IPsec VPN-ovi

Drumski razbojnici i tuneli: kako sigurno do mreže?

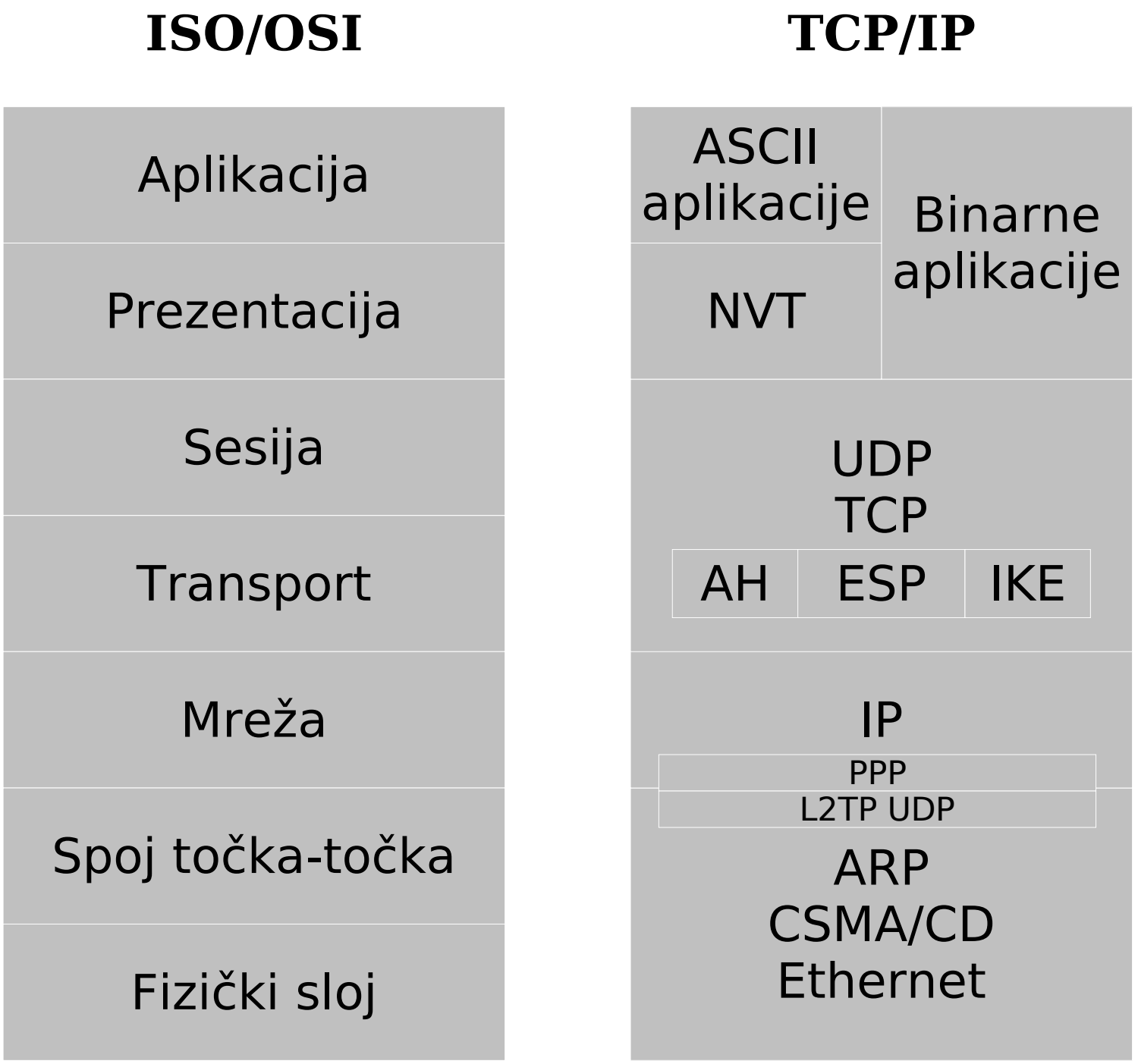
Dobrica Pavlinušić
dpavlin@rot13.org
http://www.rot13.org/~dpavlin/

Što je IPsec?

- Transparentna (aplikacijama), sigurna komunikacija
- Nadogradnja IPv4
- IPsec suite
  - Authentication Header
  - Encapsulating Security Payload
  - Internet Key Exchange

Kriptografija

- Cezarova kriptografija (rot-13?)
- Od čega se sastoji?
  - Jednosmjerne funkcije
  - Jednosmjerne hash funkcije (MD5, SHA)
  - Simetrična enkripcija (AES, CAST, Blowfish)
  - Asimetrična kriptografija (RSA, DSA)
- Perfect Forward Security


ISO/OSI
TCP/IP
Aplikacija
Prezentacija
Sesija
Transport
Mreža
Spoj točka-točka
Fizički sloj
ASCII aplikacije
Binarne aplikacije
NVT
UDP
TCP
AH
ESP
IKE
IP
PPP
L2TP UDP
ARP
CSMA/CD
Ethernet

Što ćemo napraviti?

- Provjeriti da li firewall propušta pakete
- Konfigurirati `ipsecgw`
  - Linux 2.6 kernel (setkey)
  - racoon (IKE)
  - l2tpd (L2TP podrška za udaljene korisnike)
- Konfigurirati `umldns`
  - User Mode Linux za DNS i proxy
- Dodati Windows IPsec/L2TP klijenta

Mrežna arhitektura

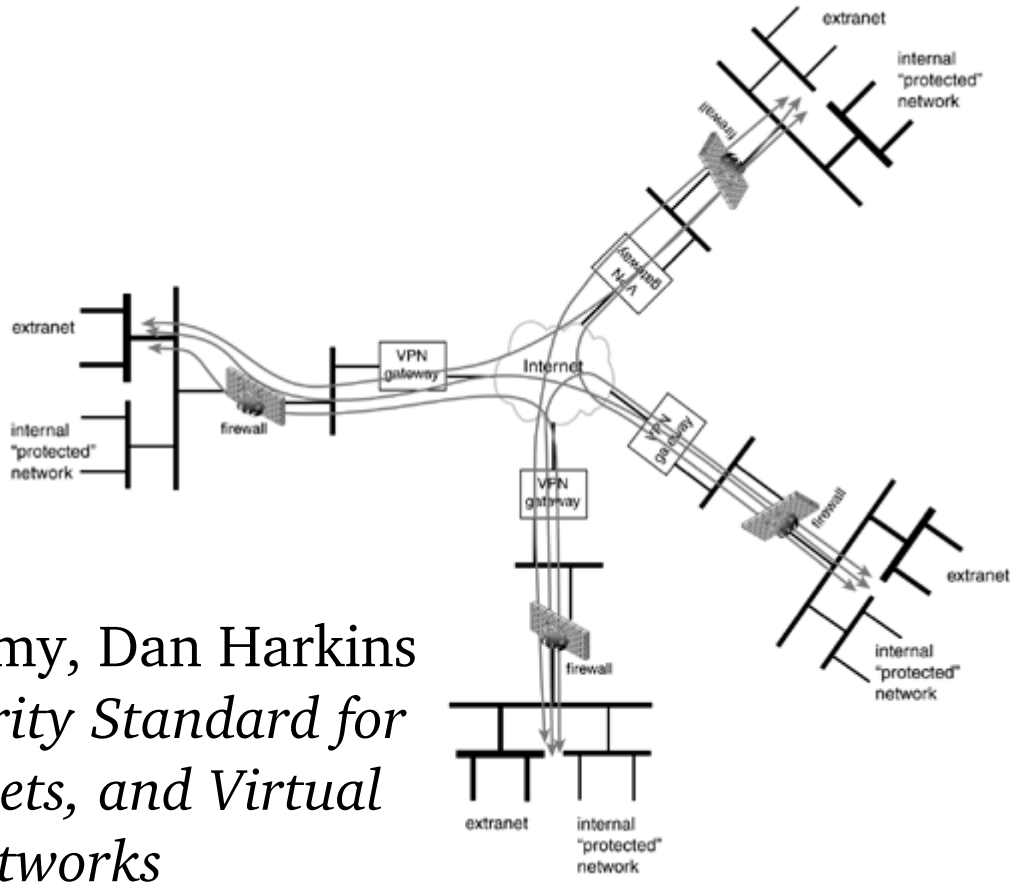
- CheckPoint FW-1
  - aaa.bbb.ccc.ddd
  - IPsec tunnel, pre-shared secret, 3DES, MD5
- Privatna udaljena mreža
  - aaa.bbb.0.0/16
- Privatna lokalna mreža
  - 192.168.220.0/24
- Mobilni klijeti (L2TP/IPsec)
  - 192.168.220.200-192.168.220.250
  - IPsec client, x509 certifikati

Rješavanje problema

- Na nivou mreže
  - tcpdump
  - ethereal
- Na nivou kernel-a
  - unofficial patchevi za netfilter
  - watchdog
  - mailing liste
    - MARC http://marc.theaimsgroup.com/
  - Google

Što nećemo napraviti?

- Kompresija
- Multicast
- PKI (CA/x509)



Naganand Doraswamy, Dan Harkins
IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks
Prentice Hall, March 2003