Tietoturvan perusteet, harjoitus 2, 29.3.-9.4. 2010

Huom: Pääsiäisloman takia torstain ryhmät siirtyvät seuraavalle viikolle.

1. Mitä pääsynvalvontamallia seuraavat tapaukset edustavat:

   a) Tavallisen käyttäjän luomat tiedostot.

   b) Opintosuoritusrekisteri Oodi.

   c) Kokeiden vastauspaperit.

   d) Valtioneuvoston kanslia.

   e) Käyttöjärjestelmän prosessit.

2. Esitä yhteenveto ja oma näkemyksesi artikkelista Herley, van Oorschot, Patrick: Passwords: If We're So Smart, Why Are We Still Using Them? FC 2009, Lecture Notes in Computer Science 5628, pp.230-237, Springer 2009.

3. Oletetaan, että salasanat koostuvat 95 näppäimistön ASCII-merkistä ja että ne ovat 10 merkin mittaisia. Murto-ohjelmisto testaa 6,4 miljoonaa salasanaa sekunnissa. Kuinka kauan siltä kestää testata kaikki salasanat?

4. Oletetaan, että käytössä on teratavun muisti. Salasanaketjuista talletetaan ensimmäinen ja viimeinen salasana. Kuinka pitkiä ketjujen tulisi olla, jotta edellisen tehtävän kaikki salasanat löytyisivät ketjuista? (Oletetaan, että ketjut ovat erillisiä ja että kaikki salasanat löytyvät niistä.)

5. Oletetaan, että ohjelma D tutkii, sisältääkö jokin koodi viruksen. Toisin sanoen, jos P on mikä tahansa ohjelma ja $D(P)$ ajetaan, niin D palauttaa arvon TOSI, jos P sisältää viruksen, muuten arvon EPÄTOSI. Tarkastellaan seuraavaa ohjelmaa:

```
program CV :=
  {....
   main-program :=
      (if D(CV) then goto next else infect-executables;

       next:
   }
```

   Yllä `infect-executables` on viruksen tartuttava ohjelma. Tutki, päätteleekö D oikein, sisältääkö CV viruksen vai ei.