SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 8:

Elektronsko poslovanje i sigurnost na Internetu

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Elektronsko poslovanje i sigurnost na Internetu

- Sadržaj poglavlja i predavanja:
  - 8.1 Infrastruktura zaštite u elektronskoj trgovini
  - 8.2 Neželjena elektronska pošta i pecanje
  - 8.3 Sigurnost VoIP mreža
  - 8.4 Sigurnost P2P mreža

Quote

Use your mentality

Wake up to reality

— From the song, "I've Got You under My Skin“ by Cole Porter

Potrebna predznanja

- Programiranje
- Za primenu:
  - Računarske mreže i protokoli
  - Operativni sistemi
  - Sistemsko programiranje
  - Internet

Elektronsko poslovanje i sigurnost na Internetu

- Elektronsko poslovanje uzima sve veći udeo u globalnom poslovanju, smanjuje troškove i omogućava neke nove načine započinjanja, razvoja i rasta posla.

- Sama činjenica da je Internet infrastrukturna osnova elektronskog poslovanja, donosi i brojne sigurnosne rizike i otvara nove mogućnosti koje potencijalni napadači mogu da iskoriste.

8.1 Infrastruktura zaštite u elektronskoj trgovini

- Razvoj Internet tehnologija, Web servisa i sistema sigurnosti i zaštite, kao i sve šira primena kreditnih kartica i „digitalnog novca“, obezbedili su podršku sve naprednijim načinima i mogućnostima elektronskog poslovanja.
- U novije vreme distribuirani sistemi i sistemi koji se oslanjaju na Internet čine osnovu poslovanja sve većeg broja preduzeća i organizacija.
- Sve češće se primenjuju veoma kompleksni portali i Integrisani distribuirani sistemi poslovanja.
- Sistemska podrška u savremenim operativnim sistemima i različitim sistemima baza podataka, transakcionim serverima i sistemima olakšava i ubrzava razvoj elektronskog poslovanja.

Elektronsko poslovanje – vidovi interakcija

- Elektronsko poslovanje danas integriše različite vidove interakcija:
  - B2B (*Business-to-Business*)
  - B2C (*Business-to-Customer*)
  - B2E (*Business-to-Employee*)
  - …
- Uz podršku pouzdanih sistema zaštite i sigurnosti – predstavlja ekonomično okruženje za prezentaciju i plasman roba i usluga.

- Prefiksi:
  - **e** – elektronsko poslovanje, poslovanje bazirano na različitim tipovima primene elektronskih komunikacija i infrastrukture, primarno uključujući (čak podrazumevajući) Internet bazirano poslovanje
  - **m** – mobilno poslovanje, poslovanje bazirano na mobilnoj telefoniji i infrastrukturi tj. mobilnim komunikacijama

Sigurnost sistema elektronske trgovine

- U sistemima elektronske trgovine, zaštita se integriše implementiranjem sledeće osnovne sigurnosne usluge:
  - Provere identiteta
  - Autorizacije
  - Privatnosti
  - Neporicanje, priznavanje (non-repudiation)

Infrastruktura javnih ključeva

- **Infrastrukturu javnih ključeva (PKI)** čini skup komponenata koje upravljaju sertifikatima i ključevima koji se koriste u servisima šifrovanja i generisanja digitalnog potpisa.

- **Sertifikati** obezbeđuju mehanizam za uspostavljanje poverenja u odnosima između javnih ključeva i entiteta koji poseduju odgovarajuće tajne ključeve, čime se garantuje da određeni javni ključ pripada određenom entitetu. Osnovni oblik sertifikata koji se danas koristi, zasniva se na ITU-T standardu X.509. Sertifikat se može posmatrati kao digitalna lična karta odgovarajućeg entiteta.

Certification Authority, CA

- Sertifikate javnih ključeva izdaje sertifikacioni centar (engl. *Certification Authority*, *CA*).
- U zavisnosti od oblasti primene, to može biti neka državna institucija od poverenja, ali i bilo koja institucija ili pojedinac koji izdaju sertifikate za svoje komintente.
- Pored opštih podataka o identitetu (naziv, adresa, organizacija, država itd.) sadrži još i javni ključ identiteta, podatke o izdavaocu sertifikata i sve to overeno digitalnim potpisom CA.
- Sertifikaciono telo izdaje sertifikate podnosiocima zahteva na osnovu uspostavljenih kriterijuma.
- CA se pojavljuje u ulozi garanta prilikom uspostavljanja korelacije između javnog ključa subjekta i ostalih identifikacionih podataka o tom subjektu koji su sadržani u izdatom sertifikatu.

Certification Authority, CA (nastavak)

- CA se mogu organizovati po hijerarhijskom modelu.
- To omogućava veću funkcionalnost i jednostavniju administraciju.
- Generalno, hijerarhija CA sadrži više CA sa strogo definisanim odnosom roditelj-dete.
- CA koji je najviši u hijerarhiji, u opštem slučaju se naziva korenski CA (engl. *root CA*) – sertifikat CA je samopotpisan (engl. *self-signed*), tj. potpisan privatnim ključem CA.

Osnovni sistemi plaćanja i digitalnog novca

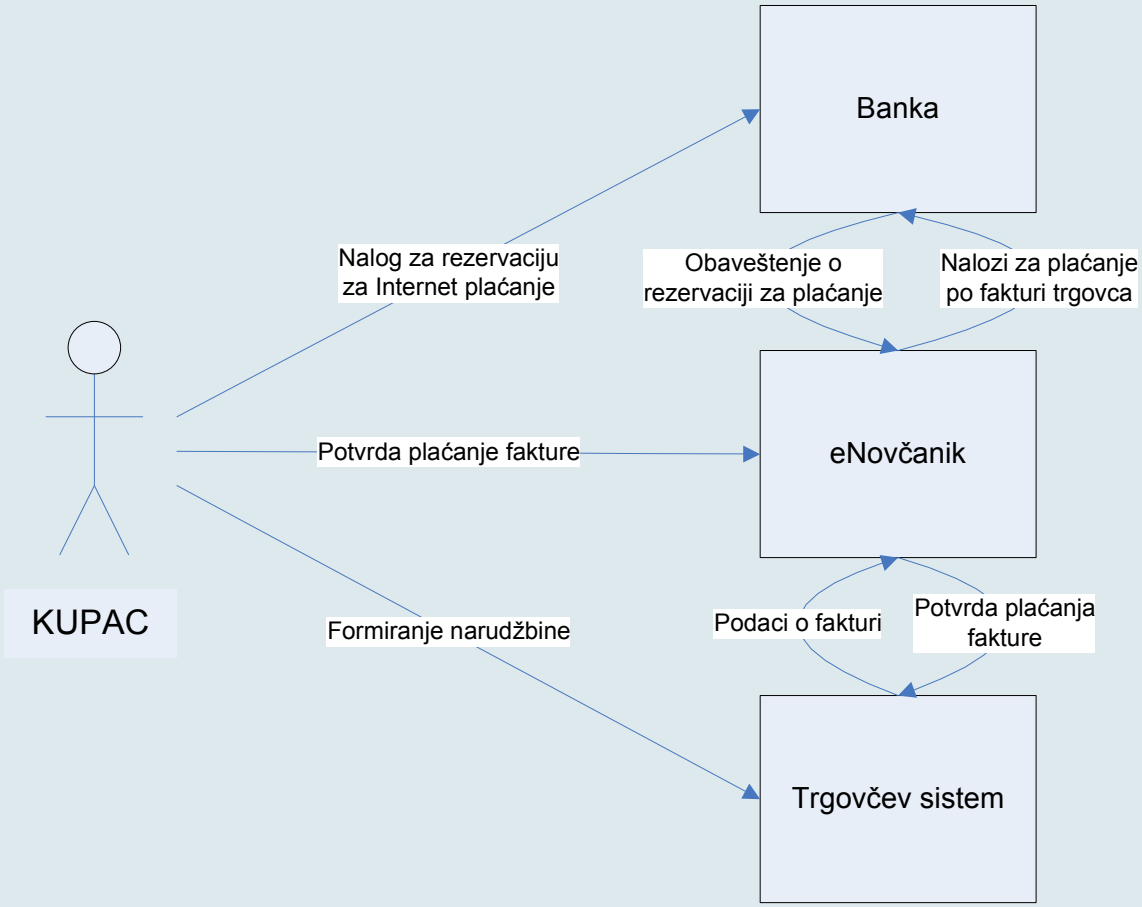
- PayPal
- CyberCash
- First Virtual (FV)
- E–Cash
- NetCash
- Mondex
- VisaCash

- eNovčanik

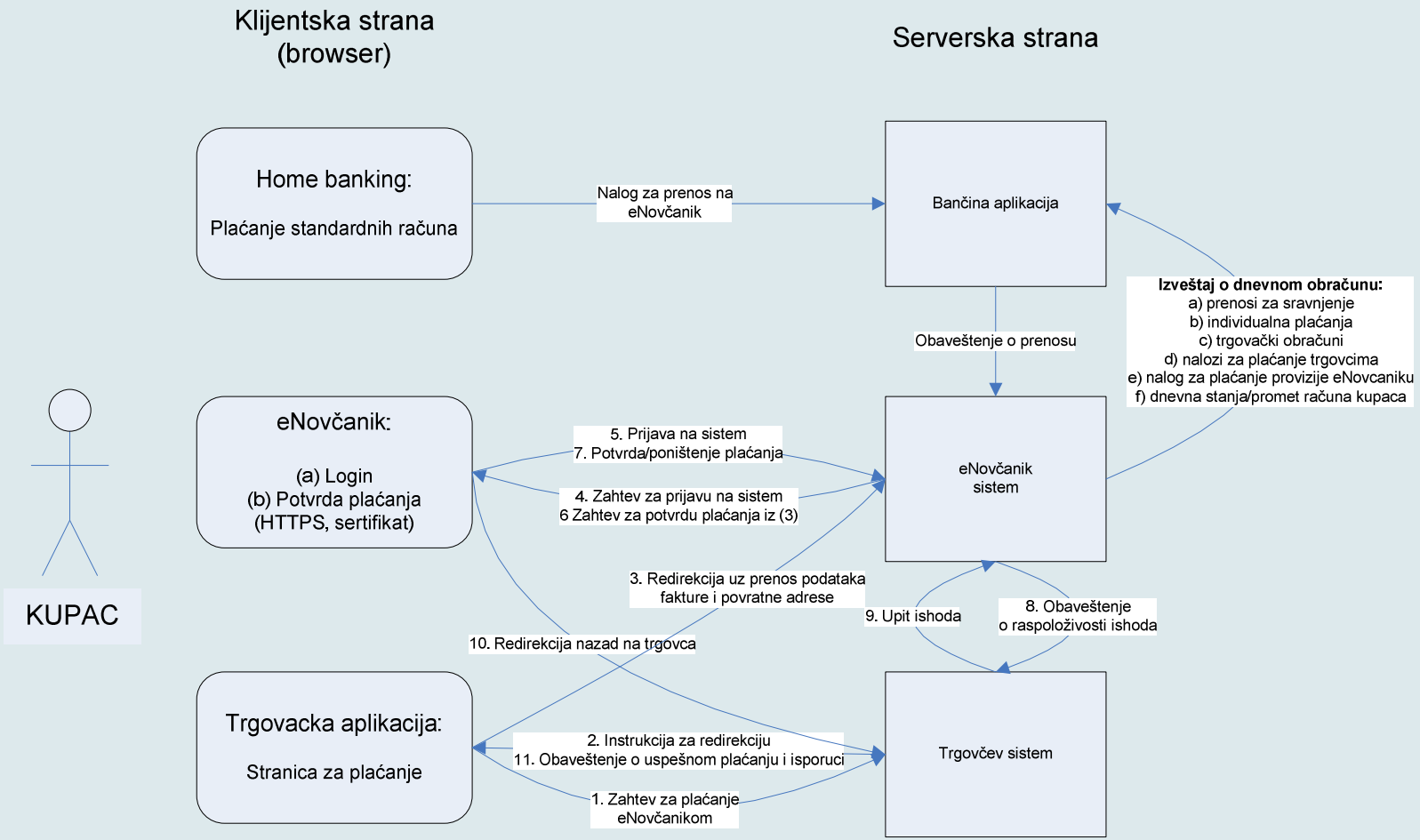
eNovčanik

- Ideja domaćeg platnog servisa na Internetu koji implementira proces ugovaranja plaćanja između trgovca i kupca

eNovčanik – Princip plaćanja



eNovčanik – Detalji plaćanja



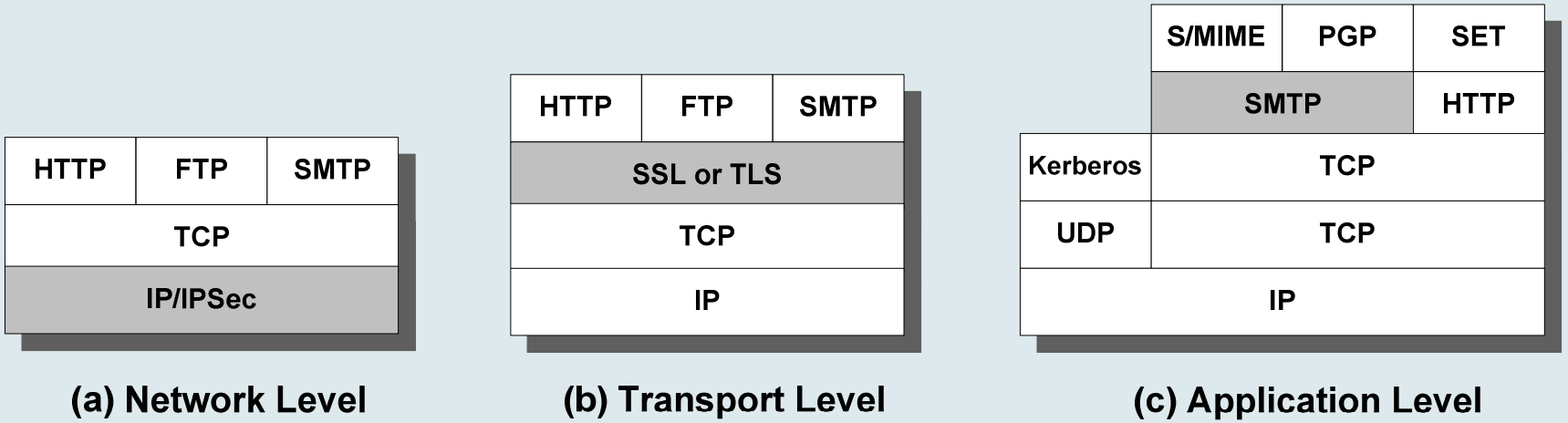
eNovčanik - Sigurnost

- **Tehnička**
  - SSL/HTTPS pristup za kupce i trgovce
  - Komunikacija sa bankom na bazi digitalno potpisanih poruka
  - Autentikacija kupaca i trgovaca na bazi lozinke
  - Dodatna autentikacija kupca pri potvrdi plaćanja na bazi transakcijskih PIN-ova dostavljenih SMS porukama (za veća plaćanja ili prelazak kumulativnog praga)
  - Administrativna aplikacija dostupna samo u privatnoj mreži
  - "Odbrana u dubinu" (koncentrični krugovi odbrane sistema i aplikacije)
  - Fizičko obezbeđenje sistema koji nosi aplikaciju
- **Operativna**
  - Plaćanje uvek autorizuje vlasnik računa; trgovac nema mogućnost da povlači novac na bazi podataka koje zna o kupcu (kao npr. kod kartica na bazi broja kartice itd)
  - Sprečavanje pranja novca: ne može se prenositi sa računa na račun u banci preko eNovčanika – samo plaćanje trgovcu ili povrat para nazad na isti račun; kupac može koristiti račune samo u jednoj banci u jednom trenutku.
  - Trgovcima plaća banka na bazi dnevnog obračuna
  - Banka ne postupa po nalozima trgovcima ako ne upari svoje prenose u novčanik (ako ima nepoznatih itd)
  - Novčanik kupca će po pravilu imati značajno raspoloživo stanje samo u toku kupovine
- **Identitet**
  - eNovčanik: SSL sertifikat
  - Kupac: na bazi ličnih podataka poslatih iz banke uz svaku uplatu
  - Trgovac: Račun se otvara tek po prijemu relevantnih potvrda identiteta poštom ili direktno, i verifikaciji sa bankom koja drži račun uplate pazara

SET protokol

- SET je predloženi standard za obavljanje transakcija kreditnim/debitnim karticama preko Interneta; zajednički ga razvijaju Visa i MasterCard, uz tehničku pomoć raznovrsnih kompanija iz oblasti informacionih sistema, kriptografije i Interneta, kao što su IBM i VeriSign.
- Bez obzira na to što ga razvijaju navedene dve kompanije, protokol može da se koristi za sve vrste kreditnih/debitnih kartica, recimo za American Express ili Discover.

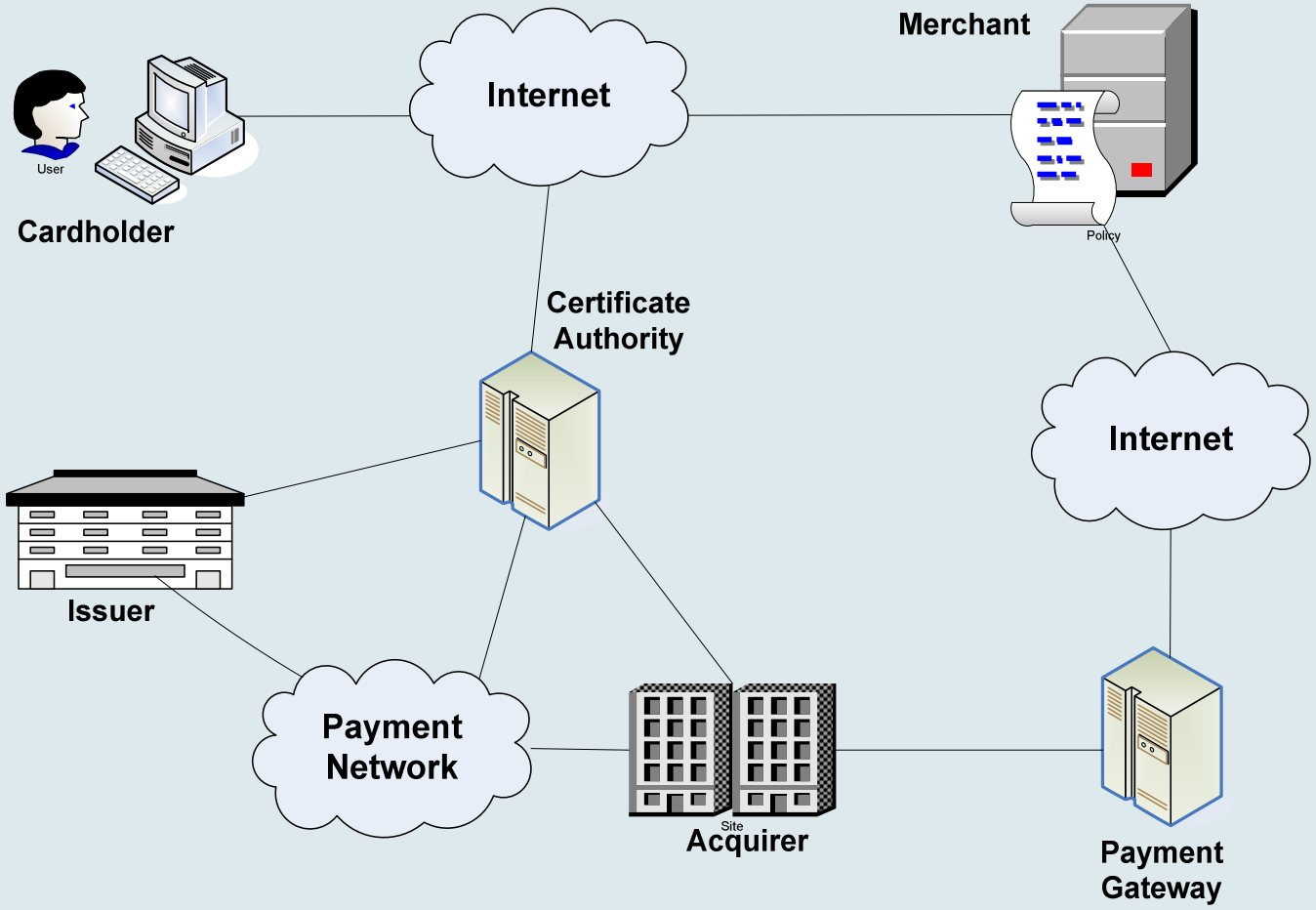
Položaj protokola SET u skupu protokola TCP/IP



SET Overview

- Osnovne karakteristike i funkcije:
  - Poverljivost informacija
  - Integritet podataka
  - Provera identiteta vlasnika kartice i njegovog naloga
  - Provera identiteta trgovca

Učesnici u SET protokolu



Proces kupovine

- Kupovina uz upotrebu protokola SET i kreditne/platne kartice odvija se u koracima koji su opisani u knjizi:
  - "Sigurnost računarskih sistema i mreža"

SSL Web server

- Protokol *Security Socket Layer* (SSL) predstavlja *de facto* standard za zaštitu podataka.
- Prepoznatljiv po prefiksu https:, kao i po ključu ili sličnom simbolu, koji je vizuelno predstavljen u većini Web čitača
- SSL i dalje dominira zbog jednostavnosti uvođenja i korišćenja.

- Manji broj prodavnica na Internetu koristi protokol *Secure Electronic Transactions* (SET).

- Posle godina nastojanja da trgovce na Internetu privole da koriste SET, Visa i srodne kompanije odlučile su da nastupe s jednostavnijim rešenjem. Novo rešenje je nazvano 3D model (Three Domain Model).

Web serveri

- Apache www.apache.org
- Netscape
- Planet www.iplanet.com
- Microsoft Internet Information Server (IIS)

Standard sigurnosti podataka industrije platnih kartica

- **PCI DSS (*Payment Card Industry Data Security Standard*)**

- [I] Izgrađivanje i održavanje sigurne mreže
  - Zahtev 1: Instalacija i održavanje konfiguracije zaštitne barijere radi zaštite podataka.
  - Zahtev 2: Ne koristiti podrazumevane vrednosti za lozinke i druge sigurnosne parametre.
- [II] Zaštita podataka vlasnika platnih kartica
  - Zahtev 3: Zaštita uskladištenih podataka.
  - Zahtev 4: Šifrovanje podataka o karticama i drugih osetljivih informacija koje se prenose preko javnih mreža.
- [III] Održavanje programa za rukovanje ranjivostima
  - Zahtev 5: Korišćenje i redovno ažuriranje antivirusnog softvera.
  - Zahtev 6: Razvoj i održavanje sigurnog sistema i aplikacija.

Standard sigurnosti podataka industrije platnih kartica (nastavak)

- **PCI DSS (*Payment Card Industry Data Security Standard*)**

- [IV] Implementacija strogih mera kontrole pristupa
  - Zahtev 7: Restrikcija pristupa podacima po poslovnom principu "treba da zna".
  - Zahtev 8: Dodela jedinstvene identifikacije svakom licu koje ima pristup računaru.
  - Zahtev 9: Ograničavanje fizikog pristupa podacima o vlasnicima kartica.
- [V] Redovno nadziranje i ispitivanje mreže
  - Zahtev 10: Praćenje i nadgledanje svih pristupa mrežnim resursima i podacima o vlasnicima kartica.
  - Zahtev 11: Redovno proveravanje sigurnosnih sistema procesa.
- [VI] Održavanje politike sigurnosti informacija
  - Zahtev 12: Održavanje politike koja se odnosi na sigurnost informacija.

Mobilna elektronska trgovina

- Mobilna elektronska trgovina (engl. *m-commerce*, *mobile commerce*) predstavlja svaku transakciju novčane vrednosti koja je realizovana preko mobilne telekomunikacione mreže.

- U skladu sa ovom definicijom, m-trgovina predstavlja podskup svih transakcija e-trgovine, kako u B2C (*business-to-customer*), tako i u B2B (*business-to-business*) segmentu.

Generatori razvoja mobilne elektronske trgovine

- Masovno tržište mobilne telefonije
- Nagli razvoj Interneta i elektronske trgovine
- Usavršavanje opreme i uređaja za mobilnu telefoniju
- Novi principi tarifiranja usluga
- Brz razvoj novih i bržih načina komunikacije kao što su UMTS (3G) itd.

Usluge mobilne elektronske trgovine

- Bankarske usluge
- Berzanske usluge
- *On-line* kupovinu
- Servise sadržaja (npr. vesti, vremenska prognoza, red vožnje i letenja, zabavni sadržaji kao što su: rezultati sportskih takmičenja, horoskop, muzika, video...)

Mobilna elektronska trgovina u poslovnim sistemima

- Integracija lanca snabdevanja
- Telemetrija
- Upravljanje transportnom flotom
- Upravljanje odnosima sa korisnicima
- Automatizacija prodaje
- WASP (Wireless Application Service Provider) i druge

8.2 Neželjena elektronska pošta, pecanje i pharming

- Neželjena elektronska pošta (engl. *spam*)
- Pecanje (engl. *phishing*)
- Farming (engl. *pharming*)

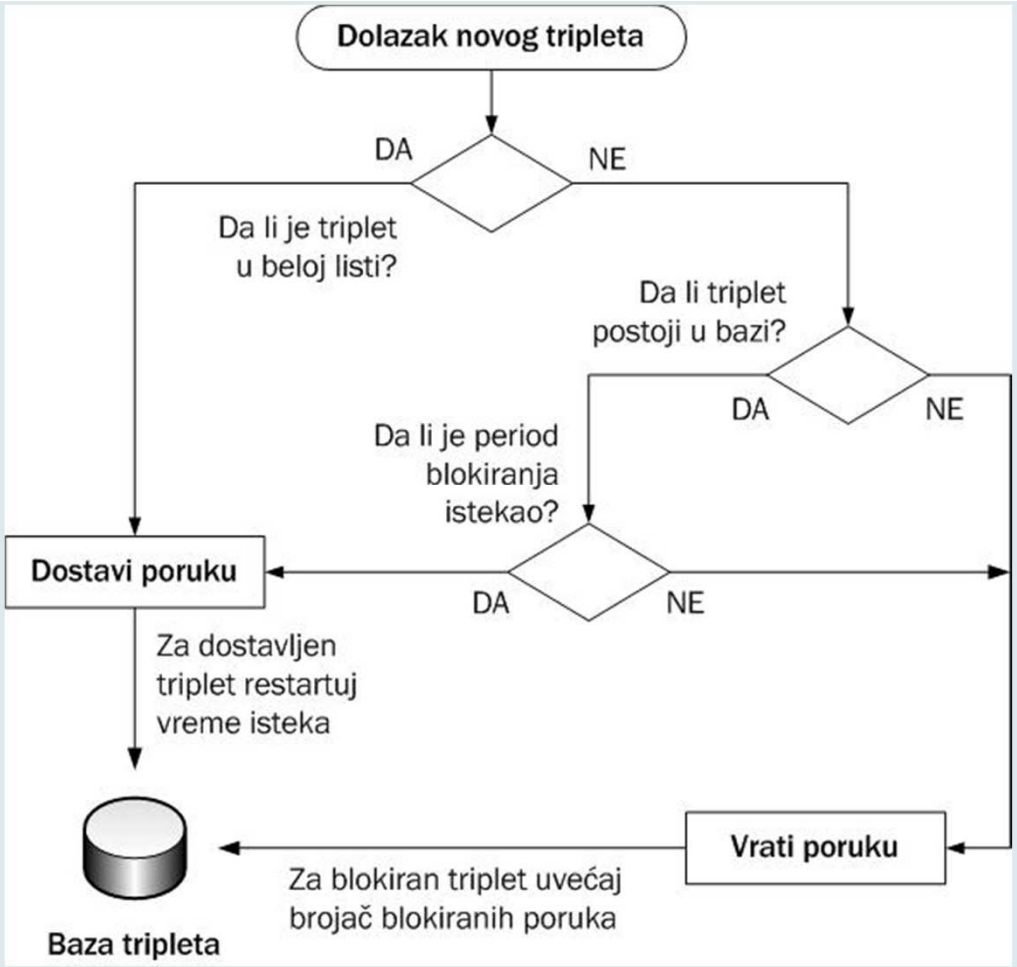
Metode filtriranja neželjene pošte

- Metoda „bele liste“(engl. *whitelisting*)
- Metoda „crne liste“ (engl. *blacklisting*)
- Metoda „sive liste“ (engl. *graylisting*)
- Bajesova tehnika filtriranja spama

Metoda „sive liste“

- Triplet - tri osnovne informacije:
  - IP adresu računara s kog je poslata poruka,
  - adresu pošiljaoca (polje MAIL FROM) i
  - adresu primaoca (polje RCPT TO).

Metoda „sive liste“...



Bajesova tehnika filtriranja spama

- Bajesova tehnika filtriranja spama (engl. *Bayesian spam filtering*) jeste proces korišćenja Bajesovskih statističkih metoda za klasifikaciju dokumenata u kategorije.

- Ovu metodu predložili su Sahami i ostali (1998.) a veliko interesovanje je pobudila tokom 2002, kada je opisana u radu „*A Plan for Spam*“ Paula Grahama. Od tada je to postao popularan mehanizam za razlikovanje neligitimne i 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.

Bajesova tehnika filtriranja spama…

- 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:

$$P(\text{spam}|\text{reči}) = \frac{P(\text{reči}|\text{spam}) \times P(\text{spam})}{P(\text{reči})}$$

gde je:

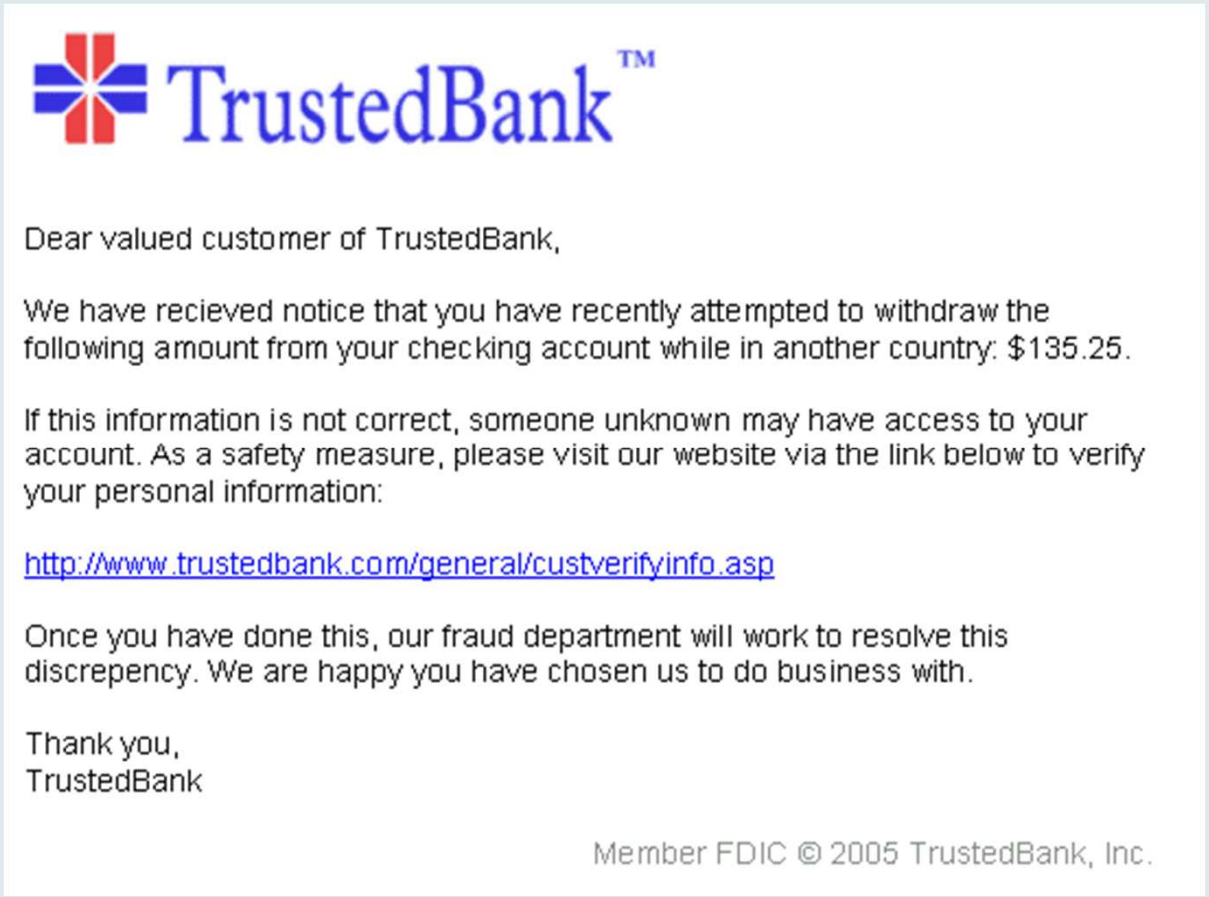
- P(spam | reči) – verovatnoća da je pošta spam (tj. da je pošta koja sadrži određene reči spam)
- P(reči | spam) – verovatnoća nalaženja ovih reči u spamu
- P(spam) – verovatnoća da je bilo koja e-pošta spam
- P(reči) – verovatnoća nalaženja navedenih reči u pošti

Pecanje

- Pecanje (engl. *phishing*) u računarstvu predstavlja vrstu kriminalne aktivnosti koja koristi tehnike društvenog inženjeringa, to jest prevara, i pomoću koje napadači dolaze do osetljivih informacija, kao što su razne lozinke i detalji o kreditnim karticama.

- Pecanje se najčešće izvodi pomoću elektronske pošte ili sistema trenutnih poruka (engl. *instant messages*).

Primer pecanja



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

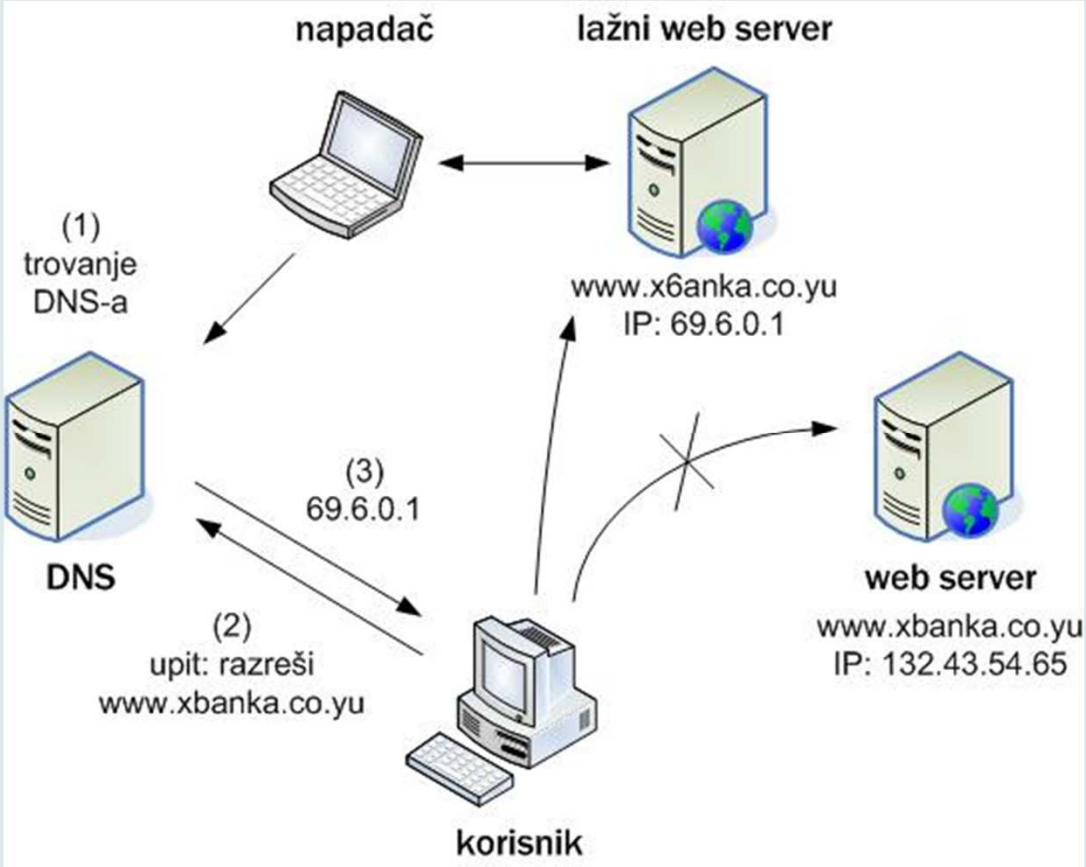
Farming

- Farming (engl. *pharming*) je napad koji za cilj ima preusmeravanje HTTP zahteva korisnika na lažirane i zlonamerne lokacije umesto na originalne.
- Farming je, uopšteno govoreći, napad čiji je rezultat sličan pecanju – korisnik koji je uspešno prevaren ostaviće osetljive podatke (lozinka ili broj kreditne kartice) na Web stranici napadača koja je lažno predstavljena kao legitimna Web lokacija.
- Ovaj napad se razlikuje od pecanja u tome što napadač ne mora da navodi korisnika da pritisne hipervezu u elektronskoj poruci; čak i ako korisnik tačno unese URL (Web adresu) u adresno polje Web čitača, napadač i dalje može da ga preusmeri na zlonamernu Web lokaciju. Zbog toga je i uvedeno novo ime – farming – kako bi se napravila razlika između ove dve vrste napada.

Farming...

- *Pharming* se obično izvodi tehnikama otimanja DNS-a ili „trovanja“ DNS keša (engl. *DNS cache poisoning*). Postoje dve različite metode otimanja DNS-a (engl. *DNS hijacking*).

Izvođenje farming napada



Zaštite od farming napada

- Postoji nekoliko dobrih preporuka kako da se zaštitite od ove prevare na Internetu, ali odmah se mora reći da apsolutna zaštita ne postoji.
- Napadači će uvek naći način da prevare naivne i neobrazovane korisnike, ali često i vrlo iskusne korisnike, pa čak i eksperte.

- Ukoliko je ikako moguće koristite samo „*pharming-conscious*“ (PhC) Web stranice
- Pažljivo proveravanje Web lokacija
- Proveravanje sertifikata
- Zaštita DNS servera kod Internet posrednika

8.3 Sigurnost VoIP mreža

- VoIP telefonija (*Voice over Internet Protocol*) jeste proces prenosa digitalizovanog glasa preko IP mreža pomoću odgovarajućih protokola.

- VoIP standardi i protokoli
  - H.323
  - SIP (*Session Initiation Protocol*)

Pretnje sigurnosti VoIP mreža

- Neovlašćeno praćenje i prisluškivanje mrežnog saobraćaja (engl. *sniffing/eavesdropping*)
- Napadi uskraćivanja (odbijanja) usluga (engl. *Denial of Service – DoS*)
- Presretanje poziva (engl. *call interception*)
- Krađom tuđeg identiteta
- Finansijska zloupotreba VoIP infrastrukture (engl. *call fraud*)

Preporuke za povećanje sigurnosti VoIP mreža

- Odvajanje IP adresa
- Virtuelne lokalne mreže
- Mrežne barijere
- Šifrovanje

8.4 Sigurnost P2P mreža

- *Peer-to-peer* ili, skraćeno, P2P mreže (mreže ravnopravnih računara) nastale su kao entuzijastički projekat ljudi koji su želeli da unaprede način deljenja datoteka.

- P2P mreže su se pokazale kao veoma dobra infrastruktura za deljenje datoteka, kojoj nisu potrebni centralni serveri emitovanje multimedijalnih sadržaja sa deljenjem opterećenja (engl. *load balancing*), kao i distribuirani sistemi za pravljenje rezervnih kopija (engl. *backup systems*).

- Zbog svega toga su P2P mreže u poslednjih nekoliko godina dostigle veliku popularnost.

Napadi na P2P mreže

- Napadi na mrežnu infrastrukturu
  - Napadi tipa DoS i DDoS
  - Napadi tipa „čovek u sredini“ (engl. *man in the middle*)
- “Trovanje” datoteka i distribuiranje zlonamernih programa
  - “Trovanje” datoteka
  - Crvi i drugi zlonamerni programi
- Napadi na P2P nivou
  - Jedan od mogućih napada na P2P nivou koji iskorišćava redundantnost resursa jeste napad višestrukim identitetima (engl. *Sybil attack*). Identitet (engl. *identity*) je u P2P mrežama apstrakcija koja predstavlja određeni entitet (čvor)
  - Napad podelom mreže (*engl. eclipse attack*)

Zaštita P2P mreža

- Prema **stepenu centralizovanosti** (odnos broja kritičnih komponenata i običnih čvorova) P2P mreže se dele na:
  - **hibridne** (engl. *hybrid*) – centralni server čuva informacije o mreži, a čvorovi podatke; čvor koji želi da kontaktira drugi čvor, najpre od servera traži njegovu adresu,
  - **čiste** (engl. *pure*) – u mreži ne postoji centralni server, i
  - **mešane** (engl. *mixed*) – mreže bez centralnog servera koje grupišu čvorove oko takozvanih superčvorova (engl. *supernode*); primer ovakve mreže je Gnutella).

- Zaštita od napada navedeni na prethodnom slajdu – dosta novo područje i implicira dosta problema.

Literatura

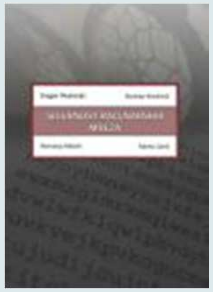
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

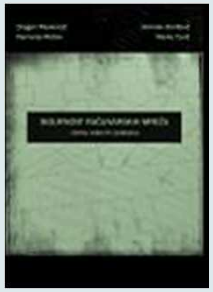
- Za predavanje 8:
  - Poglavlje 8: Elektronsko poslovanje i sigurnost na Internetu

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

  Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?