Preddiplomski studij
Računarstvo

Komunikacijske mreže

Pitanja za provjeru znanja
3. blok predavanja

Ak.g. 2007./2008.

Napomena		*Preporučena literatura, uz bilješke s predavanja, su knjige:* • *Andrew S. Tanenbaum: Computer Networks, 4th Edition, poglavlje 8 (Network Security);* • *Bažant et al.: Osnovne arhitekture mreža, poglavlja 4.6 (Bežični LAN-ovi) i 8 (Pokretljivost u mrežama)*

Zadatak 1		Koji se sigurnosni mehanizam koristi za zaštitu od nedozvoljenog korištenja mrežnih resursa: a) ovjera i ovlašćivanje b) kriptiranje c) digitalni potpisi d) prikrivanje adrese

Zadatak 2		Koji od sljedećih sigurnosnih mehanizama **ne pripadaju** transportnom sloju: a) SSL b) TLS c) SOCKS d) IPsec

Zadatak 3		Koja je prednost korištenja virtualnih privatnih mreža? a) izbjegavanje troškova iznajmljivanja vodova b) slanje prometa s privatne mreže zasebnim vodovima c) pristup anonimnih korisnika korporativnoj mreži d) pristup internetskih korisnika Web poslužitelju korporacije

Zadatak 4		Prevoditelj mrežnih adresa obavlja sljedeću promjenu na IP paketima koji odlaze na Internet a) mijenja izvorišnu adresu b) mijenja odredišnu adresu c) mijenja TTL IP paketa d) ne obavlja nikakve promjene na paketu

Zadatak 5		Označite što omogućava primjena sigurnosne stijene: a) nadzor izlaznog i ulaznog internetskog prometa b) nadzor prometa koji se razmjenjuje unutar privatne mreže c) ograničavanje broja korisnika privatne mreže d) onemogućavanje zaraze virusom računala unutar privatne mreže

Zadatak 6

Najsigurnija sigurnosna politika u sigurnosnoj stijeni je:

a) onemogućiti sav promet pa selektivno dozvoljavati iznimke
b) dozvoliti sav promet pa ga selektivno omogućavati iznimke
c) samo selektivno omogućavati promet
d) samo selektivno onemogućavati promet

Zadatak 7

Koji je način korištenja,od navedenih, karakterističan kod IPsec protokola:

a) tunelski način
b) jednosmjerni način
c) distribuirani način
d) agregacijski način

Zadatak 8

Zaglavlje AH služi za

a) tuneliranje
b) provjeru integriteta
c) kriptiranje
d) razmjenu ključeva

Zadatak 9

Zaglavlje ESP služi za

a) tuneliranje
b) kriptiranje
c) razmjenu privatnih ključeva
d) autentifikaciju

Zadatak 10

Kriptologija je

a) znanost o kriptiranju
b) umješnost izmišljanja i razbijanja šifri
c) znanost o razbijanju šifri
d) znanost primjene šifri u umrežavanju

Zadatak 11

Koji od najjači od sljedećih algoritama kriptiranja:

a) DES
b) AES256
c) 3DES
d) Cezarova šifra

Zadatak 12		Problem simetrične kriptografije je: a) razmjena ključeva b) pogađanje ključeva c) pronalaženje javnog ključa d) generiranje ključa e) trajanje kriptiranja

Zadatak 13		Algoritam RSA temelji se na: a) eliptičkim krivuljama b) složenosti faktorizacije c) neprobojnosti javnog ključa d) tajnosti svih ključeva

Zadatak 14		U kakvom su odnosu poruka i njen sažetak: a) iz poruke nije moguće saznati njen sažetak b) iz sažetka nije moguće saznati poruku c) nikada ne postoje dvije poruke s istim sažetkom d) nikada ne postoji tri ili više poruka s istim sažetkom

Zadatak 15		Modul pretplatničkog identiteta (SIM modul) fizički je smješten: a) u domaćem lokacijskom registru (HLR) b) u pokretnom komutacijskom centru (MSC) c) u baznoj stanici d) u pokretnoj postaji (MS)

Zadatak 16		Gdje su trajno zapisani svi pretplatnički podaci te trenutna lokacija pretplatnika kod GSM mobilne mreže? a) VLR (*Visiting Location Register*) b) MSC (*Mobile Switching Center*) c) HLR (*Home Location Register*) d) BSC (*Base Station Controller*)

Zadatak 17		U GSM mreži, autentifikacijski ključ pretplatnika zapisan je u: a) u domaćem lokacijskom registru (HLR) b) u pokretnom komutacijskom centru (MSC) c) u baznoj stanici d) u registru identifikacije opreme (EIR)

Zadatak 18		Lokacijsko područje u GSM mreži je: a) dio domaćeg lokacijskog registra u kojem je pohranjena trenutna lokacija korisnika b) dio domaćeg lokacijskog registra u kojem je pohranjena zadnja poznata lokacija korisnika c) područje pokrivanja radijskim signalom jedne bazne postaje d) skup ćelija kroz koje prolazi korisnik e) skup ćelija koje pripadaju jednom pokretnom komutacijskom centru

Zadatak 19		Dva načina korisničkog pristupa u digitalnoj mreži integriranih usluga su : a) temeljni i napredni pristup b) ADSL i ISDN pristup c) osnovni i primarni pristup d) TCP i UDP pristup

Zadatak 20		Karakteristika prve generacije pokretnih mreža (NMT) je: a) koncept višestrukog pristupa u vremenskoj podjeli (TDMA) b) koncept višestrukog pristupa u kodnoj podjeli (CDMA) c) činjenica da je to analogni sustav d) nepostojanje pristupne mreže, već direktno povezivanje korisnika mreže s jezgrenom mrežom

Zadatak 21		Koji funkcijski entitet se mora dodati komutacijskom čvoru telefonske mreže da bi mogao funkcionirati kao čvor inteligentne mreže? a) CCAF (*Call Control Access Function*) b) CCF (*Call Control Function*) c) SSF (*Service Switching Function*) d) SDF (*Service Data Function*)

Zadatak 22		Izbjegavanje sudara okvira u bežičnim LAN-ovima ostvareno je: a) razmjenom RTS i CTS okvira prije početka razmijene podataka b) uspostavom virtualnog kanala i virtualnog puta c) slanjem *jamming* signala u slučaju nastanka kolizije d) osluškivanjem naponske razine na mediju

Zadatak 23		Dvije osnovne topologije bežičnih lokalnih mreža (WLAN) su: a) infracrveni WLAN i WLAN s radioprijenosom b) infrastrukturni WLAN i neovisni (*ad hoc*) WLAN c) centralizirani WLAN i decentralizirani WLAN d) privatni WLAN i javni WLAN

Zadatak 24		Kod bežičnih lokalnih mreža (WLAN) susrećemo se s problemom: a) udaljene stanice b) skrivene stanice c) odspojene stanice d) pokretne stanice

Zadatak 25		Primarni pristup (PRA) digitalnoj mreži integriranih usluga (ISDN) u referentnoj točki S sadrži: a) 32 informacijska kanala i 2 signalizacijska kanala b) 2 informacijska kanala i 1 signalizacijski kanal c) 16 informacijskih kanala i 2 signalizacijska kanala d) 1 informacijski kanal i 1 signalizacijski kanal