Introduction to Computer Security, exercise 2, March 29 - April 9, 2010

Obs: The Thursday exercise groups are move to the next week because of the Easter vacation.

1. Classify each of the following as an example of a mandatory, discretionary, originator controled, or role-based controlled policy, or a combination thereof. Justify your answers.

    a) The file access control mechanisms of the UNIX operating system.

    b) The data in the register system Oodi.

    c) The papers students have given at an examination.

    d) Prime minister's office.

    e) The processes of an operating system.

2. Make a summary and express your own view on the article 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. Assume that passwords are limited to the use of the 95 printable ASCII characters and that all passwords are 10 charcters in length. Assume a password cracker with an encryption rate of 6.4 million encryptions or hash per second. How long will it take to test exhaustively all possible passwords?

4. Let us assume that there is a terabyte memory and you are constructing password chains. Of each chain, only store the first and last password. How long should the chains be so that all the passwords in the previous exercise can be found in the chains? (Assume that the chains are separate and all the passwords are in the chains.)

5. The question arises as to whether it is possible to develop a program that can analyze a piece of software to determine if it is a virus. Consider that we have a program D that is supposed to be able to do that. That is, for any program P, if we run $D(P)$, the result returned id TRUE(P is a virus) or FALSE(P is not a virus). Now consider the following program:

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

       next:
  }
```

In the preceding program, infect-executables is a module that scans memory for executable programs and replicates itself in those programs. Determine if D can correctly decide whether CV is a virus.