Security

Assignment 1, Wednesday 10 September 2008

Goals: After completing this exercise successfully you should be able to identify and reason about security requirements of informally formulated systems.

Deadline: Friday September 19, 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. Find a description of the computer system BOS (Beslis en Ondersteunend Systeem) that controls the "kering"s in Zuid-Holland. For instance, go to
   http : //www.keringhuis.nl/home_noflash.html,
   then choose "maeslantkering", then "constructie", then "beslis- en besturingssystem (BOS en BES)".

   After you have an idea how it works, give concise answers to the following questions:

   (a) what can be the safety and security issues for BOS? Attention: we are discussing safety and security of the computer system itself, but not the safety and security of the land. Hint for security: do not forget about software maintenance (updates, testing, etc.)

   (b) Describe the reasonable security goals for BOS, according to the properties of confidentiality, integrity, availability, accountability, authentication.

2. Digital Security (DS) research group is looking to implement a modern way to track appointments, meetings, classes, conference visits, etc. The group wants to use a Web-based calendar system. Group members should be allowed to enter appointments, invite each other for joint meetings, look into each others calendar, synchronize with a privately owned PDA based calendar; moreover, some group members, for example the groups management assistant, should be allowed to plan appointments for others.

   For each of the following (groups of) persons find a reason (motive) why they may want to attack the calendar systems security. Also, think of at least three other roles with associated attack motives.

Role	Motive
A student	To see when a group member is out of office in order to change one's mark.
Bart Jacobs (Prof in DS)	To check each group members private calendar in order to check for job interviews at competing research groups.
Pieter Hartel (Prof Security in Enschede)	...
Erik Poll (UHD of DS)	...
Maria van Kuppeveld (The secretary of DS)	...
An employee that was fired	...
Some script kiddie	...
The AIVD (Secret service)	...
. . .	...

Remark: For both tasks above we are not interested in implementation aspects of or concrete worked out attacks on to the calendar system, but merely in the goals and the motives. For example: guessing a password is, by itself, not a motive of an attacker final motive is always something else.

3. Answer these multiple choice questions about security goals and briefly indicate why your choice is valid (or why other choices are less valid). The length of your explanation should be shorter than the length of the question.

   (a) A scientist has copied a fragment of text from another authors article without proper citation. Which security goal is concerned?

      i. authenticity
      ii. availability
      iii. confidentiality
      iv. integrity
      v. non-repudiation

   (b) A producer of portable music players (and stylish computers for creative people) also sells music online and uses encryption in its difficult to play the music on music players sold by the competition. Which security goal is concerned?

      i. authenticity
      ii. availability
      iii. confidentiality
      iv. integrity
      v. non-repudiation

   (c) The ministry of foreign affairs is working on a database for centralized storage of biometric data of all Dutch citizens (i.e. a finger print). In the original plan such biometric data would only be stored in an embedded chip in each citizens own passport, which already allows the authorities to check whether a passport belongs to the person presenting the passport. The centralized storage allows the authorities, in addition to this, to check which citizen belongs to a given finger print. Which contradiction signifies the difference in use of biometric data between the original plan and the new approach of the ministry?

      i. biometrics for authentication versus biometrics for identification
      ii. biometrics for authorization versus biometrics for authentication
      iii. biometrics for authorization versus biometrics for identification
      iv. biometrics for confidentiality versus biometrics for authenticity
      v. biometrics for non-repudiation versus biometrics for authenticity