Predmet:
BEZBEDNOST INFORMACIONIH SISTEMA

VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA
NOVI SAD

OSNOVI ZAŠTITE INFORMACIJA

7. TEHNOLOGIJE ZAŠTITE RAČUNARSKOG SISTEMA

Ciljevi

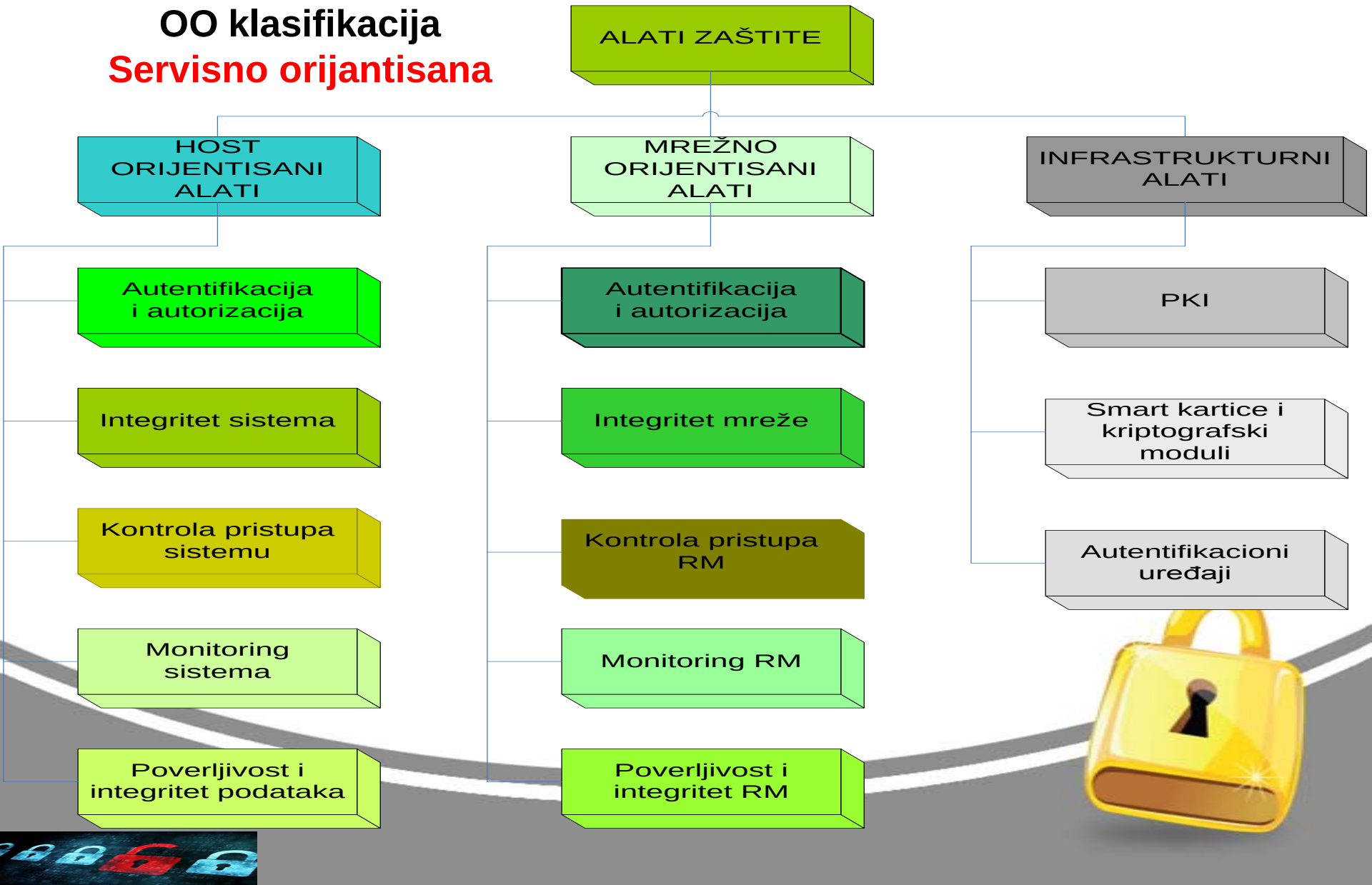
Razumet i naučiti:

- objektno orijentisanu (OO) šemu klasifikacije alata zaštite
- mehanizme i protokole zaštite računarskog sistema (RS)
- značaj NOSSS zaštite
- logičku kontrolu pristupa (LAC)
- upravljanje pasvordom

Mehanizmi (alati) zaštite RS

OO klasifikacija

Servisno orijantisana



NOSSS* servisi zaštite

- **Servisi zaštite OS**
  - Svaki s/z u krajnjem zavisi od **NOSSS**
  - Ako su ovi servisi slabi, s/z IKTS može se zaobići/probiti
  - *Bezbednost IS ne može biti veća od bezbednosti **OS?***
  - Neki s/z su na **jednom**, a neki na **više** logičkih nivoa **OS**

Primer:

- *identifikacija i autentifikacija*
- *korisnički interfejs* (na aplikativnom, prezent., sesijskom, mrežnom nivou RM)

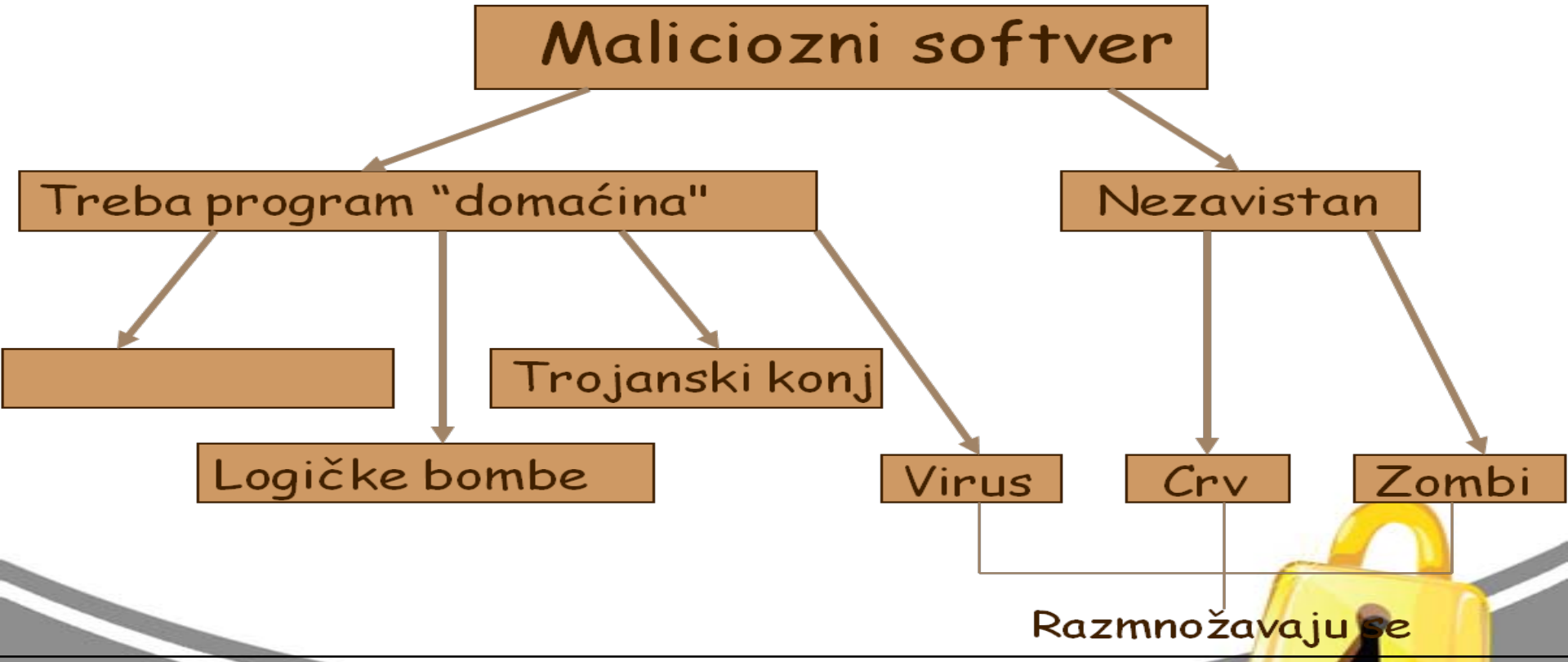
NOSSS* (*Native OS Security Subsystem*)-podsistem zaštite operativnog sistema

NOSSS servisi zaštite

- **Razlozi za zaštitu operativnih sistema (OS)**
  - Sprečiti **namerno narušavanje** *politike pristupa*
  - Sprečiti **uticaj programa sa greškom** na druge programe
  - **Poboljšati pouzdanost rada** RS
- **Šta sve treba zaštititi u računaru i OS?**
  - *hardver, softver i podatke, memoriju, I/O uređaje*
  - *šerovane programe i potprocedure, privatnost …*

Vrste napada na bezbednost OS

- ***Direktni*** - spolja (*hakeri*) ili iznutra (*nezadovoljni zaposleni)*
- ***Indirektni*** - nasumični napadi, najčešće *malveri**

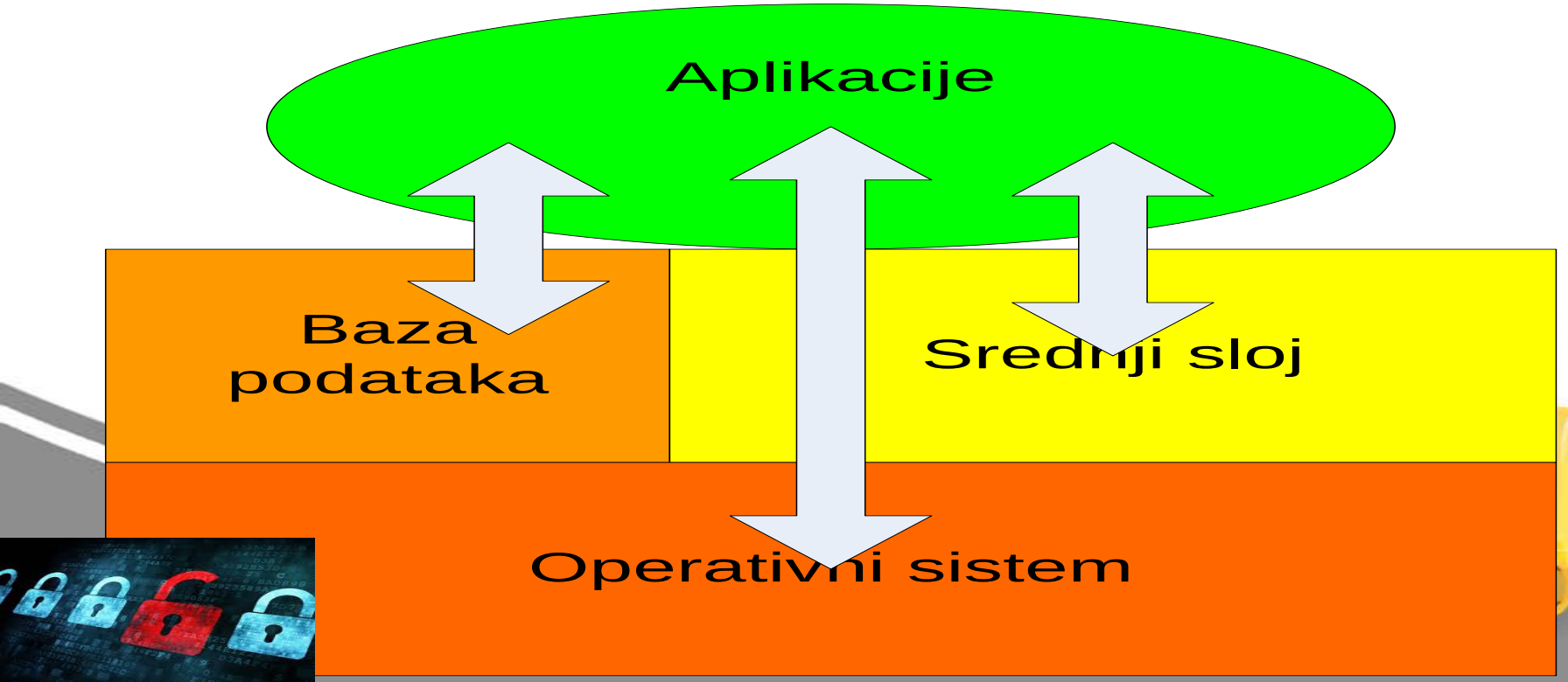


Malveri- maliciozni programi, virusi, crvi, trojanci…*

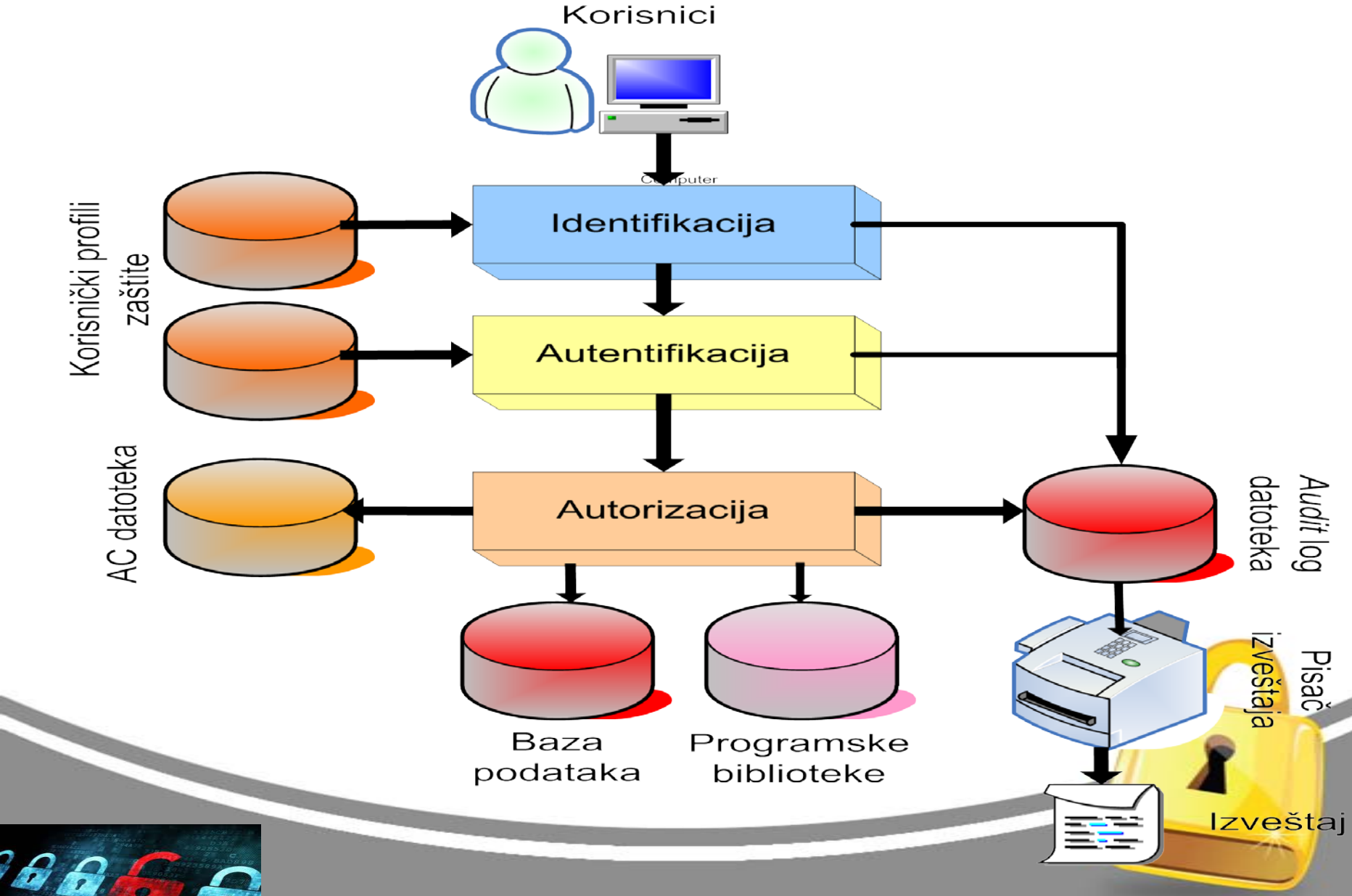
Mehanizmi zaštite RS

-*host* orijentisani-

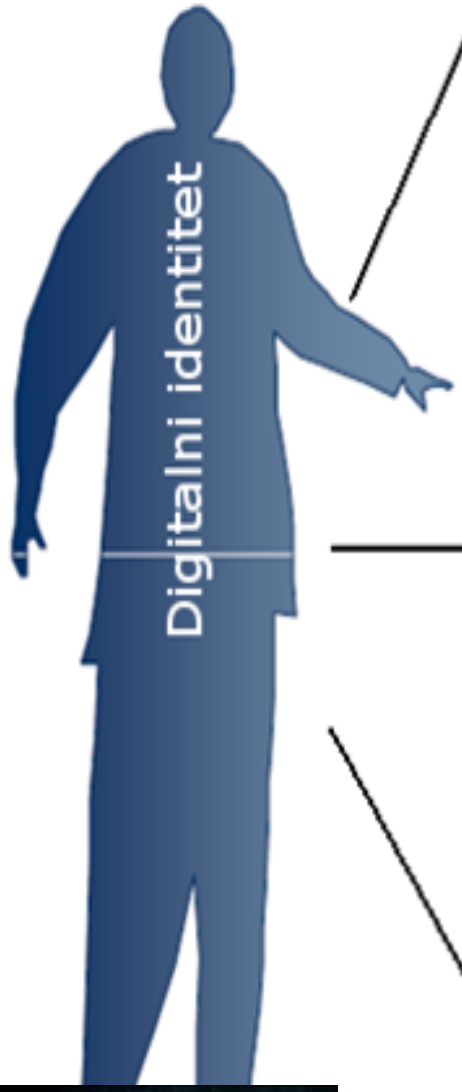
- **Bezbednosni, apstraktni slojevi RS*:***
  - *Koncept slojevite zaštita*
  - *NOSSS određuje najviši nivo zaštite IS*
  - *OS najznačajniji apstraktni sloj*



Generički servis kontrole pristupa (AC)



Digitalni identitet korisnika



- **Identifikacioni podaci** (neophodni podaci za identifikaciju)

AUTHENTICATION – authN

- korisničko ime
- tajna korisnička lozinka
- šifra
- Token + PIN
- Biometrička, itd...

- **Pristupni podaci** (neophodni podaci za dodelu ovlašćenja)

AUTHORIZATION – authZ

- Atributi (attr)
- Grupna članstva (group)
- Pripadajuće uloge (role)
- Pripadajuća organizacija (org)

- **Ostali podaci za opis**

- Delokrug, telefonski broj, adresa, itd...

Mehanizmi servisa za LAC

- **Servisi logičke kontrole pristupa (LAC):**
  - obavezna (***MAC-*** *Mandatory Access Control*)
  - diskreciona (**DAC-** *Descretionary Access Control*)
  - na osnovu liste (matrice) kontrole pristupa (**L(M)AC**)
  - na osnovu uloga (**RBAC -** *Role Based AC*)
  - na osnovu atributa posla (**ABAC –** *Atribute Based AC*)
  - na osnovu politike zaštite (**PBAC** – *Policy Based AC)*
  - adaptivan na procenu rizika (**RadAC –** *Risk Adoptive AC)*

Primer: *Default DACL* na C: particiji u Windows XP

Advanced Security Settings for Local Disk (C:)

Permissions | Auditing | Owner | Effective Permissions

To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inh...	Apply To
Allow	Administrators...	Full Control	<not ...	This folder, subfolders and files
Allow	SYSTEM	Full Control	<not ...	This folder, subfolders and files
Allow	CREATOR O...	Full Control	<not ...	Subfolders and files only
Allow	Users (TOR\...	Read & Execute	<not ...	This folder, subfolders and files
Allow	Users (TOR\...	Create Folders / Append Data	<not ...	This folder and subfolders
Allow	Users (TOR\...	Create Files / Write Data	<not ...	Subfolders only
Allow	Everyone	Read & Execute	<not ...	This folder only

Add... | Edit... | Remove

☐ Replace permission entries on all child objects with entries shown here that apply to child objects

OK | Cancel | Apply

Mehanizmi servisa za LAC (1)

1. **Sw mehanizmi za LAC** *mainfraim* RS nalazi se u većini NOSSS savremenih RS (razvijen pre više od **40 godina**)
2. Razvijena su **univerzalna rešenja za AC RS**

Danas*: Identity Managament (IBM - Tivoly itd.)*

Primer: EUA - *Enterprise User Administration*:

- interaktivno rade sa postojećim ***NOSSS***
- centralizuju upravljanje sa AC u distribuiranom sistemu

Proizvod: ESM (*Enterprise Security Mnagement*), koristi ga *Informatika AD,* Beograd

http://www.symantec.com/security_response/securityupdates/list.jsp?fid=esm

Primer: Mehanizmi servisa za LAC

3. **EUA softverski mehanizmi:**

- **upravljanje sa pravima pristupa** u velikom broju *OS, b/p i aplikacija* sa sopstvenim modelom zaštite
- obezbeđuju **centralnu administraciju prava pristupa** svim slojevima sw na različitim platformama
- **ne implementiraju** direktno **sam AC mehanizam** u OS

- **Nedostaci EUA su**:
  - **težak pregled AC podataka** iz više platformi
  - potreba **upravljanja promenama** na kontrolnim nalozima
  - **ograničeno kretanje** administratora
  - **neefikasan tok procesa autorizacije** sa slabom automatizacijom

Primer: Autentifikacioni mehanizmi Win OS

Windows sistemi koriste sledeće autentifikacione mehanizme za pristup udaljenim računarima

LAN Menadžer autentifikacija:

Koristi heš vrednost da odredi da li je udaljeni korisnik obezbedio validnu kombinaciju korisničko ime/lizinka

NT LAN Menadžer autentifikacija:

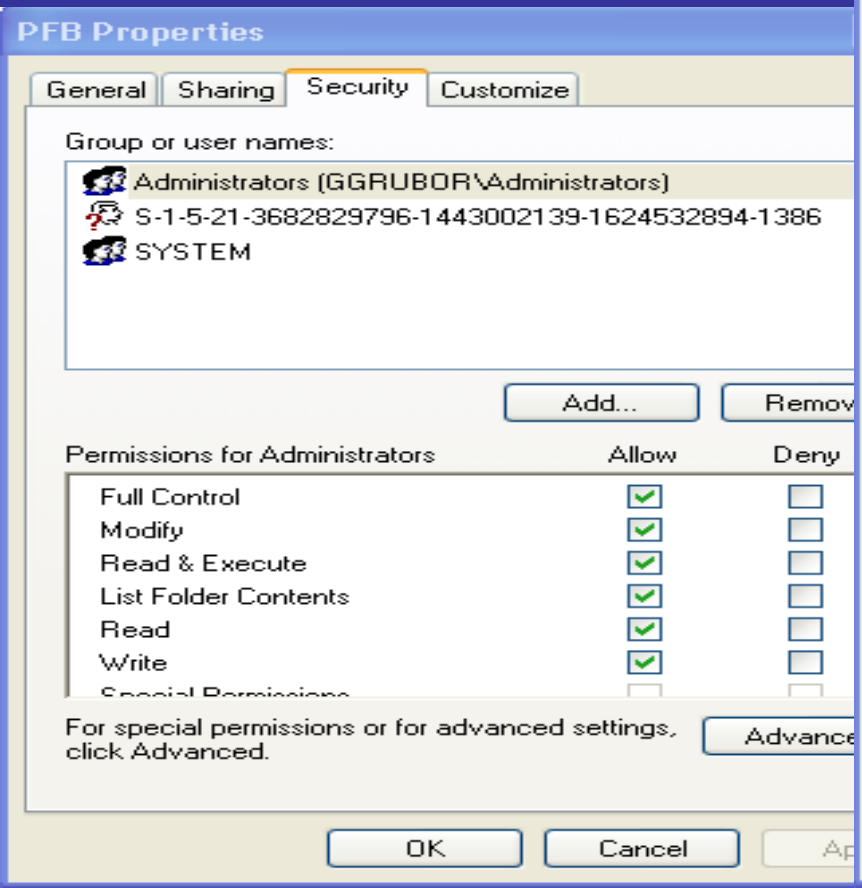
Koristi 16-bajtnu heš vrednost proračunatu za celu lozinku osetljivu na velika slova

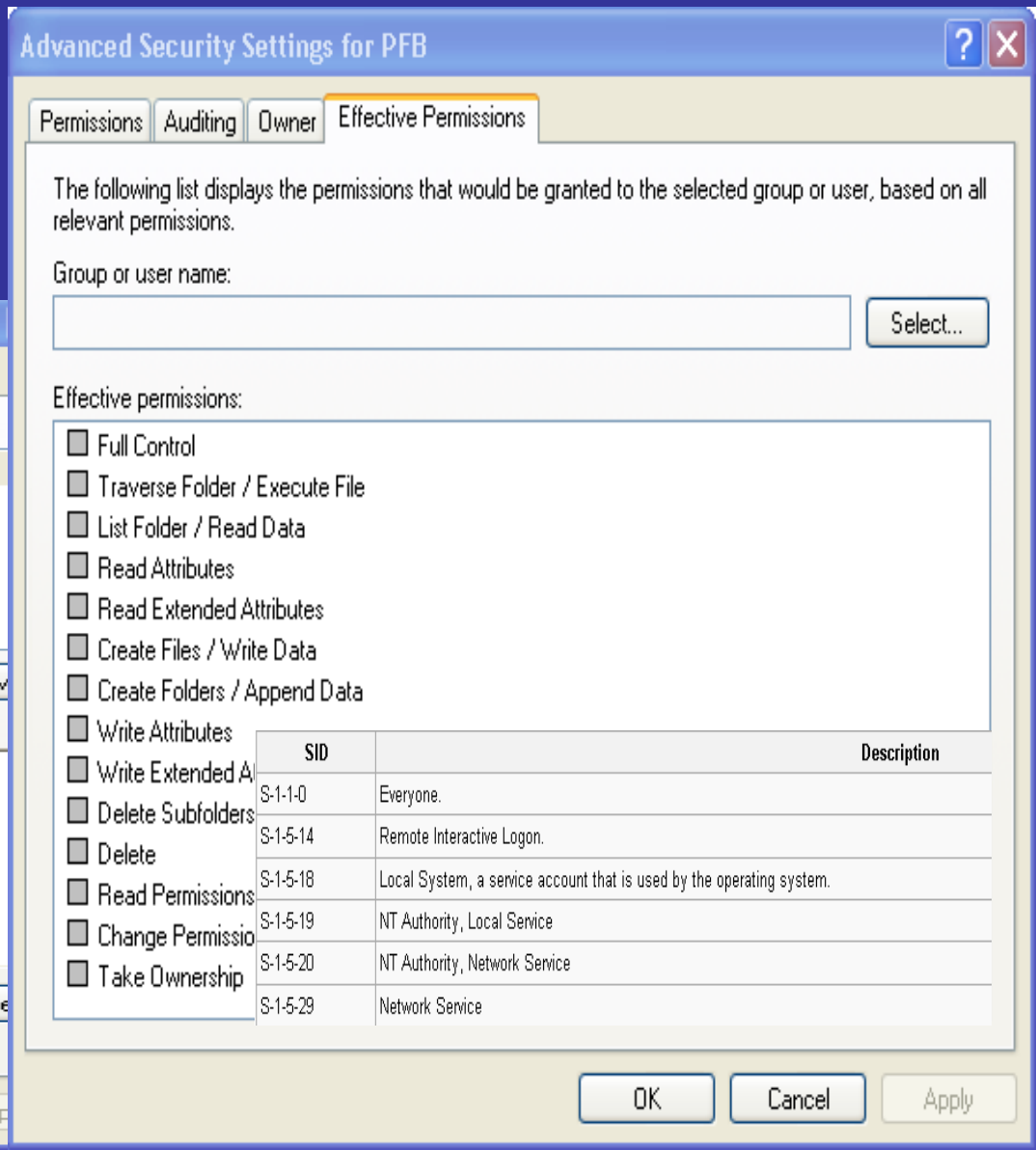
Kerberos:

Verifikacija korisničkog identiteta se vrši između Domen kontrolera i klijenta

Primer: Ovlašćenja u *Windows XP i Win Server 2003*

- **Na objektu na kojem se podešavaju ovlašćenja otvoriti list:**
  - *Properties*
  - *Security* list
  - *Advanced*
  - *Effective Permissions*





Pravila upotrebe pasvorda

- **Računar je kompromitovan (*zombiran*) ako napadač**:
  1. *Može da pokrene svoj program na vašem računaru*
  2. *Može da promeni OS na vašem računaru*
  3. *Ima nesmetan fizički pristup vašem računaru*
  4. *Može da postavi program na vašu web lokaciju*

- **Slabi pasvordi obezvređuju jaku zaštitu:**
  1. *Računar (u RM) je bezbedan toliko koliko je zaštićen administrator*
  2. *Šifrovani podaci su bezbedni toliko koliko je bezbedan ključ*
  3. *Neažuriran AVP je neznatno bolja zaštita nego da ga uopšte nema*
  4. *Apsolutna anonimnost je nepraktična u realnom svetu ili na vebu*
  5. *Tehnologija zaštite ne rešava sve bezbednosne probleme*

Upravljanje lozinkom

- **Problem**:
  - u RM **administratorski nalog** na svim R/S ima istu lozinku
  - manuelno održavanje različitih admin. lozinki za brojne servise nije moguće
- **Rešenje**: generator lozinki (npr. ***Pasgen***), koji ima dva poznata ulazna dela:
  - **frazu lozinke** i
  - **identifikator** (*naloga ili MAC mašine*)
- Koristeći *Pasgen* aplikaciju i frazu lozinke lako se generišu različite lozinke (**15 karaktera**) za veliki broj *mašina/sistema, web stranica i naloga za servise*

Primer: Funkcionalnosti tipičnog *Pasgen*

- Sintaksa za **g** funkcionalnost:
- ***Passgen g*** *<identifier> <pass phrase>* ***[-1 <desired length>]*** *[-**e** <desired character set>]* ***[-c*** *<account name> [<old password>]* ***[-m*** *<machine/domain>]* ***[-d*** *<service name>]]...*
- **Pozivom**: *passgen g <identifier> <pass phrase>* generiše se pasvord za identifikator mašine/servisa na bazi fraze lozinke i identifikatora
- **svič 1** koristi se za promenu dužine pasvorda i specificira broj za dužinu pasvorda

  Primer za 14 karaktera:

  passgen g <identifier> <pass phrase> ***-1 14***

Primer: Funkcionalnosti tipičnog *Pasgen*

- **e svič** kontroliše entropiju (neodređenost) u pasvordu
- **c svič** se koristi za promenu/resetovanje pasvorda na nalogu
- **m svič** specificira mašinu ili domen za promenu pasvorda
  - **m svič** propušten, lokalna mašina je u upotrebi
  - **m svič** specificiran, mašina/ime domena se mora specificirati
  - **m svič** se ne može koristiti bez **c sviča**
- **Pasgen r** (Generiše slučajni pasvord):
  - *Passgen r [-l <desired length>] [-e <desired character set>] [-c <account name> [<old password>] [-m <machine/domain>] [-d <service name>]]…*

Forenzički indikatori stanja bezbednosti u NOSSS

- ***Registrykeys*** **korisnika kreirani/izmenjeni u nekom T:**
  - Svi fajlovi ili *Registrykeys* kojima korisnik može pristupiti
  - Fajlovi ili *Registrykeys* sa nepoznatim/obrisanim korisnikom
  - Korisnici sa praznim/isteklim/neaktivnim/promenjenim pasv.
  - Korisnici koji se ne loguju u nekom periodu ili nikada
  - Korisnici koji direktno ili indirektno pripadaju admin. grupi
  - Korisnici sa pravima lokalnog logovanja na server
  - Korisnici sa privilegijama *dial-in* pristupa
  - Grupe sa *specifičnim*, *administratorskim*, *gost*, ili *onemogućenim* članom

Primer: Bezbednost Windows 7 OS

- *Windows Action Center* - Centar za zaštitu:
  1. Poboljšanja vezana za *User Account Control* (UAC)
  2. Poboljšanu bezbednost za *Internet Explorer 8*
  3. Mogućnost da se definiše *firewall* za specifičnu mrežu
  4. Mogućnost zaštitite od krađe podataka *BitLocker i BitLocker to Go*
  5. Automatski *update* i alarm korisniku za preduzimanje akcija
- Veća odgovornost prema zaštiti od XP OS:
  - u prvoj godini XP je imao **65 bezbednosnih popravki** ranjivosti, a **Vista 36**
  - pretnje od napada malvera na *Win 7* i dalje su velike

Bezbednost Windows 7 OS - *Internet Explorer 8*

- ***SmartScreen Filter*** *opcije u Internet Explorer's Safety*:
  - *Check This WebSite* – proverava veb sajt
  - *Turn Off (On)* ***SmartScreen Filter*** *– on/off* inteligentnog filtera
  - *Report Unsafe Website* – izveštaj o nebezbednom veb sajtu
  - *InPrivate Browsing* - čuva privatnost korisnika na veb-sajtu
  - radi u pozadini i upozorava na sajt sa liste lažnih sajtova
  - pristupom nekom vebsajtu šalje URL MS-om *SmartScreen* servisu
  - ako je sajt u bazi biće blokiran, a *URL obojena crveno*
  - ova blokada se **može zaobići na sopstveni rizik**

Antivirusna zaštita Win 7

- Windows 7 ne sadrži nikakav AV softver
- Treba odabrati neki od programa kompatibilnih sa OS Windows 7:
  - *Trend Micro Internet Security*
  - *AVG 15.0 Internet Security*
  - *Microsoft Security Essentials*
  - *Norton AntiVirus 2015*
  - *Avast! AntiVirus Home*
  - *Kapersky Anti-Virus 2015...*

Zaštita podataka i particija u Win 7/8

- *U Windows 7 Ultimate i Windows 7 Enterprise:*
- *BitLocker* :
  - služi za šifrovanje dokumenata ili particija
- *BitLocker To Go*
  - služi za šifrovanje prenosnih memorijskih uređaja (USB)

Primer procedure:

1. Priključiti *USB* na računar
2. Otvoriti *MyComputer i izabrati opciju BitLocker Drive Encryption*
3. Odabrati *Turn on BitLocker*
4. Kliknuti desnim klikom na *USB drive* ikonu
5. Pokrenuti *Wizard* u par koraka šifruje USB i traži unos pasvorda

User Account Control (UAC) Win 7

- **UAC** novi mehanizam uveden u **Vista OS**
  - sprečava eskalaciju privilegija
  - sprečava malicioznu promenu programa
- Opcijom *User Account Control Settings* mogu se izabrati 4 nivoa UAC podešavanja:

1. *Always notify* - ako korisnik pokušava da promeni setovanje ili da instalira program
2. *Default* - upozorava ako program pokušava da uvede neku promenu, ali ne i sam administrator
3. *Notify me only if a program attempts*... - obaveštava o promenama, ali ne gasi desktop
4. *Never notify* - dozvoljava automatsko unošenje promena za administratora, a odbija za ostale korisnike

Windows 7 - *AppLocker*

- Obezbeđuje kontrolu aplikacija - *dopušta/blokira*
- Dopušta samo aplikacije sa liste dozvoljenih
- Blokira sve ostale aplikacije
- **Blokira korišćenje nelicencnog softvera**
- Blokira korišćenje nepznatih aplikacija i malvera
- Blokiraju pokretanje aplikacije ako je mreža zasićena
- Blokira pokretanje aplikacije
- Usaglašava desktop okruženje sa poslovnom politikom
- itd

NOSSS Windows 8 OS

- **Windows 8 OS ima:**
- Sliku kao lozinku za logovanje
- Ugrađen AVP *Windows Defender* koji se aktivira ako ne detektuje drugi AVP
- *Unified Extensible Firmware Interface* (UEFI) koji zamenjuje BIOS ROM i verufukuje sw pre izvršenja u procesu podizanja računara
- *Windows Heap Manager* i *Windows Kernel Pool Allocator* – blokiraju malvere od iskorišćenja brojnih ranjivosti OS
- Za *ranjivosti baze registara* otežano je pisanje eksploita
- "*Security sandbox*" za aplikacije obezbeđuju pristup samo ovlašćenim aplikacijama
- Poboljšanje Internet Explorer-a 10

Antivirusni programi (AVP)

- **Ispituje otkriveni malver**
- **Identifikuje strukture kôda** (*definiciju*, *heš, DS, heuristika*)
- Detektuje prisustvo poznatih **malvera** skeniranjem *OS, b/p i aplikacija*, tražeći "*potpise*" **malvera u referentnoj bazi**
- Kada otkrije **malver** sa poznatom definicijom aktivira se set instrukcija za **uklanjanje (izolaciju)** te definicije
- Teže je kad se koristi **šifra** za skrivanje *potpisa* **malvera**
- **Savremeni AVP su dizajnirani za aplikativni sloj OS**:
  - mogu skenirati veliki obim objekata
  - poseduju napredne tehnike (dešifrovanje, slanje u karantin)

Razvoj AVP

- **Prva generacija:**
  - **jednostavni skeneri** zahtevaju **potpis virusa**
  - virusi se malo razlikuju, **u suštini imaju istu strukturu** i šemu bitova u svim kopijama
  - **drugi tip** prve generacije AVP je **upoređivao zapis sa dužinama programa** i nadgledao eventualne izmene u njihovoj dužini
- **Druga generacija:**
  - **heuristički skeneri** ne oslanjaju se na određeni potpis i koriste **heuristička pravila**
  - jedna klasa **traži delove kôda** često povezane sa virusima
  - druga klasa **skenira integritet** (sažetak, *hash*)

Razvoj AVP-1

- **Treća generacija:**
  - **skeniranje aktivnosti** u operativnoj memoriji
  - **prepoznaju virus po njegovim akcijama**, a ne strukturi
  - nemaju potrebu za razvijanjem heuristike i sakupljanjem potpisa velikog broja virusa
  - dovoljno je da identifikuju mali broj akcija koje mogu da ukažu na infekciju
- **Četvrta generacija:**
  - **potpuna zaštita** paralelnom upotrebom velikog broja AV tehnika, uključujući i sve prethodne
  - **imaju i mogućnost kontrole pristupa** (*firewall*), što smanjuje mogućnost inficiranja

Svi AVP neotporni na napad "0-dana"

Skener zaštite RS (SZRS)

- **SZRS kontrolišu integritet RS:**
  - Periodično **monitoriše stvarnu konfiguraciju** platforme, poredi sa predefinisanom, a neki automatski koriguju
  - Mogu raditi **na svim apstraktnim nivoima** (retko na aplikativnom)
  - Glavna primena - **skeneri ranjivosti OS** (manjih IS)

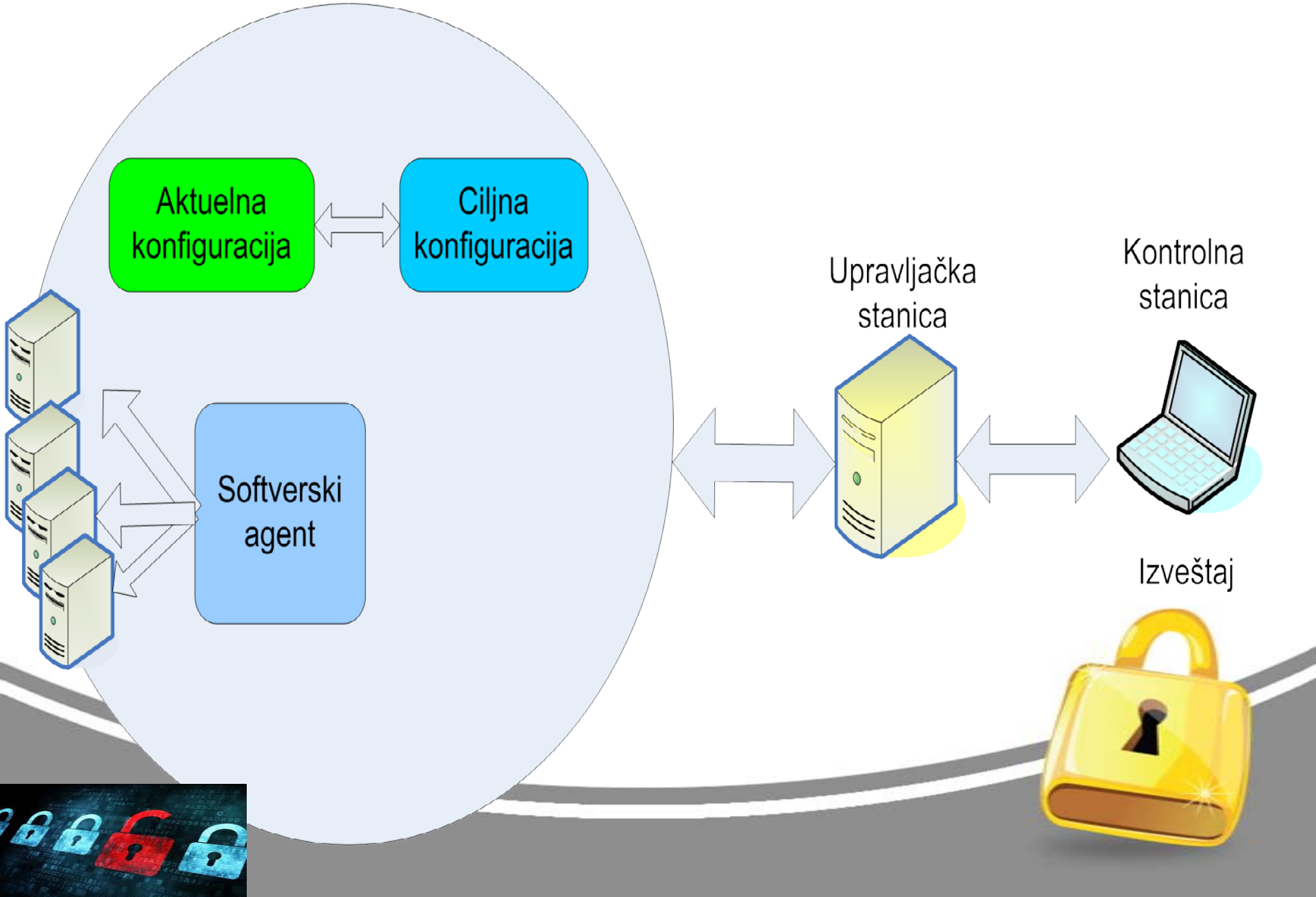
Ranjivost RS su greške: *hw i sw, konfiguracije i ljudi*

  - Osiguravaju bezbednost okruženja (srednji i veći IS)

- **Ocena efektivnosti SZRS meri se kroz smanjenje rizika**:
  - Osnovne konfiguracije S/Z na željeni nivo rizika (*bezbednom arhitekturom*)
  - Efikasnom/efektivnom korekcijom ranjivosti S/Z *(kontrolama zaštite*)

Primeri SZRS: *Belarc, Snort, Acauntec ....*

Primer: Skener ranjivosti u IKTS srednje veličine



Primer: Skeneri ranjivosti RS/RM

Qualys Inc. USA, California SaaS servisi

- Među prvim *Cloud Computing* vendorima hardvera i softvera za zaštitu informacija u svetu (SAD, 1999)
- Ranije se zvao ASP (*Application Service Provider*) – REST like HTTP API (2000)
- obezbeđuje sw/hw proizvode i servise za upravljanje bezbednosnim rizikom IKTS i usaglašenosti na zahtev korisnika (SaaS)
- ***Vulnerability Management*** – rešenje za proaktivno upravljanje bezbednosnim rizikom
- ***Policy Compliance*** – definiše reviziju (*audit*) i dokumenta za punu usaglašenost IKT sistema sa relevantnim standardima zaštite

Primer: Skeneri ranjivosti **RS/RM 1**

Qualys Inc. USA, California SaaS servisi 1

- ***PCI Compliance*** –automatizovana validacija za PCI usaglašenost institucije trgovaca (vendora) i kupaca
- ***Web Application Security*** – automatizovana zaštita i testiranje zaštite web aplikacija za kupce
- Besplatno skeniranje na prisustvo malvera
- *Qualys Go Secure Seal* – oznaka da Qualys obezbeđuje zaštitu tog sistema (600 Eu/godišnje)
- *Qualys Browser Checkup* – ispituje *plugins* web pretraživača i sugeriše poboljšanja
- *Qualys' Vulnerability R&D Lab* - vodi mesečno svakog drugog utorka *videocast* na temu ranjivosti i pretnji u MS Widows OS.

Skeneri sadržaja (SS)

- **Evaluiraju sadržaj** (e-pošte, web sajta) u odnosu na *predefinisanu politiku zaštite*
- **Komplementarni su AVP** i potencijalno moćnije detekcije:
  - slede **pravila na bazi različitih kriterijuma**
  - nisu ograničeni na statička svojstava **malvera**

a. *Jednostavni skeneri* sadržaja e-pošte vrše leksičku analizu i:
  - **odlažu u karantin** poruke sa predefinisanim rečima/frazama

b. *Sofisticirani skener* sadržaja:
  - radi **u realnom vremenu**
  - otkriva prisustvo mobilnih kodova (*Java, JavaSkript i ActiveX)*
  - izvršava akcije, ako ne ispunjava zahteve politike zaštite
  - obično *ispituje pakete u prenosu* između dva sistema
  - radi **na aplikativnom nivou**

Primer: EŠALON?

Skeneri sadržaja (SS)-1

Tipični *SS* obezbeđuje:

- više načina reagovanja na **povredu politike zaštite**
- administratoru da **konfiguriše akcije na bazi pravila**
- **odlaganje u karantin** ili brisanje dodataka e-pošte
- **odbacivanje poruka u *junk*** direktorijum
- **blokiranje** preuzetih **sadržaj mobilnih kodova**
- **prenos sumnjivih sadržaja TTPS** provajderu **na analizu**
- **detektovanje ugrađenih slika** i interpretacija teksta
- **logovanje i slanje alarma** korisniku...

Veb filteri

Namenjeni za prepoznavanje i odgovor na sadržaj veb sajta:

- Filteri **e-pošte** imaju ugrađene AVP
- **AVP počinju da ugrađuju** funkcionalnosti **SS**
- Mehanizmi **AVP i SS konvergiraju** u jedinstven mehanizam

Monitoring zaštite RS-IDPS

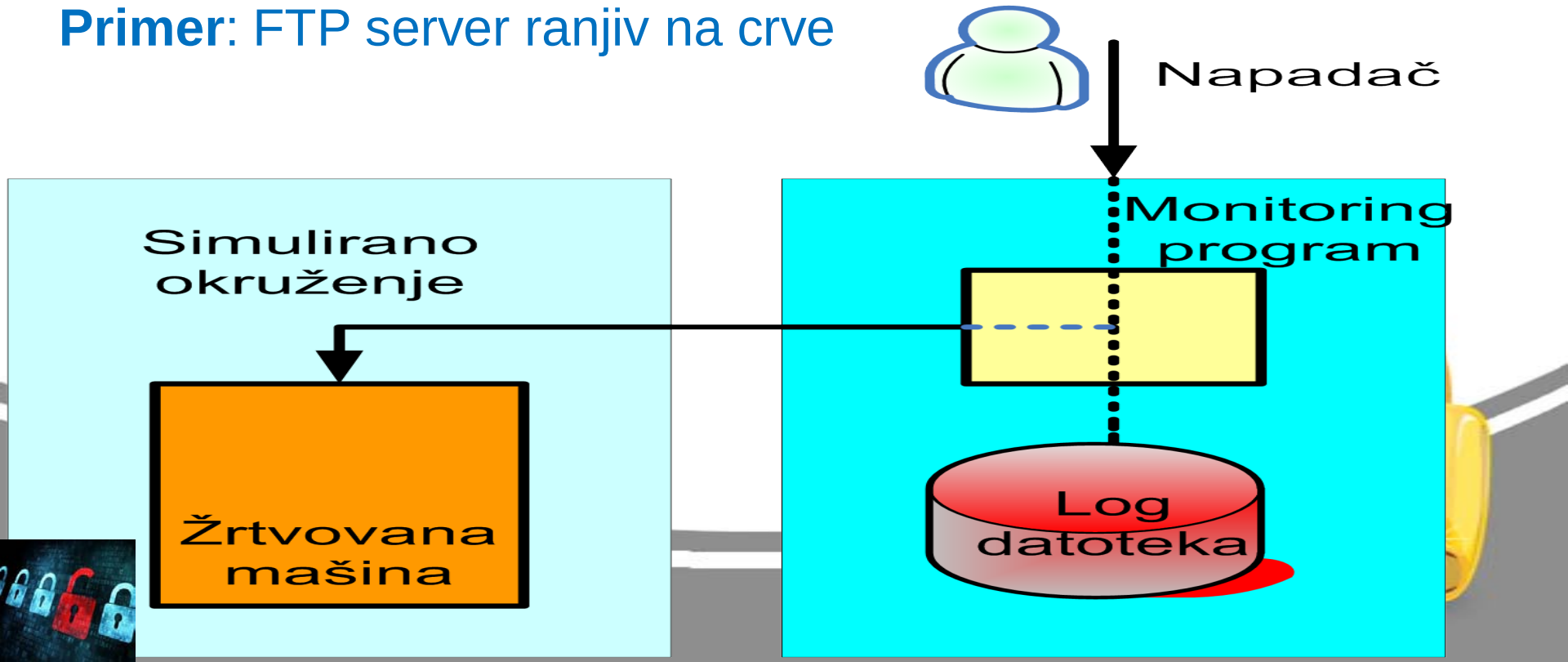
- **Detektori upada u RS (IDS)**:
  - **brzo ažuriraju definicije napada**
  - vrše **direktnu intercepciju i interpretaciju** pristupa
  - generalno-imaju **dobre sisteme izveštavanja**
  - **glavna ranjivost - mogućnost proboja u log datoteku**
- **Sistemi za sprečavanje upada u RS – IPS:**
  - pored funkcija **IDS omogućava inteligentne zamke** za napadača (tipa ćupa meda-*honey pot*) i **korektivnu akciju**
  - skreću pažnju i **izučavaju osobenosti napadača**
  - **preventivno štite od sledećeg napada**
  - **konvegiraju u jedinstven mehanizam IDPS**

Primer: IPS koncept – *COBRADOR, ISS, IBM*

Monitoring zaštite RS-IDPS koncept

- *Honeypots* - izolovan sistem za izvlačenje *eksploita* napadača
- Koristi simulirani RS sa *greškom konfiguracije*, *lakim pasvordom* itd.
- Ima dve kategorije, sa:
  (1) *visokom interakcijom* - realni sistem skuplja detalje o napadaču
  (2) *niskom interakcijom* - simulirani deo sitema za određeni *malver*

Primer: FTP server ranjiv na crve



Monitoring zaštite RS - IDPS

- **Sistemi za detekciju i sprečavanje upada u:**
  a. **RS - HIDPS** (*Host IDPS - Intrusion Detection&Protction Systems)* i
  b. **RM - NIDPS** *(Network IDPS*)
- **IDS i IPS sistemi** *konvergiraju* u jedinstven sistem:
  - prepoznaju indikacije upada, **upozoravaju** korisnika ili **koriguju** akcije
  - **analiziraju podatke** o upadu i obično su **dizajnirani za određene OS**
  - razlikuju se po načini rada i tipu informacija koje procesiraju
  - **koriste različite mehanizme** za detekciju upada na bazi:
    - *potpisa, anomalija i pseudorelacione analize kontrolnih tragova*
    - *kombinuju mehanizme potpisa i detekcije anomalija*
    - *vrše proveru integriteta datoteka (heš vrednosti)*

Mehanizmi za upravljanje log datotekama

- **Problemi korišćenja log datoteka:**
  - **veliki obim podataka** za analizu (potrebna filtracija…)
  - nedostatak **jasnih pravila** za *proaktivnu* i *reaktivnu* analizu
  - **praćenje sumnjivih aktivnosti** koje se šire kroz mrežu
- **Nedostaci filtracije log podataka**:
  - **mogu se odstraniti važne informacije**
  - teško **prepoznavanje podataka istog tipa** na različitim R/S
  - označavanje tragova za *proaktivnu* ili *reaktivnu* analizu
  - sinhronizacija časovnika za konsolidaciju hronologije napada
  - fokus na razvoj alata **za analizu bezbednosnih događaja** u **logovima *web* lokacija,** umesto analize **pristupa klijenata**

Mehanizmi za upravljanje log datotekama (1)

- **Obezbeđuju**:
  - selektivan pristup **log dat. kontrolnih tragova bezbednosno relevantnih događaja**
  - **filtriranje podataka na osnovu pravila**,
  - **skupljanje** *login* **informacija sa različitih platformi**
  - **praćenje napada ili indikacija napada**, uspostavljanjem **vremenske linije napada**

Primeri: *Splunk 4.0, Zenoss* itd.

Kriptografski mehanizmi

- **Kriptografija:**
  - tehnika **izmene** informacija pomoću neke **transformacije**
  - samo određena grupa korisnika može izvući originalnu inf.
- **Transformacija** *otvorenog teksta* (**OT**) u nečitljiv *šifrat* (**ŠT**):
  - vrši se upotrebom **kriptografskog algoritma i ključa**
- **Kriptografija** se deli na:
  - *simetričnu (isti ključ za šifrovanje/dešifrovanje)*
  - *asimetričnu (PKI – javni i privatni ključ)*
  - *hash funkcije (jednosmerne funnkcije)*
  - *naprednu kriptoanalizu*
- **Osnovni hw/sw mehanizmi štite:**
  - *poverljivosti*, *integriteta*, *neporecivosti* i *jaku autentifikaciju*:

Kriptografski mehanizmi - simetrični

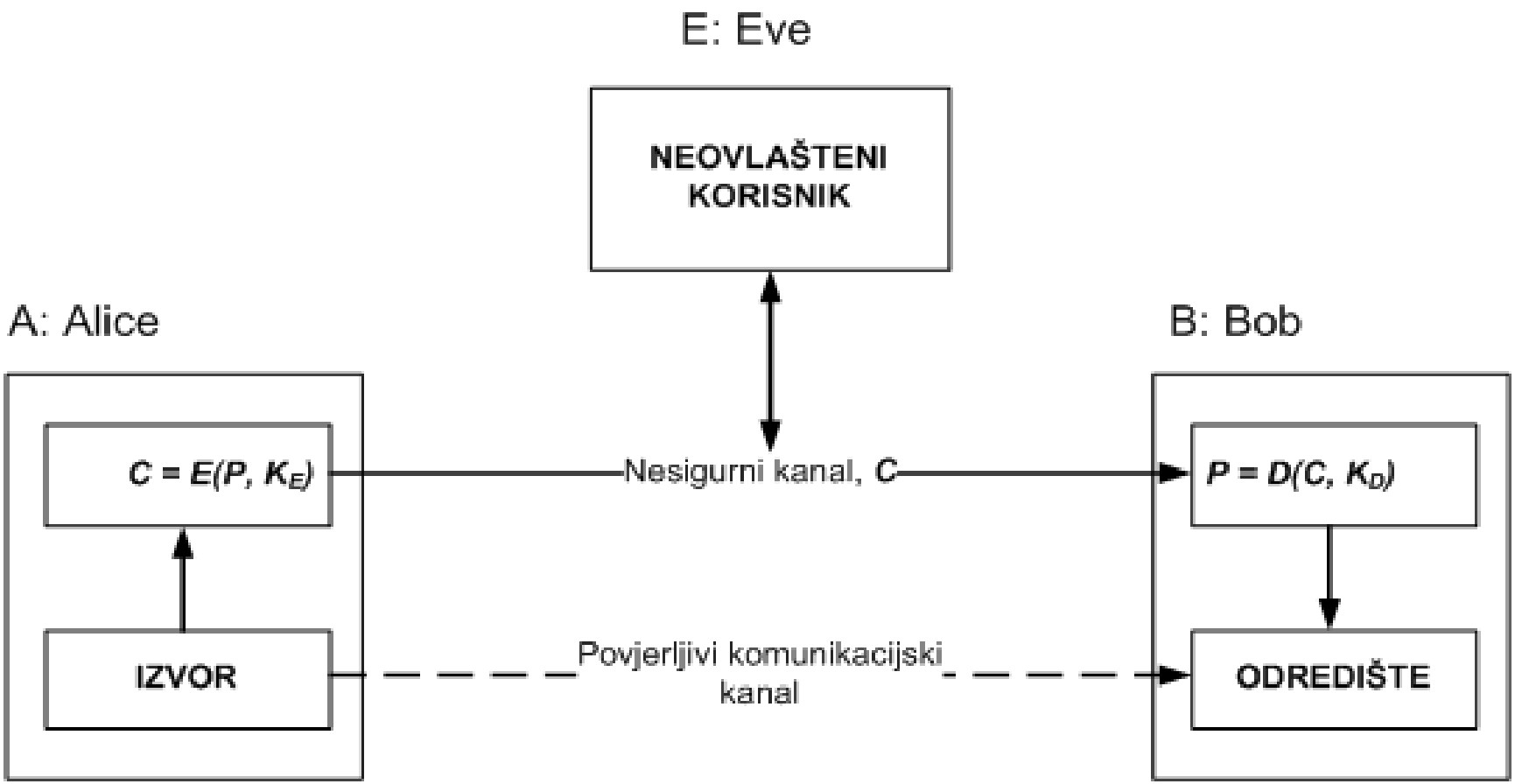
- **Kriptografske transformacije - matematičke funkcije – algoritmi:**
  - prevode nizove bitova **OT** u nizove bitova **ŠT** i obratno
- **Šifrovanje** - postupak prevođenja podatka **OT** u **ŠT**:
  - **C = E(P, K_E),** gde su: ***P*** – OT; ***C*** – ŠT; ***E***-funkcija šifrovanja; K_E- ključ za šifrovanje.
- **Dešifrovanje** obrnuto - prevodi **ŠT** u **OT**:
  - **P=D(C, K_D),** gde su: ***P*** – OT; ***C*** – ŠT; ***D*** - funkcija dešifrovanja; K_D - ključ za dešifrovanje
- **Šifarski sistem** čine **-** *šifrovanje, upravljanje ključa i dešifrovanje*
- **ilsti** ključ je za šifrovanje i dešifrovanje :
  - $K_E = K_D$ **= K,** pa je: ***C = E(P, K); P = D(C, K); P = D[E(P, K), K]***.

Kriptografski mehanizmi – simetrični 1

- **Najpoznatiji simetrični algoritmi:**
  - **DES** (*Data Encryption Standard*), **K= 56 bita**, **IBM (1977 - 2000)**
  - **DES** su probili hakeri **sredinom 90–tih** (*virtuelni super računar)*
  - **2xDES, 3xDES** poboljšanja DES-a
  - **AES** (*Advanced Encryption Standard)*, **K=128, 192 i 256** bita.
- **Generisanje ključa (K):**
  - slučajni ili pseudoslučajni niz (simetrični)
- **Upravljanja ključem:**
  - generisanje, prenos, uništavanje, zaštita integriteta i način korišćenja
- **Osnovni nedostatak simetrične kriptografije**:
  - upravljanje ključem - za **n** korisnika potrebno **n(n – 1)/2 ključeva**
  - **kriptografski ključevi – resursi koje treba izuzetno štititi**

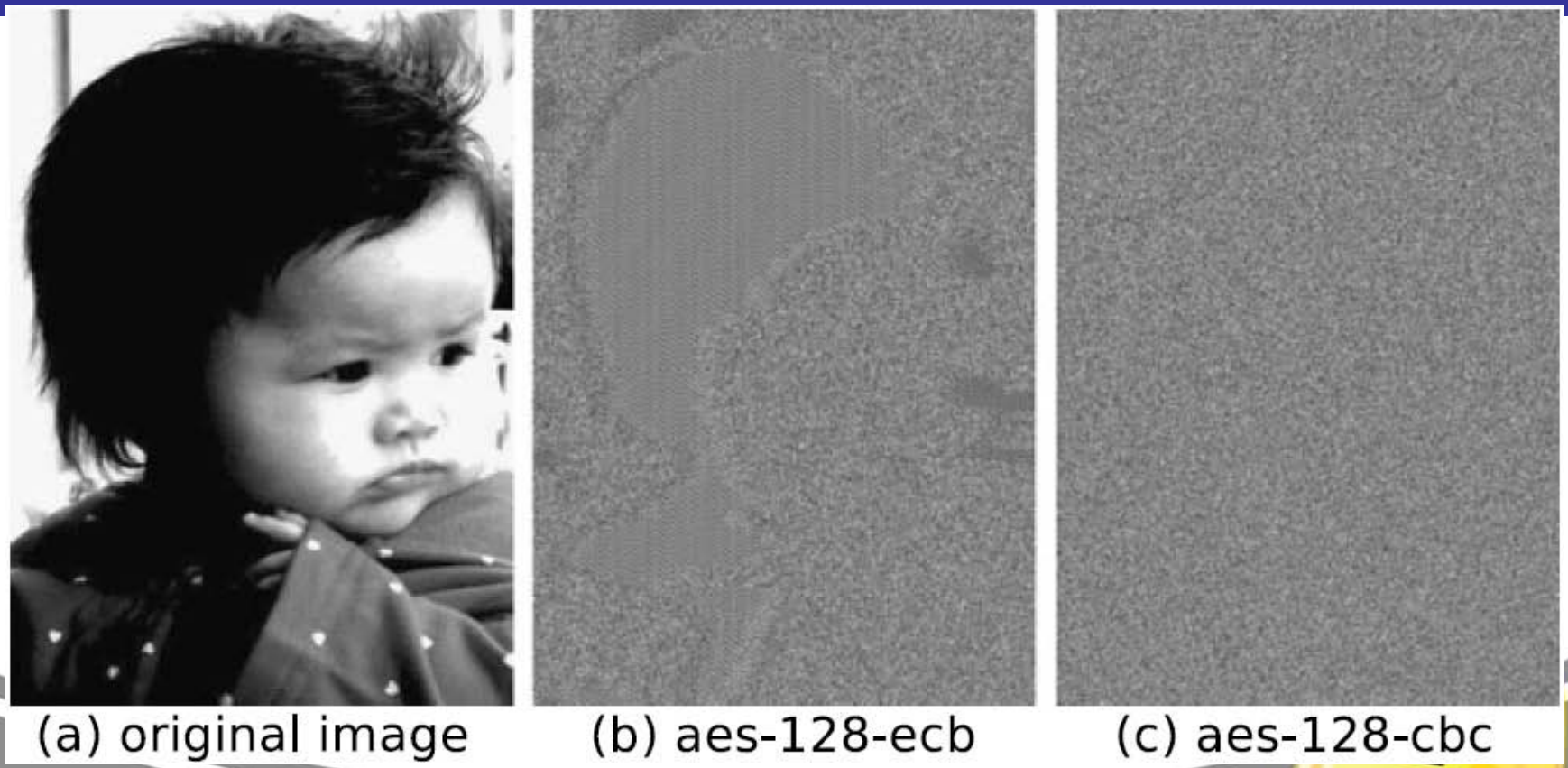
Primer: Kriptografski mehanizmi – simetrični

Komunikacioni kanal sa šifrovanjem podataka između dva korisnika



Primer simetričnog šifrovanja

Šifrovanje sa **AES alg**oritmom (128-bita fiksna veličina bloka):
(b) *Electronic codebook* (ECB) mod blok šifre (blok OT= bloku ŠT)
(c) *Cipher-block chaining* (CBC) mod blok šifre (blok OT≠ bloka ŠT)



(a) original image (b) aes-128-ecb (c) aes-128-cbc

Kriptografski mehanizmi - asimetrični

- *Infrastruktura sa javnim ključem* **(PKI):**
  - najbitnija *infrastrukturna komponenta zaštite* RM
  - obuhvata **veći broj korisnika** od simetrične kriptografije
  - delimično rešava problem distribucije ključa kod simetrične
  - korisnik zahteva samo matematički **par ključeva** (**Pk, Tk**)
  - za generisanje **Tk** i **Pk** najčešće se koriste dva algoritma:
    - *Diffie-Hellman(DH) i Riverst-Shamir-Adleman (RSA*)
  - **Pk** i **Tk** *proizvodi prostih brojeva* velikog prostog broja
  - obezbeđuje **okvir za protokole zaštite transakcija** i
  - integriše servise zaštite:
    - *digitalnog potpisa, poverljivosti i integriteta informacija, neporecivosti, jake autentifikacije, razmene simetričnog ključa*

Infrastruktura sa javnim ključem-PKI

- **Pk** - *javni ključ koji* se razmenjuje sa svim korisnicima u mreži
- **Tk** - *privatni ključ* koji se strogo čuva
- **Poverenje korisnika obezbeđuje** *digitalni sertifikat* (**DS**):
  - **sertifikaciono telo** (**CA**) potpisom **DS** sa **Tk** garantuje povezanost **Pk** i **vlasnika**
  - **DS** - e-dokument koji pouzdano pridružuje par (**Pk, Tk)** korisnika
- **DS se može primeniti** za:
  - *verifikaciju digitalnog potpisa, AC i jaku autentifikaciju*
- **DS** je usaglašen sa standardom (npr. **X.509**) i lak za lociranje
- **DS** se definiše *politikom serifikata*

PKI politike - instrukcija za izradu CS i CPS

Primer: Sadržaj standardnog ITU X.509 DS v.3.0

Verzija formata sertifikata
Serijski broj sertifikata
Identifikator algoritma kojim se vrši digitalni potpis
Naziv Sertifikacionog tela koje je izdalo sertifikat
Rok važnosti sertifikata
Naziv vlasnika sertifikata
Javni ključ vlasnika sertifikata
Određeni specifični podaci koji se odnose na uslove korišćenja sertifikata
DIGITALNI POTPIS SERTIFIKATA TAJNIM KLjUČEM SERTIFIKACIONOG TELA

Certificate Details

General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	61 10 8f 9f 00 00 00 00 00 0a
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	kundalab-KUNDALABDC1-CA, ...
Valid from	Wednesday, January 19, 201...
Valid to	Thursday, January 19, 2012 5...
Subject	NehnisaIvanis@kundalab.com

Edit Properties... Copy to File...

Learn more about certificate details

OK

Tipovi digitalnog sertifikata (DS)

- *DS identiteta* – kodira identitet principala (CA),
- *DS atributa* – kodira grupni kredibilitet,
- *DS ovlašćenja* – kodira delegiranje i restrikcije ovlašćenja,
- *DS uslova korišćenja* – kodira npr. troškove, atribute uloga, lične karakteristike i sl.
- **Generalno, DS sadrži Pk vlasnika i sadrži tri *promenljiva dela*:**

1. *tbsCertificate*: podaci za identifikaciju DS
2. *signature Algorithm*: identifikator algoritma za potpisivanje
2. *Signature*: sam digitalni potpis sa **Tk CA**

Kriptografski mehanizmi - bezbednost

- **Ovlašćeni korisnici** poseduju:
  - isti ključ - **simetrična kriptografija**
  - ključ iz matematičkog para **Pk/Tk** ključa - **PKI**
- Samo *određena grupa korisnika* može izvući **OT**
- **Bezbednost**: više u ključu nego u algoritmu
- **Tajnost ključa**: problem upravljanja ključem
- **Algoritam**: nemoguće čuvati u tajnosti
- **Vrednovanje kriptografskih algoritama (FIPS)**:
  - vrši se na osnovu kriterijuma za procenu

(**Primer**: **T.1**)

Primer: T.1 Kriterijumi procene vrednosti kriptološkog algoritma (FIPS 140-2)

Vrednost (poeni)	Prihvatljivost metode za mehanizam zaštite
5	Veoma prihvatljiv
4	Prihvatljiv
3	Prosečan (bez posebnih prednosti)
2	Relativno loš
1	Vrlo loš
0	Bez opredeljenja

Primer: Vrednovanje kriptografskih algoritama

- Vrednosti **simetričnih** i **asimetričnih** algoritama za mehanizme zaštite u odnosu na

Kriterijum	Asimetrični algoritam	Simetrični algoritam
Identifikacija	5	3
Autentifikacija	5	5
Podaci	3	3
Kašnjenje	4	2
Troškovi	1	5
Kvalitet prenosa	0	0
Opterećenje kanala	1	5
Ukupno	19	23

Primer: Vrednovanje kriptografskih algoritama

- **Simetrični algoritmi su bolji**:
  - metod kriptozaštite, u odnosu na sve kriterijume
- **Asimetrični algoritmi su bolji**:
  - za autentifikaciju korisnika:
    - mogu se kombinovati sa uređajima za jaku autentifikaciju (*smart* kartice, *tokeni*)
  - približno su ekvivalentni simetričnim za zaštitu sadržaja informacija i podataka

Kriptografski mehanizmi

- **U arhitekturi zaštite RS** koriste se za:
  - šifrovanje datoteke (npr. ***EFS*** u Win XP OS)
  - šifrovanje celog HD (npr. *Windows VISTA, Windows 7, 8*)…
- **U arhitekturi zaštite RM** koriste se za:
  - **zaštitu poverljivosti** podataka na prenosnom putu
  - **autentifikaciju** (korisnika, uređaja)
  - **neporecivost** aktivnosti
  - **protokole zaštite** (*IPSec, SSL, HTTPS, SSH* itd.)
  - **implementaciju integrisanih servisa zaštite** u PKI sistemu:
    - *autentifikacije, poverljivosti, integriteta i neporecivosti*

Kriptografski mehanizmi-*hash funkcija*

- ***Hash* funkcija –** *jednosmerna funkcija*
- **Obezbeđuje zaštitu integriteta podataka i informacija**
- **U PKI primenjuje se za digitalni potpis (DP):**
  - Korisnici **A** i **B** razmene svoje javne ključeve (**Pka i Pkb**)
  - Od originalne informacije **A** pravi *hash* (**sažetak**) sa:
    - algoritmom na bazi *jednosmerne funkcije* (**MD -***Massage Digest,* **SHA 1, SHA 256, SHA 512...SHA 2048)**
  - **A** šifruje *hash* se svojim *tajnim ključem* - **Tka**
  - **B** dešifruje poruku javnim ključem pošiljaoca **A** - **Pka**
  - **B** verifikuje *hash* **istim algoritmom (ako su** podaci izmenjeni – različit je *hash - narušen integritet***)**
  - **Skeneri zaštite** - koriste *hash* za detekciju izmene datoteka
  - **Antivirusni programi** (AVP) detektuju viruse na bazi *hash*-a
  - **Druge primene *hash-a ???***

Primeri hash *funkcija*

hello → MD5 → 5d41402abc4b 2a76b9719d91 1017c592

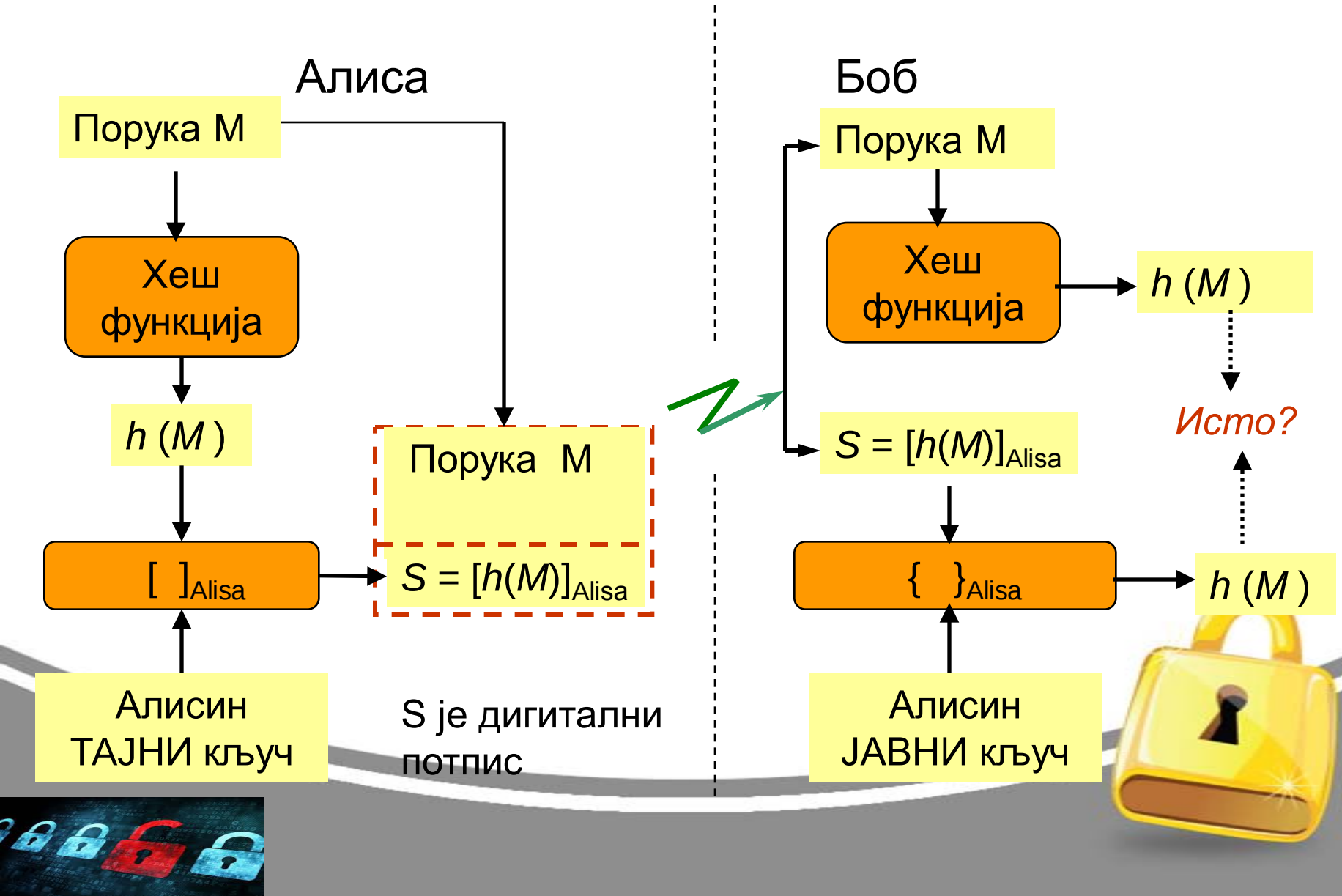
x → Хеш функција → h(x)

 → Једносмерна функција → 

 → ✗ → 

5d41402abc4b 2a76b9719d91 1017c592 → ✗ → hello

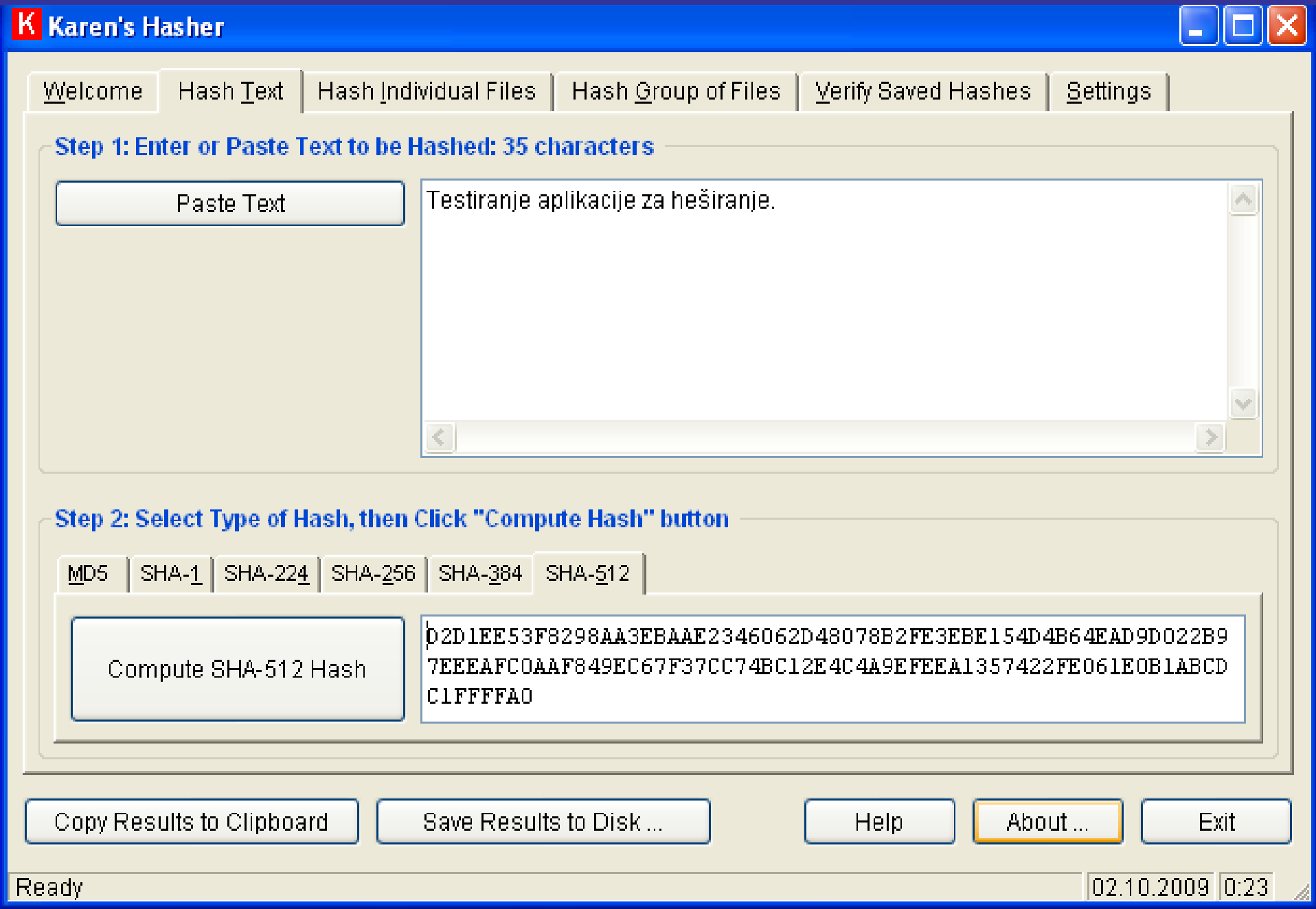
Digitalni potpis i hash funkcija



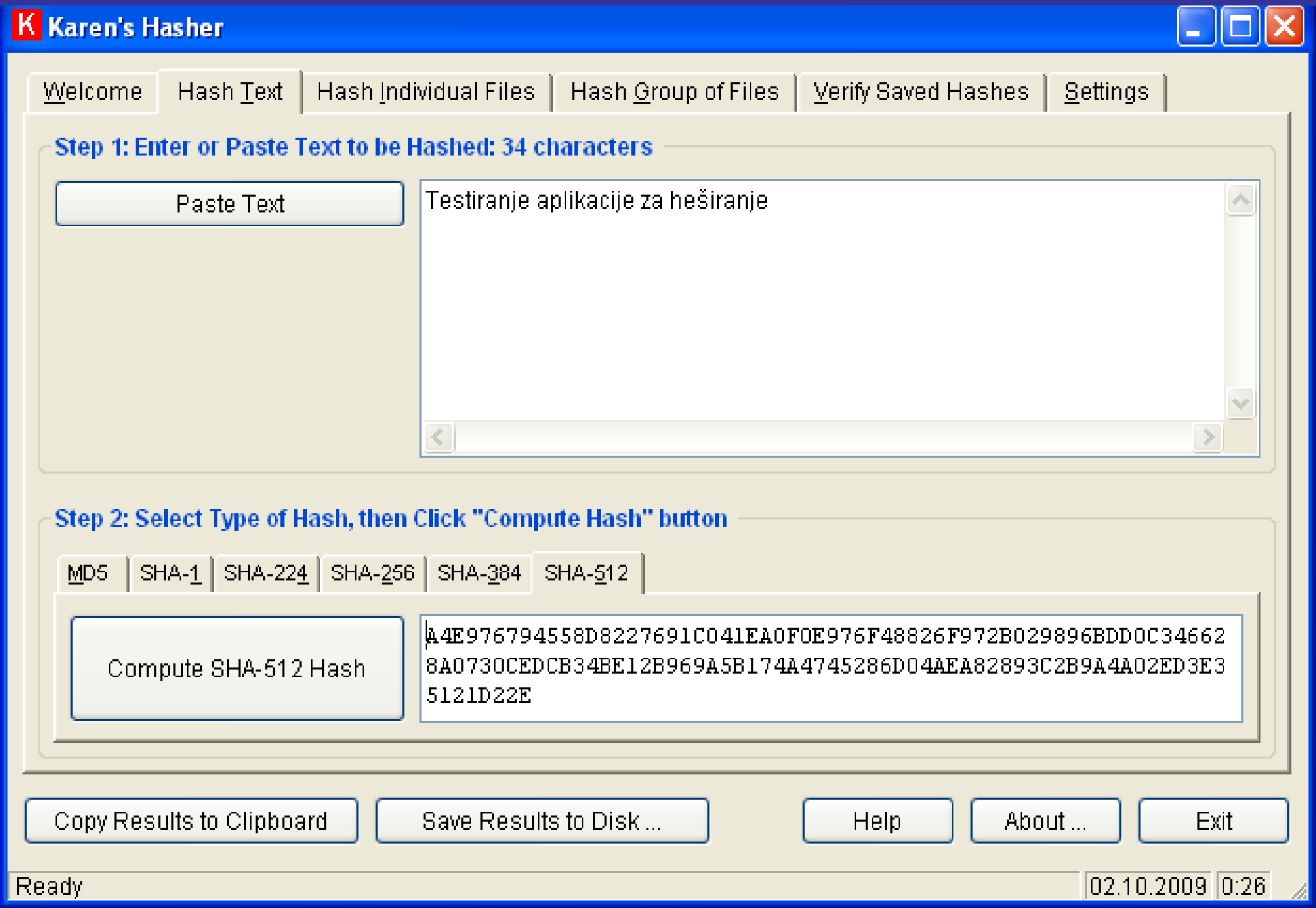
Primer: Procedura DP i šifrovanja e-transakcije

- Korisnici **A** i **B** razmene ***DS*** (svoje ***Pk***) i instaliraju u MS Outlook (2 komande – DP, Š)
- Korisnik **A** digitalno potpiše poruku sa svojim Tk
- Korisnik A šifruje DP poruku sa **Pk** korisnika **B**
- Korisnik **B** dešifruje digitalno potpisanu e-poruku sa svojim ***Tk***
- Korisnik **B** verifikuje DP sa javnim ključem korisnika A – ***Pk***

Primer: Primena *hash* algoritma



Primer: Primena *hash* algoritma



Primer: Verifikacija *hash-a*

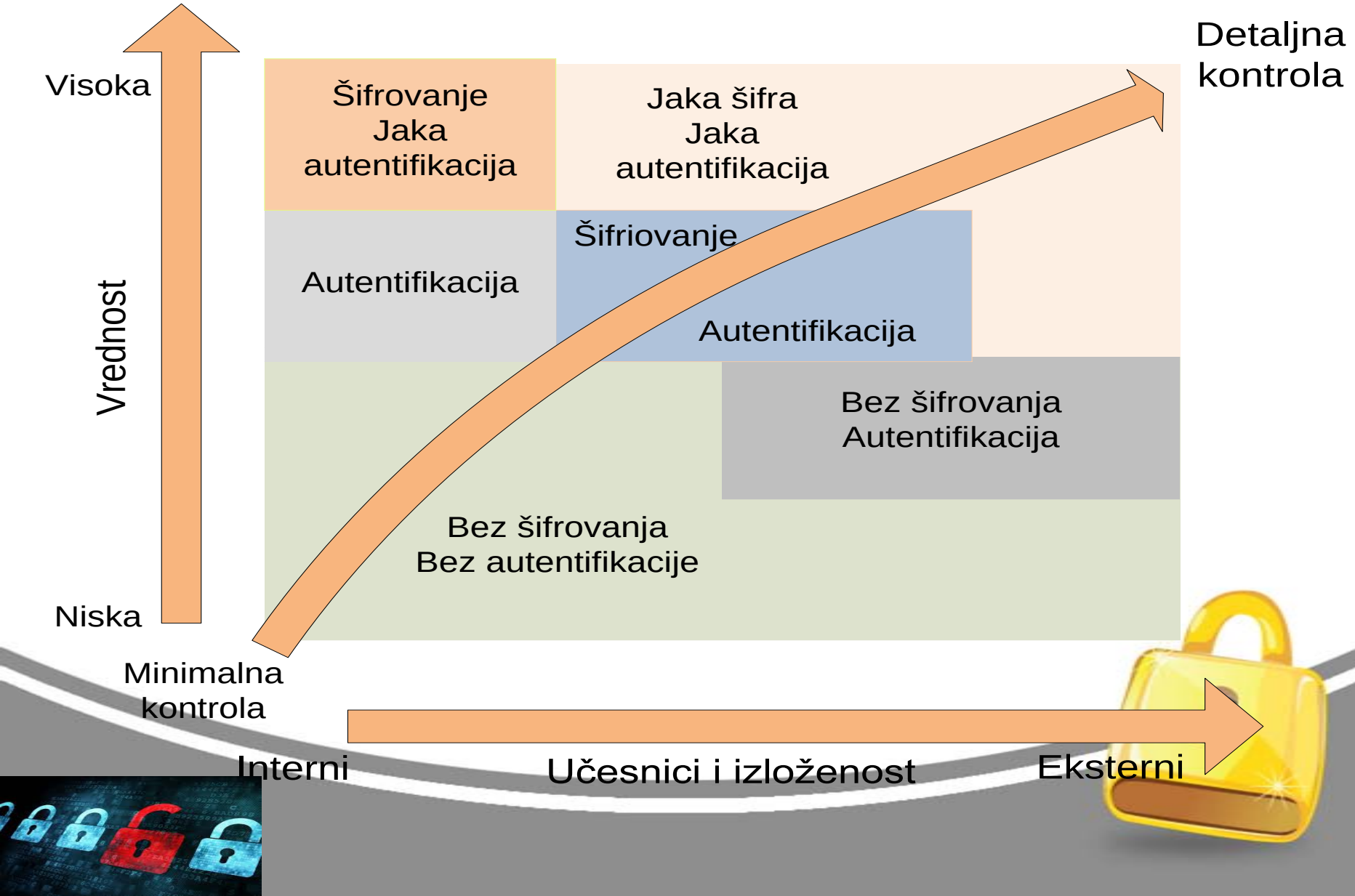
- **Karen's Hasher v2.2.1**
- http://www.karenware.com
- Date: 13.12.2008 10:22:55
- Computer: GGM-25031949
- User: Gojko
- Files Hashed: 1
- File Name SHA-256 Hash
- C:\Documents and Settings\Gojko\ Desktop\NDA.DOC

Primer: Verifikacija *hash-a*

http://www.karenware.com

- Date: 13.12.2008 10:20:24
- Computer: GGM-25031949
- User: Gojko
- Files Hashed: 1
- File Name SHA-256 Hash
- C:\Documents and Settings\Gojko\Desktop\NDA.DOC
- 32449E50929F8F979F90730B2205B52EF76FC7DCB360F421D334FD7026B16ED7
- 99D34442E07C8083EABDA75C9342489077AB77AF085FBD89F39A2FFD900F0267

Primer: Izbor mehanizama zaštite



Primer: Kako “*osigurati* “ hakerski napad?

1.	Ništa ne pečuj
2.	Koristi loše napisane aplikacije
3.	Koristi najviše moguće privilegije
4.	Otvori nepotrebne rupe u *firewalls*
5.	Dopusti interni saobraćaj bez restrikcija
6.	Dopusti saobraćaj spolja bez restrikcije
7.	Ne povećavaj zaštitu servera
8.	Koristi slabe lozinke na više mesta
9.	Koristi zajedničke nalog za servise
10.	Pretpostavi da je sve u redu

Pitanja