

Komunikacijski protokoli in omrežna varnost


Uvod in ponovitev osnov predmeta

1

1

Komunikacijski protokoli in omrežna varnost

- **Profesor:**
dr. Andrej Brodnik
- **Asistent:**
as. Aleks Huč
as. dr. Gašper Fele Žorž
- **Izvedba predmeta:**
 - 3 ure predavanj - 2 dela, 2 uri laboratorijskih vaj tedensko
 - kontakt: e-mail, govorilne ure, forum na strani predmeta

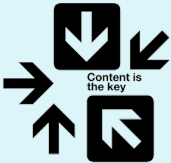


2

2

Vsebina predmeta

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



3

3

Obveznosti predmeta

Pri oceni se še upošteva:

- dopolnjevanje RFCjev
- sodelovanje na forumih
- pomoč kolegom
- priprava sledi protokolov
- ...

8

8

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
- ...

10

10

Ponovitev osnov računalniških komunikacij

11

11

ISO/OSI model

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

OSI Model Data Layer		
Data	Application Network Process to Application	aplikacijska plast
Data	Presentation Data Representation and Encryption	predstavitevna plast
Data	Session Interhost Communication	sejna plast
Segments	Transport End-to-End Communications and Reliability	transportna plast
Packets	Network Path Determination and IP (Logical Addressing)	omrežna plast
Frames	Data Link MAC and LLC (Physical Addressing)	povezavna plast
Bits	Physical Media, Signal and Binary Transmission	fizična plast

Host Layers: Application, Presentation, Session
Media Layers: Transport, Network, Data Link, Physical

12

ISO/OSI model

- plast N nudi storitve (streže) plasti N+1
- plast N zahteva storitve (odjema) od plasti N-1,
- protokol: pravila komuniciranja med istoležnima procesoma,
- entitetni par: par procesov, ki komunicira na isti plasti

13

Analogija: pogovor med dvema filozofoma

- Zakaj plasti?
 - sistematična zasnova zgradbe sistema,
 - sprememba implementacije dela sistema je neodvisna od ostalega sistema

14

ISO/OSI model

In še drugače:

- vsaka plast ima svoje protokole (= jezik, s katerim se pogovarja istoležni entitetni par procesov),
- protokoli so specifični za storitve, ki jih plast zagotavlja.

The diagram illustrates the ISO/OSI model with three layers shown: Layer 5, Layer 4, and Layer 3. Each layer contains two boxes labeled '(X) Instance' connected by a horizontal line labeled '(X) - Protocol'. Vertical dashed lines connect the instances of adjacent layers, representing communication between them.

15

OSI plasti: podrobneje

- **Aplikacijska plast**
 - najbližja uporabniku,
 - omogoča interakcijo aplikacije z omrežnimi storitvami,
 - standardne storitve: telnet, FTP, SMTP, SNMP, HTTP

The image shows a handwritten code snippet on a piece of paper, likely representing the application layer. The code includes HTML tags for document structure, such as <html>, <head>, <meta name='charset' content='utf-8' />, <link rel='stylesheet' type='text/css' href='style.css' />, </head>, <body bgcolor='white' />, and </body>.

16

OSI plasti

- **Predstavitvena plast**
 - določa pomen podatkov med entitetnima paroma aplikacijske plasti,
 - sintaksa in semantika,
 - določa kodiranje, kompresijo podatkov, varnostne mehanizme
- **Sejna plast**
 - nadzor pogovora (množice povezav) med aplikacijama,
 - logično povezovanje med aplikacijama,
 - običajno vgrajena v aplikacije.

17

OSI plasti

- **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 prenosi,
 - TCP, UDP, IPSec, GRE, L2TP, PPP

The TCP Segment Format

The UDP Segment Format

18

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

19


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

20

OSI plasti

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



21

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	

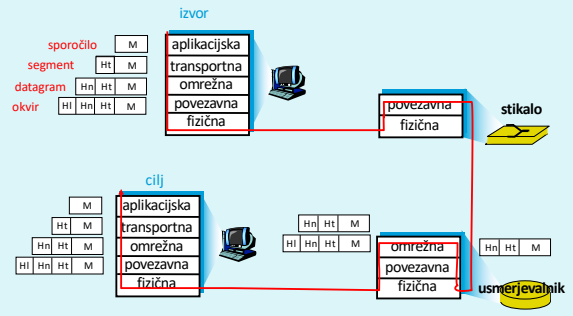
OSI Reference Model TCP/IP

Primerjava modelov:

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

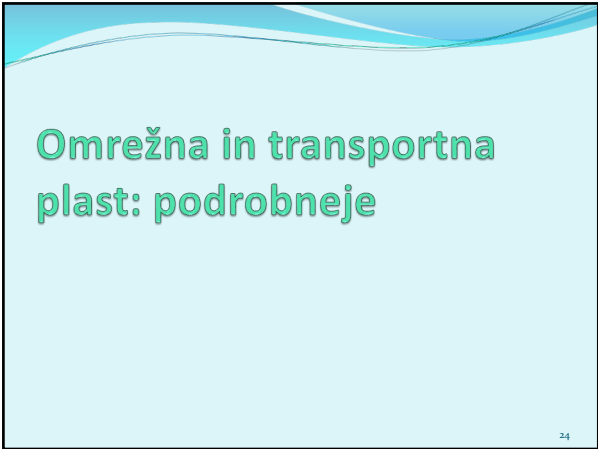
22

Enkapsulacija

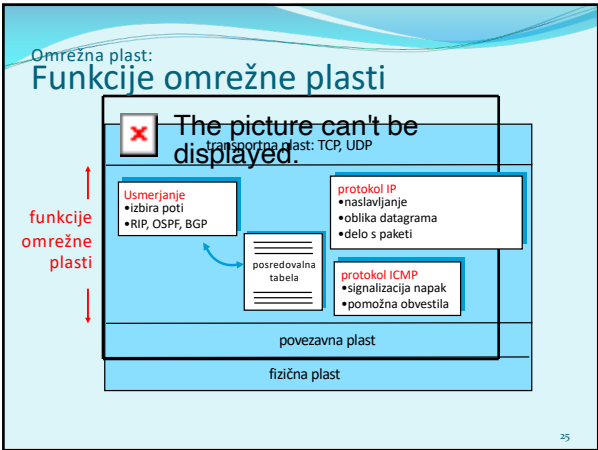


The diagram illustrates the encapsulation process. On the left, the 'izvor' (source) has a stack of layers: sporočilo (M), segment (HT, M), datagram (Hn, HT, M), and okvir (HI, Hn, HT, M). The data is sent to a computer icon. The data then passes through a stack of layers: aplikacijska, transportna, omrežna, povezavna, and fizična. It then goes through a 'stikalo' (switch) icon. The data then passes through another stack of layers: omrežna, povezavna, and fizična. Finally, it reaches a computer icon labeled 'cilj' (destination). The diagram also shows a 'usmerjevalnik' (router) icon at the bottom right.

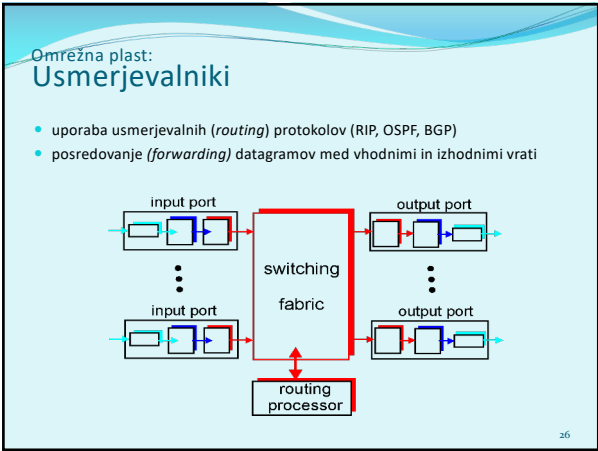
23



24



25



26

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
- **povezovališča (hub):**
 - naprava, ki deluje na fizični plasti, danes niso več v rabi

27

27

Omrežna plast:
IPv4

- protokol na omrežni (3.) plasti OSI modela
- **IPv4 naslov** je 32 bitni naslov vmesnika. Primer:
11000001 00000010 00000001 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:
111111 111111 11100000 00000000 (255.255.255.240)
pomeni, da prvih 20 bitov IP naslova predstavlja naslov omrežja, preostalih 12 pa naslov vmesnika.

28

28

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?

29

29

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

```
0010000111011010 000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000111111111 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

30

30

Omrežna plast:
Primerjava IPv4 in IPv6

Version		IHL		Type of Service				Total Length			
Identification				Flags				Fragment Offset			
Time to Live				Protocol				Header Checksum			
Source Address											
Destination Address											

Version		Traffic Class		Flow Label				Payload Length				Next Header		Hop Limit	
Source Address															
Destination Address															


31

31

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!)



32

32

Omrežna plast: IPv6 - vrste unicast naslovov

- globalni unicast** (= javni naslovi)

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

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

33

Omrežna plast: IPv6 – razpošiljanje (multicast)

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

128 Bits			
8-bits	4-bits	4-bits	112-bits
1111 1111	Lifetime	Scope	Group-ID
Lifetime	Scope		
0	If Permanent	1	Node
1	If Temporary	2	Link
		5	Site
		8	Organization
		E	Global

34

Omrežna plast: IPv6 v omrežjih IPv4

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

35

Omrežna plast:
Usmerjanje



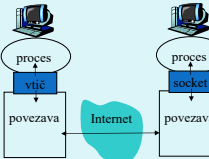
- **NAČINI**
 - statično / dinamično (upoštevanje razmer v omrežju)
 - centralizirano / porazdeljeno (glede na poznavanje stanja celega omrežja)
 - po eni poti / po več poteh
- **IMPLEMENTACIJE:**
 - z vektorjem razdalj (RIP, IGRP, EIGRP)
 - glede na stanje omrežja (OSPF, IS-IS)

36

36

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).



37

37

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 paketov)
 - sprotno potrjevanje: naslednji paket se pošlje šele po prejemu potrditve
 - tekoče pošiljanje: ne čaka se na potrditve.

38

38

Transportna plast:
TCP in UDP

The TCP Segment Format

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

The UDP Segment Format

Source Port (16)	Destination Port (16)
Length (16)	Checksum (16)
Data (variable)	

39

39

Aplikacijska plast:

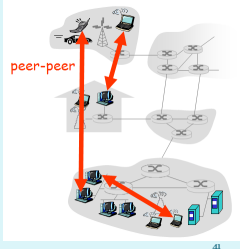
- **Klasikne storitve - odjemalec-strežnik**
 - telnet, ssh; rdesktop
 - ftp, sftp
 - WWW in HTTP,
 - SMTP, POP3, IMAP, MAPI
 - DNS,
 - SNMP, LDAP, RADIUS, ...
 - ...

40

40

Aplikacijska plast:

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



41

41

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 zunanjem svetu
- V IPv6 NAT prehodi niso potrebni

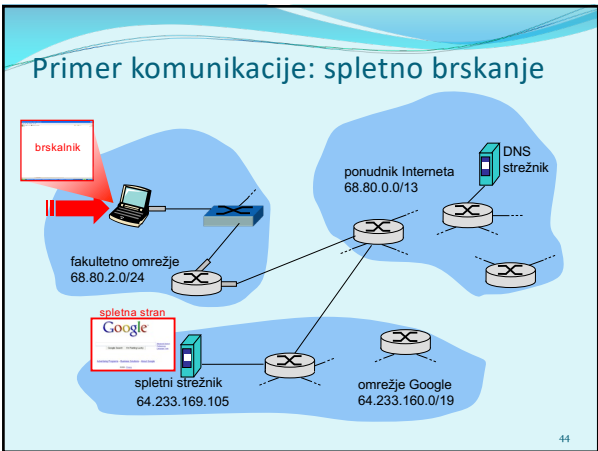
42

42

Primer komunikacije

43

43



44

Primer komunikacije: spletno brskanje

- notesnik ob priklopu na omrežje potrebuje **IP naslov** in podatke prehoda ter DNS strežnika: uporabi torej **DHCP**,
- zahteva DHCP se **enkapsulira**: UDP -> IP -> 802.1 Ethernet
- ethernet okvir se **odda** (*broadcast*) na omrežje, prejme ga usmerjevalnik, ki opravlja nalogo DHCP strežnika
- DHCP strežnik **prebere** vsebino DHCP zahteve

45

45

Primer komunikacije: spletno brskanje

- DHCP strežnik odgovori odjemalcu (notesniku) s paketom **DHCP ACK**, ki vsebuje njegov IP naslov ter naslove prehoda in DNS strežnika,
- odgovor **enkapsulira** DHCP strežnik (usmerjevalnik) in ga posreduje odjemalcu, ki ga **dekapsulira**,
- DHCP odjemalec dobi odgovor DHCP ACK,
- rezultat: odjemalec je pripravljen na komunikacijo.

46

46

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**.

47

47

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 **odklopi** zahtevek in posreduje uporabniku IP naslov spletnega strežnika **www.google.com**

The diagram illustrates the DNS lookup process. On the left, a laptop sends a DNS request through a router. The request is shown as a stack of protocols: DNS, UDP, IP, Eth, and Phy. The router forwards this request to a DNS server located in a provider network (Omrežje ponudnika). The DNS server responds with the IP address of the web server (www.google.com). The response is shown as a stack of protocols: DNS, UDP, IP, Eth, and Phy.

48

Primer komunikacije: spletno brskanje

- za pošiljanje **HTTP zahtevka**, odjemalec 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!**

The diagram shows the establishment of a TCP connection. A laptop sends an HTTP request through a router. The request is shown as a stack of protocols: HTTP, TCP, IP, Eth, and Phy. The router forwards this request to a web server (spletni strežnik). The web server responds with a TCP SYNACK segment. The response is shown as a stack of protocols: TCP, IP, Eth, and Phy. The text 'usmerjanje...' indicates the routing process.

49

Primer komunikacije: spletno brskanje

- HTTP zahtevok** se pošlje na **TCP vtič** spletnega strežnika,
- IP datagram**, ki vsebuje 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!**

The diagram shows the delivery of the web page. A laptop sends an HTTP request through a router. The request is shown as a stack of protocols: HTTP, TCP, IP, Eth, and Phy. The router forwards this request to a web server (spletni strežnik). The web server responds with an HTTP REPLY. The response is shown as a stack of protocols: HTTP, TCP, IP, Eth, and Phy. The text 'usmerjanje...' indicates the routing process. A small image of the Google homepage is shown as the content of the reply.

50

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.

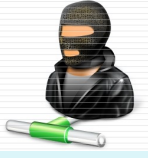
54

54

Kako lahko vdiralec škoduje sistemu?

Ima veliko močnih pristopov in tehnik!

- **prekinikovanje:** preprečevanje sporočil,
- aktivno **ponarejanje** sporočil v neki komunikaciji,
- **krnja 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,
- **onemogočanje znanja storitve (denial of service):** onemogoči uporabo regularne storitve (npr. s tem, da jo preobremeni)



55

55

Varnost: zagotavljanje zanesljivosti

NADZOR: zbiranje podatkov o delovanju, uporabi, dnevniki

UPRAVLJANJE: ukrepanje na podlagi zbranih podatkov, diagnostika, administracija

SISTEMATIČNOST: imeniki, seznanji in kazala, SNMP, postopna pravila

NACRTOVANJE: zmogljivost, razvoj, testiranje in uvajanje

RAZPRŠENOST ZASČITE: integriteta povezav, virov, vsebine, uporabnikov, sporočil



56

56

Elementi varne komunikacije

- **Zaupnost** – kdo sme prebrati? (šifriranje)
- **Overovijanje (authentication)** – dokaži, da si res ti (identifikacija – povej, kdo si, brez dokaza)
- **Razpoložljivost in nadzor dostopa** – preprečevanje nelegitimne rabe virov (avtorizacija (authorization) – ugotavljanje, ali nekaj smeš storiti, beleženje (accounting) – kaj je kdo uporabljal)
- **Integriteta sporočila** – je bilo med prenosom spremenjeno?
- **Onemogočenje zanikanja (nonrepudiation)** – res si poslal / res si prejel.

V praksi:

- požarne pregrade, zaznava vdorov (intrusion detection) sistemi,
- varnost na aplikacijski, transportni, omrežni in povezavni plasti

57

57

Zaupnost sporočil: šifriranje (zakrivanje) vsebine

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

Sporočilo **P** šifriramo s ključem **K** – dobimo **kriptogram K(P)**. Kriptogram **K(P)** predelamo v izvorno obliko s ključem **D**, dobimo izvorno sporočilo **D(K(P))=P**.

Vrste metod:


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

59

59

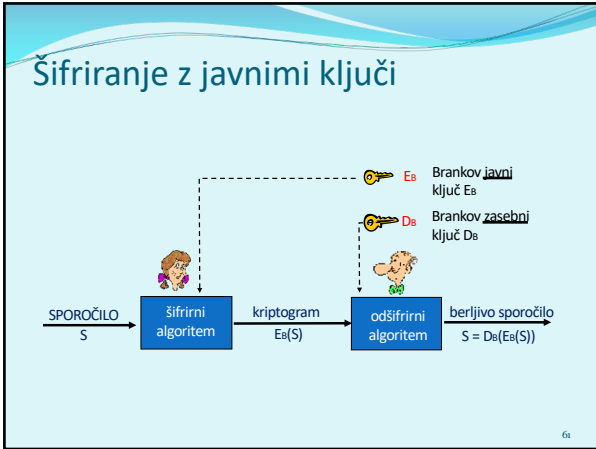
Vrste šifriranje

- Šifriranje uporablja ključ
 - šifirni algoritem je običajno znan vsem,
 - tajni so le ključi
 - šifriranje: skrivanje vsebine
 - kriptanaliza („razbijanje“ kode)
- Šifriranje z javnimi ključi
 - $E() \neq D()$: dva ključa – javni in zasebni
- Simetrično šifriranje
 - $E() = D()$: samo en ključ
- Zgoščevalne funkcije – ni šifriranje
 - ne uporabljajo ključev. Kako so lahko koristne?



60

60



61

Šifriranje z javnimi ključi

- Algoritmi za šifriranje z javnimi ključi so asimetrični, $E =$ šifrirni ključ, $D =$ odšifrirni ključ, velja $E \neq D$
- Ključa E in D morata izpolnjevati naslednje zahteve glede šifriranje 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 (od)šifriranja pa je enak računanju ostanka pri deljenju s produktom teh praštevil.

Problem: distribucija ključev, počasnost.

62

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.

63

Integriteta

- Integriteta uporabnikov:** dokazuje, (i) kdo je sporočilo poslal (elektronski podpis) in (ii) da sporočilo bere le pravi prejemnik (zakrivanje). $S, A \rightarrow B$:
 $A:: E_a(D_a(S)) \rightarrow XXX$
 $B:: D_b(XXX) \equiv D_b(E_a(D_a(S))) \equiv D_a(S) \equiv E_a(D_a(S)) \rightarrow S$
- Integriteta sporočila:** dokazuje, da sporočilo (tudi nešifrirano!) ni bilo spremenjeno. Uporabljajo se zgoščevalne funkcij, ki izračunajo podpis/izvleček sporočila $sig(S)$. To vrednost podpišemo z mehanizmom elektronskega podpisa
 $D_a(sig(S)) = sss$
 in sss pošljemo skupaj z originalnih sporočilom $S: (S, sss)$ Prejemnik ponovno izračuna $sig(S)$ in preveri $sss = sig(S)$.

64

64

Šifriranje z javnimi ključi

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

65

65

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),

66

66

Naslednjič gremo naprej!

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



67

67
