Komunikacijski protokoli in omrežna varnost
2013/14
Drugi kolokvij

Kolokvij morate pisati posamič. Pri reševanju je literatura dovoljena. Odgovorite pazljivo na *vsa* vprašanja.

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

Čas pisanja izpita je 60 minut.

Veliko uspeha!

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

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: AAA in RADIUS.

VPRAŠANJA:

1. RADIUS protokol omogoča tudi beleženje dogodkov. (i) Katere vrste dogodkov, ki jih lahko beležimo, pozna protokol? (ii) RADIUS pozna nekaj varnostnih elementov in glavni med njimi uporablja v RADIUS paketu polje `Authenticator`. Kako točno se ga uporablja pri beleženju? (iii) Ta mehanizem žal ne ščiti pred napadamo s ponavljanjem – zakaj? Kako RADIUS ali njegovi uporabniki rešujejo potem problem napada s ponavljanjem?

   NAMIG: Morda pri zadnjem delu opišete primer napada ter si s tem pomagajte pri splošnem odgovoru. Tudi, najbolje je, da za vsakega od vrste dogodkov preučite posledice napada s ponavljanjem.

2. Tokrat se je Peter odločil, da bo s prijateljem Janezom vzpostavil navidezno zasebno omrežje. Za medsebojno avtentikacijo sta se odločila, da bosta uporabila certifikate. Zataknilo se je pri ustvarjanju certifikatne agencije. Prijatelja drug drugemu sicer zaupata, a vsak od njiju hoče biti tako pomemben, da ga drugi prosijo za avtograme – torej vsak hoče imeti svojo certifikatno agencijo.

   (i) Ali imata lahko strežnik in odjemalec OpenVPN, ki vzpostavljata navidezno omrežje, različni datoteki s certifikatom certifikatne agencije (običajno `ca.crt`)? (ii) Če privzamemo, da je datoteke `peter_ca.crt`, `peter_ca.key`, `peter.key` in `peter.csr` Peter ustvaril, Janez pa `janez_ca.crt`, `janez_ca.key`, `janez.key`, `janez.csr`, katere datoteke morajo biti na koncu pri Petru in katere pri Janezu, da bo njuno omrežje delovalo? (iii) Kdo bo komu podpisal javni ključ (izdal certifikat)?

3. Peter Zmeda hrani zgoščena gesla, vendar, da bi ne bila ranljiva na mavrični napad, jih dodatno zasolil. Žal je vrednost soli izgubil. Je to pomembno? Utemeljite odgovor.

2. naloga: Imeniške strukture in LDAP.

VPRAŠANJA:

1. Standard X509 definira certifikate, ki jih Peter in Janez uporabljata v prejšnjem vprašanju. Standard predvideva v certifikatu vrsto polj in med njimi so tudi (z imeni v angleščini) polja: *Issuer*, *Subject*, *Subject Public Key Info*, ki vključuje (pod)polji *Public Key Algorithm*, *Subject Public Key* ter še polje *Subject Unique Identifier*. (i) Kaj je shranjenega v posameznem polju in ali so vsa našteta polja obezna? (ii) Beseda certifikat pomeni potrdilo.

Kdo in kaj potrjuje z X509 potrdilom? Kako vemo, da je vsebina potrdila verodostojna?

2. Standard X500 definira naslednje operacije: *Bind*, *Read*, *List*, *Search*, *Compare*, *Modify*, *Add*, *Delete*, in *ModifyRDN*. Standard RFC4511 pa definira operacije: *Bind*, *Unbind*, *Search*, *Modify*, *Add*, *Delete*, *Modify DN*, *Compare*, *Abandon*, *Extended* in *StartTLS*. (i) Uparite operacije iz obeh standardov in komentirajte razlike. (ii) V čem se razlikujeta operaciji *Search* in *Compare* ter podajte primer uporabe prve in primer uporabe druge.

3. Katere načine varne komunikacije ponuja protokol LDAP?

3. naloga: Varnostni elementi.

VPRAŠANJA:

1. Peter Zmeda je slišal, da obstaja nek podporni protokol, ki se imenuje IKE in da je povezan z varnostnimi protokoli na internetu. (i) Opišite scenarij, kjer se protokol uporablja. (ii) Opišite delovanje protokola. (iii) Recimo, da protokol ne bi obstajal, kaj bi to pomenilo? Bi se osnovna dejavnost, ki jo IKE podpira, ne mogla izvajati? Bi jo bilo težje izvajati?

2. Peter je doma postavil lokalno omrežje z nekaj računalniki. Za prehod v internet je pred temi računalniki postavil še en računalnik, na katerem poganja Linux distribucijo OpenWRT. Na treh notranjih računalnikih mu tečejo openssh strežniki. Sedaj bi rad do teh računalnikov dostopal s širnega interneta. (i) Kaj mora postoriti na prehodnem računalniku, da bo lahko dostopal do notranjih računalnikov? Predlagajte vsaj dve rešitvi. (ii) Če na vseh treh računalnikih ssh posluša na istih vratih, ali lahko sploh dostopa do vseh treh? (iii) Kakšno vlogo igra prehodni računalnik – mostiček, usmerjevlanik, požarna pregrada ali aplikacijski prehod? Utemeljite odgovor.

3. Kako ESP preprečuje napade s ponavljanjem?

4. naloga: Lokalne mreže.

VPRAŠANJA:

1. Standard IEEE 802 razdeli povezavno plast na podplasti LLC in MAC. Ena od funkcionalnosti, ki jo nudi podplast LLC je izgradnja vpetega drevesa. (i) Kaj bi se zgodilo, če bi ne tvorili vpetega drevesa, s prometom v mreži? Utemeljite odgovor s primerom. (ii) Recimo, da podplast ne bi poznala pojma mostička (*bridge*), ali bi še vedno potrebovali vpeta drevesa? Utemeljite odgovor?

2. Peter Zmeda si vzpostavlja navidezno zasebno omrežje med počitniško hišico in domom. Kadar gre v počitniško hišico, ima s seboj prenosnik. Rad bi, da na lokalnem omrežju prenosnik pridobi vedno isti naslov, ne glede na to, ali se priklaplja na omrežje na počitniški hišici ali doma. Obenem bi rad od doma dostopal do kamere, ki je nameščena na počitniški hišici, na počitniški hišici pa bi rad gledal filme z diska, ki ga ima doma. Poleg tega včasih rad igra stare računalniške igrice s svojo ženo in temu se ne bi rad odrekel, četudi je žena doma, on pa na počitniški hišici. (i) Katerega od naborov nastavitev za OpenVPN, naštetih spodaj, naj uporabi? Zakaj?

   - Konfiguracija 1:
     ```
     remote vpn.zmeda.si
     dev tun
     ifconfig 192.168.5.2 192.168.5.1
     secret skrivnost.key
     ```
   - Konfiguracija 2:
     ```
     remote vpn.zmeda.si
     dev tap
     secret skrivnost.key
     ```

   (ii) Kakšne so slabosti tovrstnega navideznega omrežja (naštejte vsaj eno)?

3. Kako lahko odjemalec ob priklopu v omrežje sploh izvede postopek 802.1X avtentikacije, če mu še ni dovoljen dostop do omrežja?