
Bezbednost poslovanja na internetu

Bezbednost poslovanja na Internetu

- Bezbednosno okruženje elektronskog poslovanja
- Mere fizičke bezbednosti u elektronskom poslovanju
- Kriptografske mere bezbednosti
- Klasična kriptografija
- Moderna kriptografija
- Primena kriptografije
- Bezbednosni protokoli
- Mesta mogućih napada i kriptoanalize

Bezbednosno okruženje elektronskog poslovanja

- Računarska konkurencija osnažila je poslovnu konkurenciju, ali isto tako je doprinela razvoju kriminala koji novim, moćnim alatima nastoji da izvrši razne pronevere i gubitke sredstava.
- Bezbednosne mere u komunikaciji putem računarske tehnologije dobijaju na značaju kako u poslovnom tako i u privatnom sektoru.
- Sistem elektronskog poslovanja treba **da spreči obavljanje transakcije koju je inicirao nelegitimni korisnik.**
- S obzirom na to da je komunikaciona mreža izložena prisluškivanju, podaci koji putuju mrežom mogu biti iskorišćeni za zloupotrebu.

Mere fizičke bezbednosti u elektronskom poslovanju

- Treba ispuniti mere **fizičke zaštite sistema** i koristiti savremene mehanizme zaštite podataka odnosno **kriptografiju.**
- Elektronske transakcije u ime firme treba da obavlja osoba koja je **obučena za korišćenje specijalizovanog softvera** koji se za te svrhe koristi kao i da bude upoznata sa osnovnim svojstvima datog sistema elektronskog prenosa sredstava.
- Vlasnik komunikacionog servisa elektronskog prenosa sredstava ovlašćuje takvu osobu koja dobija identifikacionu karticu i lični identifikacioni broj (***Personal Identification Number* – PIN**) sa kojim se vrši autorizacija.

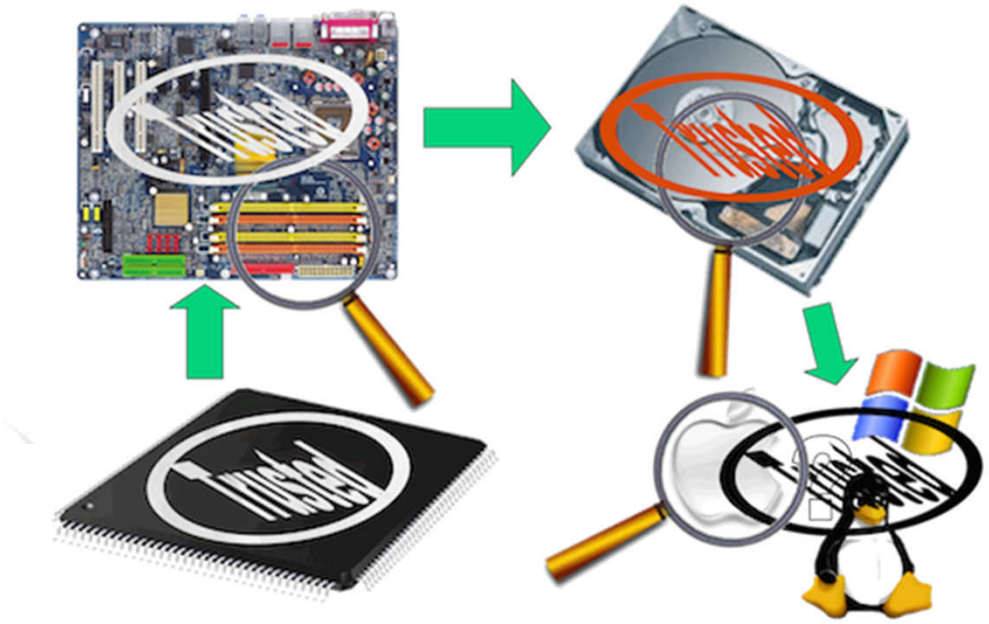
Mere fizičke bezbednosti u elektronskom poslovanju

- U uslovima šireg korišćenja elektronskog poslovanja aplikacije za obavljanje elektronskih transakcija su daleko jednostavnije što ne zahteva dodatnu obuku, te se kontrola pristupa bazira isključivo na posedovanju odgovarajuće identifikacione kartice.

- Ukoliko se operacije sa PIN-om i poverljivim podacima sa identifikacione kartice izvršavaju unutar (običnog) računara korisnika, sistem je izložen prisluškivanju.

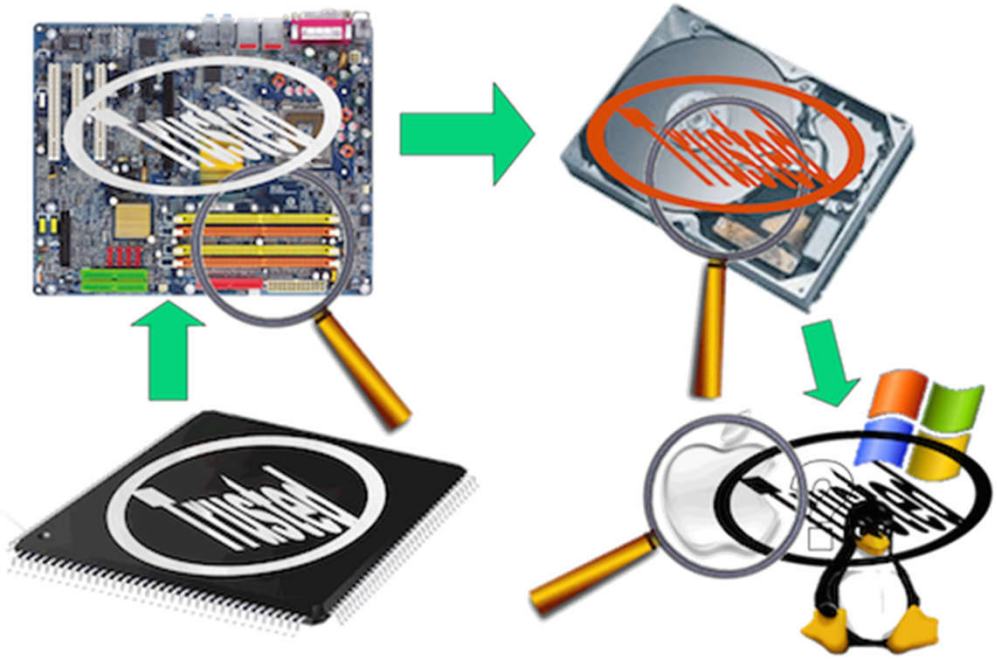
Mere fizičke bezbednosti u elektronskom poslovanju

- Iz razloga prisluškivanja proizvodi se tzv. **hardver od poverenja** (*trusted hardware*) ili **neprobojni hardver** (*tamper-resistant*) unutar kojih se izvršavaju sve delikatne operacije nad poverljivim podacima.
- Dati hardver povezan je na računar preko kojeg se pristupa komunikacionoj mreži.
- Primer može biti bezbednosni modul (*security module*) unutar POS (*Point Of Sale*) terminala (npr. kase u prodavnici).



Mere fizičke bezbednosti u elektronskom poslovanju

- Korišćenje poverljivog hardvera je obavezno u slučaju da se identifikacija vrši proverom identičnosti podataka na kartici i podataka smeštenih u bazu drugog kraja komunikacije.
- Poverljiv hardver je “produžena ruka” banke koja zajedno sa proizvođačem hardvera garantuje poverljivost.



Mere fizičke bezbednosti u elektronskom poslovanju

- U slučaju elektronskog plaćanja poverljiv hardver može biti sama **inteligentna (smart) kartica.**
- Funkcije pristupnog hardvera može preuzeti i sama kartica čime dobijamo tzv. elektronski novčanik koji je opremljen tastaturom i displejom.
- Bez bezbednosnog uređaja podaci svake transakcije su podložni zloupotrebi jer se pretpostavlja da bilo ko može ugraditi virus (npr. trojanca) u potrošačev računar koji može da snimi sve poverljive podatke koji se u njemu nalaze, kao što su PIN, lozinka, itd.
  - Virus može izazvati lokalnu transakciju između napadača i potrošačeve kartice a da on to ni ne zna.

Kriptografske mere bezbednosti

- Konkretni bezbednosni zahtevi elektronskog poslovanja variraju zavisno od karakteristika sistema i od nivoa poverenja koji se pretpostavlja u sistemu.
- Generalno, elektronski sistemi plaćanja moraju ispuniti osnovne kriptografske zahteve:
  - **Integritet poruka**
  - **Autorizaciju korisnika**
  - **Poverljivost podataka**
  - **Neporecivost**

- Sistemi plaćanja koji održavaju integritet poruka ne izvršavaju nijednu delikatnu operaciju (npr. promena stanja računa) dok se ne izvrši eksplicitna provera autentičnosti korisnika.
- Autorizacija korisnika je najvažniji zadatak u sistemima plaćanja i može se izvršiti na više načina.

Autorizacija putem pomoćnog kanala

- U ovom sistemu autorizacije (*out-band authorization*) postoje dva učesnika: verifikaciona strana (obično banka) i autorizaciona strana (kupac).
- Verifikaciona strana (banka) obaveštava kupca u vezi transakcije.
- Od kupca se zahteva da potvrdi ili opovrgne plaćanje korišćenjem posebnog, tajnog kanala (npr. poštom, telefonom...).
- Autorizacija putem pomoćnog kanala je najzastupljenija pri kupovini pomoću kreditnih kartica za telefonske ili e-mail narudžbine (kada se transakcija obavlja kroz nezaštićen kanal).
- **Svako ko zna broj nečije kartice može da kupi šta želi.**
- Korisnik ako želi da ima kontrolu nad svojim računom mora da proverava svoju listu plaćanja kod banke i da uloži žalbu u određenom roku (obično 90 dana) – inače se podrazumeva da je transakcija potvrđena.

Autorizacija pomoću lozinke

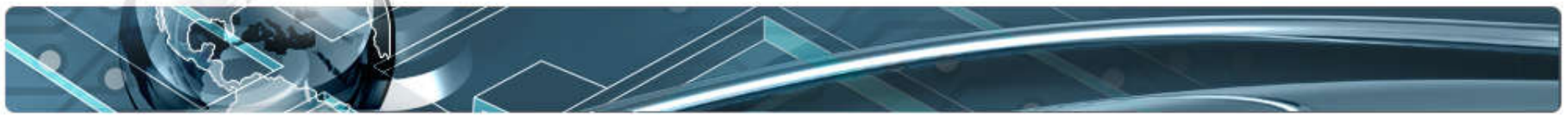
- U transakciji zaštićenoj lozinkom (***password***) zahteva se da svaka poruka koju šalje kupac sadrži posebnu kriptografsku vrednost za proveru autentičnosti koja se računa na osnovu tajne koja je poznata samo strani verifikacije (banka) i strani autorizacije (kupac).
- Tajna može biti lični identifikacioni broj (PIN), lozinka ili bilo koji drugi oblik tzv. deljene tajne (***shared secret***).
- Deljene tajne koje imaju malu dužinu – kao 4-cifreni PIN – izložene su različitim vrstama napada.
- One ne mogu obezbediti visok nivo bezbednosti, te se zato koriste samo u kontroli pristupa smart kartici koja izvršava konkretan autorizacioni algoritam primenom kriptografskih mehanizama, kao na primer digitalni potpis.

Autorizacija pomoću digitalnog potpisa

- Verifikaciona strana zahteva od kupca da digitalno potpiše transakciju
- Digitalni potpis obezbeđuje jedan od ciljeva kriptografije – neporecivost.
- Digitalni potpis obezbeđuje autentičnost poruke i na izvestan način čuva njen integritet.
- Korespodenti u elektronskoj trgovini mogu zahtevati da transakcija bude poverljiva.
- Poverljivost u kontekstu elektronske trgovine podrazumeva ograničenja u poznavanju pojedinih delova informacije koje se odnose na kupovinu: identitet kupca/prodavca, sadržaj nabavke, količina, vrednost, itd.
- Poverljivost podrazumeva da informacija koja se štiti bude dostupna samo korespodentima koji su uključeni u elektronsku transakciju.

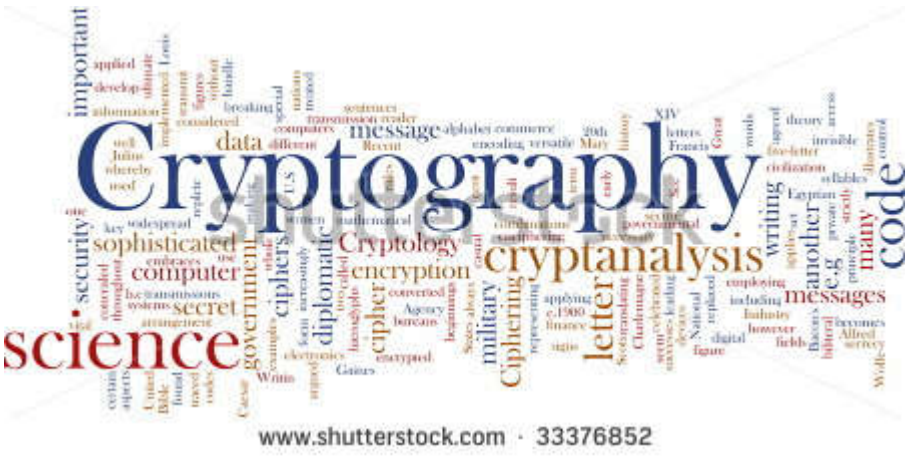
Klasična kriptografija

- **Kriptovanje** (*encryption*) jeste transformacija podataka u oblik koji je gotovo nemoguće pročitati bez određenog znanja (tajne, ključa).
- Svrha kriptovanja je da obezbedi privatnost podataka tako što skriva informaciju od svakog kome ta informacija nije namenjena, pa čak i od onih kojima je kriptovan podatak dostupan.
- **Kriptografija** (*criptography*) danas može da se shvati kao skup tehnika i aplikacija za kriptovanje koje se zasnivaju na matematički kompleksnim problemima.
- **Kriptoanaliza** (*cryptoanalysis*) je oblast u kojoj se nastoji da se kompromituju kriptografski mehanizmi.
- **Kriptologija** (*cryptology* – cryptos logos, grč. tajna reč) kao nauka o tajnim komunikacijama objedinjuje pomenute dve discipline, kriptografiju i kriptoanalizu.



Klasična kriptografija

- **Dekriptovanje** (*decription*) je inverzna operacija kriptovanju, ona transformiše kriptovane podatke u razumljivu formu.
- Kriptovanje i dekriptovanje koriste određeni vid tajne informacije, poznate pod nazivom **ključ** (*key*).
- U nekim kriptografskim mehanizmima isti ključ se koristi i za kriptovanje i za dekriptovanje, dok u pojedinim ključ za kriptovanje može biti različit od ključa za dekriptovanje.



Klasična kriptografija

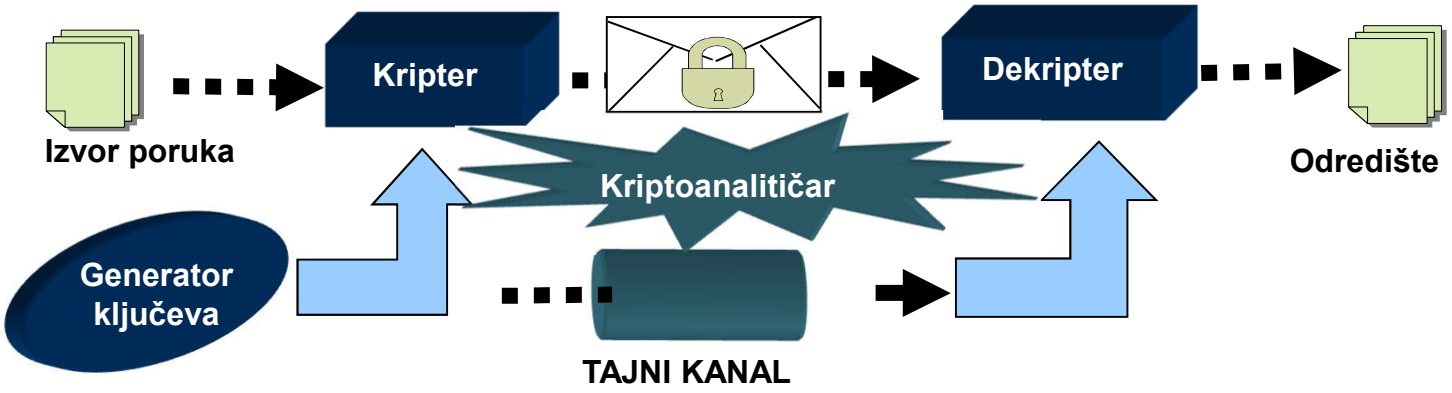
- Kriptografija daje brojne mehanizme i procedure.
- Digitalni potpis povezuje dokument sa vlasnikom odgovarajućeg ključa, dok digitalni pečat povezuje dokument sa vremenom kreiranja.
- Sa nekoliko kriptoalatki, moguće je izgraditi šeme i protokole koji nam omogućavaju da plaćamo pomoću elektronskog novca, da dokažemo da posedujemo određenu informaciju bez da znamo njen sadržaj i da razdelimo tajnu informaciju na delove na takav način da podskup delova može rekonstruisati tajnu informaciju.

Klasična kriptografija
Simetrična kriptografija

- Simetrična kriptografija ili kriptografija sa tajnim ključem je tradicionalni oblik kriptografije u kom se isti ključ koristi kako za kriptovanje tako i za dekriptovanje.
- Kriptografski algoritam vrši obradu originalne poruke, i pretvara je u *ciphertext* ili **kriptogram**, čime se ostvaruje prvi cilj kriptografije.
- Kako oba korespodenta koriste identične ključeve potrebno je na odgovarajući način razmeniti ključ (za tu priliku uveden je pojam tajnog kanala kojim se ključ razmenjuje).
- **Tajni kanal je najslabije mesto** simetričnog kriptografskog sistema.
- Osnovni problem kriptografije sa tajnim ključem jeste razmena tajnog ključa koja treba da se izvrši na takav način da niko ne otkrije sadržaj tajnog ključa.

Simetrična kriptografija

- Razmena ključa zahteva kriptografske metode u kojima se učesnici u komunikaciji ne plaše prisluškivanja.
- Prednost simetrične kriptografije leži u praktičnoj realizaciji gde se ovaj metod pokazuje kao vrlo brz, odnosno, nema velikih zahteva u računanju.



Simetričan kriptografski sistem

Algoritmi

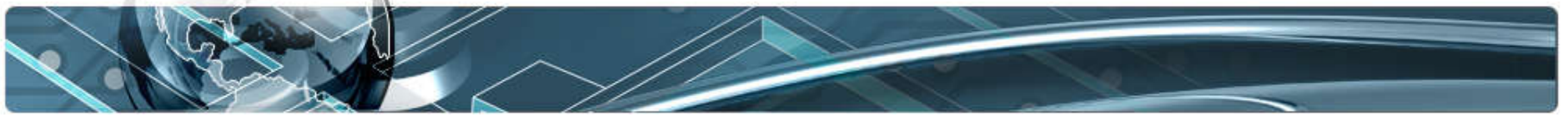
- Najčešće tehnike sa tajnim ključem su:
  - blok-šifra (*block cipher*)
  - autorizacioni kod poruke (*Message Authentication Code* – MAC)
- **Blok šifra** je vrsta simetrične kriptografije u kojoj se blok poruke fiksne dužine transformiše u blok kriptograma iste dužine.
- Transformacija se obezbeđuje primenom tajnog ključa.
- U većini primena dužina bloka je 64 ili 128 bita.
- Najzanimljivija blok-šifra je tzv. iterativna blok-šifra, koja kriptuje poruku u nekoliko ciklusa.
- U svakom ciklusu ista transformacija se primenjuje korišćenjem podključa.
- Broj ciklusa u algoritmu zavisi od željenog nivoa bezbednosti.
- U većini slučajeva povećan broj ciklusa poboljšaće bezbednost u odnosu na neiterativnu blok-šifru.

Hash funkcije

- **Hash funkcija** H(x) je transformacija poruke proizvoljne dužine u hash vrednost h = H(x) tačno definisane dužine.
- Osnovni zahtevi koje kriptografske hash funkcije moraju ispuniti su:
  - Ulazna poruka može biti proizvoljne dužine (što se može postići iterativnom ili lančanom strukturom hash algoritma).
  - Izlaz mora biti fiksne dužine (izlaz ne sme zavisiti od dužine ulazne sekvence).
  - H(x) mora biti relativno jednostavna za računanje za bilo koje x (mora imati malu kompleksnost računanja).
  - H(x) mora biti jednosmerna funkcija (određivanje inverzne funkcije je gotovo nemoguće, odnosno velike kompleksnosti).
  - H(x) mora biti otporna na koliziju (pronalaženje y takvo da je H(y) = H(x) je gotovo nemoguće, odnosno velike kompleksnosti).

Hash funkcije

- **Hash vrednost koncizno reprezentuje poruku ili dokument iz kog je izračunata.**
- Često se hash vrednost naziva siže poruke (*message digest*).
- Primeri često korišćenih hash funkcija u kriptografiji su MD2, MD4, MD5 i SHA (*secure hash algorithm*).
- **Najvažnija uloga hash funkcija u kriptografiji jeste omogućavanje provere integriteta poruke i digitalni potpis.**
- S obzirom da su hash funkcije mnogo brže nego kriptografski algoritmi, uobičajeno je da se digitalni potpis i provera integriteta omoguće primenom kriptografskih alata nad hash vrednostima koje su daleko manje dužine nego sam dokument.



MAC

- **Autentikacioni kod poruke** (*Message Authentication Code* – **MAC**) je autentikaciona reč izvedena pomoću autentikacionog protokola iz poruke korišćenjem tajnog ključa.
- Za razliku od digitalnog potpisa MAC se poredi i verifikuje pomoću istog ključa, što znači da može biti verifikovan samo od strane određenog korisnika.
- Najznačajniji tipovi MAC-a:
  - Zasnovan na hash funkcijama
  - Zasnovan na blok šifri

Moderna kriptografija

- U klasičnoj kriptografiji oba korespodenta znaju i koriste isti tajni ključ
- Glavni problem jeste kako obezbediti način da se korespodenti dogovore o tajnom ključu a da niko ne sazna tajni ključ
- Svako ko zna tajni ključ može da ga upotrebi kasnije za čitanje, modifikaciju i zloupotrebu svih poruka koje su kriptovane ili autorizovane pomoću tajnog ključa

Moderna kriptografija

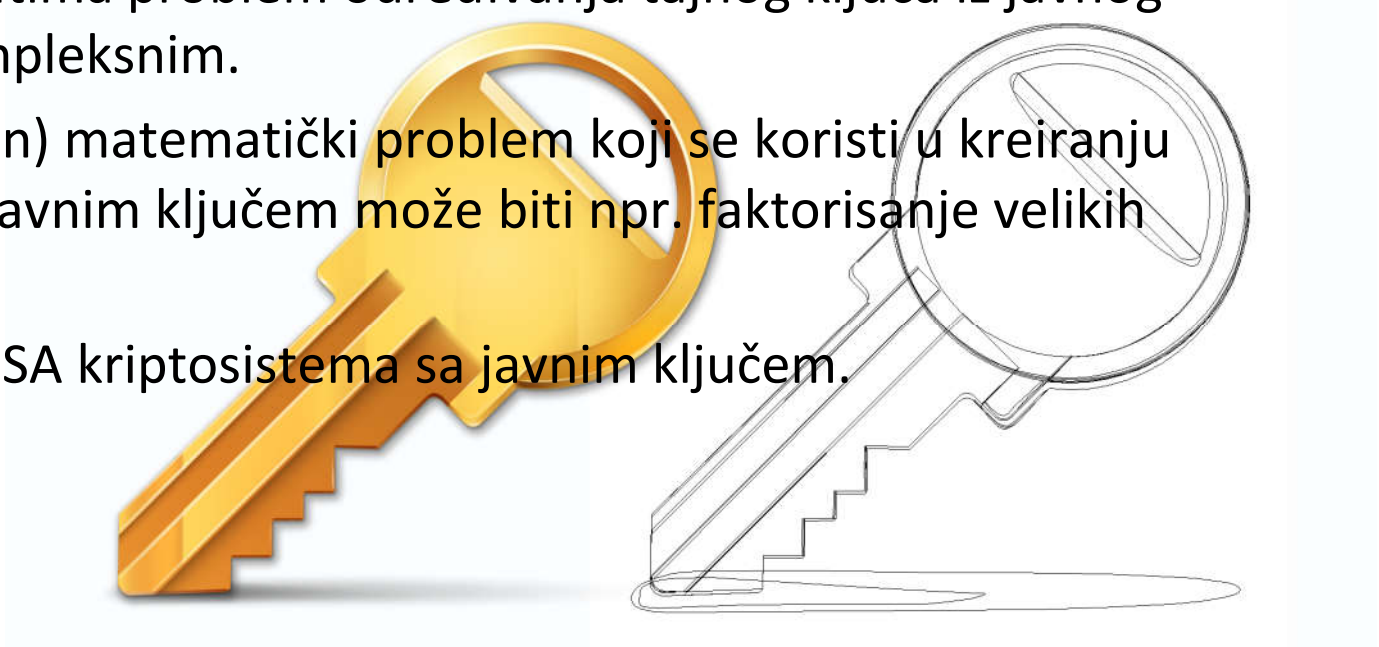
- Generisanje, prenos i skladištenje ključeva zove se upravljanje ključem (*key managment*).
- S obzirom na to da svi ključevi moraju ostati tajni, kriptografija sa tajnim ključem ima očit problem u obezbeđivanju tajnosti u upravljanju ključem, naročito u otvorenim sistemima sa velikim brojem učesnika.

Asimetrična kriptografija

- Motivisani problemom upravljanja ključem, Diffie i Hellman su 1976. godine predstavili koncept kriptografije sa javnim ključem.
- **Kriptografija sa javnim ključem ima dve značajne primene: kriptovanje i digitalni potpis.**
- Svaki učesnik dobija par ključeva, jedan tajni i jedan javni ključ.
- Javni ključ se objavljuje dok tajni čuva korisnik.
- Potreba za razmenom tajne informacije kao u slučaju simetrične kriptografije je eliminisana.
- Pre svake komunikacije prenosi se samo javni ključ, dok se tajni ključ nikad ne prenosi niti razmenjuje.
- U ovakvom sistemu nema potrebe verovati u bezbednost komunikacionih sredstava; dovoljno je pridružiti javni ključ korisniku na autentičan način (u koji se ne sumnja), na primer siguran javni imenik.

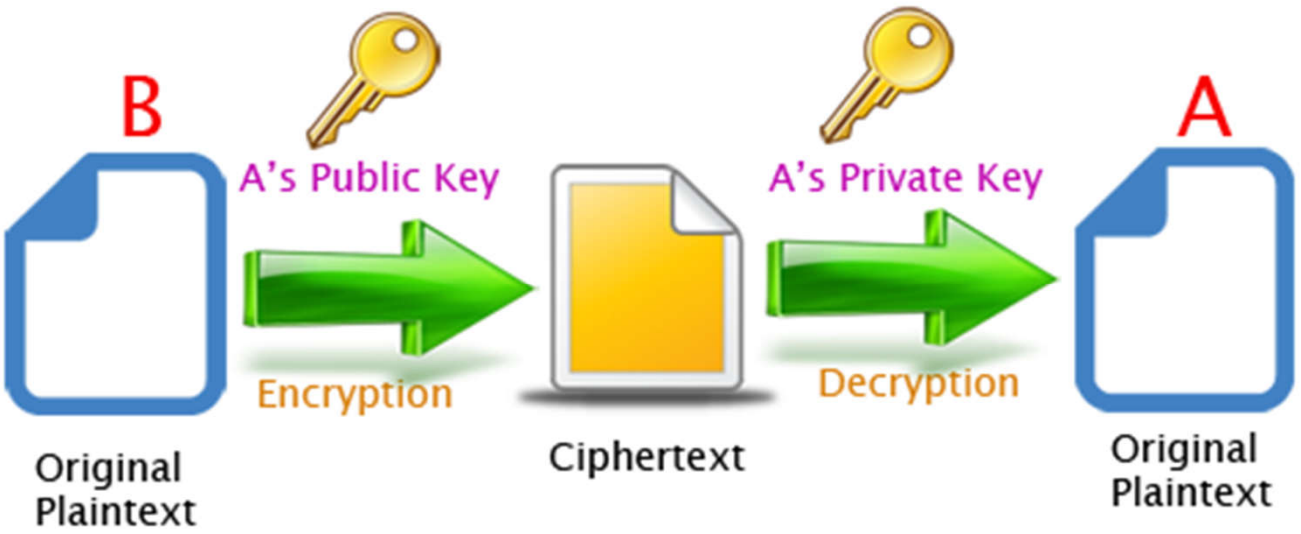
Asimetrična kriptografija

- Bilo ko može slati poruke korišćenjem javnog ključa ali takav kriptogram može biti dekriptovan samo tajnim ključem.
- U kriptosistemu sa javnim ključem, tajni ključ je matematički povezan sa javnim ključem.
- Moguće je napasti ovakav kriptosistem određivanjem tajnog ključa iz javnog.
- Odbrana od ovakvog napada ostvaruje se tako što se savremenim matematičkim alatima problem određivanja tajnog ključa iz javnog načini veoma kompleksnim.
- Težak (kompleksan) matematički problem koji se koristi u kreiranju kriptosistema sa javnim ključem može biti npr. faktorisanje velikih brojeva.
- Ta ideja stoji iza RSA kriptosistema sa javnim ključem.



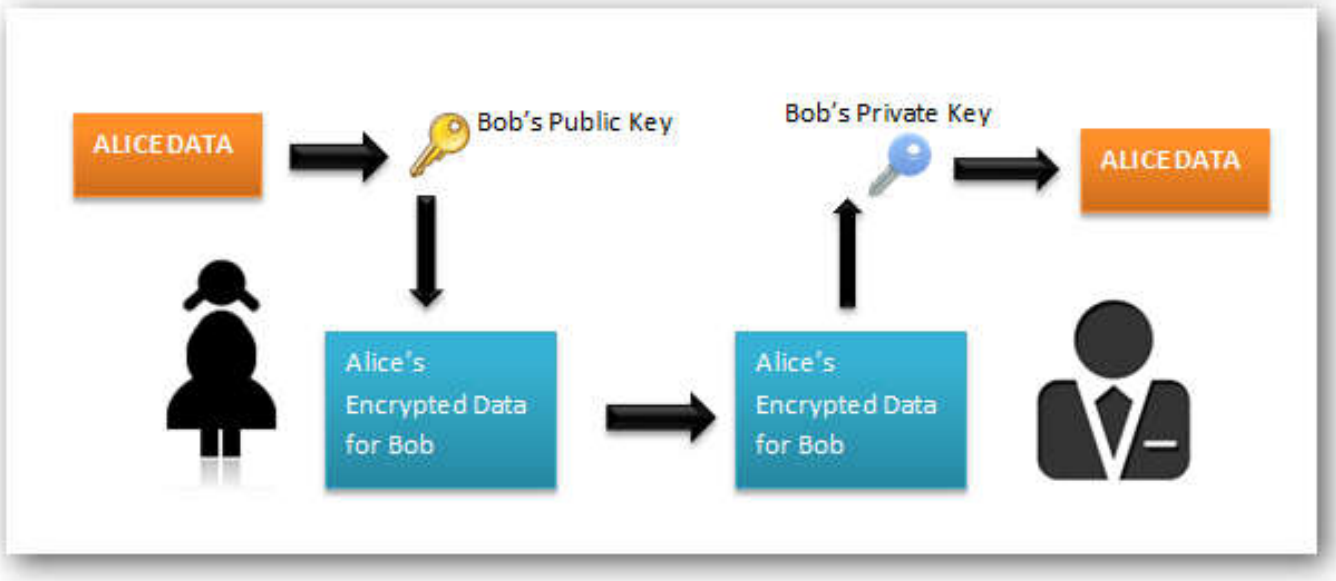
Asimetrična kriptografija

- Ako pošiljalac hoće da pošalje poruku, prvo potraži javni ključ primaoca u imeniku, koristi ga za kriptovanje poruke i šalje kriptogram.
- Primalac koristi svoj tajni ključ za dekriptovanje kriptograma i čita poruku.
- Ko god prisluškuje komunikaciju ne može dekriptovati poruke.
- Svako može slati kriptovane poruke primaocu, ali samo on može da ih čita (jer jedino on zna svoj tajni ključ).



Asimetrična kriptografija

- Da bi potpisao poruku pošiljalac koristi svoj tajni ključ i poruku.
- Izlaz je poznat kao digitalni potpis i spaja se sa porukom.
- Kako bi verifikovao potpis, primalac koristi poruku i pošiljaočev javni ključ i poredi dobijen rezultat sa digitalnim potpisom.
- Ukoliko rezultat nije korektan ili je potpis pogrešan ili je komunikacija ometana.



Moderna kriptografija
Asimetrična kriptografija

- Primarna prednost kriptografije sa javnim ključem jeste rešavanje problema distribucije ključeva.
- U sistemu sa tajnim ključem, tajni ključ mora da se prenese s obzirom da se isti ključ koristi i za kriptovanje i za dekriptovanje.
- **Sledeća značajna prednost kriptografije sa javnim ključem je mogućnost digitalnog potpisivanja koji se ne može poreći.**
- **Autentifikacija pomoću tajnog ključa zahteva razmenu određene informacije i ponekad zahteva prisustvo treće strane u čije poverenje se ne sumnja.**
- Pošiljalac može opovrgnuti autentifikaciju poruke tvrđenjem da je tajna informacija (ključ) na neki način kompromitovana.
- Slabost kriptografije sa javnim ključem je brzina računanja.
- Postoje brojni kriptografski metodi sa tajnim ključem koji su značajno brži od bilo kog trenutno korišćenog kriptosistema sa javnim ključem.

Asimetrična kriptografija

- Za kriptovanje, najbolje rešenje je kombinovan sistem kako bi se postigle prednosti kriptografije sa javnim ključem i brzina kriptografije sa tajnim ključem.
- Ovakav protokol se naziva digitalna koverta (***digital envelope***).
- Nepotrebno je koristiti kriptografiju sa javnim ključem u okruženjima sa jednim ili dva korisnika.
- U okruženjima sa više korisnika najbolje je koristiti kriptografiju sa javnim ključem.

Asimetrična kriptografija

- **Da bi se sprečilo lažno predstavljanje uvodi se dokument zvan digitalni sertifikat koji povezuje određenu osobu sa određenim javnim ključem.**
- **Sertifikaciona tela (*Certifcation Authority* – CA) izdaju digitalni sertifikat uz prethodnu proveru identiteta.**
- Uspešan napad na sertifikaciono telo omogućilo bi napadaču da se lažno predstavi i da promeni podatke u imeniku, ali se sve čini da se to ne desi.

Primena kriptografije

- Tipična primena kriptografije je komunikacioni sistem baziran na osnovnim alatkama (simetričnoj kriptografiji).
- Ovakvi sistemi mogu imati različite nivoe kompleksnosti.
- Neki od najjednostavnijih su:
  - Tajna komunikacija
  - Identifikacija
  - Autentifikacija
  - Razmena tajne
- Malo složenije primene su:
  - Elektronska trgovina
  - Sertifikacija
  - Tajna elektronska pošta
  - Rekonstrukcija ključa
  - Bezbedan pristup računarskom sistemu

Primena kriptografije
Tajna komunikacija

- Tajna komunikacija je direktna primena kriptografije (iz tog razloga je kriptografija i nastala).
- Dve osobe mogu komunicirati tajno kriptujući poruke tako da treća osoba koja prisluškuje komunikaciju nikad ne uspe da dešifruje kriptograme.
- S obzirom da je tajna komunikacija prisutna već vekovima, problem upravljanja ključem onemogućio joj je primenu po klasičnom modelu.
- Zahvaljujući kriptografiji sa javnim ključem stvoreni su alati kojima se može kreirati komunikaciona mreža sa mnoštvom korisnika koji komuniciraju u tajnosti i to bez obzira da li su ikada ranije uspostavljali vezu.

Primena kriptografije
Identifikacija

- Identifikacija je proces verifikovanja pojedinca.
- Ceo proces može se automatizovati primenom kriptografije.

- Svaka ATM kartica povezana je jedinstvenim, tajnim PIN-om, koji povezuje donosioca kartice i vlasnika računa.
- Kada se kartica ubaci u ATM, mašina traži unošenje PIN-a.
- Ukoliko je PIN korektan, mašina identifikuje osobu kao legalnog vlasnika i dozvoljava pristup.

Primena kriptografije
Digitalni potpis i autentifikacija

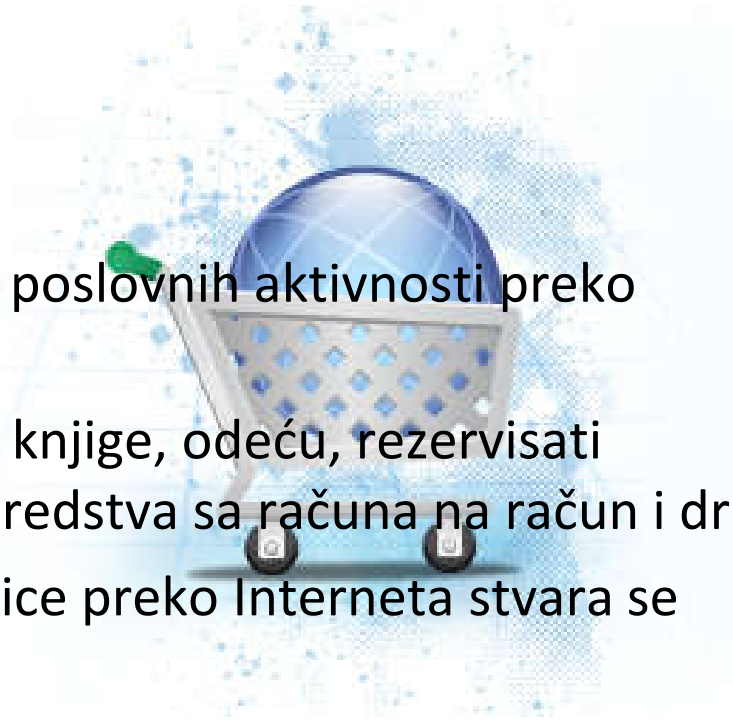
- Autentifikacija je proces u kome se dokazuje i verifikuje određena informacija.
- Ponekad se može zahtevati da se verifikuje originalanost dokumenta, da se identifikuje korisnik i tome slično.
- Digitalni potpis je kriptografsko sredstvo pomoću kog se pomenuta verifikacija može ostvariti.
- Digitalni potpis dokumenta je određena količina informacija koja je proizvedena pomoću sadržaja dokumenta i korisnikovog tajnog ključa
  - Praktično se izvodi primenom hash funkcija i kriptografskim algoritmima koji koriste asimetričnu kriptografiju
- Digitalni potpis i svojeručni potpis počivaju na činjenici da je praktično nemoguće pronaći dve osobe koje imaju isti potpis.

Primena kriptografije
Digitalni potpis i autentifikacija

- Kada se kriptografija sa javnim ključem koristi u procesu kriptovanja onda pošiljalac koristi javni ključ primaoca da bi mu poslao zaštićenu poruku.
- Kada se kriptografija sa javnim ključem koristi za digitalno potpisivanje onda pošiljalac kriptuje siže dokumenta (*digest*) pomoću sopstvenog tajnog (privatnog) ključa.
  - Svako može pomoću javnog ključa dotične osobe verifikovati potpis
- Postoji potencijalan problem sa ovakvim tipom potpisivanja:
  - Pošiljalac nije potpisao samo poruku kojoj je namenjen potpis već i sve poruke koje primenom hash funkcije daju isti siže, ta pojava naziva se kolizija
  - Svojstvo minimalne kolizije određene hash funkcije je neophodan bezbednosni zahtev za većinu šema digitalnog potpisivanja

Primena kriptografije

Elektronska trgovina



- Poslednjih nekoliko godina uvećao se obim poslovnih aktivnosti preko Interneta, tj. elektronske trgovine.
- Sedeći pokraj računara moguće je kupovati knjige, odeću, rezervisati mesto u hotelu, rentirati kola, prebacivati sredstva sa računa na račun i dr.
- Međutim, prenošenjem broja kreditne kartice preko Interneta stvara se prostor za pronevere.
- Jedan način rešavanja ovog problema je kriptovanje broja kreditne kartice kada se on unosi online, dok drugo rešenje predlaže kriptovanje cele sesije.
- Web server prima kriptovane informacije, dekriptuje ih i obrađuje bez bojazni da će broj kreditne kartice pasti u pogrešne ruke.
- Kako se poslovne aktivnosti više oslanjaju na Internet, potrebe zaštite od pronevere, krađe i korupcije postaju sve veće.

Primena kriptografije
Kriptografija na Internetu

- Internet, sačinjen od miliona umreženih računara, omogućava skoro trenutnu komunikaciju i prenos podataka širom sveta.
- WWW se koristi za online trgovinu, distribuciju podataka, marketing, istraživanje, učenje i mnoštvo drugih aktivnosti.
- **Kriptografija omogućuje bezbedne Web stranice i elektronski bezbednu transmisiju podataka.**
- Time se stvara mogućnost primene online bankarstva, online trgovanja i online kupovine pomoću kreditnih kartica, bez zabrinutosti za komprimovanje privatnih podataka, npr. o računu.
- Kriptografija je vrlo značajna i presudna u razvoju Interneta i elektronske trgovine.
- Ovakav nivo aktivnosti je nemoguć bez modernih kriptografskih alata.

Infrastruktura kriptografije sa javnim ključem

- Infrastruktura kriptografije sa javnim ključem (***Public Key Infrastructure – PKI***) predstavlja skup protokola, servisa i standarda za podšku aplikacijama koje koriste kriptografiju sa javnim ključem.
- Postoje brojni različiti opisi PKI u novijoj literaturi.
- Ponekad se PKI opisuje kao jednostavna hijerarhija poverenja zasnovana na kriptografiji sa javnim ključem, a ponekad kao kriptografski sistem sa mogućnošću digitalnog potpisivanja krajnjih korisnika.
- PKI zapravo podrazumeva servise i protokole za upravljanje ključevima i sastoji se od komponenti koje ne koriste uvek kriptografske operacije pomoću ključeva.

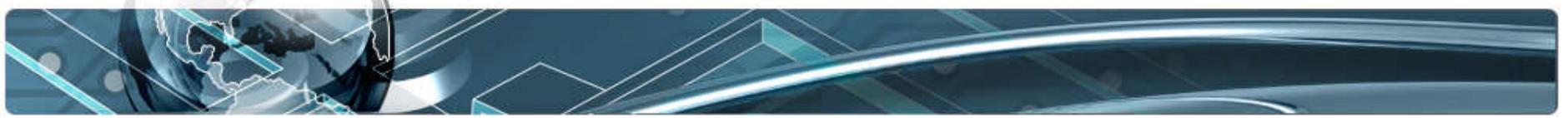
Infrastruktura kriptografije sa javnim ključem

Osnovne komponente PKI sistema su:

- Sertifikaciono telo ili autoritet od poverenja (*Certification Authority* – CA)
- Registraciono telo (*Registration Authority* – RA)

Servisi koji se često mogu naći u PKI sistemima jesu sledeći:

- **Registracija ključa**: izdavanje novog sertifikata za javni ključ
- **Povlačenje sertifikata**: poništavanje prethodno izdatog sertifikata
- **Izbor ključa**: generisanje javnog ključa korisnika
- **Procena poverenja**: određivanje validnosti sertifikata i skupa autorizovanih operacija
- **Rekonstrukcija ključa**: ponovno izračunavanje para ključeva



Infrastruktura kriptografije sa javnim ključem

- Funkcionisanje PKI sistema zasniva se na osnovnom dokumentu sistema (***Certificate Practice Statement – CPS***).
- CPS je dokument koji detaljno opisuje sve procedure bitne za funkcionisanje PKI sistema, kao i bezbednosnu politiku koja se primenjuje.
  - Ovaj dokument propisuje rad sertifikacionog tela, način rada sa digitalnim sertifikatima (način izdavanja i povlačenja, izradu lista povučenih sertifikata), ali i potpisuje način rada sa kriptografskim ključevima (generisanje, čuvanje i izdavanje korisnicima).
  - Svaki izdati elektronski sertifikat je potpisan asimetričnim šifarskim sistemom i tajnim ključem sertifikacionog tela (CA):
    - Ako je CA kompromitovano i čitav PKI sistem je kompromitovan
    - Potpuna i pouzdana zaštita tajnog ključa asimetričnog sistema CA najvažniji je zadatak koji se postavlja pred CA i čitav PKI sistem

Certification Authorities

WebTrust Baseline

EY Building a better working world

Infrastruktura kriptografije sa javnim ključem

- Interfejs između korisnika i CA je registraciono telo (RA)
  - RA prihvata zahteve za izdavanjem sertifikata, proverava identitet korisnika i prosleđuje zahteve u određenom formatu ka CA
- Kvalitet načina provere identiteta podnosioca zahteva određuje nivo poverenja koji se ugrađuje u sertifikacioni zahtev.
- Sertifikati mogu biti distribuirani na različite načine u zavisnosti od strukture PKI okruženja.
- Savremeni PKI sistemi najvišeg kvaliteta koriste smart kartice kao medijume za izdavanje elektronskih sertifikata.

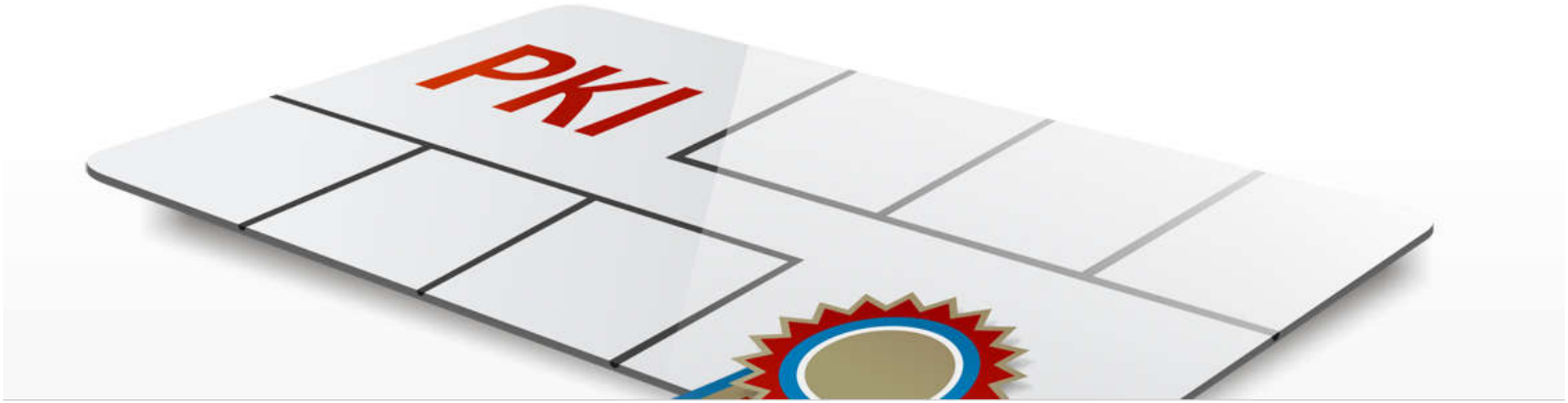
Infrastruktura kriptografije sa javnim ključem

- PKI sistem obezbeđuje pouzdano okruženje za realizaciju četiri osnovne funkcije zaštite komercijalnih i poslovnih transakcija
  - **Autentičnost strana u komunikaciji**
  - **Integritet podataka**
  - **Nemogućnost naknadnog poricanja transakcija**
  - **Zaštitu tajnosti podataka**

- Prve tri pomenute funkcije realizuju se na bazi tehnologije digitalnog potpisa primenom asimetričnih šifarskih sistema
- funkcija zaštite tajnosti najčešće realizuje primenom simetričnih šifarskih sistema

Infrastruktura kriptografije sa javnim ključem

- Primena asimetričnih šifarskih sistema ima dominantan značaj u sistemima elektronske trgovine i poslovanja.
- Asimetrični sistemi i funkcije koje se realizuju njihovom primenom, imaju sve značajniju ulogu i u specijalizovanim sistemima, kao što su vojska, policija i diplomatija, čiji se rad tradicionalno bazirao samo na primeni simetričnih šifarskih sistema.



Digitalni sertifikat

- U središtu PKI sistema nalazi se sertifikaciono telo (CA)

čija je osnovna funkcija pouzdano uspostavljanje digitalnog identiteta svih učesnika komunikacije u datoj nezaštićenoj računarskoj mreži.

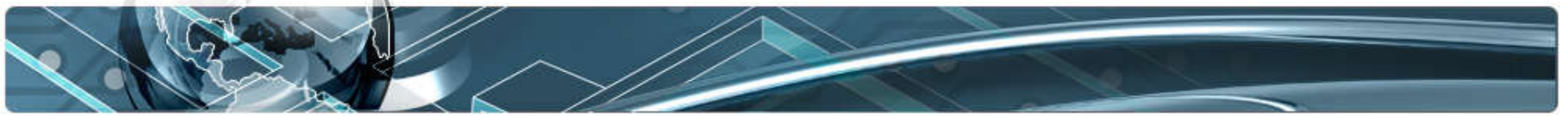
- Pomenuta funkcija postiže se primenom digitalnih (elektronskih) sertifikata koji pouzdano povezuje identitet učesnika sa javnim ključem asimetričnog šifarskog sistema.
- Digitalni sertifikat je elektronski zapis kojim se digitalni potpis povezuje sa identitetom potpisnika.
- On sadrži javni ključ i druge podatke potpisane tajnim ključem sertifikacionog tela i zaštitu elektronskog platnog prometa koji izdaje digitalne sertifikate.
- Digitalnim potpisom digitalnog sertifikata svakog učesnika, CA postaje treća strana od poverenja, pasivnog tela, za bezbednu komunikaciju bilo koja dva ovlašćena učesnika u datoj mreži koji se, u opštem slučaju, međusobno ne poznaju.

Primena kriptografije
Digitalni sertifikat

- Formati digitalnih i elektronskih poruka koje se odnose na te sertifikate regulisani su međunarodnim standardima ITU-T X.509 V3 ili PKCS.
- Digitalni sertifikat se može posmatrati kao digitalna lična karta - dokaz identiteta na Internetu.
- Lična karta predstavlja opšteprihvaćeni dokaz o identitetu vlasnika izdat od strane državne institucije.
- Pošto se veruje državnoj instituciji da je pre izdavanja lične karte izvršila proveru identiteta osobe, time se veruje u identitet osobe kojoj je izdata lična karta.
- Pošto na Internetu nema državnih organa koji bi mogli proveriti podatke i izdati ličnu kartu, pojavile su se kompanije koje imaju ulogu “treće strane” - sertifikaciona tela (CA) čija je uloga da provere i utvrde nečiji identitet i nakon toga da mu izdaju sertifikat.
- U zavisnosti od domena primene, to može biti neka državna institucija od poverenja, ali i bilo koja institucija ili pojedinac.

Digitalni sertifikat

- Pored opštih podataka o identitetu (naziv, adresa, organizacija, država i dr.) digitalni sertifikat sadrži još i javni ključ toga identiteta, podatke o izdavaocu sertifikata i sve to overeno digitalnim potpisom CA.
- CA mogu biti:
  - **Javni** (banka koja izdaje sertifikate svojim komitentima)
  - **Komercijalni** (provajder servisa kao što je Verisign koji prodaje sertifikate identifikovanim subjektima)
  - **Privatni** (kompanija koja izdaje sertifikate zaposlenima, univerzitet koji izdaje sertifikate svojim studentima)
- CA su međusobno nezavisni čak i u jednoj zemlji.
- Legalne i tehničke veze među njima grade se na bazi CPS-a, osnovnog dokumenta PKI sistema koji uređuje sve procedure i politiku u ovom sistemu.



Digitalni sertifikat

- **Sertifikaciona tela (CA)** mogu se organizovati po hijerarhijskom modelu.
- Generalno, hijerarhija CA sadrži više CA sa strogo definisanim odnosom roditelj-dete.
- CA koji je najviši u hijerarhiji se generalno naziva korenski CA (*root* CA) čiji sertifikat je potpisan sopstvenim tajnim ključem (*self-signed*).
- To je sertifikat u kome su naziv subjekta i naziv izdavaoca sertifikata identični i čiji javni ključ se može direktno uzeti za verifikaciju potpisa pridruženog uz sertifikat.
- Ukoliko postoji više od jednog CA u hijerarhiji vrši se validacija sertifikata od nižeg ka višem hijerarhijskom nivou.

Bezbednosni protokoli

- Naglo širenje Interneta u poslednjoj deceniji i njegovo korišćenje u poslovne svrhe nametnuli su potrebu za promenama u funkcionisanju svetske mreže.
- Sve veći broj poverljivih podataka koji se prenose mrežom kao i porast trgovine preko Interneta stavili su u prvi plan problem bezbednosti komunikacije.
- Standardni protokoli za komunikaciju među računarima ne nude rešenje za ove probleme.
- Razvijeno je više protokola koji obezebeđuju bezbedne komunikacije pre svega na Internetu:
  - Među primenjenim bezbednosnim protokolima najpoznatiji je **SSL (*Secure Socket Layer*)** i iz njega izvedeni TLS (*Transport Layer Security*), a u IPv6 može se očekivati i značajnija primena IPSec protokola
  - Među bezbednosnim protokolima namenjenim finansijskim transakcijama na Internetu najpoznatiji je **SET (*Secure Electronic Transaction*) protokol**

S/MIME

- **S/MIME (*Secure Multipurpose Internet Mail Extension*)** je protokol koji je nadgradnja postojećeg MIME protokola sa dodatkom digitalnog potpisa i kriptovanja poruka.
- MIME se preporučuje u naprednom korišćenju elektronske pošte.
- Elektronsko pismo sastoji se od dva dela, zaglavlja i tela poruke.
- MIME definiše strukturu tela elektronskog pisma kako bi se omogućio prenos teksta, slika, zvuka i dr. na jednoobrazan način preko elektronskih poštanskih sistema koji podržavaju MIME.
- Svrha S/MIME specifikacije jeste da obogati postojeći sistem primenom kriptografskih alata i protokola po PKCS#7 standardu za digitalni potpis i kriptografiju.
- U razvoju S/MIME protokola učestvovale su vodeće kompanije u svetu u oblasti komunikacionih mreža: ConnectSoft, Frontier, FTP Software, Qualcomm, Microsoft, Lotus, Wollongong, Banyan, NCD, SecureWare, Verisign, Netscape i Novel.

SSL

- **SSL (*Secure Sockets Layer*)** handshake protokol razvila je kompanija Netscape Communications kako bi omogućila bezbednost i privatnost prenosa podataka preko Interneta.
- Protokol podrazumeva serversku i klijentsku autentifikaciju.
- SSL je nezavisan od primene, podržava razne protokole kao HTTP (*HyperText Transfer Protocol*), FTP (*File Transfer Protocol*) i Telnet da se oslone na njega transparentno.
- SSL protokol pregovara o ključu koji će se koristiti u bezbednom prenosu i proverava autentičnost servera pre početka prenosa podataka od strane viših nivoa u komunikacionoj arhitekturi.
- SSL održava bezbednost i integritet razmenjenih podataka korišćenjem kriptovanja, autentifikacije i MAC.

Bezbednosni protokoli

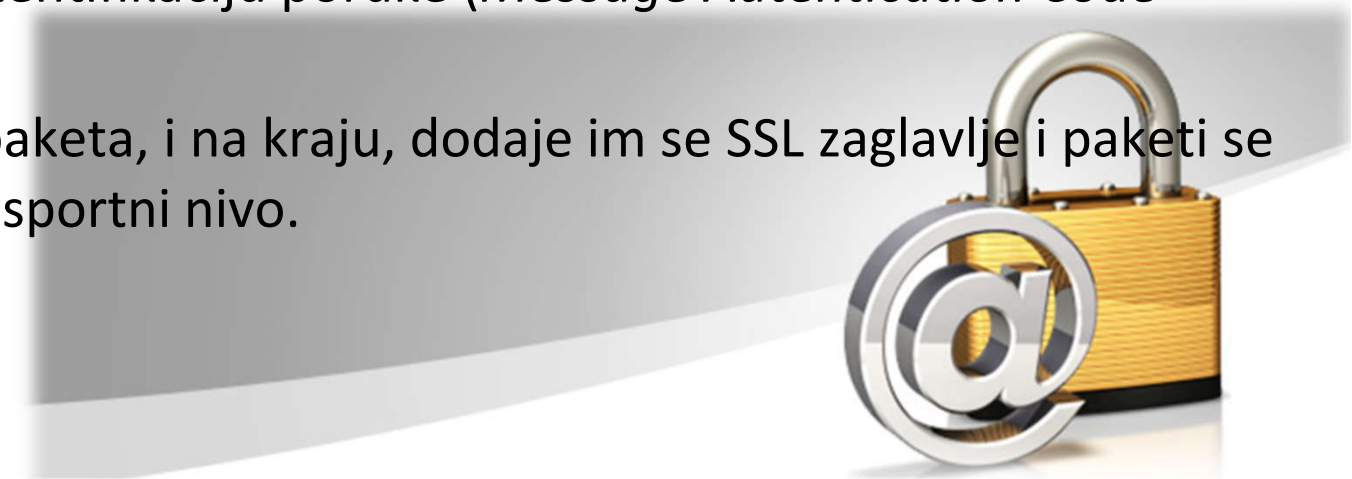
SSL

- SSL obezbeđuje privatnost, integritet podataka i autentičnost pošiljalaca korišćenjem kombinacije šifrovanja javnim ključem, simetričnog šifrovanja, kao i digitalnih sertifikata.

- Transakcija korišćenjem SSL protokola uključuje sledeće aktivnosti:
  1. Server šalje svoj digitalni sertifikat klijentu.
  2. Klijent proverava da li je sertifikat izdat od autorizovane strane (CA), i ako ustanovi da nije, pruža korisniku mogućnost da odabere da li će nastaviti transakciju ili će je prekinuti.
  3. Klijent generiše tajni ključ koji će koristiti samo u započetoj transakciji.
  4. Klijent šifruje generisani tajni ključ korišćenjem serverovog javnog ključa i šalje ga server.

SSL

- U daljem toku transakcije server i klijent koriste isti tajni ključ metodom simetričnog kriptovanja.
- Problem tajnosti u računarskim komunikacijama rešava se kriptovanjem podataka na izvoru i dekriptovanjem na odredištu.
- SSL prvo prihvata podatke upućene s aplikacionog nivoa i deli ih (fragmentira) u blokove.
- Fragmentacija je obavezna pošto je veličina paketa koji se šalju ograničena.
- Potom može da izvrši kompresiju fragmentiranih podataka pre nego što primeni kod za autentifikaciju poruke (*Message Autentication Code* – MAC).
- Sledi kriptovanje paketa, i na kraju, dodaje im se SSL zaglavlje i paketi se prosleđuju na transportni nivo.



SSL

- Najkritičnije mesto svakog sistema

  sa javnim ključem je ono na kome se čuvaju tajni ključevi.

- Bezbednost čitavog sistema ugrožena je činjenicom da su najosetljiviji podaci sačuvani na hard diskovima radnih stanica i servera gde su izloženi mogućim zloupotrebama.

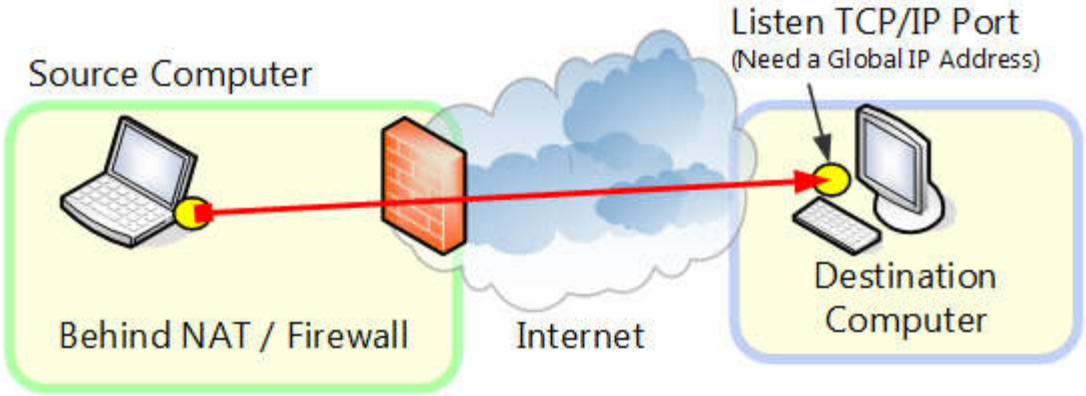
- Druga velika slabost je što proces kriptovanja i dekriptovanja obavlja operativni sistem ili aplikativni softver koji je podložan najrazličitijim bagovima i neotporan na snažnije napade.

- Rešenje ovih ključnih problema pronađeno je u upotrebi specijalizovanih hardverskih komponenti koje na sebi imaju dovoljno memorije za čuvanje svih kriptografski bitnih informacija i dovoljno procesorske snage da obavljaju osnovne kriptografske operacije nezavisno od operativnog sistema i aplikacija.

- Jedno takvo rešenje je smart kartica.

Mesta mogućih napada i kriptoanalize

- Za elektronsku trgovinu preko Interneta, mesto na koje se prvo pomisli kao moguće mesto špijunaže jesu vodovi za prenos podataka.
- Zato je TCP/IP veza između računara klijenta i komercijalnog servera predmet posebne pažnje.
- Koriste se raznovrsne kriptozaštite i šeme za autentifikaciju radi zaštite podataka od prepravljanja i špijuniranja u toku prenosa.
- Prenos podataka koji je zaštićen kriptovanjem razumno visokog kvaliteta (veličina ključa od barem 56 bita) se smatra bezbednim od napada u većini primena.
- I pored toga, mogućnosti i algoritmi za kriptografske napade na prenos podataka postoje, ali napadač koji nije profesionalni kriptoanalitičar će vrlo efikasno biti odstranjen.
- Poznat je problem TCP/IP "njuškanja" u kojem napadač pasivno posmatra saobraćaj u mreži, i relativno ga je lako otkriti.



Mesta mogućih napada i kriptoanalize

- Treba obratiti pažnju da u našoj opsednutosti da se zaštitimo od “njuškanja”, ne zaboravimo na druge tačke napada i potencijalno mnogo ozbiljnije pretnje.
- Kada aplikacija u elektronskoj trgovini koristi kriptovane vodove za prenos podataka pri komunikaciji sa serverom na drugom kraju, postoje dve krajnje tačke sistema: jedna je server na elektronskom mestu trgovca, dok je druga desktop korisnika.
  - Obe krajnje tačke su podložne napadu ako se ne zaštite adekvatno
- Šta se dešava sa podacima kada prođu kroz zaštićeni vod do servera?
  - Često se smeštaju u datoteku ili bazu podataka, koja može da sadrži informacije o kreditnoj kartici kupca, brojeve telefona, adrese, itd.
  - Obično se skupljeni podaci čuvaju nekriptovano i već je bilo slučajeva u kojima su Web serveri napadnuti i provaljeni
  - Smetnje su uglavnom bile neškodljive, ali su kompromitovale Web server sa informacijama o kreditnim karticama kupaca

Mesta mogućih napada i kriptoanalize

- Korisnici multi-korisničkih sistema imaju poseban problem rupa u bezbednosti i u najkomercijalnijim operativnim sistemima, zbog kojih se može pristupiti drugim podacima korisnika.
- Ovo može da obuhvata informacije koje korisnik otkucava na tastaturi, lozinke, informacije o kreditnoj kartici, itd.
- Ako napadač može da pročita podatke iz tekućeg programa pre nego što se postave na kriptovan vod za prenos podataka, nema potrebe da se napada kriptogram.
- Personalni i drugi računari nisu bezbedni - trojanci ili napadački programi su potencijalno sposobni da pristupe informacijama korisnika smeštenim na hard disku.

Ocena bezbednosti i anonimnosti u elektronskoj trgovini

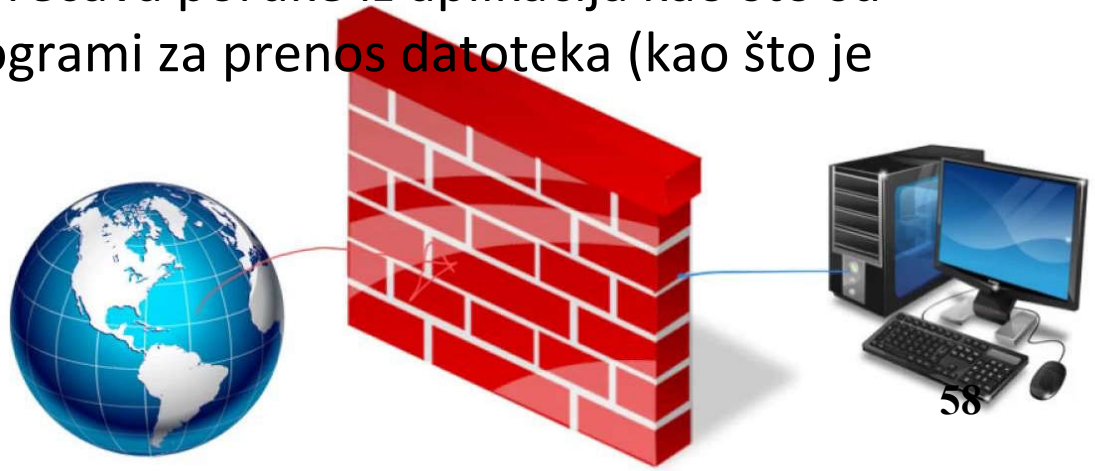
- Dosadašnja praksa ukazuje na to da su minimalne potrebe jednog preduzeća u pogledu zaštite komunikacione mreže antivirus softver i firewall.
- Danas preduzeća koja upravljaju transakcijama ili poverljivim podacima moraju da koriste PKI sisteme.
- Logovanje i tajne lozinke koje su omogućavale registrovanim korisnicima da pristupe sistemu tradicionalno su korišćeni u zaštiti mrežne infastrukture.
- Problem sa ovim pristupom je što detalji mogu biti ukradeni ili uhvaćeni od strane trećeg lica, a mreža nema druge mogućnosti autentifikacije korisnika.
- PKI uvodi digitalne sertifikate radi

  provere validnosti javnog ključa koji koristi

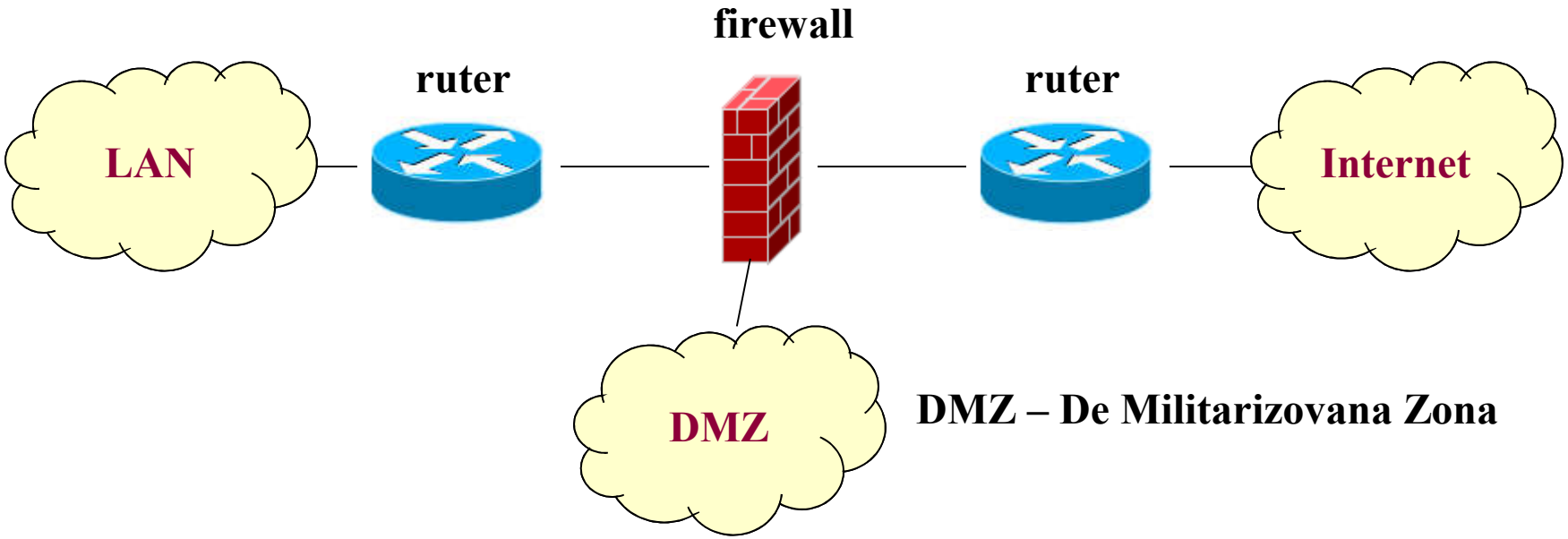
  registrovani korisnik.

Kako barijere (firewall) štite lokaciju

- Da bi zaštitili mrežu od napada hakera, mnogi administratori mreže stavljaju barijeru između Interneta i mreže
- Barijera filtrira mrežne poruke koje dolaze sa Interneta u mrežu – mrežne poruke su podaci koje programi kao što su čitači Weba i programi za ćaskanje šalju sa jednog računara na drugi
- Barijera može da bude posebna hardverska kutija ili računar na kojem je pokrenut odgovarajući softver
- Barijera dozvoljava samo HTTP porukama poslatim sa udaljenog čitača da uđu u mrežu, a sprečava poruke iz aplikacija kao što su programi za ćaskanje ili programi za prenos datoteka (kao što je FTP) da uđu u mrežu



Korišćenje firewall-a za zaštitu (tipska šema)

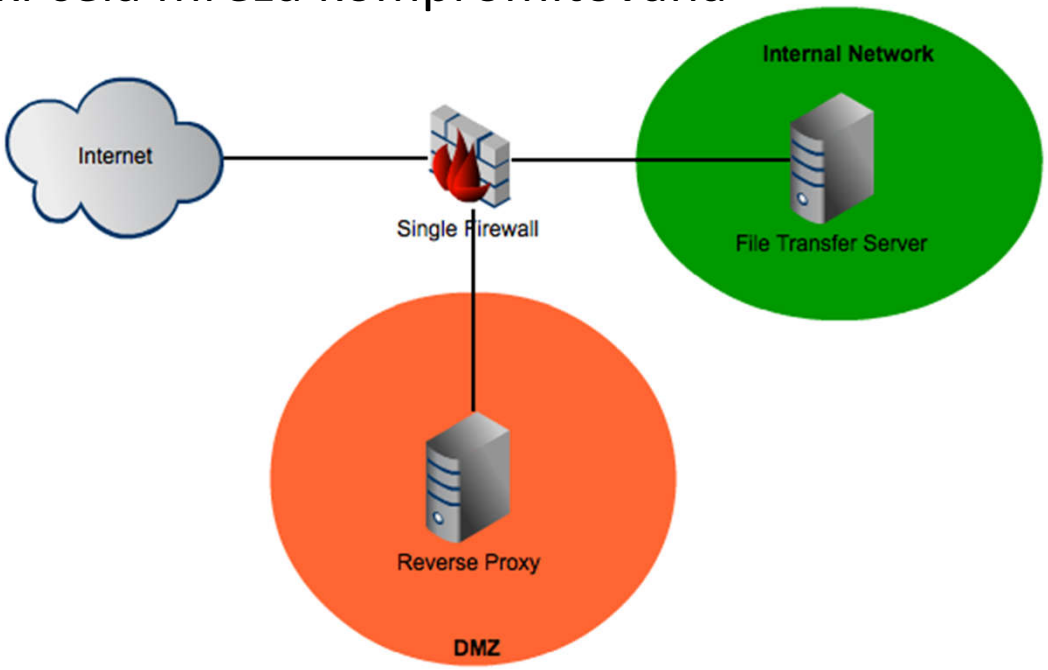


Po pravilu, *firewall* se realizuje kao uređaj sa dva ili više *ethernet* interfejsa. U zavisnosti od načina realizacije *firewall* može da bude:

- **Softverski** – softver koji se instalira na računar opšte namene
- **Hardverski** – namenski razvijen računar sa odgovarajućim softverom
- **Integrisan sa ruterom**

DMZ

- U DMZ se smeštaju serveri koji treba da budu vidljivi i sa Interneta i iz lokalne mreže
- U slučaju postojanja DMZ-a, firewall najčešće ne dozvoljava direktnu komunikaciju LAN <-> Internet već isključivo kroz DMZ
- U slučaju kompromitovanja nekog od servera u DMZ-u to ne znači da je automatski cela mreža kompromitovana



Ocena bezbednosti i anonimnosti u elektronskoj trgovini

- Samo autorizovani javni ključevi mogu autentifikovati podneti digitalni sertifikat kao ispravan.
  - Takav sistem može kriptovati e-mail, transakcije, korisničke porudžbine, a mogu i da spreče da ključni poslovni podaci dospeju u neželjene ruke
- Najefikasniji način čuvanja digitalnog sertifikata je na smart kartici.
- Kada je reč o zaštiti informacija koje se prenose mrežom, najveća nada polaže se u kriptozaštitu.
- Kriptografija je važna alatka, ali sama po sebi nije dovoljna da učini aplikaciju bezbednom.
- Sada se velika pažnja polaže na različite algoritme, ključeve sa mehanizmom razmene i tehnologije potvrđivanja.

Ocena bezbednosti i anonimnosti u elektronskoj trgovini

- Posmatrano sa gledišta bezbednosti, postoji još nekoliko važnih momenata koji se moraju uzeti u obzir za vreme procesa elektronske transakcije, a koje se primenjuju i u stvarnom životu ili telefonskoj trgovini:
- **Kako kupci znaju da posluju sa legitimnim preduzećem?**
  - U stvarnom životu teško je i skupo imitirati poznatu prodavnicu
  - Razvijen posao i prepoznavanje njegovog imena imaju veliku snagu na tržištu koju pridošlice nemaju
  - Može li to elektronska trgovina da ugrozi?
- **Kako kupac uređuje plaćanje?**
  - Elektronska trgovina skoro uvek

  preuzima neku vrstu elektronskog identiteta

  (obično kreditna kartica) koji se razmenjuje

  kao garancija plaćanja.

  - Elektronske keš tehnologije postoje, ali su još uvek manje popularne nego sistemi bazirani na kreditnim karticama.

Ocena bezbednosti i anonimnosti u elektronskoj trgovini

- **Kako preduzeće zna da posluje sa legitimnim kupcem?**
  - U nekim transakcijama trgovac ne mora i ne želi da zna identitet kupca
  - Kada kupac želi da plati kreditnom karticom, proces autorizacije pokušava da verifikuje identitet kupca proveravanjem da li je kartica aktivna, da li je prekoračen račun, datum isticanja, i često, da li se adresa isporuke i adresa računa poklapaju.
- **Kako kupac specifikuje ili menja adresu na koju proizvod treba da se isporuči?**
  - Adresa isporuke proizvoda se često koristi da smanji mogućnost prevare kreditnom karticom upoređivanjem sa adresom za naplatu kreditne kartice.
  - Sistemi elektronske trgovine koji čine lakim promenu adrese naplate i adrese isporuke, mogu biti podložni napadima preusmeravanjem proizvoda ili faktura.

Ocena bezbednosti i anonimnosti u elektronskoj trgovini

– **Za koje vidove transakcija kupac očekuje da budu privatne, a za koje zakon to zahteva?**
  - Mnoge vidove transakcija kupac ne želi da obelodani
  - Kućna adresa i broj telefona kupca, na primer, mogu da se zaštite

- Zakon može da zaštiti neke transakcije kao što su medicinski zapisi, ili bankarska salda, a trgovac može da odgovara za štete zbog njihovog obelodanjivanja.
- Nijedan mehanizam nije apsolutno siguran.
- Svaki sigurnosni mehanizam mora se s vremena na vreme unapređivati, jer kako dolazi sve brži i moćniji hardver, tako se povećava mogućnost za savladavanje bezbednosnih mehanizama sirovom računarskom snagom.
- Primer za to je SSL bezbednosni protokol sa 40-bitnim ključem, koji se današnjim računarskim kapacitetima ne previše velike vrednosti razbija za svega nekoliko minuta.