Kontrola pristupa: autentifikacija

Sadržaj

- Autentifikacija
- Lozinke
- Biometrija
- Nešto što posedujemo

Autentifikacija

- Kontrola pristupa se sastoji iz dva dela.
  - **Autentifikacija** – ko pristupa?
    - Određuje se kome je dopušten pristup.
    - Autentifikacija čoveka od strane mašine.
    - Autentifikacija mašine od strane mašine.
  - **Autorizacija** – da vam li je dozvoljeno da nešto uradite?
    - Ako vam je dozvoljen pristup, šta možete da uradite?
    - Obezbeđuje ograničenja na moguće akcije.

Autentifikacija

Ko pristupa?

- Autentifikacija predstavlja **binarnu odluku**.
  - Pristup je dozvoljen ili nije.
- Kako mašina može da autentifikuje čoveka?
- Autentifikacija može biti zasnovana:
  - Na nečemu što **znate**.
    - Npr. lozinke.
  - Na nečemu što **imate**.
    - Npr. smart kartica.
  - Na osnovu nečega **što jeste**.
    - Npr. otisak prsta.
  - Na osnovu nečaga što **možete**.
    - Npr. verifikacija govora.

Lozinke

Lozinke.

- “Idealan izbor”.
  - Nešto što znate.
  - Nešto što računar može jednostavno da proveri.
  - Nešto što “drugi” (relativno) teško može da pogodi.
- Lozinke – česta praksa.
  - Matični broj.
  - Majčino devojačko prezime.
  - Datum rođenja.
  - Ime vašeg kućnog ljubimca.
  - ...

Lozinke

Problemi sa lozinkama.

- “Lozinke su jedan od najvećih praktičnih problema sa kojima se susreću inženjeri sigurnosti danas.”
- “Ljudi ne poseduju sposobnost bezbednog memorisanja kriptografskih ključeva visokog kvaliteta, i imaju neprihvatljivu brzinu i tačnost u obavljanju kriptogrfskih operacija.”

Lozinke

Zašto lozinke?

- Zašto je “nešto što znam” popularnije od “nečeg što imam” i “nečeg što jesam”?
  - **Cena**:
    - Lozinke su besplatne.
    - Smart kartice i biometrijski uređaji nisu.
  - **Pogodnost**:
    - Jednostavnije je dodeliti/promeniti lozinku nego izdati i konfigurisati novu smart karticu.
    - Šta je sa biometrijskim podacima?

Lozinke

Ključevi i lozinke.

- Kriptološki ključevi:
  - Neka je ključ dužine 64 bita.
  - Tada postoji 2^{64} različitih ključeva.
  - Izabrati ključ slučajno.
  - Tada napadač mora da isproba oko $2^{64}/2 = 2^{63}$ ključeva.
- Lozinke:
  - Neka je lozinka dužine 8 karaktera.
  - Neka ima 256 različitih karaktera (ASCII).
  - Postoji: $256^8 = 2^{64}$ različitih lozinki.
  - Korisnici ne biraju lozinke slučajno.
  - Napadač mora da isproba daleko manje lozinki od 2^{63} (napad pomoću rečnika, *rainbow* tabela).

Lozinke

Dobre i lose lozinke.

- Loše lozinke:
  - frank, Fido, password, 4444, Pikachu, 161275 (datum rođenja), AustinStamp
- Dobre lozinke:
  - jfIej,43j-EmmL+y (problem: da li može da se zapamti?)
  - P0kem0N (da li je zamena jednog slova brojem težak izazov za napadača, ili je potrebno "produžiti" ovu kratku lozinku još nečim, npr. P204K6e8m0N?)
  - 0nceuP0nAt3m8 (lako se pamti, teško se pogađa)
  - 1B33r$1c50 (lako se pamti – osobito ako znate cenu piva, teško se pogađa)
  - ...

Lozinke

Eksperiment sa lozinkama.

- Postoje tri grupe korisnika – svakoj grupi je ponuđeno da izaberu lozinke na sledeći način:
  - Grupa A: najmanje 6 karaktera, da bar jedan nije slovo.
  - Grupa B: lozinka zasnovana na frazi (*passphrase*).
  - Grupa C: 8 slučajnih karaktera.
- Rezultati:
  - Grupa A: oko 30% lozinki je lako razbiti.
  - Grupa B: oko 10% lozinki se razbija.
    - Lozinke se lako pamte.
  - Grupa C: oko 10% se razbija.
    - Lozinke se teško pamte.

Lozinke

Eksperiment sa lozinkama.

- Korisnici slabo poštuju propisana pravila za izbor lozinki.
- U svakoj grupi, 1/3 nije poštovala uputstva (i oko 1/3 ovih se lako razbija!)
- Ponekad je najbolje dodeliti lozinke.
- Kako ih korisnici pamte?
- Ako lozinke nisu unapred dodeljene, najbolji saveti pri izboru su:
  - Izaberite lozinku zasnovanu na frazama.
  - Administrator treba da koristi alate za test slabih lozinki (Trudi sigurno hoće).
  - Zahteva se periodična zamena lozinki.
    - Korisnici to često zloupotrebljavaju: Tom $\rightarrow$ Tom01 $\rightarrow$ Tom02 $\rightarrow$ …

Lozinke

Napadi na lozinke.

- Napadač može:
  - Ciljati jedan odabrani nalog.
  - Ciljati bilo koji nalog u grupi.
  - Ciljati bilo koji nalog u celim sistemu.
  - Pokušati napad odbijanja servisa (*Denial of Service* – DoS).
- Uobičajeni redosled napada:
  - Spoljašnji korisnik $\rightarrow$ obični korisnik $\rightarrow$ administrator.
  - Potrebna je možda samo jedna slaba lozinka!

Lozinke

Uzastopno probijanje lozinki.

- Pretpostavimo da se sistem zaključa nakon 3 pogrešne lozinke.
- Koliko dugo treba da bude zaključan:
  - 5 sekundi,
  - 5 minuta, ili
  - dok sistem administrator ne obnovi servise?
- Šta su pozitivne, a šta negativne strane?
  - 5 sekundi – omogućava ciklične napade bez zastoja.
  - 5 minuta – otvara mogućnost DoS napada.

Lozinke

Verifikacija lozinki.

- Potreban je mehanizam za verifikovanje lozinki.
- Memorisanje lozinki u fajlovima je loše rešenje (očigledno).
- Kriptografsko rešenje: heš vrednost lozinke.
  - Zapisati $y = h(\text{lozinka})$.
  - Lozinka se može se verifikovati preko heš vrednosti.
- Ukoliko napadač dođe do fajla sa heš vrednostima, time nije dobio i same lozinke.
  - Može da pokuša da pogodi x za koje je $y = h(x)$.
  - Ako uspe, napadač je pronašao lozinku!

Lozinke

Verifikacija lozinki.

- Napad pomomoću rečnika (*dictionary attack*).
- Neka postoji rečnik uobičajenih lozinki.
- Neka napadač unapred izračuna $h(x)$ za svako x u rečniku uobičajenih lozinki.
- Neka napadač ima pristup fajlu sa heš vrednostima lozinki:
  - Treba samo da poredi heš vrednosti iz fajla sa heš vrednostima izračunatim na osnovu rečnika.
  - Svi naredni napadi mogu da se obave na isti način.
- Da li se može osujetiti ovakav napad ili barem, da se posao napadača učiniti težim?

Lozinke

Verifikacija lozinki.

- Bolje je zapisati heš vrednosti dobijene kombinacijom lozinke i neke slučajne vrednosti (*salt*).
- Za zadatu lozinku:
  - Izabrati slučajanu vrednost *s*.
    - Vrednost *s* nije tajana.
    - Korisnik ne pamti i ne zna s.
  - Izračunati $y = h(\text{lozinka}, s)$.
  - Memorisati parove (s, y) u datoteci.
- Lozinka se lako verifikuje.
- Napadač mora da izračuna heš vrednosti za svaku lozinku u rečniku i to da ponovi za svakog korisnika.
- Mnogo više posla!

Lozinke

Razbijanje lozinki – proračun.

- Pretpostavke:
- Lozinka ima 8 od 128 različitih karaktera.
  - Postoji $128^8 = 2^{56}$ različitih lozinki.
- Heš vrednosti lozinki se čuvaju u fajlu.
  - Neka je zapisano 2^{10} heš vrednosti lozinki.
- Napadač poseduje rečnik sa 2^{20} najčešće korišćenih lozinki.
- Verovatnoća da je data lozinka u rečniku iznosi 1/4 (kako pokazuje iskustvo).
- Posao koji je potrebno da se obavi meri se brojem heš vrednosti koje treba izračunati za analizu jedne lozinke.

Lozinke

Razbijanje lozinki – proračun.

- Analiza 4 moguća slučaja, Trudi napada:
  1. Alisinu lozinku (neku određenu), bez rečnika verovatnih lozinki.
  2. Alisinu lozinku (neku određenu), uz upotrebu rečnika verovatnih lozinki.
  3. Bilo koju lozinku, bez rečnika verovatnih lozinki, poseduje datoteku sa heš vrednostima lozinki.
  4. Bilo koju lozinku, sa rečnikom verovatnih lozinki, poseduje datoteku sa heš vrednostima lozinki.

Lozinke

Razbijanje lozinki – proračun.

- Slučaj 1. Napad na jednu lozinku bez rečnika.
  - Mora se isprobati $2^{56}/2 = 2^{55}$ vrednosti (srednja vrednost).
  - Analogno potpunoj pretrazi ključeva.

Razbijanje lozinki – proračun.

- Slučaj 2. Napad na jednu lozinku sa rečnikom.
  - Očekivani posao je oko: 1/4 (2^{19}) + 3/4 (2^{55}) = $2^{54,6}$
  - U praksi: isproba se ceo rečnik (najviše 2^{20} računanja), a verovatnoća uspeha je 1/4.

Razbijanje lozinki – proračun.

- Slučaj 3. Napad na bilo koju od 2^{10} =1024 lozinki u fajlu (poznate heš vrednosti) bez rečnika.
  - Neka je svih 2^{10} lozinki različito.
  - Potrebno je 2^{55} poređenja pre nego što se očekuje da pronađemo pravu lozinku.
  - Ako se ne koristi salt, za svaki izračunati heš sledi 2^{10} poređenja $\rightarrow$ očekivani posao (broj heševa) je $2^{55}/2^{10} = 2^{45}$.
  - Ako se koristi *salt*, očekivani posao je 2^{55} budući da svako poređenje zahteva novo računanje heša.

Lozinke

Razbijanje lozinki – proračun.

- Slučaj 4. Napad na bilo koju od 2^{10} =1024 lozinki u datoteci (poznate heš vrednosti) sa rečnikom.
  - Ignorišemo slučaj da u rečniku uopšte nema tražene lozinke.
  - Ako se ne koristi *salt*, potrebno je izračunati heš vrednost svake lozinke u rečniku (2^{20}).
  - Svaki izračunati heš se poredi sa svakom od 2^{10} poznatih heš vrednosti.
  - Posao je oko $2^{19}/2^{10} = 2^{9}$.

Lozinke

Razbijanje lozinki – proračun.

- Ako se koristi *salt*, može se pokazati da je očekivani posao je manji od 2^{22}.
- Primetimo da ako se ne koristi *salt*, možemo da preračunamo sve heševe za dati rečnik smanjujući ovaj posao.

Lozinke

Ostala pitanja oko lozinki.

- Korisnici treba da pamte više lozinki.
  - Česta upotrebi istih lozinki za različite sisteme.
  - Zašto je ovo problem?
- Ko trpi posledice zbog loših lozinki?
  - Lozinka za logovanje prema ATM PIN.
- Neuspešna promena podrazumevanih lozinki.
  - Otvoren Vam je nalog, promenite dodeljenu lozinku.
- Duštveni inženjering.
  - Ovde administrator, dajte mi lozinku...
- *Keystroke logging*, *spyware*, ...

Biometrija

Vi ste vaš ključ (Šnajer).

- Primeri:
  - Otisak prsta
  - Iris
  - Prepoznavanje lica
  - Prepoznavanje govora
  - Prepoznavanje rukopisa
  - ...

Biometrija

Zašto biometrija.

- Biometrija je viđena kao poželjna zamena za lozinke.
- Potrebna je jeftina i pouzdana biometrija.
- Danas je to vrlo aktivna oblast istraživanja.
- Biometrija se danas koristi u različitim sigurnosnim sistemima.
  - Miš sa senzorom za otisak prsta.
  - Otisak dlana za kontrolu pristupa.
  - Otisak prsta za otključavanje kola, vrata.
  - ...
- Međutim, biometrija nije “toliko” popularna (kao, npr. lozinke).
  - Još uvek nije našla (uslovno) masovnu primenu.
    - Ukoliko izuzmemo “pametne” telephone, neke značajnije kompanije, pojedine aerodrome itd.

Biometrija

Idealna biometrija.

- **Univerzalnost**. Primenljiva je na (skoro) svakog.
  - U praksi, ne postoji biometrija koja se može primeniti na svakog.
  - Zašto?
- **Razlikovanje**. Razlikovanje sa sigurnošću.
  - Da li su biometrijski podaci svakog pojedinca različiti?
  - U praksi se ne možemo nadati 100% tačnosti razlikovanja.
- **Permanentnost**. Upotrebljene i izmerene fizičke karakteristike ne bi trebale da se ikada promene.
  - U praksi se ovaj zahtev odnosi na određeni dugački vremenski period.
- **Primenljivost**. Biometrijski podaci se lako mere i memorišu.
  - Zavisi od stepena kooperativnosti subjekata.
- Pouzdana, robusna i jednostavna za upotrebu, ...

Biometrija

Identifikacija i verifikacija (autentifikacija).

- Biometrijski podaci mogu da se koriste za:
  - **Identifikaciju** – ko je tamo?
    - Identifikovati jednog od mnogo mogućih.
    - Primer: baza otisaka prstiju FBI.
  - **Autentifikaciju** – da li si to zaista ti?
    - Poređenje jedan prema jedan.
    - Primer: miš sa čitačem otiska prsta (da li je “Alisa” zaista Alisa?)
- Problem identifikacije je znatno teži.
  - Više “slučajnih” poklapanja usled mnogih poređenja.
- Pozabavićemo se autentifikacijom.

Faze biometrije.

- Postoje dve faze u biometrijskim sistemima:
  - **Faza uzimanja biometrijskih parametara** (*enrollment phase*).
    - Biometrijski podaci subjekta se pamte u bazi podataka.
    - Porebno je pažljivo izmeriti tražene podatke.
    - Ponekad je ovaj posao spor i zahteva ponovljena merenja.
    - Merenja moraju biti vrlo precizna za dobro prepoznavanje.
    - Ovo je slaba tačka mnogih biometrijskih sistema.
  - **Faza prepoznavanja** (*operation phase*).
    - Biometrijsko prepoznavanje u praksi:
      - Mora biti brzo i jednostavno.
      - Mora biti dovoljno tačno.

Kooperativni subjekat.

- Pretpostavlja se kooperativnost subjekta.
- U problemu identifikacije obično imamo nekooperativnog subjekta.
- Na primer, prepoznavanje lica.
  - Predloženo za upotrebu u kazinima za detekciju poznatih prevaranata.
  - Takođe se koristi za detekciju terorista na aerodromima.
  - Takva okruženja verovatno namaju idealne uslove za merenje (buka, gužva, ...)
  - Subjekt će verovatno pokušati da zbuni sistem prepoznavanja.
- Kooperativni subjekt čini ovu fazu mnogo lakšom!
  - Prilikom autentifikacije, subjekat je po pravilu kooperativan.

Biometrija

Biometrijske greške.

- Postoje dva tipa greške:
  - **Greška pogrešnog prihvatanja** (*False Acceptance Rate*, FAR).
    - Korisnik A se pogrešno autentifikuje kao korisnik B.
  - **Greška pogrešnog odbijanja** (*False Rejection Rate*, FRR).
    - Korisnik A se ne autentifikuje kao korisnik A.
- Za bilo koju biometriju, možemo smanjiti jednu od grešaka, ali će ona druga vrednost biti povećana.
- Jednake greške (EER): FAR = FRR.
- Najbolja mera za poređenje biometrijskih metoda.

Istorijat otisaka prstiju.

- 1823. Profesor Johannes Evangelist Purkinje diskutuje 9 različitih oblika otisaka prstiju.
- 1858. Sir William Hershel koristi otisak prsta za potpisivanje ugovora.
- 1880. Dr. Henry Faulds piše rad o otiscima prstiju za identifikaciju.
- 1883. U delu Mark Twain-a “Life on the Mississippi” ubica je identifikovan preko otiska prstiju.
- 1888. Sir Francis Galton (Darvinov rođak) je razvio klasifikacioni system.
  - Njegov sistem karakterističnih tačaka (tj. *minutia*) je još uvek u upotrebi.
  - Verifikuje da se otisci prstiju ne menjaju sa starenjem.
  - Neke zemlje propisuju broj karakterističnih tačaka za verodostojnost identifikacije u kriminalnim slučajevima.
  - U Americi nije propisan fiksan broj tačaka.

Otisak prsta.

- Primeri petlji (levo), vrtloga (sredina) i lukova (desno).
- Karakteristične tačke se dobijaju iz ovih obeležja.

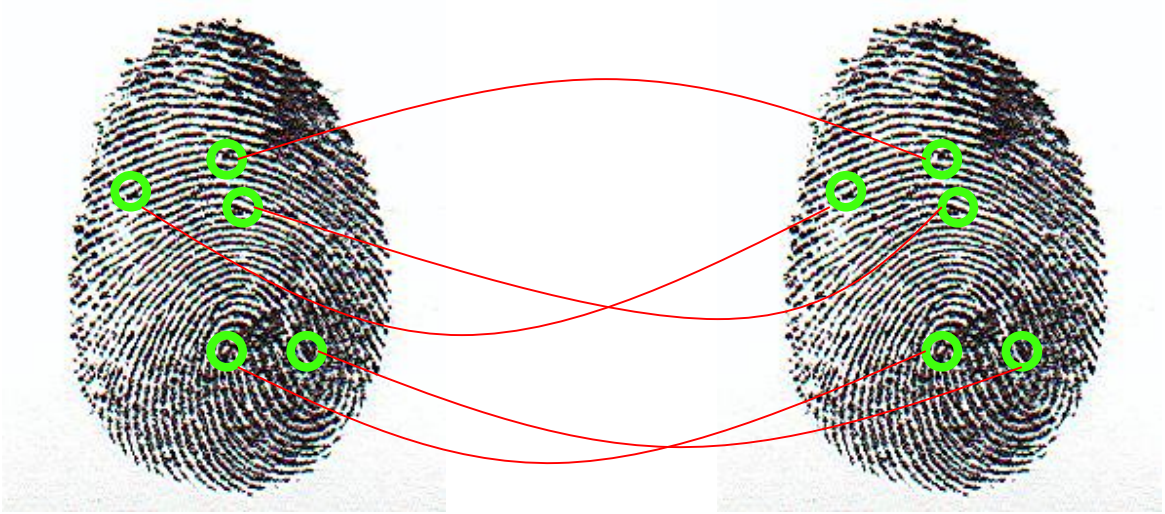


Otisak prsta.

- Grubo rečeno, faze su sledeće:
  - Snimanje slike otiska.
  - Izoštravanje slike.
  - Identifikacija karakterističnih tačaka.

Otisak prsta.

- Prepoznavanje:
  - Dobijene karakteristične tačke se porede sa onim koje su zapisane u bazi podataka.
  - Traži se statističko poklapanje (u zadatoj meri).



Biometrija

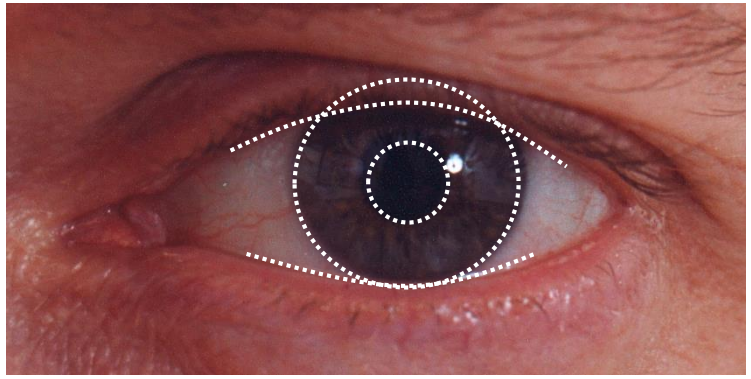
Geometrija dlana.

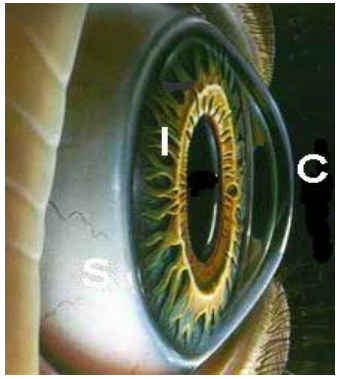
- “Popularni” oblik biometrije.
- Meri se oblik dlana: širina dlana, prstiju, dužina prstiju, itd.
- Ljudski dlanovi nisu jedinstveni.
- Geometrija dlana je dovoljna za neke primene.
  - Pogodna za autentifikaciju.
  - Nije pogodna za problematiku identifikacije.
- Nedostaci:
  - Ne može se koristiti za vrlo mlade i vrlo stare osobe.
  - Relativno visoka greška jednakosti.

Biometrija

Iris.

- Šara irisa (obojeni deo oka) je prilično “haotična”.
- Mali ili gotovo nikakav uticaj genetike.
- Različita (vrlo) čak i za identične blizance.
- Šara je stabilna kroz celokupan životni vek (počev od četvrte godine).



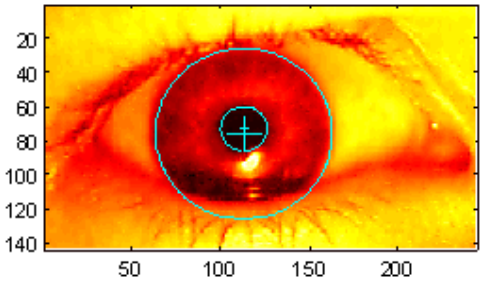


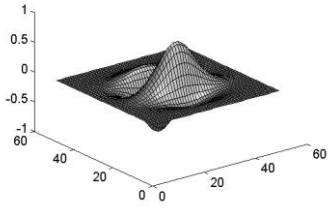
Istorijat irisa.

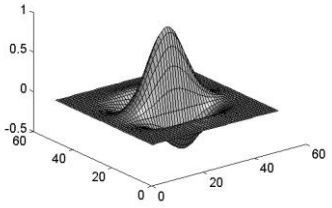
- 1936. Predložio Frank Burch.
- 1980. Filmovi James Bond-a.
- 1986. Pojava prvog patenta na ovu temu.
- 1994. John Daugman je patentirao “najbolji” savremeni sistem.
- 2002. Početak primene mašinskog učenja za prepoznavanje irisa (samo-organizujuće neuralne mreže).
- 2017. Primena dubokoobučavajućih sistema za prepoznavanje irisa (CNN).
- 2019. Primena stilometrije i mašinskog učenja za prepoznavanje irisa.

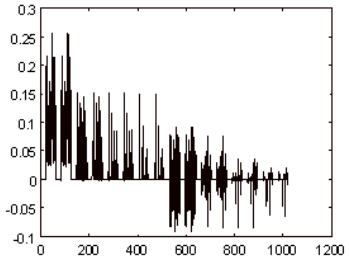
Skeniranje irisa (Daugman-ova metoda).

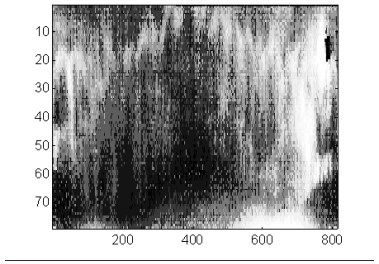
- Skener locira iris.
- Uzima se crno bela fotografija oka.
- Koriste se polarne koordinate.
- Računa se 2-D wavelet transformacija.
- Dobija se 256 bajtova iris koda (2048bita), oznaka: *x*











Merenje sličnosi irisa.

- Neka je *x* skeniran kod a *y* kod u bazi podataka.
- Merenje sličnosti se zasniva se Hamming-ovom rastojanju kodova.
- Definiše se *d*(*x*, *y*) kao količnik broja ne-poklapajućih bita i broja poređenih bita.
  - Primer:
    - *d*(0010,0101) = 3/4
    - *d*(101111,101001) = 2/6
- Računa se *d*(*x*, *y*) na 2048-bitskom iris kodu.
  - Perfektno poklapanje daje rastojanje *d*(*x*, *y*) = 0.
  - Za slučajne nizove, očekivano rastojanje je 0,50.
  - Za identičan iris, očekivano rastojanje je 0,08.
  - Poklapanje se prihvata, ako je rastojanje manje od 0,32.

Poređenje po kriterijumu jednakih grešaka (EER).

- *Equal error rate* (EER): FAR = FRR.
- Biometrija na bazi otisaka prstiju EER oko 5%.
- Teoretski, skeniranje irisa ima EER oko 10^{-6}.
- U praksi je ovo teško ostvariti.
- Faza prikupljanja podataka mora biti ekstremno tačna.

Nešto što posedujemo

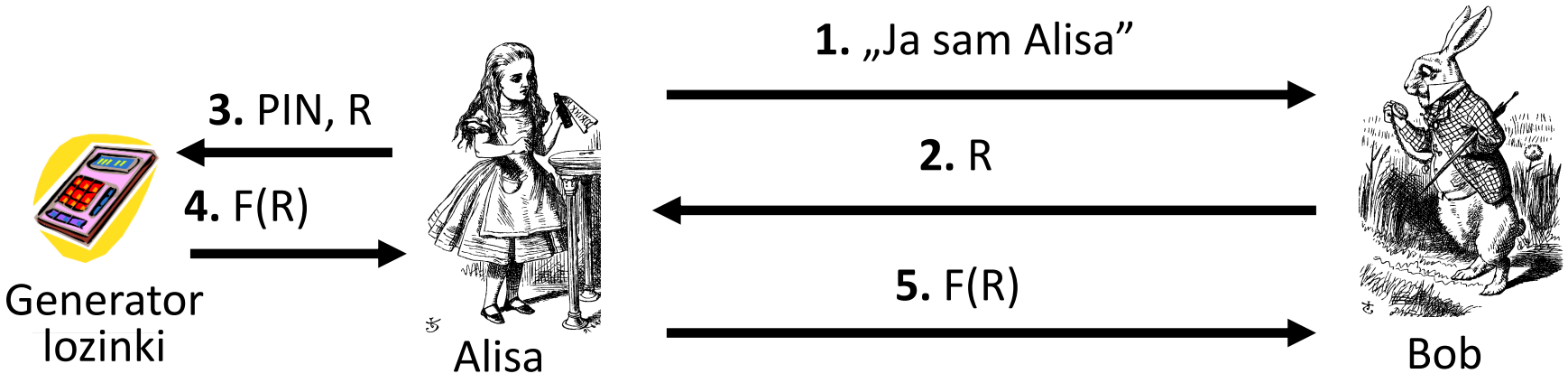
Primeri.

- Ključevi od kola.
- Laptop računar.
  - Ili specifična MAC adresa.
- Generator lozinki.
- ATM kartice, smartkartice, itd.
- Generator lozinki je uređaj koji korisnik treba da poseduje da bi se autentifikovao.
  - Alisa treba da se autentifikuje kod Boba.
  - ...

Nešto što posedujemo

Generator lozinki.

- Alisa dobija *challenge* R od Boba.
- Alisa unosi vrednost R u generator lozinki.
- Alisa šalje odgovor Bobu.
- Alisa ima generator lozinki i zna PIN.



Dvofaktorska autentifikacija

Zahteva dve od četiri stavke.

- Nešto što znate
- Nešto što imate
- Nešto što jeste
- Nešto što možete
- Primeri:
  - ATM: kartica i PIN
  - Kreditna kartica: kartica i potpis
  - Generator lozinki: uređaj i PIN
  - Smartkartica sa lozinkom / PIN

Šta je *Single Sign-on*?

- Velika je nepogodnost unositi lozinke često.
  - Korisnici žele autentifikaciju samo jedanput.
  - “Poverenje” ostaje uz korisnika bez obzira gde i kada se autentifikuje ponovo.
  - Naknadne autentifikacije su transparentne za korisnika.
- Autentifikacija na više različitih ali međusobno povezanih softverskih sistema.
- Cilj: rešiti problem pamćenja različitih lozinki, vremena unosa, problem IT podrške, centralizovane kontrole ...
- Realizacija:
  - Smart kartice (Smart Card).
    - Inicijalno, postoji zahtev za postavljanje kartice u u čitač.
    - Poseban softver koristi podatke sa kartice bez intervencije korisnika.
  - *One-Time Password* – OTP token
    - 2-faktorska identifikacija.

Literatura

1. M. Stamp (2006): *Information Security*. John Wiley and Sons.

Hvala na pažnji

Pitanja su dobrodošla.