

Komunikacijski protokoli in omrežna varnost

Uvod in ponovitev osnov predmeta

1

Komunikacijski protokoli in omrežna varnost

- **Profesor:**

dr. Andrej Brodnik (Ljubljana)
doc. dr. Zoran Bosnić (Sežana)



- **Asistent:**

as. dr. Gašper Fele Žorž

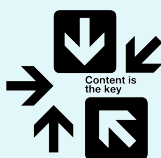
- **Izvedba predmeta:**

- 3 ure predavanj - 2 dela, 2 uri laboratorijskih vaj tedensko
- kontakt: e-mail, govornilne ure, forum na strani predmeta

2

Vsebina predmeta

- ponovitev osnov računalniških komunikacij (ISO/OSI, TCP/IP, protokoli, storitve, varnost),
- nadzor in upravljanje omrežij,
- razpošiljanje (multicasting),
- aplikacije v realnem času,
- varnost: avtentikacija, avtorizacija, beleženje, varni prenosi, VPN, certificiranje, požarni zidovi, IDS sistemi,
- podatki za delovanje omrežja, LDAP,
- IEEE 802.



3

Vsebina predmeta - okvirni načrt

teden	predavanje	DN	SEM
3.10.	Uvod v predmet	1	
10.10.	Uvod v predmet / Zagon računalnika, omrežna konfiguracija	1	
17.10.	Zagon računalnika, omrežna konfiguracija / Nadzor in upravljanje omrežij	1	
24.10.	Nadzor in upravljanje omrežij / Aplikacije v stvarnem času	2	
31.10.	Aplikacije v stvarnem času / Razpošiljanje	2	
7.11.	Razpošiljanje	2	SEM1
14.11.	Varnostni elementi omrežij / vprašanja za kolokvij	3	
21.11.	KOLOKVIJ 1	3	
28.12.	Varnostni elementi omrežij / Avtentikacija, avtorizacija in beleženje (AAA)	3	
5.12.	Avtentikacija, avtorizacija in beleženje (AAA)	3	
12.12.	vabljen predavanje	4	
19.12.	Podatki za delovanje omrežja (LDAP)	4	
26.12.	<<< božično - novoletni prazniki >>>	4	
2.1.	Družina IEEE 802	4	SEM2
9.1.	priloga na kolokvij	4	
16.1.	KOLOKVIJ 2		

4

Obveznosti predmeta

Končna ocena (≥ 50):

• 4 domače naloge:	20%
• seminarski nalogi	40%
• <u>pisni izpit ali 2 kolokvija:</u>	40%
	100%

Obveznosti:

- zapiski: 2 x na predavanje, 1x vaje
- domače naloge ≥ 40 , vsaka domača naloga ≥ 20
- seminarski nalogi ≥ 40 , vsaka seminarska naloga ≥ 20
- pisni izpit ≥ 50 , vsak od kolokvijev ≥ 40

5

Obveznosti predmeta

Pri oceni se še upošteva:

- sodelovanje na forumih
- dopolnjevanje zapiskov
- pomoč kolegom
- ...

6

Literatura

- J. F. Kurose, K. W. Ross: Computer Networking, 5th edition, Addison-Wesley, 2010.
- A. Farrel: The Internet and Its Protocols: A Comparative Approach, Morgan Kaufmann, 2004.
- E. Cole: Network Security Bible, Wiley, 2nd edition, 2009.
- Mani Subramanian: Network Management: An introduction to principles and practice, Addison Wesley Longman, 2000
- RFCji
- ...

7

Ponovitev osnov računalniških komunikacij

8

ISO/OSI model

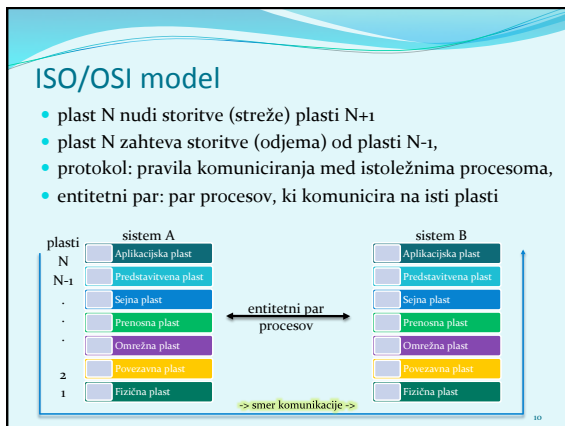
- model vsebuje 7 plasti, ki definirajo sloje sorodnih funkcij komunikacijskega sistema

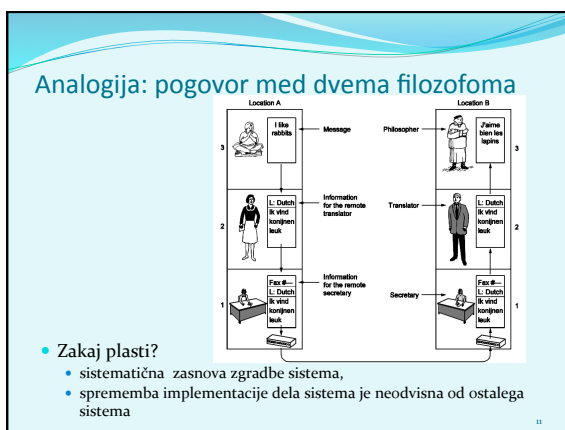
OSI Model

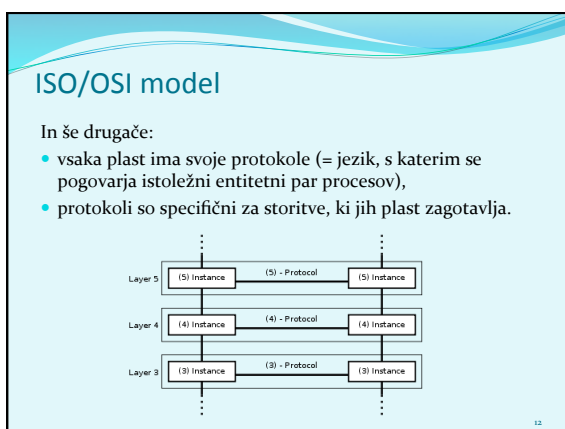
Data Layer	
Data	Application Network Protocol to Application
Data	Presentation Data Representation and Encryption
Data	Session Interhost Communication
Segments	Transport End-to-End Connections and Reliability
Packets	Network Path Determination and IP (Logical Addressing)
Frames	Data Link MAC and LLC (Physical Addressing)
Bits	Physical Media, Voltage, and Binary Representation

aplikacijska plast
predstavitevna plast
sejna plast
transportna plast
omrežna plast
povezavna plast
fizična plast

9







OSI plasti: podrobneje

- **Aplikacijska plast**
 - najbližja uporabi,
 - omogoča interakcijo aplikacije z omrežnimi storitvami,
 - standardne storitve: telnet, FTP, SMTP, SNMP, HTTP
- **Predstavitvena plast**
 - določa pomen podatkov med entitetnima paroma aplikacijske plasti,
 - sintaksa in semantika,
 - določa kodiranje, kompresijo podatkov, varnostne mehanizme

13

OSI plasti

- **Sejna plast**
 - kontrola "dialoga" (množice povezav) med aplikacijama,
 - logično povezovanje med aplikacijami,
 - običajno vgrajena v aplikacije.
- **Transportna plast** (enota: SEGMENT)
 - učinkovit, zanesljiv in transparenten prenos podatkov med uporabnikoma; te storitve zagotavlja višjim plastem,
 - mehanizmi: kontrola pretoka, segmentacija, kontrola napak,
 - povezavni, nepovezavni prenos,
 - TCP, UDP, IPSec, GRE, L2TP, PPP

14

OSI plasti

- **Omrežna plast** (enota: PAKET)
 - usmerjanje(povezavne in nepovezavne storitve)
 - prenos paketov od izvornega do ciljnega računalnika,
 - lahko zagotavlja: zagotovljeno dostavo, pravilno zaporedje, fragmentacijo, izogibanje zamašitvam,
 - usmerjanje, usmerjevalniki, usmerjevalni algoritmi,
 - protokoli: IP, ICMP, IPSec, IGMP, IPX

4 bytes				
version	id	type of service	total length	
identification		flags	fragment offset	
time to live	protocol	source address	header checksum	
destination address				
options		padding		
data				

15

OSI plasti

- **Povezavna plast** (enota: OKVIR)
 - asinhrona/sinhrona komunikacija,
 - fizično naslavljanje: npr MAC naslov,
 - zaznavanje in odpravljanje napak (pariteta, CRC, checksum)
 - kontrola pretoka, okvirjanje
 - protokoli: Ethernet, PPP, Frame Relay

16

OSI plasti

- **Fizična plast**
 - prenos bitov po kanalu (baker/optika/brezžično),
 - digitalni, analogni medij,
 - UTP, optika, koaksialni kabli, brezžična omrežja,
 - RS-232, T1, E1, 802.11b/g, USB, Bluetooth

17

OSI model in model TCP/IP

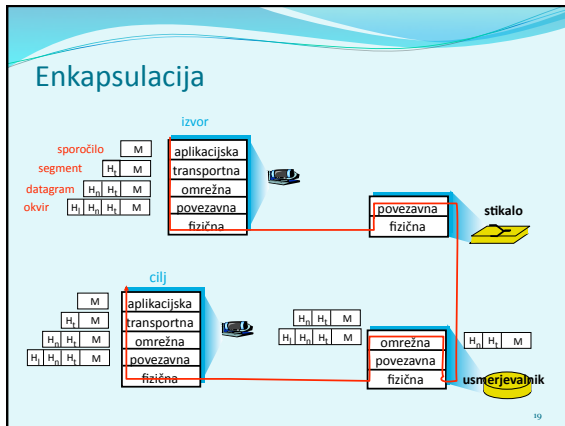
7	Application	Application
6	Presentation	
5	Session	
4	Transport	Transport
3	Network	Internet
2	Data Link	Network Interface
1	Physical	

OSI Reference Model TCP/IP

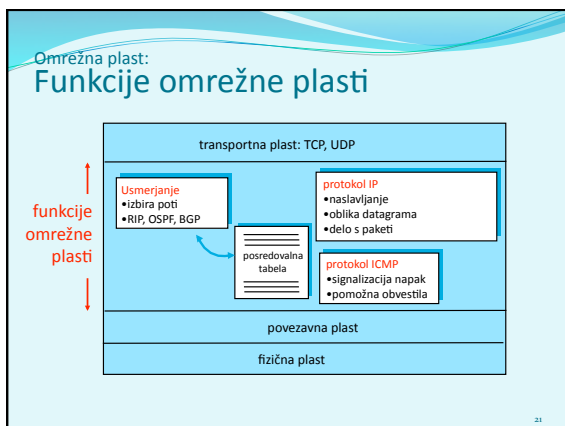
Primerjava modelov:

- ISO OSI: **de iure**, teoretičen, sistematičen, pomanjkanje imlementacij (izdelkov),
- TCP/IP: **de facto**, prilagodljiv, nesistematičen, fleksibilen, veliko izdelkov

18



Omrežna in transportna plast: podrobneje



Omrežna plast:
Usmerjevalniki

- uporaba usmerjevalnih (*routing*) protokolov (RIP, OSPF, BGP)
- posredovanje (*forwarding*) datagramov med vhodnimi in izhodnimi vrati

The diagram illustrates the internal structure of a router. It features multiple input ports on the left and multiple output ports on the right. These ports are connected to a central switching fabric. A routing processor is positioned below the switching fabric, with bidirectional arrows indicating its interaction with the fabric. The entire structure is enclosed in a red-bordered box.

22

Omrežna plast:
Primerjava aktivne opreme

- **usmerjevalnik (router):**
 - naprava, ki deluje na OMREŽNI plasti
 - vzdržujejo usmerjevalne tabele, izvajajo usmerjevalne algoritme,
- **stikalo (switch):**
 - naprava, ki deluje na POVEZAVNI plasti,
 - vzdržujejo tabele za preklapljanje, izvajajo filtriranje in odkrivanje omrežja
- **hub:**
 - naprava, ki deluje na fizični plasti, danes niso več v rabi

The diagram shows four vertical columns representing network devices. From left to right: Host, Bridge, Router, and Host. Each column has five ports numbered 1 to 5. Red lines connect the ports between adjacent devices: Host 1-2 to Bridge 1-2, Bridge 2-3 to Router 1-2, and Router 2-3 to Host 1-2. The Router's top port (3) is also connected to its bottom port (1).

23

Omrežna plast:
IPv4

- protokol na omrežni (3.) plasti OSI modela
- **IPv4 naslov** je 32 bitni naslov vmesnika. Primer:
1100001 0000010 0000001 01000010
ali
193.2.1.66
- **Podomrežje** je množica IP naslovov, ki so med seboj dosegljivi brez posredovanja usmerjevalnika. Maska (32 bitov) določa del IP naslova, ki predstavlja naslov podomrežja. Primer:
11111 11111 110000 0000000 (255.255.255.240)
pomeni, da prvih 20 bitov IP naslova predstavlja naslov omrežja, preostalih 12 pa naslov vmesnika.


24

Omrežna plast:
Vaja!

- Podana sta IP naslov nekega vmesnika in maska podomrežja:
193.90.230.25 /20

Kakšen je naslov podomrežja?

Kakšen je naslov vmesnika?



25

Omrežna plast:
IPv6

- Prednosti:**
 - večji naslovni prostor: 128 bitov
 - hitro usmerjanje in posredovanje ter QoS omogoča že format glave, fragmentacije ni,
 - implementacija IPSec znotraj IPv6 obvezna.
- Naslov:** sestavljen iz 64 bitov za ID podomrežja + 64 bitov za ID vmesnika

```
001000011101010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010
```

Zapisan šestnajstičsko, ločeno z dvopičji

21DA:00D3:0000:0000:02AA:00FF:FE28:9C5A ali (brez vodilnih ničel)

21DA:D3:0:0:2AA:FF:FE28:9C5A ali (izpustimo bloke ničel)

21DA:D3::2AA:FF:FE28:9C5A

26


Omrežna plast:
Primerjava IPv4 in IPv6

0 4 8 12 16 20 24 28 31			
Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			

0 4 8 12 16 20 24 28 32 36 40 44 48 52 56 60 63						
Version	Traffic Class	Flow Label		Payload Length	Next Header	Hop Limit
Source Address						
Destination Address						

27

Omrežna plast:
IPv6 - načini naslavljanja



- **UNICAST:**
naslavljanje posameznega omrežnega vmesnika
- **MULTICAST:**
naslavljanje skupine omrežnih vmesnikov, dostava vsem vmesnikom v množici
- **ANYCAST:**
je naslov množice vmesnikov, dostava se izvede enemu (najbližjemu?) vmesniku iz te množice

Vsak vmesnik ima lahko več naslovov različnih tipov.
 (BROADCAST naslovov - v IPv6 ni več!)

28

Omrežna plast:
IPv6 - vrste unicast naslovov

- 1.) **globalni unicast** (= javni naslovi)

48 bitov	16 bitov	64 bitov
Registev	Podomrežje	Naslov vmesnika
001	Usmerjevalna predpona	Podomrežje
- 2.) **posebni naslovi** (localhost ::1, nedefiniran 0::0, IPv4 naslovi)
- 3.) **link-local naslovi** (znotraj 1 povezave, adhoc omrežja)

10 bitov	54 bitov	64 bits
FE80::/64	1111 1110 10	000...000
		Naslov vmesnika
- 4.) **site-local** (=privatni naslovi, znotraj org., se ne usmerjajo, FEC0::/10)
- 5.) **unique-local** (=privatni naslovi, dodeli registrar, znotraj org., se ne usmerjajo, so bolj strukturirani, FC00::/7)

29

Omrežna plast:
IPv6 - multicast


- 1.) FF02::1 (link local: vsi VMESNIKI)
- 2.) FF02::2 (link local: vsi USMERJEVALNIKI)
- 3.) Struktura naslova:

128 Bits	
6-bits	4-bits
1111 1111	Lifetime
Lifetime	Scope
0 // Permanent	1 Node
1 // Temporary	2 Link
	3 Site
	4 Organization
	E Global

30


Omrežna plast:
IPv6 v omrežjih IPv4

- 1.) **dual-stack:** usmerjevalniki poznajo IPv4 in IPv6. Z možnimi govori IPv6, z ostalimi pa IPv4.
- 2.) **tuneliranje:** IPv6 paket zapakiramo v enega ali več IPv4 paketov kot podatke.



31

Omrežna plast:
Usmerjanje

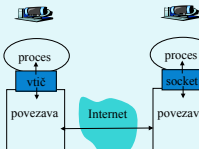


- **NAČINI**
 - statično / dinamično (upoštevanje razmer v omrežju)
 - centralizirano / porazdeljeno (glede na poznavanje stanja celega omrežja)
 - po eni poti / po več poteh
- **IMPLEMENTACIJE:**
 - z vektorjem razdalj (RIP, IGRP, EIGRP)
 - glede na stanje omrežja (OSPF, IS-IS)

32

Transportna plast:
Funkcionalnosti

- **Naloga:**
 - Sprejem sporočila od aplikacije
 - Sestavljanje segmentov v sporočilo za omrežno plast
 - Predaja aplikacijski plasti
- **Vtič**
 - vmesnik med transportno in aplikacijsko plastjo,
 - proces naslovimo z **IP številko** in **številko vrat** (www: 80, SMTP: 25, DNS: 53, POP3: 110).



33

Transportna plast:
Povezavno in nepovezavno

- **Povezavna in nepovezavna komunikacija**
 - TCP in UDP; ter ostali protokoli
 - vzpostavitev, **prenos**, podiranje – povezave
- **Potrjevanje**
 - v protokolu (TCP)
 - v aplikaciji (UDP)
 - neposredno (ACK in NACK)
 - posredno (samo ACK, sklepamo na podlagi števil paketa)
 - sprotno potrjevanje: naslednji paket se pošlje šele po prejemu potrditve
 - tekoče pošiljanje: ne čaka se na potrditve.

34

Transportna plast:
TCP in UDP

The TCP Segment Format

	Bit 15	Bit 16		Bit 32	
Source Port (16)			Destination Port (16)		
Sequence Number (32)					
Acknowledgment Number (32)					
Header Length (4)	Reserved (6)	Flags (8)	Window (16)		
Checksum (16)			Urgent Pointer (16)		
Options (0 or 32)					
Data (variable)					

The UDP Segment Format

	Bit 15	Bit 16		Bit 32	
Source Port (16)			Destination Port (16)		
Length (16)			Checksum (16)		
Data (variable)					

35

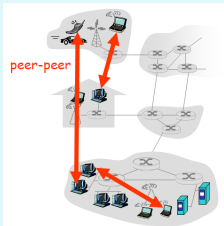
Aplikacijska plast:

- **Klasične storitve – odjemalec-strežnik**
 - telnet, ssh; rdesktop
 - ftp, sftp
 - WWW in HTTP,
 - SMTP, POP3, IMAP, MAPI
 - DNS,
 - SNMP, LDAP, RADIUS, ...
 - ...

36

Aplikacijska plast:

- **Novejše storitve – P2P:**
 - komunikacija poljubnih dveh končnih sistemov,
 - strežniki niso nenehno prižgani,
 - prekinjene povezave / spremembe IP naslovov,
 - primeri: BitTorrent, Skype



peer-peer

37

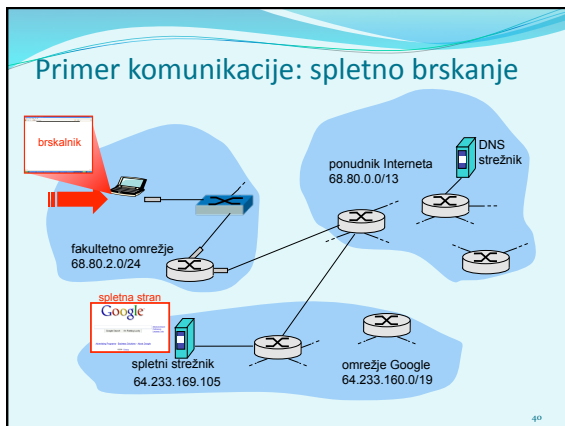
Omrežna in transportna plast:
Iz preteklosti za prihodnost

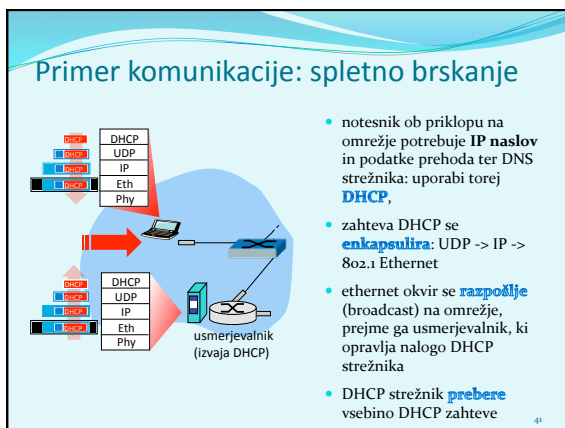
- **Problem:** pomanjkanje IPv4 naslovov
 - izkoristek zasebnih naslovnih prostorov
 - NAT prehodi – običajno hkrati požarni zidovi
 - preprosto v odjemalec-strežnik sistemih
 - v P2P potrebujemo preslikovalni naslov v zunanem svetu
- V IPv6 NAT prehodi niso potrebni

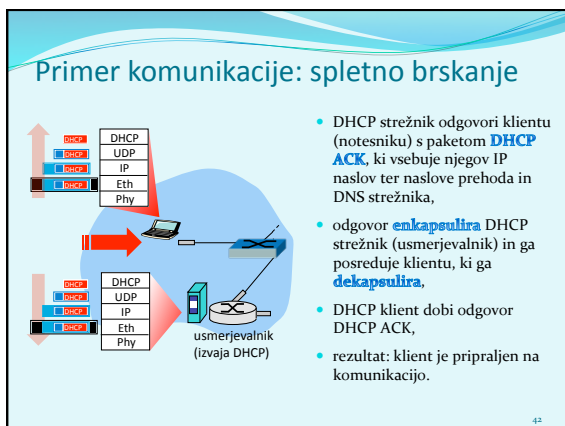
38

Primer komunikacije

39







Primer komunikacije: spletno brskanje

- pred pošiljanjem zahtevka HTTP, potrebujemo IP naslov strežnika **www.google.com**: **uporabi DNS**,
- enkapsulacija zahtevka DNS: UDP - > IP -> Ethernet. Potrebujemo MAC naslov usmerjevalnika: **uporabi ARP**
- razpošljemo **zahtevek ARP**, usmerjevalnik odgovori z **ARP odgovorom**, ki hrani njegov MAC naslov,
- klient sedaj pozna MAC naslov prehoda, ki mu lahko **pošlje DNS zahtevek**.

43

Primer komunikacije: spletno brskanje

- IP datagram z **zahtevkom DNS** se posreduje usmerjevalniku
- IP datagram se posreduje **DNS strežniku**, ki je v omrežju ponudnika (z uporabo usmerjevalnih protokolov RIP, OSPF, IS-IS ali BGP),
- DNS strežnik **dekapsulira** zahtevek in posreduje uporabniku IP naslov spletnega strežnika **www.google.com**

44

Primer komunikacije: spletno brskanje

- za pošiljanje **HTTP zahtevka**, klient najprej naslovi **TCP vtič** spletnega strežnika,
- **TCP SYN** segment se preko omrežja usmeri do spletnega strežnika
- spletni strežnik odgovori s **TCP SYNACK** (potrditev rokovanja),
- sedaj je **TCP povezava vzpostavljena!**

45

Primer komunikacije: spletno brskanje

- **HTTP zahtevek** se pošlje na **TCP vtič** spletnega strežnika,
- **IP datagram**, kivebuje spletno zahtevo po strani **www.google.com** se usmeri k spletnemu strežniku
- spletni strežnik odgovori s **HTTP REPLY**, ki vsebuje vsebino strani
- IP datagram s stranjo se usmeri h klientu,
- **WWW stran je kočno prikazana!**

46

Zajem podatkov iz omrežja

47

Zajem podatkov iz omrežja: primer DHCP

zahtevek

```
Message type: Boot Request (1)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0xb3a11b7
Seconds elapsed: 0
Roopp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wiatron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OR)
Option: (t=53, l=1) DHCP Message Type = DHCP Request
Option: (t=61, l=1) Client Identifier
Length: 7; Value: 810016323688a
Hardware type: Ethernet
Client MAC address: Wiatron_23:68:8a (00:16:d3:23:68:8a)
Option: (t=50, l=4) Requested IP Address = 192.168.1.101
Option: (t=42, l=5) Host Name = "hadu"
Option: (t=5) Parameter Request List
Length: 11; Value: 010f30627e5f19192b
0 = Subnet Mask; 5 = Domain Name
1 = Router; 6 = Domain Name Server
44 = NetBIOS over TCP/IP Name Server
```

odgovor

```
Message type: Boot Reply (2)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0xb3a11b7
Seconds elapsed: 0
Roopp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.101 (192.168.1.101)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 192.168.1.1 (192.168.1.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wiatron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OR)
Option: (t=53, l=1) DHCP Message Type = DHCP ACK
Option: (t=54, l=4) Server Identifier = 192.168.1.1
Option: (t=1, l=4) Subnet Mask = 255.255.255.0
Option: (t=1, l=4) Router = 192.168.1.1
Option: (t=61, l=5) Domain Name Server
Length: 12; Value: 445747e2445749244574092;
IP Address: 68.87.73.242;
IP Address: 68.87.73.242;
IP Address: 68.87.64.144
Option: (t=15, l=0) Domain Name = "hadu.ma.concast.net."
```

48

Omrežna varnost



49

Omrežna varnost

- **Je področje, ki:**
 - analizira možnosti vdorov v sisteme,
 - načrtuje tehnike obrambe pred napadi,
 - snuje varne arhitekture, ki so odporne pred vdori.
- **Internet ni bil snovan ozirajoč se na varnost!**
 - vizija interneta je sprva bila: "To je skupina ljudi, ki si med seboj zaupajo in je priključena na skupno omrežje"
 - pri izdelavi protokola so ga proizvajalci delali z metodologijo "krpanja",
 - varnostne mehanizme je potrebno upoštevati na vseh plasteh OSI modela.

50

Kako lahko vdiralec škoduje sistemu?

Ima veliko možnih pristopov in tehnik!

- **prisluškovanje:** prestrezanje sporočil,
- aktivno **ponarejanje** sporočil v neki komunikaciji,
- **kraja identitete (impersonacija):** ponaredi lahko izvorni naslov ali poljubno drugo vsebino paketa,
- **prevzem povezave (hijacking):** odstrani pravega pošiljatelja ali prejemnika iz komunikacije in prevzame njegovo vlogo,
- **"denial of service":** onemogoči uporabo regularne storitve (npr. s tem, da jo preobremeni)



51



- ### Elementi varne komunikacije
- **Zaupnost** – kdo sme prebrati? (enkripcija)
 - **Avtentikacija** – dokaži, da si res ti (identifikacija – povej, kdo si, brez dokaza)
 - **Razpoložljivost in nadzor dostopa** – preprečevanje nelegitimne rabe virov (*avtorizacija* – ugotavljanje, ali nekaj smeš storiti, *accounting* – storitve beleženja uporabe)
 - **Integriteta sporočila** – je bilo med prenosom spremenjeno?
 - **Preprečevanje zanikanja** (nonrepudiation) – res si poslal / res si prejel.
- V praksi:
- požarni zidovi, intrusion detection sistemi,
 - varnost na aplikacijski, transportni, omrežni in povezavni plasti
- 53

Avtentikacija

Prepričamo se o dejanski identiteti osebe - sogovornika v komunikaciji.

PRISTOPI:

- Challenge-response (izziv-odgovor),
- zaupamo tretji strani,
- avtentikacija s sistemom javnih ključev.

54

Zaupnost sporočil: kriptiranje (zakrivanje) vsebine

Je način obrambe pred **pasivnimi** vdiralci (prisluškovalci) in **aktivnimi** vdiralci (ponarejevalci).

Sporočilo **P** kriptiramo s ključem **E()** - dobimo **kriptogram E(P)**. Kriptogram **E(P)** predelamo v izvorno obliko s ključem **D()**, dobimo izvorno sporočilo **D(E(P))=P**.

Vrste metod:

- **substitucijske** (menjava znakov) / **transpozicijske** (vrstni red znakov)
- **simetrične (E=D)**, npr. DES, AES) / **asimetrične (E≠D)**, npr. RSA, ECC

55

Vrste kriptografije

- Kriptografija uporablja ključe
 - kriptirni algoritem je običajno znan vsem,
 - tajni so le ključi
 - kriptiranje: skrivanje vsebine
 - kriptanaliza ("razbijanje" kode)
- Kriptografija z javnimi ključi
 - $E() \neq D()$: dva ključa – javnega in zasebnega
- Simetrična kriptografija
 - $E() = D()$: samo en ključ
- Zgoščevalne funkcije – niso kriptografija
 - ne uporabljajo ključev. Kako so lahko koristne?



56

Kriptografija z javnimi ključi

- **PKI (Public Key Infrastructure)** je sistem, ki opredeljuje izdelavo, upravljanje, distribucijo, shranjevanje in preklid digitalnih certifikatov.
- Uporabnike avtenticiramo s pomočjo javnih ključev, ki so overovljeni s strani certifikacijske agencije (*certificate authority, CA*).



57

Kriptografija z javnimi ključi

- Algoritmi za kriptiranje z javnimi ključi so asimetrični, E= enkripcijski ključ, D= dekripcijski ključ, velja $E \neq D$
- Ključa **E** in **D** morata izpolnjevati naslednje zahteve glede kriptiranja sporočila **S**:
 - $D(E(S)) = D(E(S)) = S$
 - Iz znanih **S** in **E(S)** mora biti nemogoče ugotoviti **D**.
 - Iz **E** mora biti zelo težko / nemogoče ugotoviti **D**.
- Najbolj znan algoritem je **RSA** (Rivest, Shamir, Adelman). RSA uporablja velika praštevila za določitev D in E, postopek kriptiranja/ dekriptiranja pa je enak računanju ostanka pri deljenju s produktom teh praštevil.

Problem: distribucija ključev, počasnost.

Kriptografija z javnimi ključi

Zakaj je RSA varen?

- Denimo, da poznamo javni ključ neke osebe (določen z dvojico števil (n, e). Za ugotavljanje zasebnega ključa d moramo poznati delitelje števila n. Iskanje deliteljev nekega velikega števila pa je težko ali neizvedljivo z današnjimi računskimi kapacitetami.
- Kako poiskati dovolj velika praštevila?
 - večkrat izvedemo "ugibanje": generiramo veliko število, nato ga testiramo, ali je praštevilo,
 - za testiranje praštevil obstajajo danes učinkoviti algoritmi.

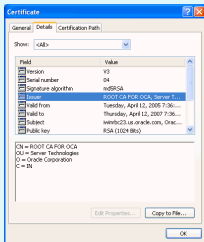
Integriteta

- Integriteta uporabnikov:** dokazuje, kdo je sporočilo poslal in da sporočilo bere le pravi prejemnik. Sporočilo S , ki ga uporabnik A pošlje B kriptiramo
 $E_B(D_A(S)) = XXX$
 in odkriptiramo: $D_B(XXX) = D_B(E_B(D_A(S))) = D_A(S)$;
 $E_A(D_A(S)) = S$
- Integriteta sporočila:** dokazuje, da sporočilo (tudi nekriptirano!) ni bilo spremenjeno. Uporabljajo se zgoščevalne funkcij, ki izračunajo podpis sporočila $sig(S)$. To vrednost podpišemo z mehanizmom elektronskega podpisa
 $D_A(sig(S)) = sss$
 in sss pošljemo skupaj s (kriptiranim) originalnih sporočilom XXX :
 (XXX, sss) Prejemnik odkriptira XXX v S , ponovno izračuna $sig(S)$ in preveri, ali $sss = sig(S)$.

61

Certifikati

- Sistem PKI vsebuje certifikacijske agencije (angl. certification authority), ki izdajajo, hranijo in preključujejo certifikate.
- Certifikati so definirani s standardom X.509 (RFC 2459)
- Certifikat vsebuje
 - naziv izdajatelja,
 - ime osebe, naslov, ime domene in druge osebne podatke,
 - javni ključ lastnika,
 - digitalni podpis (podpisan z zasebnim ključem izdajatelja),



62

Naslednjič gremo naprej!

- priključitev računalnika na omrežje
- zagon računalnika: protokola DHCP in BOOTP
- arhitektura strežnik – odjemalec,
- protokol: delovanje, njegove funkcije,
- sled protokola



63
