

Information and Communications Security SS 08 Assignment 1

Fachbereich
Wirtschaftswissenschaften

Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security
www.m-lehrstuhl.de

Prof. Dr. Kai Rannenberg
Dipl.-Kfm. André Deuker
Dipl.-Inf. Jan Zibuschka

Telefon +49 (0)69-798 25301
Telefax +49 (0)69-798 25306
E-Mail kai.rannenberg@m-lehrstuhl.de

Exercise 1: Nowadays, passwords are probably the most widely used form of authentication. Passwords are usually chosen by the user and often saved on the server in encrypted form.

- Name one defense mechanism for password authentication systems that is enacted after the user chooses a password, and one mechanism that is enacted after each login. Describe advantages and potential problems of both mechanisms.
- Classify the following proposed passwords as good choices or poor choices, and justify your reasoning: “Bayern”, “go2work”, “cat&dog“, “3.1piNUMB”

Exercise 2: Assume that you are only allowed to use the 26 characters from the alphabet and the 10 number characters to construct passwords.

- How many different passwords are possible if a password is exactly n characters long (for $n = 4, 6, 8$) and there is no distinction between upper case and lower case characters?
- How many different passwords are possible if a password is exactly n characters long (for $n = 4, 6, 8$), and passwords are case sensitive?

Exercise 3: There are several methods for authenticating users based on different classes of attributes they may supply to the service.

- Name the different forms of authentication.
- It is also possible to combine several authentication methods. Name an authentication method you would not use without combining it with other factors (Why?).

Exercise 4: A computer system uses biometrics to authenticate users. Discuss ways in which an attacker might try to spoof the system under each of the following conditions:

- The biometric hardware is directly connected to the system, and the authentication software is loaded onto the system.
- The biometric hardware is on a stand-alone computer connected to the system, and the authentication software on the stand-alone computer sends the raw biometric data read to the system, which decides whether or not the user can be authenticated.

- c. The biometric hardware is on a stand-alone computer connected to the system, and the authentication software on that stand-alone computer sends “yes” or “no” to the system, depending on whether or not the user can be authenticated.