<RSA> Sigurnost informacijskih sistema </RSA>

<AES> predavanja </AES>

<CISSP> Kontrola pristupa </CISSP>

© Jasmin Azemović

Summary

- Osnovni pojmovi
- Autentifikacija
  - Biometrija u autentifikaciji
- Autorizacija
- Case study

© Jasmin Azemović

Osnovni pojmovi

- Autentifikacija: Ko si ti i da li si to zaista ti?
  - čovjeka prema računaru (programu)
  - računar-računar
- Autorizacija: Šta smiješ da radiš?
  - Gdje korisnik ima pristup i koje su njegove privilegije?
  - Forsiranje ograničenja gdje i kada je potrebno.
- U kontrolu pristupa se još ubraja prikupljanje digitalnih dokaza o aktivnostima korisnika.

© Jasmin Azemović

Lekcija 1. Autentifikacija

- Da li si to zaista ti?
- Nešto što samo mi znamo.
- Lozinke i problem sa lozinkama.
- Nešto što imamo samo mi.
- Nešto što nas predstavlja.

© Jasmin Azemović

Da li si to zaista ti?

- Kako se sve čovjek može autentificirati prema računaru?
- Možemo koristiti slijedeće metode/tehnike…

1. Nešto što samo mi znamo
   - Npr. lozinka
2. Nešto što samo mi imamo
   - Npr. smartcard
3. Nešto što vas predstavlja
   - Npr. otisak prsta

© Jasmin Azemović

Nešto što samo mi znamo

- Lozinke
- Mnogi pojmovi iz života se tretiraju kao lozinke!
  - PIN (sa telefona, kartice i sl.)
  - JMB ili neki drugi sličan podatak
  - Važniji datumi iz života
  - Imena kućnih ljubimaca, glumaca i sl.
- ...što i nije baš najbolja praksa !

© Jasmin Azemović

Lozinke

- Trenutno jedan od velikih izazova koji rješavaju sigurnosni inženjeri danas.
- Ljudi nisu u mogućnosti da upamte velike i složene kriptografske ključeve kako bi se autentificirali.
- Zbog toga se lozinke koriste kao međukorak ili inicijator složenih mehanizama koje se nalaze u pozadini.

© Jasmin Azemović

Problemi sa lozinkama

- Klasične lozinke su 8 karaktera
- Pretpostavimo da imamo 256 različitih karaktera u opticaju.
- $256^8 = 2^{64}$ lozinki
- Korisnici ne biraju metodom slučajnog izbora „random“
- Napadač ima mnogo manje od 2^{63} pokušaja
- (dictionary attack)

© Jasmin Azemović

Nešto što samo mi imamo

- Uređaj ili predmet u vašem posjedu
- Primjeri:
  - Ključevi od automobila
  - Laptop računari (ili MAC adrese)
  - Generatori lozinki
  - Kreditne kartice, pametne kartice i sl.

© Jasmin Azemović

Nešto što nas predstavlja

- „ Ti si svoj vlastiti ključ“ - Schneier
- Uglavnom se koristi Biometrija
  - Otisak prsta
  - Svojeručni potpis
  - Prepoznavanje lica
  - Prepoznavanje glasa
  - Prepoznavanje kretanja
  - ...

© Jasmin Azemović

Lekcija 2. Biometrija u autentifikaciji

- Zašto biometrija?
- Idealna biometrija
- Način rada
- Kooperativnost
- Greške u biometriji
- Primjeri
- Zaključak

© Jasmin Azemović

Zašto biometrija?

- Mnogo sigurnija zamjena za lozinke
- Hardver i oprema danas nisu tako skupi
  - Vrlo aktivna oblast u istraživanju
- Biometrija je danas je standard u sigurnosti
  - Thumbprint ulazni uređaji
  - Prepoznavanje lica prilikom prijave
  - Fingerprint za otključavanje auta i sl..
- ..ali još nije tako popularno
  - Tehnologija još nije dostigla svoj vrhunac

© Jasmin Azemović

Idealna biometrija

- Univerzalna - primjenjiva na svakoga
  - U relanosti nije primjenjiva na svakoga
- Različitost - sigurna različitost
  - U realnosti nema 100% različitosti
- Stalna - fizičke karakteristike su stalne
  - U realnosti, ostaju stalne duži vremenski period
- Lako prikupljiva
  - Zavisi od kooperativnosti subjekta
- Sigurna
  - Zavisi od standarda, tehnologije i niza drugih faktora

© Jasmin Azemović

Način rada

- **Identifikacija** ?
  - Komparacija one-to-many
  - Npr: Baza podataka otisaka prstiju
- **Autentifikacija** ?
  - Komparacija one-to-one
  - Npr: Laptop sa skenerom prsta
- Identifikacija je teži dio posla

© Jasmin Azemović

Kooperativnost

- Autentifikacija— kooperativni subjekti
- Identifikacija— subjekti nisu kooperativni
  - Prepoznavanje lica
  - Aerodromi, kockarnice i sl.
  - Uslovi su obično vrlo loši
  - Subjekt nastoji da „zbuni“ fazu prepoznavanja
- Kooperativnost subjekata olakšava cijeli proces
- U fazi autentifikacije obično nema potrebe sa „sakrivanjem“

© Jasmin Azemović

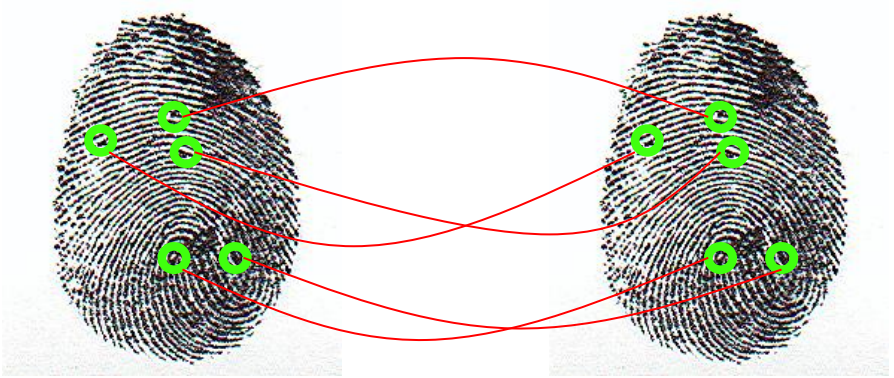
Greške u biometriji

- Stopa prevare vs. Stopa uvrede
  - Prevara - Trudy je autentificiran (pogrešno) kao Alisa
  - Uvreda - Alisa nije autentificirana kao Alisa
- U biometriji, smanjenje jedne strane vodi kao porastu suprotne
  - 99% prepoznavanje govora → mala prevara, velika uvreda
  - 30% prepoznavanja govora → velika prevara, mala uvreda

© Jasmin Azemović

Primjer: Otisak prsta

- Skeniranje otiska
- Poboljšanje rezolucije slike
- Identifikacija ključnih tačaka



© Jasmin Azemović

Primjer: Geometrija ruke

- Mjeri atribute ruke
  - Širinu šake i prstiju
  - Dužina prstiju, itd.
- Prednosti
  - Brzina
  - Ruke su simetrične
- Nedostaci
  - Nije efikasno na vrlo mladim i starijim ljudima
  - Relativno visoka stope pogreške

© Jasmin Azemović

Primjer: Zjenica oka

- Skeniranje i uzimanje uzorka je problematično
- Skoro da nema genetičkog uticaja
- Različito i kod identičnih blizanaca
- Uzorak nije promjenjiv kroz vrijeme (život)
- Nedostatak
  - Postoje primjeri gdje su se osobe autentificirale putem fotografije
- Pojačano osvjetljenje na oko bi moglo spriječiti ovakve vrste „napada“

© Jasmin Azemović

Zaključak

- Biometriju je teško falsifikovati
- Međutim, postoje slabe tačke
- Nedovoljno „inteligentna“ tehnologija
- Upotreba je još uvijek limitirana
- Sigurno dolazi do promjene u skorijoj budućnosti

© Jasmin Azemović

Lekcija 3. Autorizacija

- Šta je autorizacija ?
- Matrica prava pristupa
- Nivoi autorizacije

© Jasmin Azemović

Šta je autorizacija ?

- Autorizacija - Šta smiješ da radiš?
- Uglavnom odnosi na akcije autentificiranih korisnika
- Često se posmatra kao kontrola pristupa (mada je to samo jedna njegova cjelina).

© Jasmin Azemović

Matrica prava pristupa

- Najčešća primjena u praksi, formalizovana u matrici koja opisuje kontrolu pristupa sa pojedine subjekte
- Matrica se sastoji od:
  - S = skup subjekata (npr: jane, john, sendmail)
  - O = skup objekata (/mail/jane, edit.exe, sendmail)
  - A = skup privilegija (read, write, execute, append)

	/mail/jane	edit.exe	sendmail
jane	{r,w}	{r,x}	{r,x}
john	{}	{r,w,x}	{r,x}
sendmail	{a}	{}	{r,x}

© Jasmin Azemović

Nivoi autorizacije

- Podjela se odnosi na objekat
- Dozvola se odnosi na subjekt
- US Department of Defense (DoD) koristi 4 nivoa:
  - TOP SECRET
  - SECRET
  - CONFIDENTIAL
  - UNCLASSIFIED

© Jasmin Azemović

Lekcija 4. Case study (Autentifikacijski protokol)

- Scenario
- Jednostavna autentifikacija
  - Napad
- Malo bolja autentifikacija
- Challenge-Response
- Nonce
- Izazov i odgovor (Challenge-Response)

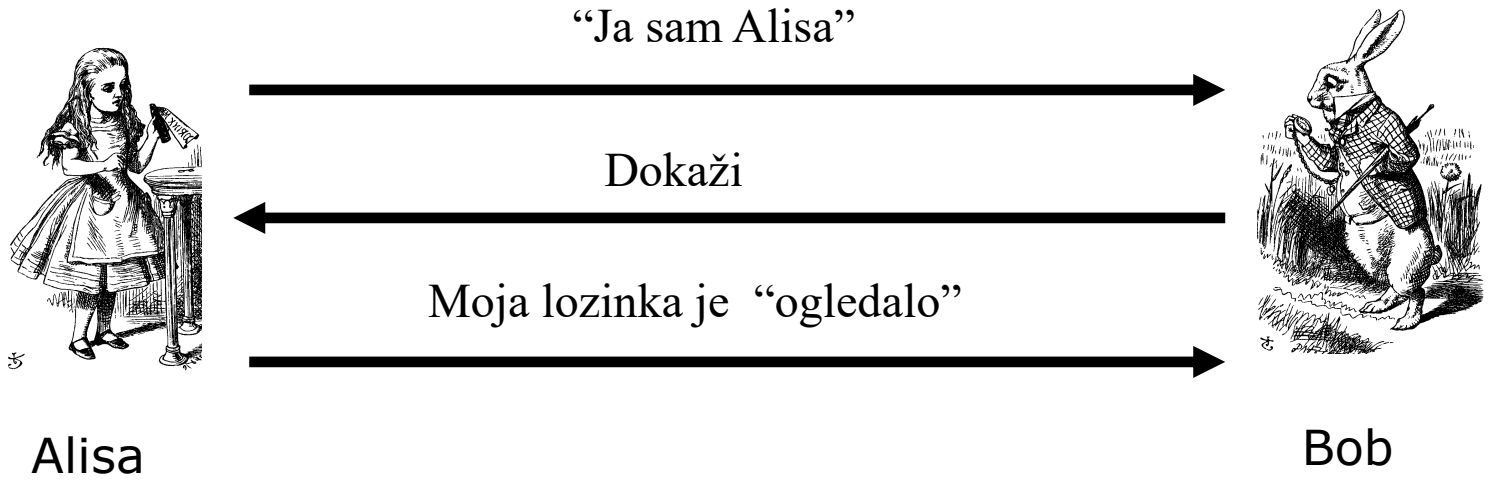
© Jasmin Azemović

Scenarij

- Alisa treba da dokaže svoj identitet Bobu
  - Alisa i Bob mogu biti ljudi i/ili računari
- Može biti potrebno da i Bob dokaže svoj identitet
  - (uzajamna autentifikacija)
- Problemi
- Autentifikacija na stand-alone računare je relativno jednostavna
- Autentifikacija putem mreže je izazov i problem
  - Napadač može biti pasivni posmatrač
  - Napadač može ponoviti poruku (mrežne pakete)
  - Aktivni napadi nisu rijetki (manipulacija nad podacima)

© Jasmin Azemović

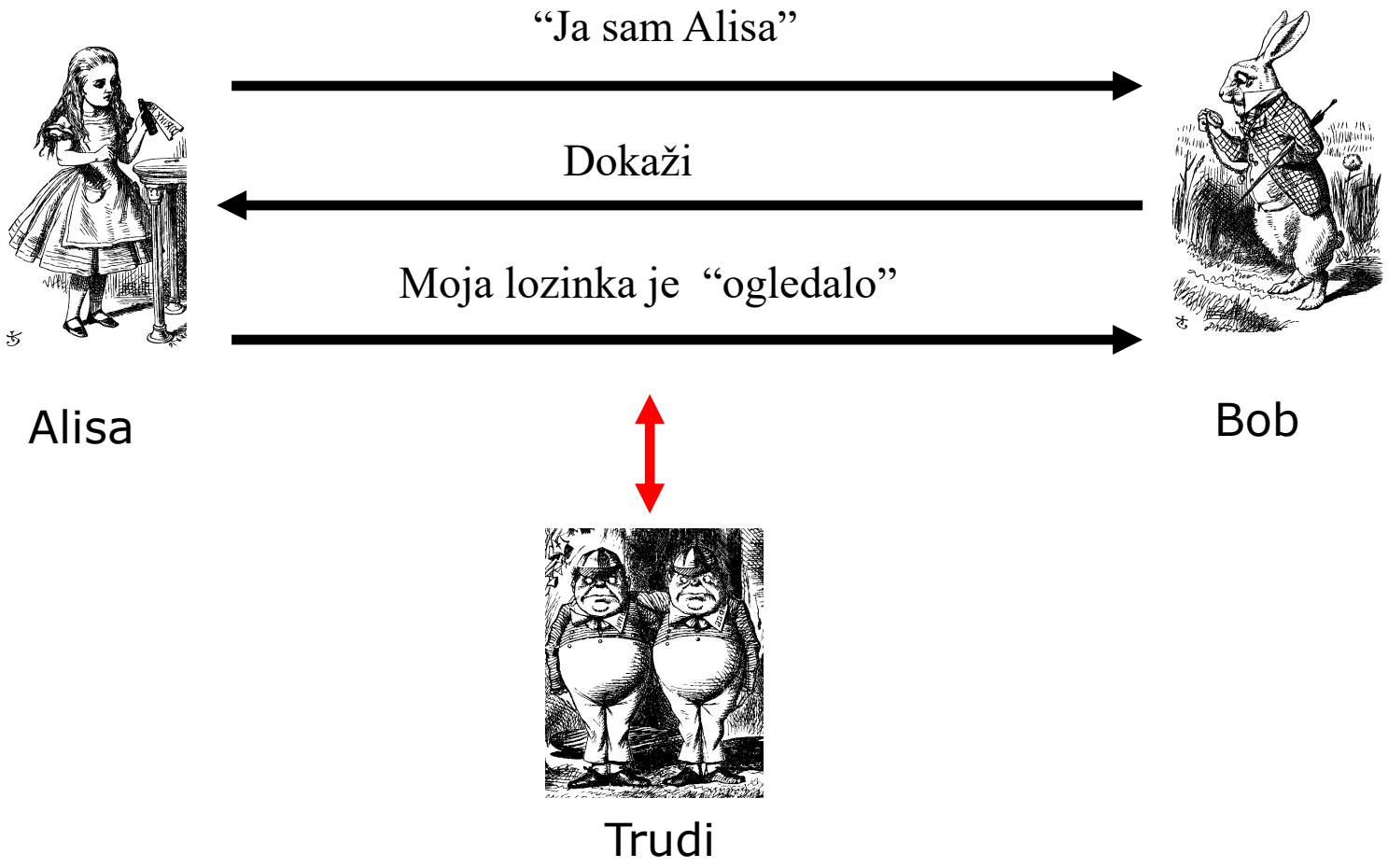
Jednostavna autentifikacija



- Jednostavno i primjenjivo u stand-alone sistemima
- Vrlo problematično u mrežnom okruženju
  - Replay napad
  - Bob mora poznavati Alisinu lozinku

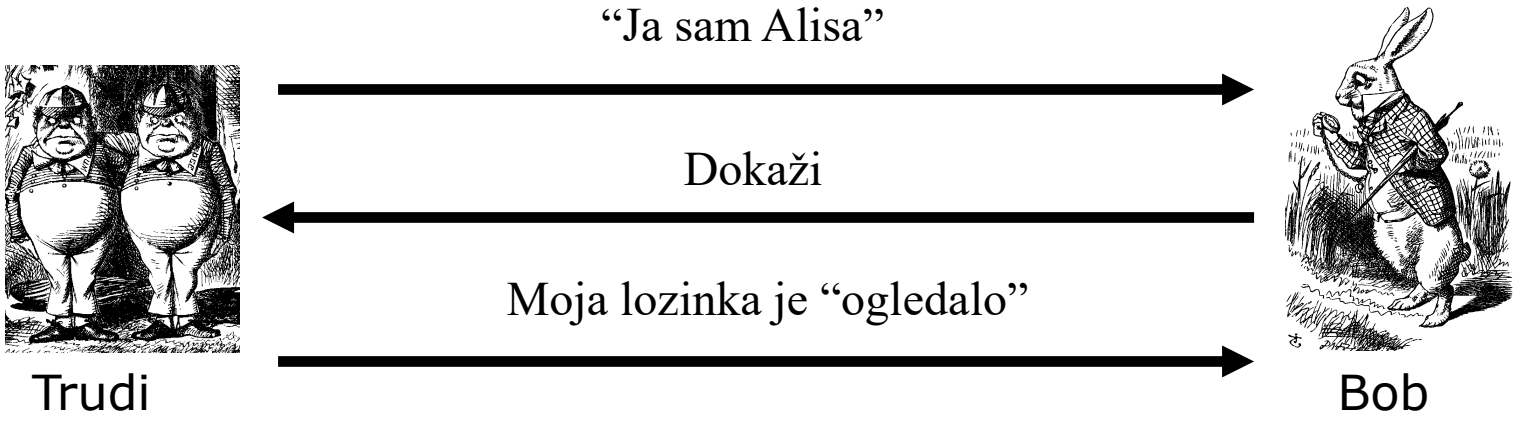
© Jasmin Azemović

Napad



© Jasmin Azemović

Replay



© Jasmin Azemović

Malo bolja autentifikacija

- Lozinka je sada sakrivena
- Ali je još uvijek predmet i meta ponavljanja

© Jasmin Azemović

Challenge-Response

- Ponavljanje se može spriječiti upotrebom challenge-response metode
- Cilj je da se osigura “svježina”
- Pretpostavimo da Bob želi autentifikovati Alisu
- Challenge se šalje od strane Boba
- Funkcioniše tako da:
  - Ponavljanje nije izvodivo
  - Samo Alisa može ispravno odgovoriti
  - Bob je tu da verifikuje odgovor

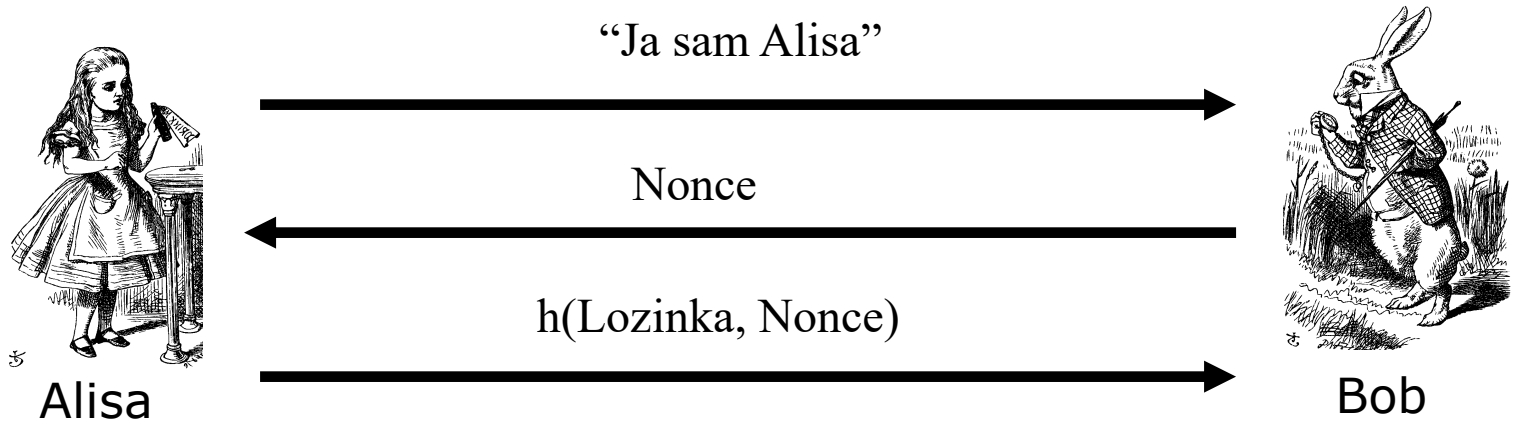
© Jasmin Azemović

Nonce

- Nonce == **n**umber used **once**
- Podatak koji se koristi samo jednom
- Poznato pod nazivom **one time password**
- Token uređaji
  - Hardverski (eBanking)
  - Softverski (two factor autentifikacija)

© Jasmin Azemović

Izazov i odgovor (Challenge-Response)



- Nonce je izazov
- Hash je odgovor
- Nema ponavljanja
- Lozinku zna Alisa
  - ...ali i Bob
- Kako riješiti ovaj problem?

© Jasmin Azemović

Pitanja

© Jasmin Azemović