

## Sigurnost računalnih sustava

# Kontrola pristupa

doc. dr. sc. Ante Đerek

doc. dr. sc. Stjepan Groš

izv. prof. dr. sc. Miljenko Mikuc

izv. prof. dr. sc. Marin Vuković

# Kontrola pristupa (engl. access control)

- Kontrola pristupa sastoji se od dva koraka
  - Autentifikacija (alternativno autentikacija, engl. authentication)
  - Autorizacija (engl. authorization)
- **Autentifikacija** je proces provjere identiteta SUBJEKTA (korisnika, procesa ili uređaja)
  - Međusobna autentifikacija (engl. mutual authentication) je slučaj kada se jedna strana drugoj autentificiraju. Dosta često samo jedna strana se autentificira.
- **Autorizacija** je proces odlučivanja može li SUBJEKT obaviti točno određenu OPERACIJU nad OBJETKOM.

# Metode autentifikacije

- Temelje se na jednom ili kombinaciji više faktora
  - Nečemu što znamo
  - Ono što jesmo
  - Ono što imamo
- Jedno-faktorska autentifikacija (1FA)
  - Najčešće korištena, u dosta slučajeva nedovoljna, trend prelaska na 2FA
- Dvo-faktorska autentifikacija (2FA)
  - Sve više korištena i dovoljno visoke razine zaštite (pod određenim uvjetima)
- Višefaktorska autentifikacija (MFA)
  - Rijetko korištena

# Primjeri autentifikacijskih mehanizama

- Lozinke (engl. Passwords)
- Dijeljene tajne (engl. shared secrets)
- Fraze (engl. pass-phrases)
- Jednokratne lozinke (engl. One-Time Passwords, OTP)
- Pametne kartice (engl. smart cards)
- Biometrijske metode (engl. biometric methods)

# Lozinke

- Temeljene na onome što znamo
  - Niz znakova
- Jednostavne za implementaciju i korištenje
- Najstariji mehanizam autentifikacije
  - Prva upotreba na računalima u operacijskom sustavu CTSS za prijavu
- Lozinke se upotrebljavaju i u procesima
  - Primjerice, Web aplikacija koja se spaja na bazu

# Provjera ispravnosti lozinke

- Protokol u načelu ima sljedeći oblik
  1. Korisnik upiše korisničko ime i lozinku
  2. Oba se dostave poslužitelju (ili poslužiteljskom procesu)
  3. Poslužitelj uspoređuje dostavljenu verziju i pohranjenu verziju  
Ako su verzije iste, tada je korisnik (osoba) dokazala da je vlasnik korisničkog imena

**Napomena: Ne raditi to na ovaj način**

# Ranjivosti i prijetnje na sigurnost lozinki

- Niska razina slučajnosti i kompleksnosti (ranjivost)
  - omogućava napade pogađanjem grubom silom (engl. brute-force) ili napadi na temelju rječnika (engl. dictionary based-attacks)
- Upotreba iste lozinke na više raznih mjesta (ranjivost)
- Krađa lozinki (prijetnja)
  - Korisnici zapisuju lozinke na mjesta koja nisu zaštićena (ranjivost)
  - Snimanje što korisnik upisuje (engl. shoulder surfing) (prijetnja)
  - Krađa pohranjenih lozinki s poslužitelja (prijetnja)
- Presretanje/krađa lozinki tijekom prijenosa (prijetnja)
- Sustav obnavljanja lozinki (engl. password reset)

# Primjeri incidenata s lozinkama

- LinkedIn: 2012 godine provaljeno te ukradeno 6.5 milijuna e-mail adresa
  - 2016 godine otkriveno još 100 milijuna
- Yahoo!: sveukupno u 2013. i 2014. oštećeno 3 milijarde korisničkih računa
  - Otkriveno tek 2016 godine



# Smanjenje ranjivosti lozinki

- Ispravno ih pohranjivati
- Trebaju biti odgovarajuće kompleksnosti i često se mijenjati
- Spriječiti pogađanje
- Korisnik ih ne smije dijeliti s nikim više te koristiti jedinstvene lozinke za svaku uslugu
- Tijekom unosa paziti da ih netko ne otkrije
- Zaštititi tijekom prijenosa

# Sigurna pohrana lozinki (1)

- Problem je ako napadač dohvati datoteku s lozinkama, onda je kompromitirao sve lozinke
  - Cilj je spriječiti da se to desi
  - To je itekako realna prijetnja s kojom obavezno treba računati!
- Ispravna pohrana znači
  - Svakoj lozinki se dodaje slučajna vrijednost (salt, seed)
  - Slučajna vrijednost i lozinka se propuštaju kroz kriptografsku funkciju sažetka
  - Na disk se pohranjuju slučajna vrijednost i rezultat kriptografske funkcije sažetka
    - Poznavanje slučajne vrijednosti ne olakšava pogađanje lozinke

# Sigurna pohrana lozinki (2)

- Ako sada napadač dođe do datoteke s lozinkama ne može vidjeti lozinke
  - Preostaje mu samo pogađanje!
- Pogađanje znači da treba pretpostaviti koja je lozinka te obaviti izračunavanje sažetka
  - Ne mora se nužno koristiti samo grubom silom, može imati određene pretpostavke o izgledu lozinki
- Slučajna vrijednost onemogućava dvije stvari
  - Ista lozinka ima isti zapis u bazi
  - Napad korištenjem tzv. Rainbow tables

# Sigurna pohrana lozinki (3)

- Moramo modificirati protokol autentifikacije zbog uvedene zaštite
  1. Korisnik upiše korisničko ime i lozinku
  2. Oba se dostavljaju poslužitelju (ili poslužiteljskom procesu)
  3. Poslužitelj za korisnika dohvaća sald/seed te izračunava sažetak lozinke i salta/seeda
  4. Uspoređuje izračunatu vrijednost i pohranjenu vrijednost
  5. Ako su verzije iste, tada je korisnik (osoba) dokazala da je vlasnik korisničkog imena

# Sprečavanje pogađanja lozinki (1)

- Pogađanje može biti on-line ili off-line
  - On-line
    - Napadač se pokušava prijaviti
  - Off-line
    - Imamo kopiju lozinki zaštićenih metodom koju smo opisali
- Obje vrste napada otežavamo ako su lozinke minimalne određena kompleksnost
  - Odnosi se na broj znakova, skup znakova iz kojeg se kreira lozinka, minimalan broj različitih vrsta znakova
  - Također, lozinke ne smiju biti kombinacija riječi iz rječnika
  - Niti bi trebale biti već kompromitirane lozinke!

# Sprečavanje pogađanja lozinki (2)

- Točni parametri ovise o okruženju i resursu koje lozinka štiti
  - Ispod 8 znakova nikako ne bi trebalo ići!
- Forsiranje lozinki određene minimalne kompleksnosti je **dobra praksa** i zbog toga podložna debatama
  - U osnovi ne smije se ići u ekstreme

# Sprečavanje on-line pogađanja

- Kako bi se spriječili pokušaji pogađanja lozinke često se uvode dva dodatna ograničenja:
  - Nakon svakog neuspjelog pokušaja upisivanja lozinke povećava se vrijeme čekanja
  - Nakon određenog broja neuspjelih pokušaja korisnik se blokira, korisnički račun se zaključava, generira se upozorenje vlasniku sustava
    - Ovo može omogućiti DoS napad na korisnika!
- Rezultat dodatnih ograničenja je da je jako smanjen broj pokušaja u jedinici vremena
  - Uz dodatne promjene lozinki smanjujemo vjerojatnost njihova pogađanja

# Alati za pogađanje lozinki

- THC Hydra
  - <https://securitytutorials.co.uk/brute-forcing-passwords-with-thc-hydra/>
- John The Ripper
  - <https://www.openwall.com/john/>
- Hashcat
  - <https://hashcat.net/hashcat/>



# Periodička promjena lozinki

- Periodički se traži promjena lozinke
  - Period promjene ovisi o okruženju i resursu koji se štiti
  - U dosta slučajeva ne dozvoljava se korištenje starih lozinki
- Ideja promjene lozinki je da
  - Ako vam je lozinka kompromitirana, smanjuje se prozor u kojemu napadač nešto može učiniti
  - Ako je napadač došao do kopije zaštićene lozinke kada otkrije lozinku, ona više ne vrijedi
- U slučaju sumnje da je lozinka kompromitirana obavezno mijenjati lozinku
  - U tvrtkama administrator može forsirati zamjenu lozinke

# Zaboravljene lozinke

- Za očekivati je da će ljudi zaboravljati lozinke
- U ograničenim sredinama (tvrtka) moguće je to riješiti tako da se djelatnik javi na helpdesk/administratoru
  - Na Internetu takav način ne funkcionira
- Često se u raznim aplikacijama na Internetu ugrađuje mogućnost resetiranja lozinke
  - Treba biti jako oprezan s tim mehanizmom kako se ne bi omogućilo napadaču da resetira korisničku lozinku
  - Zanimljivost: **Ako se desi da kada aktivirate reset lozinke na mail dobijete čistu lozinku onda znači da zaštita lozinki nije implementirana ispravno!**

# Prijenos lozinke preko mreže

- U načinu provjere lozinke postoji potencijalna ranjivost
  - Ako mjesto gdje korisnik upisuje lozinku i mjesto gdje se provjerava lozinka nisu na istom računalu
  - Napadač može snimiti lozinku i na taj način narušiti njenu sigurnost
  - Općenito, treba voditi računa može li napadač „upasti” u komunikacijski kanal
- Rješenje tog problema je izazov-odgovor način provjere (challenge, response)
  - Međutim, za korištenje ovog načina provjere na poslužitelju lozinke moraju biti pohranjene u čistom tekstu, ili se mora koristiti reverzibilna zaštita

# Izazov odgovor način provjere

- Protokol provjere ispravnosti lozinke:
  1. Poslužitelj šalje slučajan broj (nonce) na klijent
  2. Korisnik upisuje korisničko ime i lozinku
  3. Klijent slučajan broj i lozinku propušta kroz funkciju sažetka
  4. Korisničko ime i rezultat funkcije sažetka se šalju na poslužitelj
  5. Poslužitelj na temelju korisničkog imena dohvaća pohranjenu lozinku te izračunava funkciju sažetka na temelju lozinke i slučajnog broja kojeg je poslao klijentu
  6. Ako je izračunata vrijednost ista kao i primljena verzija autentifikacija je uspješna

**Napomena: Ovo je koncept i nemojte to koristiti u ovom obliku u praksi!**

# Upravljanje lozinkama

- Lozinke se danas upotrebljavaju na mnogim mjestima
  - Jako je teško stalno generirati kvalitetne lozinke te ih pamtit
- Rješenje je u vidu aplikacija pod nazivom “password managers”
  - Omogućavaju pohranu lozinki
  - Nude generiranje kvalitetnih lozinki
  - Mogućost automatskog upisivanja lozinki u razne aplikacije (primjerice, Web preglednici)

# Dijeljene tajne i fraze

- Varijacije na temu lozinki s kojima dijele i određene ranjivosti
- Dijeljene tajne (engl. Shared secrets)
  - Služe za međusobnu autentifikaciju – i jedna i druga strana dokazuju poznavanje dijeljene tajne
- Fraze (engl. Passphrases)
  - Dvije razlike u odnosu na lozinke
    - Značajno su dulje (rečenice i slično); uz njih nije vezano korisničko ime

# Jednokratne lozinke

- One-Time Passwords (OTP)
- Najčešće broj od 4 i više znamenki koji se generira po nekom poznatom algoritmu
  - Algoritam se inicijalizira početnim slijednim brojem koji mora biti tajna
- Postoje standardizirani algoritmi – ne bi trebalo izmišljati svoje!
  - TOTP – RFC6238, HOTP – RFC4226

# Implementacije jednokratnih lozinki

- Sklopovski tokeni – primjerice, za internet bankarstva raznih domaćih banaka
- Mobilna aplikacija
- Program na računalu/poslužitelju



# Lozinke i dvo-faktorska autentifikacija

- Kako bi se poboljšala sigurnost lozinki sve češće omogućava ili forsira dodavanje drugog faktora autentifikacije
  - Najčešće je u pitanju PIN koji generira nezavisna aplikacija
- Ponekad je drugi faktor PIN koji se šalje nekim drugim kanalom (mail, SMS)
  - Za sigurnost jako je bitno da je taj drugi kanal nezavisan od kanala kojim se šalje lozinka!
- Preporuka je za bilo što kritičnije da si omogućite 2FA bez obzira što vas se ne forsira na to

# Pametne kartice

- Kategorija ono što imamo (kartica) i ono što znamo (PIN)
  - Dvofaktorska autentifikacija
  - Karticu je potrebno „otključati” korištenjem PIN-a
- Temelj za autentifikaciju su privatni i javni ključevi
  - Privatni ključ se nalazi na kartici i nikada ne izlazi van, javni ključ je svima poznat
  - Kartica potpisuje nekakve podatke te na taj način imamo jamstvo da korisnik ima karticu i zna PIN
- Primjeri
  - Nove osobne iskaznice, kartice za poslovna internet bankarstva

# Biometrijske metode

- Kategorija “Ono što jesi” autentifikacije
- Koristi se jedinstvenim biološkim karakteristikama
  - Otisak prsta, slika lica, slika rožnice, stil tipkanja, otisak dlana, ...
- Sve popularnije zbog jednostavnosti za korisnika
- Problematici u slučaju krađe autentifikacijskih podataka
  - Primjerice, ako je ukraden otisak prsta nemoguće ga je zamijeniti
  - Problemi sa privatnošću

# Autorizacija (1)

- Nakon što je korisnik identificiran utvrđuje se pravo korisnika da provede nekakvu operaciju nad nekim resursom
- **Procesom autorizacije** se određuje da li SUBJEKT može obaviti OPERACIJU nad OBJEKTOM.
  - Primjeri
    - Datoteka je objekt, operacija je čitanje
    - Tablica u bazi je objekt, operacija je pretraživanje

# Autorizacija (2)

- **Subjekti** su korisnici, odnosno, procesi koji djeluju u ime korisnika
  - Subjekti mogu biti grupirani u grupe
- Koji **objekti** i **dozvole** postoje ovise o aplikaciji i onima koji su je razvijali
  - Tijekom planiranja razvoja aplikacije potrebno je definirati objekte i dozvole
    - Detaljni objekti i dozvole – velika fleksibilnost, ali i kompleksnost
    - „Grubi” objekti i dozvole – mala fleksibilnost, ali i mala kompleksnost

# Autorizacija bazirana na dozvolama

- Objekt za svaki subjekt ima definirano može li obaviti pojedinu operaciju
  - Ako subjekt koji želi obaviti operaciju nije za nju naveden u popisu onda se donosi podrazumijevana (default) odluka – **dobra praksa je da je to odbijanje provođenja operacije**
  - Često se to korisniku predstavlja kao lista pa govorimo o **pristupnim listama** (engl. access control lists)
- Dodavanje/uklanjanje dozvola svodi se na modifikaciju odgovarajućih struktura podataka

# Autorizacija bazirana na ulogama

- U praksi je puno veću fleksibilnost i upravljivost pokazala metoda autorizacije bazirana na ulogama (engl. role based access control, RBAC)
- Prava se grupiraju u uloge, a uloge se dodjeljuju subjektima
  - Jedan subjekt može imati više uloga
  - Pojedina dozvola može se nalaziti u više uloga
  - Pojedina uloga može se dodijeliti jednom ili više subjekata
- Ideja je da uloge reflektiraju nečiju funkciju

# Hvala!