Osnovni pojmovi

Sadržaj

- Uvodne napomene
- Steganografija
- Uvod u kriptografiju
- Autentifikacija i autorizacija
- O sigurnosti softvera
- Razmišljati kao Trudi
- Sigurnost počiva na čoveku

Zaštita informacija …

- Odbrana od i sprečavanje napada spolja ili iznutra.
- Odbrana od i sprečavanje industrijske špijunaže.
- Sigurnost e-poslovanja.
- Sigurnost bankovnih transakcija.
- Sigurnost intelektualnog vlasništva.
- Izbegavanje / dokazivost odgovornosti.

Pretnje informacionim sistemima

- Napadi na računarsku mrežu, e-poštu, transakcije, ...
- *On-line* pristup sistemima na kojima se čuvaju poverljivi podaci.
- Nesigurne ili “šuplje” tehnologije (npr. *wireless*).
- Trend ka poslovanju “bez papira”.
- Neprimenjivanje zaštite privatnosti kod e-pošte.
- ...
- Rešenje?
  - Zaštita / tajnost informacija i komunikacija

Tajnost komunikacija

- **Steganografija**.
- Kriptografija.

Steganografija

- Od Grčkog:
  - STEGANOS (στεγανός) – prikriveno
  - GRAPHIE (γραφή) – pisanje
- Stegnografija je tehnika **sakrivanja činjenice** da se neka informacija prenosi.
- Dakle, cilj je poslati poruku **javnim kanalom** a da niko osim pošiljaoca i primaoca to ne zna.
- Postiže se sakrivanjem **tajne informacije** unutar druge poruke kaja se naziva **nosilac**.
- Nosioci:
  - tekst,
  - slika,
  - video,
  - audio,
  - …
- Veoma bitno: tajna informacija ne sme primetno da izmeni javnu informaciju!

Steganografija (istorijat)

- Herodot opisuje neke od najstarijih steganografskih sistema (Grčka 440. PNE):
  - Robu obrijati glavu.
    Napisati poruku na obrijanoj glavi.
    Sačekati da kosa naraste.
    Poslati roba da prenese poruku.
    Robu obrijati glavu i pročitati poruku.
    Napomena: tako je preneto upozorenje o Persijskom napadu.
  - Poruku napisati na drvenoj ploči.
    Ploču prekriti voskom.
- Istorijski gledano, steganografija se više koristila nego kriptografija!

Steganografija (istorijat)

- Drugi svetski rat.
  - Nevidljivo mastilo.
  - Pisanje teksta na veoma malim površinama, veličine tačke u tekstu (engl. *microdot technology*).
  - Otvorena poruka (na primer, drugo slovo svake reči).

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.

pershingsailsfromnyjunei.

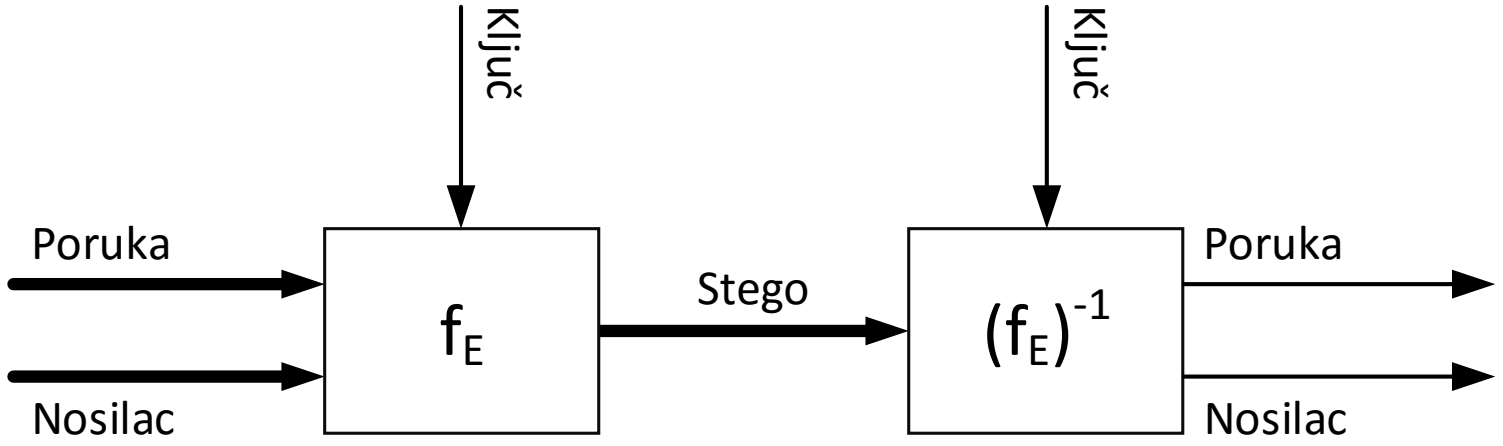
Pershing sails from NY June 1.

Steganografija (savremene tehnike)

- **Maskiranje i filtriranje**.
  - Informacija je skrivena upotrebom tehnike vodenog žiga (engl. *digital watermark*).
  - Sadrži informacije o autrskim pravima, vlasništvu, licencama, ...
  - Ne krije se prisustvo informacije.
  - Bilo kakva izmena utisnute informacije je primetna.
- **Algoritmi i transformacije**.
  - Koriste se matematičke funkcije koje se koriste i kod tehnika kompresije.
  - Cilj je utiskivanje informacije tako da se ne naruši primetno sadržaj nosioca.
  - Potrebno poznavanje parametara algoritma.
- **Utiskivanje informacije na mesto bita najmanje važnosti** (LSB).
  - Često se primenjuje kad je nosilac slika, utiskuje se informacija u LSB svakog piksela slike.
  - Narušavanje sadržaja slike je minimalno.
  - Posebno je pogodno kad je fajl sa slikom dosta veći od količine podataka koje treba sakriti.

Osnovi moderne steganografije

- $\mathbf{f_E}$: steganografska funkcija
- **Ključ**: tajni parametar steganografske funkcije
- **Stego**: poruka utisnuta u nosilac
- **Nosilac**: podatak u koji se utiskuje tajna informacija
- **Poruka**: tajna informacija



Osnovni zahtevi steganografskog sistema

- Sigurnost tajne komunikacije.
- Uskladiti veličinu nosioca sa veličinom tajne informacije.
- Otpornost na namerne i nenamerne napade.

Detekcija steganografskog sadržaja

- Detekcija steganografskog sadržaja se naziva **steganoanaliza**.
- **Vizuelna analiza**.
  - Tehnika prepoznavanja skrivenih informacija “ručno” ili uz pomoć računara.
- **Statistička analiza**.
  - Upotreba algoritama koji treba da otkriju (mala) statistička odstupanja podataka koji se prenose.
  - Odstupanja nastaju usled primene steganografskih tehnika.

Slika i steganografija

- Slika koristi 24 bita za boje: RGB
  - 8 bita za crveno, 8 za zeleno, 8 za plavo.
- Primer 1 (promena bita veće važnosti):
  - 0x7E 0x52 0x90 je **ova boja**.
  - 0xFE 0x52 0x90 je **ova boja**.
- Primer 2 (promena bita manje važnosti):
  - 0xAB 0x33 0xF0 je **ova boja**.
  - 0xAB 0x33 0xF1 je **ova boja**.
- Biti male važnosti mogu da se menjaju a da pri tome ne utiču bitno na osnovnu informaciju o boji!

Slika i steganografija

- Data je nekomprimovana slika.
  - Na primer, u BMP formatu.
- Tada možemo **ubaciti novu informaciju u RGB bite niske važnosti**.
  - Pošto RGB biti niske važnosti ne utiču značajno na sliku, rezultat ubacivanja informacije će biti nevidljiv za ljudsko oko.
  - Steganografski algoritam će međutim “videti” ubačenu informaciju.

Steganografija (primeri)

- Primer 1.
  - Originalna slika Alise (levo).
  - Slika Alise u koju je ubačeno kompletno delo *Alice in Wonderland* u PDF formatu (desno).

Steganografija (primeri)

- Primer 2.
  - Slika u kojoj se krije druga slika (levo).
  - Slika koja je sakrivena (desno).

Steganografija (primeri)

- Primer 3.
  - Prikaz Web stranice www.sajt.com/stranica.html (bez skrivene informacije):

"The time has come," the Walrus said,
"To talk of many things:
Of shoes and ships and sealing wax
Of cabbages and kings
And why the sea is boiling hot
And whether pigs have wings."

  - Izvorni kod:

```
<font color="#000000">"The time has come," the Walrus said,</font><br>
<font color="#000000">"To talk of many things:</font><br>
<font color="#000000">Of shoes and ships and sealing wax</font><br>
<font color="#000000">Of cabbages and kings</font><br>
<font color="#000000">And why the sea is boiling hot</font><br>
<font color="#000000">And whether pigs have wings."</font><br>
```

Steganografija (primeri)

- Primer 3.
  - Prikaz Web stranice www.sajt.com/stranica.html (sa utisnutom skrivenom informacijom):

"The time has come," the Walrus said,
"To talk of many things:
Of shoes and ships and sealing wax
Of cabbages and kings
And why the sea is boiling hot
And whether pigs have wings."

  - Izvorni kod:

```
<font color="#010100">"The time has come," the Walrus said,</font><br>
<font color="#000100">"To talk of many things:</font><br>
<font color="#010100">Of shoes and ships and sealing wax</font><br>
<font color="#000101">Of cabbages and kings</font><br>
<font color="#000000">And why the sea is boiling hot</font><br>
<font color="#010001">And whether pigs have wings."</font><br>
```

  - Skrivena poruka: 110 010 110 011 000 101

Steganografija (rezime)

- Neki formati (JPG, GIF, WAV, ...) su čoveku teži za čitanje od HTML formata.
- Informaciju je lako sakriti u **manje važnim** bitima.
  - Informacija sakrivena u manje važnim bitima se lako **uništava** ili izbacuje!
- Da bi sistem bio robusan (otporan na napade), informacije moraju biti sakrivene **u važnim bitima**.
  - Ali ubačena informacija ne sme da ošteti podatke!
  - Robusna steganografija je teža za implementaciju nego što izgleda.

Tajnost komunikacija

- Steganografija.
- **Kriptografija**.

Zašto kriptogafija?

- Većina ljudi zalepi koverat pre nego što pošalje pismo.
- Zašto?
  - Što da ne?
  - Navika.
  - Da pismo ne bi ispalo, ...
  - Da ga “drugi” ne bi čitali.
- Ako koverta nije zalepljena, svako ko dođe u njen posed MOŽE da:
  - Pročita pismo.
  - Da ga zameni.
  - Da ga uništi.
- Pitanja:
  - Da li će to uraditi?
  - Da li bi primetili da je pismo zamenjeno ili već pročitano?

Zašto kriptogafija?

- Elektronska pošta je zamena za klasičnu poštu.
  - Brz oblik komunikacije.
  - Ovde koverta **ne postoji**.
  - Ukolko želite privatnost komunikacije potreban je **novi mehanizam zaštite**.
- Kriptografija nudi rešenje – **šifrovanje poruke**.
- Šifrovana poruka u rukama nekoga kome nije namenjena treba da bude potpuno nerazumljiva.

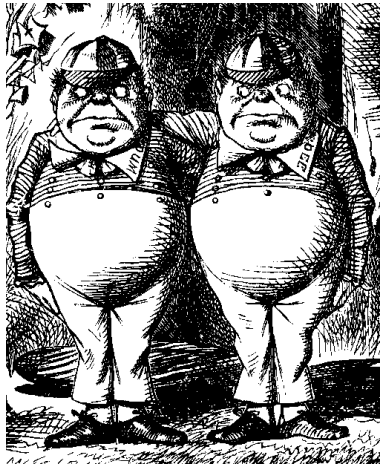
Zašto kriptogafija?

- Ima istoriju dužu od 2000 godina.
- Tradicionalni korisnici su **predstavnici države** (diplomatija, vojska, ...)
  - Do 1970-tih kriptografija je bila tajna nauka, rezervisana za državne organe.
- Danas:
  - Izučava se na mnogim univerzitetima.
  - Ima poslovnu i ličnu primenu.
- Razlozi masovne primene:
  - Automatizovano poslovanje primenom Interneta
  - e-banking
  - …

Podela uloga

- Alisa (*Alice*) i Bob (*Bob*) imaju **pozitivne uloge**.
- Povremeno će biti angažovane i epizodne pozitivne uloge kao što je, na primer, Čarli (*Charlie*).

- Trudi (*Trudy*) i Eva (*Eve*) imaju uloge **negativaca**.
  - Trudi (*intruder*) je **negativac opšte namene** – uljez.
  - Eva (*eavesdropper*) je osoba koja **prisluškuje**.



Scenario

- Alisa otvara svoju banku (*Alice's Online Bank* – **AOB**).
- Bob je njen klijent.
- Bob i Alisa svoju komunikaciju najčešće ostvaruju preko **javne mreže**.
  - Po pravilu, nemaju poverenja u javnu mrežu.
  - Postoji mogućnost da ih neko prisluškuje ili da čak menja podatke na prenosnom putu.
- **Sigunosni problemi**:
  - Njihova komunikacija je poverljiva.
  - Podaci koje razmenjuju nisu promenjeni na prenosnom putu.
  - Podaci koji se čuvaju u bazi banke su sigurni.
    - Tim podacima mogu da pristupe samo njih dvoje.
    - Izmena tih podataka je zasnovana na stvarnim uplatama i isplatama.
- Trudi: kako **iskoristiti slabe strane sistema**?
  - Trudi želi da sazna sadržaj komunikacije ili da tajno izmeni njen sadržaj, onemogući razmenu podataka, da se lažno predstavi u komunikaciji, ...

Sigurnosni ciljevi

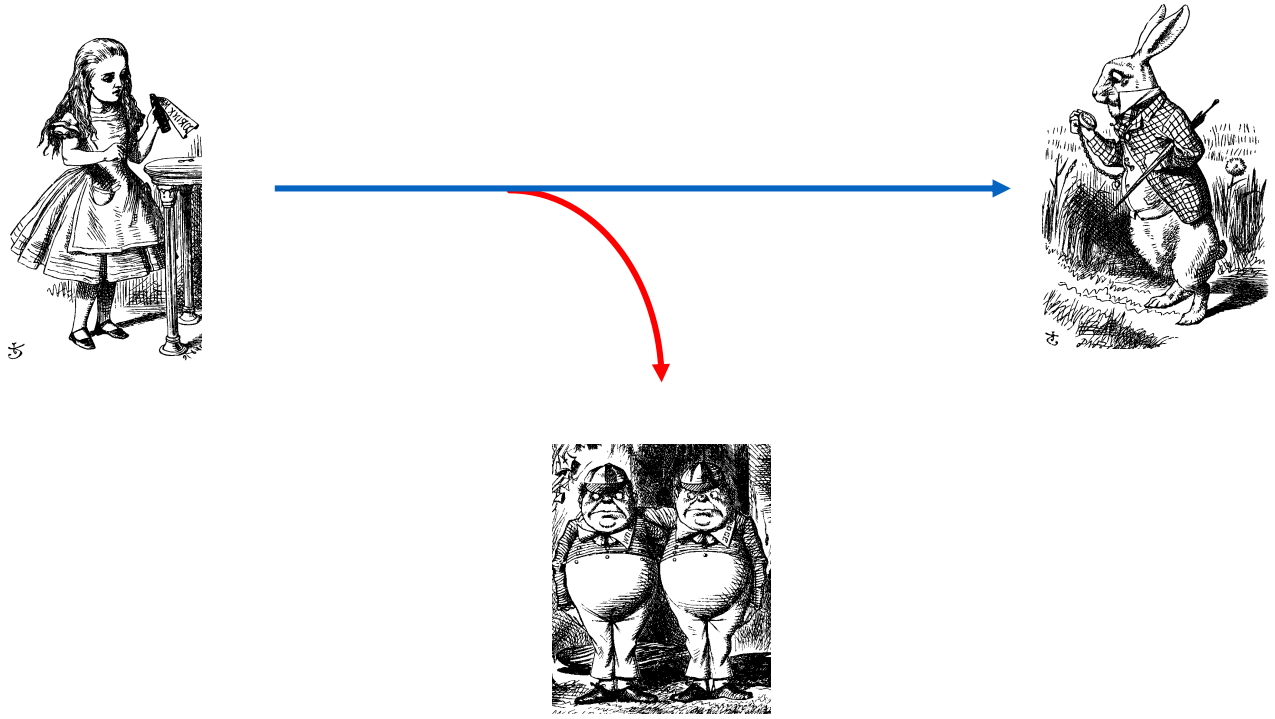
- U oblasti sigurnosti informacionih sistema, CIA je skraćenica za:
  - **Poverljivost** (*Confidentiality*)
  - **Integritet** (*Integrity*)
  - **Raspoloživost** (*Availability*)
- Confidentiality, Integrity and Availability
- Dakle, nije:
  - Central Intelligence Agency
  - Certified Internal Auditor
  - Culinary Institute of Alabama
  - Creepy Introvert Alien
  - …

Poverljivost

- ***Confidentiality*** (CIA).
- Objašnjenje:
  - Obezbediti da neautorizovana (neovlašćena) strana ne dođe do poverljivih informacija.
  - Definiše do koje mere neka informacija treba da bude dostupna, odnosno nedostupna
  - neovlašćenim korisnicima.
- Primer:
  - Alisa (AOB) mora da spreči da Trudi dođe do podataka o Bobovom računu (stanje, transakcije, uplate, ...)

Poverljivost

- Potreba?
- Sprečiti prisluškivanje.

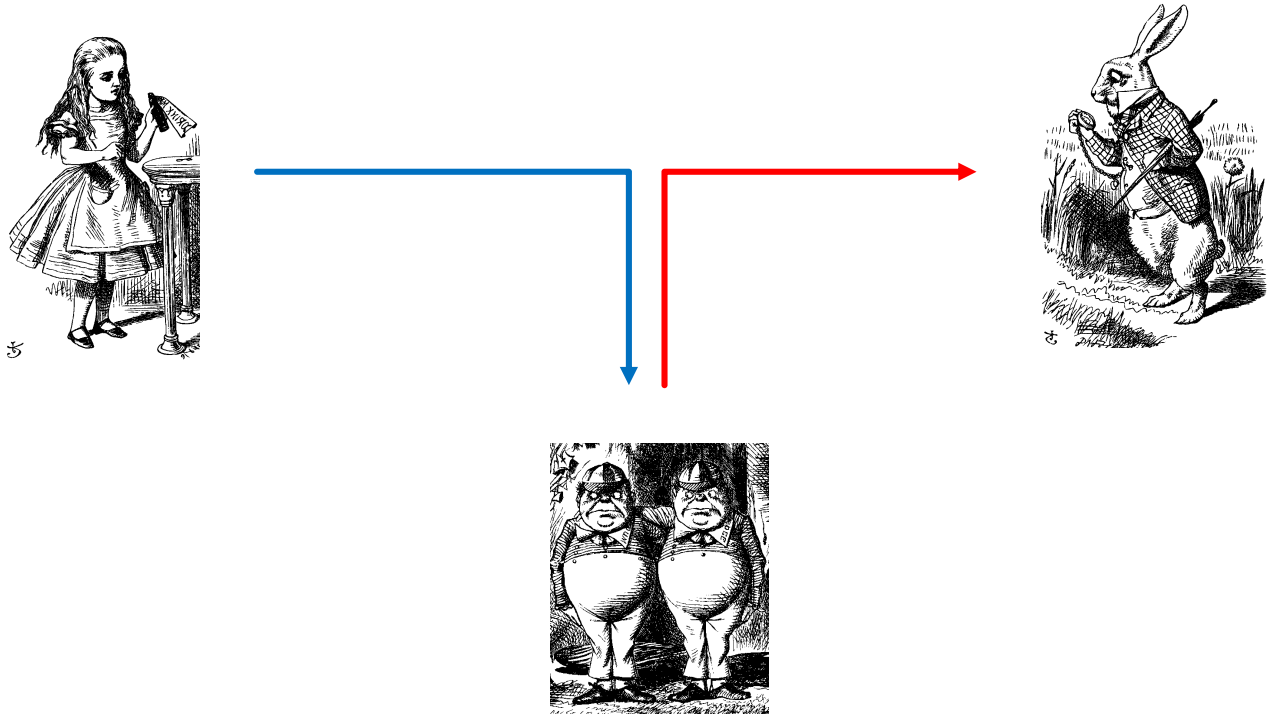


Integritet

- ***Integrity*** (C**I**A).
- Objašnjenje:
  - Primljeno = poslato?
  - Preventivne mere: onemogućiti neovlašćene izmene, brisanje ili uništavanje informacija.
  - Odnosi se na podake koji se čuvaju i prenose.
  - Napad neovlašćenih korisnika ili ovlašćenih korisnika koji zloupotrebljavaju svoja ovlašćenja.
  - Integritet predstavlja mogućnost sistema da se odupre napadima.
- Primer:
  - Trudi ne sme da ima mogućnost da menja stanje Bobovog računa.
  - Bob ne sme da ima mogućnost da na nepropisan način menja stanje svog računa.

Integritet

- Potreba?
- Sprečiti izmenu podataka.

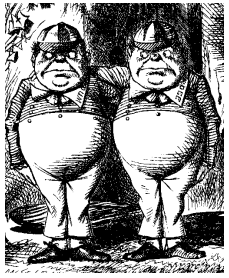


Raspoloživost

- ***Availability*** (CIA).
- Objašnjenje:
  - Raspoložovost je sposobnost sistema da pruži uslugu ovlašćenom korisniku.
  - Odgovor na napade čiji je cilj redukcija ili onemogućavanje pristupa podacima i servisama ovlašćenom korisnicima.
  - Tipičan napad: odbijanje usluge (engl. *Denial of Service*, DoS).
  - Informacioni sistem koji nije rasplođiv u momentu kada je potreban je isto toliko loš kao i da ne postoji.
- Primer:
  - Alisa mora da obezbedi Bobu dostupnost informacija o njegovom računu kad god mu je to potrebno.
  - Alisa mora da bude u stanju da obavlja transakcije bez obzira na poteškoće sa kojima se suočava na prenostnim putevima.

Raspoloživost

- Potreba?
- Sprečiti prekid komunikacije.



Sprečavanje i otkrivanje

- Sprečavanje ili otkrivanje?
- Osnovni sigurnosni koncepti mogu biti orijentisani ka:
  - **Sprečavanju**.
    - Primena mehanizama koji će u napred da ostvare željene zahteve.
  - **Otkrivanju**.
    - Brzo otkrivanje i korekcija propusta.
- Balans između sprečavanja i otkrivanja:
  - Okolnosti (**zahtevi**) primene.
  - Složenost (**cena**) primenjene tehnologije.
- Primeri:
  - Kuća može da ima vrata i prozore koji se mogu lako provaliti, ali je sigurnost zasnovana na primeni alarma.
  - Mnogi informacioni sistemi imaju metode koji treba da preduprede napade, ali koriste i metode detekcije kao što su praćenje saobraćaja i analiza aktivnosti korisnika.

Dodatni zahtevi koji se tiču sigurnosti

- Kontrola pristupa:
  - Autentifikacija.
  - Autorizacija.
- Sigurnosni problemi softvera.
- Sigurnosni problemi hardvera.

Autentifikacija

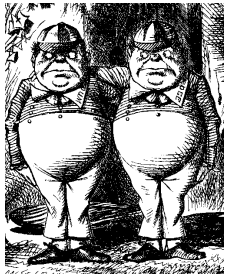
- Bob treba da pristupi podacima na svom računaru.
- Kako njegov računar “zna” da je to stvarno Bob a ne Trudi?
- Treba odgovaroriti na sledeća pitanja:
  - Ko je korisnik?
  - Da li je korisnik zaista onaj za koga se predstavlja?
- Moguće rešenje**: upotreba lozinke**.
  - Lozinka mora da se verifikuje, na osnovu kog podatka?
  - Ako je kopija lozinke na računaru, da li neko drugi može da je pročita i zloupotrebi?
  - Koji su tipični problemi vezani za upotrebu lozinke?
- Da li postoji **alternativa lozinkama**?
  - Kartica, PIN, biometrijski podaci, ...
- Sevis koji obezbeđuje proveru identiteta – **autentifikacija**.
- Autentifikacija je u savremenim sistemima zasnovana na **primeni kriptografije**!

Autentifikacija

- Bob treba da pristupi podacima koji se nalaze u AOB.
- Kako AOB zna da je "Bob" zaista Bob?
  - Kao i u slučaju usamljenog računara potrebno je da se verifikuje Bobova lozinka.
- Mada ova dva slučaja deluju veoma slična, proces autentifikacije na mreži je podložan mnogobrojnim napadima.
- Sigurnosni problemi **autentifikacije u mrežnom okruženju**:
  - Trudi ima mogućnost da “vidi” poruku koja se šalje mrežom.
  - Može da je izmeni ili da je zameni svojom porukom.
  - Može da pošalje (snimljenu) poruku iz prethodne Bobove komunikacije.
- Autentifikacija zahteva pažljiv izbor **protokola** koji se koriste u ovu svrhu.
- Kriptologija ima važnu ulogu u implementaciji **sigurnosnih protokola**.

Autentifikacija

- Potreba?
- Sprečiti lažno predstavljanje.



Autorizacija

- Kada AOB autetifikuje Boba, AOB mora da odredi **skup akcija** koje Bob može da preduzme.
- Skup Bobovih akcija je najčešće **podskup svih mogućih akcija** koje poseduje AOB – restrikcija ili dodela prava.
- Primer:
  - Bob ne može da vidi (menja, ...) stanje Čarlijevig računa.
  - Bob ne može da instalira novi softver, itd.
- Dodela prava autentifikovanom korisniku naziva se **autorizacija**.

Kontrola pristupa

- **Kontrola pristupa** je deo sigurnosne politike koja treba da ograniči korisnike i procese u izvođenju različitih akcija nad objektima kao što su datoteke, segmenti zajedničke memorije, ...
- Za svaku takvu akciju mehanizmi kontrole pristupa dodeljuju svakom korisniku posebna ovlašćenja.
- **Kontrola pristupa obuhvata autentifikaciju i autorizaciju**.

Sigurnost softvera

- Kriptografija, protokoli i kontrola pristupa se **najčešće realizuju softverski**.
- Koja su sigurnosna pitanja vezana za softver?
  - Primenjeni softver je po pravilu obiman, **veoma složen**.
    - Velika **verovatnoća postojanja grešaka** (propusta).
  - Softverski propusti su veoma često **uzrok sigurnosnih propusta**.
  - Kako identifikaovati propuste i kako se oni mogu zloupotrebiti?
  - Kako AOB može da bude sigurna da će njen softver raditi u skladu sa očekivanjima?
  - Kako razviti softver sa što manje propusta?

Sigurnost softvera

- Softverski propusti često **nastaju slučajno**.
- Ipak, postoji softver koji je **pisan sa lošom namerom**.
  - Zlonamerni softver (malver): trojanci, logičke bombe, crvi, virusi, *ransomware*, itd.
  - Pitanja:
    - Šta Alisa i Bob mogu da urade sa bi se zaštitili od zlonamerenog softvera?
    - Šta Trudi može da uradi da bi zlonamerni softver bio “efektivniji”?

Sigurnost softvera

- Koji su Bobovi sigurnosni problemi vezani za softver?
  - Kako je Bob siguran da lozinka koju je uneo neće biti “ukradena” i prosleđena Trudi?
  - Kada se Bob poveže na AOB, tj. na stranicu www.alicesonlinebank.com, kako može da bude siguran da njegova komunikacija nije preusmerena?
  - ...

Sigurnost softvera

- Operativni sistemi (OS) sadrže neke zaštitne komponente.
  - Na primer, autentifikaciju, autorizaciju, …
- OS je danas veliki, složen softver.
  - Na primer, Windows XP imao je 40.000.000 linija koda!
  - Podložan je propustima i greškama više od aplikativnog softvera!
  - Mnogi softverski propusti su osobeni za OS.
  - Da li se može verovati OS?

Razmišljati kao Trudi

- U prošlosti, nije postojao ozbiljan i detaljan izvor informacija u vezi “hakerisanja”.
  - Opravdanje: hakerima bi to pomoglo.
- U poslednje vreme se ovaj stav značajno promenio!
- **Dobri momci moraju da razmišljaju kao loši momci**!
  - Slično kao kod policijskih detktiva.
    - Mora se izučavati i razumeti ponašanje kriminalaca.
  - Što se tiče sigurnosti informacionih sistema:
    - Trebamo da shvatimo motive Trudi.
    - Trebamo da izučavamo i poznajemo metode koje koristi Trudi.
    - Često se moramo stavljati u ulogu Trudi.
    - Trebamo da mislimo kao Trudi.
    - Ali **ne smemo da POSTUPAMO** kao Trudi!

Sigurnost počiva na čoveku

- **Sigurnost narušava komfor**!
  - Što je stepen narušavanja komfora veći, veća je verovatnoća da korisnik ne primenjuje mere zaštite.
  - Korisnik koji ne primenjuje dosledno sve mere zaštite može da obesmisli i najbolje osmišljenu sigurnosnu politiku!

Sigurnost počiva na čoveku

- Primer 1.
  - Bob koristi čitač Web-a da pristupi www.amazon.com
  - Veza je zaštićena SSL protokolom koji je zasnovan na primeni kriptografskih tehnika.
  - Sigurnosne tehnike su realizovane softverski.
  - U slučaju napada u toku transakcije, Bob dobija upozorenje.
  - Ukoliko je Bob tipičan korisnik, on će to ignorisati!
- Ishod:
  - Sigurnost je narušena, bez obzira koliko je kriptografski jaka, koliko su dobro osmišljeni protokoli, kontrola pristupa i dizajn softvera.

Sigurnost počiva na čoveku

- Primer 2.
  - Savremeni zaštitni mehanizmi se dobrim delom oslanjaju na upotrebu lozinki.
  - Korisnici teže da odaberu lozinku koju će lako zapamtiti.
- Ishod:
  - Trudi ima lakši posao prilikom “pogađanja” lozinke
- Alternativa:
  - Može se odabrati “teška” lozinka.
  - Tipičan korisnik će je zapisati na papiriću koji će ostaviti na prometnom mestu ...
- Ishod?
- Pitanje: “laka” ili “teška” lozinka ili nešto treće?

Literatura

1. M. Stamp: *Information Security*. John Wiley and Sons.
2. M. Veinović, S. Adamović: Kriptologija 1. Univerzitet Singidunum, Beograd. *
3. M. Milosavljević, S. Adamović: Kriptologija 2. Univerzitet Singidunum, Beograd. *

* Može se besplatno preuzeti sa portala: www.singipedia.com

Hvala na pažnji

Pitanja su dobrodošla.