Informaciona bezbednost

Identifikacija i autentifikacija

dr Milan Stojkov

Katedra za informatiku

2022.

Fakultet tehničkih nauka
Univerzitet u Novom Sadu

Identifikacija ≠ autentifikacija ≠ autorizacija

- Identifikacija je proces pripisivanja ID-a čoveku ili drugom računaru ili mrežnoj komponenti
- Autentifikacija je proces provere identiteta
- Autorizacija je utvrđivanje prava koja korisnik ima nad resursima u sistemu

Identifikacija ≠ autentifikacija ≠ autorizacija

- Autorizacija zahteva uspešnu autentifikaciju
  - Autentifikacija prethodi autorizaciji
- Autentifikacija podrazumeva identifikaciju
  - Identifikacija je sastavni deo postupka autentifikacije

Učesnici u autentifikaciji

- Onaj koji se predstavlja kao korisnik (**prover**, claimant)
- Onaj koji proverava identitet (**verifier**, recipient)

Protokol za autentifikaciju

- Proces u realnom vremenu kojim se utvrđuje identitet
- Rezultat:
  - Korisnikov identitet je autentičan
  - Korisnikov identitet nije autentičan
- Karakteristike protokola za autentifikaciju
  - Zanemarljiva verovatnoća da treći učesnik, predstavljajući se kao prover, može da navede verifiera na pozitivan rezultat autentifikacije
  - Verifier ne može da koristi informacije koje je dostavio prover kako bi se predstavio kao prover trećem učesniku

Četiri principa autentifikacije

- Autentifikacija identiteta se može ostvariti na četiri načina:
  - Nešto što znam (lozinka)
  - Nešto što imam (tokeni - fizički ključevi, smart kartice)
  - Nešto što jesam (statička biometrija - otisak prsta, lica, irisa)
  - Nešto što radim (dinamička biometrija - prepoznavanje glasa, potpisa)

Četiri principa autentifikacije

- U svakom pristupu, pretpostavka je da niko drugi osim ovlašćenog korisnika nema pristup lozinki ili tokenu i da je verovatnoća simulacije biometrijskih podataka prihvatljivo mala
- Ove metode se mogu kombinovati
- Npr. lozinke se često kombinuju sa tokenima ili biometrijom da obezbede jaču autentifikaciju nego što je to moguće jednim pristupom
  - Npr. dvofaktorska autentifikacija se javlja kod interakcije sa bankomatom (ATM)
  - Posedovanje kartice (tokena) i poznavanje ličnog identifikacionog broja (PIN, koji odgovara lozinki) su obavezni da pristup bankovnom računu korisnika

Nešto što znam

- Potvrda autentifikacije zasnovana na lozinki je najzastupljenija
- Iako je često loše administriran i nesiguran (i frustrirajući) pristup za korisnike i administratore, lozinke mogu biti čuvane i korišćene mnogo sigurnije i praktičnije nego što jesu
- Mnogi eksperti za bezbednost su godinama predviđali da će lozinke na kraju povući iz upotrebe, da će biti zamenjene tokenima ili biometrijskim podacima, ali danas postoji konsenzus da lozinke verovatno neće uskoro nestati i da će i dalje biti dominantna tehnika autentifikacije u godinama koje dolaze
- Demonstriranje poznavanja lozinke ne potvrđuje direktnu autentičnost korisnika
- To jednostavno potvrđuje poznavanje lozinke
- Neovlašćeno znanje ili pogađanje lozinke može dovesti do lažnog predstavljanja jednog korisnika od strane drugog (*spoofing*)
- Krađu lozinke može biti teško otkriti jer nije materijalna imovina

Nešto što imam

- Autentifikacija zasnovana na posedovanju tokena koristi se tamo gde se želi veća sigurnost identiteta nego što je to moguće pomoću lozinki
- Tajna koju sadrži token može biti duža i nasumičnija od lozinke koju korisnik mora da zapamti
- Kao i kod lozinki, posedovanje tokena ne potvrđuje direktnu autentičnost korisnika nego potvrđuje posedovanje tokena i mogućnost njegovog korišćenja
- Sve više se koristi u kombinaciji sa lozinkom, čime se uspostavlja dvofaktorska autentikacija
- Teorija je da zahtev da se imaju oba elementa smanjuje verovatnoću za *spoofing*
- Izgradnja isplativih i bezbednih sistema za generisanje tokena iz kojih se tajna ne može izvući brute-force napadima pokazala se mnogo težim nego što se u početku očekivalo i lozinke i dalje ostaju jeftinija opcija za implementaciju

Nešto što imam

- Moderni tokeni su obično u nekom hardverskom uređaju koji ima sposobnost za izračunavanje tokena. Primeri uključuju:
  - Uređaji veličine kreditne kartice sa LCD ekranom koji prikazuju pseudoslučajne brojeve
  - LCD uređaji u obliku priveska za ključeve (*key fob*) koji koriste iste algoritme kao i uređaji u obliku kreditnih kartica
  - Hardverski uređaji koji se nazivaju *dongle* koji se uključuju u ulazno-izlazne portove na računarima (npr. USB dongle, interfejsi PC-kartica)
  - Soft tokeni koji se nalaze u aplikacijama na telefonu, tabletu

Contact VS Contactless

- Svi tokeni koji se koriste za autentifikaciju računara zahtevaju softver za obradu informacija
- Najznačajnija razlika je da li tokeni zahtevaju elektronski kontakt sa sistemom za autentifikaciju
- Beskontaktni tokeni su lakši za korišćenje jer ne zahtevaju specijalizovane čitače
- Kontaktni tokeni poput smart kartica zahtevaju postojanje hardverskog čitača
- Beskontaktni tokeni su ograničeniji u funkciji od kontaktnih tokena
  - Na primer, kontaktni token može da se koristi za kreiranje digitalnih potpisa, dok beskontaktni token to ne može (npr. lična karta)

Nešto što jesam

- Statičkom biometrijom se podrazumeva karakteristika osobe kao što je otisak prsta, geometrija ruke ili iris oka ili čak DNK korisnika ☺
- Verovatnoća da dve osobe imaju identične karakteristike je izuzetno mala
- Biometrija zahteva specijalizovane i skupe čitače da prikupi biometrijske podatke, što otežava široku primenu

Nešto što jesam

- Biometrija takođe pati od replay i tempering napada
- Zato biometrijski čitač mora biti pouzdan i dobro zaštićen
  - Ovo smanjuje verovatnoću da napadač dođe u posed ulaznih podataka i reprodukuje ih kasnije, ili kreira lažne biometrijske profile
  - Biometrijski podaci moraju biti preuzeti u blizini korisnika kako bi se smanjila verovatnoća zamene
  - Ako se podaci prenose na udaljeni server radi autentifikacije, prenos zahteva bezbedan protokol, gde će poruke imati timestamp i kratak period validnosti podataka

Nešto što radim

- Dinamička biometrija obuhvata dinamičke aktivnosti a ne statičke karakteristike korisnika
- Npr. dinamika potpisa uključuje praćenje brzine i ubrzanja ruke osobe pri potpisivanju na posebnoj tabli za pisanje
  - Umesto samo oblika potpisa, prate se i dinamičke karakteristike kretanja tokom pisanja kojima se potvrđuje autentičnost osobe (pokreti koje je izuzetno teško simulirati)
- Druga mogućnost je da se prepoznaju karakteristike glasa osobe kada naglas čita neki tekst
- Treća mogućnost je praćenje dinamike pritiska tastera pri kucanju
- Četvrta mogućnost je praćenje dinamike hoda osobe

Klasifikacija šema za autentifikaciju

- Slabe (*weak*) šeme
  - Jednostavne za implementaciju
  - Podložne napadima
  - Npr. lozinka, PIN
- Jake (*string*) šeme
  - Zasnovane na challenge-response protokolu
  - Obuhvataju kriptografske tehnike

Password-based authentication

- Najraširenij metod za autentifikaciju
- Lozinka ~ tajni ključ
- Postupak:
  - korisnik se prijavljuje pomoću para (korisničko ime, lozinka)
  - server proverava da li dati par postoji u registru postojećih korisnika
- Registar = sistemski fajl, zaštićen od čitanja
- Ako se lozinka smešta direktno u sistemski fajl, nema zaštite od privilegovanih korisnika sistema ili čitanja fajla iz bekapa

Password-based authentication

- Jedna od najopasnijih praksi koja se danas koristi je skladištenje nešifrovanih korisničkih lozinki koje su dostupne administratorima sistema
- Negde novi korisnici dobijaju lozinke koje im dodeljuju administratori sistema
  - Ako se koristi ovaj pristup, ove lozinke treba koristiti samo jednom, za početno prijavljivanje, nakon čega korisnik mora biti primoran da promeni lozinku
  - Često administratori čuvaju na papiru?! lozinke korisnika za brzi pristup kada korisnici zaborave svoje lozinke
  - Ovim se poništava bitna karakteristika koju identifikacija i autentifikacija treba da obezbede – neporecivost (*nonrepudiation*)
  - Ovo je teško je osporiti, posebno na sudu koji npr. razmatra optužbu za zloupotrebu od strane ovlašćenog korisnika te lozinke

Password-based authentication

- Možda najveći rizik kod korišćenja lozinki je da se mogu ukrasti bez znanja korisnika
- Posmatranje nekoga tokom ukucavanje lozinke je dovoljno i ovo se može desiti bez eksplicitnog znanja žrtve
- Sličan rizik je otkrivanje lozinke napadaču koji ubeđuje legitimnog korisnika da otkrije lozinku predstavljajući se kao administrator sistema kome je potrebna lozinka da bi učinio nešto korisno za korisnika
- Gubitak lozinke može se otkriti samo ako se otkrije njegova zloupotreba ili pronađe u npr. *dumpu* spiska lozinki koje su razbijene korišćenjem programa za razbijanje lozinki (korišćenjem *dictionary* napada)

Password-based authentication

- Veliki rizik je i deljenje lozinki (Netflix ☺)
- Osnovni uzrok zašto se ovo dešava unutar organizacije je nedostatak efikasnog mehanizma kojim se mogu delegirati odabrane privilegije jednog korisnika drugom za deljenje lozinke
- Jedan od načina da se spreči deljenje bi mogao da bude da se veže lozinka sa nekom osetljivom informacijom korisnika (npr. broj kreditne kartice) i u slučaju *leak-a* da se sve informacije objave
- Još jedan način bi bio da se kreiraju one-time lozinke (tokeni) koji se menjaju u nekom kratkom vremenskom intervalu i koji se vezuju za tačno jednog korisnika

Password-based authentication

- Korisnici imaju tendenciju da ponavljaju istu lozinku na više servisa
- Ako se kompromituje korisnička lozinka na jednom servisu koji ima lošu zaštitu (najslabija karika u lancu) to može dovesti do preuzimanja naloga korisnika na drugim servisima
- Ovde su bitni edukacija i podizanje svesti korisnika
- Korišćenje *password manager*-a koji će generisati i čuvati različite lozinke (KeePass, LastPass, Dashlane, Bitwarden, 1Password,...)
  - Ovde treba voditi računa o bezbednosti master lozinke
- Korišćenje sertifikata umesto lozinki

Password-based authentication

- Sistemi za autentifikaciju su podložni *guessing* napadima
- Obično se dešava da korisnici imaju lako pamtljive lozinke koje su nekako povezane sa korisničkim imenom, čestim rečima, porodicom, prijateljima, kućnim ljubimcima, itd.
- Posebna kategorija loših lozinki je podrazumevana (*default* ili kanonska) lozinka koja nije promenjena pri prvom logovanju
- Zaštita podrazumeva definisanje minimalne kompleksnosti lozinke koja treba da uključi velika i mala slova, brojeve, specijalne karaktere
- Kompleksna lozinka nije garancija da se *guessing* napad ne može desiti, ali tu može pomoći logovanje podataka o samoj autentifikaciji za potrebe dalje detekcije da li je došlo do zloupotrebe
- Dodatna zaštita može biti forsiranje pravila da postoji n pokušaja unosa pogrešne lozinke pre nego što se zaključa nalog
  - Ovo može dovesti do *Denial of Service* (DoS) u slučaju *brute-force* napada
  - Umesto zaključavanja naloga zauvek, može se zaključati na n minuta

Password-based authentication

- Primer *offline* napada na sisteme koji koriste lozinke kao vid autentifikacije je napad rečnikom (*dictionary attack*)
- Takvi napadi počinju kopiranjem datoteke sa lozinkama na računar koji je pod kontrolom napadača
- Datoteka lozinki obično koristi jednosmernu enkripciju (*one-way*) koja omogućava sistemu da šifrira unetu lozinku i uporedi je sa šifriranom formom originalne lozinke i traži podudaranje
- Napad rečnikom je poznat kao *offline* jer napadač priprema sve što je potrebno za izvršenje napada unapred bez kačenja na ciljanu mrežu
- Mitigacija: ne čuva se lozinka, već njen heš sa *salt* vrednošću
  - *Salt* - slučajan niz znakova koji se dodaje na lozinku pre izračunavanja heša
  - Salt i heš se smeštaju u fajl
  - Napad na konkretnu lozinku traži heširanje kompletnog rečnika za dati salt
- Fun fact - Windows čuva lozinke u registry-ju u otvorenom tekstu ☺

Password-based authentication

- Još neki tipovi napada:
  - Napadi sa ponovljenim porukama (replay attacks)
    - Napadač prisluškuje komunikaciju u toku autentifikacije i ponavlja je
    - Npr. ako nalog za plaćanje potpiše pravi korisnik banke, a napadač ponavo šalje istu poruku banci (time ponavlja plaćanje)
    - Anti-replay mere - dodavanje timestamp, slučajnog broja, itd.

Password-based authentication

- Još neki tipovi napada:
  - Napadi sa uvođenjem kašnjenja (forced delay attacks)
    - Napadač presretne poruku, sačeka određeni period vremena, i prosledi je na odredište
    - Korisnik dobije timeout, misli da je transakcija otkazana, a ona je stigla na odredište
    - Mere zaštite - dodavanje slučajnih brojeva i redukovani vremenski prozori

Password-based authentication

- Ako se lozinka prenosi u izvornom obliku (*plain text*) od klijenta do servera, podložna je čitanju komunikacije (*password sniffing*)
- Mnogi sistemi zahtevaju slanje lozinke serveru u izvornom obliku
- Neki zahtevaju prenos heša lozinke (obično bez salt-a)
  - Heš je dovoljan za dictionary napad osim ako se salt ne koristi i čuva na bezbednom mestu
  - Napadač ne mora čak ni da dođe do lozinke, već može ponovo da prosledi samo heš lozinke kada je to potrebno

Jake šeme za autentifikaciju

- Challenge-response princip
  - Korisnik potvrđuje svoj identitet tako što demonstrira poznavanje tajne informacije
- Ako poznaje tajnu informaciju, smatra se da je autentičan
  - Pri tome se tajna informacija ne odaje sistemu
- Sistem korisniku šalje podatak koji se menja tokom vremena koji može da uključuje:
  - Timestamp
  - Random number
  - Sequence number
- Korisnik izračunava odgovor na osnovu dobijenog podatka i tajne informacije
- Ako je odgovor ispravan, sistem smatra da je korisnik autentičan

Jake šeme za autentifikaciju

- Realizacija challenge-response postupka pomoću:
  - Kriptosistema sa tajnim ključem
  - Kriptosistema sa javnim ključem
  - *Zero-knowledge* tehnika

Challenge-response sa tajnim ključem

- Korisnik i sistem dele tajni ključ i unapred dogovoreni simetrični algoritam
- Postupak:
  1. Sistem šalje korisniku slučajan broj r
  2. Korisnik šifruje r tajnim ključem i šalje ga sistemu
  3. Sistem dešifruje r i proverava da li je jednak originalnom
- Broj r koji se šifruje može se dopuniti proizvoljnom porukom m, kako bi se sprečili replay napadi
- Ako je dodatna poruka dugačka, može se šifrovati heš od $[r, m]$

Challenge-response sa tajnim ključem

- Moguća je i obostrana autentifikacija
  - Sistem šalje korisniku slučajan broj r
  - Korisnik šalje poruku koja se sastoji iz šifrovanog broja r (tajnim ključem) i novog slučajnog broja r'
    - Ako se dešifrovanjem dobije originalni broj r korisnik je autentičan
  - Sistem šalje korisniku šifrat broja r'
    - Ako se dešifrovanjem dobije originalni broj r' sistem je autentičan

Challenge-response sa javnim ključem

- Postupak:
  1. Sistem generiše slučajan broj r, računa njegov heš $h(r)$, šifruje r i proizvoljnu poruku m korisnikovim javnim ključem $c(r, m, pk)$ i šalje korisniku $[h(r), c(r, m, pk)]$
  2. Korisnik dešifruje šifrovani deo poruke (time dobija r), izračunava svoj heš $h(r)$ i poredi ga sa primljenim, ako su jednaki, šalje r sistemu
  3. Sistem proverava da li je primljeni r jednak originalnom

Password-based authentication

- Jedan pristup za mitigaciju za *password sniffing* je upravo korišćenje javnog ključa servera za šifrovanje bilo kog prenosa informacija vezanih za lozinku na server
  - Samo server može da dešifruje informacije koristeći svoj privatni ključ
  - Secure Shell (SSH) i Secure Sockets Layer (SSL) ovo rade
    - *Server-side mode* zahteva da server ima sertifikat
    - *Client-side mode* zahteva da i klijent ima sertifikat
- Alternativni pristup je izbegavanje prenošenja lozinke i korišćenje protokola koji zahteva samo poznavanje lozinke da bi se uspešno pokrenuo (Kerberos)

Password-based authentication

- Vremenom su osmišljeni protokoli koji se baziraju na ideji da dve strane mogu da demonstriraju da znaju lozinku bez da je obznane
- Takvi protokoli se zovu *zero-knowledge password proofs*
- Ove metode zavise od mogućnosti da obe strane nezavisno odaberu isti broj ali bez znanja koji je konkretan broj
- Npr. Fiat-Shamir algoritam

Password-based authentication

- Jedan popularan konceptualni model ovog procesa radi na sledeći način:
  1. Dve strane žele da testiraju da li dele isti broj (recimo između 1 i 10, i u ovom primeru neka je to broj 3)
  2. Dve strane imaju špil od 10 karata
  3. Prva strana odbrojava do treće karte i stavlja oznaku na desnu ivicu te karte
  4. Špil karata se raspoređuje tako da druga strana može da označi levu ivicu karte, ali da ne vidi desnu ivicu
  5. Druga strana odbrojava do treće karte i obeležava levu ivicu
  6. Špil karata se meša tako da se izgubi redosled , a zatim se prikazuje obema stranama
  7. Ako jedna karta ima oznaku i na desnoj i na levoj ivici, onda dve strane dele isti tajni broj, ali nijedna nije morala da otkrije koji je to broj bio

Password-based authentication

- Još neki tipovi napada:
  - Napadi sa preplitanjem (interleaving attacks)
    - Napadač ubacuje lažne poruke u sklopu protokola da bi ga poremetio
    - Oracle session attack
    - Parallel session attack

Password-based authentication

- Oracle session attack
  - A i B koriste isti ključ
  - Napadač C se predstavlja kao A i počinje sesiju sa B slanjem neke šifrirane poruke $c(n_1)$
  - B odgovara sa dešifrovanom vrednošću n_1 i svojom šifriranom challenge porukom $c(n_2)$
  - C iskorištava tu šifriranu poruku da komunicira sa A koristeći ga kao *oracle* koji će dešifrovati i dobiti n_2
  - C prekida komunikaciju sa A i šalje $c(n_2)$ ka B

Password-based authentication

- Parallel session attack
  - Napadač presreće poziv od A ka B sa challenge porukom n_1, i izbacuje B iz komunikacije
  - Pretvara A u oracle protiv samog sebe
  - Pošto C ne može da odgovori na challenge poruku n_1, pretvara se da je B pokušavajući da započne paralelnu sesiju navodeći A da da ključ za tu sesiju

Password-based authentication

- Microsoft Windows kroz *Group Policy Object* (GPO) nudi mogućnost podešavanja pravila za lozinke i naloge
- Preporuke Centra za Internet bezbednost (CIS) su sledeće:
  - *Enforce Password History: 24*
  - *Maximum password age: 60 or fewer days*
  - *Minimum password age: 1 or more*
  - *Minimum password length: 14*
  - *Password must meet complexity: Enabled*
  - *Store passwords using reversible encryption: Disabled*

Password-based authentication

- Ako se uključi *Password must meet complexity* obezbeđuje se sledeće:
  - *Not contain the user's account name or parts of the user's full name that exceed two consecutive characters*
  - *Be at least six characters in length*
  - *Contain characters from three of the following four categories:*
    - *English uppercase characters (A through Z)*
    - *English lowercase characters (a through z)*
    - *Base 10 digits (0 through 9)*
    - *Non-alphabetic characters (for example, !, $, #, %)*

Alternativni pristupi

- Jednokratne lozinke
  - Prilikom svakog prijavljivanja koristi se različita lozinka
- Naredna lozinka se određuje pomoću liste unapred definisanih lozinki
  - Ne koriste se sekvencijalno već sistem traži i-tu lozinku iz liste
- Naredna lozinka se određuje pomoću sekvencijalnog ažuriranja
  - Nakon pozitivne autentifikacije korisnik će poslati lozinku za naredno prijavljivanje
  - Prva lozinka je unapred poznata
- Naredna lozinka se određuje pomoću sekvencijalnog izračunavanja
  - Prva lozinka je unapred poznata
  - Svaka sledeća lozinka je heš prethodne lozinke: $h(h(...h(pwd)...))$

SKEY postupak

- Korisnik unese slučajan broj R
- Sistem generiše $f(R) = x_1, f(f(R)) = x_2, ...f(f(...f(R)...)) = x_{100}$ i daje niz x_{1-100} korisniku, a skladišti i x_{101}
  - Prilikom prvog prijavljivanja korisnik šalje x_{100}, server izračunava $f(x_{100})$ i poredi ga sa x_{101}
  - Ako su jednaki, korisnik je pozitivno autentifikovan
    - Sistem zamenjuje x_{101} sa x_{100}
    - Korisnik za dalje prijavljivanje koristi poslednji neiskorišćeni broj iz niza
- svaki broj se koristi samo jednom, a f je jednosmerna funkcija
- napadač ako i pročita x_{101}, taj podatak mu ne znači puno

Token-based autentifikacija

- Autentifikacija zasnovana na tokenima oslanja se na nešto što korisnik poseduje a što se pretpostavlja da nijedan drugi korisnik nema ili ne može da pridobije
- Ova autentifikacija se može postići na mnogo načina:
  - Karticama za pristup
  - Karticama na kontakt
  - Smart karticama i *dongle* uređajima
  - *One-time password* generatorima
  - Soft(verskim) tokenima

Kartice

- Za postavku podataka na kartice mogu se iskoristiti optički bar kod, magnetna traka, čipovi koji čuvaju biometrijske podatke, itd.
- Kartice sa magnetnim trakama imaju dosta mana:
  - Ne mogu da čuvaju mnogo podataka
  - Lako se menjaju, kopiraju ili brišu podaci
- Kartice koje imaju metalne delove su efikasnije
- Kartice koje zahtevaju kontakt ili blisku udaljenost sa uređajem za čitanje koriste infracrvene i mikrotalasne zrake za prenos informacija

Smart kartice i dongle

- Smart kartice obično koriste PC čitač kartica umesto specijalizovanih čitača
- Dongle su ”smart kartice” koje se mogu očitati kroz USB portove (npr. YubiKey)
- Smart kartice imaju sopstvenu mogućnost obrade i obično čuvaju tajni ključ povezan sa korisnikom
- Često su potrebni lozinka ili PIN za pristup kartici, čime se obezbeđuje mogućnost dvofaktorske autentifikacije

Softverski tokeni

- Softverski tokeni ili soft tokeni su predloženi kao jeftinija alternativa za hardverske tokene
- Rani soft tokeni sastojali su se od tajnog ključa korisnika koji je šifrovan lozinkom i uskladišten na nekom prenosivom medijumu kao što je disketa
- Takva pristup je ranjiv na dictionary napade
- Fizički transport disketa i kasnije nedostatak flopi disk čitača doveli su do toga da se ovi tokeni čuvaju na serverima kako bi bili dostupni po potrebi
- Zaštita pristupu soft tokenima na serveru svodi se na probleme autentifikacije zasnovane na lozinki
- Neki noviji soft tokeni se oslanjaju na kriptografiju sa javnim ključem (PKI)

One-time password generatori

- Popularan oblik tokena gde se generiše one-time kombinacija 6-8 cifara koja se menja svaki put kada istekne vreme od poslednjeg korišćenja ili kada se pritisne fizičko dugme na uređaju
- Korisnik unosi svoj ID i trenutnu vrednost koju vidi
- Često se koristi kao drugi faktor za dvofaktorsku autentifikaciju
- Tokeni su zasnovani na korišćenju zajedničkih tajnih ključeva, tako da i token i server imaju zajedničku tajnu
- Server i token treba da se inicijalizuju i sinhronizuju da bi ova šema mogla da radi
- Najpopularniji proizvođač je RSA Security LLC, a uređaj SecurID

Autentifikacija pomoću mobilnih uređaja

- Jedan oblik *token-based* autentifikacije je i korišćenje mobilnih uređaja kao što su mobilni telefon ili tablet koji su sposobani da prime SMS poruke ili instaliraju specijalne aplikacije koje generišu kodove (Google Autehenticator, Microsoft Authenticator)
- Tokom prijavljivanja korisnik dobija jednokratni kod za ulazak na web sajt
- Često se koristi kao drugi faktor za dvofaktorsku autentifikaciju

Biometrijska autentifikacija

- Predstavlja automatsku identifikaciju osobe na osnovu njenih fizioloških karakteristika ili ponašanja
- Dok tokeni i smart kartice autentifikuju korisnika na osnovu nečega što korisnik poseduje, a lozinke potvrđuju autentičnost korisnika na osnovu onoga što korisnik zna, biometrija omogućava autentifikaciju i proveru identiteta na osnovu toga ko je korisnik
- Iako su početni troškovi prilično visoki, implementacija biometrijskih sistema obično rezultuje mnogo nižim administrativnim troškovima od drugih pristupa zbog manjeg broja poziva za tehničku podršku za resetovanje lozinki, nema potrebe za izdavanjem zamenskih smart kartica, itd.

Biometrijska autentifikacija

- Biometrija treba da zadovolji četiri zahteva prema autorima Jain i Bolle, Connell, Pankanti, Ratha i Senior:
  - Univerzalnost (*Universality*) - svaka osoba treba da ima biometrijske karakteristike
  - Jedinstvenost (*Uniqueness*) - dve osobe ne bi trebalo da budu iste u pogledu biometrijskih karakteristika
  - Permanentnost (*Permanence*) - biometrijski podaci bi trebalo da bude relativno nepromenljivi u određenom vremenskom periodu
  - Naplativost/Prikupljivost (*Collectability*) - biometrijska karakteristika bi trebalo da se može izmeriti

Biometrijska autentifikacija

- Primarna upotreba biometrije se može podeliti u četiri kategorije:
  - Logički pristup sistemu
  - Fizički pristup sistemu
  - Obezbeđivanje jedinstvenosti korisnika
  - Sistem javne identifikacije

Logički pristup sistemu

- Logički pristup sistemu podrazumeva nadgledanje, ograničavanje ili odobravanje pristupa podacima ili informacijama
- Primeri uključuju pristup računaru, mreži ili nalogu
- U ovim sistemima biometrija zamenjuje ili dopunjuje PIN-ove, lozinke i tokene
- Najčešći pristup je korišćenje otiska prsta sa USB priključkom ili sa čitačem ugrađenim u laptop
- Proizvođači ugrađuju *Trusted Platform Module* (TPM) u nove laptopove da podrže različite kriptografske aplikacije
- U kombinaciji sa biometrijskim uređajima kao što su čitači otiska prsta, TPM čip može da dozvoli aplikacijama poput *Microsoft BitLocker*-a da primeni biometrijske kontrole pristupa na šifrovanim diskovima

Fizički pristup sistemu

- Fizički pristup sistemu podrazumeva nadgledanje, ograničavanje ili odobravanje kretanja osobe u ili iz određenog područja
- U ovim sistemima, biometrija zamenjuje ili dopunjuje ključeve i kartice koje dozvoljavaju ovlašćenim licima pristup prostorijama, trezorima, itd.
- Ovakvi sistemi se često postavljaju na aerodromima, bezbednosnim kontrolnim punktovima i graničnim objektima u cilju nadgledanja i ograničavanja kretanja neovlašćenim ili sumnjivim licima
- Pored kontrole ulaska u prostorije ovi sistemi često uključuju i sisteme za praćenje vremena i evidentiranje prisustva (npr. na poslu)

Obezbeđivanje jedinstvenosti korisnika

- Biometrijski sistemi se obično fokusiraju na sprečavanje dvostrukog upisa u aplikacije, kao što je program socijalnih davanja
- Glavna upotreba ove aplikacije se javlja u javnom sektoru, iako bi se slični sistemi mogli primeniti kako bi se sprečio dupli upis u programe beneficija zaposlenih

Sistem javne identifikacije

- Biometrija se može koristiti za potrebe za identifikaciju kriminalaca i terorista

Prikupljanje podataka

- Biometrijski podaci korisnika se inicijalno prikupljaju i izdvaja se skup karakteristika iz dobijenih podataka i od njih se kreira šablon
- Za potrebe verifikacije ili identifikacije, korisnik predstavlja ponovo svoje biometrijske podatke, koji se zatim obrađuju i konvertuju u šablon koji se poredi sa šablonom u bazi

Tipovi biometrije

- Otisak prsta
- Prepoznavanje lica
- Prepoznavanje geometrije šake
- Skeniranje irisa (dužice)
- Prepoznavanje glasa

Tipovi grešaka

- *False Accept (false positive)* - verovatnoća, izražena u procentima, da će prevarant biti uparen sa validnom biometrijom korisnika (najvažnija metrika)
- *False Reject (false negative)* - verovatnoća da će šablon koji je kreiran na osnovu prezentovanih podataka korisnika biti pogrešno procenjen da ne odgovara njegovom šablonu iz baze
- *Crossover Error Rate (CER)* ili *Equal Error Rate (EER)* - predstavlja presek prva dva
  - Niži CER ukazuje da je biometrijski uređaj tačniji i pouzdaniji od drugog biometrijskog uređaja sa višim CER
- *Failure To Enroll (FTE)* - situacija u kojoj pojedinac nije u mogućnosti da upiše svoju biometriju kako bi se napravio šablon odgovarajućeg kvaliteta za naknadno automatizovan rad

Cena tehnologija za autentifikaciju

- Mišljenje je da je korišćenje bilo čega osim lozinki skupo i da su lozinke besplatne
- Analiza cene upravljanja lozinkama koja je sprovedena od strane RSA Security kompanije koja proizvodi SecurID tokene kaže da je potrebno oko $12 za kreiranje naloga po korisniku i oko $660 za upravljanje lozinkama (zamena zaboravljenih lozinki i resetovanje zaključanih naloga) tokom 3 godine
- Čitači otiska prsta mogu koštati $50 dok sistemi za prepoznavanje glasa koštaju i do $50.000
- Ispada da lozinke nisu besplatne ☺ i da su tokeni i biometrija alternative koje se možda mogu porediti po ceni