Security

Assignment 6, Wednesday October 22, 2008

Goals: After successfully completing this exercise you should be able to analyse simple authentication protocols.

Deadline: Friday October 31, 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) Tanenbaum, exercise 8.30.
2. (3 points) Tanenbaum, exercise 8.31.
3. (4 points) An exercise from Flavio G. Consider the following authentication protocol between a user A and a server S. The server stores: $\langle A, n, Y = h^n(PWD_A)\rangle$. The user A stores her password PWD_A. The protocol looks as follows:

$$\begin{aligned} A &\rightarrow S: \ A \\ S &\rightarrow A: \ n \\ A &\rightarrow S: \ X = h^{n-1}(PWD_A) \end{aligned}$$

   The server checks if $h(X) = Y$, then decrements n and sets $Y := X$. Otherwise authentication fails.

   When $n = 0$ the password needs to be reset.

   Questions:

   - Is this protocol vulnerable to dictionary attacks? (Explain, why.)
   - How can an evil middle-person E abuse this protocol when E intercepts a logon attempt. (Explain, why this abuse will work.)