Kontrola pristupa: autorizacija

Sadržaj

- Kontrola pristupa
- Lampsonova matrica kontrole pristupa
- Modeli sigurnosti sa više nivoa
- Multilateralna bezbednost
- Tajni kanal
- Kontrola zaključivanja
- Captcha
- Mrežne barijere
- Sistemi za detekciju upada

Kontrola pristupa

- Kontrola pristupa se sastoji iz dva dela: autentifikacije i autorizacije
  - **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.
- Primedba:
  - Kontrola pristupa se često koristi kao sinonim za autorizaciju …
  - … ili autentifikaciju?

Autorizacija

- Autorizacija je jedan vid kontrole pristupa.
  - **Subjekat** – korisnik resursa.
    - Ne mora da bude čovek.
  - **Objekat** – sistemski resurs.
- Autorizacija se sprovodi pomoću dva osnovna koncepta:
  - **liste kontrole pristupa** (*Access Control Lists* – ACL) i
  - **liste mogućnosti** (*Capabililities* – C *lists*).
- ACL i C liste su izvedene iz **Lampsonove matrice** kontrole pristupa.

Lampsonova matrica kontrole pristupa

- **Subjekti** – **S**: (korisnici) indeksiraju redove.
- **Objekti** – **O**: (resursi) indeksiraju kolone.

x – izvršenje
w – upis
r – čitanje

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	---	---
Alisa	rx	rx	r	rw	rw
Sem	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

Da li vam je dozvoljeno da to uradite?

- Matrica kontrole pristupa sadrži potrebne informacije.
- Kako?
- Kako upravljati velikom matricom kontrole pristupa (*Access Control*, AC)?
- Ako ima 1000 korisnika i 1000 resursa,
  - tada AC matrica sadrži 1,000,000 elemenata.
  - Potrebna je provera u ovoj matrici pre pristupa bilo kom resursu u sistemu.
- Ovo je vrlo neefikasan način.

Kako povećati efikasnost?

- Matrica kontrole pristupa se deli na kolone ili na redove.
  - Kada je podelimo **na kolone** (ACL):
    - svaka kolona predstavlja jedan objekat,
    - prava pristupa objektu su definisana u koloni.
  - Kada je podelimo **na redove** (C lista):
    - svaki red predstavlja jedan subjekat,
    - prava pristupa subjekta su definisana u redu.

Liste kontrole pristupa

- ACL: deljenje matrice kontrole pristupa po **kolonama**.
- Primer: ACL za *insurance data* je plava.

x – izvršenje
w – upis
r – čitanje

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	---	---
Alisa	rx	rx	r	rw	rw
Sem	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

Prava (C – liste)

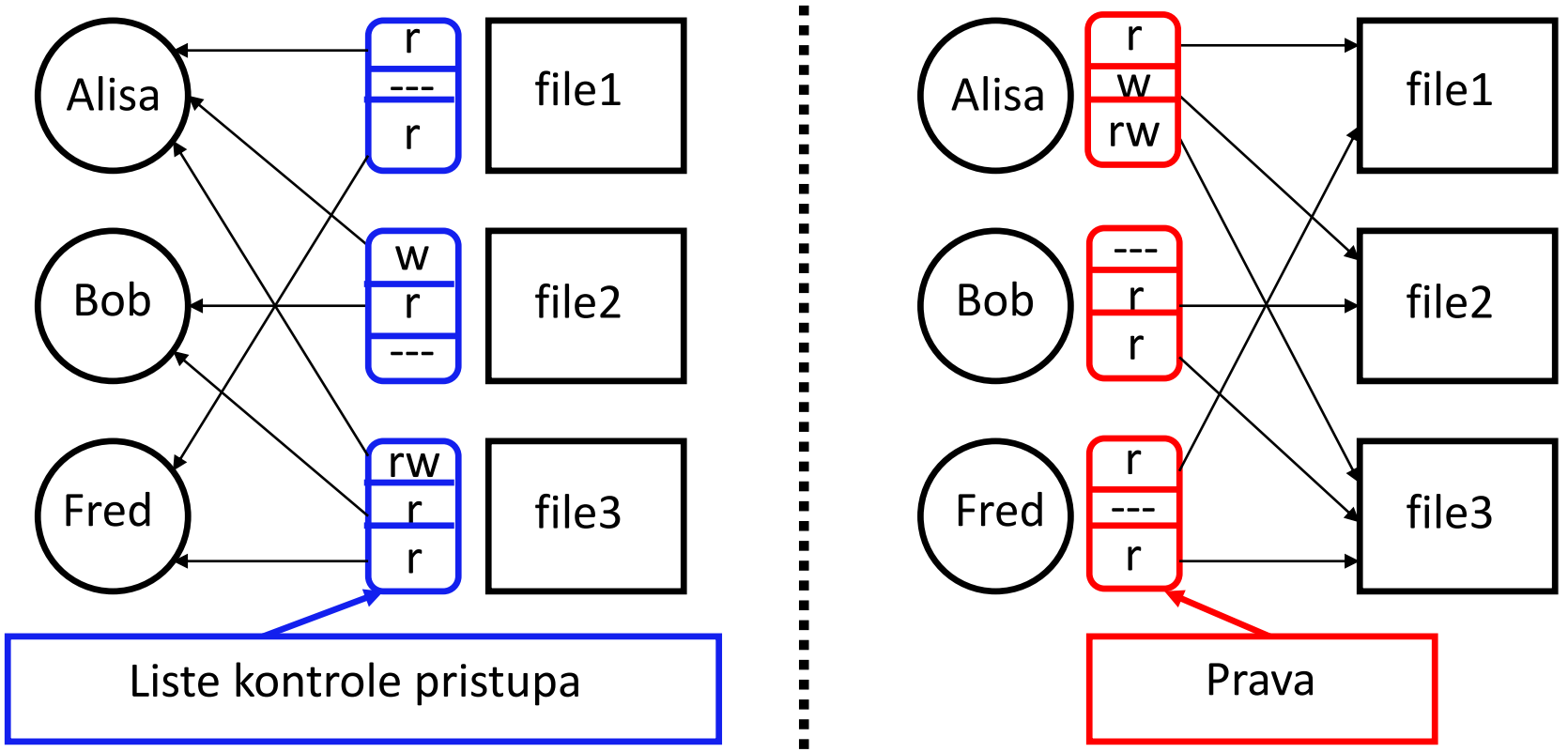
- C – liste: deljenje matrice kontrole pristupa po redovima.
- Primer: prava za Alisu su crvena.

x – izvršenje
w – upis
r – čitanje

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	---	---
Alisa	rx	rx	r	rw	rw
Sem	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

ACL / C – liste

- Primetite da su strelice usmerene u suprotnim smerovima.
- ACL zahtevaju poseban metod za povezivanje korisnika i datoteka.
- C liste – povezivanje korisnika i fajlova je ugrađeno u sistem.

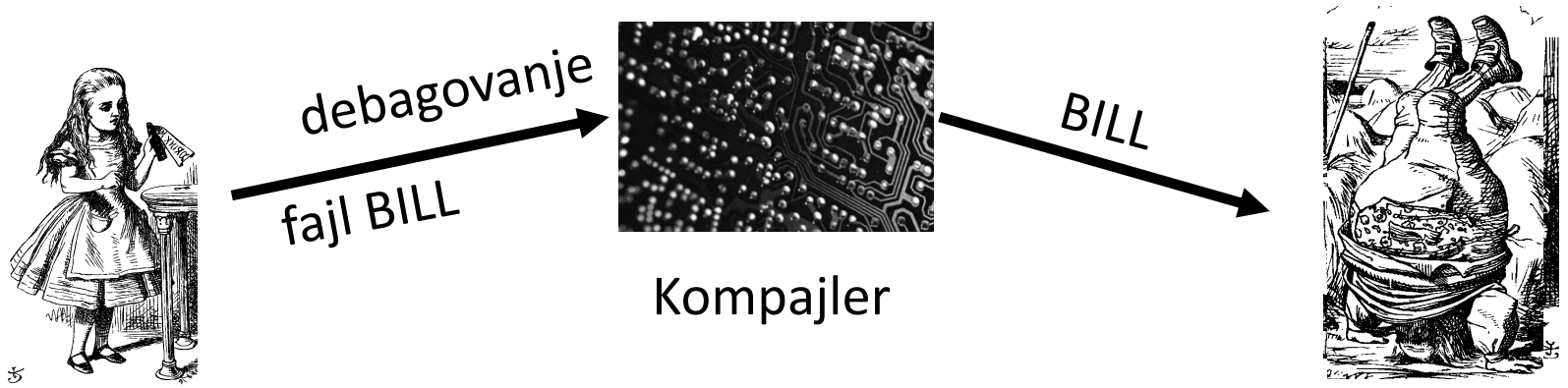


Zbunjeni izaslanik

- Klasičan sigurnosni problem.
- **Dva resursa**.
  - Kompajler i datoteka BILL (informacije o računima).
  - Kompajler može da upisuje u datoteku BILL.
- **Jedan korisnik** (Alisa).
  - Alisa može da pokrene kompajler i dodeli ime datoteci za debagovanje.
  - Alisi nije dozvoljen upis u datoteku BILL (da ne bi narušila sadržaj).
- Matrica kontrole pristupa:

	Kompajler	BILL
Alisa	x	---
Kompajler	rx	rw

ACL i zbunjeni izaslanik



- Kompajler je izaslanik koji deluje u ime Alise.
- Kompajler je zbunjen.
- Alisi nije dozvoljeno da upisuje u datoteku BILL.
- Kompajler je zbunjen jer umesto da radi na osnovu Alisinih prava i dalje radi u skladu sa svojim pravima.
- Izmeniće sadržaj datoteke BILL.

Zbunjeni izaslanik

- Kompajler koji radi za Alisu je zbunjen.
- Sa ACL, ovaj problem se teže rešava.
- Sa C listama, ovaj problem se lakše prevazilazi.
  - Kada Alisa pozove kompajler on može da proveri njenu C – listu.
  - Kompajler može da “vidi” da Alisa nema prava da menja sadržaj datoteke BILL.

ACL / C – liste

- **ACL**.
  - Dobre ako korisnici sami upravljaju svojim datotekama.
  - Zaštita je orijentisana prema podacima.
  - Lako se menjaju prava u odnosu na resurse.
- **C – liste**.
  - Lako se menjaju prava u odnosu na korisnike.
  - Lako se dodaju i brišu korisnici.
  - Lakše se rešava problem zbunjenog izaslanika.
  - Teže su za implementaciju.
- C liste su popularnije u akademskim krugovima, dok se u praksi više koriste ACL.

Modeli sigurnosti sa više nivoa

Stepeni tajnosti i odobrenja

- Stepeni tajnosti se primenjuju **na objekte**.
- Odobrenja se primenjuju **na subjekte**.
- *US Department of Defense* (DoD) koristi 4 stepena tajnosti/odobrenja:
  - *TOP SECRET* – najviši stepen tajnosti,
  - *SECRET* – tajna,
  - *CONFIDENTIAL* – poverljivo i
  - *UNCLASSIFIED* – nije poverljivo.

Stepeni tajnosti i odobrenja

- Da bi se dobilo odobrenje za *SECRET* zahteva se rutinska provera.
- Odobrenje za *TOP SECRET* zahteva ekstenzivnu proveru.
- Praktični problemi određivanja stepena tajnosti:
  - **Pravi stepen poverljivosti** je teško odrediti (dve osobe će dati verovatno različito mišljenje o stepenu poverljivosti neke informacije).
  - **Granularnost** – na kom nivou primenjivati stepene tajnosti (poglavlja mogu biti nepoverljiva, a cela knjiga poverljiva).
  - **Agregacija** – dolaženje do viših stepena poverljivosti analizom nepoverljivih informacija.

Subjekti i objekti

- Neka je O objekat, a S subjekat.
  - Objekat O poseduje stepen poverljivosti.
  - Subjekat S poseduje odobrenje za odgovarajući stepen poverljivosti.
  - Nivo sigurnosti se označava sa L(O) i L(S).
- Za DoD stepene poverljivosti, imamo:
  - *TOP SECRET > SECRET > CONFIDENTIAL > UNCLASSIFIED*.

Modeli sigurnosti sa više nivoa

- MLS (*Multi Level Security*) je neophodan kada subjekti/objekti različitog nivoa koriste iste resurse sistema.
- MLS ima formu **kontrole pristupa**.
- Vojska/država je oduvek imala veliki interes za MLS.
  - Država je uložila velika sredstva u istraživanju MLS.
  - Snaga i slabosti MLS su relativno dobro izučene (teorijski i praktično).
  - Postoje mnoge praktične primene MLS i van vojske (poslovni sistemi i poslovne tajne).

MLS primene

- Poverljive državne/vojne informacije.
- Poslovni primer – informacije ograničene na
  - top menadžere,
  - sve menadžere,
  - sve u kompaniji,
  - opštu javnost.
- Mrežne barijere – držati uljeza na niskom nivou poverljivosti u cilju ograničavanja štete.
- Poverljivost medicinskih informacija, baza podataka, itd …

MLS modeli sigurnosti

- MLS modeli obrazlažu **šta** mora biti urađeno.
- Modeli **ne** govore **kako** to implementirati.
- Modeli su deskriptivni.
  - Opisi na visokom nivou opštosti, bez konkretnih algoritama.
- Postoji obilje MLS modela.
- Prodiskutovaćemo najprostiji MLS model.
  - Ostali modeli su realističniji.
  - Ostali modeli su kompleksniji, teži za uvođenje, teže se verifikuju itd.

Bell-LaPadula – BLP

- BLP model sigurnosti je dizajniran u cilju deklarisanja osnovnih zahteva MLS.
- BLP se odnosi na tajnost.
  - Cilj je sprečavanje neautorizovanog čitanja.
- Podsetimo se da je O objekat, S subjekat.
  - Objekt O poseduje stepen tajnosti.
  - Subjekat S ima odobrenje za odgovarajući stepen tajnosti.
  - Nivoi sigurnosti su označeni sa L(O) i L(S).

Bell-LaPadula – BLP

- BLP se sastoji od sledećeg:
  - **Prost sigurnosni uslov**:
    - S može da čita O ako i samo ako je $L(O) \leq L(S)$
    - Cilj: sprečiti da npr. subjekat sa SECRET ovlašćenjima čita TOP SECRET podatke.
  - *** - svojstvo** (zvezda svojstvo): S može da menja (piše) O ako i samo ako je $L(S) \leq L(O)$.
    - Cilj: sprečiti da se npr. TOP SECRET podatak zapiše i dokument nivoa SECRET.
  - **Ne čitaj naviše, ne piši naniže**.

McLean-ova kritika BLP

- McLean: BLP je “toliko trivijalan, da je teško zamisliti realni model sigurnosti za koji ovo ne važi”.
- McLeanov “sistem Z” dozvoljava administratoru promenu nivoa sigurnosti objekta, a zatim njegov “upis naniže”
- Da li je ovo fer?
- Narušava se duh BLP, ali nije eksplicitno zabranjen u stavovima BLP.
- Postavlja se fundamentalno pitanje o prirodi (i ograničenjima) modelovanja.

Odgovor na kritiku

- BLP je usavršen dopunom **svojstva mirovanja**.
  - **Jako svojstvo mirovanja**: bezbednosne oznake se nikad ne menjaju.
  - **Slabo svojstvo mirovanja**: bezbednosne oznake se mogu menjati samo ako promena ne narušava “utvrđenu politiku bezbednosti”.
- Jako svojstvo mirovanja je nepraktično u realnom svetu.
  - Često želimo da podržimo “najmanje privilegije”.
  - Daje korisnicima najmanje privilegije neophodne za obavljanje tekućeg posla.
  - Nakon toga se privilegije povećavaju, ako je to potrebno (i ako to politika sigurnosti dozvoljava).
  - Ovaj princip je poznat pod nazivom ***high water mark*** princip.

Bell-LaPadula – BLP

- BLP je jednostavan, ali verovatno isuviše jednostavan.
- BLP je jedan od malog broja sigurnosnih modela koji se mogu koristiti za dokazivanje bezbednosnih svojstava sistema.
- BLP je inspirisao ostale modele sigurnosti.
  - Većina drugih modela teže da budu što realniji.
  - Drugi modeli sigurnosti su znatno složeniji.
  - Drugi modeli su teški za analizu i/ili primenu u praksi.

Biba model

- BLP je sigurnosni model za **tajnost**, dok je Biba model za **integritet**.
  - Biba sprečava neautorizovano upisivanje.
- Biba je (u izvesnom smislu) **dualan u odnosu na BLP**.
- Model integriteta.
  - Pretpostavimo da verujemo integritetu O^* ali ne i O^{**}.
  - Ako objekat O sadrži objekte O^* i O^{**} tada više ne možemo verovati integritetu objekta O.
- Nivo integriteta O je minimum integriteta od svih objekata koje O sadrži.
- ***Low water mark*** princip za integritet.

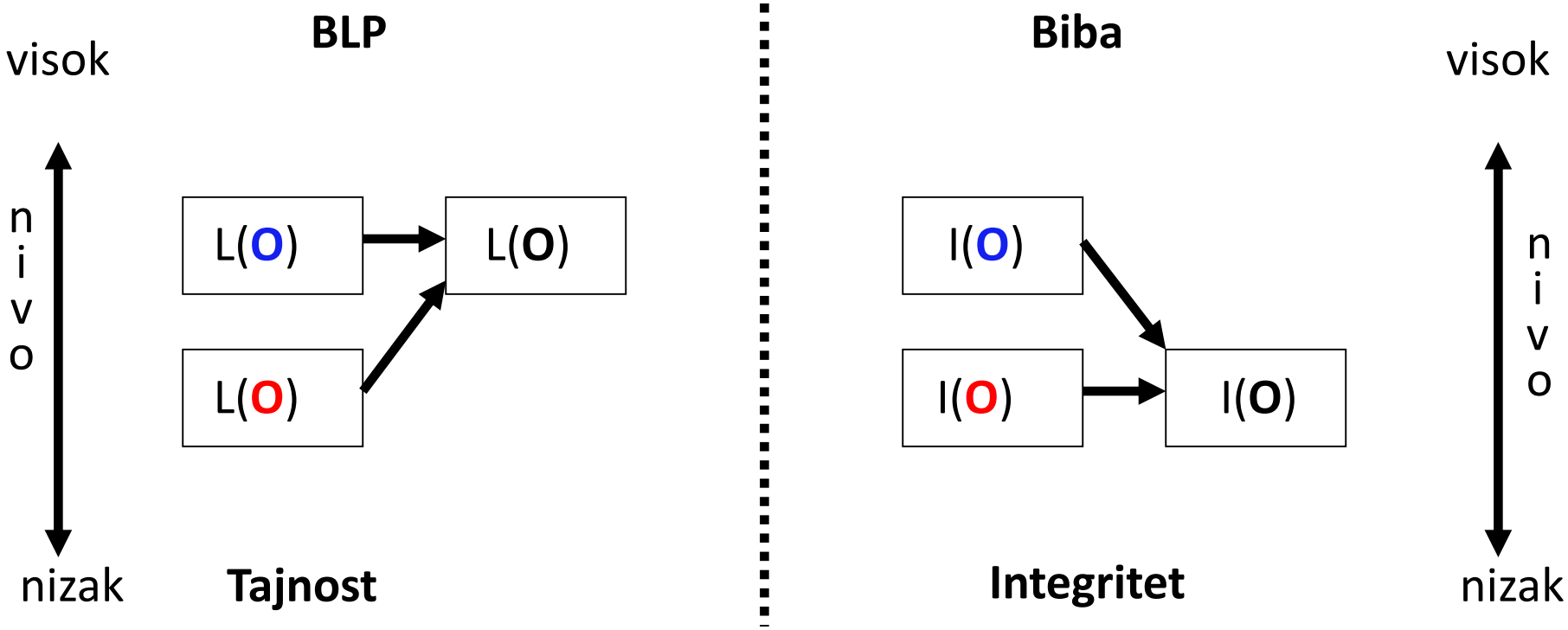
Biba model

- Neka I(O) označava integritet objekta O a I(S) integritet subjekta S.
- Biba se može formulisati na sledeći način:
- **Pravilo pristupa upisivanja**: S može da menja (piše u) O ako i samo ako $I(O) \leq I(S)$.
  - Ne verujemo u ono što je S napisao ništa više nego što verujemo S.
- **Biba model**: S može da čita O ako i samo ako je $I(S) \leq I(O)$.
  - Integritet S nije ništa veći od najmanjeg integriteta onoga što je pročitao.

Biba model

- Ovaj model je, takođe, veoma restriktivan.
- Sprečava S da čita objekte koji imaju niži stepen integriteta.
- Često je poželjno da se Biba Model zameni sa *Low Water Mark* pravilom:
  - Ako S čita O, tada je I(S) = min(I(S), I(O))
- Integritet S se smanjujnje kada pristupa objektima nižeg nivoa.

BLP/Biba


BLP
visok
nivo
nizak
L(O)
L(O)
L(O)
L(O)
Tajnost
Biba
visok
nivo
nizak
I(O)
I(O)
I(O)
I(O)
Integritet

Multilateralna bezbednost

Multilateralna sigurnost

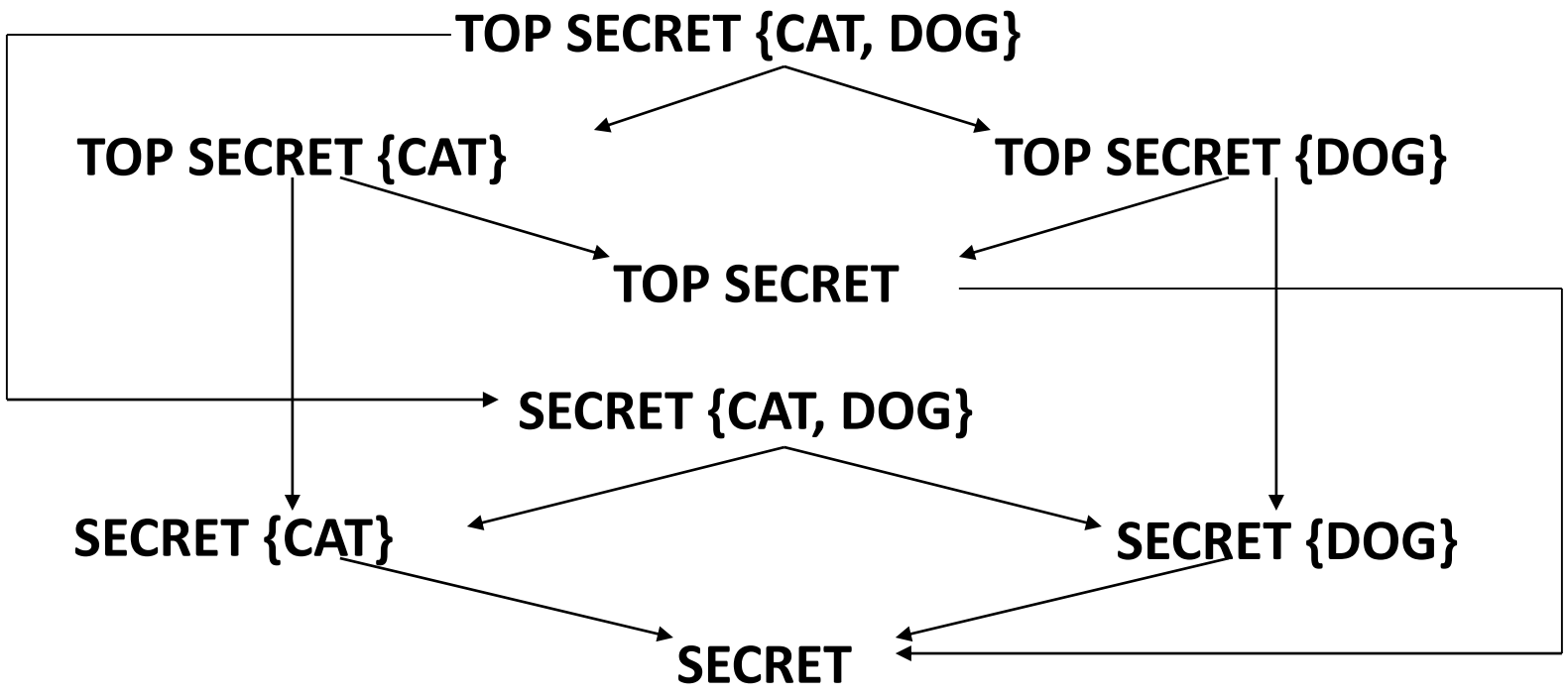
- **MLS** (*Multilevel Security*) nameće kontrolu pristupa na gore i na dole.
- Prosta hijerarhija sigurnosnih oznaka nije dovoljno fleksibilna.
- Multilateralna sigurnost nameće kontrolu pristupa nad kreiranjem posebnih odeljaka.
- Neka je TOP SECRET podeljen na TOP SECRET {CAT} i TOP SECRET {DOG}.
- Oba su TOP SECRET ali su informacioni tokovi ograničeni unutar TOP SECRET odeljka.

Multilateralna bezbednost

- Zašto odeljci?
  - Zašto se ne kreira novi sigurnosni nivo?
- Zato što možda ne želimo da važi:
  - TOP SECRET {CAT} ≥ TOP SECRET {DOG}
  - TOP SECRET {DOG} ≥ TOP SECRET {CAT}
- Odeljci omogćavaju nametanje principa “neophodno je znati”.
  - Bez obzira na ovlašćenja, omogućen je pristup samo onim informacijama koje je neophodno da znate.

Multilateralna bezbednost

- Strelice označavaju relaciju ≥.
- Nisu svi nivoi sigurnosti uporedivi, npr. TOP SECRET {CAT} prema SECRET {CAT, DOG}.



Multilateralna bezbednost

- MLS se može koristiti bez multilateralne bezbednosti i obrnuto.
- Ali, MLS skoro uvek uključuje multiratelarnost.
- Primer:
  - MLS je primenjen za zaštitu medicinskih dosijea Britanske medicinske asocijacije (*British Medical Association*, BMA)
  - AIDS je TOP SECRET, a recepti su SECRET.
  - Šta je nivo sigurnosti lekova za AIDS?
  - Sve teži ka nivou sigurnosti TOP SECRET.
  - Narušava se svrha sistema!
- Umesto ovog pristupa koristi se multilateralna sigurnost.

Tajni kanal

Tajni kanal

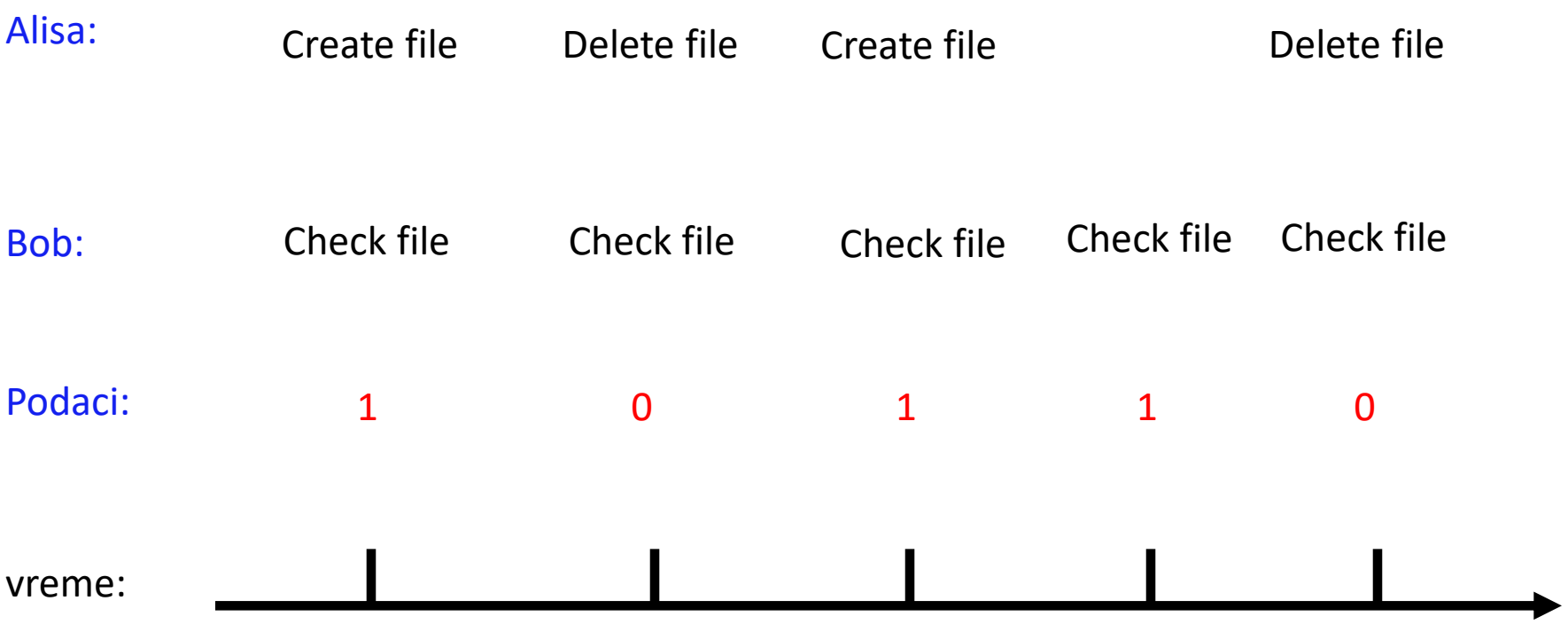
- MLS je namenjen za restrikciju legitimnih kanala komuniciranja.
- Možda postoje i neki drugi načini za protok informacija.
- Na primer, resursi deljeni između različitih nivoa mogu prenositi neke informacije.
- **Tajni kanal** je komunikacioni kanal koji nije predviđen od strane dizajnera sistema.

Tajni kanal

- **Primer**.
  - Alisa ima TOP SECRET ovlašćenje, Bob poseduje CONFIDENTIAL ovlašćenje.
  - Pretpostavimo da memorijski prostor datoteka dele svi korisnici.
  - Alisa kreira datoteku FileXYzW ako želi da prenese informaciju “1” Bobu, i briše ovu datoteku ako želi da prenese informaciju “0”.
  - Svakog minuta Bob izlistava datoteka.
    - Ako datoteka FileXYzW ne postoji, Alisa je poslala 0.
    - Ako datoteka FileXYzW postoji, Alisa je poslala 1.
  - Alisa može na ovaj način da šalje TOP SECRET informacije Bobu!

Tajni kanal

- **Primer**.



Tajni kanal

- **Drugi primeri**:
  - red čekanja za štampanje,
  - ACK poruke,
  - mrežni saobraćaj, itd.
- Kada tajni kanal postoji?
  1. Predajnik i prijemnik dele neke zajedničke resurse.
  2. Predajnik može da varira neka svojstva koja može da posmatra prijemnik.
  3. Komunikacija između predajnika i prijemnika može biti sinhronizovana.

Tajni kanal

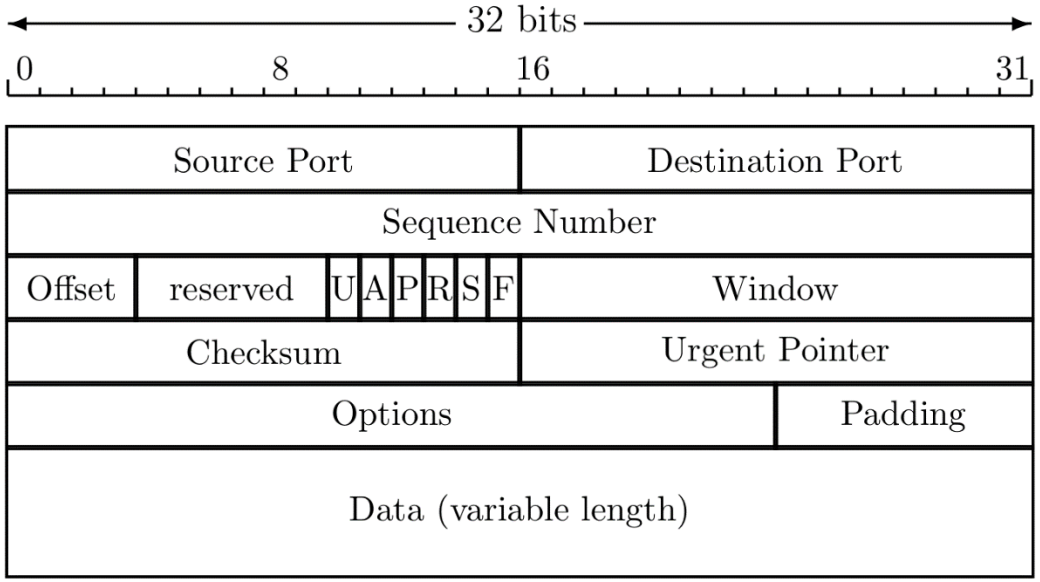
- Tajni kanali postoje gotovo svugde.
- Tajni kanal se lako eliminiše.
  - Pod uslovom da se eliminišu svi zajednički resursi i sve komunikacije.
- Gotovo je nemoguće eliminisati sve tajne kanale u bilo kom korisnom sistemu.
- DoD uputstvo: cilj je redukcija kapaciteta tajnog kanala na ne više od 1 bit/sekundi.
  - Ova preporuka znači da je DoD odustalo od eliminacije tajnih kanala!

Tajni kanal

- Razmotrimo 100MB TOP SECRET datoteku.
  - Otvoreni tekst je smešten u TOP SECRET lokaciju.
  - Šifruje se AES algoritmom i 256-bitnim ključem, a šifrat se smešta na UNCLASSIFIED lokaciju.
- Pretpostavimo da smo redukovali kapacitet tajnog kanala na 1 bit po sekundi.
- Bilo bi potrebno više od 25 godina da bi informacije iz datog dokumenta iscurele tajnim kanalom.
- Ali, trebalo bi samo 5 minuta da iscuri 256-bitni AES ključ kroz isti tajni kanal!

Tajni kanal

- Praktični tajni kanal.



- Sakrivanje podataka u TCP “reserved” polju zaglavlja.
- Upotrebiti covert_TCP, alat za sakrivanje podataka u poljima: sequence number, ACK number …

Kontrola zaključivanja

- Pretpostavimo sledeći upit jednoj bazi podataka.
  - Pitanje: Kolika je prosečna zarada profesora računarskih nauka ženskog pola na univerzitetu SJSU?
    - Odgovor: $95,000.
  - Pitanje: Koliko ima profesora računarskih nauka na univerzitetu SJSU?
    - Odgovor: 1.
- Specifične informacije se mogu dobiti iz odgovora na opšta pitanja!

Kontrola zaključivanja i istraživanja

- Npr, medicinski dosijei su privatni, ali su od velike važnosti za istraživanja.
- Kako učiniti informacije iz ovih dosijea dostupnim istraživačima a da se ne naruši privatnost?
- Kako pristupati ovim podacima bez mogućnosti izvlačenja specifičnih informacija?

Naivna kontrola zaključivanja

- Izbaciti imena iz medicinskih dosijea?
- I dalje se mogu lako dobiti specifične informacije iz takvih “anonimiziranih” podataka.
- Isključivanje imena nije dovoljno.
  - Kao što se vidi iz prethodnog primera.
- Šta još treba učiniti?

Manje naivna kontrola zaključivanja

- Kontrola dimenzije skupa upita.
  - Ne davati odgovor ukoliko je skup odgovora isuviše mali.
- *N*-ispitanika, *k*% dominatno pravilo.
  - Ne davati statistiku ukoliko se *k*% ili više rezultata izvodi iz *N* ili manje subjekata
  - Primer pitanje: kolika su prosečna primanja u susedstvu Bila Gejtsa?
    - Iz tog pitanja se na osnovu odgovarajućeg izbora *N* i *k* ne mogu odrediti primanja Bila Gejtsa.
- Randomizacija.
  - Dodavanje malog šuma podacima.
- Mnoge druge metode – nijedna nije zadovoljavajuća.

Kontrola zaključivanja – zaključak

- **Robusna kontrola zaključivanja** možda nije ni moguća.
- Da li je slaba kontrola zaključivanja bolja od nepostojanja bilo kakve kontrole?
  - **Da**, redukuje se količina informacija koja curi, a time se i ograničava šteta.
- Da li je slaba kriptozaštita bolja od nepostojanja bilo kakve kriptozaštite?
  - **Verovatno ne**: bolje znati da nije sigurno nego...

CAPTCHA

Tjuringov test

- Predložio Alan Tjuring 1950.
- Čovek postavlja pitanja drugom čoveku i računaru (ne videći ih i ne znajući ko je ko).
- Ako čovek (ispitivač) ne može da razlikuje ko je čovek a ko računar, kažemo da je računar prošao Tjuringov test.
- “Zlatni standard” veštačke inteligencije.
- Ni jedan računar do danas nije prošao ovaj test.

CAPTCHA

- CAPTCHA – ***C****ompletely* ***A****utomated* ***P****ublic* ***T****uring test to tell* ***C****omputers and* ***H****umans* ***A****part*.
  - U prevodu: potpuno automatizivani javni Tjuringov test za razlikovanje čoveka od računara.
- *Automated* – računar generiše test i ocenjuje od odgovore.
- *Public* – program i podaci su javni.
- *Turing test* kaže … – ljudi mogu proći test, ali mašine ne mogu.

CAPTCHA paradoks

- “… CAPTCHA je program koji generiše i ocenjuje testove …”
- Paradoks – računar kreira i ocenjuje rezultate testa, koje ni sam ne može da prođe!
- CAPTCHA je dizajniran za restrikciju pristupa nekim resursima.
- CAPTCHA je koristan za kontrolu pristupa.

CAPTCHA upotreba

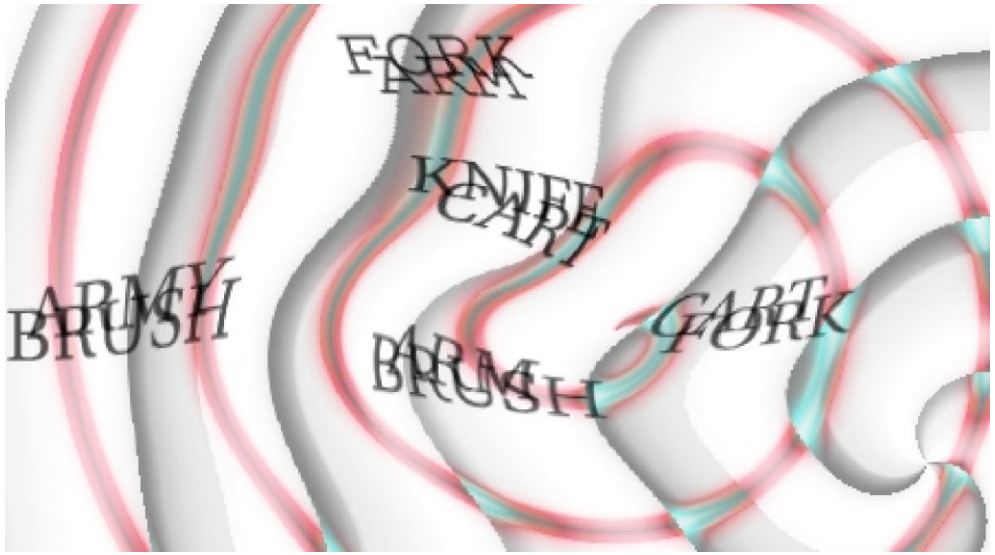
- Originalna motivacija: sprečavanje da automatizovani Web roboti pune glasačku kutiju za glasanje za najbolju školu iz računarskih nauka (MIT, CMU).
- Besplatni servisi e-pošte – spameri koriste Veb robote u cilju otvaranja na hiljade email naloga
  - Yahoo mail itd.
- Sajtovi koji ne žele da budu automatski indeksirani od nekog pretraživača.
  - ...

CAPTCHA – pravila igre

- Mora biti laka prepreka za većinu ljudi.
- Mora biti teška ili nesavladiva prepreka za prolaz automatizovanih sistema.
  - Čak i uz poznavanje CAPTCHA softvera.
- Poželjno je imati različite CAPTCHA testove.
  - Slepi ljudi ne mogu da prođu vizuelni test, itd.

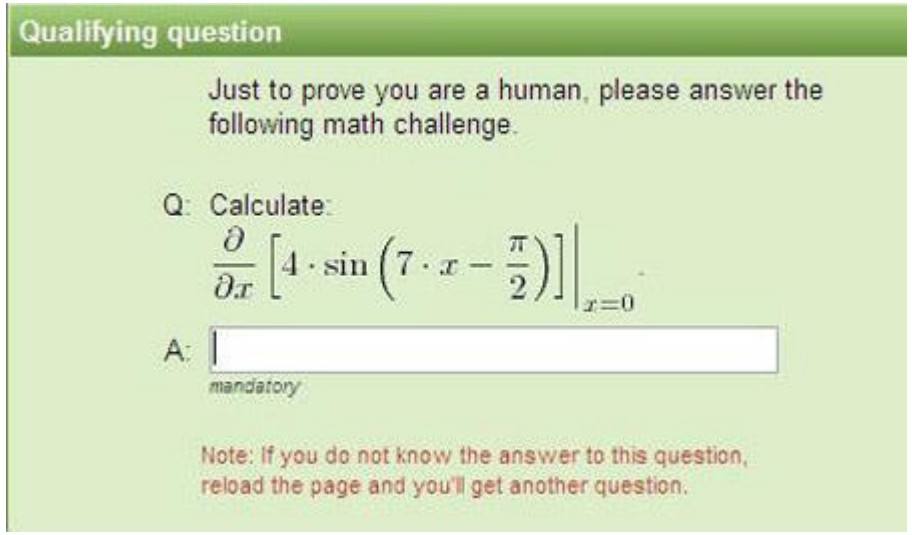
Da li CAPTCHA postoji?

- Test: naći dve reči u ponuđenoj slici.
- Lako za većinu ljudi, teško za računare (OCR problem).



CAPTCHA

- Savremene vrste CAPTCHA.
  - Vizuelne:
    - kao prethodni primer,
    - mnoge druge.
  - Audio:
    - izobličene reči ili audio zapis.
  - ...

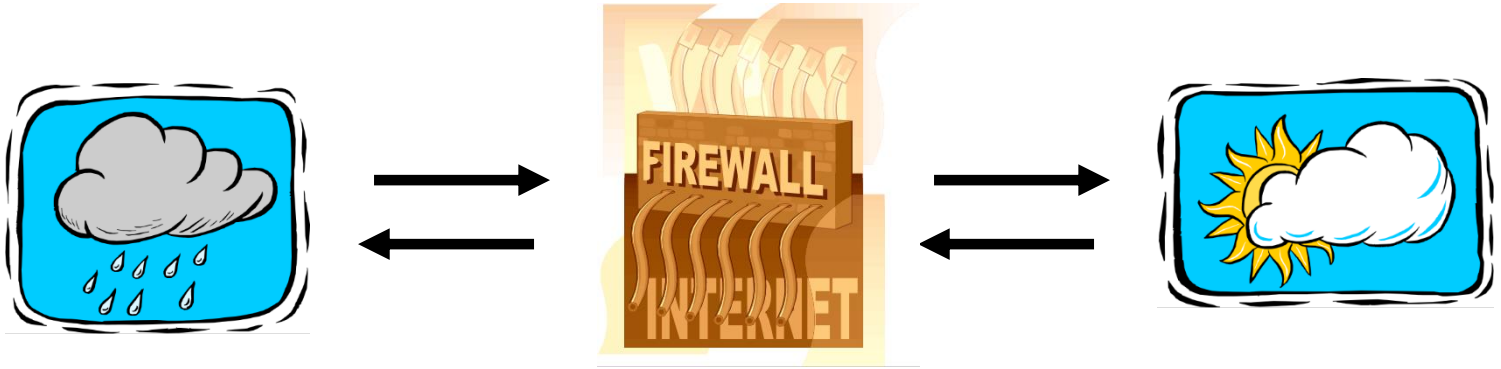


CAPTCHA i veštačka inteligencija

- Računarsko prepoznavanje izobličenog teksta je problem veštačke inteligencije.
  - Čovek ovo sa lakoćom rešava.
- Isto važi za izobličeni zvuk.
  - Čovek je dobar u rešavanju i ovog problema.
- Hakeri koji razbiju CAPTCHA bi rešili jedan težak problem veštačke inteligencije.
- Stavljanje hakerskih napora u korisnu funkciju!

Firewalls

Firewalls



Internet Firewall Interna mrežica

- *Firewall* mora da odredi šta će se propustiti u internu mrežu i/ili šta će se dopustiti da iz nje izađe.
- Interna mreža se (ne)opravdano smatra sigurnom.
- Statistika: 80% napada iznutra.
- Kontrola pristupa za mreže.

Firewalls

- *Firewall* je sličan sekretarici.
- Da bi ste se sreli sa nekim rukovodiocem:
  - prvo kontaktirate njegovu sekretaricu,
  - sekretarica procenjuje da li je sastanak opravdan,
  - sekretarica filtrira mnoge zahteve.
- Želite da se sastanete sa predsednikom departmana univerziteta?
  - Sekretarica će izvršiti izvesno filtriranje.
- Želite da se sastanete sa predsednikom države?
  - Sekretarica će da izvrši značajno filtriranje!

Firewalls – teminologija

- Ne postoji standardizovana terminologija.
- Svi tipovi se zasnivaju na ispitivanju podataka u paketima do određenog nivoa protokola.
- Tipovi *firewalla*:
  - *packet filter* – radi na mrežnom sloju,
  - *stateful packet filter* – transportni sloj,
  - *application proxy* – aplikacioni sloj,
  - *personalni firewall* – bilo koji od tri prethodna dizajniran za pojedinačnog korisnika ili malu kućnu mrežu.

Packet filter

- Radi na mrežnom sloju, na relativno niskom nivou TCP/IP pprotokola.
- Administrator definiše pravila (najčešće).
- Filtracija se zasniva na:
  - IP adresi izvora,
  - odredišnoj IP adresi,
  - portu pošiljaoca (*source port*),
  - odredišnom portu,
  - *flag* bitovima (SYN, ACK, itd.),
  - definisanim pravilima za odlazne i dolazne pakete.

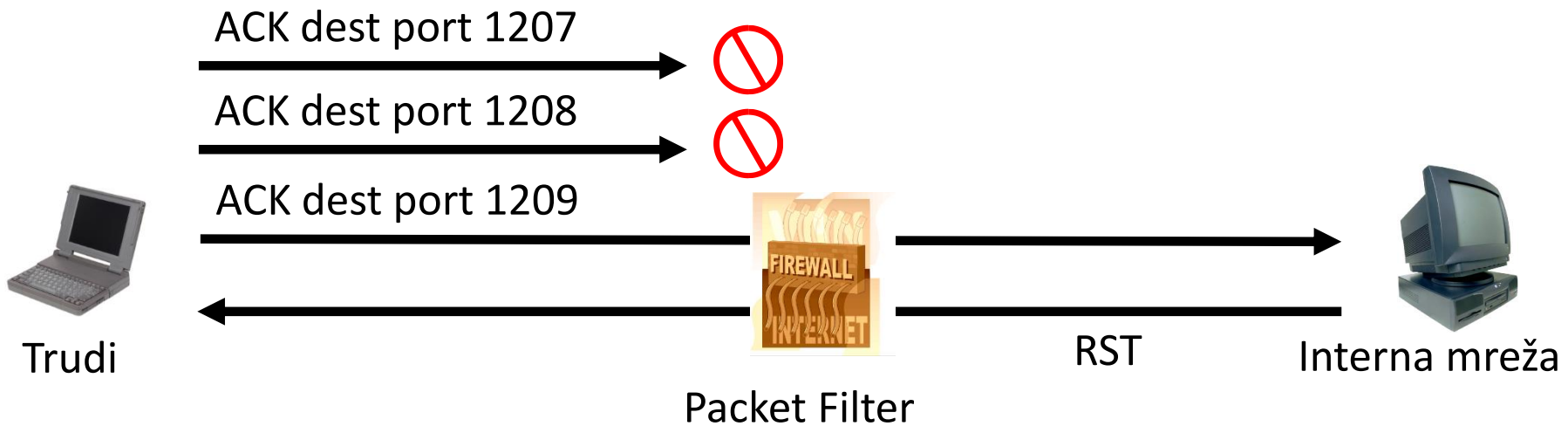
Packet filter

- Prednosti:
  - brzina,
  - efikasnost.
- Nedostaci:
  - Svaki paket se ispituje nezavisno (kontekst?)
  - Ne može da ispita TCP konekciju.
  - “Slep” za aplikacione podatke u kojima se danas upravo kriju mnogi virusi.

TCP ACK skeniranje

- Napadač šalje inicijalni paket sa setovanim ACK bitom, bez poštovanja protokola (prvi paket treba da ima SYN bit).
- Narušava TCP/IP protokol.
- ACK paketi prolaze kroz filter paketa *firewalla*.
  - Izgleda kao deo već uspostavljene konekcije.
- Na prijemnom hostu se detektuje problem i šalje se RST paket koji kaže pošiljaocu da završi konekciju.
- Napadač skenira otvorene portove kroz *firewall*, tako što šalje ACK na odabrani port, pa ako dobije RST paket, zaključuje da firewall propušta pakete u internu mrežu kroz taj port.
- Ako pak ne dobije RST paket, taj port je pod blokadom *firewalla* (nije otvoren) – **napad: TCP ACK scan**.

TCP ACK skeniranje



- Napadač zna da je port 1209 otvoren kroz *firewall*.
- *Stateful packet filter* može da spreči ovakve napade.
- Pošto ACK skeniranje nije deo uspostavljene konekcije.

Stateful packet filter

- Dodaje stanja paketskom filtru – prati (analizira) tok konekcije.
- Radi na transportnom sloju.
- Pamti TCP konekciju i fleg bit.
- Može čak da pamti UDP pakete (tj., DNS zahteve).
- Prednosti:
  - Mogu da urade sve što mogu da urade filtri paketa i mnogo više od toga ...
  - Čuva informacije o tekućoj konekciji.
- Nedostaci:
  - Ne vide se aplikacioni podaci.
  - Sporiji je od paketskog filtra.
    - Zahteva dodatnu analizu podataka.

Application Proxy

- *Proxy* je nešto što radi u vaše ime.
- *Application Proxy* posmatra i ulazne aplikativne podatke.
- Verifikuje da su podaci sigurni pre njihovog prihvatanja.
- Kreira novi paket pre slanja u internu mrežu.
- *Proxy* ima kompletan uvid u konekciju.
- Prednosti:
  - Kompletan pogled na konekciju i aplikativne podatke.
  - Filtrira loše podatke na aplikacionom sloju (virusi, Word makroi, ...)
- Nedostaci:
  - Brzina.

Sistemi za detekciju upada

Sprečavanje upada

- Želimo da onemogućimo pristup lošim momcima.
- Sprečavanje upada je tradicionalni interes računarske sigurnosti.
  - Autentifikacijom se vrši sprečavanje upada.
  - *Firewall* je jedan od oblika sprečavanja upada.
  - Odbrana od virusa, takođe.
  - Uporedivo je sa zaključavanjem vrata automobila.
- Ipak, ne može se uvek sve sprečiti ...

Detekcija upada

- I pored sprečavanja upada, loši momci uspevaju da se probiju u sistem.
- Sistemi za detekciju upada – (*Intrusion detection systems* – IDS)
  - detektuju upade (pre, za vreme i posle),
  - tragaju za “neuobičajenim” aktivnostima.
- IDS je razvijen na osnovu analize log fajlova.
- IDS je danas vrlo aktuelna oblast istraživanja.

Sistemi za detekciju upada

- Ko je najverovatniji uljez?
  - Možda je neko spolja pošto je prošao *firewall*.
  - Možda je zlonamerni insajder.
- Šta uljez može da uradi?
  - Primeni dobro poznate napade.
  - Primeni varijacije dobro poznatih napada.
  - Primeni novi ili malo poznati napad.
  - Iskoristi sistem da napadne druge sisteme.
  - Itd …

IDS

- Dve metode za detekciji upada:
  - IDS zasnovani na potpisu.
  - IDS zasnovani na detekciji anomalija.
- Dve osnovne IDS arhitekture:
  - *Host-based* IDS (HIDS).
  - *Network-based* IDS (NIDS).
- Većina sistema se može klasifikovati na ovaj način …
  - Uprkos suprotnim marketinškim tvrdnjama!

HIDS

- Nadgleda aktivnosti na hostu u cilju detekcije
  - poznatih napada,
  - sumnjivih aktivnosti.
- Namenjen za detekciju napada, kao što su
  - prekoračenje bafera,
  - zloupotreba (prekoračenje) privilegija,
  - itd …
- Ovi sistemi imaju malu ili uopšte nemaju mogućnost praćenja mrežnih aktivnosti

NIDS

- Nadgledanje i analiza mrežne aktivnosti.
  - Poznati napadi.
  - Sumnjive mrežne aktivnosti.
- Dizajnirani da detektuju napade kao što su
  - DoS (*Denial of Service*),
  - *network probes*,
  - formiranje malicioznih paketa,
  - itd …
- Ovi sistemi imaju malu ili uopšte nemaju mogućnost praćenja napada na *host*.

Detekcija potpisa – primer

- Greške u logovanju mogu ukazati na postojanje napada tipa krekovanja lozinki.
- IDS može da koristi pravilo “N pogrešnih prijavljivanja na sistem u M sekundi” kao potpis.
- Ukoliko se detektuje N ili više neuspešnih pokušaja u M sekundi, IDS upozorava na napad.
- Ovo upozorenje je specifično.
  - Administrator se upozorava da se sumnja na napad.
  - Administrator može da verifikuje napad (ili lažnu uzbunu).

Detekcija potpisa – primer

- Neka IDS izdaje upozorenje kad god imamo N ili više pogrešnih prijavljivanja na sistem u M sekundi.
- N i M se moraju tako postaviti da nema previše lažnih uzbuna.
- Ovo možemo uraditi na osnovu normalnog režima rada.
- Ako napadač zna N i M, može preduzeti sledeću strategiju: pokušati N-1 prijavljivanja na system u svakih M sekundi!
- U ovom slučaju, detekcija potisa usporava napad, ali ga ne može sprečiti.

Detekcija potpisa – primer

- Mnoge tehnike se koriste da bi se detekcija potpisa mogla obaviti što robusnije.
- Uobičajeni cilj je detekcija tzv. “skoro potpisa”.
- Na primer, ako je “oko” N pokušaja logovanja u “oko” M sekundi.
  - Upozoriti na mogući napad krekovanja lozinki.
  - Šta su razumne vrednosti za “oko”?.
  - Može se koristiti iskustvo, statistika itd.
  - Mora se pri tome voditi računa da se ne poveća verovatnoća greške lažnog alarma.

Detekcija potpisa

- Prednosti detekcije potpisa:
  - jednostavna,
  - detektuju se poznati napadi,
  - zna se koji je napad u igri u trenutku detekcije,
  - efikasna (za razuman broj potpisa).
- Nedostaci detekcije potpisa:
  - baza potpisa mora biti ažurna,
  - broj potpisa ne sme biti prevelik,
  - mogu se detektovati samo poznati napadi,
  - varijacije poznatih napada se ne mogu uvek detektovati.

Detekcija anomalija

- Sistemi za detekciju anomalija tragaju za nobičnim i nenormalnim ponašanjem.
- Postoje barem dva izazova.
  - Šta smatrati normalnim za jedan sistem?
  - Koliko “daleko” od normalnog je nenormalno?
- Neophodna je statistika!
  - Srednja vrednost definiše normalnost.
  - Varijansa ukazuje koliko daleko je nenormalno ponašanje od normalnog.

Detekcija anomalija

- Kako meriti normalnost?
  - Mora se meriti u toku “reprezentativnog” ponašanja.
  - Ne sme se meriti u toku napada jer će u suprotnom i napad izgledati kao normalan!
  - Normalan je statistička srednja vrednost.
  - Mora se meriti i varijansa da bi postojala realna šansa za uspešnu detekciju.

Detekcija anomalija

- Nenormalno je relativno u odnosu na “normalno”.
  - Nenormalnost ukazuje na mogući napad.
- Tehnike statističke diskriminacije:
  - Bajesova statistika,
  - linearna diskriminaciona analiza (LDA),
  - kvadratna diskriminaciona analiza (QD),
  - neuronske mreže, skriveni Markovljevi modeli, itd.
- Koriste se i moderne tehnike modelovanja, kao što su veštački imunološki sistemi.

Problemi detekcije anomalija

- Sistem se neprekidno menja, i sa njim se mora menjati i IDS.
- Statički sistemi preopterećuju administratore.
  - S druge strane IDS koji evolvira čini mogućim da napadač polako ubeđuje IDS da je napad normalan!
  - Napadač pobedjuje jednostavnom strategijom “napreduj polako”
- Šta “nenormalan” stvarno znači?
  - Samo da postoji mogućnost napada.
  - Ne govori ništa konkretno o napadu!
- Kako odgovoriti na ovakve nejasne informacije?
- Detekcija potpisa nam govori egzaktno o kom napadu je reč.

Detekcija anomalija

- Prednosti sistema za detekciju anomalija:
  - postoji šansa da detektuju nove vrste napada,
  - mogu biti efikasni.
- Nedostaci sistema za detekciju anomalija:
  - danas se ne koriste sami za sebe,
  - moraju se koristiti zajedno sa sistemima zasnovanim na potpisu,
  - pouzdanost nije jasna,
  - podložan je napadima,
  - detekcija anomalija indicira nešto neuobičajeno.
  - nedostaju specifične informacije o mogućem napadu!

Literatura

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

Hvala na pažnji

Pitanja su dobrodošla.