2. kolokvij RKVB, VSS, FRI, 1. letnik, 3. 6. 2014

RKVB

List z nalogami lahko obdržite, razen če rešujete naloge nanj – v tem primeru ga podpišite.

Ime: _____

Priimek: _____

Vpisna številka: _____

*Pozorno preberite navodila! Literatura **ni** dovoljena. Odgovarjajte kratko! Čas pisanja je **60** minut.*

1. (20%) Ugotovite, ali so naslednje trditve pravilne ali napačne. Pojasnite svojo odločitev (tudi za pravilne), napačne pa popravite ali dopolnite tako, da bodo postale pravilne.
   a. TCP segment ima v glavi polje »*receive window*«, katerega vrednost je ves čas trajanja neke TCP povezave nespremenjena.
   b. Denimo, da naprava A pošilja po TCP povezavi napravi B veliko datoteko. Število nepotrjenih bajtov, ki jih odda naprava A, ne sme preseči velikosti sprejemnega vmesnika.
   c. Denimo, da je bil zadnji izmerjeni čas vrnitve (RTT) v neki TCP povezavi enak 1 s. Na podlagi tega podatka bo izračunana vrednost intervala časovne kontrole (Timeout Interval). Če je bila dosedanja ocena odmika 0.25 s, bo v našem primeru bo izračunani interval časovne kontrole zagotovo večji od 1 s.
   d. Naprava A pošlje napravi B TCP segment z zaporedno številko 38 in dolžino podatkovnega dela 4 byte. Številka potrditve v glavi tega segmenta bo torej 42.

2. (15%) Navedite razlike med simetričnim in asimetričnim kriptiranjem. Nato pojasnite, za kakšne namene v avtentikacijskih protokolih uporabljamo simetrične in za kakšne asimetrične metode?

3. (10%) Predpomnenje (caching) spletnih vsebin na lokaciji uporabnika lahko zmanjša odzivne čase za uporabnika. Vendar pa lahko to pomeni, da te vsebine ne bodo več primerno sveže, torej da se je na originalnem strežniku vsebine med tem, ko je predpomnjena pri uporabniku, že spremenila. Kako HTTP rešuje to težavo?

4. (10%) Navedite, na katero plast po ISO-OSI modelu sodijo naslednje storitve in protokoli.

a) SMTP	f) BitTorrent
b) HTTP piškotki	g) Ping
c) MIME	h) IEEE 802.15
d) UDP	i) enkripcija
e) RSA	j) IPv6

5. (10%) Spodaj je del glave resničnega spam e-mail sporočila. Ali lahko ugotovite, iz katerega poštnega strežnika in katere države izvira?

```
MIME-Version: 1.0
Received: from ns.fri.uni-lj.si (212.235.188.18) by ns-relay.fri.uni-lj.si
 (212.235.188.39) with Microsoft SMTP Server id 14.3.174.1; Sun, 1 Jun 2014 19:56:52 +0200
Received: from localhost (localhost [127.0.0.1]) by ns.fri.uni-lj.si (Postfix)
 with ESMTP id 77B89808D for <mojca.ciglaric@fri.uni-lj.si>; Sun, 1 Jun 2014 19:57:20 +0200 (CEST)
X-Virus-Scanned: amavisd-new at fri.uni-lj.si
X-Spam-Flag: YES
Received: from ns.fri.uni-lj.si ([127.0.0.1])  by localhost (ns.fri.uni-lj.si [127.0.0.1]) (amavisd-new, port 10024) with
ESMTP id IV1Y2oSzyPPx for <mojca.ciglaric@fri.uni-lj.si>; Sun, 1 Jun 2014 19:57:18 +0200 (CEST)
X-Greylist: delayed 405 seconds by postgrey-1.32 at ns; Sun, 01 Jun 2014 19:57:17 CEST
Received: from 176.61.238.28 (176-61-238-28.wmx.slovanet.sk [176.61.238.28]) by ns.fri.uni-lj.si (Postfix) with
SMTP id 3D177808B  for <mojca.ciglaric@fri.uni-lj.si>; Sun, 1 Jun 2014 19:57:16 +0200 (CEST)
Received: from unknown (HELO localhost) (mail@metor.ru@97.27.91.142) by 176.61.238.28 with ESMTPA; Sun, 1
Jun 2014 10:52:00 -0800
Subject: ***SPAM*** Why is your love life such a disaster?
```

6. (15%) Kaj od spodnjega velja za protokole tipa izziv – odgovor? Za vsako trditev napišite, ali je pravilna ali napačna.
    a. Sogovornika se morata vnaprej dogovoriti za skupno skrivnost (ali dve), ki jo poznata oba.
    b. Protokol je občutljiv za napad s prestrezanjem (man in the middle), ni pa občutljiv za napad z zrcaljenjem.
    c. Če protokol zahteva, da iniciator prvi dokaže svojo identiteto, je protokol varen.
    d. Vir težav je to, da je možnih več vzporednih sej med sogovornikoma.
    e. Če je napadalec prestregel in zlorabil postopek za vzpostavljanje skupne skrivnosti, tudi najvarnejši protokol izziv-odgovor ne zadošča.

7. (10%) S programom Wireshark smo iz paket izluščili podakte o protokolu aplikacijske plasti, ki jih prikazuje spodnji izpis:

```
Secure Socket Layer
  TLSv1 Record Layer: Handshake Protocol: Multiple...
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 571
  Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 77
    Version: TLS 1.0 (0x0301)
  Random
    gmt_unix_time: Jun  6, 2011 09:49:42.000000000
    random_bytes: 79aeba12ce22a8abcd51be006ca...
  Session ID Length: 32
  Session ID: 4dec8696cf5...
  Cipher Suite: TLS_RSA_WITH_AES_128_CBC_MD5
  Compression Method: null (0)
  Extensions Length: 5
  Extension: renegotiation_info
```

```
Handshake Protocol: Certificate
  Handshake Type: Certificate (11)
  Length: 425
  Certificates Length: 422
  Certificates (422 bytes)
    Certificate Length: 419
    Certificate (id-at-commonName=lrk.fri.uni-lj.si)
  Handshake Protocol: Certificate Request
    Handshake Type: Certificate Request (13)
    Length: 53
    Certificate types count: 2
    Certificate types (2 types)
    Distinguished Names Length: 48
    Distinguished Names (48 bytes)
  Handshake Protocol: Server Hello Done
    Handshake Type: Server Hello Done (14)
    Length: 0
```

a) Za kateri protokol aplikacijske plasti gre? Katere verzije je in katere verzije je zadnja različica?
b) Kateri protokol na transportni plasti prikazani protokol uporablja in zakaj?
c) Kateri algoritmi se bodo uporabili v tej seji? *Protokole naštejte in na kratko opišite njihov namen in dolžino uporabljenih ključev v tem protokolu aplikacijske plasti.*
d) Kakšno je ime strežnika, ki je zapisano v digitalnem potrdilu?
e) Naštej nekaj standardnih napadov, proti katerim je ta protokol neobčutljiv.

8. (10%) Imamo kriptosistem, ki ga sestavlja škatla P0 in škatli S0 in S1. Permutacije v škatlah so:
    - P0 = (6 1 0 4 7 2 3 5)
    - P znotraj S0 = (3 1 7 6 12 0 8 13 15 14 9 10 11 2 4 5)
    - P znotraj S1 = (8 5 0 7 14 2 15 13 10 11 3 4 1 12 9 6)

   V kaj se kriptira niz **0111 1101**? Pokažite tudi vmesne korake.

   Kriptosistem prikazuje spodnja slika, koder in dekoder v škatlah S pa sta podana v spodnji tabeli:

4/16	
0000	8
0001	5
0010	11
0011	12
0100	13
0101	9
0110	6
0111	14
1000	15
1001	3
1010	4
1011	1
1100	2
1101	10
1110	0
1111	7

16/4	
0	1000
1	0110
2	1100
3	1111
4	0000
5	0111
6	1001
7	1010
8	1011
9	0001
10	0010
11	1101
12	1110
13	0011
14	0100
15	0101