The electronic health card, summer 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

7. Exercise sheet
Hand in solutions until Monday, 9 June 2008.

Exercise 7.1 (PKI). (6 points)

Before Bob can communicate with Alice he needs her public key.

(i) So Alice sends her public key in plaintext over the internet to Bob. Should Bob now use and trust it? Argue. [1]

(ii) Charlie has published his public key in various newspapers. You've got copies of two independent newspapers containing it. A comparison shows that Charlie's public key is identical in both copies. Should you now trust Charlie's signatures that you verify with his key? Argue. [2]

(iii) Explain how Charlie can convince Bob in a more elegant way that his public key is authentic. [2]

(iv) Explain an advantage of a hierarchic PKI. [1]

Exercise 7.2 (Authentication for health cards). (6 points)

In class we discussed the advantages and disadvantages of different authentication methods. For example we were comparing PINs and fingerprints. Create a table with the pros and cons of both of these authentication methods. Decide on your favourite method and justify your decission. [6]

Exercise 7.3 (Requirements vs. Threads). (6 points)

While we were talking about the general concepts of the electronic health card, a number of threads emerged. Pick one requirement for the electronic health card, describe which kind of threads are connected to this requirement. Describe which ideas you have to counteract these threads. If you do not have any ideas how to counteract them, describe which problems you had to face. [6]

Exercise 7.4 (Different kinds of data). (5 points)

5

In class we have seen that various types of data, like referral to a specialist or information about the drugs prescribed, differ in their degree of confidentiality, integrity, availability, authenticity and non-repudiation. Grade and justify the data object "Prescription of hospital treatment" in terms of the above five aspects.