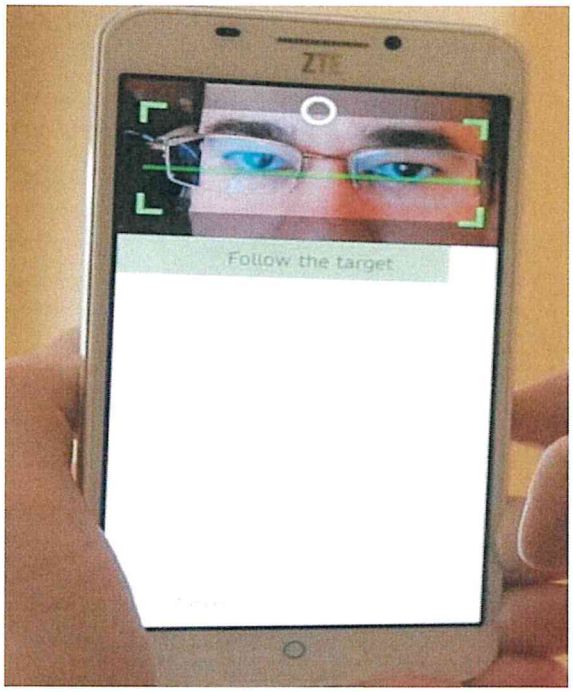
Jedna česta metoda ovog autentifikacijska faktora oslanja se na očitavanje otiska prsta. Razne oblike čitača otisaka prstiju danas je jeftino implementirati, pa je ova metoda sve češće dostupna na pametnim telefonima i prijenosnim računalima. Autentifikacija temeljena na otisku prsta je prilično praktična, ali ne i izrazito sigurna. Kroz svakodnevne radnje svaka osoba ostavi otiske svojih prstiju na raznim predmetima. Između ostaloga, otisci se ostavljaju i na pametnim telefonima i prijenosnim računalima koji se pokušavaju 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, s kojim je zatim moguće uspješno se autentificirati na sustav koji očekuje stvarni prst od legitimnog korisnika.

Za stvaranje takvog umjetnog vrha prsta može biti dovoljna fotografija otiska prsta ostavljenog na nekoj površini u kombinaciji s jeftinim materijalima i alatima. Otisak prsta ostavljen na pametnom telefonu se može fotografirati te na temelju fotografije izraditi umjetni vrh prsta. Taj umjetni vrh prsta zatim može otključati pametni telefon jednako kao i stvarni prst koji se inače koristi za otključavanje.[25]

Osim uzoraka na otisku prsta, metode ovog faktora mogu koristiti i uzorke na šarenici oka ili uzorke na mrežnici oka. Očitanje uzoraka šarenice oka slično je fotografiranju očiju korisnika fotoaparatom koji podržava snimanje dijela infracrvenog spektra, primjerice u kontekstu funkcionalnosti za noćno snimanje. Na tako snimljenoj fotografiji zatim je moguće

[25] https://srlabs.de/page/3/Fingerprints are not fit for secure device unlocking/12.02.2019

vidjeti i izolirati složeni uzorak šarenice korisnika. Slično kao i kod očitavanja 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, dok moćniji uređaji mogu očitati uzorke šarenice s čak 12 metara. Na slici 8. prikazano je otključavanje pametnog telefona očitanjem uzoraka šarenice oka.[26]



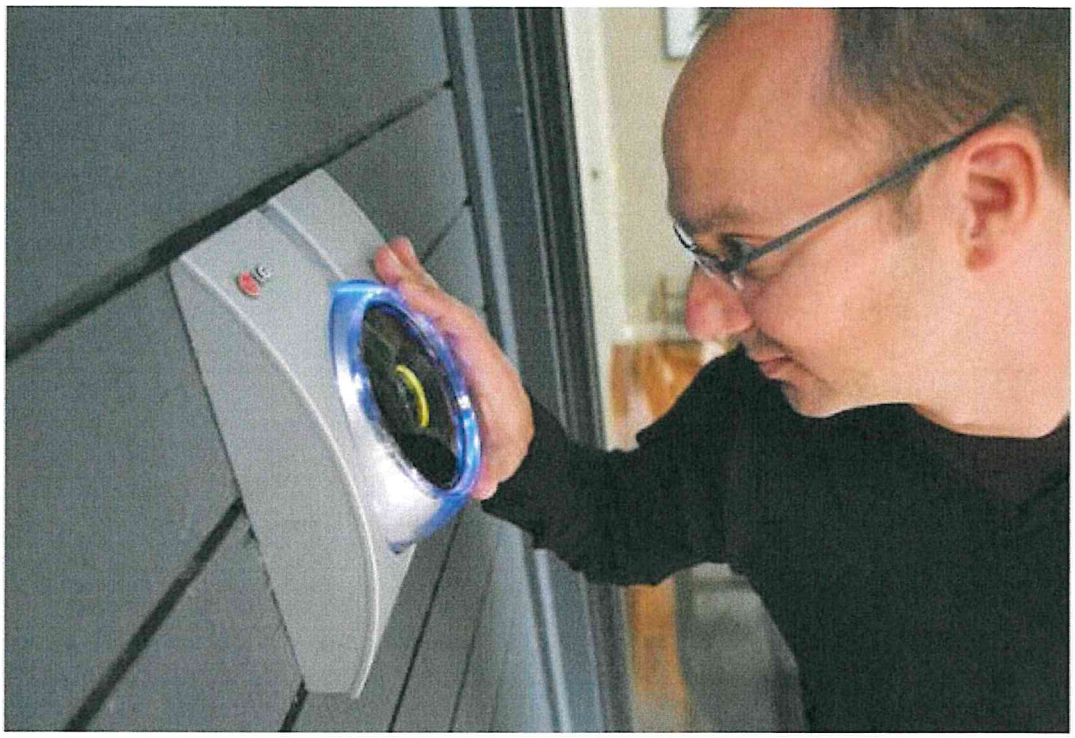
Slika 8. Otključavanje pametnog telefona očitanjem uzoraka šarenice oka. Preuzeto s https://webcusp.com/list-of-all-eye-scanner-iris-retina-recognition-smartphones(25.5.2019)

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.

[26] www.theatlantic.com/Robinson Meyer/Longg-Range Iris Scannin Is Here/12.02.2019

Za razliku od očitanja uzoraka šarenice oka, implementacija autentifikacijske očitanjem uzoraka mrežnice oka je skupa, no ujedno i prilično sigurna. Zato se ova metoda koristi gotovo najčešće u vojsci, obavještajnim agencijama i sličnim okruženjima. Očitanje uzoraka mrežnice oka moguće je samo s visoko specijaliziranom opremom te s kratkih udaljenosti. Primjer autentifikacije očitanjem uzoraka mrežnice oka prikazan je na slici 9.



Slika 9. Autentifikacija očitanjem uzoraka mrežnice oka. Preuzeto s https://www.cert.hr/wp-content/uploads/2018/12/visefaktorska_autentifikacija.pdf(25.5.2019)

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.

3.1.3. Fizički objekt - Nešto što osoba posjeduje

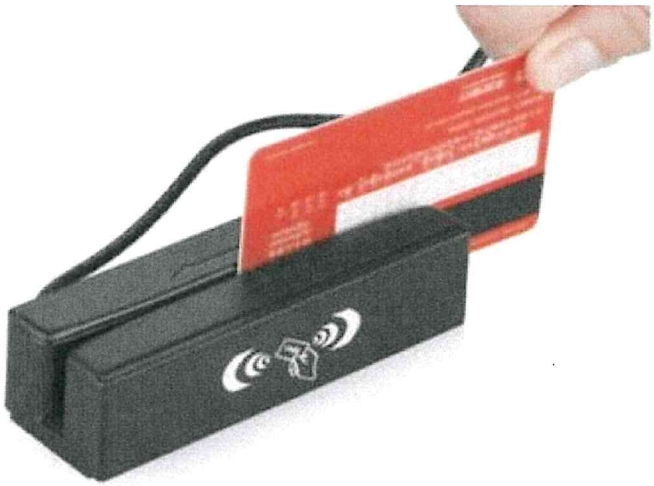
Sigurnost metoda autentifikacijskog faktora „nešto što osoba posjeduje“ temelji se na nekom objektu kojega samo odgovarajući korisnik posjeduje. Ovaj faktor moguće je implementirati na razne načine, no općenito, kada je potrebna autentifikacija:

- 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 10. U tom slučaju, ključ je objekt kojega samo legitiman korisnik posjeduje, a brava je izrađena tako da ju isključivo taj ključ može otključati.

Slika 10. primjer ključa koji otključava bravu na vratima. Preuzeto s https://www.cert.hr/wp-content/uploads/2018/12/visefaktorska_autentifikacija.pdf(25.5.2019)

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 11. Primjer kartice s memorijskim čipom kojega je moguće očitati na daljinu RFID tehnologijom (skraćeno od eng. Radio-frequency identification) te odgovarajućeg čitača prikazan je na slici 12. Uz kartice, postoje i razne značke, privjesci te slični uređaji koji su zapravo funkcionalno isti kao i prethodno opisane.[27]

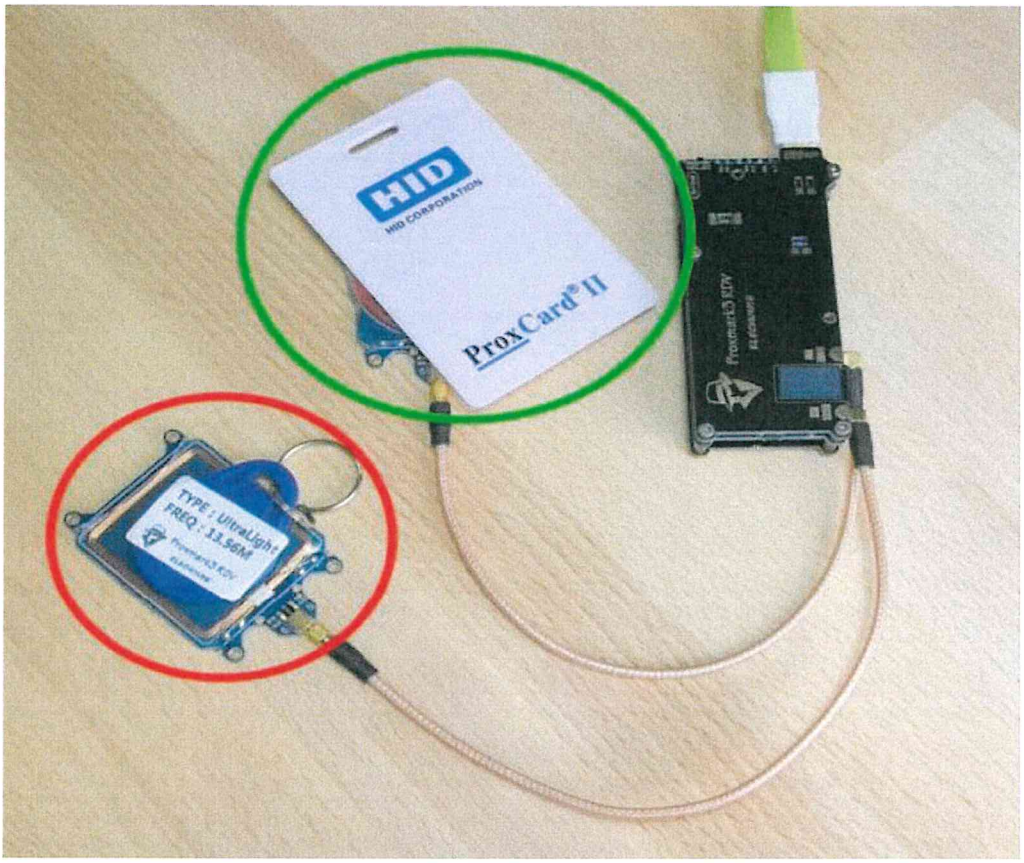


Slika 11. Primjer kartice s magnetskom trakom te odgovarajućeg čitača. Preuzeto s https://www.cert.hr/wp-content/uploads/2018/12/visefaktorska_autentifikacija.pdf(25.5.2019)

Slika 12. Primjer RFID kartice te odgovarajućeg čitača. Preuzeto s https://www.cert.hr/wp-content/uploads/2018/12/visefaktorska_autentifikacija.pdf(25.5.2019)

[27] www.cert.hr/Višefaktorska autentifikacija/02.11.2019

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 13. 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.



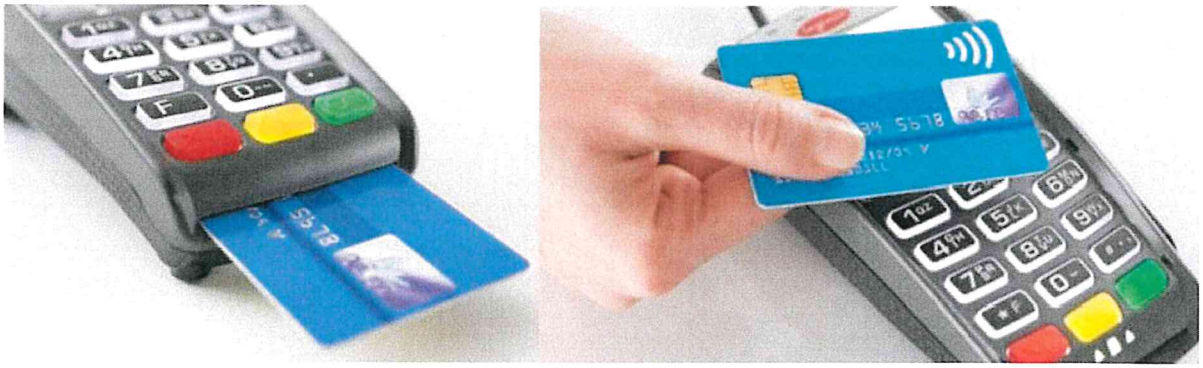
Slika 13. Primjer kloniranja RFID privjeska. Preuzeto s https://www.cert.hr/wp-content/uploads/2018/12/visefaktorska_autentifikacija.pdf(25.5.2019)

Sigurnija, ali složenija i skuplja varijanta kartica su tzv. pametne kartice. 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 pametne kartica prikazan je na slici 14. Moguće je prepoznati da se radi o pametnoj kartici po kontaktima ugrađenog računala (označeni crveno na slici 13). Uz bankovne kartice, još jedan primjer pametnih kartica su elektroničke osobne iskaznice Republike Hrvatske.

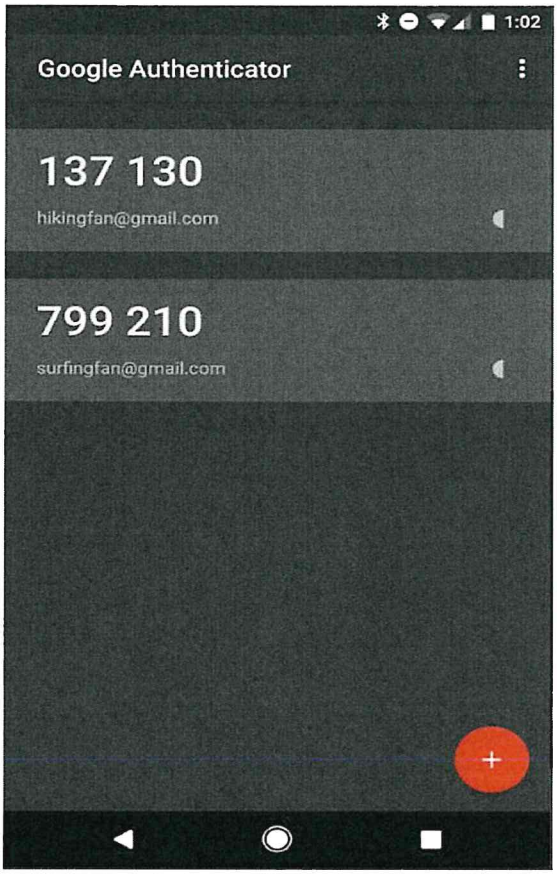
Slika 14. Primjer pametne kartica (kontakti ugrađenog računala označeni su crveno). Preuzeto s https://www.kartice.hr/id-kartice/pametne-kartice-smart-card-cip-kartice(07.07.2018)

Pametne kartice mogu se koristiti priključivanjem na čitač, a neke se mogu koristiti čak i beskontaktno kao što je prikazano na slici 15. 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 15. prikaz korištenja pametne kartice priključivanjem na čitač(lijevo) i beskontaktno korištenje pametne kartice(desno). Preuzeto s https://www.cert.hr/wp-content/uploads/2018/12/visefaktorska_autentifikacija.pdf(25.5.2019)

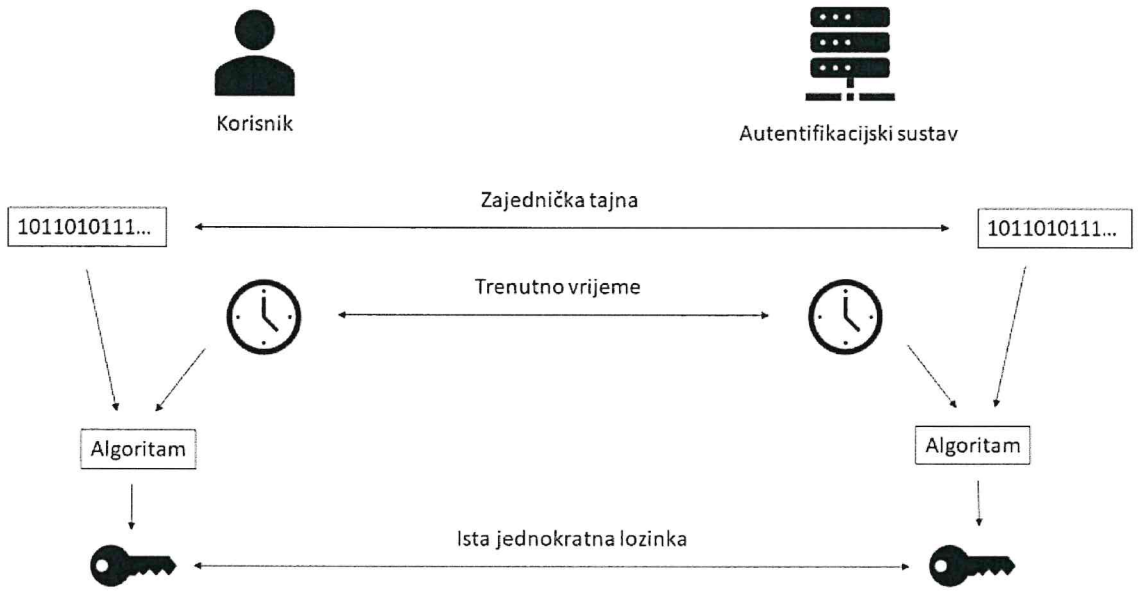
Pod autentifikacijskom faktorom "nešto što osoba posjeduje" također pripadaju i metode koje koriste sigurnosni token za generiranje jednokratne lozinke. Takav sigurnosni token može biti izveden fizički, kao samostalni uređaj, ili softverski, primjerice kao aplikacija na pametnom telefonu. Na slici 16. prikazan je primjer sigurnosnog tokena za generiranje jednokratne lozinke u obliku aplikacije za pametni telefon.



Slika 16. Sigurnosni token za generiranje jednokratne lozinke u obliku aplikacije za pametnitelefon; na zaslonu su prikazane trenutne jednokratne lozinke za dva različita računa e-pošte. Preuzeto s https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_US(07.07.2019)

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".

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 17. prikazana je shema 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 .[28]

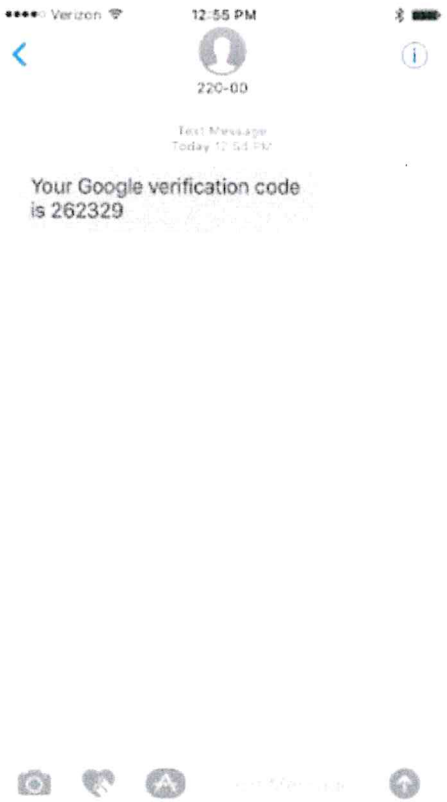


Slika 17. Shema generiranja jednokratne lozinke na temelju zajedničke tajne i trenutnog vremena. Preuzeto s https://www.cert.hr/wp-content/uploads/2018/12/visefaktorska_autentifikacija.pdf(02.11.2019)

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

[28]www.cert.hr/Višefaktorska autentifikacija/02.11.2019

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 18. prikazan je primjer SMS poruke s tajnim kodom za autentifikaciju kojega je u ovom slučaju poslao servis Gmail.



Slika 18. Primjer SMS poruke s tajnim kodom za autentifikaciju koji je u ovom slučaju poslao servis Gmail. Preuzeto s https://authy.com/guides/gmail/(07.07.2019)

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 male udaljenosti.Ova metoda autentifikacije putem SMS poruke je glavna tema ovoga rada i zato ću o njoj reći više u nastavku ovoga rada..[29]

[29]www.cert.hr/Višefaktorska autentifikacija/02.11.2019

3.2. Prednost SMS-a kao medija

Danas, ako uzmemo u obzir porast popularnosti Over-The-Top (OTT) aplikacija za razmjenu izravnih poruka kao što je WhatsApp, velika većina korisnika WhatsAppa i dalje smatra da će SMS uvijek biti bitan oblik komunikacije za njih. I što je još važnije, usluge OTT poruka ne dopuštaju korisnicima da šalju poruke velikog obujma(bulk traffic), što stavlja SMS na vrh popisa najkorisnijih marketinških alata. Aplikacije za razmjenu izravnih poruka kao što su Viber, Snapchat ili Facebook Messenger nadmašile tradicionalni promet tekstualnim porukama za razmjenu tekstualnih i slikovnih poruka od osobe do osobe (P2P). Vodstvo takvih aplikacija nad MMS-om je veliko, moglo bi se reći da ova usluga polako izumire jer većina ljudi radije šalje fotografije ili videozapise putem chat aplikacija i usluga za dijeljenje fotografija, nego MMS-om.

Glavni razlog zašto se to dogodilo je taj da najnoviji programi za slanje poruka šalju informacije putem podatkovnog kanala mobilnog telefona i stoga korisnici ne plaćaju dodatne naknade (za razliku od SMS-a). Da bi korisnik koristio OTT aplikacije za razmjenu poruka, potreban mu je mobilni telefon s pristupom internetu. Aplikacije za razmjene izravnih poruka su jednostavne za korištenje, pristupačne i već su široko prihvaćene.Tako su aplikacije za izravno razmjenjivanje poruka prešle u svakodnevnu upotrebu, uglavnom zato što nema ograničenja broja poruka koje se mogu poslati, poruke su gotovo besplatne jer se te usluge ne naplaćuju po poruci. [30]

Međutim, s poslovnog gledišta, aplikacije za razmjenu izravnih poruka nisu toliko korisne jer niti jedna od njih ne omogućuje slanje marketinških poruka u na velik broj korisnika odjednom. Za sada ne postoji funkcionalnostkojom se korištenjem takvih servisa može poslati veliki broj poruka. Masovni SMS obično se koristi za dosezanje široke publike iz razloga marketinga ili određene publike s prilagođenim sadržajem SMS-a.

[30] www.horisen.com/en/blog/ott-vs-bulk-sms/OTT vs. Bulk SMS/02.18.2019

Glavna prednost SMS-a nad aplikacijama za dopisivanje je da je SMS zrela tehnologija, vrlo dobro uspostavljena s milijardama ljudi koji su upoznati s ovom uslugom razmjene poruka. To je razlog zašto velike firme, trgovci i sve ostale vrste različitih poduzeća odlučuju koristiti Bulk SMS kako bi proveli svoje marketinške kampanje i promovirali svoje proizvode i usluge. SMS je i dalje jedina zajednička značajka za sve mobilne uređaje, za razliku od aplikacija za dopisivanje koje trebaju internet za rad i određena tehnološka znanja za pronalaženje i preuzimanje određene aplikacije za dopisivanje. Tako su aplikacije za razmjenu izravnih poruka uobičajenije među modernim i mladim ljudima, dok je SMS standardno među svima koji koriste mobilne telefone.

Dok je tržište messenger aplikacija visoko fragmentirano pa npr. WhatsApp, Viber, Snapchat, itd. imaju različite skupine korisnika koji se razlikuju po demografskim, geografskim, tehnološkim i drugim faktorima pa se kod marketing kampanja tim alatima treba voditi računa o tome da nemaju svi korisnici iste aplikacije, dok je SMS dostupan na svakom mobilnom uređaju te time čini jedinstven komunikacijski kanal. Korisnici koji preferiraju aplikacije za dopisivanje moraju preuzeti više od jedne aplikacije ako žele ostati povezani sa svim drugim korisnicima koji koriste neke druge aplikacije za razmjenu poruka.[31]

Na tržištu postoji više tvrtki koji nude takve usluge kao što suWhatsApp, Viber ili neke druge aplikacije za razgovor. Štoviše, ove aplikacije povremeno nadograđuju svoje ponude, pokušavajući osvojiti nove korisnike, tako da u jednom trenutku neki od njih mogu ponuditi nešto što drugi nemaju (npr. Prijenos uživo videozapisa) i tako svježu, novu uslugu. više preuzimanja aplikacija i novih korisnika.

Jedini siguran način na koji možete doprijeti do svih,primjerice, klijenata i potencijalnih klijenata je poruka na temelju SMS-a. To je razlog zašto tvrtke odabiru SMS za transakcijske, informativne i marketinške aktivnosti. Takve se usluge izvršavaju pomoću specijaliziranih servisa zvanih A2P Messaging for Enterprises odnosno Bulk SMS koji je široko prihvaćen, pouzdan i jeftin kanal brze komunikacije.[32]

---

[31] www.horisen.com/en/blog/ott-vs-bulk-sms/OTT vs. Bulk SMS/02.18.2019

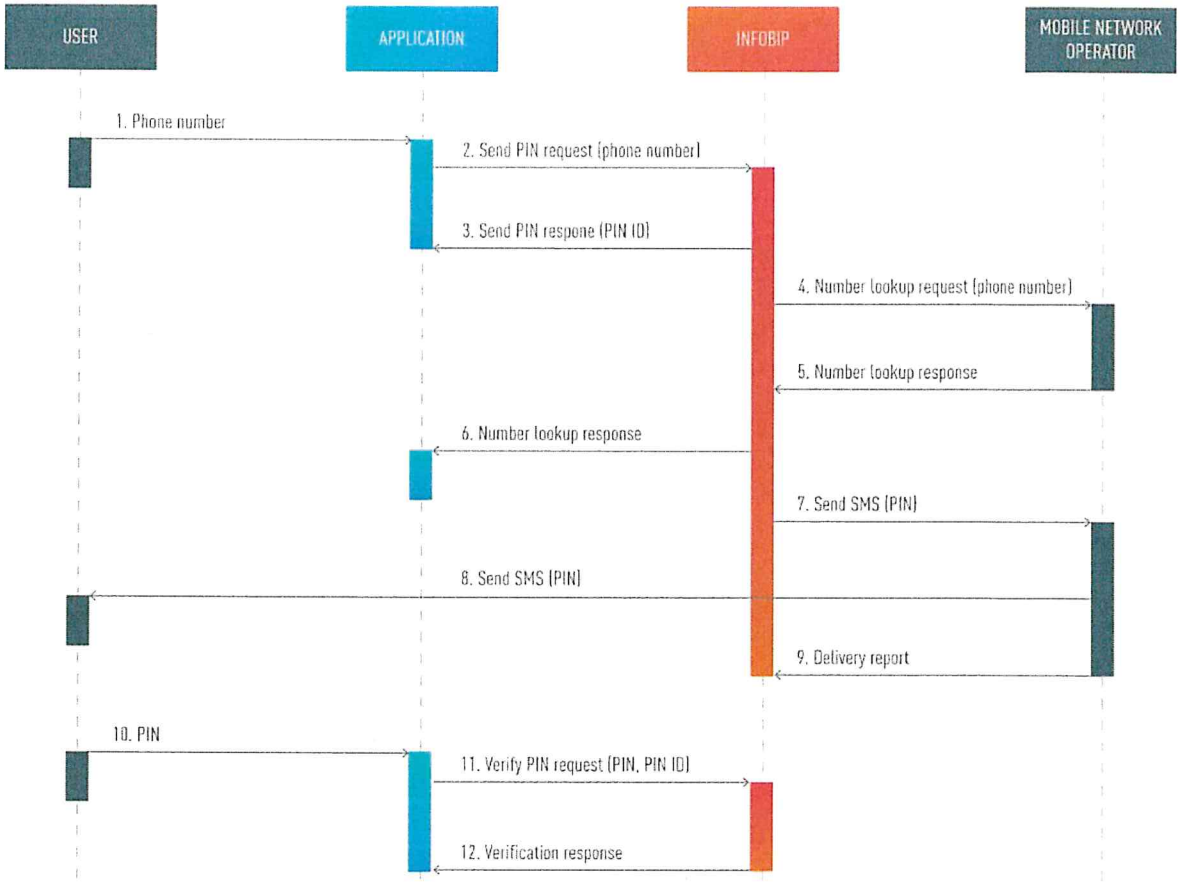
[32] Ibidem

3.3. Funkcionalnost i prednosti 2FA primjenom SMS-a

Implementacija 2FA naspram samog korištenja lozinke ima niz prednosti. Tradicionalne kombinacije korisničkog imena i lozinke su neučinkovite i podložne zloupotrebi. Korisnici često iz praktičnih razloga stavljaju lako pamtljive lozinke koje se lako probijaju. Čak i takozvane "jake" lozinke koje čine kombinacija brojki, slova i specijalnih znakova, osjetljive su na sve sofisticiranije tehnike probijanja lozinki. Implementacija 2FA odnosno OTP-a(one time password) je praktična i isplativa tehnika povećanja sigurnosti jer ne zahtijeva nikakav dodatan hardver već mobilni telefon koji svatko posjeduje.

Distribucija 2FA putem SMS poruke omogućava bolje korisničko iskustvo zato što bilo gdje, u bilo kojem trenutku korisnik može primiti OTP. Zahvaljujući rasprostranjenosti mobilnih telefona, ovakav sustav je praktičan, pristupačan i primjenjiv te čini dodatan sloj zaštite putem SMS-a. Iskoristite prednosti jedne stavke koju korisnici nose sa sobom gdje god idu - svojim mobilnim telefonima. Proces 2FA je još sigurniji jer su OTP-i važeći samo za jednu sesiju prijave ili transakciju. Niži troškovi i administrativni troškovi znače da organizacije mogu primijeniti 2FA na veći postotak svojih korisnika, što znači povećanu sigurnost smanjenjem ili čak uklanjanjem „slabih veza".

Implementacijom 2FA smanjena je stalna administracija što znači da tvrtke ne moraju izdavati, pratiti, povlačiti, slati ili zamjenjivati žetone. SMS također smanjuje troškove podrške za stolove vezane za izgubljene ključeve ili probleme sa soft aplikacijama. Neovisno o uređaju i OS-u, koji pruža standardnu platformu isporuke za provjeru autentičnosti radeći s bilo kojim standardnim mobilnim telefonom na tržištu danas. Upotreba jedinstvenog SMS koda za potvrdu identiteta je iznimno učinkovita. 2FA poruke stižu u roku od dvije sekunde, tako da će poruka stići na korisnikov mobitel gotovo odmah.Na slici 19. je prikazan i objašnjen proces 2FA u najvećoj Hrvatskoj telekomunikacijskoj kompaniji, Infobip-u:



Slika 19. Proces autentifikacije s 2 faktora u firmi Infobip. Preuzeto s https://dev.infobip.com/2fa(07.07.2019)

1. Korisnik unosi telefonski broj u aplikaciju klijenta (mobilnu ili web aplikaciju). Druga mogućnost je da klijent izvuče telefonski broj iz svoje korisničke baze podataka.
2. Aplikacija šalje zahtjev za PIN kodom s korisničkim brojem telefona na Infobip
3. Infobip generira PIN i PIN ID i šalje PIN ID aplikaciji
4. Infobip šalje zahtjev za traženje broja MNO-u(Mobile network operator)
5. Infobip prima odgovor za traženje broja od MNO
6. Infobip šalje odgovor na traženje broja na aplikaciju
7. Ako je rezultat traženja broja važeći, Infobip generira PIN kôd i šalje ga putem SMS-a
8. MNO šalje SMS s PIN kodom
9. Infobip prima izvješće, "potvrdu dostave" za poslanu poruku
10. Korisnik unosi primljeni PIN u aplikaciju
11. Aplikacija šalje zahtjev za provjeru s PIN kodom i PIN ID-om
12. Infobip provjerava primljeni PIN i šalje odgovor na zahtjev[33]

[33] https://dev.infobip.com/2fa-process-overview(21.05.2019)

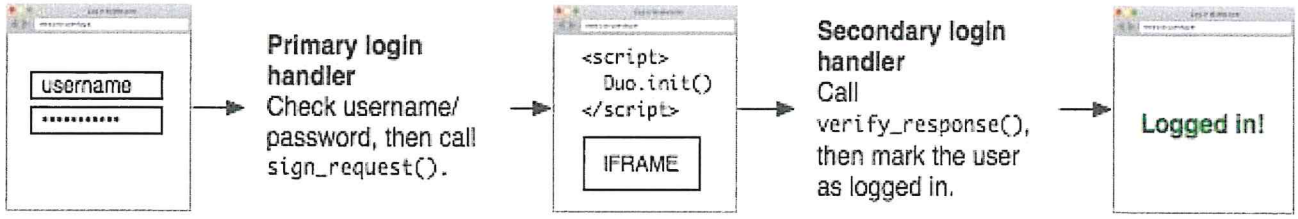
4. IMPLEMENTACIJA 2FA NA WEB STRANICAMA

4.1. Kreiranje korisničkog računa i generiranje ključeva

Prilikom odluke o povećanju sigurnosti integracijom 2FA, potrebno je najprije definirati zahtjeve te odabrati pružatelja usluge koja zadovoljava tehničke ali i komercijalne uvjete. Za prikaz primjera implementacije odabrana je usluga tvrtke Duo koja je specijalizirana za povećanje sigurnosti u procesu autentifikacije.

Implementacija autentifikacije s dva faktora nezahtijeva integraciju dijela koda pružatelja 2FA usluge na web stranicu prijave, čime se prijava dijeli u dva koraka. Nakon kreiranja korisničkog računa na webu duo.com, s administracijskog panela potrebno je preuzeti integracijski ključ, tajni ključ i API (application programming interface). Također potrebno je preuzeti i instalirati biblioteke s obzirom na programski jezik koji koristimo na našem webu. Dostupni su paketi za programske jezike Python, Ruby, ASP, ASP.NET, Java, PHP, Node.js, ColdFusion, Perl. U procesu autentifikacije značajno je da vremena oba računala (ono koje autentificira i koje se autentificira) budu precizno sinkronizirana. To se postiže pomoću internet servisa za točno vrijeme - NTP Network Time Protocol.

Slika 20. Uobičajeni proces prijave za bez 2FA. Preuzeto s https://duo.com/docs/duoweb(25.5.2019)



Slika 21. Proces autentifikacije nakon implementacije 2FA. Preuzeto s https://duo.com/docs/duoweb(25.5.2019)

Postoje tri koraka koje je potrebno učiniti prilikom integracije koda:

1) pozivanje funkcije sign_request (),
2) dodavanje JavaScript u IFRAME,
3) pozivanje funkcije verify_response ().

- Generiranje akey-a (ključa)

Akey je niz koji se generira od kompanije pružatelja 2FA usluge i čuva se u tajnosti. U ovom primjeru koristi se ključ kompanije Duo). Akey mora biti dugačak najmanje 40 znakova i pohranjen zajedno s integracijskim ključem aplikacije u koju implementiramo 2FA (ikey) te tajnim ključem (skey) u konfiguracijsku datoteku na poslužitelju.

U Pythonu se može generirati slučajni niz pomoću sljedećih naredbi:

```
>>>importos, hashlib
>>>print hashlib.sha1(os.urandom(32)).hexdigest()
8b8d4270fe28b2cf2df1426eef1c41153482ddb8
```

Sigurnost Duo aplikacije vezana je uz sigurnost skeya i akeya. Te podatke treba tretirati kao lozinku i oni bi trebali biti pohranjeni na siguran način s ograničenim pristupom, bilo da se radi o bazi podataka, datoteci na disku ili drugom mehanizmu pohrane. Uvijek ih treba prenositi putem sigurnih kanala i ne slati putem nešifrirane e-pošte.[34]

- Poziv funkcije sign_request ()

Nakon izvršenja primarne provjere autentičnosti (korisničkim imenom i zaporkom korisnika koji su spremljeni u bazi podataka), poziva se funkcija *sign_request()* koja inicijalizira proces sekundarne provjere autentičnosti. *Sign_request()* uzima kao argumente funkcije *ikey* i *skey* iz konfiguracijske datoteke, generiran *akey* te korisničko ime korisnika koji je uspješno završio primarnu provjeru autentičnosti.

[34] https://duo.com/Implementing Duo two-factor authentication into your site/02.25.2019

Primjer pozivanja funkcije u Python-u:

```
sig_request = sign_request(ikey, skey, akey, username)
```

Sign_request() izvršava *hash* operaciju pomoću HMAC-SHA1 nad korisničkim imenom, integracijskim ključem i vremenskom oznakom koristeći tajni ključ aplikacije kao ključ HMAC (hash-based message authentication code). Time se osigurava da je korisnik doista ovlašten (autoriziran) nastaviti sa sekundarnom fazom provjere autentičnosti.

4.2. Integracija forme IFRAME-a na aplikaciju

Proces autentifikacije se tehnički odvija otvaranjem IFRAME-a (HTML dokument koji je ugrađen u drugi HTML dokument) gdje će se zapravo na web stranicama aplikacije prikazati HTML s funkcionalnošću provjere autentičnosti koji se nalazi na webu tvrtke Duo. Time se nakon generiranja potpisanog zahtjeva omogućava da web aplikacija koristi Duovu funkcionalnost za provjeru autentičnosti. Komunikacija i upravljanje postavkama između oba poslužitelja kontrolira se pomoću dijela JavaScript koda, koji se ugrađuje u stranicu kao snippet (kratki isječak koda[35]).

Primjer JavaScript i izmijenjena verzija:

```
<script src="/path/to/Duo-Web-v2.js"></script>
<script>
  Duo.init({
    'host': 'host',
    'sig_request': 'sig_request',
    'post_action': 'post_action'
  });
</script>
```

[35] https://duo.com/Implementing Duo two-factor authentication into your site/02.25.2019

U ovom primjeru, Duo.init () ima sljedeće opcije:

host	Vaše ime hosta API-ja (i.e. api-XXXXXXXX.duosecurity.com
sig_request	Potpisani zahtjev generiran od strane sign_request ()
post_action	URI poslužitelja na kojem se sekundarni rezultati provjere autentičnosti (potpisani odgovor) trebaju poslati

Tablica 2. - Opis nekih autentifikacijskih funkcija u Python-u

Zatim se na stranicu s ID-om *duo_iframe* uključuje IFRAME koji služi za sekundarni upit provjere autentičnosti. Postoje opcije prilagodbe IFRAME za različite vrste uređaja odnosno njihovih ekrana, tako ga je moguće prilagoditi za uređaje manjih zaslona, kao što su telefoni i tabletni uređaji. Ta se prilagodba radi pomoću CSS-a te se mogu postaviti odgovarajuće dimenzije okvira.

Primjer integracije iframe s CSS parametrima za dimenzije okvira

```
<iframe id="duo_iframe">
</iframe>
<style>
 #duo_iframe {
   width: 100%;
   min-width: 304px;
   max-width: 620px;
   height: 330px;
   border: none;
 }
</style>
```

Kako bi se osiguralo da su dimenzije stranice ispravno postavljene (da nisu zumirane) za uređaje manjih zaslona, može se dodati meta oznaka okvira za prikaz u zaglavlju stranice:

```
<head>
<meta name="viewport" content="width=device-width, initial-scale=1">
...
</head>
```

S obzirom na to da različiti web preglednici drugačije prikazuju web stranice, potrebno je osigurati da se prikaz prilagodi različitim web preglednicima. Tako npr. za Internet Explorer dodaje se dodatna meta oznaka pri vrhu HTML koda u zaglavlje<head>:[36] Kada se stranica učita, JavaScript isječak će ispravno postaviti IFRAME te zatražiti od korisnika sekundarnu provjeru autentičnosti i POST vratiti rezultate na poslužitelj.
U suprotnom moglo bi se dogoditi na se na nekim preglednicima ili nekim dimenzijama ekrana ne prikazuje ispravno forma za autentifikaciju te se time onemogući pristup web aplikaciji.

Primjer prilagodbe prema internet pregledniku.

```
<meta http-equiv="X-UA-Compatible" content="IE=edge">
```

[36] https://duo.com/Implementing Duo two-factor authentication into your site/02.25.2019

4.3. Postavke parametara u kod

- Verify_response()

Nakon uspješne verifikacije (nakon provjere autentičnosti putem upisivanja koda dobivenog putem SMS-a), IFRAME će generirati potpisani odgovor *sig_response* i poslati ga natrag na predefinirani URL *post_action.*
Na strani poslužitelja gdje je aplikacija, poziva se *verify_response()* funkcija da bi provjerilo da li je potpisani odgovor legitiman.
verify_response() funkcija uzima kao argumente ključ integracije (*ikey*), tajni ključ (*skey*), tajni ključ za integraciju (*akey*) i potpisani odgovor te vraća kao rezultat korisničko ime autentificiranog korisnika ako je odgovor valjan, ili *null* vrijednost ako je odgovor nevažeći odnosno ako autentifikacija nije prošla ispravno.[37]

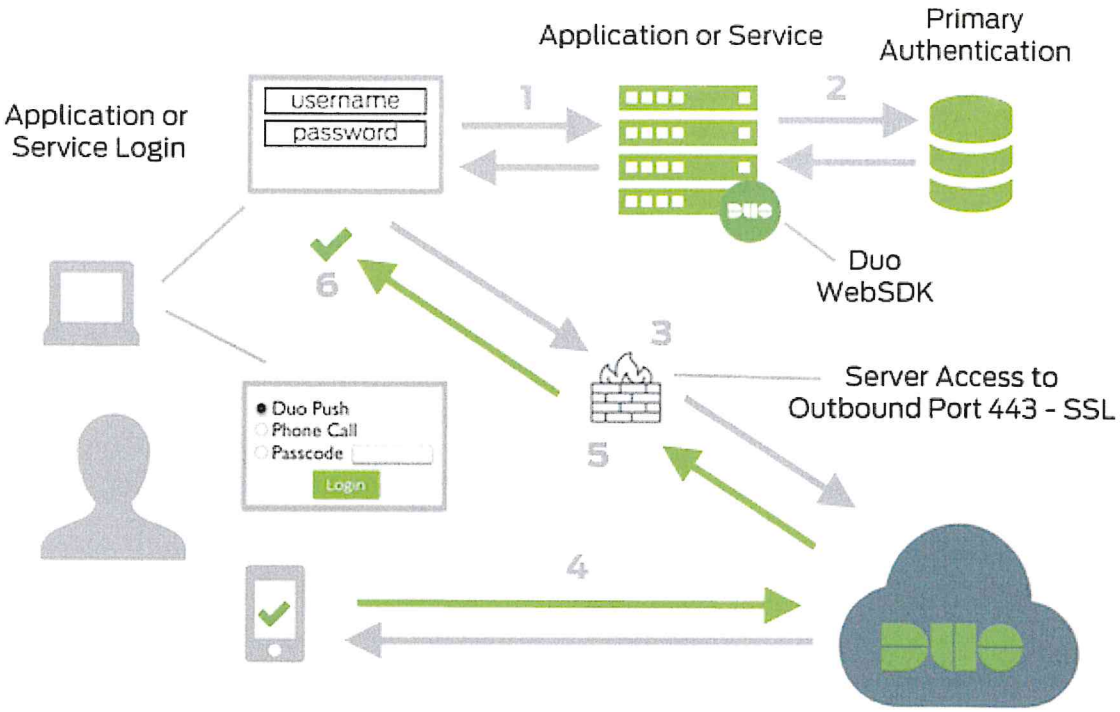
Primjer poziva funkcija u Pythonu:

```
sig_response = self.get_argument("sig_response")
authenticated_username = verify_response(ikey, skey, akey, sig_response)
if authenticated_username:
  log_user_in(authenticated_username)
```

Time je i sekundarna provjera autentičnosti zadovoljena te se aplikacija može nastaviti koristiti prema potrebi. Najčešće se postavlja neki identifikator (npr. kolačić, stanje sesije, itd.) čime korisnik može nastaviti koristiti aplikaciju kao autentificirani korisnik.

Duo omogućava različite načine 2FA akcija koje korisnik mora napraviti da bi potvrdio svoj identitet. Cijeli proces prikazan je na slici 18.

[37] ibidem



Slika 22. Shema procesa autentifikacije na web stranici od kompanije Duo. Preuzeto s https://duo.com/docs/duoweb(25.5.2019)

1. Pokrenuta je veza web-aplikacije ili usluge
2. Primarna provjera autentičnosti
3. Veza s web-aplikacijom ili uslugom uspostavljena na Duo Security preko TCP priključka 443
4. Sekundarna provjera autentičnosti putem usluge Duo Security
5. Web-aplikacija ili usluga prima odgovor za provjeru autentičnosti
6. Sesija web-aplikacije ili usluge prijavljena

5. ZAKLJUČAK

Uobičajeno korištenje jednog faktora za autentifikaciju u sustavu je praktično ali ne i dovoljno sigurno. Kako bi se spriječiloneovlašteno korištenje i pristup podacima, razvijene su aplikacije za povećanje sigurnosti autentifikacije s dva faktora. Te su aplikacije jednostavne za korištenje aznačajno povećavaju sigurnost dodavanjem dodatnog sloja sigurnosti. Unatoč njihovoj jednostavnosti korištenja, vrlo se malo koristi te mnoge tvrtke nisu implementirale autentifikaciju s dva faktora. Jedan od razloga je ignoriranje rizika te nepoznavanje sigurnosnih mjera.

Dvofaktorski sustavi provjere autentičnosti u kombinaciji s tradicionalnim sustavom lozinki mnogo su sigurniji od jednostavnog korištenja vjerodajnica. Mnogi od sigurnosnih incidenatakoji uključuje krađu korisničkih podataka mogli su biti spriječeni da je bio uspostavljen sustav autentifikacije s dva faktora. Čak i uz poznavanje lozinke, neovlašten pristup korisničkom računu ne bi bio moguć jer je potreban drugi autentifikacijski faktor odnosno pristupni kod.

Provedbom ove mjere sigurnosti ne rješavaju se svi sigurnosni problemi, međutim, uzevši u obzir relativno mali trošak i jednostavnost implementacije u odnosu na velik rizik i posljedice do kojih dolazi prilikom sigurnosnih incidenata, ova metoda zaštite svakako se preporučuje implementirati.

Primjeri krađeračunalnih podataka te njihova sprječavanja navedeni su kroz ovaj završni rad te se time potvrđuje hipoteza ovog rada:

bez obzira na veličinu tvrtke i poslovanja, te broj korisnika koji se želi zaštititi, primjena autentifikacije u dva faktora na web aplikacijama je relativno laka za implementaciju uzevši u obzir kompleksnost web tehnologije te stvara dodatan sloj sigurnosti koji značajno povećava sigurnost informacijskih sustava. Time je hipoteza ovog rada potvrđena.

Implementacija sigurnosnih mjera je uvijek kompromis između lakoće korištenja i same razine sigurnosti. Tendencija je da će se sljedeće generacije metoda za provjeru

autentičnosti razvijatitako da će osiguravati korisnicima da uz pomoćviše faktora autentifikacije ostvarujujoš veću sigurnost uz jednostavnost korištenja.

Kako bi metode autentifikacije bile pouzdanijei jednostavnije za korisnika, razvijaju se biometrijske tehnologije kojesudonedavno bile skupe i nepouzdana ali postaju sve preciznije i pristupačnije.

Tako se skeniranjem otisaka prstiju, šarenice oka ili čitavog lica podiže razina sigurnosti uz jednostavnost primjene za samog korisnika. Ovdje se otvaraju pitanja privatnosti pojedinca, te je stoga interesantno obraditi pitanje privatnosti podataka u biometrijskim metodama i tehnikama te se u tom kontekstu preporučuju daljnja istraživanja.

LITERATURA

1. Petrunić, R. Sigurnost elektroničkog poslovanja. Zagreb : Algebra, 2011.Str 46

2. Ždrnja, B. Sigurnost informacijskih sustava. Zagreb : Algebra, 2010.Str 13

3. Kou, W. Networking security and standards. Boston ; Dodrecht ; London : Kluwer Academic Publishers, cop. 1997.

4. Majić, I. Provođenje analize ranjivosti računalnih mreža (2007) ; str. 111-115.

5. www.cert.hr/sigurnosna_politika_ustanove.pdf/02.09.2019

6. www.cert.hr/Višefaktorska autentifikacija/02.11.2019

7. www.history.com/History.com Editors/The Invention of the Internet/02.07.2019

8. www.statista.com/Number of internet users worldwide/25.5.2019

9. www.horisen.com/en/blog/ott-vs-bulk-sms/OTT vs. Bulk SMS/02.18.2019

10. www.cis.hr/Sigurnosna politika/04.10.2019

11. www.upwork.com/Carey Wodehouse/Inside IT Security:How to Protect Your Network from Every Angle/02.07.2019

12. www.poslovni.hr/Ozren Podnar/Samo je nebo granica za cloud – najvažnije o računalstvu u oblacima/02.08.2019

13. www.htbridge.com/Top 10 Application Security Data Breaches of 2018/02.09.2019

14. www.betanews.com/Web applications leave companies vulnerable to breaches/02.09.2019

15. www.arstechnica.com/Bright Peter. Sony hacked yet again, plaintext passwords, e-mails/02.09.2019

16. www.teamsid.com/Morgan/worst-passwords-2016/Announcing our Worst Passwords of 2016/02.09.2019

17. www.troyhunt.com/what-do-sony-and-yahoo-have-in-common/Troy Hunt/What do Sony and Yahoo! have in common? Passwords!/02.10.2019

18. https://srlabs.de/Fingerprints are not fit for secure device unlocking/12.02.2019

19. www.theatlantic.com/Robinson Meyer/Longg-Range Iris Scannin Is Here/12.02.2019

20. https://dev.infobip.com/2fa-process-overview/21.05.2019

21. https://duo.com/Implementing Duo two-factor authentication into your site/02.25.2019

22. www.bishopfox.com/resources/tools/rfid-hacking/attack-tools/Bishop Fox/RFID Hacking Tools & Downloads/02.18.2019

POPIS SLIKA

POPIS TABLICA