SIGURNOST U UNIFIED COMMUNICATION OKRUŽENJU

Dalibor Dukić
Tomislav Krajcar

Sedam IT
Primjena informatičkih tehnologija

CISCO

20. i 21. ožujka 2008.
Hotel Dubrovnik Palace
Dubrovnik

Welcome to the Human Network.

CISCO

Sedam IT
Primjena informatičkih tehnologija

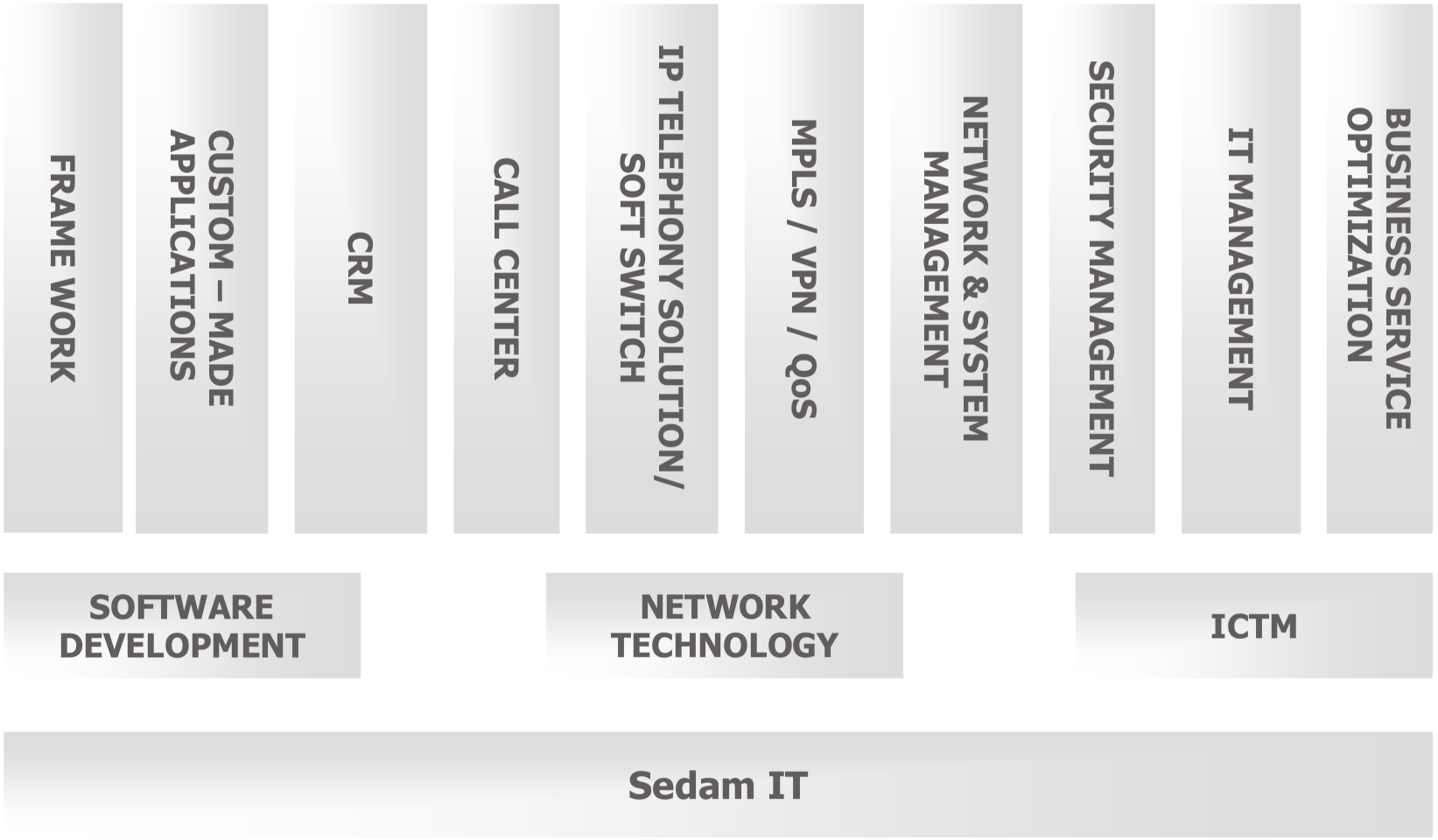
Sadržaj

- **Sedam IT**
- **Sigurnost u UC okruženju**
- **Sigurnosni mehanizmi**
- **Zaključak**

Sedam IT

Primjena informatičkih tehnologija

Sedam IT



Sedam IT
Primjena informatičkih tehnologija

Razvoj programske podrške

Sedam CRM

- **CRM - sustav za upravljanje odnosa s korisnicima**
- **vlastito rješenje, modularni pristup**
  - Korisnički data management modul
  - Modul za katalogizaciju proizvoda i usluga
  - Modul za information channel management
  - Modul Contact management
  - Prodajni module
  - Marketing modul
  - Modul za izvješća
- **Cisco IP Contact Center integracija**
- integracija s poslovnim procesima korisnika i IT okruženjem
- sistemska integracija u Active Directory okruženju (LDAP,...)
- integracija s Microsoft SMS, CA Service Management i HP OpenView produktima

Sedam CRM

CISCO PARTNER ATP – CVP Partner

CISCO PARTNER ATP – IPCC Enterprise Partner

Sedam IT
Primjena informatičkih tehnologija

Mrežne tehnologije

- Rješenja temeljena na proizvodima vodećeg svjetskog proizvođača mrežne opreme, de-facto standarda u mrežnim rješenjima
- Stručnost i široko iskustvo naših certificiranih inženjera jamče kvalitetu naših usluga
- Specijalizirani u IP Communication i VPN Security tehnologijama
- Advanced Technology Partner za IP Contact Center

Iskustvo u aplikacijama novih tehnologija u složenim okruženjima za zahtjevne korisnike:

- **IP telefonija / VoIP**
- **Multichannel IP Contact Center**
- **Sigurnost**
- **MPLS / VPN / QoS**
- **Kvaliteta usluge**
- **upravljanje i nadzor mreže**

Sedam IT
Primjena informatičkih tehnologija

ICTM Management

- **IT management**
  - osigurava optimalnu dostupnost sistema i perfomanse
  - desktop računala, aplikacije, middleware, baze, poslužitelji, mreže
- **Sigurnosni Management**
  - Identity i Access Management
  - security information management
  - threat management
- **Optimizacija poslovnih usluga**
  - prevođenje poslovnih zahtjeva u IT usluge
  - učinkovita primjena usluga u poslovanju
- **Mrežni i sistemski Management**
  - OSS Fault / Performance / Inventory / Ticketing / IT Service Management

ca
vmware
Microsoft GOLD CERTIFIED Partner

Sedam IT
Primjena informatičkih tehnologija

Sadržaj

- Sedam IT
- **Sigurnost u UC okruženju**
- Sigurnosni mehanizmi
- Zaključak

Sedam IT
Primjena informatičkih tehnologija

Hakiranje IP telefonije - povijest

- **1964 – g. John Draper koristi Bosun Whistle (2600Hz), a koji indicira da je telefon spreman za uspostavu novog poziva**
- **Dovelo do otkrića još nekolicine tonova koji su koristili u AT&T**
- **Phreak Book**

Sedam IT
Primjena informatičkih tehnologija

Cijena neimplementiranja Sigurnosti u VoIP okruženju?

- Manjak kvalitete u radu zaposlenika
- Gubitak povjerljivih podataka
- Preslušavanje poziva
- Upadi u data i voice mreže
- Napadi virusa i crva
- Iskorištavanje telefonskog sustava

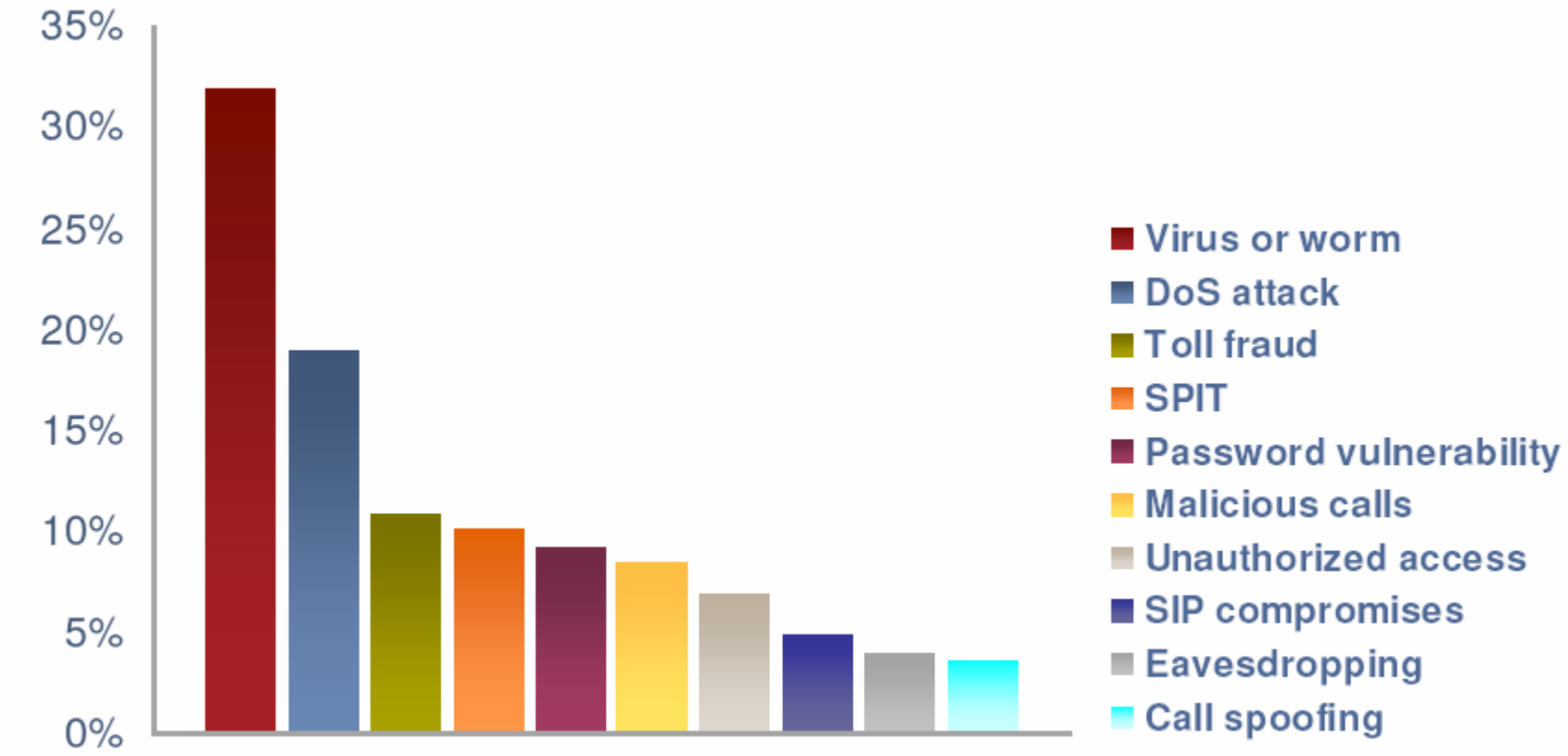
Sedam IT
Primjena informatičkih tehnologija

Najvažnije sigurnosne prijetnje u VoIP okruženju

- DoS – Denial Of Service
- Preslušavanje / upadanje u poziv
- Neovlašteno korištenje sustava / Toll Fraud
- Virusi, crvi, …
- *"Slabe"* Lozinke
- SPIT – Spam over IP Telephony

Sedam IT
Primjena informatičkih tehnologija

Sigurnosne prijetnje u VoIP okruženju

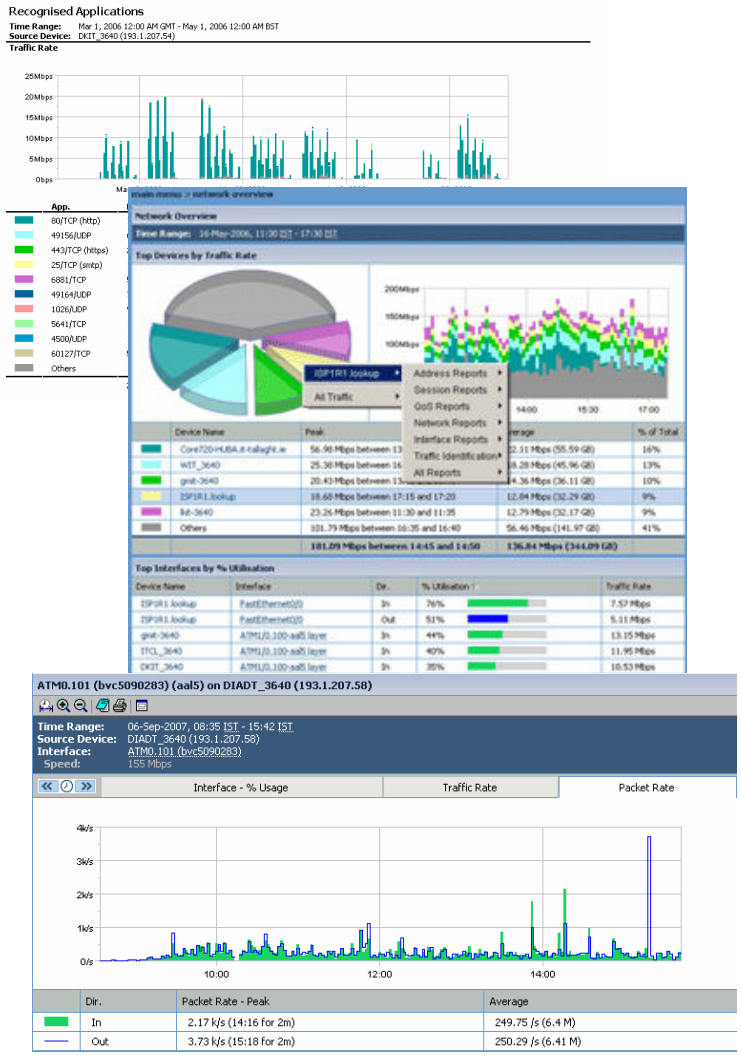


Izvor podataka: NetIQ Survey

Sedam IT
Primjena informatičkih tehnologija

Elementi sigurnosnih rješenja (1)

- **Fluke networks – NetFlow Tracker**
  - Network engineering - Real-time troubleshooting
  - Network security - Forensic
  - Network architecture - Capacity planning



Sedam IT
Primjena informatičkih tehnologija

Elementi sigurnosnih rješenja (2)

- **hardening CallManager OS-a**
  - slabi password – primjer dobrog passworda +@2xtzJ\]SL}
  - bugs & exploits – najnovije zakrpe
  - virusi, trojan and DOS napadi
  - standardni MS Windows exploit
  - CISCO CM 5.x na Linux OS-u
- **hardening IP telefona**
  - Pristup VOICE VLAN-u
  - http, PC VLAN, …
- **TOLL FRAUD**
  - Call-transfer/Call-Forward restrikcije

Sedam IT
Primjena informatičkih tehnologija

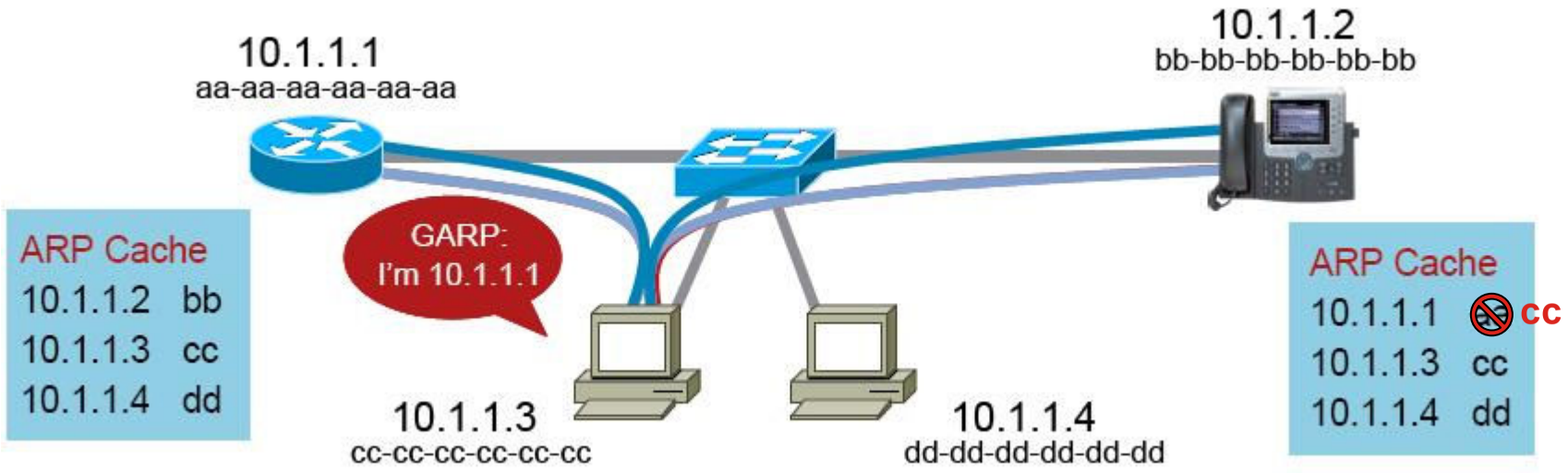
Sadržaj

- Sedam IT
- Sigurnost u UC okruženju
- **Sigurnosni mehanizmi**
- Zaključak

Sedam IT
Primjena informatičkih tehnologija

Sigurnosni mehanizmi

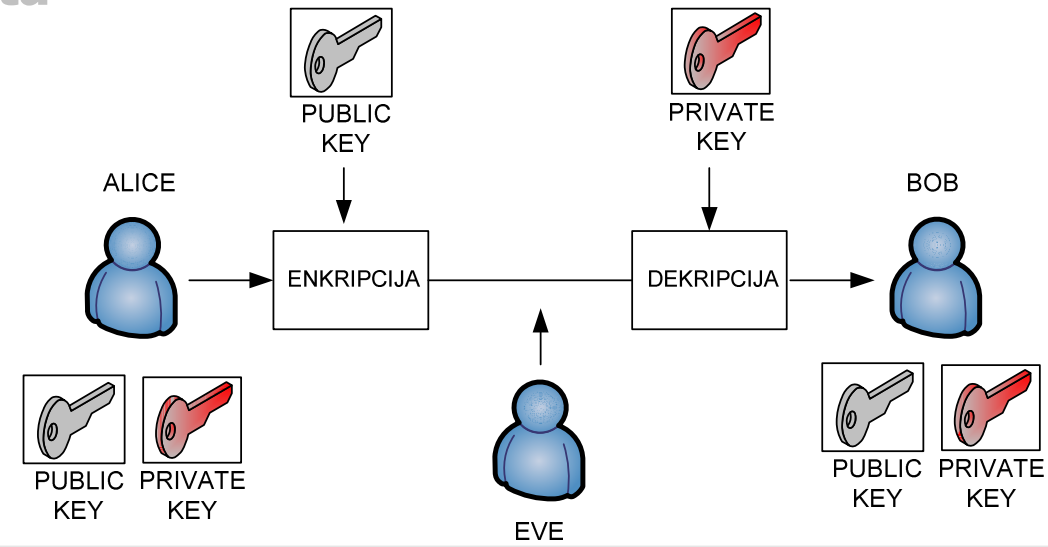
- **Man-in-the-middle napad – Gratuitous ARP**
- **napadač posrednik između telefona i CM-a**
- **alati dostupni na Internetu: ettercap, dsniff**
- **zaštita, DHCP snooping, IP source guard**
- **onemogućiti GARP protokol**



Sedam IT
Primjena informatičkih tehnologija

Kriptografija

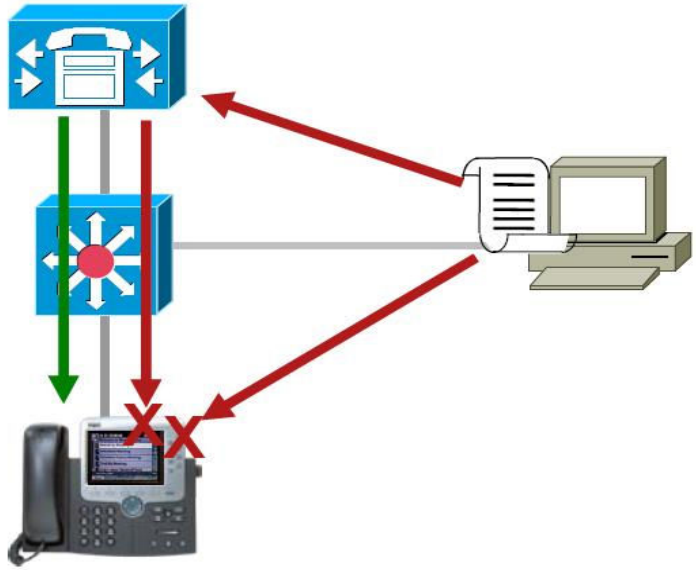
- Sigurna komunikacija preko nesigurnog kanala
- Zahtjevi: tajnost, integritet, autentičnost
- Asimetrični kriptosustav – par javni i tajni ključ
- Infrastruktura javnih ključeva– raspodjela javnih ključeva u obliku digitalnog certifikata
- Digitalni certifikat – veže identitet i javni ključ entiteta



Sedam IT
Primjena informatičkih tehnologija

Autentikacija firmware-a IP telefona

- TFTP - prijenos konfiguracije i firwmare-a na telefon
- nesiguran protokol – plain-text
- image i konfiguracije potpisane od strane CISCO developmenta tima
- CallManager 4.1 sadrži javni ključ
- CCM 5.0 enkriptira TFTP payload



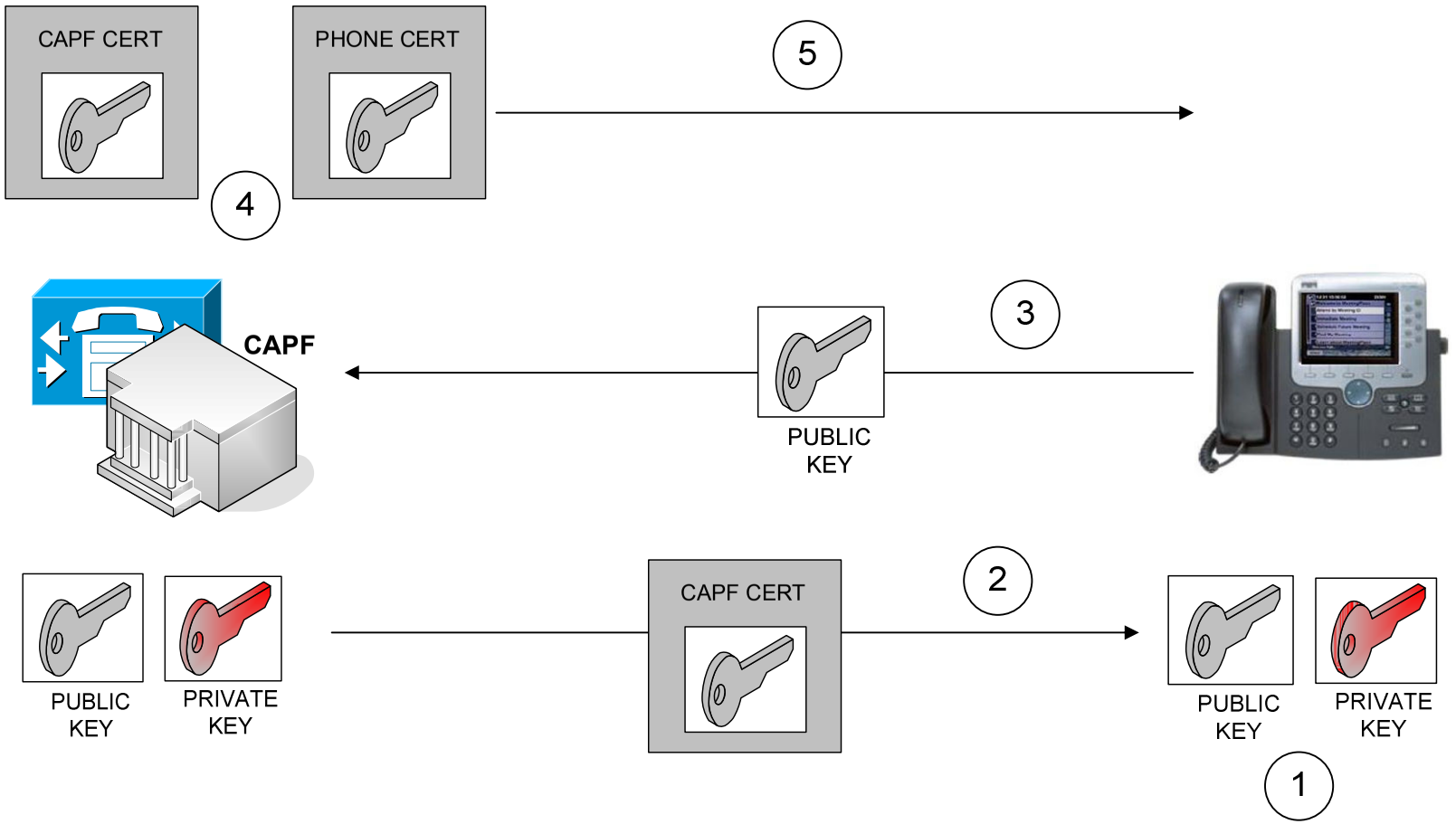
Sedam IT
Primjena informatičkih tehnologija

CAPF – Certificate authority proxy function

- **CAPF na CISCO Call Manager-u**
  - certifikacijsko tijelo
  - izdaje digitalne certifikate za sve sudionike
  - integracija s postojećim PKI sustavom
- **autentikacija telefona**
- **očuvanje integriteta**
- **enkripcija poziva**
  - signalne poruke - TLS (AES 128 bit)
  - voice poruke SRTP (AES 128 bit)

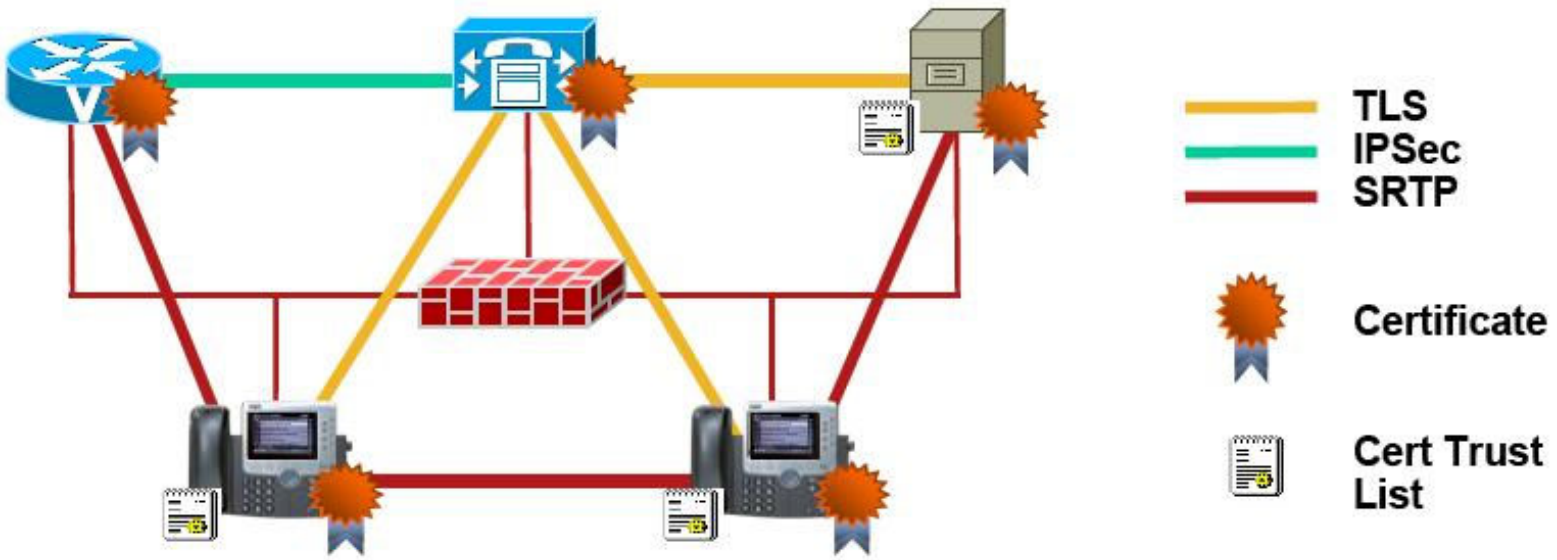
Sedam IT
Primjena informatičkih tehnologija

CAPF – Certificate authority proxy function (2)



Sedam IT
Primjena informatičkih tehnologija

Provjera valjanosti i integritet poziva

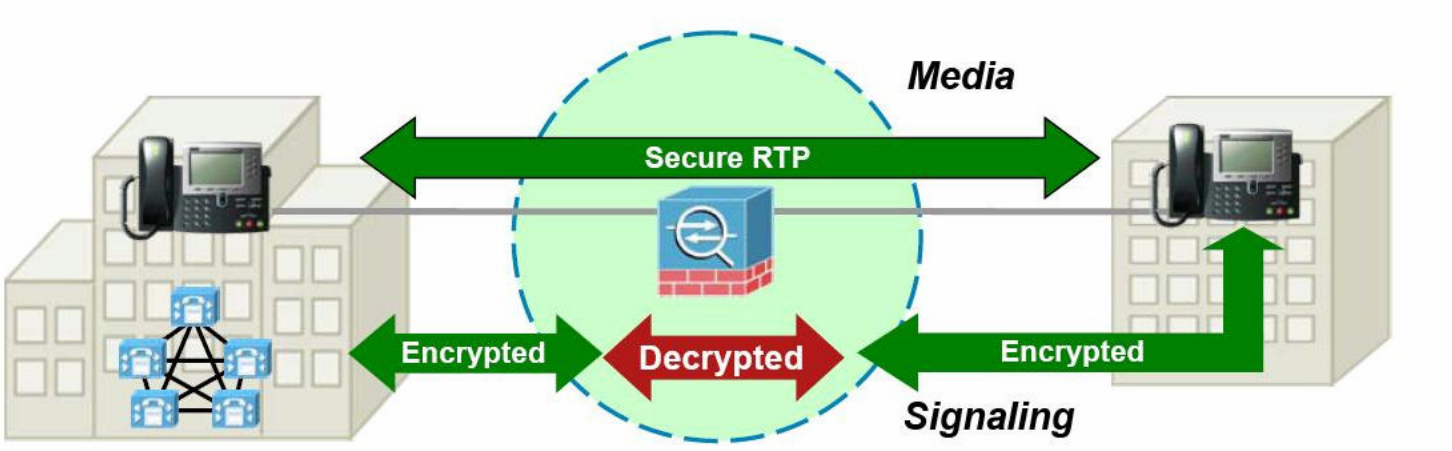


- **povezivanje u CTL trust listu PKI sustava**
- **pametna kartica u obliku USB tokena**
  - par ključeva - certifikat potpisan od CISCO manfacturing CA
  - potpisuje Certificate Trust List

Sedam IT
Primjena informatičkih tehnologija

Cisco ASA 55XX mogućnosti

- **TLS proxy ASA 8.0(2) – inspect enkriptiranih voice poruka**
- **inspect signalnih poruka SIP, SCCP, H.323, MGCP**
- **dinamičko otvaranje portova – application inspection**
- **SIP rate limit**



Sedam IT
Primjena informatičkih tehnologija

Sadržaj

- Sedam IT
- Sigurnost u UC okruženju
- Sigurnosni mehanizmi
- **Zaključak**

Sedam IT
Primjena informatičkih tehnologija

Zaključak

- **Prema istraživanju iz 2002 dvije trećine ljudi na kolodvoru u Londonu spremno je dati svoju lozinku u zamjenu za grafitnu olovku**
- **Sigurnost - sve prisutniji problem današnjice**
- **Cilj:**
  - Minimizirati izloženost sustava napadima
  - Osigurati predaju znanja o sigurnosnim problemima
  - Povećati nivo zaštite i omogućiti obranu na svim slojevima mreže

Sedam IT
Primjena informatičkih tehnologija

Pitanja?

Q & A

Sedam IT
Primjena informatičkih tehnologija