

Information and Communications Security SS 11 Assignment 1

Fachbereich
Wirtschaftswissenschaften

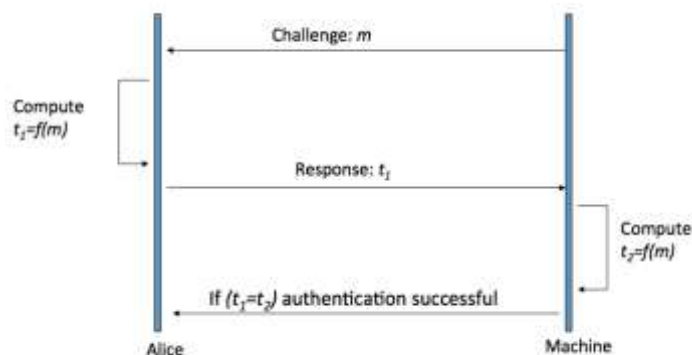
Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security
www.m-chair.net

Prof. Dr. Kai Rannenberg
M.Sc. Ahmad Sabouri
Dipl.-Ing. (FH) Christian Weber

Telefon +49 (0)69-798 34705
Telefax +49 (0)69-798 35004
E-Mail sec@m-chair.net

Study the following questions and return your answers by email to ahmad.sabouri@m-chair.net, before **18th of April 2011, 18:00 pm**. Please put “SEC-SS11-HW1” in the subject of the email.

Exercise 1: Alice and a remote machine are supposed to perform a *mutual authentication* (where both parties want to make sure about the identity of each other) during the login phase. Does the following challenge/response scheme fulfill this requirement? If yes, how? And if no, why?



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 and passwords are case sensitive?
- How many different passwords are possible, if a password is exactly n characters long, passwords are case sensitive and it should contain at least 1 number and 1 capital letter?

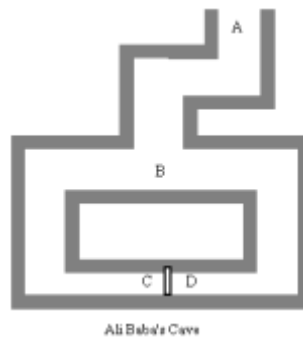
Exercise 3: Ali Baba's cave is a simple example of a Zero-Knowledge proof protocol. Alice wants to prove to Bob that she knows the secret words that will open the portal CD, but she does not wish to reveal the secret to Bob. In this scenario, Alice's commitment is to go to point C or point D. A typical round in the proof proceeds as follows: Bob goes to point A and waits there, while Alice goes to C or D. Bob then goes to B and shouts to ask Alice to appear from either the right side or the left side of the tunnel. If Alice does not know the secret words (e.g., "Open Sesame"), there is only a

Campus Westend • Grüneburgplatz 1 • D-60629 Frankfurt am Main

H i e r w i r d W i s s e n W i r k l i c h k e i t



50% chance that she will come out from the right tunnel. Bob can repeat this round as many times as he desires, until he is certain that Alice knows the secret words. No matter how many times that the proof repeats, Bob does not learn the secret words. And if Alice really knows the secret word, she should be able to come back in the correct direction all the time.



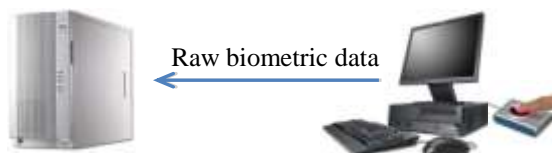
If Bob wants to reach over 99% confidence about Alice's knowledge of the secret word, how many times he has to repeat this game?

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:

- a. The biometric hardware is directly connected to the system, and the authentication software is loaded onto the system.



- b. 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.

