JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

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

Fachbereich
Wirtschaftswissenschaften

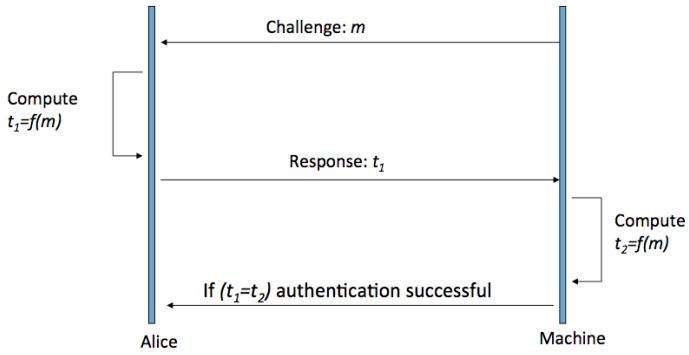
Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security
www.m-chair.de

Prof. Dr. Kai Rannenberg
M.Sc. Fatbardh Veseli
M.Sc. Ahmed S. Yesuf
M.Sc. Christopher Schmitz

E-Mail sec@m-chair.de

Information and Communications Security
WS 14/15
Assignment 1
Solution

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 fulfill this requirement? If yes, how? And if no, why?



Answer:
This protocol does not satisfy a mutual authentication. In the way that it works, only the Machine can make sure that the other side is Alice. Because it receives the response of the challenge and can compare it to its own answer. Since Alice does not examine the Machine, there is no way for her to ensure about the identity of the device.

Exercise 2: **(Updated)** 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?

Solution:

a. We have *n* characters for the password and each one can be either an
-uppercase letter,
-lowercase letter, or
-a digit (number).

Therefore, **each character** can take one of the 26 + 10 = 36 possible values.
As a result, a password consisting of n characters can have $\mathbf{36^n}$ different combinations.

b. Considering that now we have to count both upper and lower-case letters (case sensitive), the number of combinations for a character is:
26 + 26 + 10 = 62. For n characters, that would then be 62^n different combinations.

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.

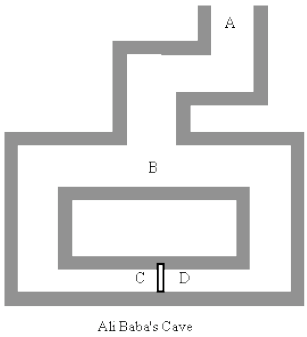
a) Discuss what you think happened from reading the logs of the server below.
b) What could be used to improve the security situation in this case?

```
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
```

Solution:

Someone attempted to get access to the protected file "/exam.ps" in the server a number of times without success (brute force attack or similar). Finally, the attacker seems to have found the right password and downloaded the requested file.
A number of solutions could be used to enhance the security in this case. For instance, adding additional authentication factors, limiting the number of suspicious activities by detecting multiple trials from the same source, etc.

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.



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?

Solution:
In order to have over 99% confidence, we need to repeat the protocol till the point that the probability of answering all the challenges correctly without knowing the secret key becomes less than 1%. If the chance for a correct answer without the knowledge of the secret key is 50%, after one round the probability of a false authentication is 0.5, after two rounds is 0.5^2=0.25, and so on.
We need $0.5^n < 0.01$, therefore n=7.

Exercise 5: In the lecture, you learnt about three 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.

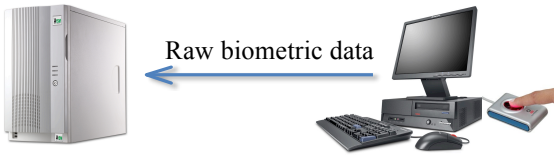
a) Explain what false-accepts and false-rejects are. Are the above-mentioned rates suitable for this kind of application?
b) If Tom finds a way to manipulate the fingerprint-reader as he wants, what interesting data would he be able to collect? How can he exploit what he collects?

Solution:
If a non-authorized person is successfully authenticated to the server and given access to the room, then we talk about False Acceptance. A false rejection means that the fingerprint of an authorized person (employee) was wrongly rejected as unauthorized. Since the False Acceptance Rate and the False Rejection Rate are negatively related (increasing one decreases the other and vice verca), it is essential in the current application that the FAR be much less than the FRR, and low enough in general. The fact that the user is allowed to attempt five times partially compensates for the given relatively-high FRR.
If Tom can hack the fingerprint-reader as he wants, then he could basically read and copy all digital fingerprints of the employees using this reader. Having the digital fingerprints available, he could then potentially counter the authentication server by directly sending the fingerprints of other employees and access the room.

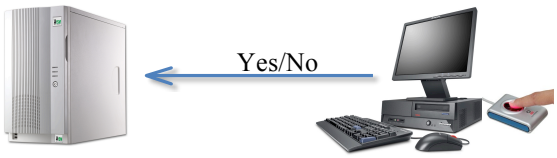
Exercise 7: A computer system uses biometrics to authenticate users. Discuss ways in which an attacker might try to spoof the system under each of the following conditions:

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.



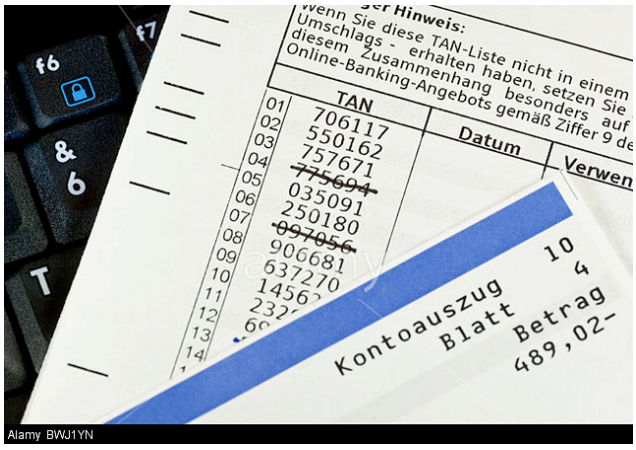
Solution:

a. When the authentication module is directly connected to the server, it provides the most secure way. But usually data servers are located somewhere else, so the users need to communicate through a network.
b. This case gives a more flexible access to the end user but on the other hand, an attacker can spoof the communication channel. In order to proceed with the authentication, the attacker needs to somehow get the biometric data of a valid user, provide it to the server through the intercepted link and then gets access to the server.
c. The last case is more vulnerable to the spoofing attacks because as soon as the attacker intercepts the communication and convinces the server that it is the terminal, it can send a "Yes" and perform a fake authentication. There is no need to find the biometrics of a valid user.

Discussion point 8: As an everyday example of authentication is the use of e-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?


3G
15:37
Ihre Bank
15.08.2011 13:18
Ihre mobileTAN lautet:
952422, fuer Empfaenger:
67492750, Uhrzeit: 13:16:37
UHR.


Hinweis:
TAN
Datum
706117
550162
757671
775694
035091
250180
897056
906681
637270
Kontoauszug
Blatt
Betrag
489,02-
Alamy BWJ1YN


VASCO
TAN, F oder Menü
1
2
3
TAN
4
5
6
F
7
8
9
MENU
C
0
,
OK
DIGIPASS