Komunikacijski protokoli in omrežna varnost
2021/22
Pisni izpit 10. svečana 2022

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena.

Če boste uspešno vsaj delno odgovorili na vsa vprašanja, bo možno dobiti dodatne točke.

Čas pisanja izpita je 105 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Osnove.

VPRAŠANJA:

A) Primer kodiranja je kodiranje TLV. (i.) Opišite čim podrobneje (dele zapisa in njihov pomen) TLV kodiranega sporočila. (ii.) Vemo, da ima ASCII koda znaka `A` vrednost 65_{10}. Zapišite TLV zakodirano sporočilo `ANA`. (iii.) Butalci so posebni ljudje in imajo posebna prepričanja. Tako so se odločili, da bodo kodirali vsa sporočila s 6 bitnimi zlogi. Pomagajte jim ter predlagajte kodirno shemo, ki bo omogočala kodiranje vseh velikih in malih črk slovenske abecede, vseh števk od 0 do 9, presledka in ločil `.,;:-?/+*()[]#!` tako, da bo koda čim krajša, a še vedno organizirana po zlogih.

B) Peter bi rad računalnik zaganjal preko spleta, saj je splet dandanes moderen. Slišal je, da je z uporabo gPXELINUX to mogoče, saj gPXELINUX podpira protokol HTTP. Trenutno uporablja ISC DHCP strežnik, PXELINUX, atftpd, apache2 in strežnik NFS (nfs-kernel-server). (i.) Kateri kos, oziroma katere kose programske opreme bo moral zamenjati, če bi se rad povsem izognil uporabi protokola TFTP? (ii.) Utemeljite svoj odgovor za vsak program posebej.

C) Kateri od naslednjih naslovov IPv6 ni veljaven in zakaj?

(1) `1:2:3:4:a:b:c:d`
(2) `2a00::804::2004`
(3) `0:1::1:2`
(4) `dead::beef`

2. naloga: Čas in slika.

VPRAŠANJA:

A) Petrova postaja predvaja predvsem glasbo ter vsako uro napovedovalec prebere še podatke o vremenu. Peter uporablja RTP protokol. (i.) Predlagajte dva bistveno različna načina, kako naj Peter ob glasbi posreduje tudi naslove skladb. (ii.) Peter bi želel definirati vsakourno vremensko poročilo kot ločeno sejo. Kako naj naredi to? (iii.) Do soljudi, ki ne slišijo moramo biti posebej občutljivi. Kako jim pomagati, da bodo vseeno deležni vremenskega poročila, čeprav ne slišijo, medtem ko ga bodo ostali lahko še vedno poslušali? Podajte čim natančneje tehnološko rešitev[1].

B) Kako program, ki po RTP sprejema glasbo in jo predvaja na zvočni kartici, ve, v kakšnem formatu je glasba zapisana? Razložite kako je zapisan ta podatek.

(a) Podatek o kodeku je zapisan v glavah, enkapsuliranih v RTP podatkih.
(b) Po polju type, specificiranem v RFC3550.

[1] Uporaba RTP protokola?

(c) Po polju type, specificiranem v RFC3551.
(d) Po imenu formata v SDP (*Session Description Protocol*) paketih.

C) Peter se je odločil, da bo izboljšal protokol `time`, ki ga uporablja program RDATE. Predvsem bi rad dosegel boljšo natančnost, rad pa bi tudi poenostavil implementacijo. Primer implementacije RDATE v pythonu:

```
import socket
import struct
import datetime
sock = socket.socket()
sock.connect(("ntp1.arnes.si", 37))
data = sock.recv(4)
cas = struct.unpack("!I", data)[0]
print(datetime.datetime.fromtimestamp(cas - 2208988800))
```

(i.) Program popravite, da se bo čas štel v tisočinkah sekunde namesto v sekundah. (ii.) Pa še tako, da čas ne bo več 32-bitno število sekund od polnoči, 1. 1. 1900, temveč predznačeno 64-bitno število od polnoči, 1. 1. 1970. (iii.) Če bi namesto 64-bitnih števil uporabil 32-bitna, do kdaj bi deloval njegov program? Kaj pa sedaj, ko ima 64-bitna? Odgovor utemeljite. Program seveda lahko prepišete v poljubnem berljivem, široko uporabljanem programskem jeziku (rešitev v Whitespace, Malbolge ipd. ne bomo upoštevali).

3. naloga: Moje omrežje in njegovo upravljanje. S programom Wireshark smo zajeli naslednji (skrajšan) paket `p1`:

```
Internet Protocol Version 4, Src: 192.168.122.1, Dst: 192.168.122.21
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
    Transaction ID: 0x966d682c
    Your (client) IP address: 192.168.122.21
    Option: (54) DHCP Server Identifier (192.168.122.1)
    Option: (3) Router
    Option: (6) Domain Name Server
```

VPRAŠANJA:

A) (i.) Za kateri protokol (na najvišji plasti) gre pri paketu `p1`? (ii.) Ali je paket `p1` poslan enemu prejemniku (*unicast*), skupini (*multicast*) ali gre za oddajanje (*broadcast*)? Utemeljite odgovor. (iii.) Katere podatke posredujeta opciji 3 in 6 ter katere funkcionalnosti na odjemalcu bi ne delovale, če teh podatkov bi ne bilo? Utemeljite odgovor. (iv.) Kaj bi se lahko zgodilo, če ne bi imeli polja *Transaction ID*?

B) Vračamo se k zajetemu paketu `p1`. (i.) Kdo ga pošilja komu in kaj z njim sporoča? (ii.) Kaj je sporočal paket `p0`, ki je bil razlog za pošiljanje paketa `p1`? Utemeljite odgovor. (iii.) Čim natančneje zapišite polja paketa `p0` od omrežne plasti navzgor in utemeljite svoj odgovor.

C) Peter bi rad usposobil avtentikacijo prek IEEE 802.1x na svojem domačem ožičenem omrežju. (i.) Kako bi to naredil s čim manj dodatnih nakupov? Uporablja ceneno dostopno točko, na kateri teče nek Linux in ki uporablja BCM5352F kot čip za stikalo. (ii.) Utemejite svojo odločitev.

(a) Za tovrstno avtentikacijo bo moral popraviti nastavitve omrežja na dostopni točki - nastaviti bo moral strežnik RADIUS.
(b) Moral bo popraviti programsko opremo na dostopni točki, saj tovrstne funkcionalnosti programska oprema na dostopnih točkah praviloma ne omogoča.
(c) Za tovrstno avtentikacijo bo moral kupiti zunanje stikalo, ki podpira tovrstno avtentikacijo. Oprema za domačo uporabo namreč nima tovrstne funkcionalnosti.
(d) Če za avtentikacijo na brezžičnem omrežju uporabi WPA2-Enterprise, se možnost avtentikacije prek 802.1x običajno prikaže avtomatično.

4. naloga: Varnost tako in drugače.

VPRAŠANJA:

A) Zakaj se v protokolu SSL uporablja certificat? Utemeljite odgovor z opisom, kako se uporablja.

(1) Za avtentikacijo.
(2) Da ena stran zagotovo ve, da je javni prejeti javni ključ res od druge strani.
(3) Zaradi skladnosti med SSL in TLS.
(4) Da se zagotavlja zakritost komunikacije.

B) Celovitost podatkov je eden elementov varnosti. (i.) Kaj pravzaprav pomeni celovitost (*integrity*) podatkov? (ii.) Kako jo zagotavljamo pri prenosu podatkov? Zakaj je opisani način zadovoljiv? (iii.) Ali sporočila pri RADIUS protokolu vsebujejo varovanje celovitosti? Če ne, zakaj ne (kako lahko napademo celovitost); in če da, kako se varuje celovitost (opišite na primeru).

C) Peter Zmeda bi se rad priklopil na VPN podjetja, za katero naj bi delal. V podjetju uporabljajo OpenVPN. S pomočjo Easy-RSA je ustvaril datoteke ca.key, ca.crt, peter.key, peter.crt in vse poslal administratorki. (i.) Katere datoteke so bile pri tem odveč? Katere datoteke pričakuje, da bo dobil nazaj? (ii.) Katere dodatne datoteke vsebujejo podatke, ki jih v podjetju dejansko potrebujejo? (iii.) Je vse naredil pravilno? Bi moral poslati še kakšno datoteko? Utemeljite odgovor.