XII-Bezbednost elektronskog poslovanja

S A D R Ž A J

12 – Osnovni pojmovi

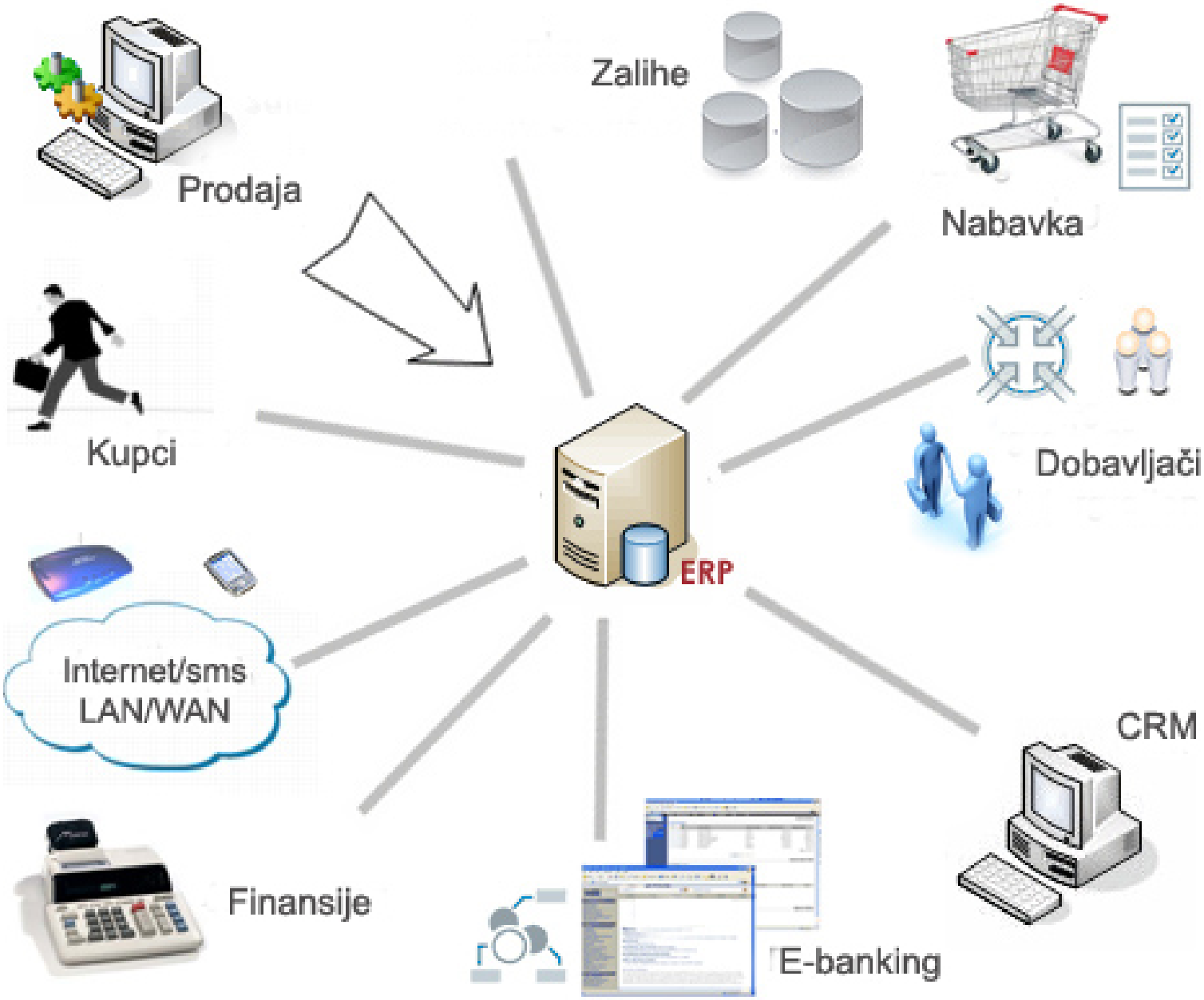
- Elektronske transakcije postaju sve dominantniji način poslovanja
- Svrha prelaska na elektronski način poslovanja (e-business) je, između ostalog, optimizacija poslovnih procesa (proizvodnje, marketinga, distribucije, prodaje, naplate), unapređenje odnosa i poslovnih servisa kompanije sa poslovnim partnerima (klijentima, dobavljačima, distributerima, bankama, vladinim agencijama) i dr.
- Naglo širenje Interneta u poslednjoj deceniji i njegovo sve intenzivnije korišćenje u poslovne svrhe nametnuli su potrebu za promenama
- Sve veći broj poverljivih podataka koji se prenose mrežom kao i porast trgovine preko Interneta stavili su u prvi plan problem sigurnosti veza
- Ovaj problem naročito dolazi do izražaja kod komunikacije sa Web-om
- Ako imamo komercijalnu Web prezentaciju i treba nam mehanizam naplate proizvoda ili usluga na njoj ono što nam je neophodno je **program potrošačke korpe** koji bi omogućio da se izaberu proizvodi, odlože u korpu, a zatim ukupni račun prikaže kupcu
- Preostaje da informaciju o kupcu (njegov bankovni račun) sa novčanim iznosom kupovine, samo prosledimo banci na naplatu.

12 – Osnovni pojmovi

- Povećanje kupovine preko kreditne kartice stvara potrebu za zaštitom, sa jedne strane podataka potrošača, a sa druge strane prodavca od zlonamernih potrošača i upotrebe ukradenih kreditnih kartica
- Neophodan je razvoj sistema za proveru kartice i autorizacije plaćanja
- Šifrovanje javnim ključem se danas koristi kao softver koji štiti podatke potrošača (prvenstveno broj kreditne kartice) i cele transakcije
- Iako je ovo jedan od najsigurnijih načina za zaštitu podataka danas, moguće su greške u implementaciji ovog sistema
- Veliki problem je opasnost od lažnih prezentacija (lažnih prodavnica)
- Postoje 2 pristupa kojima se može obezbediti sigurnost transakcija:
  1. **SecureHTTP** – SHTTP - minimalna primena u praksi
  2. **SSL** (*Secure Socket Layer*) – dominantna primena
- SSL je dobio i verifikaciju identiteta klijenata, što bi trebalo da sigurnost komunikacije na ovaj način podigne na još veći nivo.

Bilo kakvu elektronsku prodavnicu koja nudi bilo šta na prodaju, a ne sadrži Secure server, treba potpuno ignorisati, bez obzira na povoljnosti koje nudi.

12 - Vrste elektronskog poslovanja



12 – Vrste elektronskog poslovanja

- *Elektronsko poslovanje* je opšti koncept koji obuhvata sve oblike poslovnih transakcija ili razmene informacija koje se izvode korišćenjem informacione i komunikacione tehnologije i to:
  - ✓**B2B** (*Bisiness-to-Business*) - između preduzeća,
  - ✓**B2C** (*Business-to-Customer*) - između preduzeća i njihovih kupaca,
  - ✓**B2E** (*Business-to-Employee*) - između preduzeća i javne administracije
- Elektronsko poslovanje uključuje i elektronsko trgovanje dobrima i uslugama.
- Elektronsko poslovanje može se posmatrati sa više stanovišta:

1. ***Sa aspekta komunikacija*** - elektronsko poslovanje je elektronska isporuka informacija, proizvoda i usluga i elektronsko plaćanje korišćenjem računarskih i drugih komunikacijskih mreža.
2. ***Sa poslovnog aspekta*** - to je primena tehnologije u svrhu automatizacije poslovnih transakcija i poslovanja.
3. ***Sa stanovišta usluga*** - to je alat koji omogućuje smanjenje troškova poslovanja uz istovremeno povećanje kvaliteta i brzine pružanja usluga korisnicima.

12 – Vrste elektronskog poslovanja

- ***Elektronsko poslovanje (e-business) uključuje:***
  - kupovinu i prodaju robe i usluga,
  - saradnju sa poslovnim partnerima,
  - elektronske transakcije unutar organizacije.

- ***Elektronska trgovina (e-commerce) se definiše iz perspektive:***
  - Komunikacija - kao isporuka robe, servisa, informacija ili isplata preko računarske mreže,
  - Trgovine - omogućavanje kupovine i prodaje robe, servisa, informacija preko Internet-a.
- Često se susreće i pojam Internet ekonomije, čija se suština određuje u iskorišćenju novih pogodnosti otvorenih komunikacija.
- Omogućene su interaktivne veze proizvođača tj. dobavljača i kupaca uz povećanje produktivnosti i smanjenje troškova.

12 - Vrste elektronskog poslovanja

- Model umreženog globalnog poslovanja omogućio je preduzećima koja ga koriste:
  - ✓ rast prihoda i proizvodnje,
  - ✓ rast zaposlenosti,
  - ✓ uštede u troškovima poslovanja,
  - ✓ zadovoljne kupce,
  - ✓ smanjenje vremena isporuke robe i smanjenje broja reklamacija,
  - ✓ poboljšanje podrške korisnicima i
  - ✓ uštede u troškovima distribucije.
- Prednosti elektronskog poslovanja proizilaze iz kombinacije ekonomskih i tehnoloških razloga.
- Među ekonomskim razlozima su:
  - ✓ smanjenje troškova poslovanja,
  - ✓ smanjenje grešaka kod elektronskih transakcija,
  - ✓ jeftino globalno publikovanje transakcija i
  - ✓ mogućnost zamene skupih kancelarija.

12 - Sistemi plaćanja

- ***First Virtual (FV)*** bio je jedan od prvih platnih sistema na Internetu, a počeo da se koristi oktobra 1994.
- ***Cyber Cash*** je platni sistem zasnovan na programu Cyber Cash Wallet, koji kupci koriste prilikom kupovine, 1995. godine.
- ***E-Cash*** je anonimni digitalni novac čiju ispravnost, *on-line* proverava odgovarajuća finansijska institucija, nju je razvila firma DigiCash.
- Metoda ***NetCash*** osmišljena je na Univerzitetu Južne Kalifornije, značajna karakteristika ove metode je upotreba postojećih računovodsvenih sistema i procedura u finansijskim institucijama, što bi trebalo da utiče na smanjenje početnih investicija.
- ***Mondex*** sistem digitalnog novca razvija Modex U.K. - MasterCard.
- ***VisaCash*** je projekat kompanije Visa.
- ***PayPal*** je on-line servis koji omogućava naplatu i prenos novca preko Interneta. Kompanija PayPal Corp. nastala je u martu 2000. godine.
- Domaći platni servis na Internetu pod imenom ***eNovčanik*** osnovan je 2006. godine, i predstavlja praktičan i bezbedan metod plaćanja u Internet prodavnicama tj . Internet trgovini.

12 - Sistemi plaćanja

- **PayPal** firma čiji je vlasnik eBay, je jedna od najpoznatijih alternativa kreditnim karticama, čekovima i gotovini.
- PayPal korisnici za plaćanje preko Interneta ne moraju odavati osetljive podatke kao što su broj kreditne kartice ili bankovnog računa.
- Umesto davanja pomenutih podataka direktno prodavcu, korisnik kaže PayPal aplikaciji da prebaci korisnikovu uplatu na prodavčev račun.
- Pri tome PayPal identifikuje korisnika prodavcu isključivo preko adrese elektronske pošte.
- PayPal pruža svoje usluge trgovcima, na aukcijama, i ostalim komercijalnim korisnicima kojima naplaćuje proviziju.
- Ponekad takođe naplaćuje transakcionu proviziju za primanje novca.
- Provizija se naplaćuje u zavisnosti od:
  - ✓ valute koja se koristi,
  - ✓ odabranog tipa plaćanja,
  - ✓ države u kojoj se korisnik nalazi i države u kojoj je primalac,
  - ✓ iznosa novca i tipa računa.

12 - Sistemi plaćanja

- PayPal je najpoznatiji i najrašireniji internet servis za prenos novca.
- Paypal odlikuje jednostavnost, sigurnost i široka prihvaćenost
- Za online kupovinu treba otvoriti PayPal račun na www.paypal.com
- Za registraciju PayPal računa potrebna je debitna ili kreditna kartica
- Kartice koje možete koristiti za registraciju su Visa, Visa Electron, MasterCard i American Express.
- Važno je da kartica ima **CVV** (*Card Verification Value*) broj koji se nalazi na poleđini kartice i jedinstven je za svaku karticu.
- Njega upisujemo prilikom registracije na PayPal, odmah na početku.

12-Osnovne pretnje elektronskom poslovanju

- Elektronska trgovina predstavlja skup tehnologija i procedura koje automatizuju poslovne transakcije putem elektronskih sredstava.
- Informacije se prenose putem elektronske pošte (e-mail), sistema EDI (*Electronic Data Interchange*) ili preko servisa World Wide Web.
- Elektron. trgovina smanjuje troškove poslovanja i olakšava poslovanje.
- Postoje i potencijalni rizici upotrebe te tehnologije.
- Sa ekonomske tačke gledišta, posledice otkaza tehnološke prirode ili zloupotrebe ove tehnologije od strane korisnika mogu biti sledeće:
  - ✓ *Direktni finansijski gubici kao posledica prevare*
  - ✓ *Gubljenje vrednih i poverljivih informacija*
  - ✓ *Gubljenje poslova zbog nedostupnosti servisa*
  - ✓ *Neovlašćena upotreba resursa*
  - ✓ *Troškovi izazvani neizvesnim uslovima poslovanja*
- Zbog navedenih problema, potrošači koji koriste takve servise elektron.trgovine mogu pretrpeti direktne ili indirektne finansis.gubitke
- Rizici koje sa sobom nosi upotreba elektronske trgovine mogu se izbeći upotrebom odgovarajućih mera bezbednosti.

12-Osnovne pretnje elektronskom poslovanju

- Ove mere mogu biti tehnološke i pravne.
- U tehnološke mere spadaju, između ostalog: autentifikacija, poverljivost i integritet podataka.
- Da bi se ove mere sprovele u praksi, neophodna je upotreba kriptoloških tehnologija: šifre sa javnim ključevima i digitalni potpis.
- Potencijalne pretnje jednom informacionom sistemu koji sadrži podsistem za elektronsku trgovinu su:
  - ✓ ***Infiltracija u sistem*** - Informaciju neophodnu za infiltraciju, napadač dobija koristeći neku drugu vrstu napada.
  - ✓ ***Prekoračenje ovlašćenja*** - ostvaruju kako napadači iznutra ("*insiders*") tako i napadači spolja.
  - ✓ ***Suplantacija*** - postavljanje programa koji će omogućiti da se olakšaju napadi u budućnosti: ***"trojanski konj"***
  - ✓ ***Prisluškivanje*** - praćenje protoka podataka u komunikacionoj mreži
  - ✓ ***Promena podataka na komunikacionoj liniji***
  - ✓ ***Odbijanje servisa*** - DoS napadi.
  - ✓ ***Negacija transakcije*** - poricanje urađene transakcije

12-Osnovne pretnje elektronskom poslovanju

- Najčešće provale su od:
  - 48% - autorizovani zaposleni;
  - 24% - neautorizovani zaposleni;
  - 13% - spoljni saradnici

    (zaposleni ukupno: 85%);
  - 12% - hakeri, teroristi;
  - 3% - ostali.

12 – Metode zaštite

- Bezbednost elektronskog poslovanja podrazumeva postojanje ***bezbednosnih servisa*** (aktivnosti organizacije u vezi sa bezbednošću)
- Bezbednosne servise čini skup pravila koja se odnose na sve aktivnosti organizacije u vezi sa bezbednošću – politika bezbednosti, kao i delovi sistema koji realizuju aktivnosti koje pariraju bezbednosnim pretnjama
- Zaštita se integriše implementiranjem tri osnovne sigurnosne usluge: ***provere identiteta***, ***autorizacije*** i ***privatnosti***.

1. **Provera identiteta** korisnika u distribuiranim sistemima kao što je Web lokacija za e-trgovinu, realizuje se pomoću dva osnovna modela: *modela predstavljanja/delegiranja* i *modela poverljivog servera*.
2. **Autorizacija** obezbeđuje strogo kontrolisan pristup resursima ili servisima
3. **Privatnost**, predstavlja zaštitu tajnosti, podrazumeva šifrovanje podataka u cilju sprečavanja neovlašćenog uvida u tajne informacije

12 – Metode zaštite

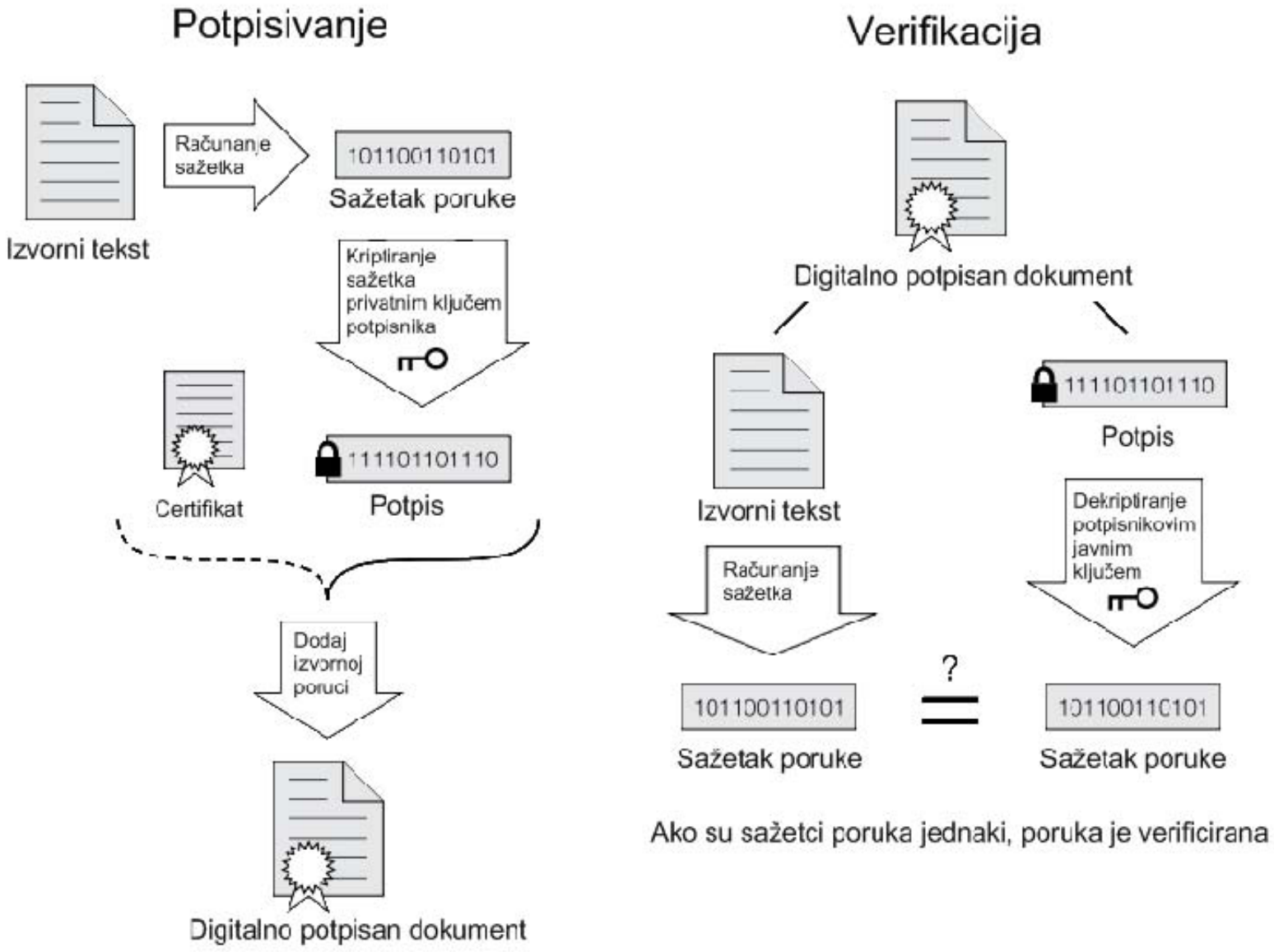
- Zaštita se realizuje kroz sledeće pristupe:

1. **Kriptografske tehnike** - postupak pretvaranja čitljivih podataka u nečitljive;
2. **Autentifikacija** - utvrđivanja identiteta osobe koja se prijavljuje kao i autorizacija – određivanje prava pristupa;
3. **Digitalni potpis** - niz bitova koji omogućava identifikaciju učesnika poslovanja;
4. **Digitalni sertifikat** - elektronski dokument, identifikuje računar, osobu, preduzeće ili sertifikatora;
5. **SET** (*Secure Encryption Transaction*) – za sigurne transakcije
6. **SIP** (*Session Initation Protocol)* – za multimedijalne sesije
7. **SSL** (*Secure Socket Layer*) - aplikativni sigurnosni protokol, služi za siguran prenos podataka preko Web-a;
8. **SSH** (*Secure Shell*) - protokol koji obebeđuje autentifikaciju, enkripciju i integritet podataka;
9. **VPN** (*Virtual Private Network*) - bezbedna komunikacija preko nebezbednog Interneta.

12 – Digitalni potpis

- Predstavlja prvi stepen u identifikaciji strana koje razmenjuju poruke.
- Jedan način implementacije digitalnog potpisa je korišćenje *inverznog postupka javnog ključa.*
- Privatni ključ koristi pošiljalac kako bi potpisao poruku dok primalac koristi javni ključ pošiljaoca da dešifruje poruku.
- Obzirom da samo pošiljalac poznaje privatni ključ, primalac je siguran da je poruka stvarno došla od pošiljaoca.
- Samo sažetak poruke ili *message digest* se potpisuje korišćenjem privatnog ključa(kompromis zbog zahtevnosti algoritma javnog ključa)
- Digitalni potpisi ne pružaju enkripciju poruka, tako da enkripcijske tehnike moraju biti korišćene ukoliko želimo očuvati tajnost poruka.
- RSA algoritam možemo koristiti za digitalne potpise i za enkripciju.
- DSA (*Digital Signature Algorithm*) koji je standard u SAD može se koristiti samo za digitalne potpise (***hash funkcije***).
- ***Infrastruktura javnih ključeva*** *(PKI)* čini skup komponenata koje upravljaju sertifikatima i ključevima koji se koriste u servisima šifrovanja i generisanja digitalnog potpisa.

12 - Digitalni potpis

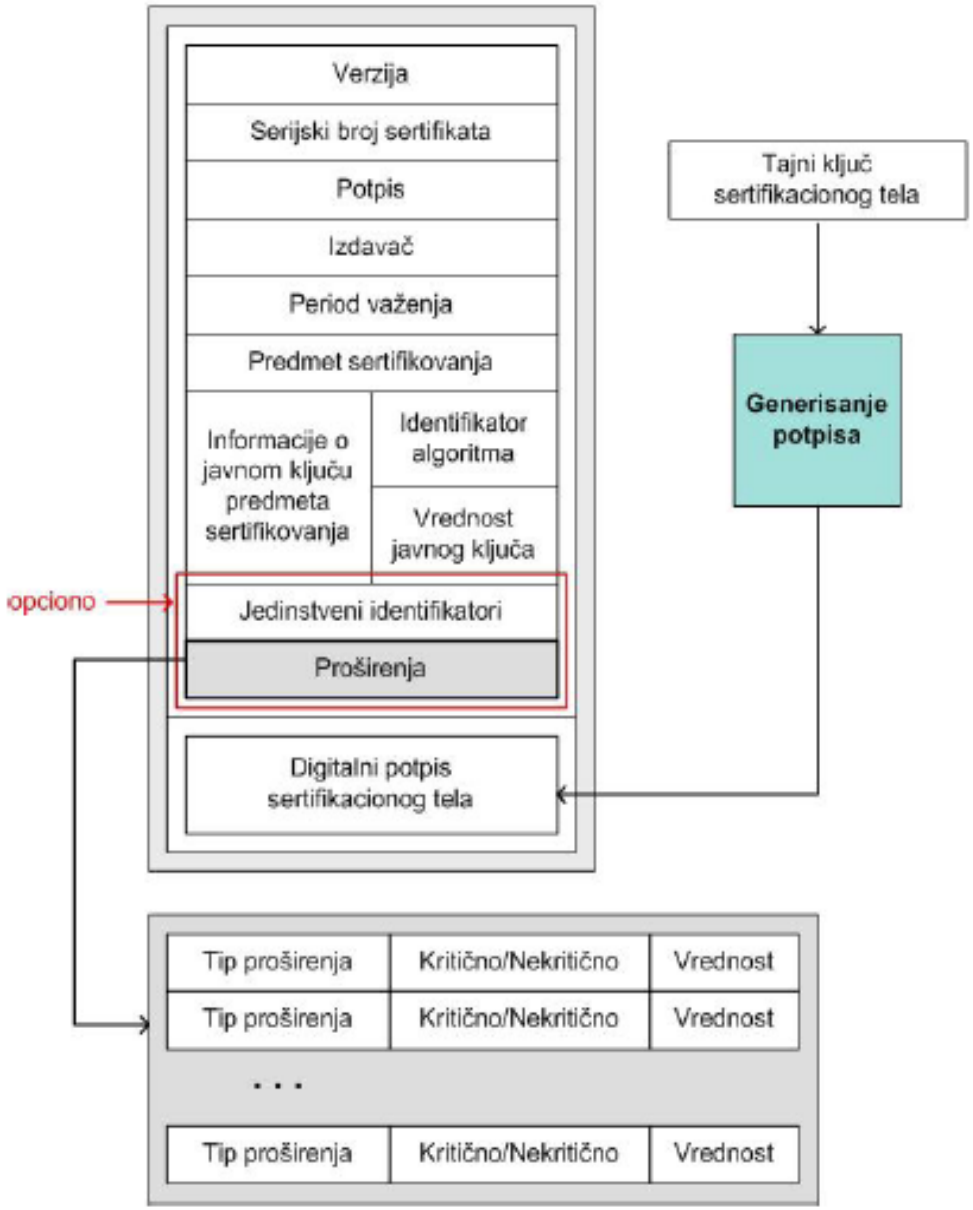


Digitalno potpisivanje dokumenta i verifikacija

12 Digitalni sertifikat

- ***Sertifikati*** obezbeđuju mehanizam za uspostavljanje poverenja u odnosima između javnih ključeva i entiteta koji poseduju odgovarajuće tajne ključeve-garantuje se da određeni javni ključ pripada tom entitetu
- Sertifikate javnih ključeva izdaje sertifi.centar (*Certification Authority*)
- Pored opštih podataka o identitetu (naziv, adresa, organizacija, država) sadrži još i javni ključ identiteta, podatke o izdavaocu sertifikata i sve to overeno digitalnim potpisom CA.
- **Primer**: *centralna banka izdaje sertifikate za komercijalne banke (korenski) a komercijalne banke izdaju sertifikate za svoje klijente.*
- Klijent jedne banke ne mora da veruje sertifikatu izdatom od druge banke, ali veruje korenskom sertifikatu koji je izdala centralna banka.
- Validnost sertifikata deponenata druge banke proverava se tako što se proveri digitalni potpis njegovog sertifikata pomoću javnog ključa uzetog iz sertifikata banke koja je izdala taj sertifikat.
- Zatim se proveri potpis na sertifikatu banke pomoću javnog ključa centralne banke, čime je dokazanost validnost sertifikata klijenata.
- Ako se koristi sertifikat kome se ne veruje, Web čitač će nas upozoriti

12 - Digitalni sertifikat



12 - Izdavanje sertifikata

12 - SSL WEB server

- *Security Socket Layer* (SSL) predstavlja standard za zaštitu podataka.
- Manji broj prodavnica na Internetu koristi protokol SET.
- Uprkos nastojanjima velikih kompanija koje se bave elektronskim poslovanjem da što veći broj Internet prodavnica počne da koristi SET, SSL i dalje dominira zbog jednostavnosti uvođenja i korišćenja.
- Prepoznatljiv po prefiksu **https**, kao i po ključu koji je vizuelno predstavljen u većini Web čitača.
- Visa i srodne kompanije odlučile su da nastupe sa jednostavnim rešenjem nazvano **3D** model (*Three Domain Model*).
- 3D model koristi postojeću SSL infrastrukturu na Internetu i dodaje mali broj novih zahteva:
  - ✓ Obavezno identifikovanje klijenata (E-PIN pri plaćanju preko E-Bank sistema),
  - ✓ Obavezno identifikovanje prodajnog mesta na Internetu,
  - ✓ *Electornic Wallet* kao dodatni modul (plug-in) u Web čitaču korisnika kartice,
  - ✓ SET komunikacija između banke korisnika kartice i banke trgovca.

12 - SSL WEB server

- HTTP komunikacije su prihvatljive za Web servere - obične stranice.
- Ako Web server koristimo za elektronsku trgovinu ili neki drugi servis koji zahteva bezbedne transakcije, mora se obezbediti šifrovanje podat.
- Razvijen je *Secure Socket Layer* (SSL) protokol, koji koristi javni kriptografski ključ za zaštitu poverljivih informacija korisnika
- SSL koristi digitalne certifikate izdate od strane validnog sertifikacionog tela (CA) radi autentifikacije obe strane u transakciji
- Da bi se povezao na sigurnu Web lokaciju, klijent koristi **https**://
- Kada klijent inicira bezbednu vezu, realizuje se SSL „*handshake*“
- Pretraživač proverava sertifikat da bi utvrdio identitet servera, validnost CA, i potvrdu da sertifikat nije istekao.
- Klijent i server pregovaraju o modelu šifrovanja i korišćenom ključu
- Kada se *handshake* završi, novi ključ je kreiran, i ovaj ključ se koristi za kreiranje ključeva sesije koji se koriste za šifriranje komunikacije
- Kada se pošalje HTTP GET zahtev, polja u formi odgovora i program. promenljive koje su označene na kraju URL se uklanjaju iz URL adrese i ubacuju u šifrovani blok podataka

12 – Protokol SET

- ***S**ecure **E**ncryption **T**ransaction* je predloženi standard za obavljanje transakcija kreditnim ili debitnim karticama preko Interneta
- Razvijaju ga Visa i MasterCard zajedno, uz pomoć kompanija iz oblasti informacionih sistema, kriptografije i Interneta.
- Protokol može da se koristi za sve vrste kreditnih ili debitnih kartica, recimo za American Express ili Discover.
- Osnovne karakteristike i funkcije:
  - ✓ Poverljivost informacija i integritet podataka,
  - ✓ Provera identiteta prodavca i vlasnika kartice i njegovog naloga
- Trgovci i kupci moraju imati softver koji sadrži SET kako bi ga koristili za transakcije kreditnim ili platnim karticama.
- SET koristi sistem sertifikata za proveru identiteta a ne centraliz.server
- Sertifikate izdaje poverljivi entitet i predstavlja dokaz da dati potpis pripada entitetu koji ga je podneo.
- Ovi sertifikati se prosleđuju između platnog softvera kupca, trgovca i poslovne banke kako bi se dokazalo da je svaki entitet koji je uključen u datu transakciju, zaista onaj koji se predstavlja.

12 – Protokol SET

- SET ima prednost nad ostalim platnim sistemima zato što ne zahteva da neka treća strana prati transakcije kreditnim ili platnim karticama
- SET smanjuje troškove transakcija karticama preko Interneta.
- SET koristi jaku kriptografsku zaštitu i modele za proveru.
- Prodavac nema uvid u broj kreditne ili platne kartice kupca.
- Takođe, novac se prebacuje na račun prodavca u roku koji je jednak uobičajenom roku za transakcije karticama.
- Još jedna pogodnost protokola SET jeste i to što ga podržavaju poznate kompanije kao što su MasterCard i Visa.
- SET ima i svoje nedostatke, prvi je taj što mora postojati instaliran softver i na klijentu i na serveru koji omogućavaju obradu SET transakcija.
- I banke moraju da sklope ugovore sa nekom kompanijom koja će upravljati njihovim platnim mrežnim prolazom, ili će same instalirati takav prolaz.
- Pored toga, prodavci moraju da otvore račun kod poslovne banke koja je osposobljena da prima SET transakcije.

12 – Protokol SIP

- ***S**ession **I**nitation **P**rotocol* služi da bi se uspostavla, održavala, modifikovala i raskinula multimedijska sesija.
- Učesnici u sesijama mogu biti ljudi ili računarski mehanizmi
- SIP poziv koristi se za kreiranje sesije i definisanje njenih parametara.
- Mobilnost korisnika podržana je kroz *proxy* i *redirect* servere, preusmeravanjem poziva na trenutnu lokaciju korisnika.
- Korisnici mogu na jednostavan način registrovati svoje nove lokacije, koje se beleže na SIP serverima.
- Protokol je koncipiran nezavisno od transportnog medijuma
- Ipak isključivo se koristi na IP protokolu, a u transportnom sloju može koristiti ravnopravno i TCP i UDP protokole
- Implementacija SIP protokola je jednostavna.
- Temelji se na dobro razrađenom HTTP protokolu i slično njemu poseduje tekstualnu reprezentaciju poruka.
- Ova činjenica ga čini jednostavnim za otklanjanje grešaka kao i za analizu ispravnosti rada kod razvoja aplikacija

12 – Protokol SIP

- SIP u svom radu koristi različite protokole:

1. **RSVP** (*Resource reSerVation Protocol*) koji se koristi za rezervaciju mrežnih resursa i pomaže za ostvarivanje određenog nivoa kvaliteta usluge
2. **RTP** (*Real Time Protocol*) / RTCP (*Real Time Control Protocol*) / RTSP (*Real Time Streaming Protocol*) – protokoli aplikacijskog nivoa koji služe za slanje podataka u realnom vremenu,
3. **SAP** (*Session Announcement Protocol*) - protokol za objavljivanje multimedijalnih sesija
4. **SDP** (*Session Description Protocol*) – protokol za opis multimedijalnih sesija

12 - Spam - Elektronska pošta

- Neželjena elektr. pošta (*spam*) jedan je od najvećih problema Interneta
- To su poruke sličnog/istog sadržaja koje se šalju hiljadama korisnika
- Sadržaj same poruke najčešće je reklama nekog proizvoda, finansijska ponuda ili neka druga vrsta usluge.
- Adrese se najčešće skupljaju posebno prilagođenim skriptama koje pretražuju *Usenet* grupe i *Web* stranice ili se stvaraju nasumičnim kombinovanjem najčešćih korisničkih imena i poznatih domena.
- Statistika kaže da je danas između **55%-60%** svih *e-mail* poruka *spam*
- Osim ometanja korisnika pri korišćenju elektronske pošte, *spam* troši ogromne količine resursa, stvarajući finansijske i tehnološke gubitke.
- Udeo *spama* u sveukupnom broju *e-mail* poruka neprestano raste.
- Razvijen je veliki broj metoda i alata namenjenih blokiranju *spama*.
- Iako do sada nije osmišljen način potpunog uklanjanja *spam*-a, postoje specifična rešenja koja na nivou lokalnih računarskih mreža pokazuju izvrsne rezultate.

12 - Spam - Elektronska pošta

- Metode filtriranja neželjenih poruka koje se najčešće koriste, a ne baziraju se na analizi sadržaja poruke (prve tri metode), jesu:
  1. Metoda "**bele liste**"(*whitelisting*),
  2. Metoda "**crne liste**"(*blacklisting*),
  3. Metoda "**sive liste**"(*graylisting*),
  4. **Bajesova tehnika filtriranja spama**.
- Bajesova metoda se jedina bazira na analiziranju sadržaja poruke
- One se vrlo često kombinuju radi postizanja boljeg stepena filtriranja.
- Kod primene ***Whitelisting*** metode prihvataju se sve poruke koje se nalaze na *whitelist* popisu (IP adrese) dok se ostale tretiraju kao *spam*.
- Kod ***Blacklisting*** metode važi pak pravilo da se sve poruke pristigle s *blacklist* popisa proglašavaju *spam*-om dok se ostale propuštaju.
- Iako se popis može čuvati lokalno, najčešće se ti popisi proveravaju u realnom vremenu, sa servera namenjenih upravo tome www.dnsbl.info

12 - Spam - Elektronska pošta

- ***Greylisting*** je zamišljen kao *antispam* metoda koja će krajnjem korisniku biti potpuno transparentna a od administratora servera elektronske pošte zahtevati minimalnu količinu održavanja.
- Može se grubo opisati kao kombinacija *whitelist* i *blacklist* metoda.
- U terminima elektronske pošte, to su komplementarne metode koje se temelje na bezuslovnom prihvatanju odnosno odbacivanju sve pošte
- Prilikom pokušaja dostave poruke elektronske pošte, *greylisting* metoda pregledava tri osnovne informacije:
  1. IP adresu računara koji pokušava dostaviti poruku,
  2. *e-mail* adresu pošiljalaca („MAIL FROM“ polje) i
  3. *e-mail* adresu primaoca („RCPT TO“ polje).
- Kombinacija ovih informacija čini jedan triplet.
- U slučaju da je određeni triplet prvi put viđen, odbija se njegova isporuka kao i isporuka svih poruka sa istim tripletom koje stignu u određenom vremenskom periodu.
- SMTP (*Simple Mail Transfer Protocol*) protokol specificira mogućnost privremene nemogućnosti isporuke elektronske pošte

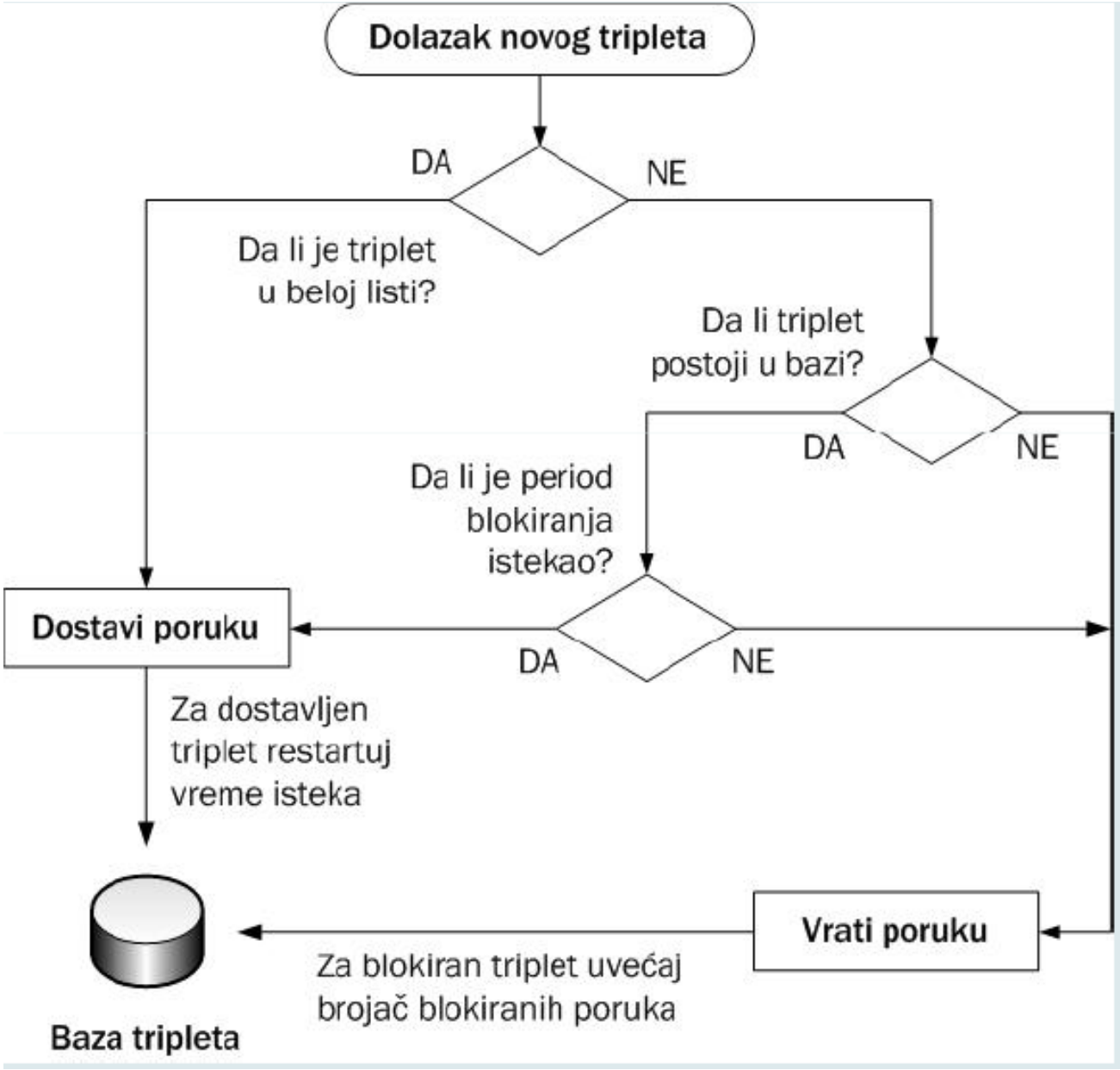
12 - Spam - Elektronska pošta

- ***M**ail **T**ransfer **A**gent* nakon određenog intervala pokušava ponovo da pošalje istu ranije odbijenu poruku
- Kako je većina *spam* poruka poslata koristeći aplikacije koje su razvijene samo u tu svrhu one ne implementiraju u potpunosti SMTP
- Najčešće koriste privremene, dinamičke IP adrese, što automatski onemogućava ponovni pokušaj slanja poruke.
- Važan aspekt ove metode, koji je razlikuje od većine drugih, je činjenica da ne može doći do lažne klasifikacije valjane poruke kao *spam*-a (sve dok MTA potpuno implementira specifikaciju SMTP).
- Metoda je posebno efikasna po pitanju potrošnje resursa u vidu procesorskog vremena, odnosno mrežnog saobraćaja.
- Za razliku od heurističkih metoda raspoznavanja *spam* poruka koje se baziraju na analizi sadržaja poruke, kod *greylisting* metode uopšte se ne pregledava sadržaj poruke.
- Šta više, sadržaj poruke se u slučaju odbacivanja iste čak i ne prima, što uveliko doprinosi smanjivanju mrežnog saobraćaja.

12 - Spam - Elektronska pošta

- Implementacija *greylisting* metode zahteva zapisivanje informacija o pojedinim **tripletima** (IP adresa ko šalje, E-mail pošiljaoca i primaoca)
- Koristi se neki od postojećih sistema za upravljanje bazama podataka, no zbog jednostavnosti operacija moguća su i jednostavnija rešenja.
- Struktura baze podataka vrlo je jednostavna i sastoji se od:
  - ✓ vreme prvog dolaska određenog tripleta,
  - ✓ vreme isteka perioda blokiranja tripleta,
  - ✓ vreme isteka zapisa o tripletu (za stare zapise),
  - ✓ broj blokiranih pokušaja dostave poruke s određenim tripletom i
  - ✓ broj poruka sa određenim tripletom koje su uspešno dostavljene.
- Implementaciju je moguće upotpuniti s dodatnim informacijama, no navedene su dovoljne za ispravni rad *greylisting*-a.
- *Greylisting* je danas implementiran na velikom broju E-mail servera i pokazao se kao jako dobar filter za spam poruke.

12 - Spam - Elektronska pošta



12 - Spam - Elektronska pošta

- Rešenje koje bi u potpunosti uklonilo problem primanja neželjenih mail poruka još uvek nema.
- *Greylisting* je metoda koja ne može zaustaviti slanje *spam* poruka, ali sigurno može pošiljaocima *spam*-a taj proces učiniti vremenski zahtevnijim a samim time i finansijski neisplativim.
- U idealnom slučaju koji podrazumeva distribuirano korišćenje metode na velikom broju servera elektronske pošte, ona može izuzetno poskupeti postupak slanja *spam*-a, do te mere da slanje *spam* poruka pošiljaocima postane neisplativo.
- Metoda ima i svoje nedostatke, u prvom redu to je unošenje vremenskog kašnjenja kod „legalnih“ poruka.
- Iako se kašnjenje događa samo prilikom prve interakcije dveju strana koje koriste servis elektronske pošte, nekim je korisnicima to neprihvatljivo pa stoga ne koriste ovu metodu.

12 - Spam - Elektronska pošta

- *Bayesian spam filtering* je proces korišćenja Bajesovskih statističkih metoda za klasifikaciju dokumenata u kategorije.
- Popularan mehanizam za razlikovanje neželjene pošte od legitimne
- Mnogi moderni klijentski programi za e-poštu, kao što je, na primer, Mozilla Thunderbird, implementiraju ovu metodu za filtriranje spama.
- Filtri e-pošte na serverskoj strani, kao što su SpamAssassin i ASSP, koriste Bajesovu tehniku filtriranja spama, a funkcionalnost je nekad ugrađena i u sam server za poštu.
- Bajesovi filtri e-pošte koriste Bajesovu teoremu.
- Prema Bajesovoj teoremi, verovatnoća da je neka e-pošta spam (tj. da sadrži određene reči) računa se na sledeći način:

$$P(spam|reči)=P(reči|spam)xP(spam)/P(reči)$$

P(spam|reči)-verovatnoća da je pošta spam,
P(reči|spam)-verovatnoća nalaženja ovih reči u spamu,
P(spam)-verovatnoća da je bilo koja e-pošta spam,
P(reči)-verovatnoća nalaženja navedenih reči u pošti.

Hvala na pažnji !!!

Pitanja

? ? ?