Tietoliikenteen perusteet 2014, viikko 7

Viikon teemat: tietoturva

Harjoitukset ke 10.12 - to 11.12.2014.

1. Professori Sasu Tarkoman sähköpostin lähetys vielä kerran.
Tähän saakka olemme tarkastelleet sähköpostin lähettämistä perustilanteessa, jossa ei ole mitenkään huomioitu tietoturvaa. Miten sähköpostin lähettämisestä saadaan turvallisempaa? Mitä kaikkea voidaan tehdä protokollapinon eri kerroksilla tiedon suojaamiseksi, kommunikoivien osapuolien tunnistamiseksi, luvattoman lukemisen estämiseksi yms? Tarkastele asiaa kerros kerrallaan. Kullakin kerrokselle mieti, kyseisen kerroksen protokollia ja niiden toiminnallisuutta tietoturvan näkökulmasta.

a. Sovelluskerros
b. Kuljetuskerros
c. Verkkokerros

2. RSA avaimista (kirjan tehtävä Ch8P8)
RSAn avainten laskenta perustuu alkulukuihin ja moduloaritmetiikkaan. Käy läpi avainten muodostusprosessi. Käytä tässä tehtävässä alkulukuina p=7 ja q=13.

a. Mitkä ovat silloin n ja z?
b. Valitaan e=17. Onko tämä kelvollinen valinta?
c. Mikä olisi silloin d, jotta de=1 (mod z).
d. Käytä muodostamiasi avaimia salaamaan viesti m=9 käyttäen avainta (n.e). Mikä on salattu viesti tässä tapauksessa. Kuvaa sekä salaus- että purkuprosessit välivaiheineen. (Vinkki: www.wolframalpha.com laskee luvut tarvittavalla tarkkuudella)

3. BitTorrent tiedostojenjakelu (Ch8P13)
BitTorrentin tiedostojenjakeluprotokollassa (katso luku 2, luento 4) lähde (seed) jakaa tiedoston lohkoiksi ja vertaiset (peers) jakelevat näitä lohkoja toisilleen. Ilman mitään suojauksia hyökkääjä voi helposti aiheuttaa hämmennystä/häiriötä yhden vertaistoimijaryhmän (torrent) sisällä tekeytymällä hyväntahtoiseksi vertaiseksi ja lähettämällä vääriä valelohkoja muutamalle (=pienelle osajoukolle) ryhmän vertaisista. Nämä luottavaiset vertaiset puolestaan välittävät näitä vääriä valelohkoja edelleen muille ryhmän vertaisille, jotka välittävät niitä edelleen, jne. Tämän vuoksi BitTorrentin toiminnalle on elintärkeää että vertainen voi varmistua lohkon eheydestä (integrity), jotta ei välitä valelohkoja tai viallisia lohkoja edelleen. Oletetaan nyt, että vertaistoimijaryhmään liittyvä vertainen saa .torrent –tiedoston täysin luotettavasta lähteestä. Kuvaile yksinkertainen menetelmä, jolla vertainen voi tällöin varmistaa lohkon eheyden.

4. Todentaminen julkisen avaimen salauksella (Ch8P15 ja Ch8P16)
Bob ja Alice käyttävät julkisen avaimen salausta todentamiseen. Alice ottaa yhteyttä Bobiin 'I am Alice'. Bob lähettää Alicelle haasteen (nonce), jonka Alice palauttaa salattuna omalla salaisella avaimellaan. Bob voi Alicen julkisella avaimella todentaa Alicen. Tässä ei käytetä varmenteita.

a. Piirrä viestien vaihto Alicen ja Bobin välillä. Kirjaa julkiset ja salaiset avaimet kirjan (ja kalvojen) käyttämällä notaatiolla.
b. Kuvaa kuinka Trudy voi pujottaa itsensä Alicen ja Bobin väliin kaappaamalla Alicen viestit ja tekeytymällä Aliceksi Bobille.
c. Miksi ja miten varmenteiden käyttö estää Trudyn toiminnan b-kohdassa kuvatulla tavalla?

5. Palomuuri (Ch8P25)
Muodosta tilalliselle palomuurille mahdollisimman rajoittava pääsynvalvontalistoihin pohjautuva suodatustaulu (filter table) ja yhteyksien tilaa säilyttävän tilataulu (connection table), kun palomuurin pitää kuitenkin

- sallia kaikkien sisäverkon käyttäjien telnet yhteydet ulkopuolisiin palvelimiin
- sallia ulkopuolisille käyttäjille www-sivujen katselu palvelimelta 222.22.0.12
- estää kaikki muu sisään- ja ulospyrkivä liikenne

Sisäverkon verkkopeite on 222.22/16. Yhteyksientilataulussa voit ajatella tarkasteluhetkellä olevan kolme yhteyttä sisältä ulospäin. Keksi tarvittavat IP-osoitteet ja porttinumerot.

6. Täytä kurssipalaute tai lupaa pyhästi täyttää se oitis tentin jälkeen.

☆YLIMÄÄRÄINEN TEHTÄVÄ: Kuinka paljon eri varmentajia selaimesi tuntee? Mistä tämän listan löydät ja kuinka voit poistaa varmentajia listalta?

☆WIRESHARK: Kirjan tehtävä P19, luvusta 8 sivulta 775 eli Ch8P19 on hyvä wireshark tehtävä SSL:ään liittyen. Kirjassa on kuvakaappaus wiresharkin toiminnasta ja joukko kysymyksiä tähän kuvakaappaukseen liittyen. Varsinaisesti wireshark ohjelmaa ei tehtävässä tarvita.