JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Fachbereich Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security

Fachbereich
Wirtschaftswissenschaften

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

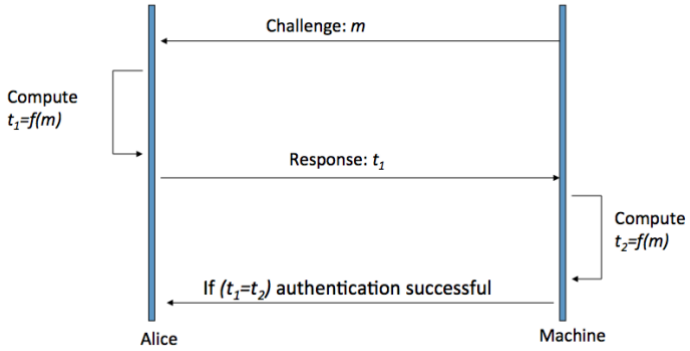
Prof. Dr. Kai Rannenberg
Sascha Löbner, MSc.

E-Mail security@m-chair.de

Information and Communications Security
WS 2020/21
Assignment 1
Authentication

Please prepare your solutions for the following exercises. We will discuss them on the 26th of October 2016.

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



Exercise 2: Assume that you are only allowed to use a combination of letters and numbers to construct a password. For the letters, let us assume we are using the English alphabet, which consists of 26 different characters, and for the numbers the Arabic numbers from 0-9.

a) How many different passwords are possible if a password is exactly *n* characters long, and passwords are case not sensitive?
b) How about when we have a distinction between case-sensitive and non-case-sensitive characters?

Exercise 3: A web-server stores teaching and administrative material for the security course at the university. Among others, there is a file called “exam.ps” which is particularly interesting for the students. Access to the server requires authentication through passwords.

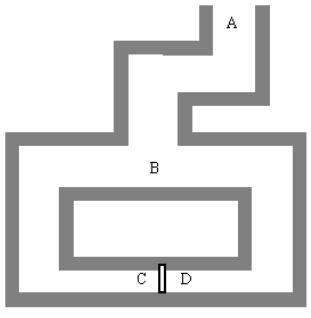
a) Discuss what you think happened from reading the logs of the server below.
b) What could be used to improve the security situation in this case?

```
212.1.5.50 [11/Feb/07:18:46:59] "GET /exam.ps" 401 482 user sec: password
mismatch
212.1.5.50 [11/Feb/07:18:47:01] "GET /exam.ps" 401 482 user sec: password
mismatch
212.1.5.50 [11/Feb/07:18:47:09] "GET /exam.ps" 401 482 user sec: password
mismatch
212.1.5.50 [11/Feb/07:18:48:38] "GET /exam.ps" 401 482 user sec: password
mismatch

[200 similar lines]

212.1.5.50 [11/Feb/07:19:21:42] "GET /exam.ps" 401 482 user sec: password
mismatch
212.1.5.50 [11/Feb/07:19:22:00] "GET /exam.ps" 401 482 user sec: password
mismatch
212.1.5.50 [11/Feb/07:19:23:12] "GET /exam.ps" 401 482 user sec: password
mismatch
212.1.5.50 [11/Feb/07:19:23:53] "GET /exam.ps" 401 482 user sec: password
mismatch
212.1.5.50 [11/Feb/07:19:23:53] "GET /exam.ps" 200 62664 transfer ok
```

Exercise 4: 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 A or B. A typical round in the proof proceeds as follows: Bob goes to 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 50 percent chance that she will come out from the right tunnel. Bob will 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.



Ali Baba's Cave

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 5: In the lecture, you learnt about four types of authentication based on the authentication factor, based on „what you know“, „what you have“, „what you are“, and „where you are“. Give an example of each of them.

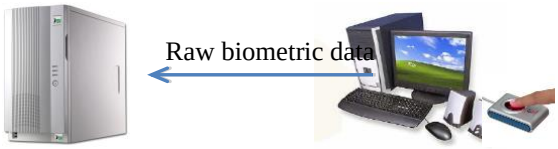
Exercise 6: A bank uses a biometric system to authenticate employees entering the safe where the money is stored overnight. To get in the room, one has to type in the username and put his/her finger on the sensor. The fingerprint is then digitalized and sent to the authentication server, which accepts or rejects access to the room. The authentication server relates the username with the digital version of the fingerprint. Statistical analysis show that the authentication server has a false-reject rate of 10% and a false-accept rate of 0,5%. The user is allowed to try five attempts, after which security guards are called and the user is intercepted.

a) Explain what false-accepts and false-rejects are. Are the above-mentioned rates suitable for this kind of application?
b) If Tom finds a way to manipulate the fingerprint-reader as he wants, what interesting data would he be able to collect? How can he exploit what he collects?

Exercise 7: 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.

Exercise 8: As an everyday example of authentication is the use of mobile-banking.

a) What experiences do you have with your bank? What kind of authentication scheme does the bank use?
b) What are the possible attacks on the authentication scheme of the bank?
c) What are the drawbacks of the given scheme? Think about usability, convenience, and ease of use.
d) Can there be improvements to the security of the authentication scheme? If yes, what?