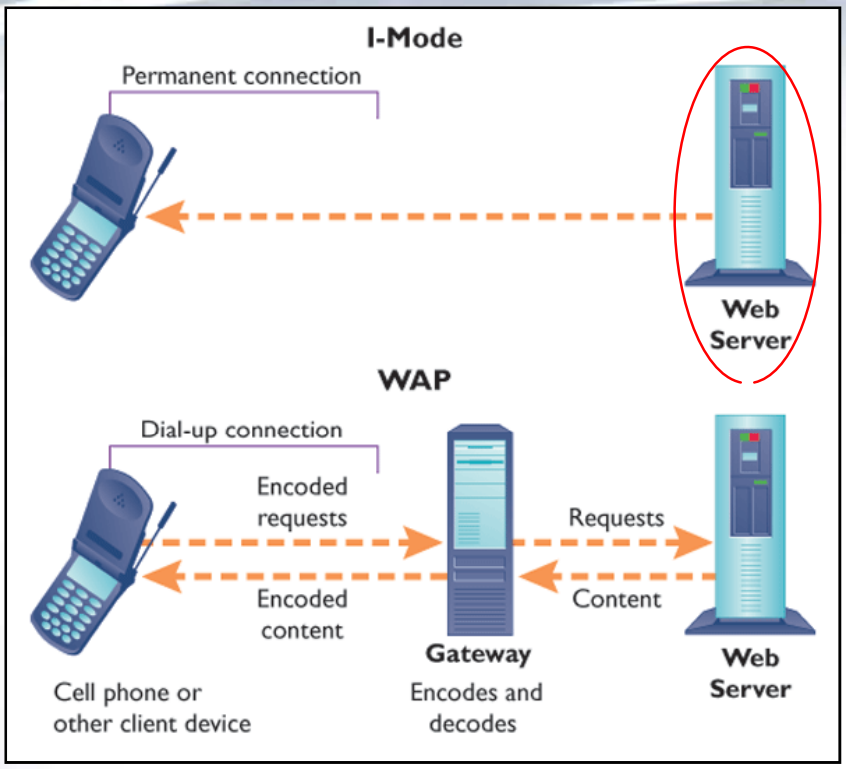
ELEKTRONSKO POSLOVANJE



dr Siniša RANKOV, redovni profesor

Brankica Pažun, asistent

Izvor: Laudon, The Internet: Information Technology Infrastructure for the Digital Firm, PHI 2005

MEGATREND UNIVERZITET
FAKULTET ZA POSLOVNE STUDIJE

ELEKTRONSKO POSLOVANJE

План и програм рада за летњи семестар, школске 2013-14
Предмет: ЕЛЕКТРОНСКО ПОСЛОВАЊЕ
Обавезна литература:

1. **Dave Chaffey, *E-Business and E-Commerce Management*, Pearson Educations, Harlow, 2007.**
2. **Efraim Turban, David King, Dennis Viehland, Jae Lee, *Electronic Commerce 2006: a managerial perspective*, Pearson Education, Upper Saddle River, 2006.**
3. **Kenneth C. Laudon, Carol Guercio Traver, *E-commerce: business, technology, society*, Pearson Educations, Boston, 2004.**
4. **Новаковић, Ј., *Електронско пословање*, Мегатренд, Београд, 2008.**

Професор: Др Синиша РАНКОВ, презентација предавања: http://www.megatrend.edu.rs

Нед	Проф.др Синиша Ранков **Наставна јединица** предавања	**Бр.часова** предавања нед. по студ. групи
1.	Појам е-пословања и фактори који су условили развој е-пословања, дефиниције електронског пословања, дигитална економија, примена електронског пословања у домену науке и образовања (академске мреже, e_science grid computing)	4
2.	Користи од преласка са традиционалног на е-пословање, виртуелне организације, примери	4
3.	Појам инфраструктуре и управљање инфраструктуром е-пословања, СВИФТ стандарди, социјалне мреже (Facebook, Twitter,...)	4
4.	Технологије е-пословања, СВИФТ поруке и модели плаћања, e-banking, системи плаћања	4
5.	Интернет, интранет, екстранет, интернет 2, WEB 2.0, СВИФТ технологија-налози и процеси мапирања, примери	4
6.	Xml, WEB портали, PMS системи и остале технологије е-пословања, СВИФТ мрежа и сервиси, примери	4
7.	Трендови информационих и комуникационих технологија	4
8.	Појам е-тржишта, главне компоненте и учесници, front-end, back-end, СВИФТ инфраструктура, размена порука на СВИФТ МРЕЖИ	4
9.	***I колоквијум*** *– поглавља:ДЕО I, ДЕО II, СВИФТ технологија, модели електронског пословања*	4
10.	Модели е-трговине B2B, B2P, P2P, трговина унутар компаније, примери	4
11.	Остали модели е-трговине:е-влада, m-трговина, е-образовање, примери	4
12.	Стратегије е-пословања	4
13.	Управљање ланцем понуда, MRP, MRPII, ERP i SPM системи и оптимизације	4
14.	Управљање односима с потрошачима, примери, Безбедносни аспект е-пословања и механизми заштите, крипрографија, модели шифрирања	4
15.	***II колоквијум*** *– поглавља:ДЕО III, ДЕО IV, ДЕО V, ДЕО VI i СВИФТ технологија,,*развојне стратегије за апликације е-пословања, развој апликација према MSF оквиру	4
	укупно	**60**

Неде-ља	**ВЕЖБЕ** Наставна јединица асистент:Бранкица Пажун	**Бр.часова** предавања нед. по студ. групи
1.	Основе е-пословања; пројектовање и начин израде web страница, планирање и организовање садржаја web локације	2
2.	Појам статичких и динамичких web страница; израда web презентација, увод у HTML	2
3.	Израда web презентација, HTML, PSS	2
4.	Израда web презентација, HTML, PSS (наставак)	2
5.	Системи за управљање садржајем (PMS); системи за управљање web садржајима; платформе: mambo, joomla, drupal, postnuke	2
6.	Израда и одржавање вебсајта - систем joomla (могућности; основни елементи; неопходно окружење – инсталирање wamp сервера; појам база података; MySQL – импорт&експорт базе)	2
7.	Основе администрирања Joomla система: чеони и позадински приказ локације, палета менија, алатки, радни простор; администраторске функције на палети менија	2
8.	Припрема садржаја презентације: управљање секцијама, категоријама и чланцима; уређивање садржаја – чланака (WYSIWYG едитор)	2
9.	Менији и навигација (Menu manager), проширења (Extension manager), модули (уграђени, креирање произвољног HTML модула), шаблони (инсталирање, едитовање)	2
10.	Израда web локације школе/факултета помоћу система Joomla – пример 1	2
11.	Израда web локације за ресторан помоћу система Joomla - пример 2	2
12.	Презентације студената – одбрана семинарског рада (пример креирања сајта уз детаљну документацију)	2
13.	Презентације студената – одбрана семинарског рада (пример креирања сајта уз детаљну документацију)	2
14.	Презентације студената – **одбрана семинарског рада** (пример креирања сајта уз детаљну документацију)	2
15.	Сумирање резултата и договор за испит	2
	укупно	**30**

Slajdovi koji su dati u prezentaciji su samo za INTERNU UPOTREBU.
Namenjeni su studentima **MEGATREND UNIVERZITETA – FAKULTETA ZA POSLOVNE STUDIJE** za pripremu **kolokvijuma, ispita i seminarskih radova** iz predmeta **ELEKTRONSKO POSLOVANJE**.

pogl		**DEO V : BEZBEDNOST i ZAŠTITA e-POSLOVANJA**
15		**BEZBEDNOSNI ASPEKT e-POSLOVANJA**
	15.1	Ekonomske posledice zloupotrebe ili otkaza tehnologija u e-poslovanju
	15.2	Opšte pretnje sistemu
	15.3	Osnovni ciljevi mera bezbednosti u informacionom sistemu
	15.4	Proces utvrdjivanja identiteta korisnika
	15.5	Poricanje transakcija
16		**MEHANIZMI ZAŠTITE**
	16.1	Kriptografija i tehnologija digitalnog potpisa
		16.1.1 Asimetrično šifrovanje
		16.1.2 Simetrično šifrovanje
	16.2	Infrastruktura javnih ključeva
	16.3	Sigurnosni protokoli
	16.4	Ostali mehanizmi zaštite
	16.5	Sigurnost zaštitnih mehanizama

CILJEVI proučavanja poglavlja

- ekonomske posledice otkaza ili **zloupotrebe Internet tehnologija u e-poslovanju**;
- pretnje sistemu i osnovnim ciljevima mera bezbednosti;
- vrste bezbednosnih servisa:

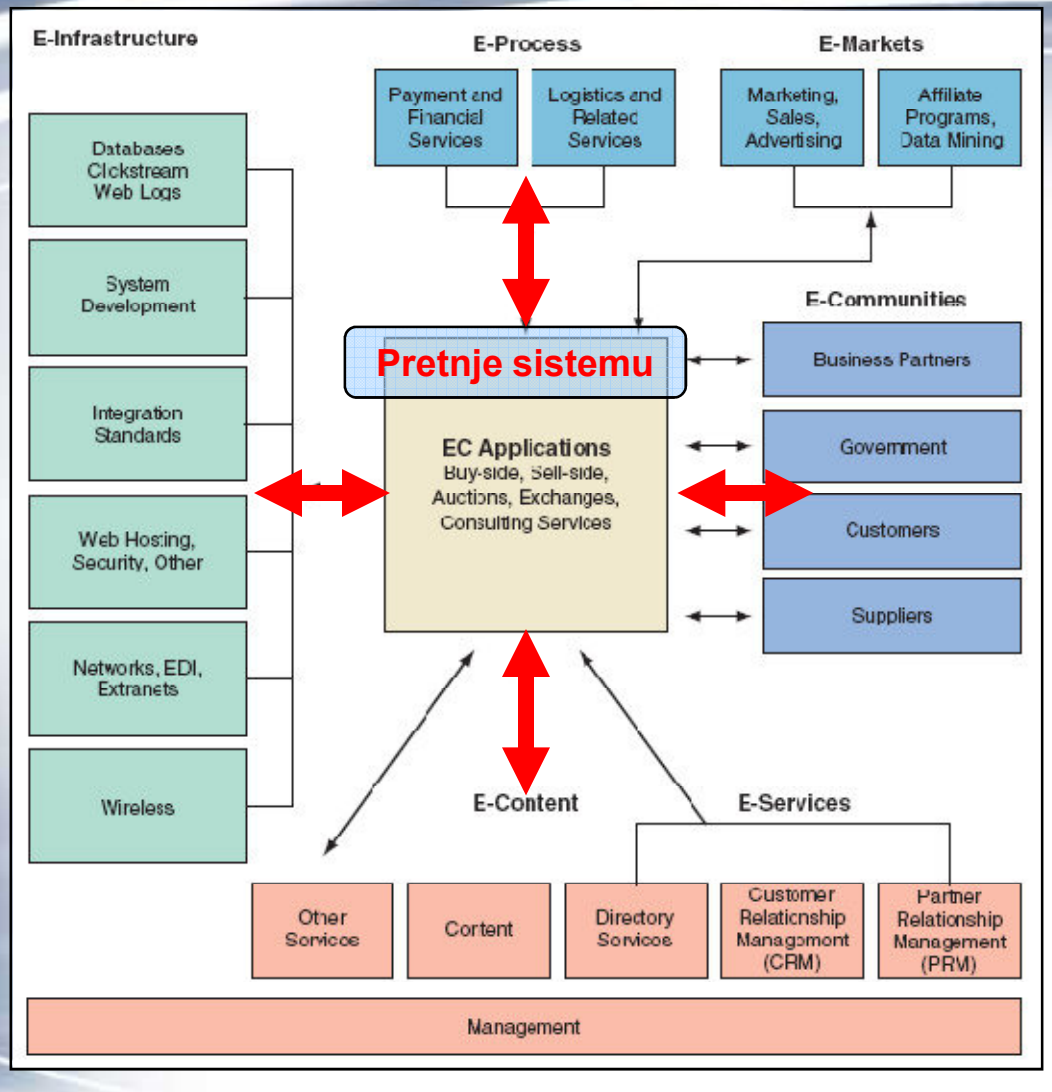
1. **autentifikacija,**
2. **privatnost,**
3. **integritet podataka,**
4. **servis kontrole pristupa,**
5. **servis za onemogućavanje poricanja transakcije**
6. **raspoloživost resursa;**

- mehanizmi zaštite: kriptografija, digitalni potpis, infrastruktura javnih ključeva, sigurnosni protokoli;
- simetrični i asimetrični šifarski sistemi;
- tehnologija digitalnog potpisa;
- vrste certifikata i komponente infrastrukture javnih ključeva;
- funkcionisanje SSL protokola i ostalih mehanizama zaštite;
- sagledavanje sigurnosti postupka zaštite.

Zaštita podataka u e-poslovanju

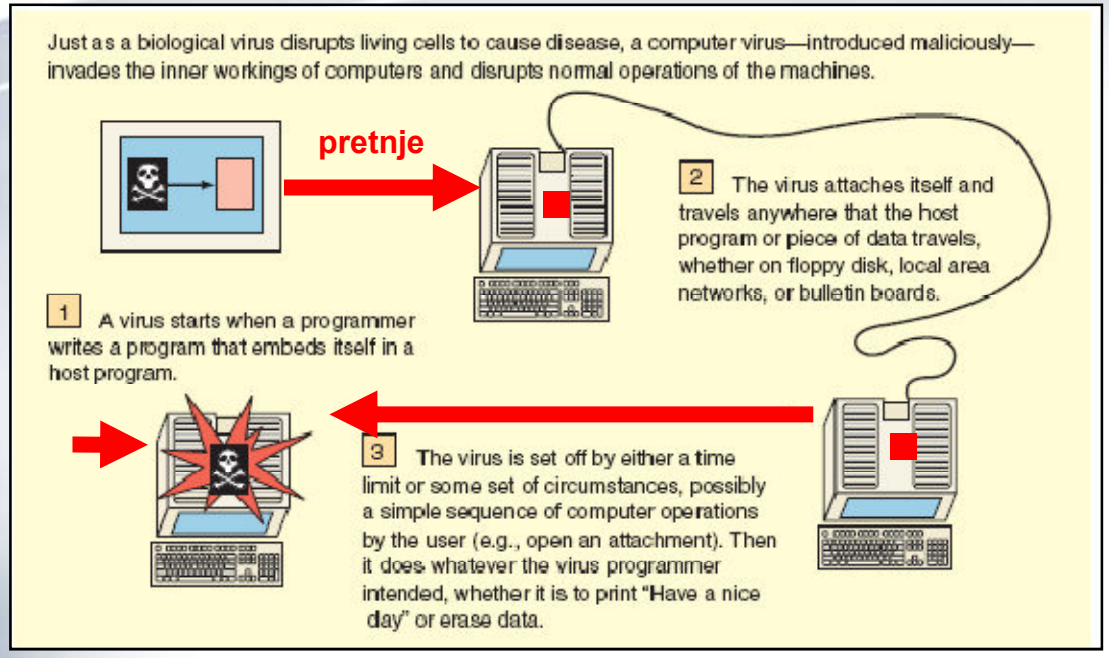
1. Uvod
2. Pretnje sistemu
3. Mere bezbednosti
4. Osnove kriptografije i kriptografske tehnologije
5. Infrastruktura javnih ključeva
6. Sigurnosni protokoli
7. Sigurnost postupka za zaštitu

Bezbednost e-poslovanja



Izvor:Information Technology For Management 6th Edition
Turban, Leidner, McLean, Wetherbe
Lecture Slides by L. Beaubien, Providence College

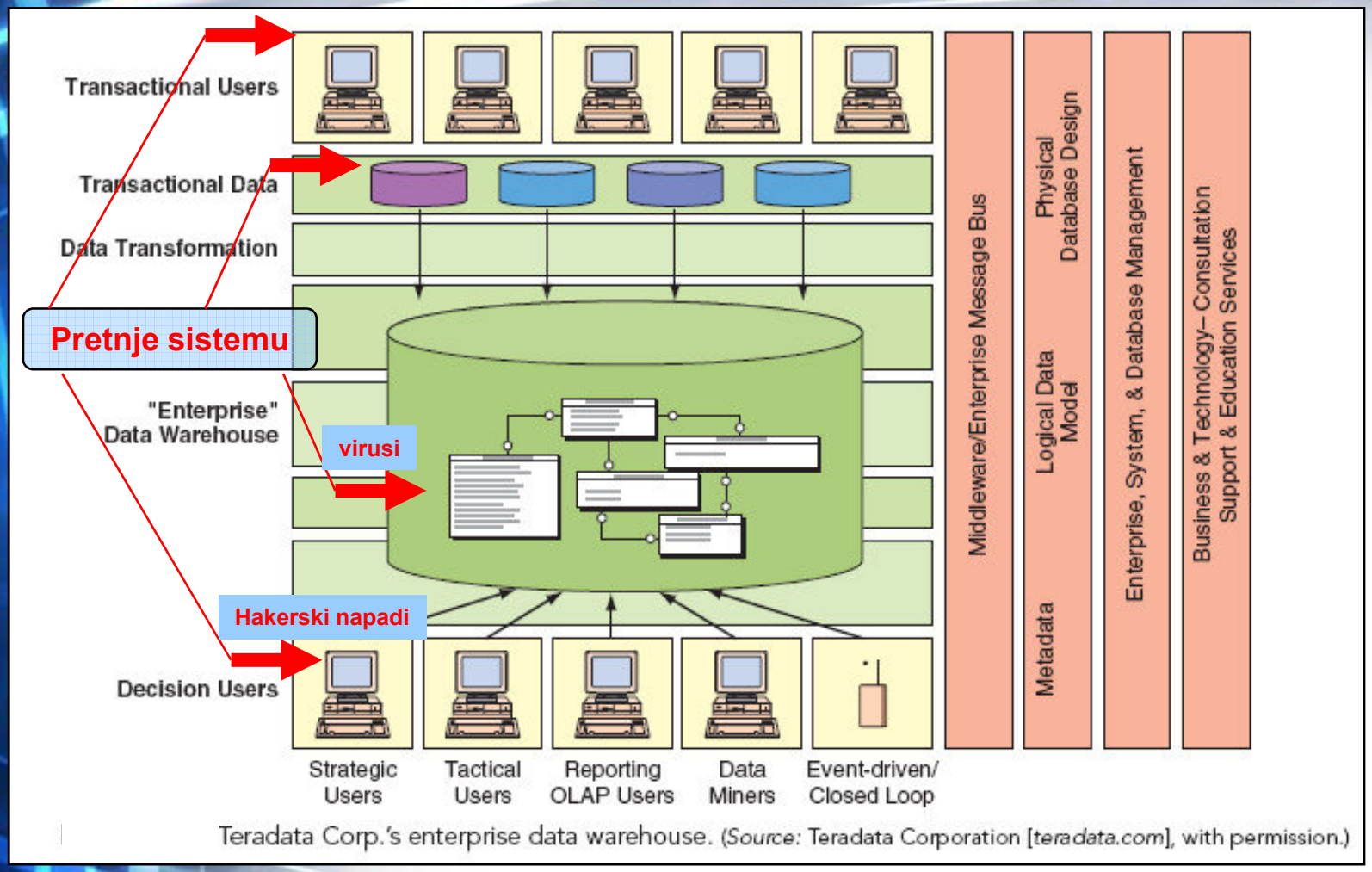
kako virusi rade



Izvor:Information Technology For Management 6th Edition
Turban, Leidner, McLean, Wetherbe
Lecture Slides by L. Beaubien, Providence College

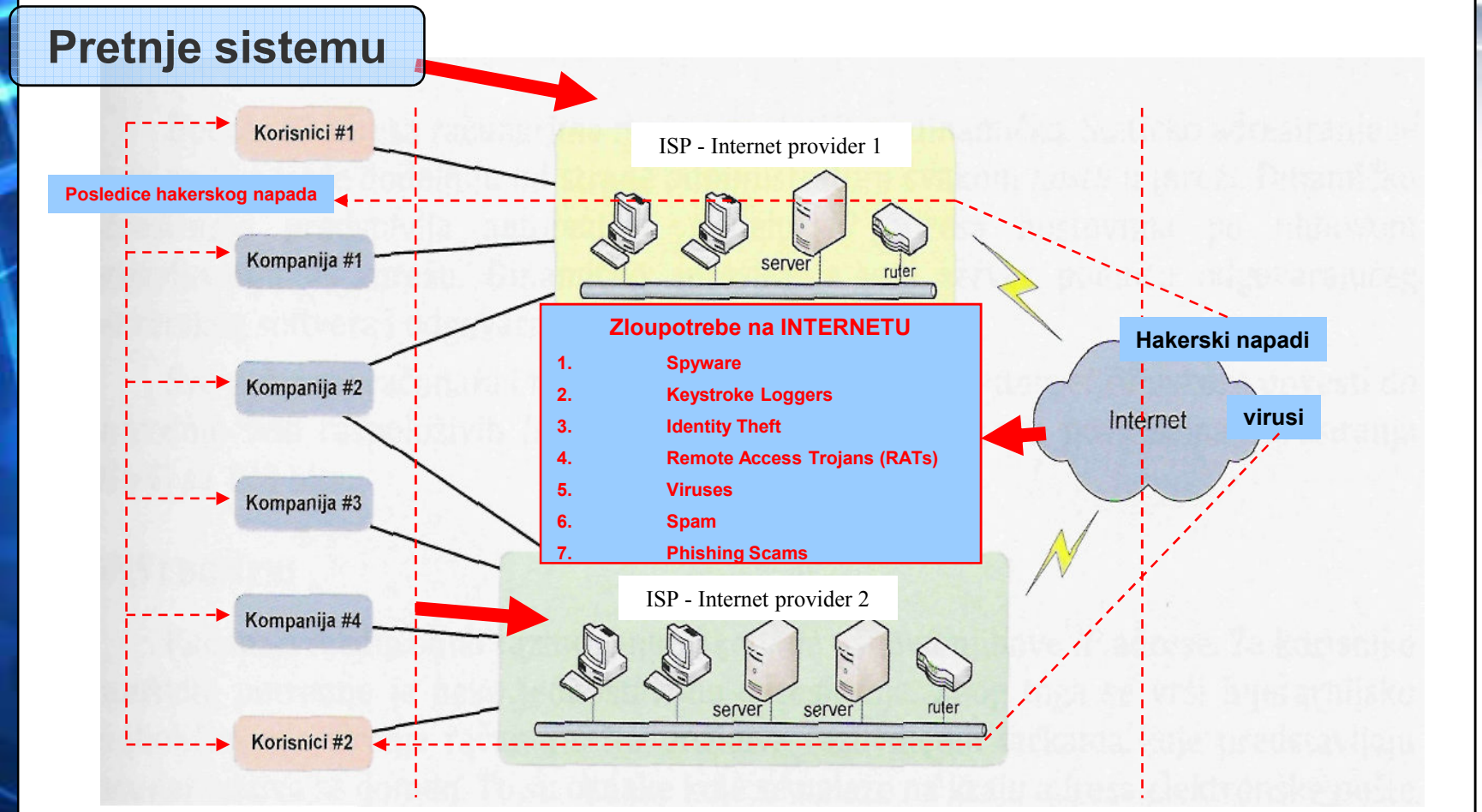
Web-based Data Management Systems

pretnje sistemu



Teradata Corp.'s enterprise data warehouse. (*Source:* Teradata Corporation [*teradata.com*], with permission.)

Pretnje sistemu: hakerski napadi i virusi



Izvor: Rankov, 2009

procenat povećanja i zastupljenost vrsta zloupotreba

	procenat povećanja zloupotreba	u mil £	u mil£	
rb	vrsta zloupotrebe	2003	2004	2003/2004
1	Pard skimming i klonirane kartice	110.6	129.7	17%
2	Izgubljene i ukradene kartice	112.4	114.4	2%
3	Pard-not-present zloupotrebe	122.1	150.8	24%
4	"Presretanje" kreditnih kartica	45.1	72.9	62%
5	Triangulacija	30.2	36.9	22%
	Ukupno	420.4	504.8	

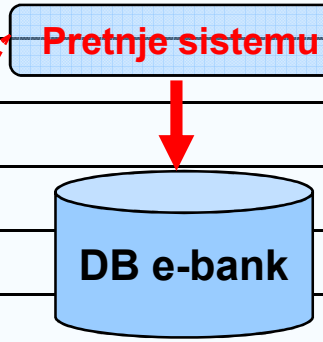
Izvor: www.crimereduction.gov.uk/sta_index.htm

	Zastupljenost pojedinih vrsta zloupotreba u SAD	
rb	vrsta zloupotrebe	%
1	Izgubljene i ukradene kartice	48%
2	Pard skimming i klonirane kartice	26%
3	Triangulacija	15%
4	"Presretanje" kreditnih kartica	6%
5	Ostale zloupotrebe	5%

INTEGRALNO UPRAVLJANJE e-banking sistemom

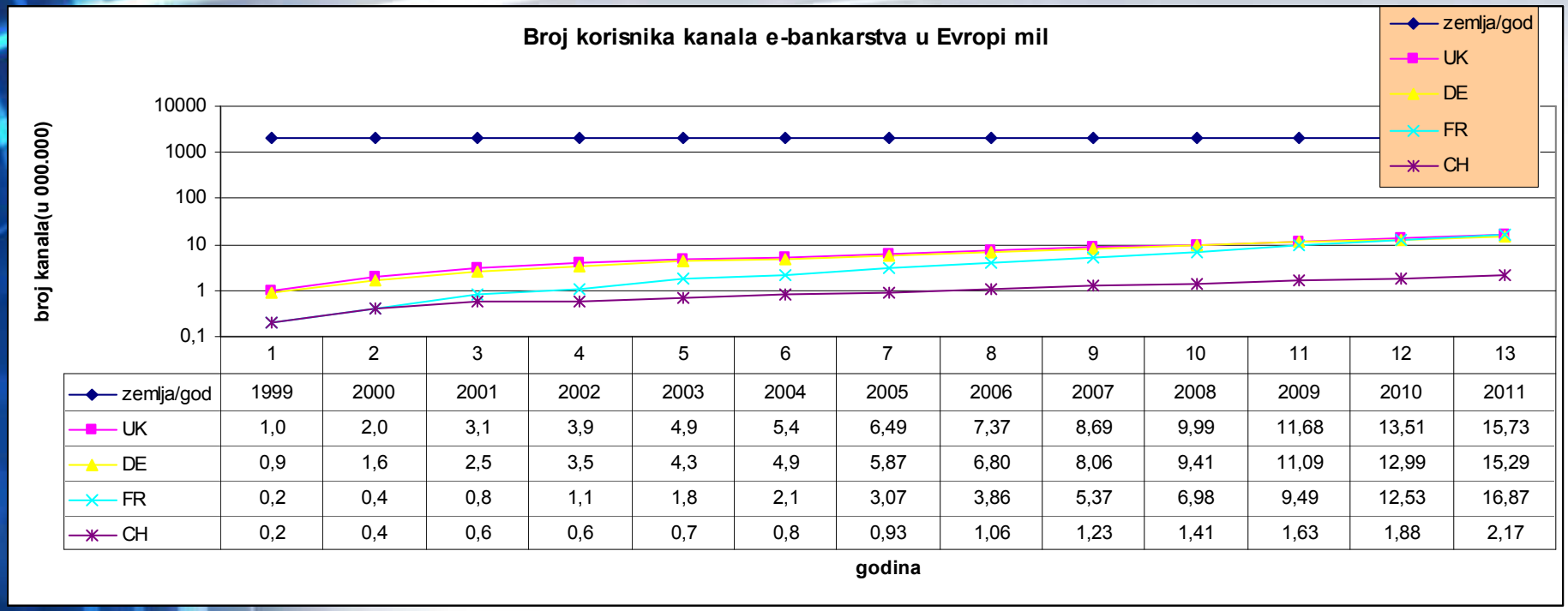
osnova za upravljanje bezbednošću e-banking sistema

	e-bank plaćanja i broj transakcija	% promena
1	Broj računa u u dom PS – platnom sistemu	3,75
2	Broj aktivnih računa u PS	4,86
3	Broj neaktivnih klijentskih računa	-0,23
4	Broj aktivnih klijentskih računa	18,25
5	Ukup. broj klijentskih računa u e-banking sistemu	11,68
6	% aktivnih klijentskih računa	12,82
7	% e-banking računa	7,61
8	Broj transakcija u dom PS	**24,56**
9	Broj naloga za plaćanje u e-banking 1	51,25
10	Broj naloga za plaćanje u e-banking 2	52,6
11	Ukupan broj naloga za plaćanje u e-banking	51,27
12	% e-banking platnih naloga	**21,46**
13	Broj EFT-(Elektronski Prenosi Sredstava) u PS	**27,45**
14	Ukupan broj e-bank platnih naloga u PS	**51,27**
15	% e-banking platnih naloga	18,7
16	iznos e-banking udela u profitu banke(e-banking margin)	54,84



Izvor: Rankov, 2009

ELEKTRONSKO POSLOVANJE



	1	2	3	4	5	6	7	8	9	10	11	12	13
zemlja/god	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
UK	1,0	2,0	3,1	3,9	4,9	5,4	6,49	7,37	8,69	9,99	11,68	13,51	15,73
DE	0,9	1,6	2,5	3,5	4,3	4,9	5,87	6,80	8,06	9,41	11,09	12,99	15,29
FR	0,2	0,4	0,8	1,1	1,8	2,1	3,07	3,86	5,37	6,98	9,49	12,53	16,87
CH	0,2	0,4	0,6	0,6	0,7	0,8	0,93	1,06	1,23	1,41	1,63	1,88	2,17

Ekonomske posledice otkaza

- **Direktni finansijski gubici kao posledica prevare** Zlonamerna osoba može, npr., da prebaci izvesnu količinu novca sa jednog računa na drugi ili može da obriše podatke finansijske prirode.

- **Gubljenje vrednih i poverljivih informacija** Mnoga preduzeća memorišu i šalju informacije tehnološke prirode ili podatke o svojim kupcima i dobavljačima, čija poverljivost je od najveće važnosti za njihovo postojanje. Ilegalan pristup takvim informacijama može prouzrokovati značajne finansijske gubitke ili štete druge vrste takvoj organizaciji.

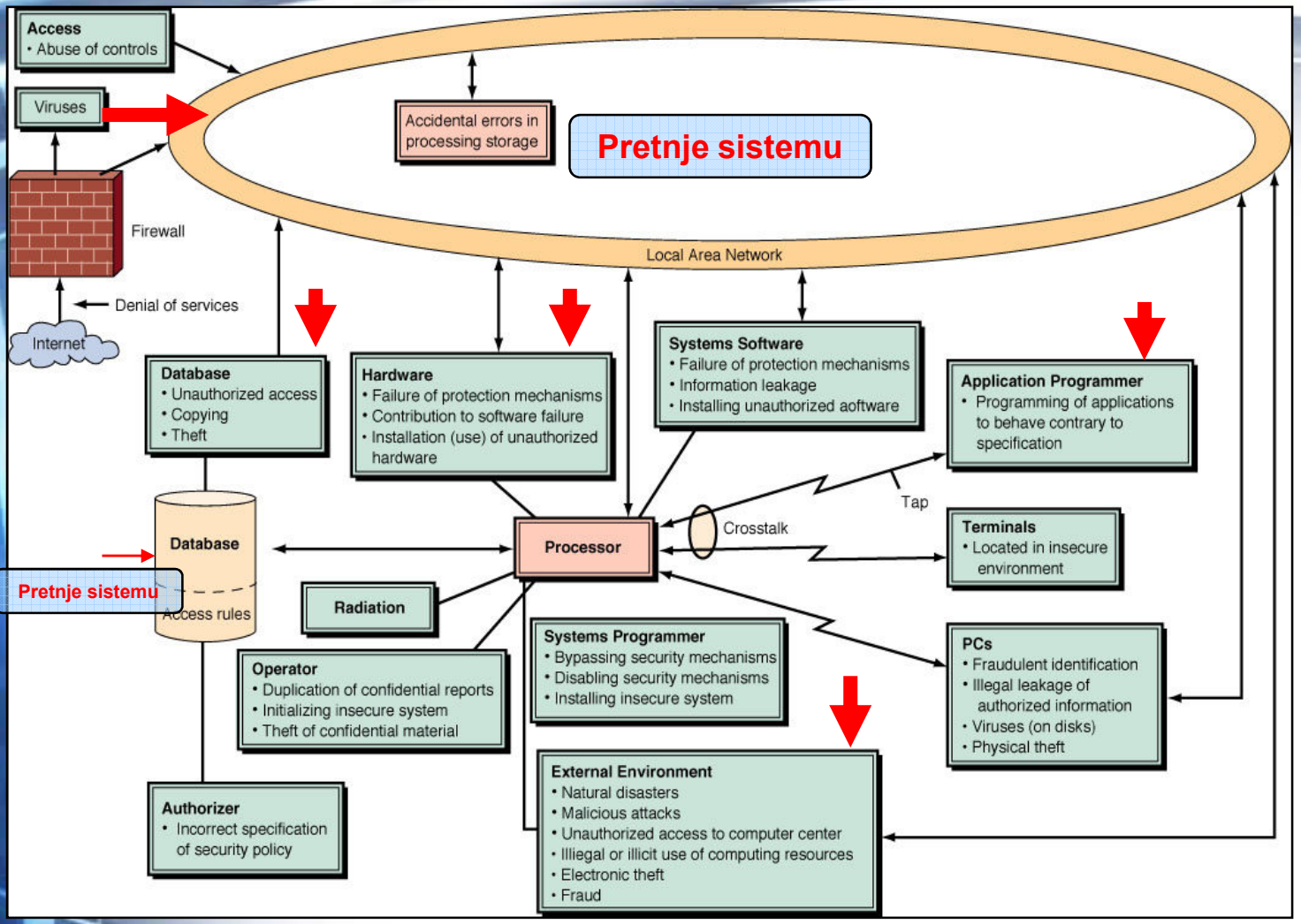
- **Gubljenje poslova zbog nedostupnosti servisa** E-servisi mogu biti nedostupni u dužem vremenskom periodu ili u periodu značajnom za obavljanje konkretnog posla, zbog napada na sistem od strane zlonamernih osoba ili zbog slučajnih otkaza sistema.

- **Neovlašćena upotreba resursa** Napadač koji ne pripada organizaciji koju napada može neovlašćeno pristupiti nekim resursima njenog računarskog sistema i upotrebiti ih radi pribavljanja imovinske koristi.

Ekonomske posledice otkaza ili zloupotrebe Internet tehnologije (nastavak)

- **Gubljenje poslovnog ugleda i poverenja klijenata** Preduzeće može pretrpeti značajne gubitke zbog lošeg iskustva svojih klijenata ili zbog negativnog publiciteta koji mogu biti posledica napada na njegov servis e-trgovine, ili ponašanja zlonamerne osobe koja se predstavlja kao pripadnik tog preduzeća.
- **Troškovi izazvani neizvesnim uslovima poslovanja** Česti prekidi funkcionisanja servisa, izazvani napadima spolja ili iznutra, greškama i sl. mogu paralisati izvršenje poslovnih transakcija u značajnom vremenskom periodu. Npr., potvrde transakcija koje ne mogu da se prenesu komunikacionim kanalima, transakcije koje mogu biti blokirane od strane trećih lica itd. Finansijski gubici koje ovakvi uslovi poslovanja mogu izazvati mogu biti značajni.

Pretnje bezbednosti



Izvor:Information Technology For Management 6th Edition
Turban, Leidner, McLean, Wetherbe, 2003, str.669

Potencijalne pretnje

- **Infiltracija u sistem** – Neovlašćena osoba pristupa sistemu i u stanju je da:
  1. **modifikuje datoteke,**
  2. **otkriva poverljive informacije**
  3. **koristi resurse sistema na nelegitiman način**

U opštem slučaju, infiltracija se realizuje tako što se napadač predstavlja kao ovlašćeni korisnik ili korišćenjem slabosti sistema (npr. mogućnost izbegavanja provera identiteta i sl.). Informaciju neophodnu za infiltraciju, napadač dobija koristeći neku drugu vrstu napada. Primeri takvih napada su "dumpster diving attack", kod koga napadač dobija potrebnu informaciju pretražujući korpu za otpatke svoje žrtve, i "socijalni inženjering" kod koga napadač dobija neophodnu informaciju primoravajući na neki način (ucena, pretnja i sl.) svoju žrtvu da mu je da.

Potencijalne pretnje (nastavak)

- **Prekoračenje ovlašćenja** Lice ovlašćeno za korišćenje sistema koristi ga na neovlašćeni način. To je tip pretnje koju ostvaruju kako napadači iznutra tako i napadači spolja. Napadači iznutra mogu da zloupotrebljavaju sistem radi sticanja beneficija. Napadači spolja mogu da se infiltriraju u sistem preko računa sa manjim ovlašćenjima i nastaviti sa infiltracijom u sistem koristeći takav pristup radi neovlašćenog proširenja korisničkih prava.

- **Suplantacija** Obično posle uspešno izvršene infiltracije u sistem, napadač ostavlja u njemu neki program koji će mu omogućiti da olakša napade u budućnosti. Jedna od vrsta suplantacije je upotreba **"trojanskog konja"** – to je softver koji se korisniku predstavlja kao normalan, ali koji prilikom izvršenja otkriva poverljive informacije napadaču. Npr., tekst procesor može da kopira sve što ovlašćeni korisnik unese u jednu tajnu datoteku kojoj može da pristupi napadač.

Potencijalne pretnje (nastavak)

- **Prisluškivanje** Napadač može da pristupi poverljivim informacijama (npr. lozinci za pristup sistemu) prostim prisluškivanjem protoka informacija u komunikacionoj mreži. Informacija dobijena na ovaj način može se iskoristiti radi olakšavanja drugih vrsta napada.

- **Promena podataka na komunikacionoj liniji**
  Napadač može da promeni informaciju koja se prenosi kroz komunikacionu mrežu. Npr., on može namerno da menja podatke finansijske prirode za vreme njihovog prenošenja kroz komunikacioni kanal, ili da se predstavi kao ovlašćeni server koji od ovlašćenog korisnika zahteva poverljivu informaciju.

TROJAN virus programi : učitavanje, instalacija, prekid

TROJAN virus program vrši učitavanje fajla iz URL

1

The **Trojan** downloads a file from the URL shown below:

http://***gcdon.com.cn/v.exe**

This file is saved to the Windows temporary directory as shown below:

%Temp%\gbn.exe

Instalacija i kopiranje TROJAN virus programa posle lansiranja

2

Once launched, the **Trojan copies its body to the Windows temporary directory as shown below:**

%Temp%\hbgdown.exe%Temp%\msdtc.exe

In order to ensure the Trojan is launched next time the system is started, it creates a service called **"HTTP SSH":**

[HKLM\SYSTEM\CurrentControlSet\Services\HTTP SSH]"DisplayName" = "HTTP SSH""ErrorControl" = "0""ImagePath" = "%Temp%\msdtc.exe""ObjectName" = "LocalSystem""Start" = "2""Type" = "10"

Korišćenje Task Manager-a za prekid aktivnosti Trojan virus programa

3

Use **Task Manager** to terminate the Trojan process.
Delete the following system registry key:
[HKLM\SYSTEM\CurrentControlSet\Services\HTTP SSH]
Delete the original Trojan file (the location will depend on how the program originally penetrated the victim machine).
Delete the following files:
%Temp%\hbgdown.exe%Temp%\msdtc.exe%Temp%\gbn.exe
Delete all files from %Temporary Internet Files%.
Update your antivirus databases and perform a full scan of the computer (download a trial version of Kaspersky Anti-Virus).

Izvor: http://support.kaspersky.com/faq/?qid=208279351

Trojan-Dropper

Instalacija

The Trojan copies its executable file as follows:

%WinDir%\system\svhost.exe

In order to ensure that the Trojan is launched automatically when the system is rebooted, the Trojan adds a link to its executable file in the system registry:

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"WSVCHO" = "%WinDir%\system\svhost.exe"

Trojan virus progam pokašava da spreči aktiviranje AVP – Anti Virus Programa:

AntiVir
Avast Antivirus
AVG Antivirus
BitDefender
Dr.Web
Kaspersky Antivirus
Nod32
Norman
Authentium Antivirus
Ewido Security Suite
McAfee VirusScan
Panda Antivirus/Firewall
Sophos
Symantec/Norton
PC-cillin Antivirus
F-Secure
Norton Personal Firewall

Izvor: http://support.kaspersky.com/faq/?qid=208279351

Potencijalne pretnje (nastavak)

- **Odbijanje servisa** Zbog čestih zahteva za izvršenje složenih zadataka izdatih od strane neovlašćenih korisnika sistema, servisi sistema mogu postati nedostupni ovlašćenim korisnicima.
- **Poricanje transakcije** Posle izvršene transakcije, jedna od strana može da **poriče da se transakcija dogodila**. Iako ovakav događaj može da nastupi usled greške, on uvek proizvodi konflikte koji se ne mogu lako rešiti.

Rizici i mere bezbednosti

- Zbog navedenih problema, potrošači koji koriste takve servise e-trgovine mogu pretrpeti **direktne ili indirektne finansijske gubitke**.
- **Rizici** koje sa sobom nosi upotreba e-trgovine mogu se izbeći upotrebom odgovarajućih mera bezbednosti.
- **Bezbedna e-trgovina** – e-trgovina kod koje se koriste bezbednosne procedure u skladu sa procenjenim rizicima. Mere bezbednosti mogu biti tehnološke i pravne.
- Tehnološke mere bezbednosti:
  - **autentikacija**
  - **poverljivost**
  - **integritet podataka**
- Pravne mere bezbednosti

Ciljevi mera bezbednosti u IS

- **Poverljivost** – obezbeđuje nedostupnost informacija neovlašćenim licima.
- **Integritet** – obezbeđuje konzistentnost podataka, sprečavajući neovlašćeno generisanje, promenu i uništenje podataka.
- **Dostupnost** – obezbeđuje da ovlašćeni korisnici uvek mogu da koriste servise i da pristupe informacijama.
- **Upotreba sistema isključivo od strane ovlašćenih korisnika** – obezbeđuje da se resursi sistema ne mogu koristiti od strane neovlašćenih osoba niti na neovlašćen način.

Mere zaštite podrazumevaju:

- **Prevenciju** – preduzimanje preventivnih aktivnosti za zaštitu podataka i računarskih sistema od mogućeg uništenja (kod e-trgovine npr. šifrovanje broja kreditne kartice).
- **Detekciju** – otkrivanje kako je narušena zaštita, kada je narušena i ko je narušio (kod e-trgovine npr. listing svih transakcija u toku meseca urađenih datom kreditnom karticom).
- **Reakciju** – preduzimanje aktivnosti koje dovode do restauracije podataka ili do restauracije računarskog sistema (kod e-trgovine npr. blokiranje stare kartice i podnošenje zahteva za izdavanje nove).

Bezbednost

- Glavne naučne discipline čiji rezultati se koriste da bi se ostvarili pomenuti ciljevi su:
  - **nauka o bezbednosti komunikacija** označava zaštitu informacija u toku prenosa iz jednog sistema u drugi.
  - **nauka o bezbednosti u računarima** označava zaštitu informacija unutar računara ili sistema – ona obuhvata bezbednost operativnog sistema i softvera za manipulaciju bazama podataka.

Bezbednosni servisi

- Skup pravila koja se odnose na sve aktivnosti organizacije u vezi sa bezbednošću - **politika bezbednosti.**
- Bezbednosni servisi - delovi sistema koji realizuju aktivnosti koje pariraju bezbednosnim pretnjama (obično deluju na zahtev).

Vrste bezbednosnih servisa

- **Autentifikacija -** omogućava utvrđivanje identiteta korisnika:
  - nečim što samo korisnik zna, kao što je lozinka,
  - nečim što samo korisnik ima, kao što je kartica ili obeležje,
  - nečim što samo korisnik jeste, kao što je potpis, glas, otisak prsta, snimak oka, geometrija šake, fotografija lica..., što se sprovodi biometrijskim kontrolnim sredstvima.
- **Privatnost -** sprečava neautorizovani pristup podacima ili presretanje istih tokom komunikacijskog procesa i ostvaruje se enkripcijom podataka.
- **Integritet podataka -** osigurava se izvornost podataka, odnosno sprečavanje promene podataka.
- **Servis kontrole pristupa**
- **Servis za onemogućavanje poricanja transakcije**
- **Servis za onemogućavanje odbijanja usluge**

Pitanja za razmatranje

	DEO V : BEZBEDNOST i ZAŠTITA e-POSLOVANJA
15	**BEZBEDNOSNI ASPEKT e-POSLOVANJA**
139	Objasniti bezbednosni aspekt e-poslovanja
140	Koje su ekonomske posledice zloupotrebe ili otkaza tehnologija u e-poslovanju
141	Koje su opšte pretnje sistemu
142	Koje su osnovni ciljevi mera bezbednosti u informacionom sistemu
143	Objasniti autentifikaciju
144	Objasniti poricanje transakcija

Bezbednosni servisi

- Ispunjenje ovih pretpostavki osigurava se pre svega **kriptografski**, a time se postiže i pravno valjani dokaz o inicijatoru, kao i o samoj transakciji.

- Tehnologije koje su se nametnule kao opšte prihvaćeno rešenje za sigurnost **e-transakcija**, odnosno realizaciju neporecivosti informacija su koncept :
- **Digitalnog potpisa** (digital signature)
- **Public Key Infrastrukture (PKI).**

Podela podataka

- **javni podaci** – podaci u koje svi imaju uvid,
- **autorizovani podaci** – podaci u koje svi imaju uvid, ali su od eksploatacije zaštićeni autorskim pravom,
- **poverljivi podaci** – podaci koji su tajni, ali njihovo postojanje nije,
- **tajni podaci** – podaci kod kojih i njihovo postojanje predstavlja tajnu.

Predmet zaštite moraju biti samo poverljivi i tajni podaci.

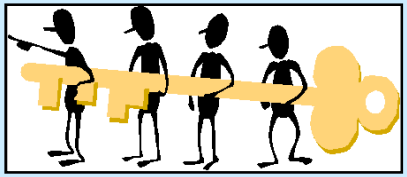
Osobe koje neovlašćeno pristupaju podacima, sa namerom da ih unište ili zloupotrebe, **nazivaju se hakeri. Njihove akcije se smatraju** komjuterskim kriminalom, a njihova motivacija su slava i novac.

Pojam i namena kriptografije

Kriptografija je stručni naziv za proces pretvaranja informacija u gomilu nepovezanih podataka koje niko osim primaoca ne može pročitati.

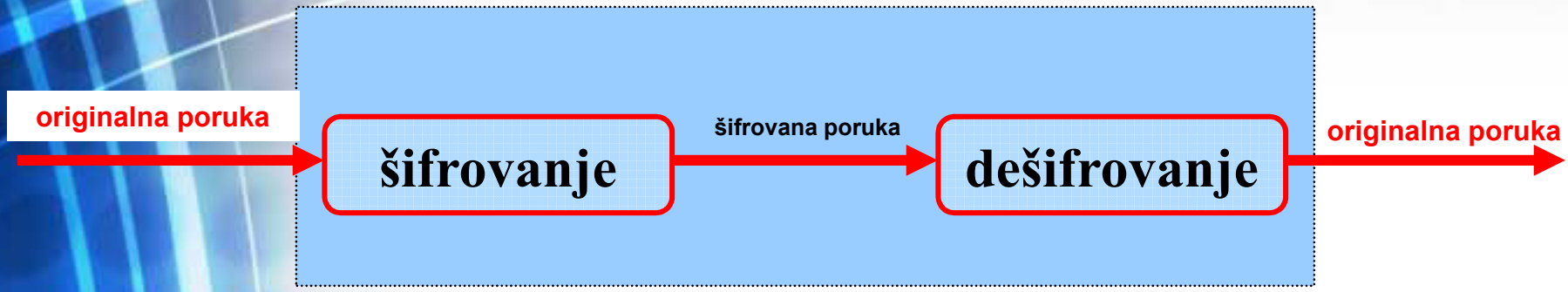
Namena **kriptografije** je da:

- zaštiti memorisanu informaciju bez obzira ako je neko pristupio podacima,
- zaštiti prenetu informaciju bez obzira ako je prenos bio posmatran (“monitoring”).



Šema kriptografskog procesa

Kriptografski proces



Kriptografija uključuje dva postupka:

enkripciju (šifrovanje)

dekripciju (dešifrovanje)

Izvor:Vuković, Ćurčić, 2003
Novaković, 2008

Kriptografija i vrste algoritama

- Osnovni element koji se koristi u kriptografiji naziva se **šifarski sistem** ili **algoritam šifrovanja**.
- Svaki šifarski sistem obuhvata par transformacija podataka, koje se nazivaju:
  - **šifrovanje** i
  - **dešifrovanje**.

Šifrovanje i dešifrovanje

- **Šifrovanje** je procedura koja transformiše originalnu informaciju (otvoreni tekst) u šifrovane podatke (šifrat).
- **Dešifrovanje** rekonstruiše originalni tekst na osnovu šifrata.
- U šifarskoj transformaciji, pored otvorenog teksta, takođe se koristi jedna nezavisna vrednost koja se naziva **ključ** šifrovanja.
- **Šema šifrovanja ima 5 komponenti**:

1. **Tekst** koji se šifruje
2. **Algoritam šifrovanja**
3. **Tajni ključ**
4. **Šifrovani tekst**
5. **Algoritam dešifrovanja**

Kriptografski algoritmi

- **Kriptografski algoritmi** zasnovani su na **matematičkoj funkciji** koja se koristi za šifrovanje i dešifrovanje.
- Razlikuju se dve vrste algoritama:
  - **Ograničeni algoritmi**: bezbednost se zasniva na tajnosti algoritma (istorijski interesantni).
  - **Algoritmi zasnovani na ključu**: bezbednost se zasniva na ključevima, a ne na detaljima algoritma koji se može publikovati i analizirati (algoritam je javno poznat, a ključ se čuva tajnim).

Šifrovanje

- **Šifrovanje** je, pojednostavljeno, matematičkom funkcijom čiji izlaz zavisi od dva ulazna parametra:

  - originalna poruka koja se šifrira,

  - ključ.

  Rezultat je niz naizgled nepovezanih brojeva koji se mogu, bez straha od mogućnosti da poruka dođe u neželjene ruke, prenositi do osobe kojoj je namenjena.

Dešifrovanje

- Da bi šifrovanu poruku druga osoba mogla da koristi potrebno je sprovesti obrnuti postupak od šifrovanja, dešifrovanje.
- **Dešifrovanje** je, pojednostavljeno, matematičkom funkcijom čiji izlaz zavisi od dva ulazna parametra:
  - **šifrovana poruka,**
  - **ključ K^{-l},**
- kao rezultat funkcije dobija se originalna poruka.

Ključevi K i K^{-l}

- Minimalna i potrebna informacija koju dve osobe moraju da dele, ako žele da razmenjuju podatke na siguran način, **skup ključeva** **(K, K^{-l})**.
- Prema odnosu ključeva K i K^{-l} kriptografske sisteme delimo na:
  - **simetrične** i
  - **asimetrične**.

Sigurnost kriptovanog algoritma

- **Vreme potrebno za "razbijanje" algoritma mora da bude duže od vremena u kome podaci moraju da ostanu tajni.**
- Takođe, potrebno je da bude zadovoljen i uslov da **broj podataka šifrovanih jednim ključem bude manji od broja potrebnih podataka da se dati algoritam "razbije".**

Simetrično šifrovanje

- **Simetrično šifrovanje** je šifrovanje tajnim ključem, pri čemu je ključ za šifrovanje identičan ključu za dešifrovanje:

$$K = K^{-1}$$

- u slučaju simetričnog šifrovanja pošiljalac i primalac poruke koriste isti tajni ključ.

- Ključ mora da se drži u tajnosti, što znači da pošiljalac i primalac poruke moraju pre slanja poruke da se dogovore o ključu ili da postoji centar za distribuciju ključeva koji ih distribuira korisnicima šifarskog sistema putem sigurnog kanala.

Poznati simetrični algoritmi

- **DES (Data Encryption Standard)** – ključ je dužine 56 bita.
- **Triple DES, DESX, GDES, RDES** – ključ je dužine 168 bita.
- **(Rivest) RC2, RC4, RC5, RC6** – promenljiva dužina ključa do 2048 bita.
- **IDEA – osnovni algoritam za PGP** – ključ je dužine 128 bita.
- **Blowfish** – promenljiva dužina ključa do 448 bita.
- **AES (Advanced Encryption Standard)** - radi sa blokovima od po 128 bita i koristi ključeve dužine 128, 192 i 256 bita.

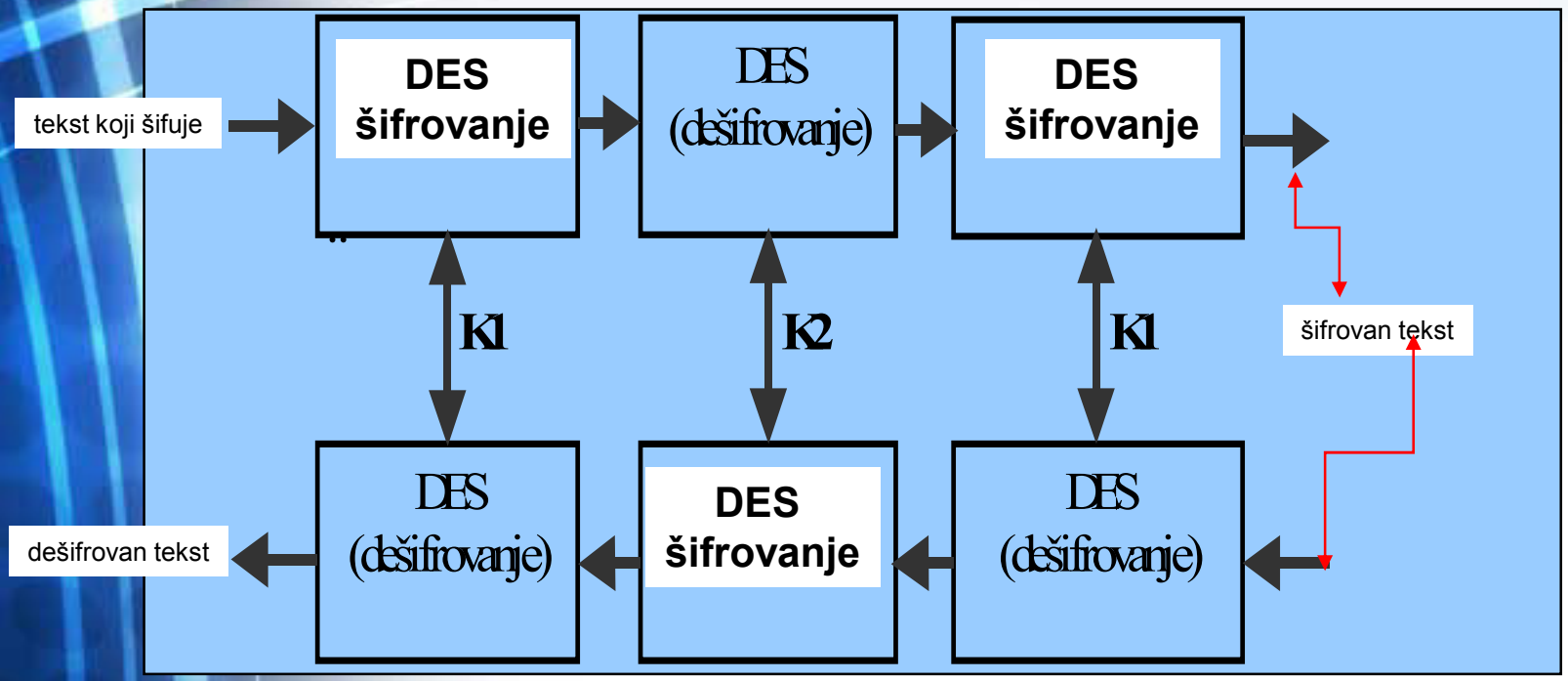
DES

- **DES** je simetričan algoritam koji je **IBM** predstavio 1975.
- Razvijan je od strane brojnih organizacija za kriptovanje poruka i podataka pa je postao najrasprostranjeniji komercijalni algoritam.
- DES je blok šifra što znači da algoritam kriptuje podatke u 64-bitna bloka i koristi 64-bitni ključ.
- U realnosti, samo 56 bitova se koristi za kriptovanje/dekriptovanje podataka gde preostalih 8 bitova rade kao analogni.
- Upotreba 56 bita omogućava veliki prostor za ključ.
- 2^{56} potencijalnih mogućnosti za ključ, čine razbijanje ovog koda teškim kada su u pitanju brutalni napadi.

Triple DES algoritam

- U poslednjih nekoliko godina zabeležen je veliki broj probijanja **DES algoritma** razbijanjem ključa za kriptovanje. Vlada SAD ne priznaje više DES kao standard, pa su mnoge organizacije prešle na **Triple DES algoritam**.
- Tripl DES koristi tri ključa za kriptovanje podataka, što povećava veličinu ključa na 168 bita. Postoji više metoda Triple DES algoritma:
  - **Prvi metod**: podaci se kriptuju tri puta sa tri odvojena ključa.
  - **Drugi metod**: podaci se kriptuju sa prvim ključem, dekriptuju sa drugim, i ponovo se kriptuje trećim ključem.
  - **Treći metod**: sličan je sa prethodna dva, sa tim što se isti ključ koristi u prvoj i trećoj operaciji.
- Vlada SAD razvija različite algoritme koji će postati **AES** (Advanced Encryption Standard) standardi.

Tripl DES



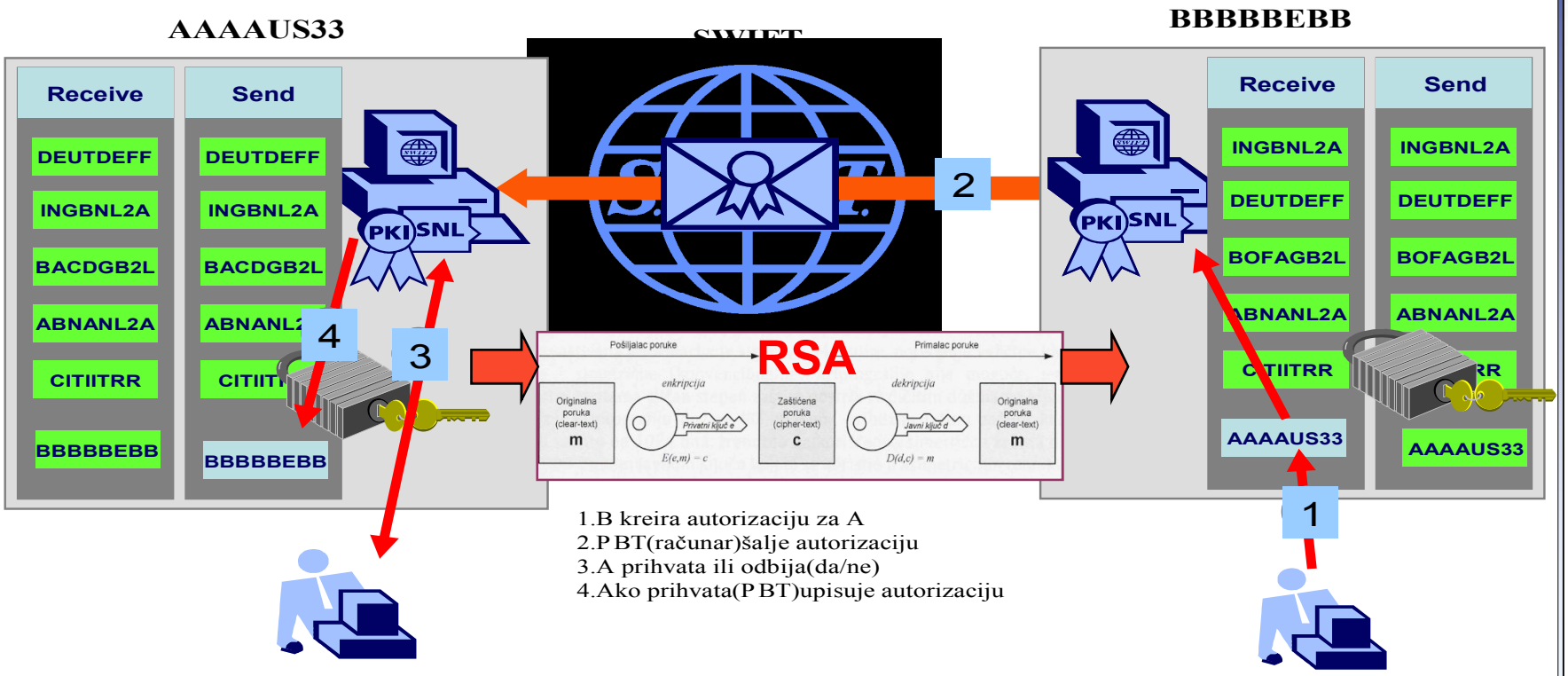
Izvor:Vuković, Ćurčić, 2003
Novaković, 2008

Asimetrično šifrovanje

- Asimetrično šifrovanje je **šifrovanje javnim ključem**.
- Svaki učesnik u komunikaciji koristi **dva ključa**.
- Jedan ključ je **javni** **i koristi se za šifrovanje**, dok je **drugi** **tajni** **i koristi se za dešifrovanje**.
- **Tajni ključ je dostupan samo vlasniku.**
- Oba ključa su vezana za entitet (računar ili korisnika) koji treba da:
  - dokaže svoj identitet,
  - elektronski potpiše ili
  - šifruje podatke.
- Svrha javnog ključa je da bude svima dostupan.
- Kad šaljemo podatke nekoj osobi, šifrujemo ih javnim ključem.
- Kada osoba primi podatke, dešifruje ih svojim privatnim ključem, koji samo ta osoba poseduje.

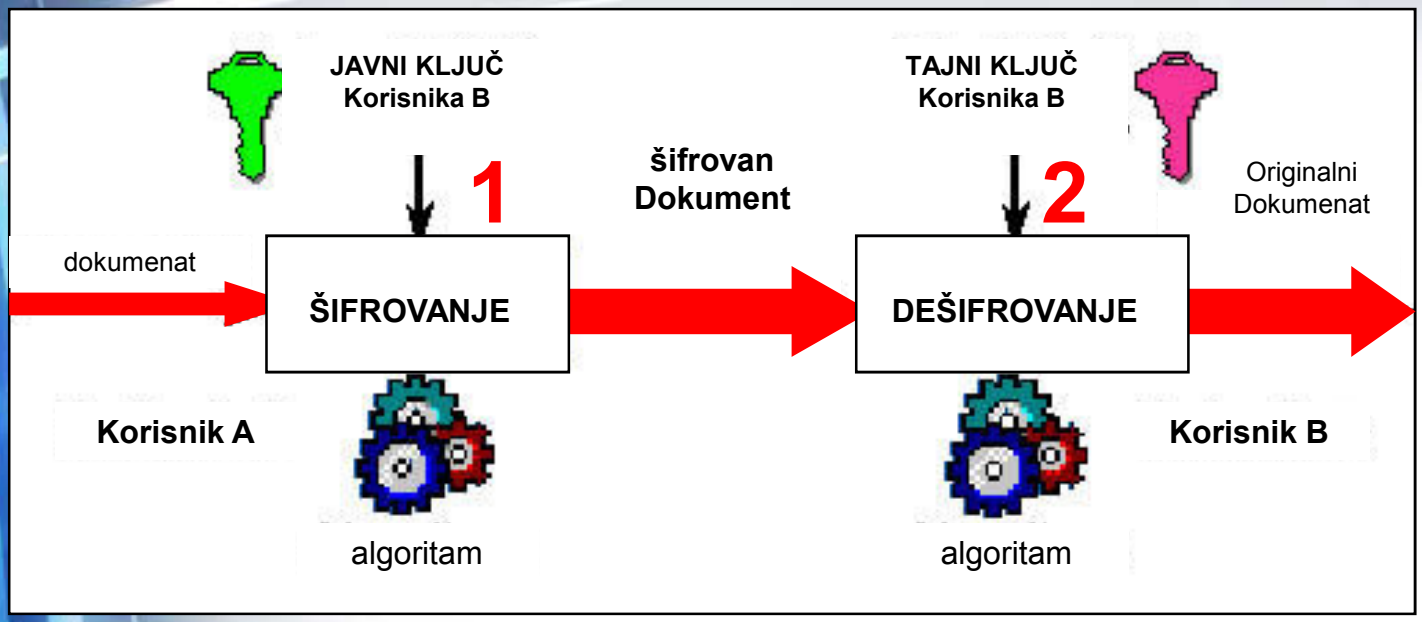
Tehnologija razmene i kontrole ključeva – PKI

PKI – Public Key Infrastucture *(javna infrasturktura za razmenu ključeva)*



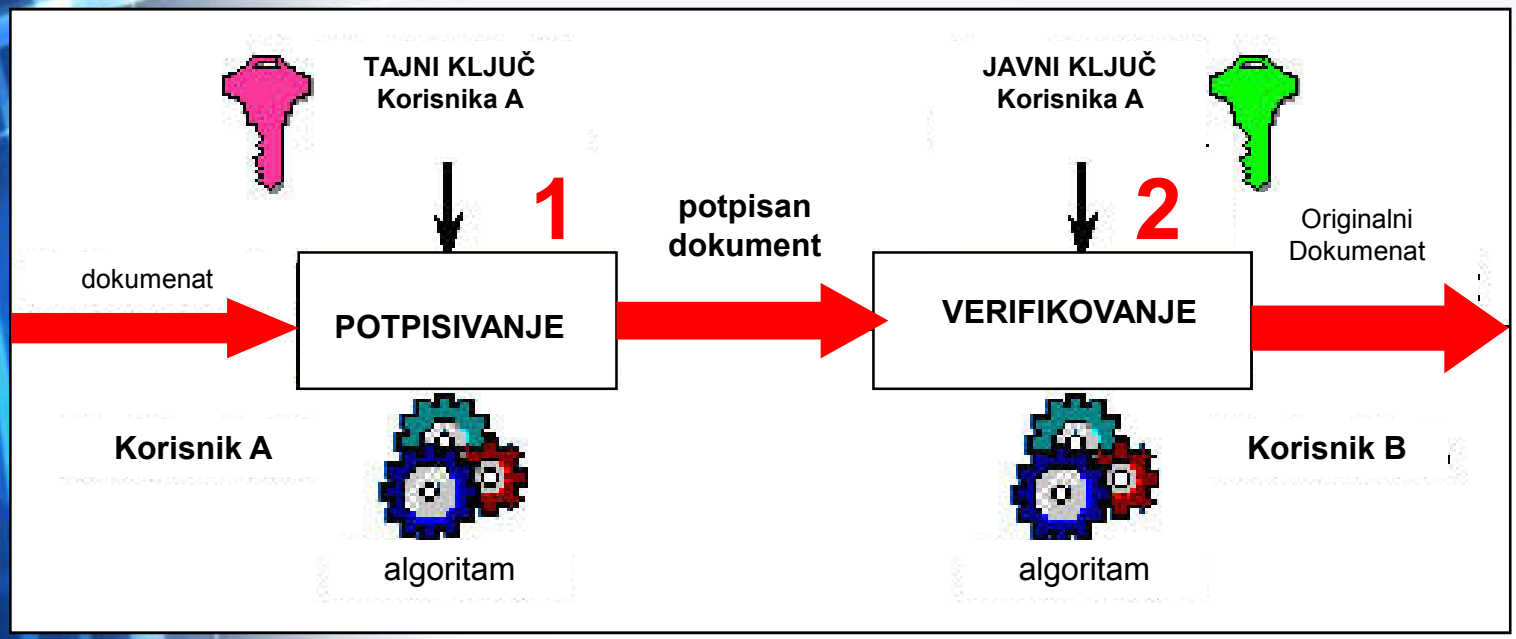
Izvor:swift.com, prezentacija regionalnog direktora u Srbiji 2006
Rankov, 2009

Prikaz asimetričnog šifrovanja (RSA)



Izvor:Vuković, Ćurčić, 2003
Novaković, 2008
Rankov, 2009

Tehnologija digitalnog potpisa



Izvor:Vuković, Ćurčić, 2003
Novaković, 2008
Rankov, 2009

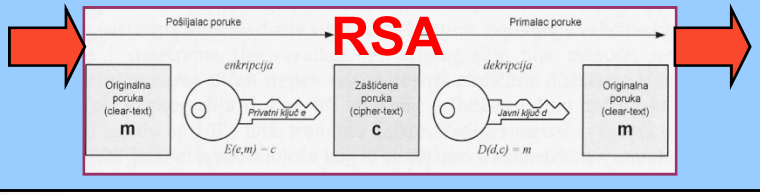
algoritam algoritam

Algoritam za asimetrično šifrovanje

- Kao primer algoritma za asimetrično šifrovanje navodi se

RSA **(Rivest Shamir, Adelman, 1978)**

algoritam sa dužinama ključa od **512** do **1024** bita.



RSA Public Key Standard

- **RSA** Public Key je asimetrični algoritam šifrovanja koji koristi javni i privatni ključ za kriptovanje i dekriptovanje podataka.
- RSA sistem je zasnovan na odgovarajućim matematičkim operacijama razvijen je na pretpostavci da je teško razložiti na činioce velike brojeve koji su proizvod dva prosta broja.
- RSA sistem sa javnim ključem i DES (ili neki drugi sistem sa simetričnim ključem) se obično koriste zajedno.

  Razlog: RSA je relativno spor za kriptovanje velikih blokova podataka, dok je DES pogodan za to.
- Sistemi koriste RSA da bi razmenili DES ključeve međusobno, a zatim koriste DES algoritam da kriptuju blokove podataka. Ovakav protokol prepoznaje dve strane i omogućava sigurnu razmenu ključeva.

RSA Public Key Standard (nastavak)

- RSA sistem javnog ključa se koristi za kriptovanje i digitalni potpis.

KRIPTOVANJE

- **Primer 1**: Petar šalje kriptovanu poruku Ani. Kriptovanje poruke vrši Aninim javnim ključem i emituje poruku. Pošto Ana ima privatan ključ (*odgovarajući Aninom javnom ključu*) dekriptuje podatke i čita poruku. Podaci ostaju poverljivi u toku razmene.

DIGITALNI POTPIS - prepoznaje pošiljaoca poruke.

- **Primer 2**: Da bi se identifikovao, Petar šalje Ani poruku šifriranu svojim tajnim ključem. Kada Ana dobije poruku, dešifruje je upotrebom Petrovog javnog ključa. Uspešno dešifrovanje potvrđuje da je Petar pošiljalac (poruka je šifrirana Petrovim tajnim ključem, koji je u njegovom vlasništvu.

Certifikati

- **Preduslov implementacije public-key kriptografije, odnosno ostvarenje neporecivosti primenom PKI, je jednoznačna veza između javnog ključa i njegovog korisnika.**

- Kao sredstvo ostvarivanja jednoznačne veze između javnog ključa i korisnika pojavljuju se **certifikati**. Postoje dve vrste certifikata:
  - **Soft Certifikati**, na magnetnom mediju, npr. na hard disku računara.
  - **Hard Certifikati**, koji se proizvode na sigurnim hardverskim uređajima npr. pametnim karticama.

PKI

- **Infrastruktura koja osigurava komponente neophodne za administraciju (izdavanje, proveru....) javnih ključeva i certifikata naziva se Public Key Infrastrusture – PKI.**
- **Tri osnovne softverske komponente PKI su:**
  1. **Certificate Authority (CA),**
  2. **Registration Authority (RA),**
  3. **Certificate Repository.**

Certificate Authority (CA)

- **CA** je centralna komponenta PKI sa funkcijama izdavanja, administriranja i revokacije certifikata.
- CA se može realizovati kao in-house rešenje, implementacijom PKI rešenja Baltimorea, Entrusta, Xcerta, i sl., ili kao Third - Party rešenje korišćenjem CA outsourcing servisa ponuđača kao što su Valicert, GlobalTrust ltd.
- CA je odgovoran za proizvodnju certifikata i njihovu valjanost, slično kao što je u stvarnom svetu npr. vozačka dozvola.

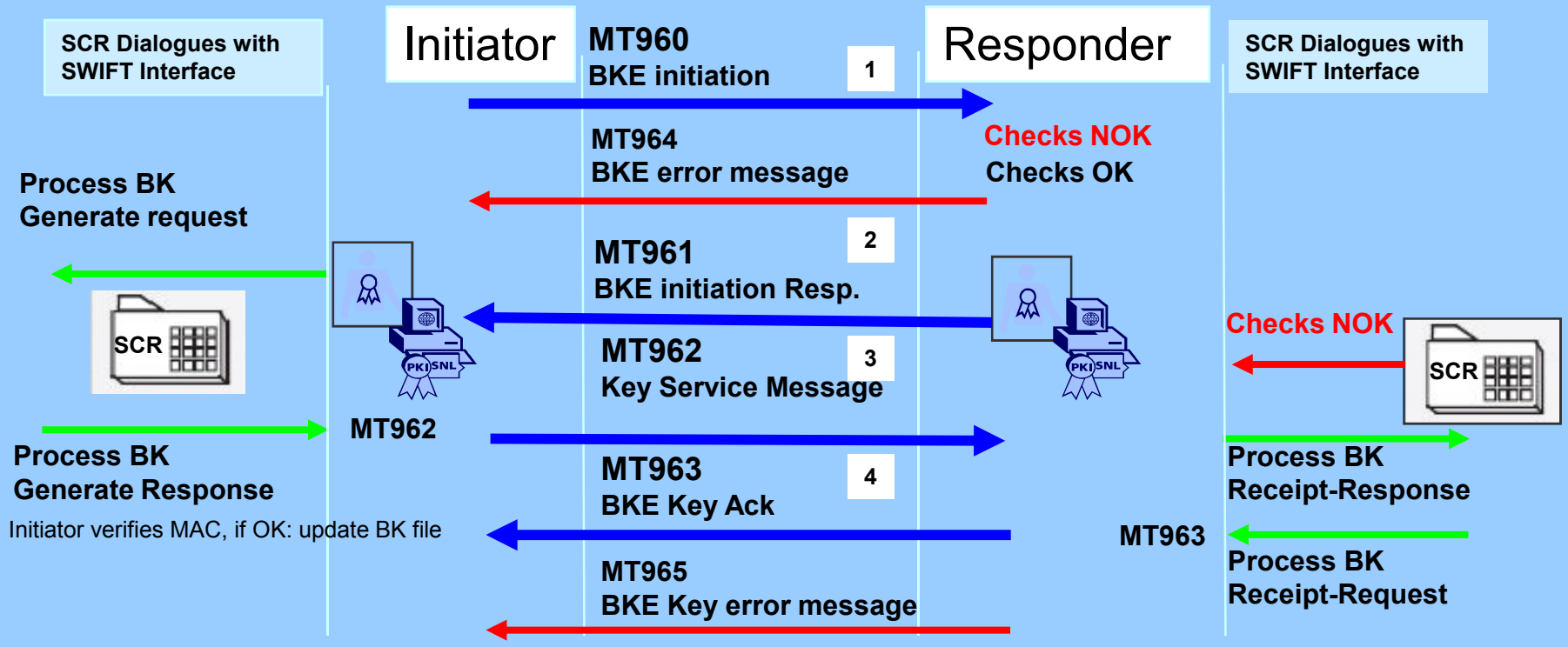
Registration Authority (RA)

- **RA je komponenta PKI koja osigurava proces registracije korisnika, prihvata i obrađuje zahteve za izdavanjem certifikata, i iste prosleđuje CA radi izdavanja certifikata.**
- Koncept RA se implementira sa ciljem realizacije procesa registracije što bližeg korisniku, jer je identifikacija korisnika prilikom registracije ključni korak u izdavanju certifikata.
- Proces registracije predstavlja prvu i najvažniju kariku u realizaciji neporecivosti.
- Ukoliko se certifikat, odnosno Digitalni Identitet izda pogrešnoj osobi, čitav sistem ostvarivanja neporecivosti je kompromitovan.

Certificate Repository

- **U repozitoriju se prave javni ključevi i certifikati korisnika, kao i tzv. revokacijske liste** (**CRL**).
- Pored ove tri ključne komponente PKI obuhvata i brojne druge softverske, hardverske i organizacijske komponente, kao što su razni gateway softverski moduli, Hardware Security Moduli i politike sigurnosti.

Bilateralna razmena ključeva na SWIFT mreži - BKE process flow



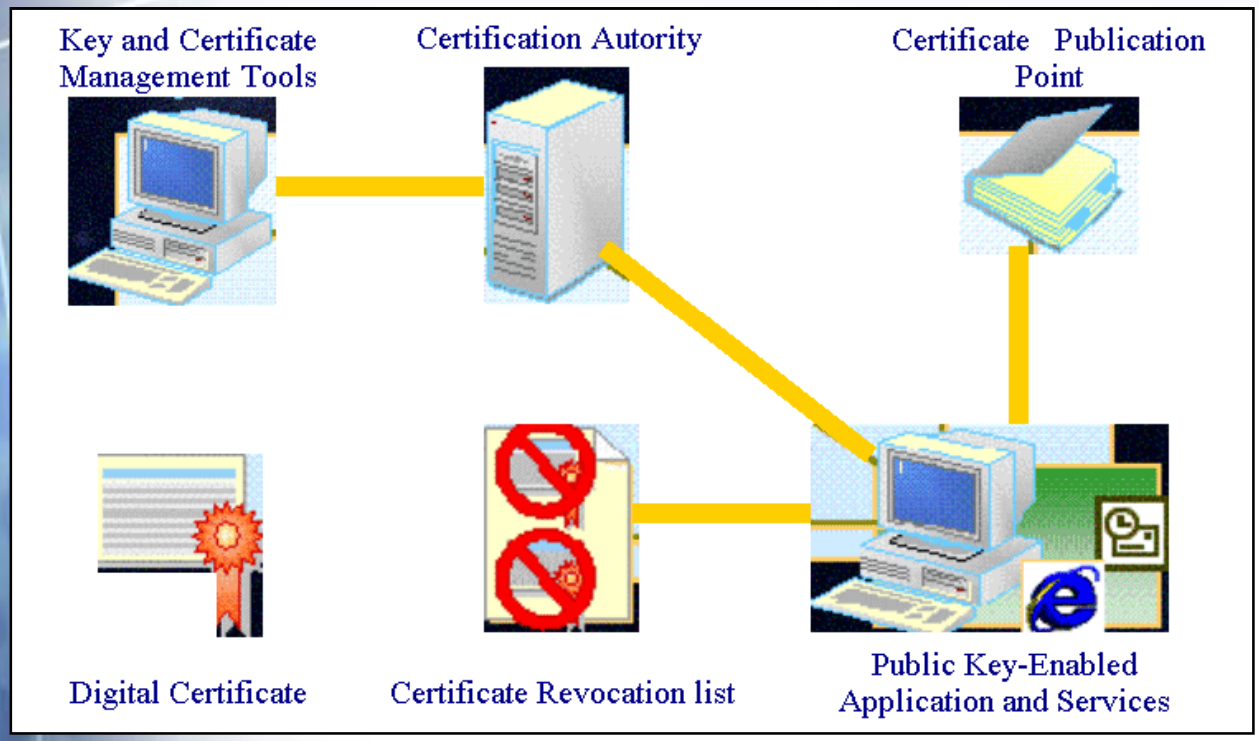
Checks at Initiator's SCR:
- validates responder's CV,
- determines the value of its public key
- creates a new Bilateral key (by using responder's public key
- Signs the result using initiator's Secret key

Checks at responder's SCR:
- determine value of new key,
- verify signature of initiator's enciphered key (via public key of initiator)
-Decipher enciphered key (via public key of initiator)
- new (enciphered) bilateral key is returned to interface and stored on disk

Izvor: Alke De Bour, SWIFT RAM,

Filipović, SWIFT biro, SWIFTNet Phase 2 RMA roadshow **2007**

PKI osigurava funkcionalnosti i servise neophodne za administraciju digitalnih certifikata i enkripcijskih ključeva korisnika, koji koriste PKI za sigurnu e-komunikaciju

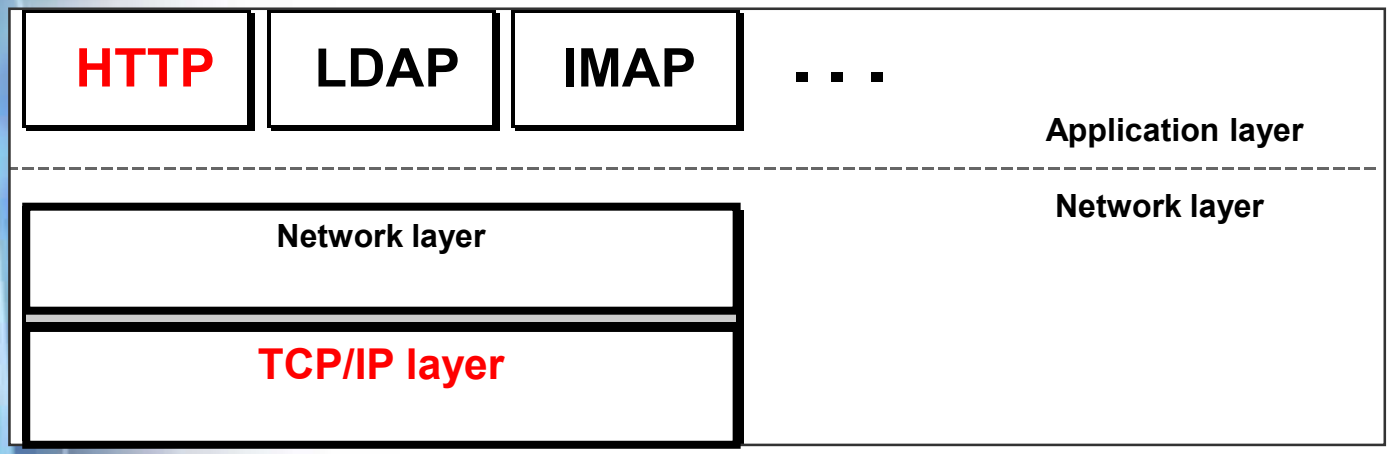


Upotreba SSL protokola

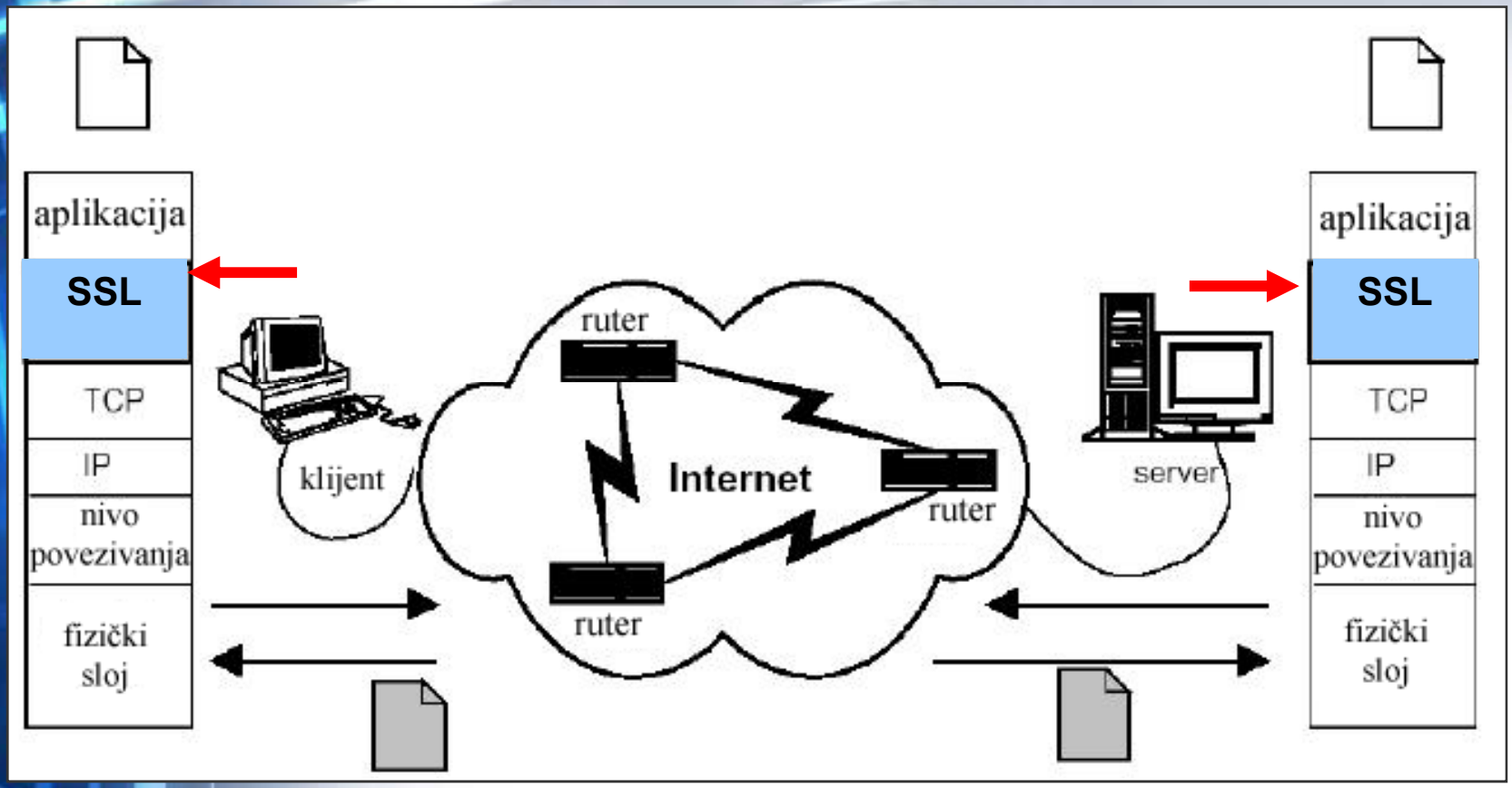
- Upotreba **SSL** protokola je garancija sigurnog i pouzdanog prenosa podataka između dve strane u komunikaciji jer su podaci kriptovani i procesiraju se certifikatima.
- **SSL** je razvijen od strane Netscape Communications Corporation.
- Za kriptovanje podataka SSL najčešće koristi dve dužine ključeva: **40-bitni** i **128 bitni ključ** zavisno od željene zaštite i web browsera koji se koristi.

Prednost SSL protokola

Prednost SSL protokola je što nije vezan za određeni informacioni servis (npr. WWW), već se koristi kao dodatak između pouzdanog prenosnog nivoa (TCP) i aplikacijskog nivoa (HTTP, FTP,...)



Funkcionalni model SSL protokola



Izvor:Sherif, Serhrouchni, Gaid, Farazmandnia, 1998

Svojstva SSL protokola

- **privatnost komunikacije** (za šifrovanje prenošenih podataka koristi se simetrična kriptografija **DES**, **RC4** ...)
- **identitet strana u komunikaciji** (dokazuje se upotrebom asimetrične kriptografije javnog i tajnog ključa **RSA**, **DSS** ...)
- **pouzdanost prenosa podataka** (uključena je provera integriteta podataka korišćenjem sigurnih **HASH** funkcija)

Osnovni ciljevi SSL protokola

- **Kriptografska sigurnost** postiže se upotrebom proverenih algoritama za zaštitu podataka, ali i razvijenim protokolima za njihovu pravilnu upotrebu.
- **Interoperabilnost** garantuje komunikaciju između dve strane (aplikacija) koje koriste različite implementacije SSL protokola (npr. između Netscape korisnika i Internet Explorer korisnika).
- **Proširljivost** omogućuje dodavanje novih načina zaštite podataka u protokol uz istovremeno zadržavanje interoperabilnosti sa starijim verzijama protokola.
- **Relativna delotvornost** odnosi se na opterećenje računara na kojima se SSL koristi. Kriptografski algoritmi su procesorski vrlo zahtevni (zavisno od vrste algoritma), pa je poželjno korišćenje što jednostavnijih algoritama bez smanjenja stepena sigurnosti.

Postupak prenosa podataka

- Postupak prenosa podataka korišćenjem SSL protokola deli se u dva odvojena koraka:
  - **uspostavljanje sigurne veze** (**handshake**),
  - **prenos podataka**.

Kriptografski parametri

U postupku uspostavljanja veze između strana dogovaraju se kriptografski parametri potrebni za uspešno kreiranje sigurnog komunikacijskog kanala.

Osnovni parametri koji se dogovaraju su:

- **verzija protokola**,
- **kriptografski algoritmi koji će biti upotrebljeni** (koje obe strane podržavaju),
- **opciona provera identiteta učesnika u komunikaciji** (međusobna razmena certifikata),
- **generisanje zajedničke tajne**.

Prenošenje podataka sastoji se od:

- **fragmentiranja podataka u pakete fiksne dužine**,
- **kompresije podataka**,
- **zaštite integriteta podataka**,
- **šifrovanja podataka**.

⇨Takvi podaci prosleđuju se nižem nivou prenosa podataka (**TCP**), koji se brine za njihov siguran dolazak na ciljnu **IP adresu i port**.

Ostali mehanizmi zaštite

- **SET** (**Secure Electronics Transaction**) je predloženi sveobuhvatni standard za obradu kreditne kartice;
- **SHTTP** ima za cilj zaštićeni prenos pojedinačnih poruka, dok SSL ima zadatak da ostvari zaštićeni kanal između klijenta i servera. Zbog neuspešnog marketinga koji ga je pratio, ovaj protokol se malo koristi;
- **S-MIME** (Secure-MIME) kao osnovu za proveru ispravnosti i šifrovanje koristi sistem javnih ključeva;
- **PGP** je proizvod koji pruža mogućnost identifikovanja privatnim ključem, proveru integriteta i šifrovanje, ali ne podržava proveru ispravnosti pomoću potvrda;
- **PCT** (Private Communication Technology) je proizvod *Microsoft*-a koji je nastao kao reakcija na SSL protokol verziju 2. Kad se pojavila nova verzija SSL protokola, PCT protokol je prevaziđen i danas se retko koristi.

Asimetrični i simetrični algoritmi

- **Asimetrični algoritmi** koriste autentikaciju strana u komunikaciji i generisanje zajedničkih tajni i ključeva. Upotreba asimetričnih algoritama je minimizirana zbog njihovih velikih zahteva na procesorske resurse (*tipično 100 puta sporiji od simetričnih algoritama*).

- **Simetrični** algoritmi koriste se za šifrovanje podataka u paketima i zaštitu podataka od promene (generisanje potpisanih sažetaka dokumenta jednosmernim HASH funkcijama).

Biometrijske identifikacije

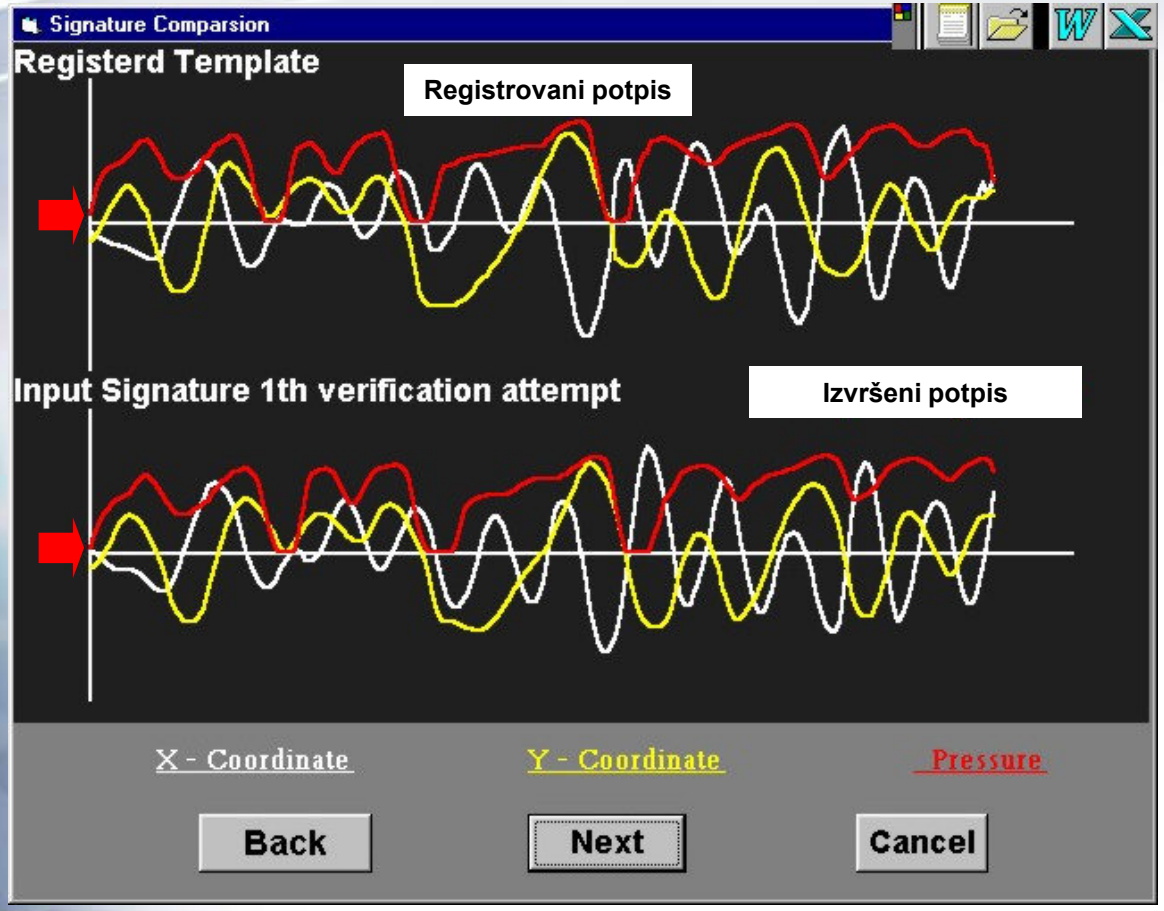
- Zahvaljujući velikoj memoriji inteligentnih kartica postoji i mogućnost da se umesto korišćenja **PIN-a** upotrebe alternativne identifikacione tehnologije.
- Ove alternative poznate su kao **biometričke** jer podrazumevaju merenje nekih karakteristika koje su posebne za svako ljudsko biće.
- **Biometrijske identifikacije** podrazumevaju:
  1. **overu potpisom,**
  2. **otisak prstiju i dlana,**
  3. **geometriju ruke,**
  4. **skeniranje očne mrežnjače,**
  5. **procenu glasovnog zapisa**
  6. **zapis venskog obrasca.**

Overa potpisom

- Postupak provere vizuelnog obrasca potpisa, je izuzetno složen, a ulaganja u tehnologiju za taj nivo provere je preskupo.
- Postoji određeni broj karakteristika individualnog potpisa koje su jedinstvene i koje je moguće na jednostavniji način iskontrolisati. Te karakteristike su vezane za pritisak, relativnu brzinu i druge dinamičke karakteristike u procesu pisanja. Jedan od korišćenih alternativnih pristupa je **Verisign**, koga je razvila Nacionalna fizička laboratorija u Velikoj Britaniji. Procenat grešaka kod ovog pristupa je ispod 1%.

Overa potpisom

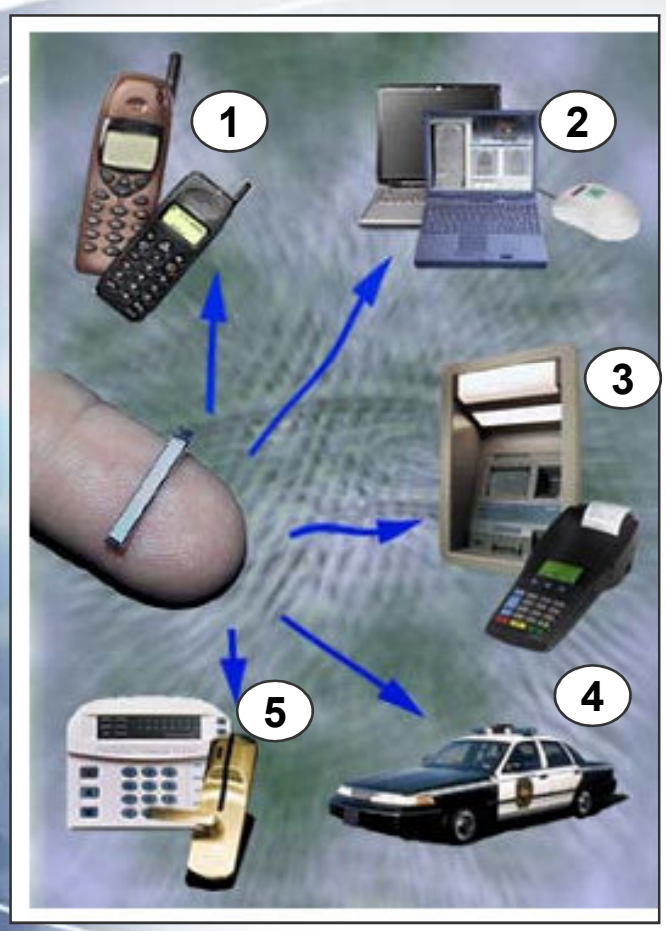
uporedjivanje registrovanog potpisa sa izvršenim potpisom



Upoređivanje otisaka prstiju i dlana

- Identifikacija korisnika se vrši uzimanjem **otiska prsta i podrazumeva upoređenje sa otiskom prsta koji je memorisan u kartici**. Korisnik ubacuje svoju karticu u žljeb, a prst u naročito konstruisan otvor iznad žljeba. Skeniranje se vrši propuštanjem svetlosnog zraka kroz sistem optičkih objektiva i upoređivanjem otiska sa deponovanim otiskom na kartici.
- Identifikacija korisnika na osnovu upoređenja linija dlana ruke naziva se overa otisaka dlana.

Upoređivanje otisaka prstiju

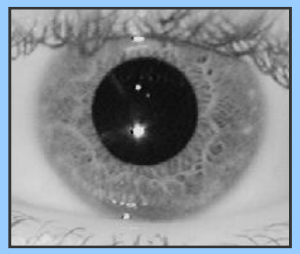


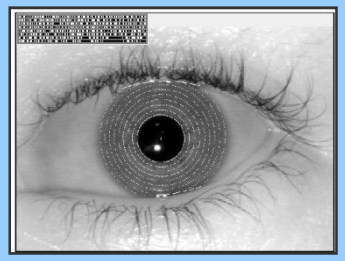
Geometrija ruke

- Kao metoda provere identiteta vlasnika kartice može da se koristi **geometrija ruke**, obzirom da se pokazalo da je **kombinacija dužine pojedinih prstiju** različita od osobe do osobe.
- Kod ovog pristupa najpre se precizno postavlja ruka iznad ekrana, zatim **fotoelektrični uređaj**, pod svetlošću visokog intenziteta, **vrši detekciju dužine prstiju kao i njihovu providnost.**

Skeniranje očne mrežnjače

- Ovaj pristup identifikacije podrazumeva korišćenje uređaja za identifikaciju obrasca očne mrežnjače. Uređaji koriste svetlosne zrake niskog intenziteta za ispitivanje obrasca na stražnjem zidu unutrašnjosti oka. Pri tome se meri i zapisuje toplota koju emituju karakteristični obrasci krvnih sudova u pozadini oka, da bi se potom ovaj podatak digitalizovao i skladištio na kartici.





Digitalizovani podaci

Uređaj za identifikaciju obrasca očne mrežnjače

Glasovna identifikacija

- Ovaj pristup identifikaciji zasniva se na činjenici da su glasovi osoba različiti.
- Prilikom pristupa kartici, osoba čita u mikrofon naročito odabrane reči.
- Ovaj sistem konvertuje komponente frekvencije određenih reči u digitalne signale koji se mogu analizirati, meriti i memorisati za buduće upoređenje.
- Kod ovog pristupa procenat greške je ispod 2,5%.

Venski obrasci

- **Venski obrasci**, odnosno venska provera je naziv sistema u kojem se koriste jednostavno **infracrveno skeniranje i tehnike kodiranja za analizu broja, relativne pozicije i veličine potkožnih krvnih sudova** u ljudskoj šaci ili ručnom zglobu. Kod svakog čoveka raspored razgranatih vena je takav da je uz pomoć tehnike moguće razlikovanje pojedinih osoba.

- Ovaj sistem je još u fazi razvoja, ali se pokazuje da je u primeni vrlo jednostavan sa izuzetno malim procentom greške.

Pitanja za razmatranje

16	MEHANIZMI ZAŠTITE
145	Šta je kriptografija
146	Koji su ciljevi kriptografije
147	Objasniti simetrično šifrovanje
148	Objasniti tripl DES algoritam
149	Šta je asimetrično šifrovanje
150	Objasniti tehnologiju digitalnog potpisa
151	Šta je infrastruktura javnih ključeva
152	Koji su osnovni sigurnosni protokoli
153	Šta je SSL
154	Koji su ostali mehanizmi zaštite