Komunikacijski protokoli in omrežna varnost
2010/11
Drugi kolokvij

Kolokvij 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 50 minut.

Veliko uspeha!

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

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Čeprav je to vprašanje osredotočeno na AAA, se AAA pojavlja tudi v drugih vprašanjih in v tem vprašanju se pojavlja tudi vsebina iz drugih poglavij.

VPRAŠANJA:

1. Glej ga Petra Zmedo, spet je nekaj pogruntal. Ugotovil je, da je avtentikacijski strežniški program CHAP proizvajalca JCN napisan tako, da uporablja svoj generator naključnih števil, ki je naslednja deterministična funkcija:

   ```
   Init()::
     seed:= 110121;
   Random()::
     seed:= (seed * 65539) mod 2**(31);
     return seed,
   ```

   Dejansko je funkcija opisana v knjigi *The Art of Computer Programming* in tam dokazana, da je dobra.[1] Tako generirana naključna števila uporablja strežniški program protokola CHAP za generiranje izzivov. Kako naj Peter izvede napad s ponavljanjem na avtentikacijo?

   NAMIG: Peter lahko vedno ugasne JNC strežnik ter ga ponovno prižge.

2. Druga Petrova ideja je, da ponudi preko spleta svojo novo storitev KMD. Za uporabo storitve se mora uporabnik avtenticirati. Žal uporabniki pozabljajo gesla in jim je potrebno pri tem pomagati. Predlagajte Petru vsaj eno možno rešitev tega problema ter jo *ocenite/komentirajte* iz varnostnega zormega kota (prestrezanje, ponavljanje, ...).

3. Na predavanjih smo zapisali vsebino PPP okvirja in vsebino IEEE 802 okvirja. Zapišite za vsakega od okvirjev polja, ki jih vsebujeta, ter primerjajte posamezna polja v obeh okvirjih. Katera polja so prisotna v obeh okvirjih in katera ne? Obrazložite oba odgovora.

2. naloga: Varnostni elementi omrežij.

VPRAŠANJA:

1. Kaj je to SA (*security association*):
   - Kakšna je funkcija (vloga) SA?
   - Koga združuje?
   - Naštejte polja, ki jih vsebuje ter zakaj potrebujemo ta polja?

[1] Znak `**` pomeni eksponent.

2. Tokrat bi se Peter rad pogovarjal s prijateljico Ano preko medmrežja (Internet) in pri tem uporabljal VoIP. Poleg tega ne želi, da bi lahko kdorkoli prisluškoval pogovoru – se pravi, prestrezal pakete in jih ,,poslušal“. Naštejte vsaj tri načine, kako se lahko pred prisluškovanjem zaščiti ter za vsak način napišite prednost, ki jo ima pred drugima dvema.

3. naloga: Podatki za delovanje omrežja.

VPRAŠANJA:

1. Ko govorimo o LDAP, kaj je pravzaprav to: kos programske opreme, opis podatkov, ki jih odjemalec lahko pridobi, protokol ali nekaj tretjega? Utemeljite odgovor.

2. Na predavanjih smo omenili, da obstajata dve inačici LDAP: v2 in v3. Zapišite in opišite vsaj dve podrobnosti, v katerih se razlikujeta.

3. Med odjemalcem in strežnikom se pri LDAP vzpostavi seja. Med drugim sta ukaza, ki jih seja pozna, `bind` in `unbind`. Ali v seji oba ukaza vedno nastopata? Utemeljite odgovor – morda najbolje z opisom primera.

4. naloga: Družina IEEE 802.

VPRAŠANJA:

1. Peter je včasih neizmeren vir idej. Tokrat se je odločil, da bo spremenil protokol IEEE 802.1x tako, da bo dovolil uporabo enkratnega gesla (*one-time password*). Kaj mora narediti, da bo to delovalo. Za več točk dodajte podrobnosti, kaj je potrebno spremeniti, dopolniti, parametrizirati v uporabljenih protokolih.

2. Pri protokolu RADIUS smo omenili, da so trije udeleženci. (i) Kateri trije so ti udeleženci, (ii) kakšna je vloga vsakega od njih v protokolu RADIUS ter (iii) kje se nahajajo pri protokolu IEEE 802.1x, konkretno pri EDUROAM (t.j., kako se natančno uporablja RADIUS v protokolu IEEE 802.1x)?

   NAMIG: Ali je morda kakšen od ,,udeležencev“ sestavljen iz večih dejanskih strežnikov? Preverite natančno RADIUS protokol.