Security

Assignment 8, Wednesday November 5 (very late), 2008

Goals: After successfully completing this exercise you should have a working grasp of Bell-Lapadula model, hierarchical (tree) certification authorities, message authentication codes.

Deadline: Friday November 14, during the lecture or earlier in Flavio's or Olha's post box (in the white cabinet near the printer at the station-side-end of the corridor on the second floor of the Huygens building).

1. (3 points) In the Bell-Lapadula model (recall Bart's lecture on 31/10) the "read down and write up" restriction guarantees:

   - Authentication
   - Confidentiality
   - Integrity
   - Non-repudiation

   Instead, if you consider the "read up and write down" restriction, it guarantees:

   - Authentication
   - Confidentiality
   - Integrity
   - Non-repudiation

2. (3 points) Tanenbaum 8.24.

3. (4 points) Recapitulate the definition of *Message Authentication Code (MAC)*.

   - which properties MAC guarantees:
     - Authentication
     - Confidentiality
     - Integrity
     - Non-repudiation?
   - what differs MAC from *digital signatures*?