Overjanje, gesla in digitalno podpisovanje

Marko Hölbl

Annotation

Ta predmet predstavlja koncept overjanja in gesel ter osnovne koncepte in tehnologije. Poleg tega je predstavljena vloga digitalnega podpisa pri overjanju ter njegovi osnovni koncepti in tehnologije.

Objectives

Ta tečaj vsebuje osnovne informacije o overjanju, njenih elementih in overjanju z geslom ter o tem, kako ustrezno zaščititi gesla tako na strani uporabnika kot na strani overjanja. Obravnavani so koncepti upravljanja gesel, večfaktorskega overjanja n overjanja brez gesla.
Poleg tega so predstavljene informacije o tehničnem ozadju digitalnega podpisovanja, vključno s zgoščevalnimi funkcijami, kriptografijo javnih ključev in infrastrukturo javnih ključev. Nazadnje je predstavljeno digitalno podpisovanje kot sredstvo overjanja.

Keywords

gesla, overjanje, digitalni podpisi, infrastruktura javnih ključev, zgoščevalne funkcije

Date of Creation

06.01.2022

Duration

15 ur

Language

English

ISBN

Literature

[1] Batten, L. M. (2013). Public key cryptography: applications and attacks, John Wiley & Sons.

[2] Boonkrong, S. (2021). Authentication and Access Control: Practical Cryptography Methods and Tools, Springer.

[3] Buchmann, J., et al. (2013). Introduction to public key infrastructures, Springer.

[4] Burnett, M. (2006). Perfect password: Selection, protection, authentication, Elsevier.

[5] Grassi, P. A., et al. (2017). "NIST special publication 800-63b: digital identity guidelines." National Institute of Standards and Technology (NIST).

[6] Grimes, R. A. (2020). Hacking Multifactor Authentication, John Wiley & Sons.

CHAPTER 1

Uvod

DEFINITION

Overjanje je postopek preverjanja identitete nekoga ali nečesa.

Pri tem se uporabljajo informacije, ki jih zagotovi subjekt, ki ga je treba preveriti. Postopek overjanja v zasebnih in javnih računalniških sistemih, kot so računalniška omrežja, pogosto zahteva, da nekdo, običajno uporabnik, za prijavo uporabi poverilnice, ki jih izda sistem. Dejstvo, da ima uporabnik geslo, naj bi dokazovalo, da je pristen. Najpogostejša metoda overjanja je kombinacija uporabniškega imena in gesla. Vendar obstajajo tudi druge možnosti overjanja, vključno z biometrijo, pametnimi karticami, žetoni za enkratno uporabo itd.

V večini primerov overjanje zahteva predložitev pooblastil ali sredstev, ki utemeljujejo trditev, da ste tisti, za katerega se izdajate. Predmeti vrednosti ali poverilnice temeljijo na več različnih značilnostih, ki dokazujejo, kaj veste, imate ali ste.

- **Nekaj, kar veste:** To je lahko vaša duševna lastnost, na primer geslo, ki ga poznata tako uporabnik kot overitelj. Čeprav je to stroškovno učinkovita upravna rešitev, je občutljiva na izpade spomina ljudi in druge pomanjkljivosti, kot je varno shranjevanje datotek z gesli s strani sistemskih administratorjev. Uporabnik lahko uporablja isto geslo za vse prijave v sistem. Gesla, gesla in osebne identifikacijske številke (PIN) so primeri takšnih dejavnikov.

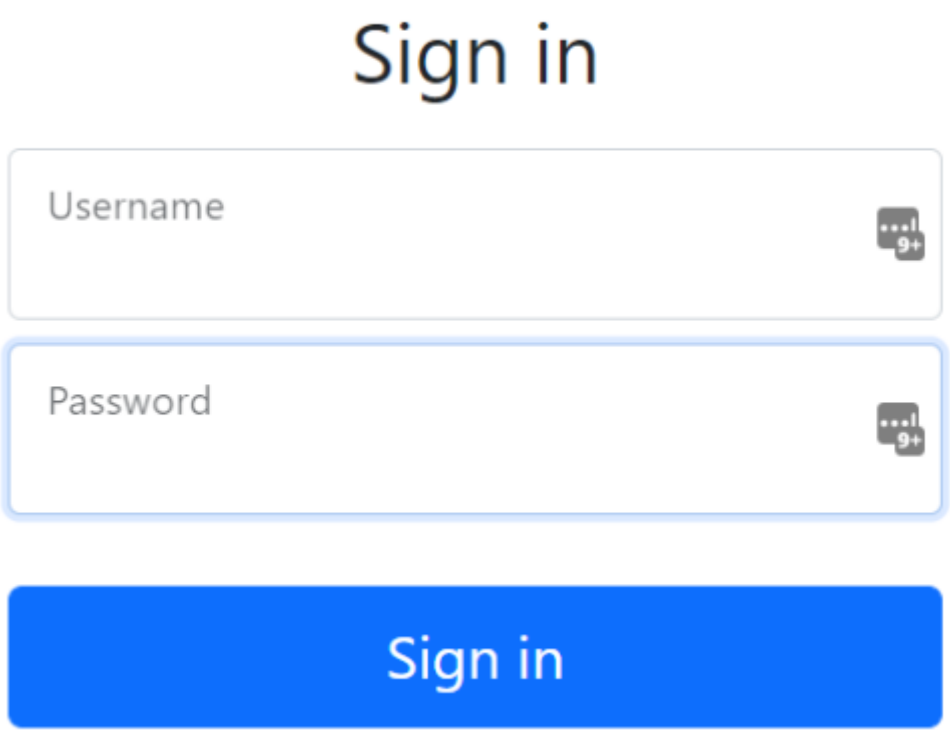


Fig. 1. Primer prijave uporabnika z uporabniškim imenom in geslom.

- **Nekaj, kar imate**: To je lahko katerakoli vrsta izdanega ali pridobljenega žetona ali oznake za samoidentifikacijo, vključno s pametnimi karticami, strojnimi žetoni, mobilnimi telefoni in različnimi drugimi sredstvi. Ker je posamezne fizične identifikacije težko zlorabiti, je ta oblika varnejša od prvega pristopa (nekaj, kar poznate). Na primer, izgubiti pametno kartico je težje kot si zapomniti številko kartice.

Fig. 2. Primeri strojnih žetonov za tip overjanja "Nekaj, kar imaš".

- **Nekaj, kar ste**: To je naravno pridobljena telesna lastnost, kot je prstni odtis. Ta vrsta overjanja se večinoma imenuje biometrija. Čeprav je uporaba biometričnih podatkov preprosta, lahko stroški pridobivanja biometričnih čitalnikov predstavljajo težavo. Primeri tega dejavnika so prstni odtisi, vzorci očesne mrežnice, vzorci DNK in prepoznavanje obrazov.

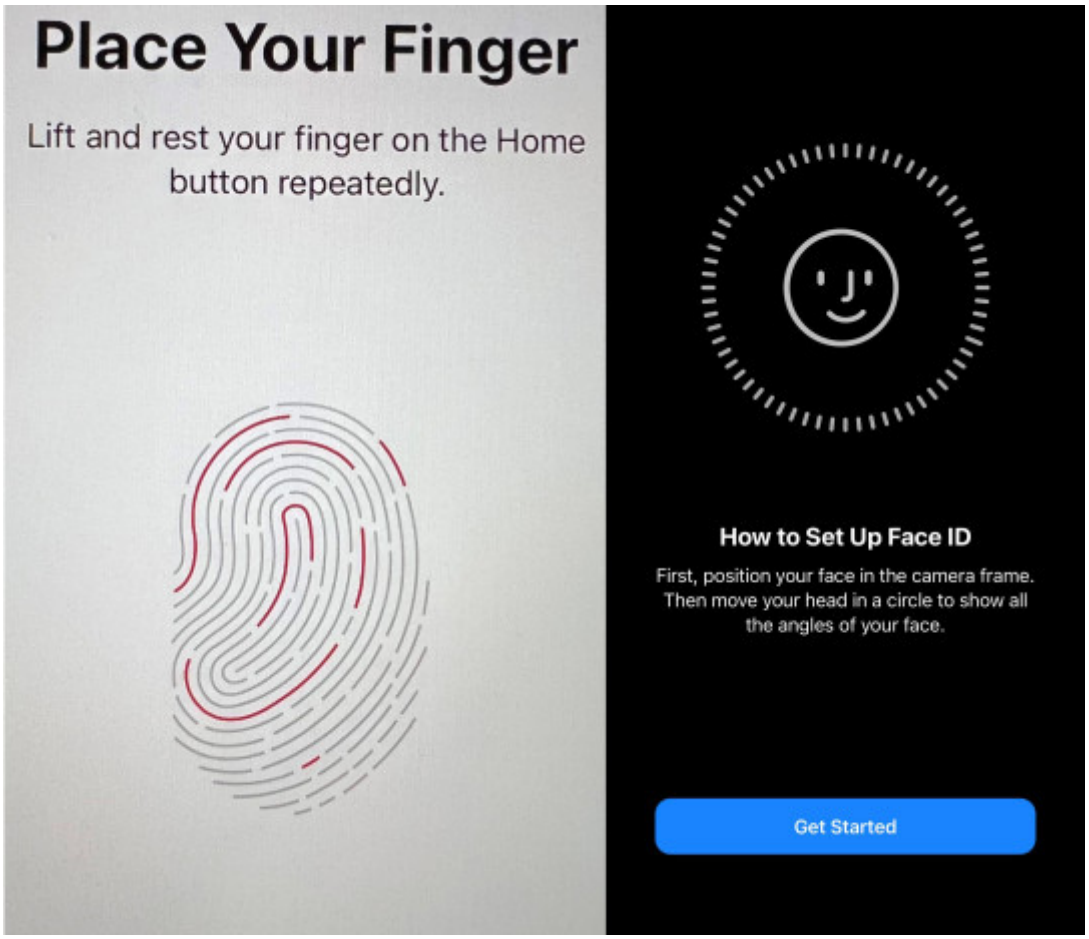


Fig. 3. Primeri biometričnega overjanja s pametnim telefonom.

ADVANTA

Če sistem sistematično zahteva številne dejavnike overjanja, lahko doseže zanesljivo varnost.

DISADVANTA

Vendar ima lahko prepogosto overjanje nasproten učinek, saj ogroža udobje uporabnika.

Interaktivní prvek

Drug način obravnavanja overjanja je po sredstvih, ki jih uporablja in posledično zavzamejo eno od treh oblik:

- **Osnovno overjanje** vključuje strežnik. Strežnik na primer hrani uporabniško datoteko z gesli, uporabniškimi imeni in nekaterimi drugimi bistvenimi podatki za overjanje. To je najbolj razširjen način overjanja uporabnikov. Vendar ima več pomanjkljivosti, med drugim pozabljanje in napačno shranjevanje podatkov za overjanje, kot so gesla.

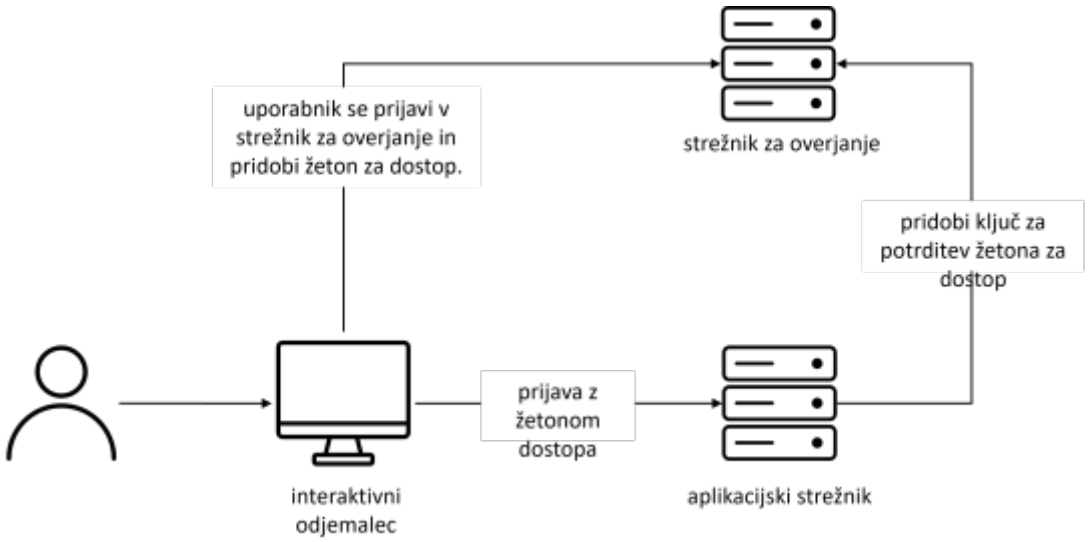


Fig. 4. Osnovno overjanje na podlagi strežnika

- **Izziv-odgovor** je metoda overjanja, pri kateri strežnik ali drug sistem overjanja gostitelju, ki zahteva overjanje, pošlje izziv in počaka na odgovor. Primer tega je uporaba enkratnika - časovno spremenljivega poljubnega števila ali zaporedja bitov, ki se uporabijo samo enkrat, da se preveri, ali so podatki uporabljeni samo enkrat.
- **Centralizirano overjanje** se nanaša na sistem, v katerem strežnik overja, avtorizira in revidira uporabnike omrežja. Ti trije postopki se izvajajo kot odziv na dejavnost strežnika. Primer takega overjanja je Kerberos.

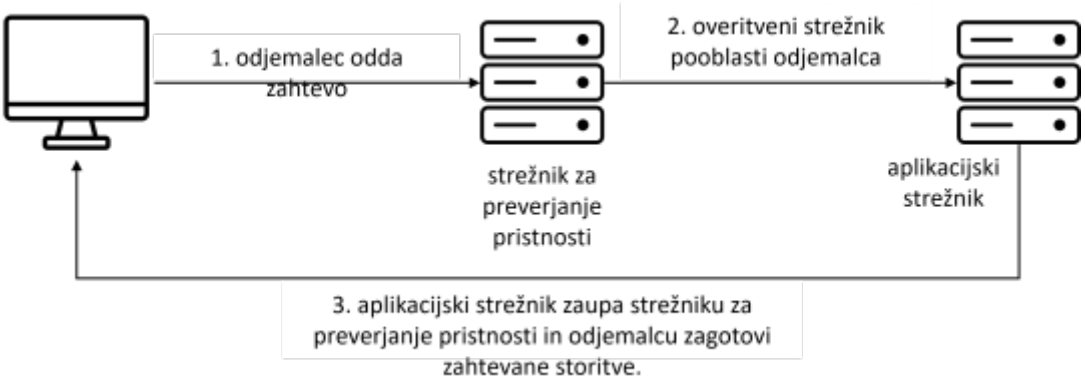


Fig. 5. Centralizirano overjanje

Interaktivní prvek

CHAPTER 2

Elementi in postopek overjanja

Overjanje zahteva postopek overjanje, ki temelji na:

- subjekt ali skupina subjektov, ki želi pridobiti overjanje;
- razlikovalna značilnost od subjekta/subjektov, katerih pristnost se preverja;
- overitveni napravi (običajno strežnik);
- overitveni mehanizem za preverjanje pravilnosti overitvenih značilnosti;
- mehanizem za nadzor dostopa za sprejem ali zavrnitev overjanja.

Prvi element so pogosto **posamezniki, procesi ali sistemi,** ki želijo pridobiti dostop do sistema. Če delujejo individualno, morajo biti pripravljeni overitvenemu organu pokazati dokaz, da so pooblaščeni za uporabo zahtevanega sistemskega vira.

Drugi element overjanja je **razlikovalna značilnost** uporabnika. O teh smo že govorili in jih delimo na nekaj, kar poznate, nekaj, kar imate, in nekaj, kar ste. Nekateri od teh elementov morda ne bodo zadostovali za popolno overjanje subjekta, za izboljšanje overjanja in zagotavljanje močnejših zagotovil pa je mogoče uporabiti kombinacijo elementov iz več dejavnikov in zaupanja.

Naloga **overjanja** je pozitivno in samodejno preverjanje poverilnic entitete in ugotavljanje, ali je tej entiteti dovoljen dostop do zahtevanega sistemskega vira ali ne. Ko je poslana zahteva za overjanje, overitelj zahteva poverilnice za dokončanje postopka overjanje. Nato overitelj zbere podatke in jih pošlje mehanizmu za overjanje. Kot overitelj lahko deluje strežnik, ki ga določi uporabnik, virtualno zasebno omrežje (VPN), požarni zid, spletni strežnik, namenski strežnik v celotnem podjetju, neodvisna storitev overjanja ali kakšna druga vrsta globalne storitve identitete. Ne glede na to, kaj se uporablja kot overjanje, mora biti postopek overjanja izveden tako, da se dobi vrednost, kot je žeton, ki se lahko kasneje uporabi za ugotavljanje informacij o pooblaščenem uporabniku.

Pregled tega postopka overjanja je prikazan na sliki 5.

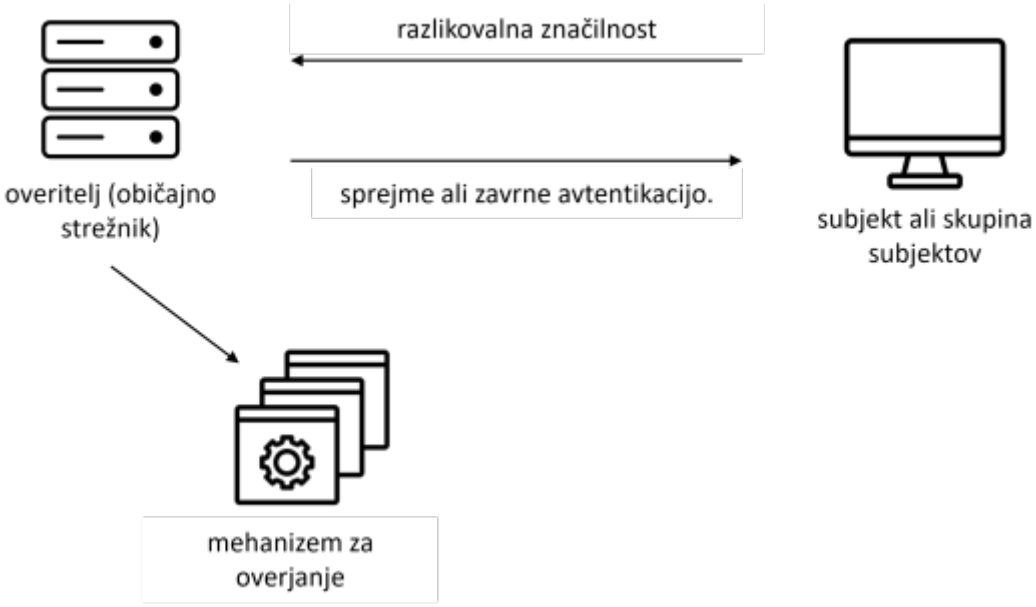


Fig. 6. Osnovni postopek overjanja in njegovi elementi.

Metoda overjanja je sestavljena iz treh delov, ki skupaj zagotavljajo prisotnost overitvenih lastnosti uporabnika:

- vnos,
- prometni sistem in
- preveritelja.

Interaktivní prvek

Vhodna komponenta služi kot interakcija uporabnika z mehanizmom overjanja. Primeri so računalniška tipkovnica, čitalnik kartic, video kamera, telefon ali podobna naprava. Zajeti elementi za identifikacijo uporabnika se prenesejo na mesto, kjer se pregledajo, analizirajo in sprejmejo ali zavrnejo. Vendar pa je treba te izdelke prepeljati, da pridejo na to lokacijo. Zato je za prenos podatkov med vhodno komponento in elementom, ki lahko preveri identiteto osebe, odgovoren transportni del sistema. Ti podatki se v sodobnih overitvenih sistemih prenašajo prek omrežja, kjer jih lahko zaščitijo protokoli. Zadnja komponenta sistema za overjanje je preverjanje, ki je mehanizem za nadzor dostopa.

Interaktivní prvek

2.1 Vrste overjanje

Opredelili smo tri dejavnike, ki se uporabljajo pri overjanju uporabnika. Opozorili smo tudi, da so ti dejavniki sicer dobri, vendar so v nekaterih od njih tudi ranljivosti. Preglednica 1 prikazuje pomanjkljivosti vsakega od dejavnikov.

Table 1. Kategorije overjanja

Dejavnik	Primeri	Ranljivosti
kaj veste	geslo, PIN	se lahko pozabijo, uganejo, podvojijo, zlahka pridobijo v primeru goljufije (npr. ribarjenja)
kaj imate	žetoni, pametna kartica, enkratno geslo, poslano na vašo telefonsko številko.	se lahko izgubijo, ukradejo, razmnožijo.
kaj ste.	prstni odtis, obraz, šarenica	neizpodbojna - ni je mogoče spremeniti v primeru zlorabe.

DISADVANTA

Omenili smo, da lahko prva dva dejavnika, "kar veš" in "kar imaš", povzročita težave overitelju, saj so lahko posredovane informacije netočne. Lahko so nezanesljive, ker so ti dejavniki podvrženi številnim znanim težavam, vključno z možnostjo izgube, ponarejanja ali enostavnega razmnoževanja predmetov. Znanje se lahko tudi pozabi, znanje in stvari pa se lahko delijo ali ukradejo.

Interaktivní prvek

2.1.1 Overjanje z več dejavniki

DEFINITION

Pri večfaktorski overjanju (MFA) se uporabljata vsaj dva različna dejavnika (kaj poznate, kaj ste in kaj imate). Pri dvofaktorski overjanju (2FA) je enako, vendar se uporabljata natanko dva dejavnika.

Če se dandanes uporablja večfaktorska avtomatizacija, je to skoraj vedno dvofaktorska avtomatizacija. Običajno je prvi dejavnik geslo ali PIN (nekaj, kar poznate), drugi pa je običajno bančna kartica, SMS ali koda, ki jo ustvari aplikacija (kar imate - tj. vaša mobilna naprava). Uporaba prstnih odtisov, skeniranja očesne mrežnice itd. (kar ste) je mogoča, vendar se redkeje uporablja, ker je potrebna dodatna strojna oprema (višji stroški).

Večfaktorsko overjanje je dober način za zmanjšanje tveganja in verjetnosti ogrožanja poverilnic. Oglejmo si na primer kombinacijo gesla in kode aplikacije. Tudi če je ogroženo samo spletno mesto ali je

geslo pridobljeno od drugod, se napadalec ne more prijaviti, saj lahko sicer predloži ustrezno uporabniško ime in geslo, ne more pa predložiti kode, ustvarjene v mobilni napravi. Ukradeno geslo tako postane neuporabno (razen če napadalec ukrade tudi mobilno napravo, vendar to ni razširljiv napad in zato za večino ljudi ne predstavlja resne grožnje). Medtem lahko sistemski administratorji še vedno zaznajo neuspešne poskuse prijave in prosijo določenega uporabnika, naj spremeni geslo, ali pa vse uporabnike, če je bil njihov sistem ogrožen in so uhajala vsa gesla.

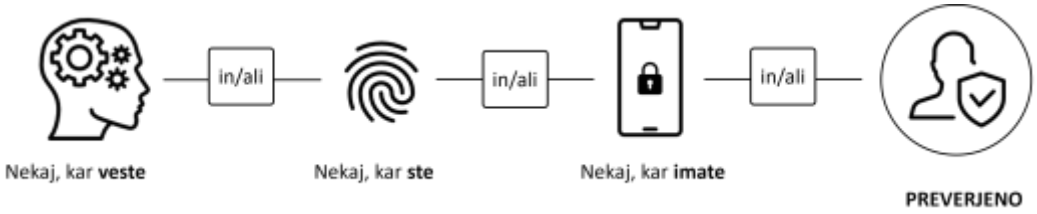


Fig. 7. Večfaktorska overjanje.

CHAPTER 3

Overjanje na podlagi gesla

Tehnika overjanja z geslom je najpogostejša in najlažja za uporabo. V številnih sistemih je običajno privzeto nastavljena. Gesla za večkratno uporabo, enkratna gesla (OTP), gesla z izzivom in odgovorom ter gesla s kombiniranim pristopom so primeri overjanja z geslom.

Gesla za večkratno uporabo

Pri overjanju z geslom za večkratno uporabo obstajata dve obliki overjanje: overjanje uporabnika in overjanje odjemalca.

- **Overjanje uporabnika** je najbolj razširjena vrsta overjanja in večina uporabnikov jo verjetno pozna. Vedno jo začne uporabnik, ki strežniku predloži zahtevo za overjanje in pooblastilo za dostop do določenega sistemskega vira. Ko strežnik prejme zahtevo, od uporabnika zahteva uporabniško ime in geslo. Strežnik ju ob predložitvi primerja s kopijama v svoji podatkovni zbirki. Avtorizacija se zagotovi na podlagi ujemanja.
- **Overjanje odjemalca.** Običajno uporabnik zahteva overjanje in nato dovoljenje za dostop do sistema ali niza sistemskih virov od strežnika. Overjanje uporabnikom ne omogoča dostopa do vseh želenih sistemskih virov. Z overjanje je treba določiti pooblastilo uporabnika za uporabo želenih virov v zahtevanem obsegu in ne več. Overjanje odjemalca je ime za to vrsto overjanje. Z njo se ugotovi identiteta uporabnikov in jim omogoči nadzorovan dostop do sistemskih virov.

Ker se ti načini overjanja najpogosteje uporabljajo, so tudi najpogosteje izkoriščani.

DISADVANTA

Poleg tega so tudi nezanesljive, ker jih ljudje pozabljajo, si jih zapisujejo, jih delijo, in kar je najbolj kritično, zlahka jih je uganiti, saj ljudje izbirajo preprosta gesla. Prav tako pa so ranljiva za nadzor in razbijanje. Poleg tega so šibka gesla (npr. , kratka, za preprosto strukturo) ranljiva za današnje super in močne računalnike, ki jih lahko z izčrpnim iskanjem zlomijo s surovo silo.

Enkratna gesla

Overjanje seje je drugo ime za enkratno overjanje z geslom. Za razliko od gesel za večkratno uporabo, ki se lahko uporabijo večkrat, se enkratna gesla uporabijo samo enkrat in se nato zavržejo.

ADVANTA

Uporabljajo se močni generatorji naključnih števil in se generirajo naključno. Tako se zmanjša verjetnost, da jih bo kdo uganil. V številnih okoliščinah so gesla pred pošiljanjem šifrirana, da se

zmanjša možnost njihovega prestrezanja.

Enkratna gesla so na voljo v različnih oblikah. Primeri vključujejo gesla SIKey in gesla z žetoni. SIKey je sistem za ustvarjanje enkratnih gesel, opredeljen v RFC 1760.

Drug primer je tako imenovana številka TAN, ki so jo v preteklosti uporabljali v Nemčiji (slika 8). Enkratna gesla so sicer običajno varnejša, vendar imajo številne pomanjkljivosti, med drugim težave s sinhronizacijo, ki nastanejo zaradi pretečenega časa med časovnim žigom v geslu in sistemsko uro. Gesla ni mogoče uporabiti, ko se ti dve časovni uri ne ujemata.

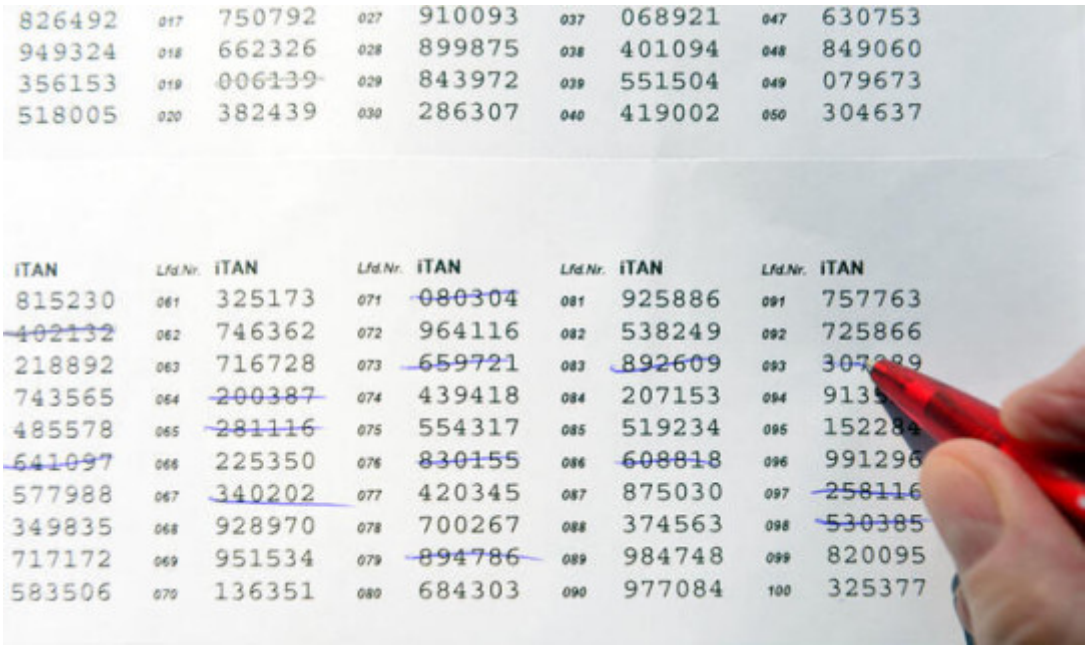


Fig. 8. Številke TAN so primer enkratnih gesel (OTP).

Nekatere vrste enkratnih gesel (npr. kode SMS in kode, ki jih generirajo aplikacije) se običajno uporabljajo kot drugi dejavnik pri uporabi 2FA.

Gesla z odgovorom na izziv

DEFINITION

Kot metoda overjanja, ki temelji na geslu, je postopek overjanja z izzivom in odgovorom postopek overjanja s tresenjem rok, pri katerem overitvena naprava izzove uporabnika, ki zahteva overjanje. Uporabnik mora za overjanje ponuditi pravilen odgovor.

Odvisno od sistema ima lahko izziv različne oblike. Lahko gre za osnovno zahtevo za geslo, številko, razčlenitev ali neujemanje. Posameznik, ki želi biti overjen, mora odgovoriti na izziv sistema. Danes se odgovori pošiljajo prek enosmerne funkcije in žetona z geslom, ki sta znana kot asinhrona žetona. Ko strežnik prejme uporabnikov odgovor, dvakrat preveri geslo.

Najpogostejša uporaba overjanja z izzivom in odgovorom je v porazdeljenih sistemih. Kljub svoji priljubljenosti se overjanje z izzivom in odgovorom sooča s težavami zaradi pomanjkljivosti, kot so vpletenost uporabnikov in napadi po načelu poskusi-napaka. Težava z vključevanjem uporabnikov je

v tem, da lahko uporabnik najde izziv na tipično razmetanih zaslonih. Uporabnik mora nato hitro vnesti odgovor.

Odvisno od zahtevane stopnje varnosti se lahko od uporabnika zahteva, da se spomni dolgega odgovora, ali pa ga mora zapisati, nato pa ga mora prepisati in vnesti. Pri tem lahko pride do napak.

INTERESTING

Nekateri proizvajalci so poskušali razbremeniti uporabnika pri pomnjenju in pisanju dolgih nizov z avtomatizacijo večine postopka, bodisi z izrezovanjem in pripenjanjem izziva in odgovorov bodisi z nizkim samodejnim postopkom, ki omejuje uporabnikov odziv na odgovore da/ne.

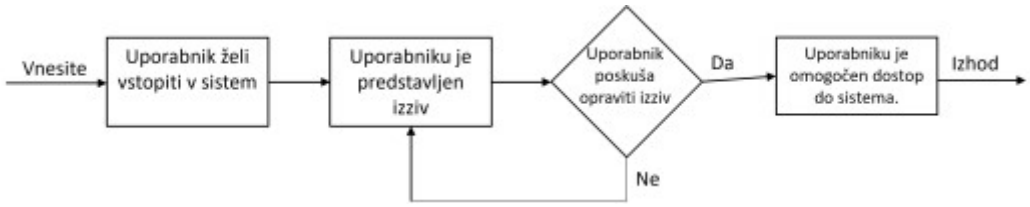


Fig. 9. Postopek overjanja v sistemu izziv-odgovor.

Prav tako je treba opozoriti, da je mogoče odzive na izzive, ki zahtevajo gesla, zlorabiti v njihovi najosnovnejši obliki, saj je gesla razmeroma enostavno pridobiti. Gesla je mogoče prestrezati, če so poslana v odprti obliki. Ker pa se geslo po omrežjih ne sporoča v odprtem besedilu, to ne predstavlja varnostnega vidika.

Interaktivní prvek

3.1 Težave z varnostjo gesel

V kibernetskih napadih so kršitve varnosti podatkov ena najpogostejših vrst napadov in ciljev napadalcev. Zato gesla kot mehanizem overjanja postajajo vse bolj problematična.

Edinstvenost gesla je ena od njegovih najpomembnejših značilnosti. Vendar so številna gesla vse prej kot to. Najbolj priljubljena gesla in fraze, ki jih uporabljajo ljudje po vsem svetu, so navedeni v preglednici 2.

Table 2. 10 najpogostejših gesel, vir: cybernews.com.

Gesla
123456
123456789
qwerty
geslo
12345
qwerty123
1q2w3e
12345678
111111
1234567890

DISADVANTA

Poleg tega se pojavljajo še druge težave v zvezi z gesli. Veliko ljudi se odloči, da bodo svoja spletna mesta povezali z nečim, kar si zlahka zapomnijo, da bi ustvarili preproste in zapomnljive kombinacije. Vendar to ne pomeni, da je geslo edinstveno, temveč ravno nasprotno.

V preiskavi Cybernews so pregledali približno 15 milijard vnosov in jih razvrstili v več kategorij in besednih zvez. Rezultati so pokazali, da so nekatere značilnosti gesel problematične - podatki, povezani z uporabnikom. Poleg tega so raziskovali dolžino gesel glede na število znakov, ki so jih vsebovala. Na žalost je večina uporabljenih gesel vsebovala 8 znakov ali manj.

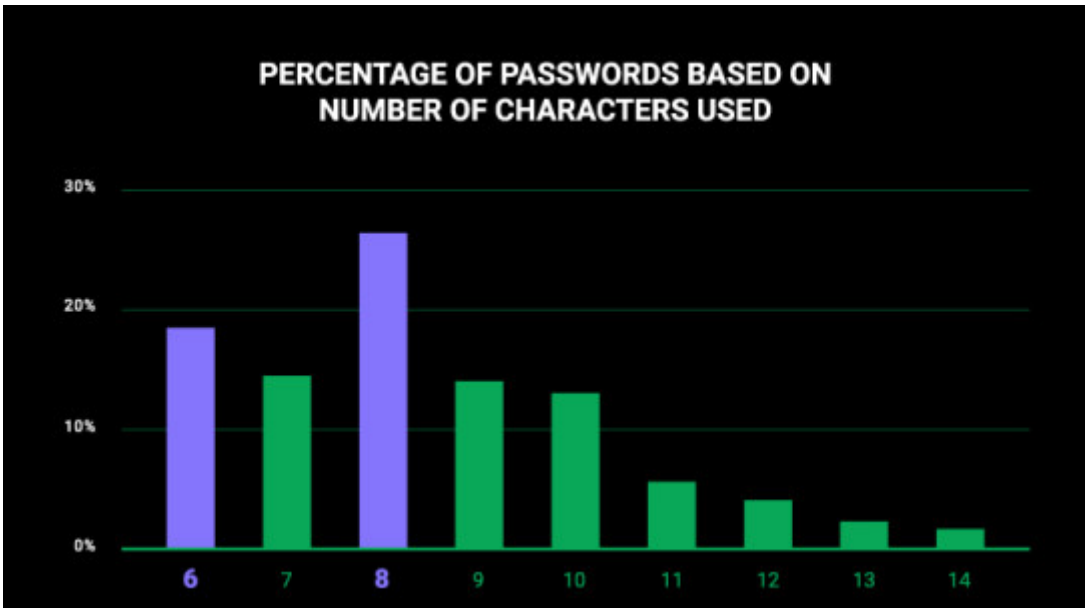


Fig. 10. Statistični podatki o dolžini gesel, vir: cybernews.com.

Obstajajo učinkovitejše metode za ustvarjanje močnega gesla. Če kot element gesla uporabimo "heat", je lahko na primer preprosto geslo "letsgoheat" (10 znakov), zahtevnejše geslo pa je lahko "heatromearsenalhjamesp" (geslo z 22 znaki). Ljudje varna gesla ustvarjajo tudi z mnemotehničnimi pripomočki, ki so primernejši, ker so pogosto dolgi in vsebujejo naključne besede brez logične povezave med njimi, zaradi česar si jih oseba lažje zapomni, algoritem pa jih težje razbije.

3.2 Napadi na gesla

Gesla je mogoče napasti na različne načine, na splošno pa lahko napade razvrstimo na naslednji način:

- Za neelektronske napade ni potrebno tehnično znanje za razbijanje gesla. Takšni napadi so na primer deskanje po ramenih, socialni inženiring in potapljanje v smetišču.
- Elektronski napadi zahtevajo tehnično znanje. Primeri takšnih napadov so napadi s slovarjem in napadi z grobo silo ter napadi z mavrično tabelo.

3.2.1 Neelektronski napadi

DEFINITION

Socialni inženiring je vrsta napada, pri katerem napadalec poskuša izkoristiti naravno nagnjenost ljudi, da zaupajo vsakomur. Z izkoriščanjem tega zaupanja napadalec hitro pridobi poverilnice žrtve in jih uporabi za poznejši dostop do njenega računa.

Phishing, Pharming in Whaling so le nekateri primeri. Upoštevajte, da je za nekatere od njih potrebno določeno tehnično znanje (npr. phishing).

Fig. 11. Potek phishing napada.

Pri napadu z brskanjem po ramenih napadalec stoji za vami in opazuje, kako vnašate poverilnice, ki jih nato uporabi za dostop do vašega računa.

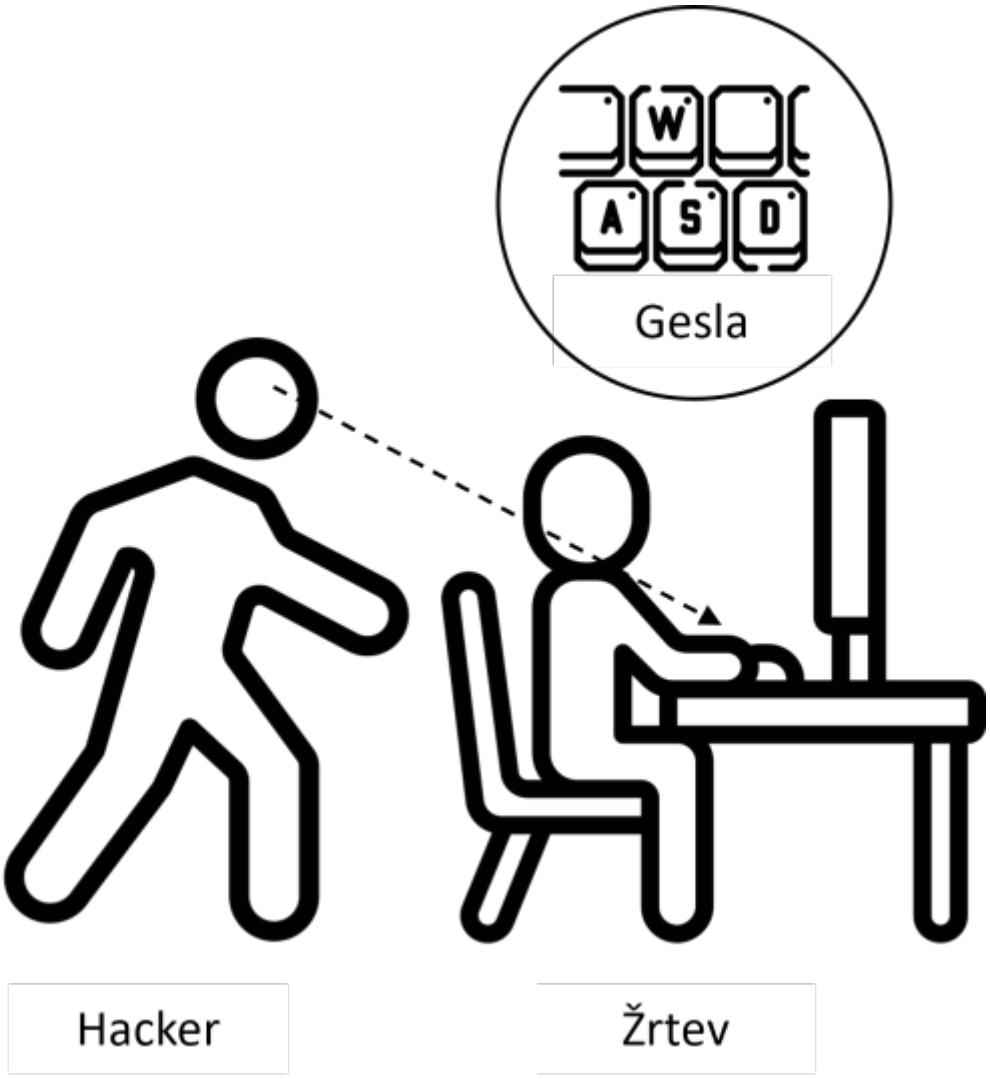


Fig. 12. Primer deskanja po ramenih.

Napadalec, ki se potaplja v smeti, v njih odkrije nekaj dragocenega, na primer geslo ali pin za kreditno kartico.

3.2.2 Elektronski napadi

DEFINITION

Napad s slovarjem je napad, pri katerem napadalec poskuša vstopiti v sistem, zaščiten z geslom, tako da vsako besedo iz slovarja uporabi kot geslo za ta sistem.

Pri tem je treba preizkusiti vse nize na vnaprej pripravljenem seznamu. V preteklosti so se v takih napadih uporabljale besede iz slovarja (od tod besedna zveza slovarski napad).

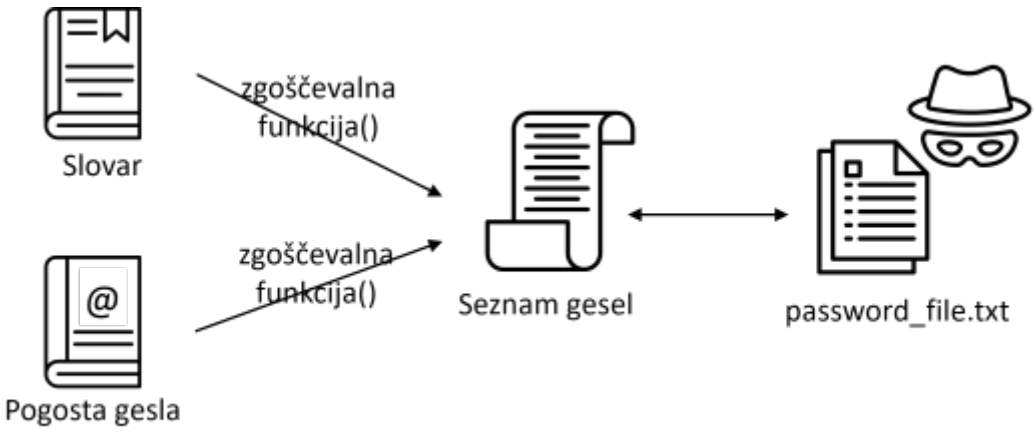


Fig. 13. Delovanje slovarskega napada.

DEFINITION

Pri slovarskem napadu se preizkušajo samo možnosti, za katere se domneva, da bodo najverjetneje uspešne.

Veliko ljudi je nagnjenih k izbiri kratkih gesel, ki so navadne besede ali običajna gesla ali različice, pridobljene na primer z dodajanjem številk ali ločil. Slovarski napadi so pogosto uspešni, ker je veliko ljudi nagnjenih k izbiri kratkih gesel, ki so navadne besede ali običajna gesla ali različice, pridobljene na primer z dodajanjem številke ali ločilnega znaka.

Ker razpoložljivi seznami zajemajo večino tipičnih strategij oblikovanja gesel, je slovarske napade težko premagati z generiranjem vzorcev v programski opremi za razbijanje. Varnejši način je uporaba orodja za upravljanje gesel ali ročne metode za naključno oblikovanje velikega gesla (15 črk ali več) ali gesla z več besedami.

Napadi z grobo silo

DEFINITION

Preprosto opisano je grobo izsiljevanje pristop k razbijanju gesel, pri katerem napadalec z uporabo nabora parametrov preizkusi čim več možnih kombinacij gesel.

Spletno mesto lahko na primer določi parameter, ki zahteva, da je geslo dolgo od 8 do 16 znakov. V najosnovnejši različici lahko helikopter začne z 00000000. Nato lahko poskuša z 00000001, 00000010, 00000100 in tako naprej, dokler ne izčrpa vseh možnih kombinacij znakov.

Za geslo dolžine 8 - Vsako polje je lahko:

- mala abeceda (26 možnosti)
- velika abeceda (26 možnosti)
- število (10 možnosti od 0 do 9)

- ločila ali druge posebne znake (33 možnosti).

Glede na vse to lahko izračunate končno število možnih gesel za geslo z 8 znaki: 3 025 989 069 143 040 ali približno 3 kvadrilijonov, pri čemer je vsak poskus ločen.

Morda mislite, da nekdo sestavi program, ki gre na spletno mesto, vnese vaše uporabniško ime in geslo, pritisne gumb za prijavo in poskuša uganiti vaše geslo. Nato postopek ponovi še trikrat kvadrilijonkrat. Vendar ni tako. Če spletna stran za nalaganje strani potrebuje 2 sekundi, sta to 2 sekundi čakanja za vsak poskus, da se prikaže stran "napačno geslo". Z drugimi besedami, če spletna stran ne zaklene prijave po določenem številu sumljivih poskusov, lahko traja do 9 kvadrilijonov sekund ali 287,9 milijona let. V resnici se takšen napad izvede z uporabo razkritih uporabniških imen in gesel. Ta so bila razkrita zaradi vdora v sistem (kar se dogaja pogosteje, kot si mislite). Geslo je torej mogoče razkriti na dva načina:

- Vaše geslo ni šifrirano in je shranjeno v obliki navadnega besedila v izjemno nezavarovanem okolju. Od bralca se zahteva le kopiranje in lepljenje gesla. Če je vaše geslo na primer geslo1, bi vsakdo, ki bi prebral vsebino kršitve podatkov, videl geslo1. V tem primeru je grobi preizkus nepotreben, saj je spletno mesto vaše podatke že predalo na srebrnem pladnju.
- Vaše geslo je v varnejšem okolju shranjeno v obliki gesla in ne v obliki prostega besedila. Če bi spletno mesto vaše geslo zgostilo s funkcijo SHA-256, bi bilo na primer geslo1 prikazano kot 0b14d501a594442a01c6859541bcb3e8164d183d32937b851835442f69d5c94e.

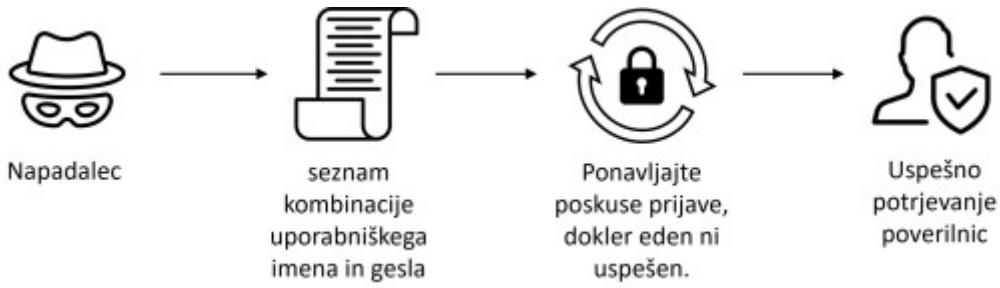
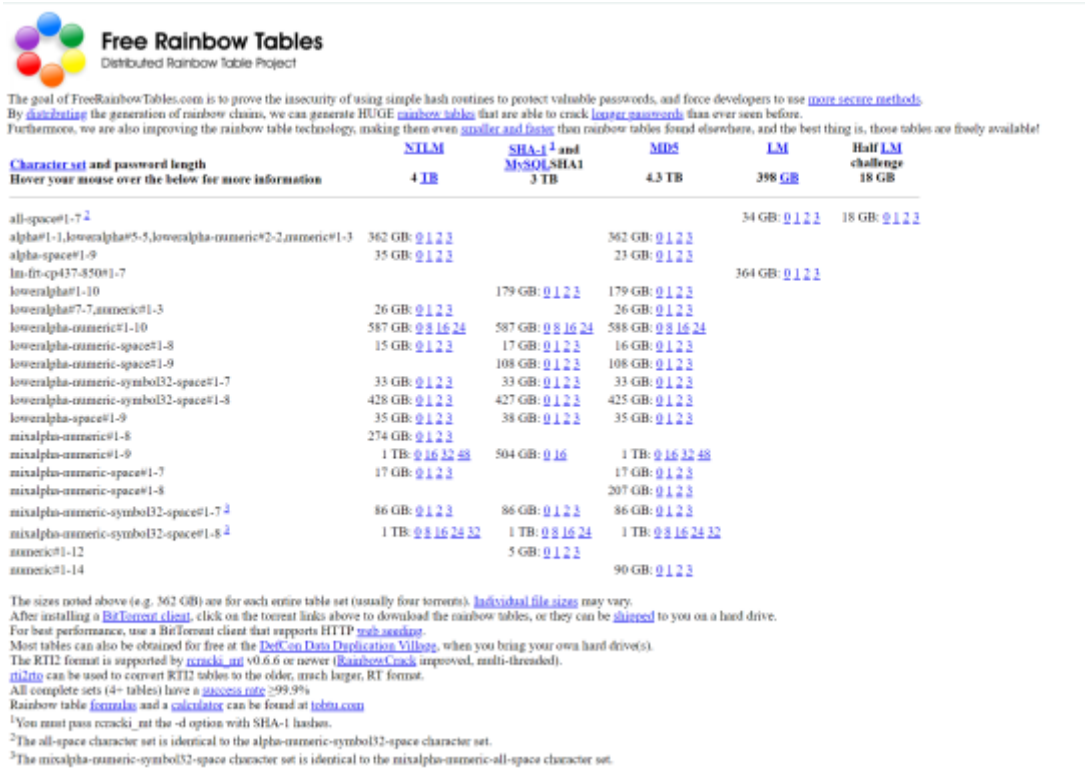


Fig. 14. Napad z grobo silo na gesla.

Mavrične tabele so posebna vrsta napada na gesla z grobo silo. Namenjen je razbijanju gesel, shranjenih v obliki izvlečka. Ker so mavrične tabele vnaprej izračunan seznam izvlečkov slovarskih izrazov ali predhodno razbitih gesel, ki so shranjeni v podatkovni zbirki, pri čemer je izvleček uporabljen kot ključ, gre za kompromis med časom in pomnilnikom. Ustvarjanje mavrične tabele lahko traja dolgo, vendar jo je treba ustvariti samo enkrat. Po končanem delu lahko poiščete izvlečke gesel in hitro dobite ustrezno geslo. Da bi si predstavljali velikost teh podatkovnih zbirk, lahko nekatere mavrične tabele dosegajo velikost 7-9 TB.



Free Rainbow Tables
Distributed Rainbow Table Project

The goal of FreeRainbowTables.com is to prove the insecurity of using simple hash routines to protect valuable passwords, and force developers to use more secure methods.
By distributing the generation of rainbow chains, we can generate HUGE rainbow tables that are able to crack longer passwords than ever seen before.
Furthermore, we are also improving the rainbow table technology, making them even smaller and faster than rainbow tables found elsewhere, and the best thing is, those tables are freely available!

Character set and password length Hover your mouse over the below for more information	NTLM 4 TB	SHA-1 [3] and MySQL SHA1 3 TB	MD5 4.3 TB	LM 398 GB	Half LM challenge 18 GB
all-space#1-7 [2]				34 GB: 0 1 2 3	18 GB: 0 1 2 3
alpha#1-1,loweralpha#5-5,loweralpha-numeric#2-2,numeric#1-3	362 GB: 0 1 2 3		362 GB: 0 1 2 3		
alpha-space#1-9	35 GB: 0 1 2 3		23 GB: 0 1 2 3		
lm-frt-cp437-850#1-7				364 GB: 0 1 2 3	
loweralpha#1-10		179 GB: 0 1 2 3	179 GB: 0 1 2 3		
loweralpha#7-7,numeric#1-3	26 GB: 0 1 2 3		26 GB: 0 1 2 3		
loweralpha-numeric#1-10	587 GB: 0 8 16 24	587 GB: 0 8 16 24	588 GB: 0 8 16 24		
loweralpha-numeric-space#1-8	15 GB: 0 1 2 3	17 GB: 0 1 2 3	16 GB: 0 1 2 3		
loweralpha-numeric-space#1-9		108 GB: 0 1 2 3	108 GB: 0 1 2 3		
loweralpha-numeric-symbol32-space#1-7	33 GB: 0 1 2 3	33 GB: 0 1 2 3	33 GB: 0 1 2 3		
loweralpha-numeric-symbol32-space#1-8	428 GB: 0 1 2 3	427 GB: 0 1 2 3	425 GB: 0 1 2 3		
loweralpha-space#1-9	35 GB: 0 1 2 3	38 GB: 0 1 2 3	35 GB: 0 1 2 3		
mixalpha-numeric#1-8	274 GB: 0 1 2 3				
mixalpha-numeric#1-9	1 TB: 0 16 32 48	504 GB: 0 16	1 TB: 0 16 32 48		
mixalpha-numeric-space#1-7	17 GB: 0 1 2 3		17 GB: 0 1 2 3		
mixalpha-numeric-space#1-8			207 GB: 0 1 2 3		
mixalpha-numeric-symbol32-space#1-7 [3]	86 GB: 0 1 2 3	86 GB: 0 1 2 3	86 GB: 0 1 2 3		
mixalpha-numeric-symbol32-space#1-8 [3]	1 TB: 0 8 16 24 32	1 TB: 0 8 16 24	1 TB: 0 8 16 24 32		
numeric#1-12		5 GB: 0 1 2 3			
numeric#1-14			90 GB: 0 1 2 3		

The sizes noted above (e.g. 362 GB) are for each entire table set (usually four torrents). Individual file sizes may vary.
After installing a BitTorrent client, click on the torrent links above to download the rainbow tables, or they can be shipped to you on a hard drive.
For best performance, use a BitTorrent client that supports HTTP web seeding.
Most tables can also be obtained for free at the DefCon Data Duplication Village, when you bring your own hard drive(s).
The RTI2 format is supported by rcracki_mt v0.6.6 or newer (RainbowCrack improved, multi-threaded).
rti2rto can be used to convert RTI2 tables to the older, much larger, RT format.
All complete sets (4+ tables) have a success rate ≥99.9%
Rainbow table formulas and a calculator can be found at tobtu.com
[1]You must pass rcracki_mt the -d option with SHA-1 hashes.
[2]The all-space character set is identical to the alpha-numeric-symbol32-space character set.
[3]The mixalpha-numeric-symbol32-space character set is identical to the mixalpha-numeric-all-space character set.

Fig. 15. Velikosti mavričnih tabel s spletne strani freerainbowtables.com.

Interaktivni prvek

Interaktivni prvek

3.2.3 Orodja za napade na gesla

Orodja za vdiranje v gesla so v teh dneh vse bolj priljubljena, zato bomo pregledali več teh orodij. Orodja za razbijanje gesel se večinoma uporabljajo za preizkušanje moči gesla ali izvedbo sovražnega napada. Na voljo so številna spletna orodja in orodja brez povezave, ki so namenjena samo razbijanju gesel. Cilj spletnih napadov so vmesniki za oddaljeno prijavo, kot so storitve SSH in RDP. Po drugi strani pa se napadi brez povezave pojavijo po tem, ko so bile datoteke odtujene. Takoj zatem so cilj gesla.

Nekatera orodja, ki so na voljo, so Hashcat, John the Ripper ali Thc Hydra.

Hashcat je medplatformni program za obnovitev gesel, ki deluje tako z grafičnim kot s centralnim procesorjem. Program Hashcat je leta 2009 ustvarila univerza MIT, priznan pa je po tem, da podpira številne zgoščevalne algoritme, kot so "LM Hash, NT Hash, MD4, MDS in številni drugi". Ko je bil ta program prvič razvit, je podpiral štiri različne vrste napadov.

- Slovarski napadi: več kot 14 milijonov gesel, začenši z najbolj priljubljenimi in končajo z najmanj pogostimi. Uganil bo geslo, ga zgostil in ga primerjal z geslom, ki ga želi razvozlati.

- Kombinatorni napadi: podobni napadom na slovarje, vendar namesto da bi kot "slovarje" uporabljali sezname dveh besed, ustvarijo nov seznam besed, na katerem je vsaka beseda združena z vsako drugo besedo.
- Če na primer veste, da je geslo vašega računa dolgo 9 znakov in se konča s številko, veste, da bo za uganko gesla potrebna kombinacija 52+109, kar bo trajalo približno 4 leta. Če pa veste, da se geslo začne z veliko črko in konča s številko, se bo čas skrajšal za polovico.
- Napad na podlagi pravil: program hashcat lahko določi, katero geslo naj poskusi glede na to, kako žrtev ustvari geslo.
- Napad z grobo silo: poskuša vse, dokler ne najde nečesa, "kar običajno traja dolgo, saj poskuša vse možne kombinacije."

Splošna javna licenca GNU **John the Ripper** je leta 1996 objavljeno odprtokodno orodje za varnost gesel, revizijo in obnovitev, ki podpira na stotine vrst zgoščevalnih algoritmov in šifer. Na voljo je na različnih platformah, kar omogoča uporabo istega razbijača na kateri koli od njih. Kot je bilo že navedeno, to orodje podpira različne vrste zgoščevalnih algoritmov.

Pri izvajanju na različnih platformah se lahko te vrste zgoščevalnih algoritmov razlikujejo. To orodje ima veliko načinov razbijanja, med drugim:

- Način besednega seznama: V tem načinu določite besedilno "besedilno datoteko", ki jo je najbolje urediti, geslo pa se primerja z geslom, ki ga poskušate razbiti.
- Enotna razpoka: To je prvi način, s katerim lahko začnete razbijati. Uspešno geslo se namreč primerja z vsemi naloženimi gesli, da se preveri, ali ima kateri od uporabnikov enako geslo, kar pospeši postopek.
- Postopni način: najmočnejši način lomljenja, ki preizkusi vse možne kombinacije, vendar se zaradi velikega števila možnih kombinacij ne ustavi.
- Zunanji način: to so funkcije, napisane v jeziku C, ki jih orodje sestavi ob zagonu in vsebujejo program, ki ga bo uporabilo za ustvarjanje gesla.

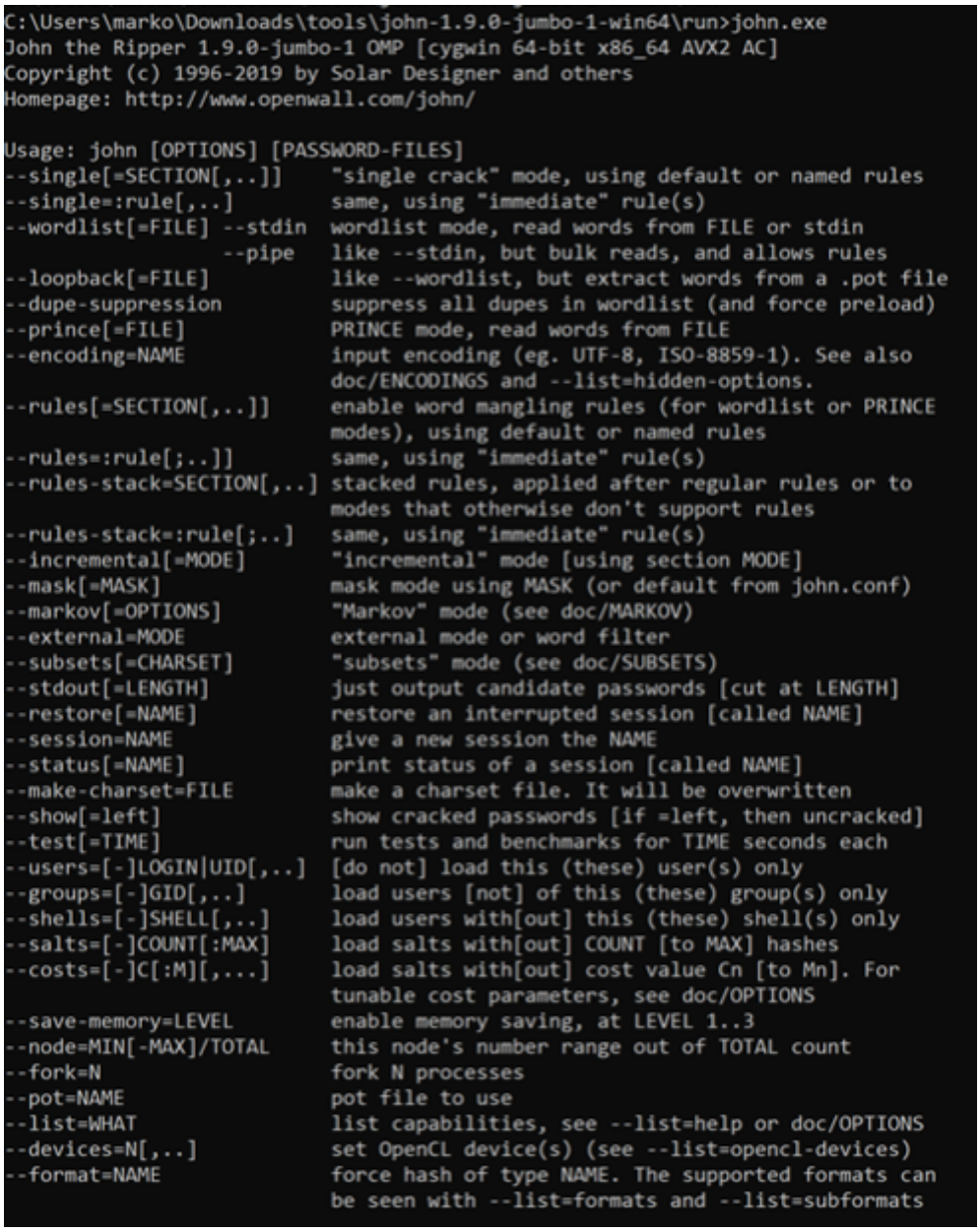


Fig. 16. John Razparač v akciji.

THC hydra, ki ga je leta 2001 zasnoval Van Hauser, je spletni program za razbijanje, ki prikazuje, kako preprosto je pridobiti nepooblaščen dostop do oddaljenega računalnika. Ta program podpira različne protokole, vključno s "FTP, HTTP, HTTPS, MySQL, Postgress ...", in različne platforme, vključno z UNIX, MacOS, Windows in mobilnimi napravami. To orodje lahko izvede vzporedni slovarski napad, napad z grobo silo ali hibridni napad, vzporedni napad na več strežnikov in še več. THC Hydra je prepoznavna po tem, da je hitra in učinkovita, vendar je to odvisno od protokola.

Glavna razlika med tem orodjem in orodjem John the Ripper je, da je to orodje spletno orodje za razbijanje gesel, medtem ko je John the Ripper orodje brez povezave.

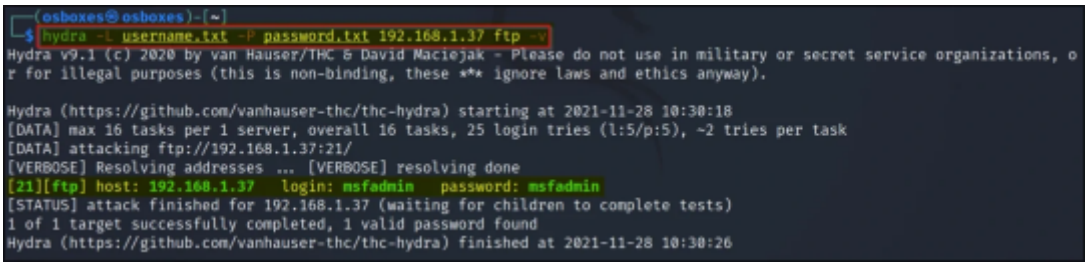


Fig. 17. THC Hydra v akciji.

Interaktivní prvek

CHAPTER 4

Različni vidiki varnosti gesel

V tem poglavju bomo obravnavali različne vidike varnosti gesel, ki jih lahko razdelimo na:

- V uporabnika usmerjen
- Osrednji strežnik.

Ti vidiki vključujejo smernice za varnostna gesla, dvofaktorsko overjanje, ustrezno shranjevanje gesel na strani strežnika itd.

4.1 Smernice in dobre prakse za varna gesla

Gesla so prevladujoča metoda overjanja, saj jih razvijalci najlažje implementirajo, uporabniki pa razumejo in uporabljajo. Vendar so z uporabo gesel povezane nekatere konceptualne slabosti (npr. slabo izbrana, zlahka uganljiva itd.). Ameriški nacionalni inštitut za standarde in tehnologijo (NIST) redno posodablja svoja priporočila za ustvarjanje in upravljanje gesel. V enem od nedavnih premikov v paradigmi varnosti gesel je predlagal, naj se uporabniki osredotočijo na dolžino gesla namesto na kompleksnost (kombinacije posebnih znakov, številk, malih ali velikih črk), saj si je kompleksna gesla težko zapomniti. Posledično se uporabniki nagibajo k temu, da kompleksnost dosežejo na predvidljive načine (npr. z dodajanjem številke 1 na koncu gesla). Eden od načinov doseganja dolžine je z nesmiselnimi gesli, pri katerih so besede v zaporedju, ki nima nobenega pomena. Iz istega razloga NIST ne priporoča več strogih pravil za sestavo znakov pri ustvarjanju gesla. Priporočajo pa redno primerjanje gesel (ali vsaj vseh novih gesel) s seznamom kompromitiranih gesel, da bi prepoznali že razkrita in šibka gesla. Kljub temu je priporočena najmanjša dolžina gesla 12 znakov. V preteklosti je bilo priporočeno redno menjavanje gesel, vendar to ne velja več, saj je zaradi tega manj verjetno, da si bodo uporabniki po spremembi gesla zapomnili in namesto tega začeli uporabljati ista gesla z majhnimi spremembami.

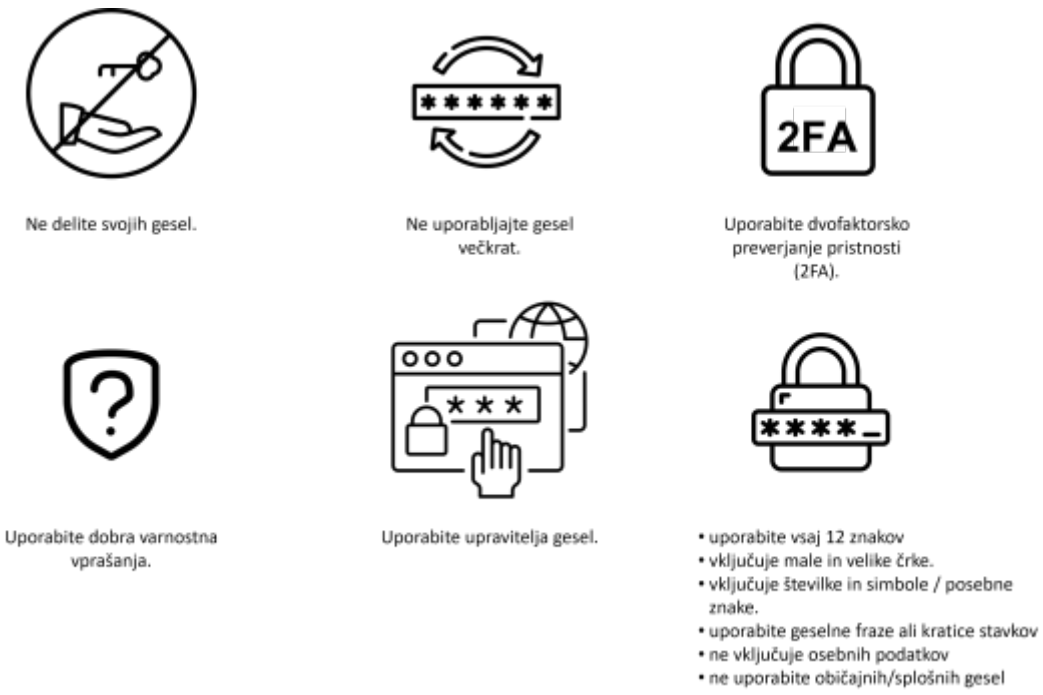


Fig. 18. Najboljše prakse za uporabo gesel.

Za varno geslo, ki ga ustvarite sami, je treba upoštevati naslednje zahteve:

- uporabite vsaj 12 znakov
- vključujejo male in velike črke.
- vključuje številke in simbole / posebne znake.

- uporabljati gesla ali kratice stavkov.
- ne vključujejo osebnih podatkov.
- ne uporabljajte običajnih/splošnih gesel.

Ne pozabite, da geslo NE sme vsebovati osebnih podatkov, kot so datum rojstva, ime hišnega ljubljenčka, vaše ime ali e-poštni naslov.

Čeprav lahko s tehničnimi ukrepi zagotovite, da uporabniki izberejo močna gesla, je nemogoče nadzorovati, kaj uporabniki počnejo s temi gesli. Lahko jih zapišejo na papir ob računalniku, jih delijo z drugimi ljudmi ali jih uporabijo za druge račune. Slednje je še posebej nevarno, saj uporaba istega gesla za več računov ogrozi vse račune, če pride do vdora v katero od storitev, ki uporabljajo ista gesla. To pomeni, da če uporabljate isto geslo za dostop do knjižnice in e-poštnega računa ter nekdo vdre v varnost knjižnice (kar bi moralo biti veliko lažje kot v strežnike velikega ponudnika e-poštnih storitev - npr. Googla) in ukrade geslo, lahko te podatke uporabi za dostop do vašega e-poštnega računa. Izobraževanje uporabnikov je edina prava rešitev za preprečevanje takšnih slabih praks. Zato je treba uporabnike poučiti (o tem, kako) ustvariti močna gesla, jih ne zapisovati kamor koli, kjer so dostopna, in nikoli ponovno uporabiti istega gesla.

Obstajajo tudi druge dobre prakse za zaščito gesel na strani uporabnika:

- Uporaba različnih gesel za različne scenarije
- Uporaba gesla
- Uporaba upravitelja gesel
- Uporabite dvofaktorsko overjanje (2FA)

Čeprav se zdi nedolžno, je uporaba istega gesla na več spletnih mestih nevarna. Vdori v osebne podatke na potrošniških spletnih mestih so vse bolj razširjeni. Če so vaši podatki ukradeni s spletnega mesta družabnih omrežij, vi pa isto geslo uporabljate v aplikaciji za spletno bančništvo in na nekaj spletnih mestih za spletno nakupovanje, bo napadalec dobil prost dostop do vseh teh spletnih mest. Obstajajo aplikacije in programska oprema, ki vas lahko dejansko opozorijo, da so bila vaša gesla del kršitve varnosti podatkov. Če so vaši podatki pricurljali v javnost, vas lahko na primer na to opozori Googlov upravitelj gesel.

Interaktivní prvek

Naslednja dobra praksa je uporaba več kot ene besede. Geslo je zaporedje besed, ki je videti kot stavek, vendar ne sme imeti nobenega pomena. Geslo ne sme vsebovati osebnih podatkov, ki jih je mogoče zlahka pridobiti, prav tako kot geslo ne sme vsebovati osebnih podatkov, ki jih je mogoče zlahka pridobiti. Uporabite lahko celo generatorje za ustvarjanje naključnega niza besed uporabnik.

Interaktivní prvek

S pomočjo različnih spletnih storitev lahko preverite, ali je bilo vaše geslo kršeno. Ena najbolj znanih tovrstnih storitev je spletna stran haveibeenpwned.com. Vendar obstajo tudi druge spletne storitve, kot je ta.

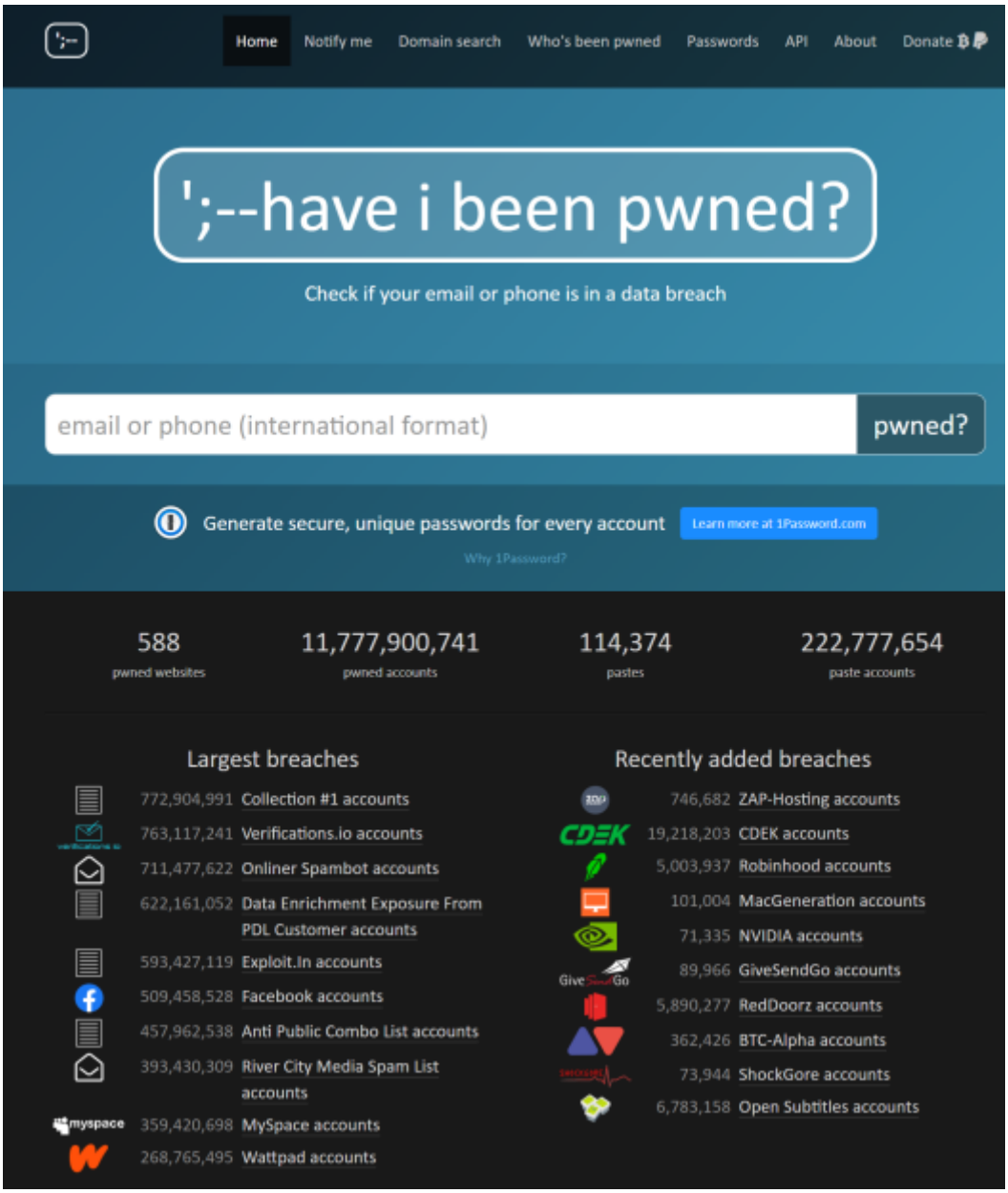


Fig. 19. "';--have I been pwned? " spletne storitve.

4.2 Upravljavci gesel

Poleg dvostopenjskega overjanja je dober način za zagotavljanje varnosti gesel tudi uporaba upravitelja gesel. Ta možnost deluje skoraj univerzalno, izboljša varnost vaših gesel in naredi postopek prijave bolj kot ne priročen.

Dobri upravitelji gesel pa vaše podatke temeljito šifrirajo. Tudi če napadalec dobi dostop do podatkovne datoteke, jo mora najprej dešifrirati, preden pridobi uporabne informacije. V večini okoliščin je to izredno težko in se ne splača truditi. V primerjavi z drugo možnostjo redna uporaba upravitelja gesel zagotavlja, da imate vedno na voljo seznam računov, ki ga lahko po potrebi posodobite.

Napadalce odvrača, če podatke shranjujejo lokalno in ne v oblaku. Pridobivanje podatkov ene osebe ali družine zahteva veliko truda. Z dobrimi upravitelji gesel lahko izberete, kje so shranjeni vaši podatki o geslih.

Veliko ljudi ima sisteme, ki si običajno delijo skupne stvari, tako kot skupna gesla. Te taktike napadalci dobro poznajo. To znanje je bilo vgrajeno v algoritme za razbijanje, zato so lahko sistemi bolj škodljivi kot koristni. Zaradi argumentacije si predstavljajmo, da je vaš sistem odličen. Kljub temu še vedno obstaja tveganje. Z dodatnimi kršitvami, ki razkrivajo vaše geslo, se povečuje verjetnost, da bo vaš sistem vdrt. Ko je vaš sistem enkrat vdrt, ga lahko napadalec uporabi za ugibanje vaših prijavnih podatkov na drugih spletnih mestih. Uporaba vašega sistema namesto upravitelja gesel je dejansko počasnejša.

Dolge gesla so pogosto primernejša od gesel. Vendar jih številna spletna mesta ne podpirajo (omejitve znakov in dolžine). Poleg tega si jih je sicer lažje zapomniti kot gesla, vendar ne rešujejo vprašanja, da ljudje uporabljajo isto geslo na različnih spletnih mestih ali se zanašajo na sistem.

Vendar je kot glavno geslo za upravitelja gesel, ki je ključ za odklepanje vseh podatkov o geslih, priporočljivo uporabiti geslo. Tako lahko zlahka izberete in si zapomnite izjemno dolgo glavno geslo.

Če razmišljate o shranjevanju gesel v brskalniku, obstaja več razlogov, zakaj je ta rešitev slaba. Brskalniki varnosti gesel ne jemljejo tako resno, kot bi jo morali, saj za dostop ne zahtevajo glavnega gesla. Vse, kar morate storiti, je, da ste prijavljeni v računalnik. Pri uporabi računalnikov, ki niso vaši, je ta metoda neprijetna. Gesla za brskalnike so učinkovita le znotraj brskalnika. To dandanes ni primerna možnost, saj se geslo pogosto zahteva tako za spletne kot mobilne aplikacije.

Upravljavci gesel omogočajo shranjevanje več kot le preprostih gesel, kar je zelo koristno. Upravitelja gesel lahko uporabite za shranjevanje in dopolnjevanje poverilnic, kot so kreditne kartice, kar lahko storite tudi v brskalnikih. V upravljalniku gesel lahko hranite tudi druge občutljive podatke, kot so licence, identitete, številke bančnih računov in druge informacije.

Upravljavec gesel naj bo digitalni trezor, ki ga lahko nosite s seboj.

ADVANTA

Poleg tega upravitelji gesel ponujajo tudi druge prednosti, povezane z uporabnostjo:

- Vključen je v področja, kjer morate uporabljati gesla, ter omogoča hitro in preprosto ustvarjanje, posodabljanje in izpolnjevanje gesel.
- Združljiv je s številnimi platformami, gesla pa so sinhronizirana.
- Odlično se obnese v najrazličnejših okoliščinah in izvedbah ter je običajno dobro vzdrževan.
- Varnost jemlje resno in si prizadeva (močno šifriranje od konca do konca), da bi zagotovil varnost podatkov tudi v primeru kršitve.

Da bi bil upravitelj gesel učinkovit, si morate zapomniti nekaj ključnih točk:

- Uporabljajte ga na vseh svojih spletnih mestih. Povsod. Izjeme samo povečajo ranljivost in zapletenost sistema (verjetnost uspeha je manjša).
- Za vsako spletno mesto ustvarite edinstveno geslo. Če imate možnost, naj bo čim daljše. Uporabite najmanj 20-30 znakov. Težje je razbiti geslo, daljše je (pravzaprav eksponentno težje). Ker jih bo upravitelj gesel večino časa izpolnil namesto vas, vam jih ne bo treba vnašati.
- Vsako spletno mesto ne podpira vseh upraviteljev gesel, zato je treba gesla občasno kopirati v odložišče, preden jih prilepite v prijavni obrazec. To ni preveč varno, saj lahko na različne načine razkrije vaše geslo. Večina upraviteljev gesel bo po kratkem času samodejno odstranila podatke o geslu iz odložišča
- Nekatere storitve še vedno postavljajo nesmiselne zahteve glede gesel, na primer, da morajo biti gesla dolga vsaj 12 znakov. Tu pridejo prav upravitelji gesel, saj takšna gesla generirajo naključno, kar je približno tako varno, kot je glede na omejitve mogoče.
- Glavno geslo naj bo čim daljše in uporabite geslo, ki ga je težko uganiti. Prav tako je dobro, da glavno geslo redno spreminjate, da zmanjšate nevarnost, da bi prišlo do kompromitiranja le-tega.
- Če želite izmenjati gesla, naj druga oseba ustvari svoj trezor in ji s funkcijo deljenja v upravljalniku gesel omogočite deljenje posameznih gesel.

Med priljubljenimi upravitelji gesel so:

- LastPass
- Dashlane
- LogMeOnce
- 1Password
- Keeper
- KeePass

Nekatere so na voljo brezplačno, za nekatere je treba plačati. Nekateri so brezplačni, vendar morate za napredne funkcije plačati.

Interaktivní prvek

4.3 Overjanje z dvema dejavnikoma (2FA)

DEFINITION

2FA je dodatna raven zaščite, ki preverja, ali je vsakdo, ki poskuša dostopati do spletnega računa, tisti, za katerega se izdaja.

Uporabnik mora najprej navesti svoje uporabniško ime in geslo. Nato bo moral predložiti še en podatek, preden bo lahko dobil dostop.

Dober primer dvostopenjskega overjanje je dvig denarja na bankomatu. Transakcijo je mogoče opraviti le s pravilno kombinacijo bančne kartice (nekaj, kar imate) in kode PIN (osebna identifikacijska številka, nekaj, kar poznate).

Večina spletnih mest ponuja možnost preverjanja prek SMS-sporočil. Vendar pa mobilne naprave pridobivajo na veljavi za 2FA.

ADVANTA

Prednosti so očitne:

- Ker uporablja mobilne naprave, ki jih (običajno) ves čas nosite s seboj, ne potrebuje dodatnih žetonov.
- Dinamično generirane gesla so varnejša kot fiksni (statični) prijavni podatki, saj se stalno spreminjajo.

DISADVANTA

Obstajajo pa tudi slabosti:

- Neprijetnost - kadar koli je potrebna overjanje, morajo imeti uporabniki napolnjen mobilni telefon in biti v dosegu mobilnega omrežja. Dostop je pogosto nemogoč brez rezervnih načrtov, če telefon ne more prikazati sporočil, na primer če je poškodovan ali se izklopi zaradi posodobitve ali zaradi ekstremnih temperatur (npr. izpostavljenost pozimi). Možno je, da besedilna sporočila ne bodo prispela takoj, kar bo povzročilo dodatne zamude v postopku overjanja zaradi kopiranja ali ročnega vnosa.

Upoštevajte, da sporočila SMS niso tako varna, kot morda pričakujete. Prenos besedil SMS na mobilne telefone je nezanesljiv in izpostavljen prestrezanju. Zato lahko tretje osebe ukradejo in uporabijo žeton. Pri obnovi računa se 2FA z mobilnim telefonom pogosto zaobide. Sodobni pametni telefoni se uporabljajo za preverjanje elektronske pošte in prejemanje besedilnih sporočil. V večini primerov je elektronska pošta vedno prijavljena. Ker lahko telefon prejme drugi dejavnik, je v primeru izgube ali kraje telefona mogoče vdreti v vse račune, za katere je e-pošta ključ. Zaradi tega pametni telefoni združujejo obe merili v eno. Če je uporabniku ukraden telefon, lahko kriminalec pridobi dostop do uporabnikovih računov. Hekerji lahko dostop do omrežij mobilnih telefonov pridobijo s kloniranjem

kartic SIM. Če naprava ne podpira sporočil SMS, je dvostopenjska overjanje z glasovnim klicem izvedljiva možnost za praktično vse ostale.

Mobilna aplikacija Authy

Recimo, da imate pametni telefon ali drugo mobilno napravo. V tem primeru lahko kodo dvostopenjskega overjanja pridobite brez uporabe sporočil SMS ali glasovnih klicev, tako da prenesete in namestite eno od številnih priljubljenih aplikacij za dvostopenjsko overjanje neposredno v svojo napravo. To je veliko varnejši način prijave z uporabo dvostopenjskega overjanje. Aplikacije, kot sta Authy in Google Authenticator, ustvarijo kodo TOTP (Time-based One-Time Passcode) neposredno v aplikaciji.

ADVANTA

Tudi če bi napadalcu uspelo prepričati vašega ponudnika mobilnih storitev, da zamenja kartico SIM, še vedno ne bi mogel dostopati do vaših kod za overjanje. Informacije, potrebne za izdelavo teh kod, so shranjene v vaši dejanski napravi in ne na kartici SIM.

Zdaj, ko ste v telefon namestili Authy, boste želeli nastaviti prve račune 2FA. To storite tako, da z aplikacijo optično preberete kodo QR (ki jo posreduje spletno mesto, na katerem želite zavarovati račun). Ko boste zajeli začetno kodo in zaščitili prvi račun, boste verjetno začeli ščititi druge račune.

Fig. 20. Skeniranje kode QR v mobilni aplikaciji Authy.

Zdaj se morate odločiti, ali boste vse žetone 2FA hranili v eni napravi ali jih varnostno kopirali v oblak.

DISADVANTA

Če se odločite za prvo možnost, nato pa napravo izgubite, nadgradite ali vam jo ukradejo, boste morali vse storitve, v katerih ste aktivirali funkcijo 2FA, prepričati, da jo izklopijo. Ko boste zamenjali telefon, se boste morali nato vrniti v svoj račun in ročno ponovno omogočiti 2FA v vsaki storitvi.

ADVANTA

Zato Authy omogoča varnostno kopiranje žetonov 2FA v našo varno shrambo v oblaku, do katere lahko dostopate samo vi, tako da lahko vedno obnovite svoje račune, če izgubite, ukradete ali

zamenjate zastarelo napravo.

Pri varnostni kopiji žetonov 2FA v oblak vas prosimo, da nastavite geslo za varnostno kopijo, to geslo pa uporabimo za šifriranje vaših podatkov in jih nato sinhroniziramo z našo storitvijo v oblaku. Vaši podatki so v naši platformi v oblaku izjemno varni, saj vašega gesla nikoli fizično ne shranimo - vendar je ključnega pomena, da si ga zapomnite.

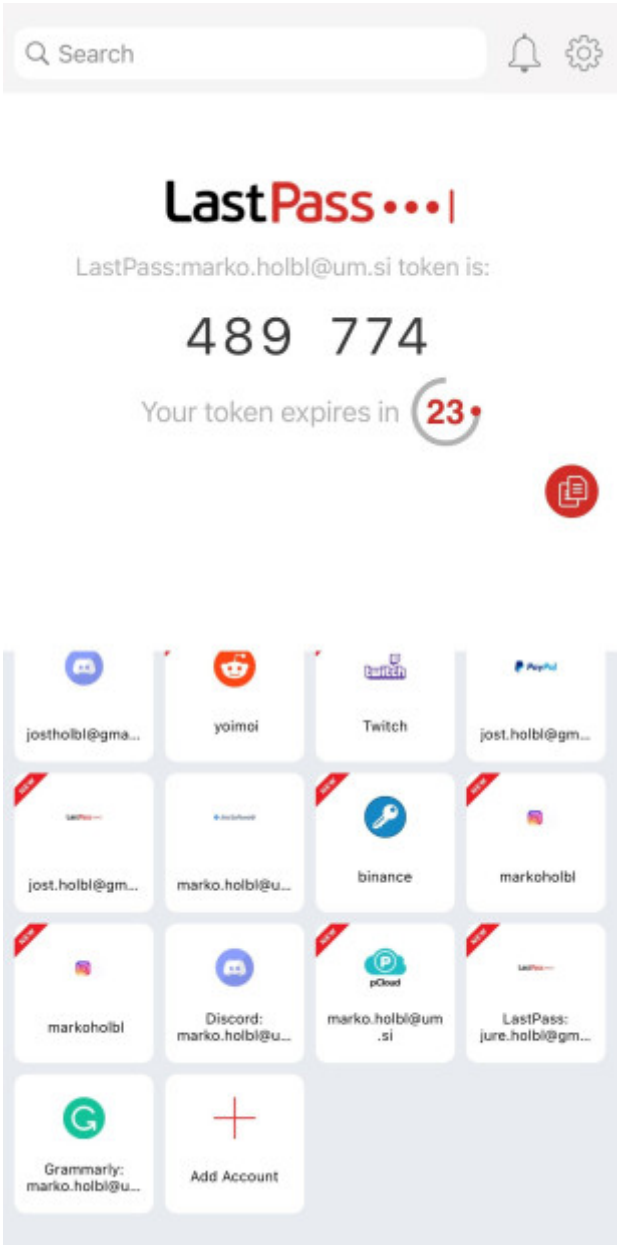


Fig. 21. Uporaba mobilne aplikacije Authy.

Nato je priporočljivo, da Authy namestite v drugo napravo. Aplikacija bo samodejno sinhronizirala žetone v vsako napravo, v kateri imate nameščen Authy, če ste jih sinhronizirali z oblakom Authy. Če imate samo eno mobilno napravo, lahko prenesete tudi aplikacijo Authy Desktop, ki je neodvisna od brskalnika.

Interaktivní prvek

4.4 Vidiki varnega shranjevanja gesel (na strani strežnika)

Gesla morajo biti ustrezno zaščitena na strani overitelja (običajno strežnika). Vsak dan se poroča o številnih kršitvah varnosti podatkov, zato se ne moremo zanašati na varnost sistemov overitelja. Zato gesel ni mogoče hraniti v obliki navadnega besedila in jih je treba hraniti na zaščiten način. Vendar bomo najprej na kratko predstavili nekaj konceptov, ki so potrebni za razumevanje varnega shranjevanja gesel.

4.4.1 Shranjevanje zgoščenih gesel

DEFINITION

Kriptografska zgoščevalna funkcija sprejme vhod (ali sporočilo) in vrne alfanumerični niz fiksne dolžine.

Niz je znan kot izvleček.

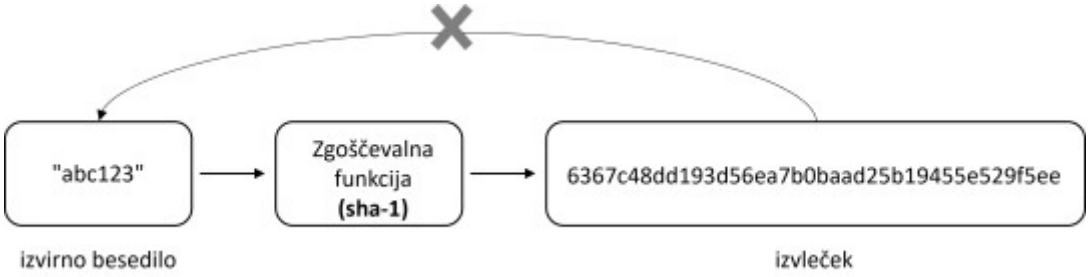


Fig. 22. Kako deluje zgoščevanje.

Slika 22 prikazuje postopek zgoščevanja. Začnemo z besedo "abc123" in uporabimo zgoščevalno funkcijo SHA-1, da dobimo alfanumerični rezultat fiksne velikosti, ki ga imenujemo izvleček. S pomočjo izvlečka ne moramo obnoviti prvotnega vhodnega besedila. Izvleček ne moremo obrniti, da bi našli izvirno vsebino, saj so zgoščevalne funkcije enosmerne in zato nepovratne. Če isto gradivo pošljemo skozi isto funkcijo zgoščevalno funkcijo, mora biti izhodni/naslovni rezultat enak. Zato lahko namesto shranjevanja gesla v izvornem besedilu uporabimo zgoščevalno vrednost in shranimo izvleček.

upor_ime	geslo
John	abc123
sam	abc123
Alice	xyz456

→

upor_ime	Zgoščeno geslo
John	6367c48dd193d56ea7b0baad25b19455e529f5ee
sam	6367c48dd193d56ea7b0baad25b19455e529f5ee
Alice	0772dbe339a885eb2ed73c1fe842d2ef6e9003a3

Fig. 23. Zaščita shranjenih gesel z uporabo zgoščevalne funkcije.

Ko se uporabnik poskuša prijaviti v sistem, uporabimo zgoščevalno funkcijo izračun izvlečka uporabnikovega gesla in jo primerjamo s shranjenim izvlečkom. Uporabniku lahko dovolimo prijavo v sistem, če sta obe vrednosti enaki. Na sliki 23 imata John in Sam enako geslo "abc123", njuna izvlečka

sta po uporabi zgoščevalnega algoritma enaka. Razmislite o primeru, ko ima john dostop do podatkovne zbirke in lahko vidi izvleček gesla. Takrat lahko john vidi, da je njegov izvleček gesla enak izvlečku Samovega gesla. Zato bo lahko john uporabil Samove poverilnice za prijavo v sistem. Da bi to zaobšli, lahko uporabimo tehniko, ki se imenuje soljenje.

4.4.2 Soljeno zgoščevanje

Naš cilj je, da je izvleček gesla edinstvena. Zato sistem ustvari naključno zbirko znakov, imenovano sol. Ko uporabnik vnese geslo v navadnem besedilu, se mu doda ustvarjena naključna zbirka znakov. Nato z zgoščevalno funkcijo iz vstavljenega besedila pridobimo vrednost izvlečka (soljeni izvleček - salted hash). V tem primeru je treba shraniti vrednost soli za vsakega uporabnika.

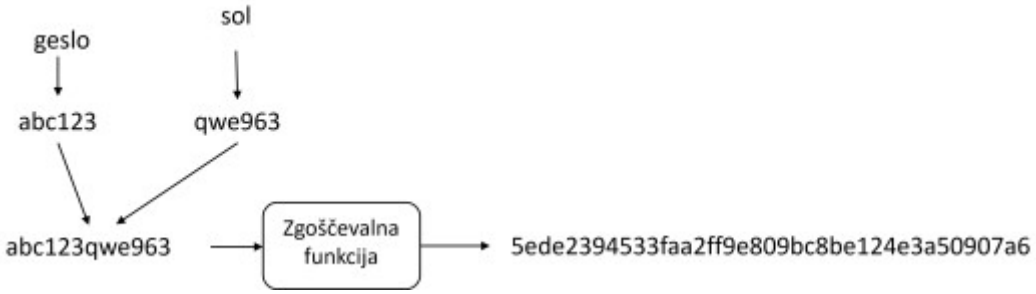


Fig. 24. Postopek soljenega zgoščevanja.

Čeprav imata John in Sam enako geslo, sta njuna izvlečka različna (glej Sliko 25).

Interaktivní prvek

Med postopkom prijave sistem iz zbirke podatkov pridobi ustrezno vrednost soli uporabnika, jo doda vhodnemu geslu, ga pošlje skozi zgoščevalno funkcijo in primerja dobljen izvleček s shranjenim izvlečkom. Uporabnik je uspešno overjen, če se obe vrednosti ujemata.

upor_ime	Vrednost_soli	Soljeno_zgoščeno_geslo
John	qwe963	5ede2394533faa2ff9e809bc8be124e3a50907a6
sam	hjk521	6367c48dd193d56ea7b0baad25b19455e529f5ee
Alice	asd753	0772dbe339a885eb2ed73c1fe842d2ef6e9003a3

Fig. 25. Primer tabele, v kateri so shranjena soljenja in zgoščena gesla.

Minimalna zaščita shranjenih gesel mora vključevati zgoščevanje in uporabo soli. Poleg tega NIST predlaga, da se uporabniku onemogoči dostop do sistema, če prevečkrat uporabi napačno geslo (npr. po treh neuspešnih poskusih uporabnik eno minuto ne sme ponovno poskusiti), da se v geslih dovolijo emojiji, znaki ASCII in Unicode ter da se v poljih z gesli dovolijo funkcije kopiraj in prilepi, da bi bila uporaba upraviteljev gesel in večfaktorskega overjanje bolj priročna.

Interaktivní prvek

CHAPTER 5

Overjanje brez gesla

Glede na vse težave in slabosti gesel zamisel o overjanju brez gesel ni nova. Kot pove že ime, overjanje brez gesla uporabniku omogoča prijavo ali dostop brez vnosa gesla ali odgovarjanja na varnostna vprašanja. Overjanje brez gesla zmanjšuje potrebo po nevarnih geslih in njihovem upravljanju, hkrati pa izboljšuje varnost uporabniških računov, saj zmanjšuje njihovo ranljivost za napade. Obstajajo različni mehanizmi overjanja brez gesla, kot so fizični žetoni, naprave/ključi USB, čarobne povezave, biometrično prepoznavanje, mobilne aplikacije itd. Večina teh tehnik se običajno uporablja pri večfaktorskem overjanju za povečanje varnosti. Vendar se lahko nekatere od teh rešitev uporabijo kot sistem za overjanje prvega dejavnika.

Ti elementi se običajno delijo v dve kategoriji:

- Primeri elementov lastništva so pametni telefoni, žetoni OTP, pametne kartice ali strojni žetoni ("nekaj, kar ima uporabnik").
- Prstni odtisi, skeniranje mrežnice, prepoznavanje obraza ali glasu in drugi biometrični identifikatorji so primeri dejavnikov inherence ("to, kar uporabnik je").

Overjanje brez gesla se pogosto zamenjuje z večfaktorskim overjanjem (MFA), saj se pri obeh uporabljajo različni dejavniki overjanje. Medtem ko se večfaktorska overjanje uporablja kot dodatna varnostna plast na vrhu overjanja z geslom, pa overjanje brez gesla ne zahteva zapomnjene skrivnosti in običajno uporablja samo en zelo varen dejavnik za preverjanje identitete, kar je za uporabnike hitrejše in enostavnejše.

Gesla si je težko zapomniti, zahteve pa postajajo vse bolj zapletene. Različna spletna mesta imajo lahko različne politike gesel, zato geslo, ustvarjeno za eno spletno mesto, morda ne bo delovalo na drugem. Zapomniti si geslo, ustvarjeno za sodobno izboljšano politiko gesel, je pogosto zahtevno.

Podobno kot pri hitri identiteti na spletu (FIDO) so tudi tu v igri različni standardi. Čeprav overjanje brez gesla in tehnologija FIDO obstajata že nekaj časa, ju spletne storitve in ponudniki identitet še niso začeli uporabljati v večjem obsegu. Overjanje brez gesla bo postala prihodnost overjanja zaradi vgradnje biometričnih funkcij v večino sodobnih mobilnih naprav in prenosnih računalnikov.

ADVANTA

Overjanje brez gesla izboljša izkušnjo končnega uporabnika, saj odpravlja utrujenost z geslom. Uporabniku ni več treba ustvariti daljšega in varnejšega gesla, temveč lahko pridobi enoten dostop do vseh programov s preprosto povezavo z napravo USB ali skeniranjem prstnega odtisa.

5.1.1 Hitra spletna identiteta (FIDO)

Fast Identity Online (FIDO) je sklop odprtokodnih protokolov za overjanje, ki ga je vzpostavilo združenje FIDO Alliance, da bi odpravilo gesla. Protokoli FIDO za varno overjanje uporabljajo osnovne algoritme kriptografije z javnim ključem. Zasebni ključi nikoli ne zapustijo varnostne naprave, vsi pogovori pa so šifrirani.

Fig. 26. Primer overjanja na podlagi FIDO.

Zveza FIDO je izdala tri sklope standardov.

- UAF (Universal Authentication Framework): V protokol FIDO UAF je vključena možnost overjanja brez gesla. Uporabniki, ki uporabljajo ta protokol, morajo podpisati izziv, ki ga zagotovi strežnik FIDO, z uporabo enega ali več varnostnih dejavnikov, ki so na voljo v njihovi varnostni/digitalni napravi.
- U2F (univerzalni drugi faktor): Protokol FIDO U2F omogoča overjanje drugega faktorja. Uporabniki morajo za potrditev svoje identitete predložiti dva dokaza. Z uvedbo protokola FIDO2 se je preimenoval v CTAP1.
- FIDO2: Najnovejši sklop specifikacij zavezništva FIDO je znan kot FIDO2.

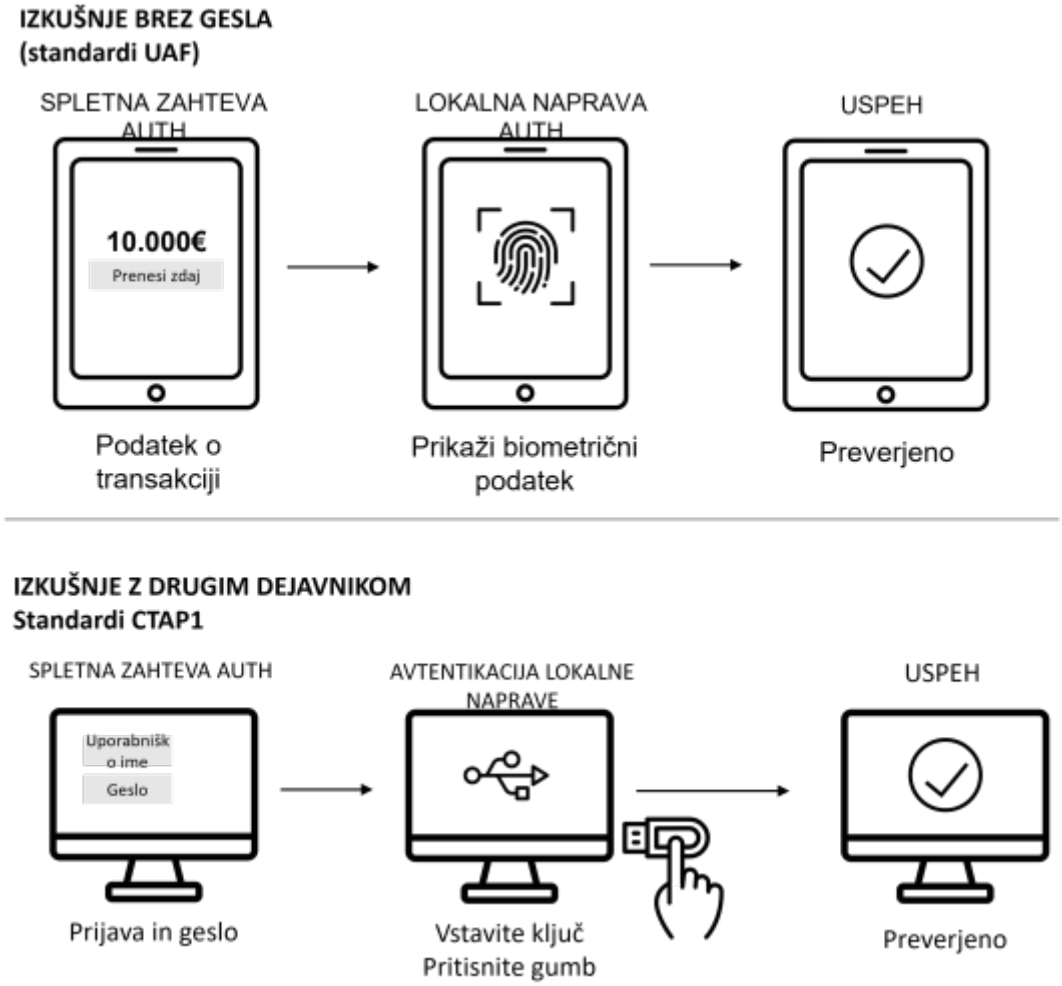


Fig. 27. Standardi UAF in U2F (CTAP1) za overjanje brez gesla.

5.1.2 FIDO2 in Webauthn

Specifikacijo FIDO2 sestavljajo:

- standard W3C za spletno overjanje (WebAuthn) in
- protokol 2 odjemalca FIDO za overjanje (CTAP2).

FIDO2 uporabnikom omogoča, da z običajnimi napravami brez težav overjajo pri internetnih storitvah v mobilnem in namiznem okolju. WebAuthn je standardni spletni vmesnik API za overjanje FIDO, ki je vključen v platforme in brskalnike. CTAP2 je različica CTAP, ki uporabnikom omogoča uporabo zunanjih in vgrajenih overitvenih naprav za zagotavljanje overjanja brez gesla, dvo- ali večfaktorske overjanja. API WebAuthn je orodje za ustvarjanje in upravljanje poverilnic z javnim ključem. Pregled metode overjanjeFIDO2 je prikazan na sliki 28.

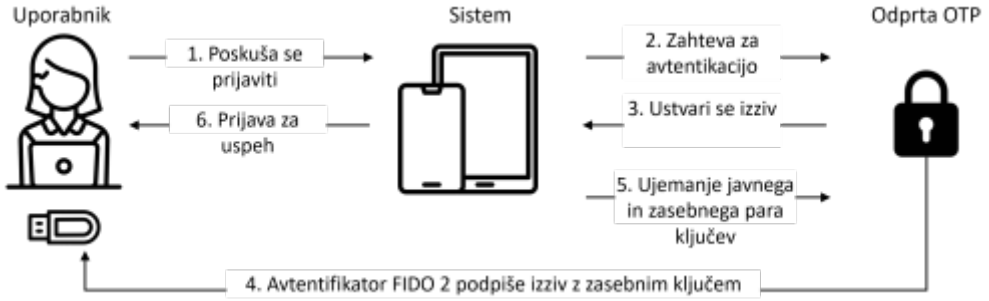


Fig. 28. Metoda overjanja FIDO2.

Interaktivní prvek

CHAPTER 6

Uvod v digitalno podpisovanje

DEFINITION

Matematični sistem za preverjanje veljavnosti digitalnih sporočil ali dokumentov je znan kot digitalni podpis.

Pravi digitalni podpis daje prejemniku dober razlog, da verjame, da je sporočilo ustvaril znani pošiljatelj (avtentičnost) in da ni bilo spremenjeno med prenosom, če so izpolnjeni predpogoji (celovitost).

Glavni cilji, ki jih želi doseči digitalni podpis, so:

- **Overjanje**: Digitalni podpisi so vezani na določenega uporabnika prek njegovega zasebnega ključa. Tako lahko ugotovi, kdo je lastnik zasebnega ključa, ki je bil uporabljen za podpis izvirnega podatka/sporočila (npr. dokumenta, e-pošte ali datoteke). Za več informacij o zasebnih in javnih ključih glejte v nadaljevanju.
- **Integriteta**: Pri digitalnih podpisih se uporablja tehnika zgoščevanja, ki zagotavlja, da sporočilo ni bilo spremenjeno. Za več informacij o zgoščevanju glejte spodaj.

Digitalni podpisi so torej eden od načinov overjanja entitete, vendar moramo najprej pojasniti nekaj pojmov, preden lahko pokažemo, kako lahko digitalni podpis uporabimo pri overjanju.

6.1 Kriptografija z javnim ključem

Da bi razumeli digitalne podpise, moramo najprej pojasniti asimetrično kriptografijo, pogosto imenovano kriptografija z javnim ključem. V nasprotju s klasičnim (simetričnim) šifriranjem, ki za šifriranje uporablja samo en ključ, asimetrično šifriranje uporablja par ključev. Šifriranje je postopek kodiranja informacij, kot je prikazano na sliki 29.

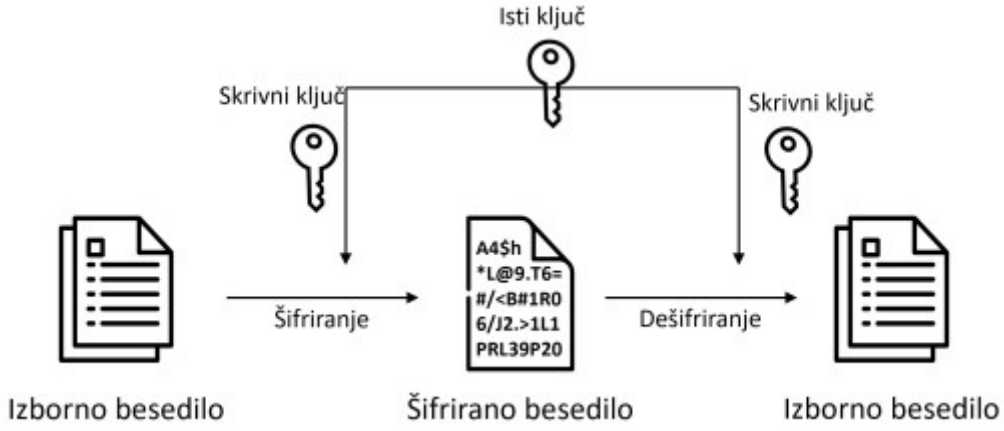


Fig. 29. Simetrično šifriranje

Predstavljajte si, da želite nekomu poslati šifrirano sporočilo z uporabo klasičnega šifriranja. V tem primeru se morata obe strani dogovoriti o enem samem ključu. Tega si ne moreta posredovati, ker ga lahko potem nekdo vidi in bo lahko videl vsa vajina sporočila.

DEFINITION

Po drugi strani pa asimetrično šifriranje uporablja par ključev, javni in zasebni ključ, ki sta matematično povezana. Samo povezan zasebni ključ lahko dešifrira tisto, kar je šifrirano z javnim ključem.

Če nekdo želi, da mu drugi pošiljajo šifrirana sporočila, preprosto objavi svoj javni ključ, da ga vsi vidijo. Za dešifriranje sporočil, šifriranih z njihovim javnim ključem, preprosto uporabijo svoj zasebni ključ, saj je sporočila, šifrirana z njihovim javnim ključem, mogoče dešifrirati le z njihovim zasebnim ključem. To je koristno, saj nam ni treba skrbeti za varno deljenje javnega ključa.

Če hočeta dve stranki varno komunicirati z asimetričnim šifriranjem, je postopek naslednji:

- Stranki si izmenjata javne ključe.
- Oseba 1 šifrira sporočilo, ki ga želi poslati, z javnim ključem osebe 2 in ga pošlje osebi 2.
- Oseba 2 dešifrira sporočilo s svojim zasebnim ključem.

Ta postopek je prikazan na sliki 30.

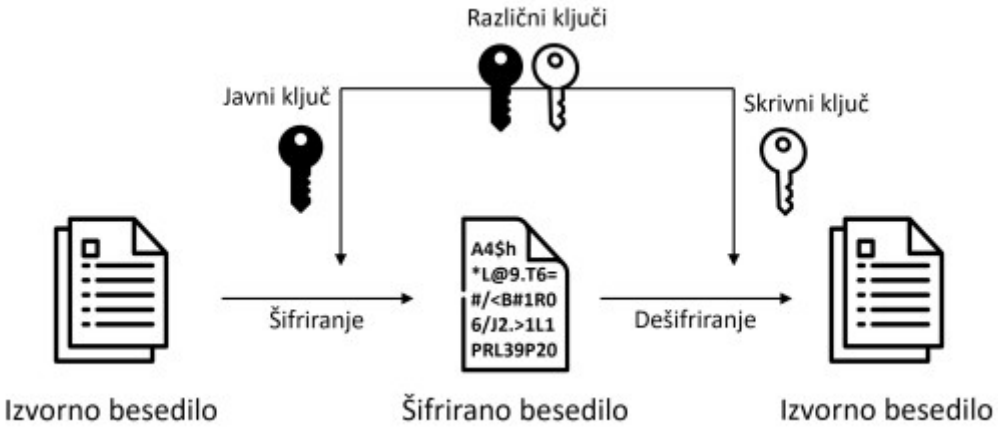


Fig. 30. Postopek asimetričnega šifriranja (z javnim ključem).

DEFINITION

Digitalni podpisi delujejo tako, da z zasebnim ključem podpišejo (šifrirajo) karkoli, kar se nato potrdi z javnim ključem, ki je povezan z njim. Tako se ključa v paru ključev uporabljata nasprotno.

Podpisnik je namreč edina oseba, ki ima dostop do zasebnega ključa, uporabljenega za podpis. Zato ste lahko prepričani, da je podpisala prav ta oseba. Vsakdo lahko z javnim ključem preveri (tj. uspešno dešifrira sporočilo), da je sporočilo ustvaril lastnik javnega ključa.

Interaktivní prvek

6.2 Postopek digitalnega podpisovanja

Kot smo že omenili, se pri digitalnem podpisovanju uporablja par ključev, sestavljen iz javnega in zasebnega ključa. Kriptografski pari ključev se uporabljajo za šifriranje (zaklepanje) in dešifriranje (odklepanje) izvornih podatkov na enak način, kot se za zaklepanje in odklepanje uporabljajo fizični ključi. Zasebni ključi so varni in zaupni, saj če nekdo izve zasebni ključ druge osebe, lahko podpiše izvorne podatke kot ta oseba. Po drugi strani pa naj bi bili javni ključi deljeni z vsemi. Podatke, šifrirane z zasebnim ključem, je mogoče dešifrirati le z javnim ključem, s čimer se razkrijejo izvirni podatki.

DEFINITION

Vendar pa postopek digitalnega podpisovanja vključuje asimetrično kriptografijo in zgoščevalne funkcije.

Ta dva gradnika sta združena v dejanski postopek podpisovanja, kot sledi:

1. Pošiljatelj z zgoščevanjem izračuna izvleček izvorne vsebine, ki jo želi dostaviti.
2. Pošiljatelj šifrira izračunani izvleček s svojim zasebnim ključem in tako ustvari digitalni podpis.
3. Nato lahko vsebino in digitalni podpis pošljete prejemniku.
4. Ko prejemnik prejme sporočila, z uporabo pošiljateljevega javno dostopnega javnega ključa dešifrira šifrirani digitalni podpis pošiljatelja. Če je to uspešno, se potrdi identiteta pošiljatelja kot lastnika zasebnega ključa, ki je bil uporabljen za šifriranje datoteke.
5. Prejemnik nato iz prejetega sporočila pridobi izvirno vsebino in ustvari izvleček te vsebine.
6. Vsebina je potrjena kot enaka vsebini, ki jo je posredoval pošiljatelj, če se prejemnikov izračunani izvleček ujema s pošiljateljevim. Če se ne ujemata, je bila vsebina prirejena, zato podpis ni veljaven.

Grafični prikaz postopka je prikazan na sliki 31.

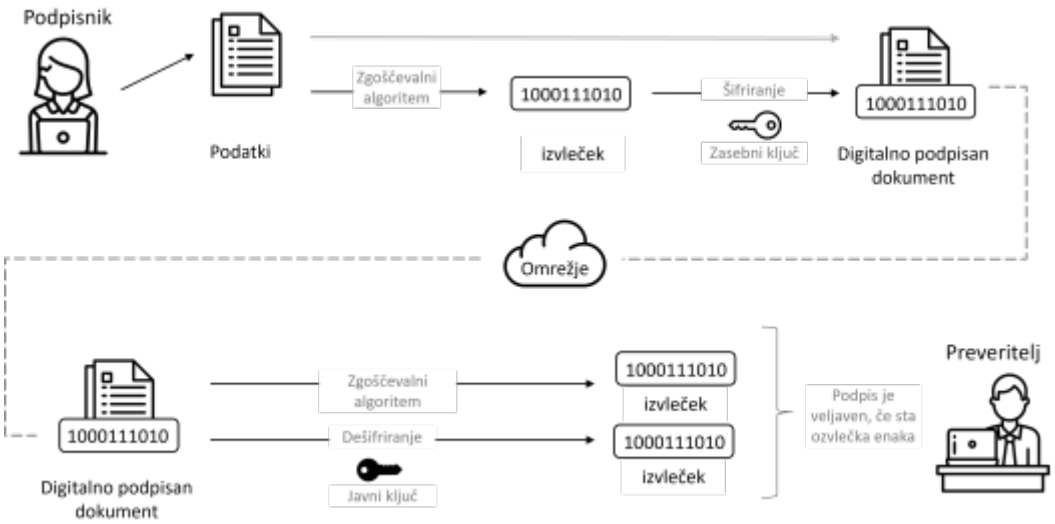


Fig. 31. Shematski prikaz ustvarjanja in preverjanja digitalnega podpisa.

Ker je pošiljateljev javni ključ javno dostopen, lahko šifrirano vsebino, ki jo pošiljatelj pošlje, dešifrira vsakdo. Zato ta metoda šifriranja preverja samo celovitost, ne pa tudi zaupnosti.

Vprašali bi se, zakaj pred podpisovanjem podatkov ustvarimo izvleček podatkov? Preprosto zato, ker je tako podpis veliko manjši, postopek ustvarjanja in preverjanja digitalnega podpisa pa hitrejši, saj se primerjajo le izvlečke in ne celotni podatki/dokument. Upoštevajte, da to deluje zato, ker zgoščevalni algoritmi vedno ustvarijo vrednost določene dolžine.

ADVANTA

Kot ste morda že uganili, imajo digitalni podpisi več prednosti, med drugim naslednje:

- povečujejo varnost in zaupanje, saj jih ni mogoče povratno analizirati ali ponarediti;
- šifriranje izvornih podatkov zagotavlja ne-zanikljivost;
- zagotavljanje celovitosti prenesenih podatkov.

DISADVANTA

Vendar imajo digitalni podpisi tudi pomanjkljivosti, kot so:

- dejstvo, da ni mogoče preklicati podpisov (zaupanja v podatke vira) po njihovi distribuciji, zaradi česar so sodbe nepovratne;
- uporaba javnih ključev onemogoča tajnost. Podpis lahko preveri vsakdo, ki ima javni ključ.

Interaktivní prvek

CHAPTER 7

Infrastruktura javnih ključev

Spoznali smo že koncepta digitalnega podpisovanja in kriptografije javnega ključa. Izkazalo se je, da za pravilno delovanje celotnega koncepta v resničnem življenju potrebujemo še nekaj več. Potrebujemo nekaj, kar se imenuje infrastruktura javnega ključa (PKI).

DEFINITION

PKI je skupek tehnologij, procesov in subjektov, ki omogočajo varno komunikacijo prek nezanesljivih javnih omrežij.

Na primer, PKI je tisto, kar HTTPS dodaja oznako S, in če si to vsebino ogledujete v spletnem brskalniku, ga verjetno uporabljate, da zagotovite, da je iz zaupanja vrednega vira. PKI omogočajo reguliran dostop do sistemov in virov, zaščito podatkov in odgovornost transakcij z ugotavljanjem identitete posameznikov, naprav in storitev.

PKI se uporablja v različnih aplikacijah, vključno z zagotavljanjem komunikacijske varnosti v internetu stvari (IoT) in podpisovanjem digitalnih dokumentov. PKI, ki temelji na asimetrični kriptografiji, se običajno uporablja za vzpostavitev varnih elektronskih komunikacij, kot so spletno nakupovanje, bančništvo in e-pošta, ter komunikacije med uporabniki in spletnimi mesti, s katerimi se povezujejo z uporabo protokola HTTPS. PKI omogoča močno overjanje, šifriranje podatkov in digitalne podpise za ljudi, storitve in predmete z zagotavljanjem digitalnih identitet. Te varnostne metode zagotavljajo varen dostop do fizičnih in digitalnih virov, varno komunikacijo med ljudmi, storitvami in stvarmi ter digitalno podpisovanje dokumentov, transakcij ali drugih podatkov.

7.1 Sestavni deli infrastrukture javnih ključev (PKI)

PKI sestavljajo naslednje komponente:

- organ za izdajo potrdil (CA).
- registracijski organ (RA).
- organ za potrjevanje (VA).
- digitalna potrdila

In seveda kriptografija z javnim ključem (PKC).

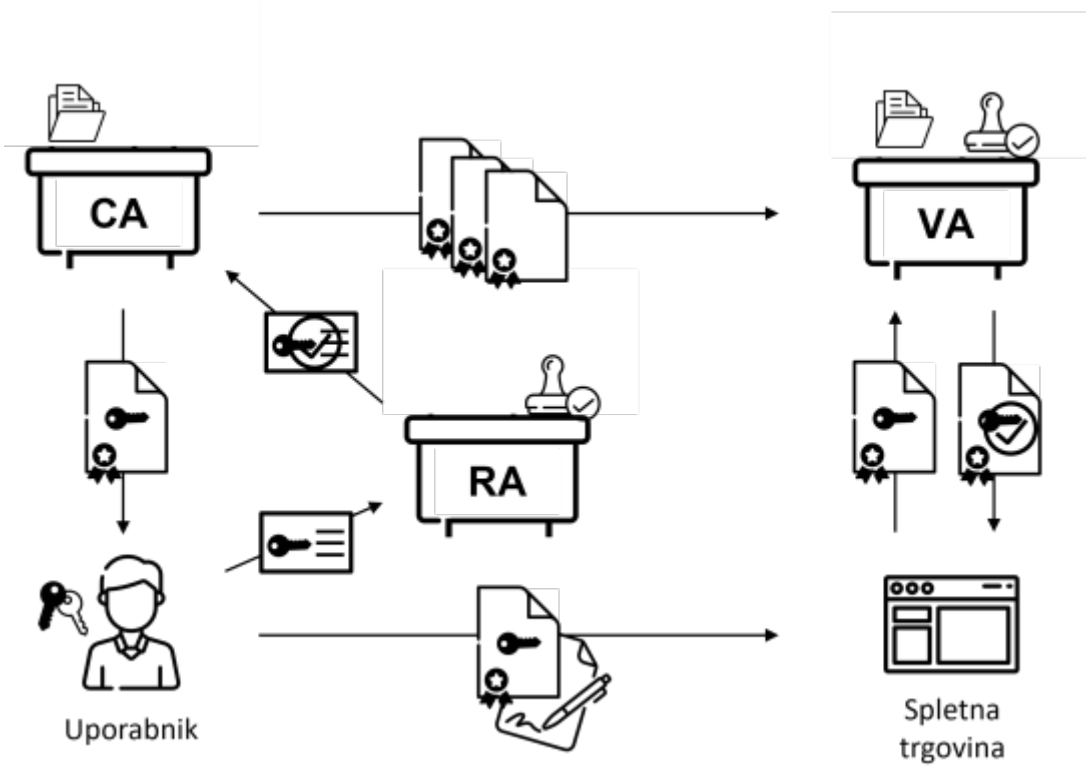


Fig. 32. Sestavni deli infrastrukture javnih ključev (PKI).

Organ za potrjevanje

DEFINITION

Organ za izdajo potrdil, pogosto znan kot certifikacijski organ (CA), je podjetje, ki ustvarja in distribuira digitalna potrdila.

Digitalno potrdilo potrjuje, da je imenovani subjekt potrdila lastnik javnega ključa. Drugi (zanašajoče se stranke) lahko zaupajo podpisom in trditvam o zasebnem ključu, ki se ujema s potrjenim javnim ključem. Overitelj služi kot zaupanja vredna tretja oseba, ki ji zaupata subjekt (lastnik) potrdila in stranka, ki se zanaša na potrdilo.

Podpisovanje potrdil, ki se uporabljajo v protokolu HTTPS za varno brskanje, je ena od najpogostejših uporab organov za potrdila. Druga priljubljena uporaba je za nacionalne vlade, ki izdajajo osebne izkaznice, ki se lahko uporabljajo za digitalno podpisovanje ali e-upravo.

Registracijski organ

DEFINITION

V infrastrukturah javnih ključev je organ za registracijo (RA) funkcija za vpisovanje potrdil. Zadolžena je za sprejemanje zahtevkov za podpisovanje potrdil od posameznikov, strežnikov, stvari in drugih aplikacij, bodisi za začetni vpis bodisi za podaljšanje. Registracijski organ te zahteve preveri in jih posreduje organu za izdajo potrdil (CA).

Registracijski organ skrbi tudi za upravljanje življenjskega cikla potrdil. Obravnavajte primer preklica. RA vključuje poslovno logiko za sprejemanje zahtevkov, vključno z metodami za preverjanje izvora prosilca in stranke, ki bi morala imeti potrdilo.

Zaradi dostopnosti in varnosti je registracijski organ običajno ločen od organa za izdajo potrdil. Do RA je mogoče dostopati prek uporabniku prijaznega grafičnega vmesnika ali prek vmesnikov API in standardnih protokolov, ki jih je enostavno integrirati.

Organ za potrjevanje

Potrdila PKI potrdi organ za potrjevanje PKI (VA). Dostop do seznamov preklicanih potrdil (CRL), protokola OCSP (Online Certificate Status Protocol) in prenosa verižnih potrdil CA so primeri storitev potrjevanja potrdil. Ker je potrdila mogoče izdati in preklicati, je nujno preveriti pristnost potrdila, preden mu zaupamo. Organ za potrjevanje je zadolžen za reševanje tega vprašanja.

Organ za izdajo potrdil je odgovoren za zagotavljanje posodobitev stanja potrdila organu za potrjevanje v skladu z vzpostavljeno politiko. Pri uporabi seznamov CRL (CA) se zanašate, da bo vsak povezan organ za potrdila izdal seznam preklicanih digitalnih potrdil.

Digitalno potrdilo

Digitalno potrdilo je vrsta elektronske identifikacije za posamezne subjekte ali organizacije, podobna osebni izkaznici. Vsebuje informacije, kot so identifikacija, serijska številka in datum poteka veljavnosti. Vidimo lahko tudi digitalni podpis overitelja, ki zagotavlja pristnost potrdila, in javni ključ imetnika potrdila znotraj informacij. PKI na primer omogoča overjene povezave in v kombinaciji z drugimi kriptografskimi pristopi tudi varuje povezave med dvema komunicirajočima napravama, saj je mogoče identiteto obeh strank potrditi z digitalnimi potrdili. Skoraj vsa danes izdana potrdila so skladna s standardom X.509.

Potrdila so različnih vrst:

- **Potrdila za podpisovanje kode**: Koda je bila potrjena, kot da prihaja od razvijalcev in ni bila spremenjena, zato je programska oprema zanesljiva. Uporablja se za podpisovanje izdaj programske opreme in potrjevanje programske opreme prodajalca ali razvijalca, da se potrdi, da je zakonita.

- **e-poštna potrdila:** Protokol S/MIME se lahko uporablja za varovanje in potrjevanje e-poštnih sporočil, s čimer lahko pošiljatelj ugotovi avtorstvo in prepreči ponarejanje.
- **Potrdila za podpisovanje dokumentov:** Adobe, Microsoft in druge programe je treba uporabljati za podpisovanje dokumentov, da se zagotovi njihova nespremenjenost in zanesljivost. To potrdilo se skoraj vedno uporablja, ko na dokumentu vidite digitalni podpis.
- **potrdila TLS (HTTPS):** Uporabljajo se za varne povezave HTTPS.

Fig. 33. Primer digitalnega potrdila v operacijskem sistemu Microsoft Windows.

Interaktivní prvek

7.2 Hierarhična struktura infrastrukture javnih ključev (PKI)

Hierarhija overiteljev, ki podpisujejo in izdajajo digitalna potrdila ali poverilnice, je običajna v PKI. Vsaka CA pooblasti pod-CA za podpisovanje digitalnih potrdil za naprave. Končne naprave sporočajo digitalna potrdila na dnu, ki jih dovoli pod-CA nad njimi, ki jih je ustvarila in podpisala. Ti se včasih imenujejo potrdila naprav. Pod-CA, ki ustvarjajo potrdila naprav, imajo svoja potrdila, ki jih dovoljuje digitalni podpis CA nad njimi, in tako naprej. PKI na koncu doseže korenski sistem, ki služi kot temelj za to posebno domeno ekosistema PKI.

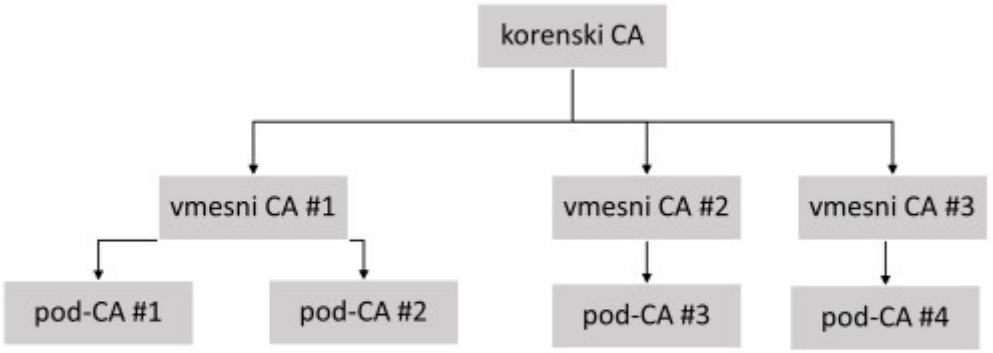


Fig. 34. Primer hierarhije PKI.

Z razvrstitvijo ekosistemov PKI v hierarhije lahko omogočimo posebne ravni preklica ali zavrnitve dostopa v primeru uhajanja ali kompromitiranja zasebnega ključa v ekosistemu.

Vsakdo lahko prekliče potrdilo katerega koli elementa PKI, od naprave do CA na visoki ravni, odvisno od narave varnostne kršitve. Vendar pa preklic potrdila prekliče tudi vse elemente, ki so v hierarhiji pod njim.

Poleg tega to kaže, zakaj so izvedbe PKI organizirane v drevesnih hierarhijah. Takšna zasnova omogoča lastniku ekosistema selektivno obvladovanje škode v primeru kršitve. Zato izdajanje potrdil za naprave iz korenske CA ni dobra zamisel, saj omejuje prilagodljivost. Če gre v tem primeru kaj narobe, bomo morda morali razveljaviti in preklicati celoten PKI in vse nameščene naprave na terenu. Zato potrdila naprav praktično vedno izdajajo podrejeni overitelji pod korenskim overiteljem.

7.3 Življenjski cikel digitalnega potrdila

Življenjski cikel digitalnega potrdila se začne z njegovo izdelavo in ga lahko na kratko razložimo na naslednji način:

- **Vpis v certifikat:** Organ za potrjevanje (CA) prejme zahtevo za potrdilo od subjekta. Za entiteto se lahko šteje oseba, naprava ali celo nekaj vrstic kode.
- **Izdaja potrdila:** RA mora preveriti identiteto prosilca, kar običajno stori s poverilnicami ali z zanašanjem na identiteto drugega RA, ki je prosilca že preveril.
- **Potrjevanje certifikata:** Strežnik ob vsaki uporabi potrdila za overjanje preveri, ali je potrdilo še vedno veljavno in ni poteklo ali bilo preklicano.
- **Preklic potrdila:** Ko so potrdila prvič izdana, imajo naveden datum poteka veljavnosti. Ko ta datum poteče, overitelj potrdilo uvrsti na seznam preklicanih potrdil (CRL), ki je nekakšen črni seznam, ki strežniku sporoča, naj ne zaupa določenim potrdilom.
- **Podaljšanje certifikata:** Overitelje je mogoče konfigurirati tako, da samodejno obnovijo potrdila, ko jim poteče rok veljavnosti, čeprav običajno zahtevajo ponovno preverjanje identitete.

Interaktivní prvek

Organi potrdil in veriga zaupanja

Izraz "veriga zaupanja" se nanaša na razmerje med digitalnim potrdilom in zaupanja vrednim overiteljem. Da bi bilo potrdilo zaupanja vredno, ga je treba izslediti do zaupanja vrednega korenskega overitelja, ki ga je izdal, kar pomeni, da morajo biti vsa potrdila v verigi - strežniško, vmesno in korensko - ustrezno zaupanja vredna.

Na sliki 35 vidimo, da je za strežnik google.com GTS-CA 1C3 CA spodnje ravni. GTS-Root R1 je CA srednje ravni. R1 je najvišji korenski CA za GlobalSign. S to metodo je mogoče vzpostaviti verigo zaupanja.

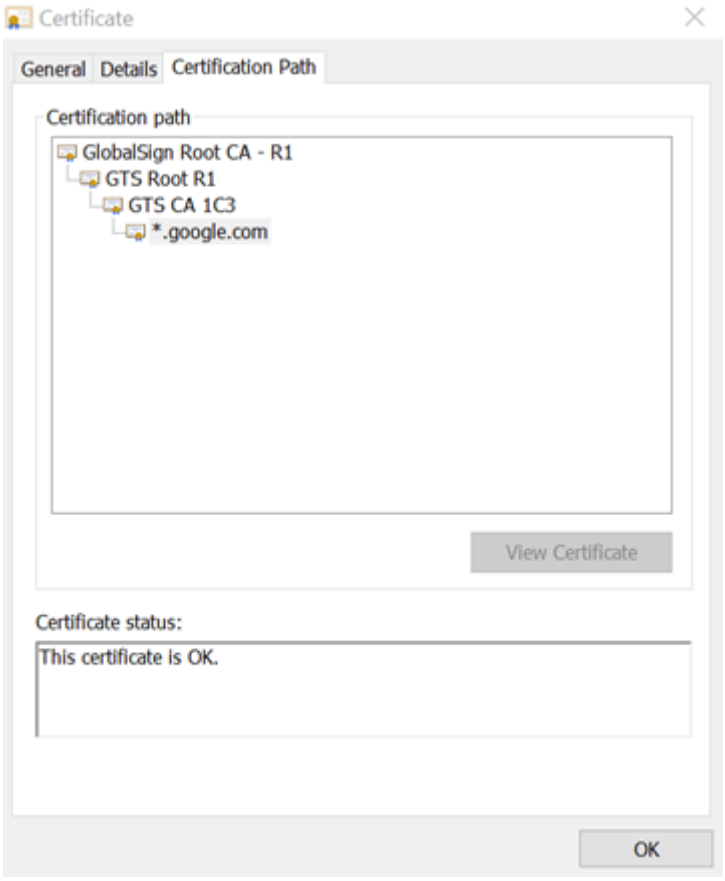


Fig. 35. Primer verige zaupanja.

Veriga zaupanja ima tri dele:

- **Korensko potrdilo** je digitalno potrdilo, ki pripada overitelju, ki ga je izdal. V večini brskalnikov je na primer že nameščeno in shranjeno v "zaupanja vredni shrambi". Organi za potrjevanje skrbno spremljajo korenska potrdila. GlobalSign Root CA- R1 je na primer korenski CA.
- **Vmesna potrdila** so kot veje na drevesu, korensko potrdilo pa je kot deblo drevesa. Služijo kot povezava med zaščitenimi korenskimi potrdili in javno izdanimi strežniškimi potrdili. V verigi je vedno vsaj eno vmesno potrdilo, lahko pa jih je tudi več.
- **Strežniško potrdilo** je tisto, ki je bilo dodeljeno določeni domeni (v tem primeru www.google.com).

7.4 Overjanje z uporabo protokolov PKI in PKC

V digitalnem svetu je infrastruktura javnih ključev (PKI) sistem za overjanje oseb in naprav. Ena ali več zaupanja vrednih strank digitalno podpiše dokumente, s katerimi preveri, ali določen kriptografski ključ pripada določenemu uporabniku ali napravi. Ključ se lahko nato uporabi kot identiteta uporabnika v digitalnih omrežjih.

Digitalna potrdila se lahko uporabljajo tudi za overjanje 2FA ali overjanje brez gesla.

Ko uporabnik poskuša preveriti svojo identiteto v strežniku, strežnik ustvari naključne podatke in jih pošlje uporabniku. Uporabnik nato podatke šifrira s svojim zasebnim ključem in jih vrne strežniku. Strežnik podatke dešifrira z javnim ključem uporabnikovega digitalnega potrdila in če se dešifrirani podatki ujemajo s prejetimi podatki, strežnik ve, da je uporabnik tisti, za katerega se izdaja. To je osnovni postopek uporabe PKI+PKC za overjanje.

CHAPTER 8

Test

Najvarnejši način shranjevanja gesel je:

- ◯ šifriranje
- ◯ zgoščevanje
- ◯ izvorno besedilo
- ◯ soljeno zgoščevanje

Kakšen je cilj overjanja?

- ☐ preveriti svojo identiteto.
- ☐ prepoznati nekoga
- ☐ preverjanje, do česa lahko nekdo dostopa.
- ☐ je bistveni del kibernetske varnosti.

Solenje gesel otežuje napade, saj je slovarski napad specifičen za vsako geslo posebej:

- ◯ uporabnik
- ◯ napadalec
- ◯ naprava
- ◯ geslo

Kateri so najpogostejši načini overjanja?

- ☐ uporabniško ime in geslo
- ☐ skeniranje obraza

- ☐ e-pošta in geslo
- ☐ RSA SecureID

Katera je najbolj izrazita pomanjkljivost značilnosti "kaj ste"?

- ◯ ni verodostojen
- ◯ se lahko izgubi
- ◯ se lahko pozabi
- ◯ je mogoče ukrasti

Katere so glavne kategorije overjanja?

- ☐ kako ste videti
- ☐ kaj veš
- ☐ kdo ste
- ☐ kaj imate

Kaj je večfaktorsko overjanja?

- ◯ overjanje, ki uporablja vsaj dva različna dejavnika.
- ◯ overjanje, ki uporablja natanko dva različna dejavnika
- ◯ overjanje, ki uporablja natanko enega različnega dejavnika.
- ◯ To je enako kot dvofaktorsko overjanje (2FA).

Primeri overjanja po načelu "kar imaš" vključujejo:

- ☐ pametni telefon
- ☐ geslo
- ☐ prstni odtis
- ☐ pametno kartico

Pri metodi overjanja z izzivom in odgovorom, komu se predstavi izziv?

- ◯ uporabniku
- ◯ strežniku
- ◯ programu
- ◯ overitveni napravi

Osnovni postopek overjanja vključuje:

- ☐ strežnik
- ☐ podatki za overjanje
- ☐ uporabnika
- ☐ ključno besedo

V metodo overjanja so vključeni naslednji gradniki:

- ☐ vnos
- ☐ preveritelja
- ☐ računalnik
- ☐ transportni sistem

Kako dolga morajo biti gesla v skladu s trenutnimi smernicami in najboljšimi praksami?

- ◯ 6 znakov
- ◯ 4 znake
- ◯ 7 znakov
- ◯ vsaj 12 znakov

Kaj počne zgoščevalna funkcija?

- ◯ tvori hashtag
- ◯ izračuna edinstven identifikator podatkov
- ◯ ustvarja gesla
- ◯ prepreči overjanje

Kateri elementi se lahko uporabijo za dvofaktorsko overjanja?

- ☐ sporočilo SMS
- ☐ identifikacijski žeton
- ☐ aplikacijo pametnega telefona
- ☐ uporabniško ime

Kateri je standard za overjanje brez gesla?

- ◯ FIDO2
- ◯ FIBA
- ◯ UFI
- ◯ UPA

Trenutni industrijski standardi za varno shranjevanje gesel vključujejo:

- ☐ šifriranje
- ☐ zgoščevanje
- ☐ shranjevanje v izvorni obliki
- ☐ soljeno zgoščevanje

V kakšnem zaporedju se v postopku digitalnega podpisovanja uporabljajo ključi?

- ◯ pošiljateljev zasebni ključ in prejemnikov javni ključ
- ◯ pošiljateljev zasebni ključ in pošiljateljev javni ključ

- ◯ prejemnikov zasebni ključ in prejemnikov javni ključ
- ◯ pošiljateljev javni ključ in prejemnikov zasebni ključ

Katera vrsta napada je zaradi tehnike soljenega zgoščevanja gesel težja?

- ☐ napadi s slovarjem
- ☐ napadi s surovo silo
- ☐ napadi na strežnik
- ☐ napadi na uporabniško napravo

Katere so ranljivosti tehnike overjanja "kaj veš"?

- ☐ ga je mogoče pozabiti
- ☐ ga je mogoče izgubiti
- ☐ ga je mogoče podvojiti
- ☐ se ga lahko zavrne

Če se za šifriranje uporablja kriptografija z javnim ključem, kateri ključ se uporabi za šifriranje podatkov?

- ◯ javni ključ prejemnika
- ◯ pošiljateljev javni ključ
- ◯ zasebni ključ prejemnika
- ◯ zasebni ključ pošiljatelja

Katere so ranljivosti tehnike overjanja "kaj imaš"?

- ☐ ga je mogoče pozabiti
- ☐ lahko se izgubi
- ☐ je mogoče podvojiti

☐ je mogoče zavrniti

Kakšno je zaporedje ključev, ki se uporabljajo pri asimetričnem šifriranju?

◯ zasebni ključ pošiljateljev in javni ključ prejemnika

◯ zasebni ključ pošiljatelja in javni ključ pošiljatelja

◯ zasebni ključ prejemnika in javni ključ prejemnika

◯ javni ključ pošiljatelja in zasebni ključ prejemnika

Kakšno je pravilno zaporedje korakov v postopku digitalnega podpisovanja?

◯ izvleček, podpis in pošiljanje

◯ podpišite, zgostite in pošljite

◯ šifriranje, stiskanje in pošiljanje

◯ zgoščevanje, kodiranje in pošiljanje

Kateri so primeri overjanja z geslom?

☐ enkratna gesla

☐ gesla za večkratno uporabo

☐ strukturirana gesla

☐ poverilnice

Katere so komponente infrastrukture javnega ključa (PKI)?

◯ CA, MA, LA, digitalni podpis

◯ CA, RA, PA, digitalni podpis

◯ CA, RA, PKC, digitalno potrdilo

◯ CA, RA, PKC, digitalni podpis

Kateri so neelektronski napadi na gesla?

- ☐ brskanje po ramenih.
- ☐ socialni inženiring
- ☐ napad s slovarjem
- ☐ napad s surovo silo

Katera je glavna naloga overitelja?

- ◯ izdajanje potrdil
- ◯ izdajanje digitalnih podpisov
- ◯ preverjanje digitalnih podpisov
- ◯ preverjanje posameznikove identitete

Kateri so elektronski napadi na gesla?

- ☐ ribarjenje
- ☐ socialni inženiring
- ☐ napad s slovarjem
- ☐ napad s surovo silo

Kako je udejanjen PKI?

- ◯ kot drevesna struktura
- ◯ kot sistem odjemalec-strežnik
- ◯ v strojni opremi
- ◯ zaporedno

Katera od naslednjih orodij so orodja za razbijanje gesel?

- ☐ John the cracker
- ☐ John the ripper
- ☐ Hydra
- ☐ Hibridni

Česa gesla ne smejo vsebovati?

- ☐ različne vrste znakov
- ☐ besede, povezane z vami
- ☐ rojstni datumi
- ☐ posebni znaki

Katere funkcije običajno vključujejo upravitelji gesel?

- ☐ samodejno dokončanje
- ☐ ustvarjanje gesel
- ☐ ocenjevanje gesel
- ☐ zastarelost gesla

Katere so pomanjkljivosti 2FA?

- ☐ neprijetnosti
- ☐ večja varnost
- ☐ pomisleki glede zasebnosti
- ☐ močnejše preverjanje pristnosti

Kateri so glavni cilji digitalnega podpisa?

- ☐ zagotavljanje overjanja
- ☐ zagotavljanje celovitosti

- ☐ zagotavljanje zaupnosti
- ☐ zagotavljanje avtorizacije

Katere vrste ključev se uporabljajo pri asimetričnem šifriranju?

- ☐ javni ključ
- ☐ tajni ključ
- ☐ ključ zasebnosti
- ☐ zasebni ključ

Kateri gradniki so vključeni v postopek digitalnega podpisovanja?

- ☐ zgoščevalne funkcije
- ☐ simetrični algoritmi šifriranja
- ☐ algoritmi za izmenjavo ključev
- ☐ asimetrični algoritmi šifriranja

Kakšno je pravilno zaporedje korakov v postopku preverjanja digitalnega podpisa?

- ☐ pridobitev izvlečka iz podpisa, pridobitev izvlečka iz podatkov, primerjava
- ☐ pridobitev izvlečka iz podatkov, pridobitev izvlečka iz podpisa, primerjava
- ☐ primerjava, pridobitev izvlečka iz podatkov, pridobitev izvlečka iz podpisa
- ☐ primerjava, pridobitev izvlečka iz podpisa, pridobitev izvlečka iz podatkov

Katere so komponente infrastrukture javnih ključev (PKI)?

- ☐ CA
- ☐ PA
- ☐ digitalni podpis
- ☐ digitalno potrdilo

Katere so značilne sestavine digitalnih potrdil?

- ☐ datum izteka veljavnosti
- ☐ izdajatelj
- ☐ dolžina
- ☐ digitalni podpis

Kateri so glavni deli verige zaupanja v PKI?

- ☐ Korensko potrdilo
- ☐ vmesno potrdilo
- ☐ digitalni podpis
- ☐ upravno potrdilo

Kako se lahko digitalna potrdila uporabljajo za preverjanje pristnosti?

- ☐ služijo kot glavni dejavnik overjanja
- ☐ služijo kot drugi dejavnik avtentikacije
- ☐ jih ni mogoče
- ☐ za podpisovanje dokumentov