CUC 2007

Sigurnost Windows Vista operacijskog sustava

Sveučilište u Zagrebu

Fakultet elektrotehnike i računarstva

Laboratorij za sustave i signale

Tihomir Katić <tihomir.katic@fer.hr>

Sadržaj

- Sigurnost na razini jezgre
- Sigurnost na razini mreže
- Sigurnost na razini korisnika
- Sigurnost kroz enkripciju
- Dodatni sigurnosni elementi

Sigurnost jezgre Vista sustava

- **Sigurnosni razvoj**
  - SDL (*Security Development Lifecycle*)
- **Redizajn arhitekture OS-a**
  - Segmentiranje servisa
  - Izolacija servisa
  - Nove razine servisa (*Local Service* i *Network Service*)
  - Ukinute nepotrebne ovlasti
  - SID (*Security Id*) registriran u ACL (*Access Control List*) štiti resurse servisa

Sigurnost jezgre Vista sustava

- **ASLR (*Address Space Layout Randomization*)**
  - Slučajni odabir lokacije DLL-ova i izvršnih datoteka kod svakog podizanja
  - Prednosti i nedostaci
- **DEP (*Data Execution Prevention*)**
  - Onemogućava pokretanje zlonamjernih kodova
  - Od XP SP2 sustava
  - Sklopovski DEP
  - Programski DEP

Sigurnost jezgre Vista sustava

Provjera integriteta koda

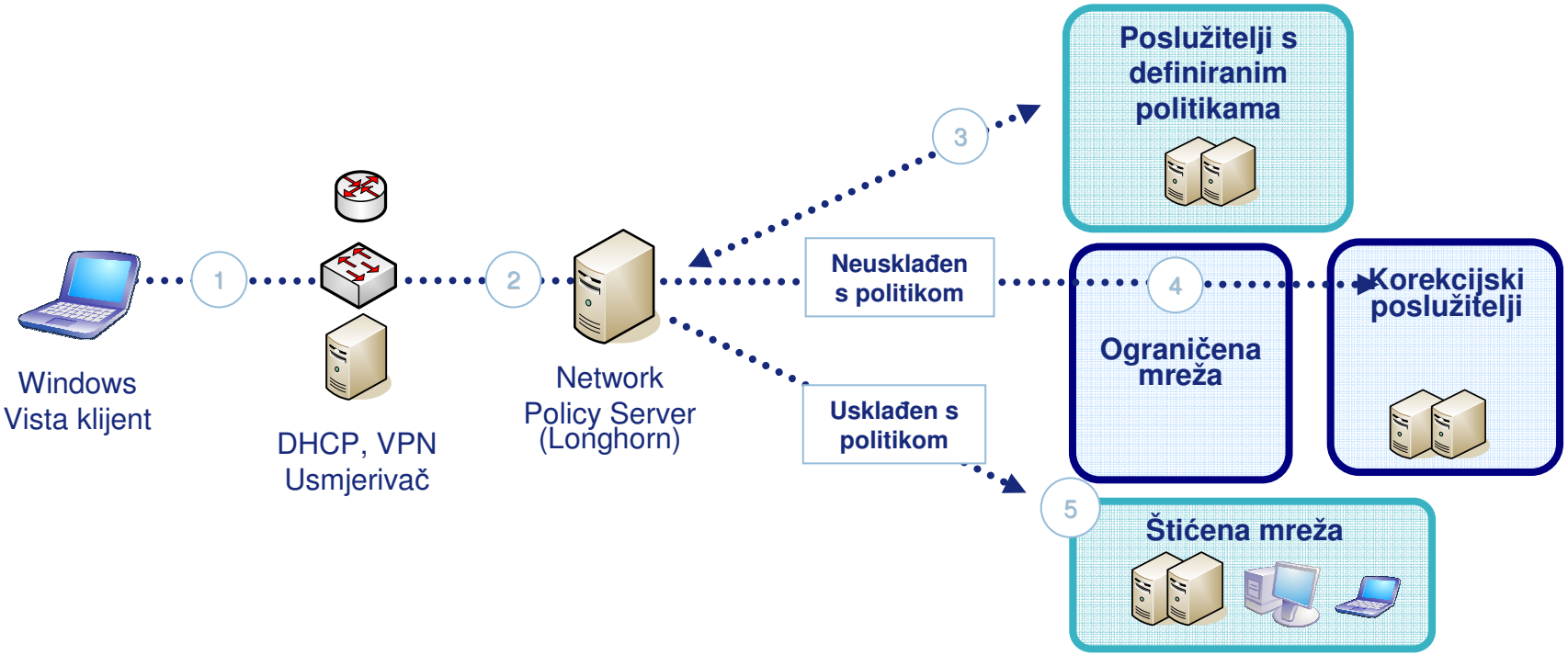
- KMCS (*Kernel Mode Code Signing*) – korištenje pouzdanog *kernel* koda
- OS loader verificira potpise prilikom unosa komponenti u memoriju
  - Provjerene tvrtke
  - CA (*Certificate Authorities*)
- Na x64 64-bitnim platformama
  - Sav jezgrin kod mora biti verificiran
  - Sistemska kontrola
- Na x86 32-bitnim platformama
  - Administrator može prihvatiti sav kod

Sigurnost na razini mreže

- **Zaštita pristupa mreži (NAP – *Network Access Protection*)**
  - Cilj: zaštita mreže i pojedinih računala
  - Poslužitelj (*Network Policy Server*) samo "Longhorn"
  - Politika zasnova na:
    - posjedovanju sigurnosnih zakrpa,
    - obnavljanju virusnih definicija,
    - postojećim aplikacijama, i sl.
  - Privremena mreža – za "popravak" neregularnih računala

Sigurnost na razini mreže

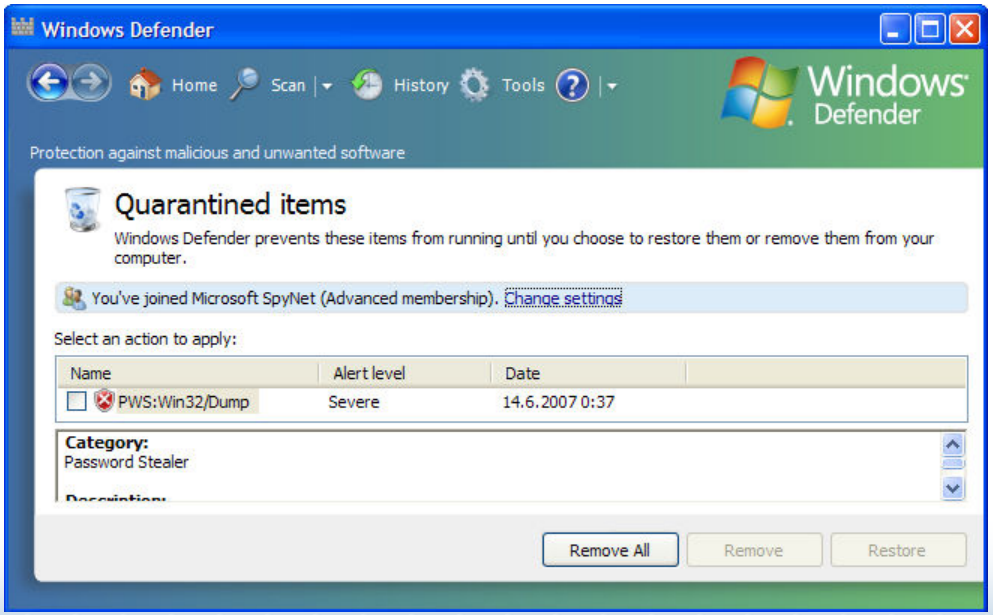
NAP – *Network Access Protection*



Sigurnost na razini mreže

Windows Defender

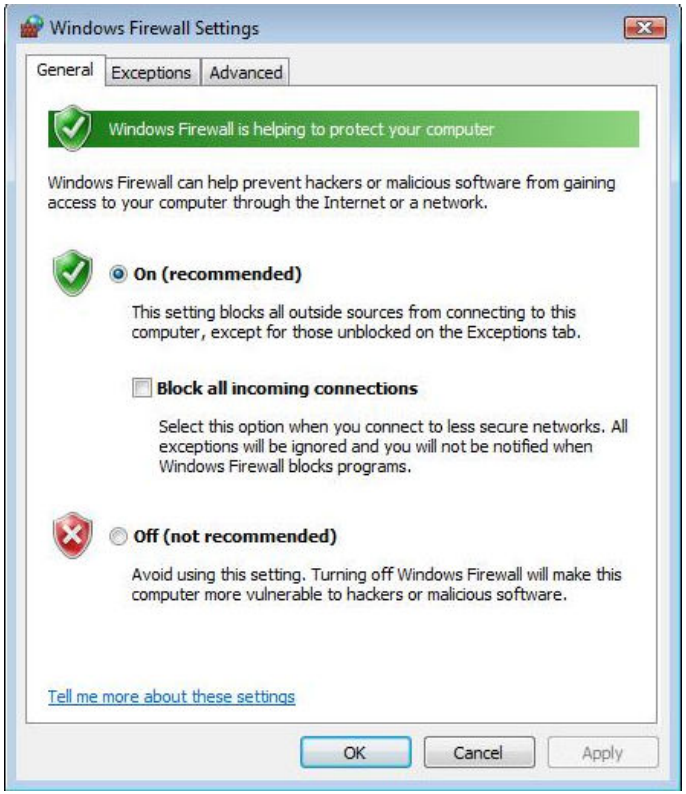
- Detekcija, čišćenje i blokiranje nepoželjnih aplikacija
- Besplatan, raspoloživ i za XP
- SpyNet zajednica
- Relativno slabe detekcije



Sigurnost na razini mreže

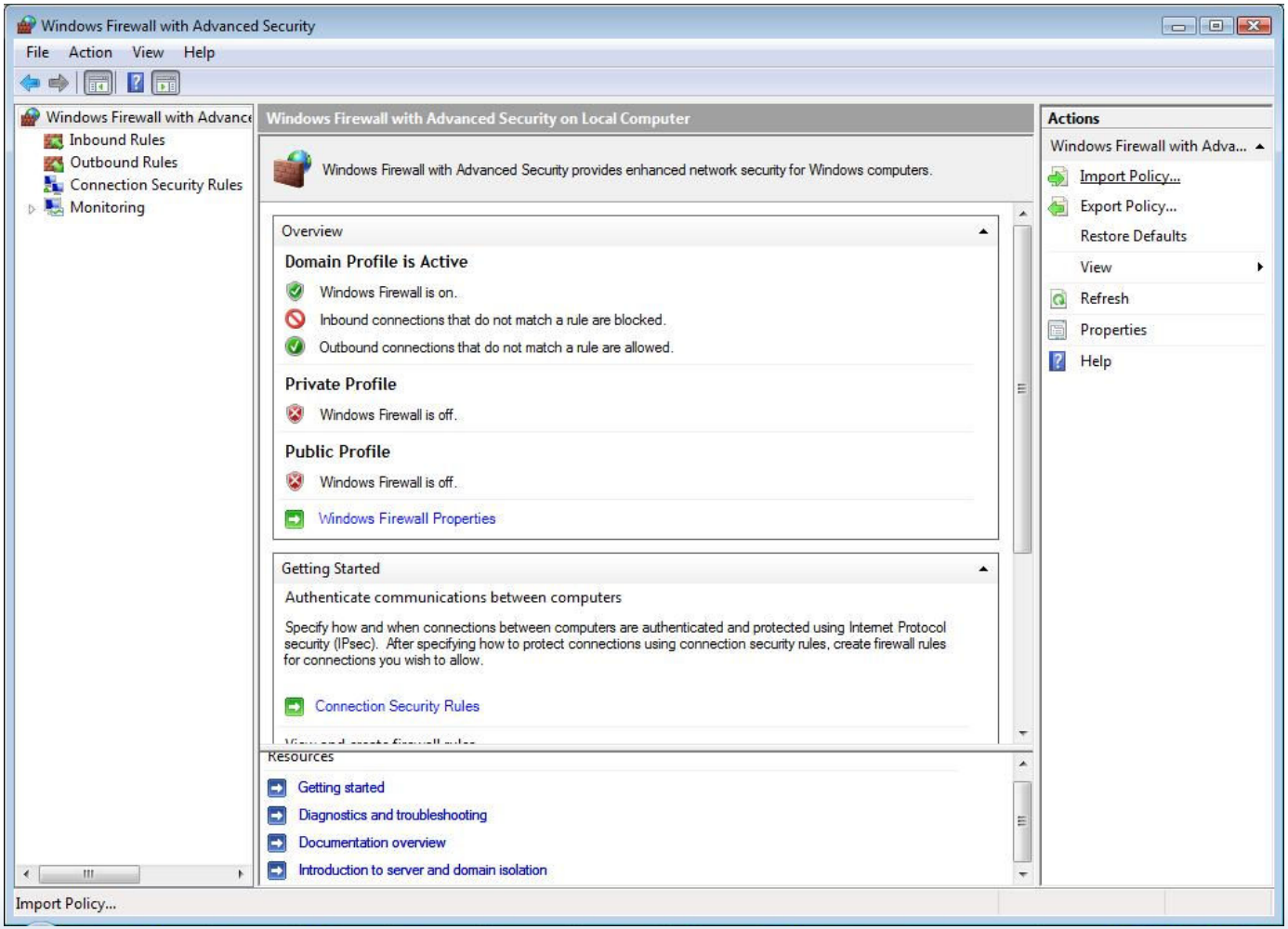
Windows Firewall

- Unapređenje standardnog vatrozida
- Kontrola odlaznog i dolaznog prometa
- Različite politike za različite mreže
- Definiranje pravila (*rules*) po različitim principima:
  - Korisnici, IP adrese,TCP/UDP portovi, ICMP, servisi
- Logiranje prometa



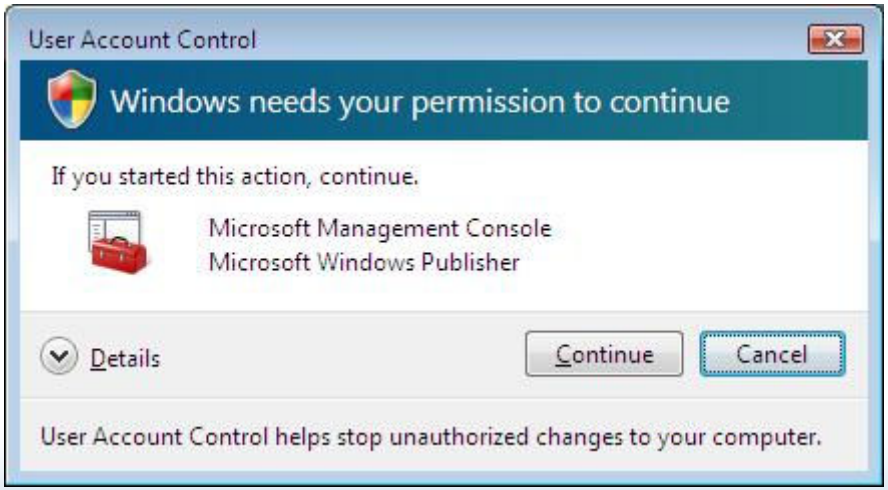
Sigurnost na razini mreže

Windows Firewall



Sigurnost na razini korisnika

- **Kontrola korisničkih ovlasti (UAC)**
  - Razdvaja standardne privilegije i zadatke od onih koji traže admin. ovlasti
  - UIPI (*User Interface Privilege Isloation*)
  - Datoteke i *registry* zapisi imaju definiranu razinu integriteta
  - Procesi niskog integriteta ne mogu pisati u objekte višeg integriteta (MIC - *Mandatory Integrity Control*)



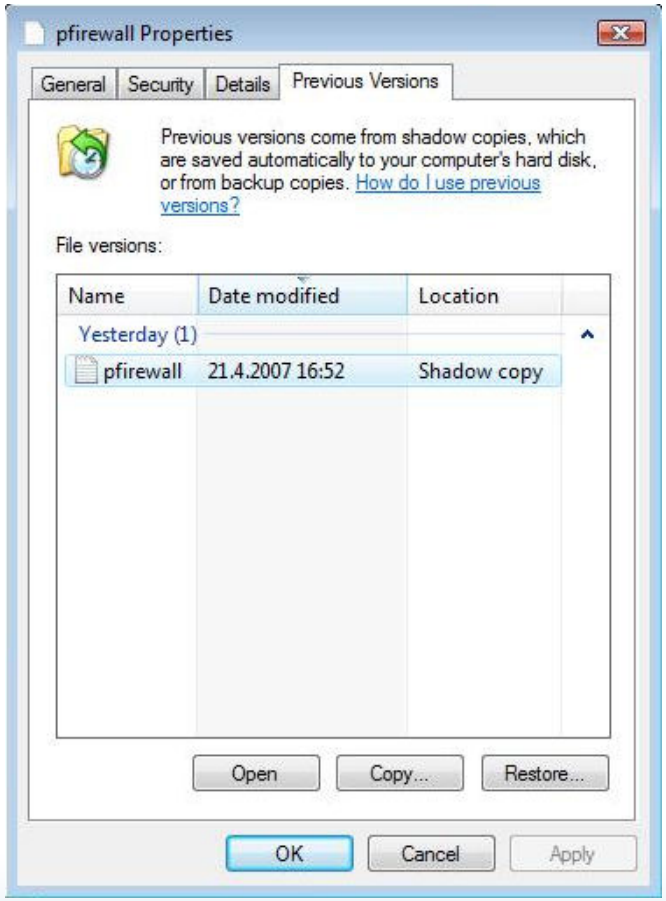
Sigurnost na razini korisnika

- ***Windows Cardspace***
  - Jedinstveno korisničko sučelje za odabir i administraciju identiteta
  - Cilj: kombiniranje različitih identiteta preko različitih Windows programa
  - Višestruki elektronički identiteti: PKI, zaporka, token, …
  - Zajedničko sučelje bez obzira na proizvođača

Sigurnost na razini korisnika

Izrada sigurnosnih kopija

- *Backup & Restore*:
  - Cijeli sustav ili različite vrste podataka
  - Vremensko definiranje
- *Shadow Copy*
  - Windows 2003
  - Automatsko spremanje objekata
  - Verzije dokumenata



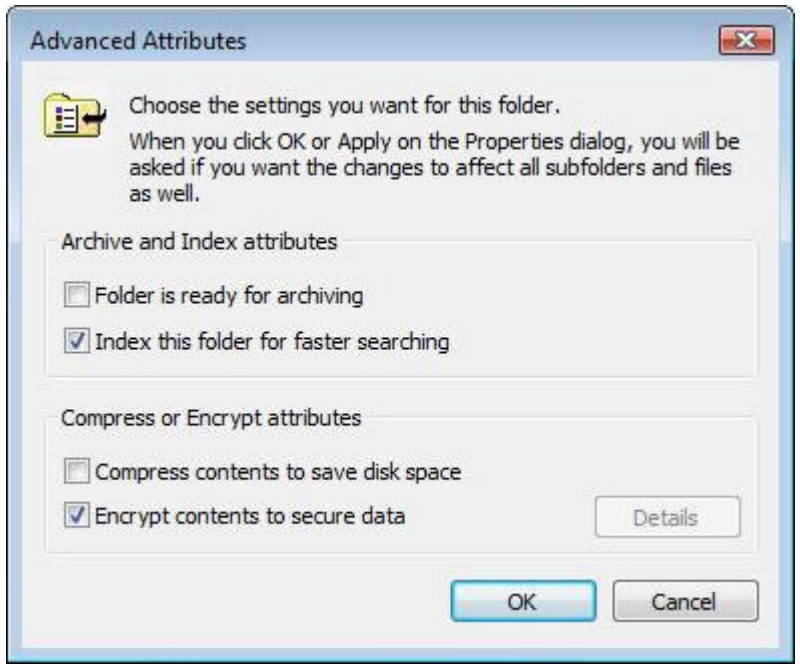
Sigurnost na razini enkripcije

BitLocker šifriranje pogona

- Enkripcija sistemskih particija diska
- Cilj: zaštiti podatke u slučaju krađe računala (najčešće prijenosnog)
- TPM čip uz odgovarajući BIOS – čuva ključeve:
  - nakon 3 neovlaštena pokušaja – zaključava se!
  - nakon 10 neovlaštenih pokušaja – uništava se!!!
- Ostali mehanizmi: USB, PIN ili zaporka

Sigurnost na razini enkripcije

- **EFS *(Encryption File System)***
  - Standardna funkcionalnost
  - Enkripcija na razini direktorija i datoteka
  - Višestruki korisnici resursa
  - Zaštita postoji i dok je računalo upaljeno
  - Zabrana enkripcije Windows datoteka



Dodatni sigurnosni elementi

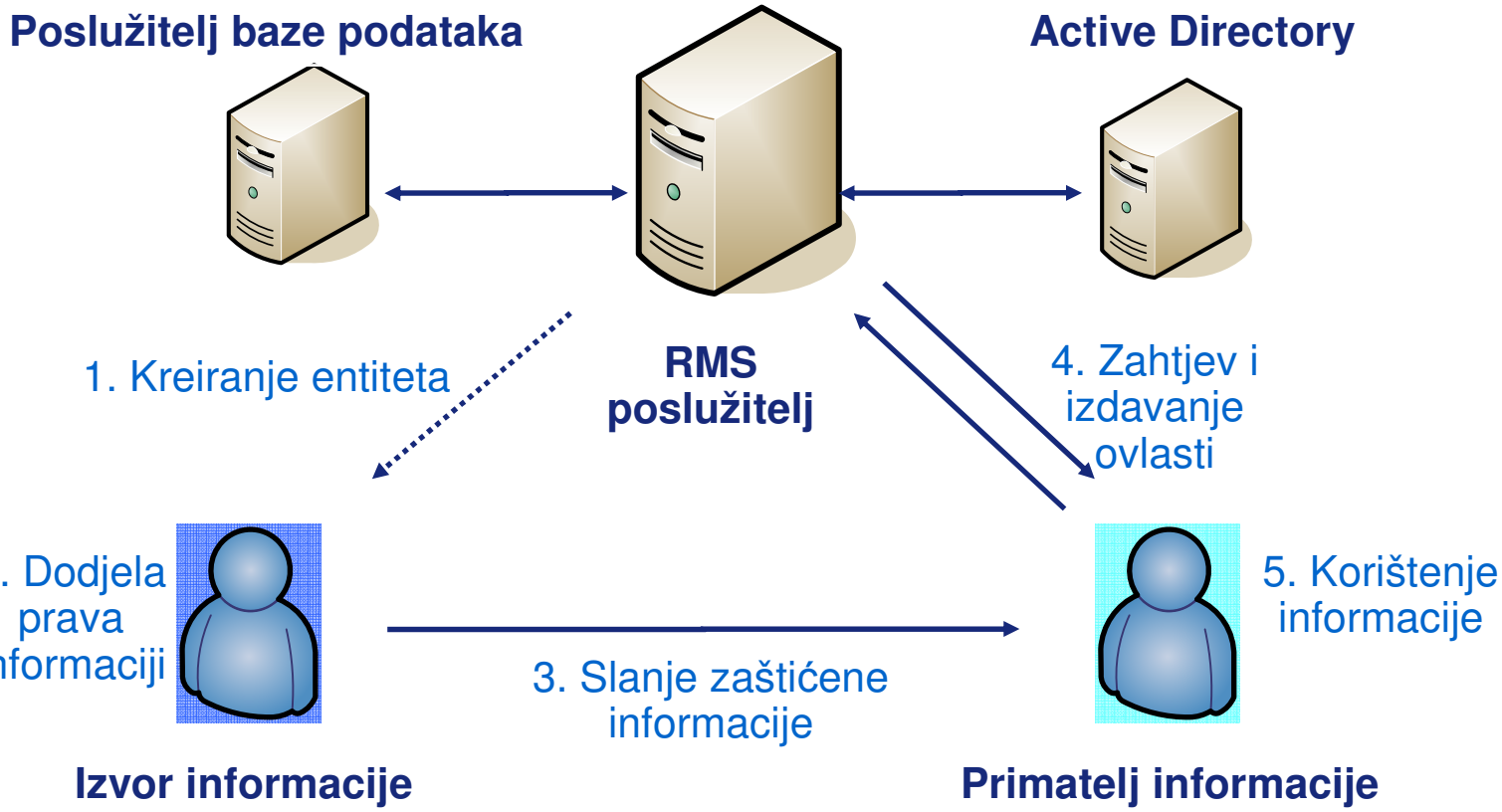
- **SRP - *Software Restriction Policies***
  - Zabrana pokretanja pojedinih programa i datoteka
  - Definiranje pristupa zajedničkim datotekama
- **Kontrola instalacije uređaja – *Device Control***
  - Definiranje korisnika i računala i njihovih dozvole glede instaliranja i korištenja različitih uređaja

Dodatni sigurnosni elementi

- **RMS (*Rights Management Services*)**
  - Nova funkcionalnost
  - Uspostava ovlasti na nivou MS Office dokumenata prema definiranoj politici
  - Moguć razvoj i drugih aplikacija s podrškom za RMS
  - Zaštita podataka od autoriziranih korisnika
  - Ograničenje uređivanja prema korisnicima
  - Zaštita informacije putuje s informacijom

Dodatni sigurnosni elementi

RMS (*Rights Management Services*)



Dodatni sigurnosni elementi

- **Windows LiveOne Care**
  - Komercijalan
  - Objedinjuje:
    - Antivirus
    - Integracija s *antispyware* alatom (Defender)
    - Podešavanje sustava
    - Izrada sigurnosnih kopija
    - Kontrola osvježavanja sustava

- ***Forefront Client Security***
  - Zaštita od neželjenih programa
  - Komercijalna verzija Defender-a sa poslužiteljem, sigurnosnim politikama i antivirusom

Dodatni sigurnosni elementi

Internet Explorer 7

- Zasnovan na UAC (niski integritet)
- *Protected mode* (samo za Vistu)
  - ovlasti pisanja samo za privremene datoteke
- Podrška za internacionalne URL-ove
- Obavezan prikaz web adrese
- Podrška za EV (Extended Validation) SSL certifikate
- Filtar protiv krađe identiteta (Phishing Filter)
  - Dinamička zaštita od lažnih web stranica

Zaključak

- **Vista – najsigurniji Windows sustav**
  - Sigurnost od temelja
  - Nove mrežne funkcionalnosti
  - Bolja sigurnost na razini korisnika
  - Poboljšane metode kriptografske zaštite
  - Nove sigurnosne funkcionalnosti i proizvodi
- **Ipak….**

Pitanja

Hvala na pažnji

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Laboratorij za sustave i signale http://www.lss.hr

Tihomir Katić <Tihomir.Katic@FER.hr>