mobile business

Assignment 1

Authentication

Information and Communications Security (WS 2018/19)

Prof. Dr. Kai Rannenberg
Abtin Shahkarami(M.Sc.)
Welderufael B. Tesfay (M.Sc.)

Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

What is **authentication**?

- **Definition:** Authentication is the binding of an identifier to a subject.
- The subject must provide information to enable the system to confirm the relation between subject and identifier.
- In technology: The verification of the identity of a person or process. In a communication system, **authentication verifies that messages really come from their stated source**, like the signature on a (paper) letter.

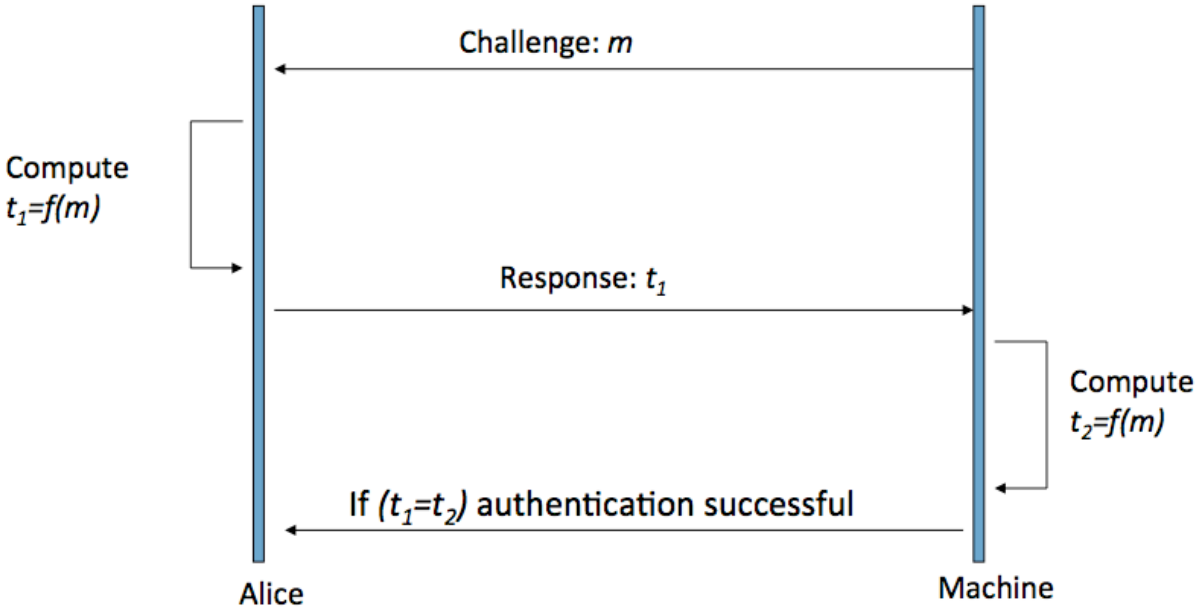
[Dict16][Bi05, modified]

mobile business

Exercise 1: Mutual authentication

Exercise 1: Mutual Authentication

- Alice and a Machine are supposed to perform a *mutual authentication* (where 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 to Exercise 1

- No. In the way that it works, only the *Machine* can authenticate *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 authenticate the device.

mobile business

Exercise 2: Password combinations

mobile business

Exercise 2: Password combinations

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

Exercise 2.a) Password combinations:

- Step by step:
  - Each character can be either a letter or a number.
  - Each letter can have 26 possible values.
  - Each number can have 10 possible values.
- If password is 1-character long, we can have

  One of the 26 letters OR one of the 10 numbers =

  $26 + 10 = 36$

  different options.
- For 2 characters, we have

  (*Letter or number*) * (*Letter or number*) =

  $36 * 36 = 36^2$
- For 3 characters, we have

  $36 * 36 * 36 = 36^3$
- …
- For *n* characters, we can have

  $36 * 36 * 36 * \ldots * 36$ (n-times) = 36^n

  different combinations.

mobile business

Solution to Exercise 2(b)

b. What if we distinguish between case-sensitive and non-case-sensitive letters?

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

Each character can possibly have

$$26 + 26 + 10 = 62$$

different values.

For *n* characters, $\mathbf{62^n}$ different combinations can be used as a password.

mobile business

Exercise 3: Server logs

Server logs (1)

- **Q:** 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.
  - Discuss what you think happened from reading the logs of the server below.
  - What could be used to improve the security situation in this case?

mobile business

Server logs (2)

What do you think has happened?

```
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
```

Server logs (3)

What can be done to improve the security?

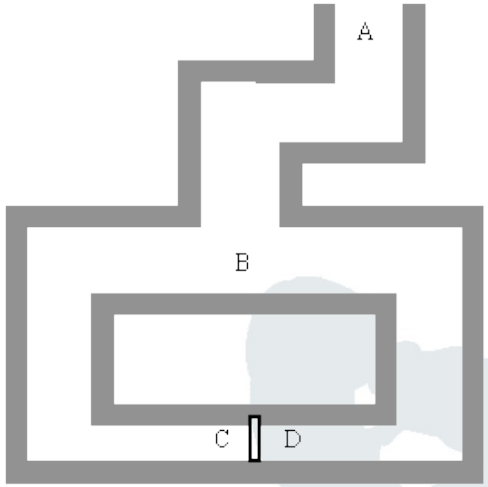
- Detect suspicious activity. Limit login attempts from the same source.
- Provide a different authentication mechanism from passwords.
- Add more authentication factors (two or more).

mobile business

Exercise 4: Zero-knowledge proofs

4: Ali Baba's Cave – ZK proof
The scenario

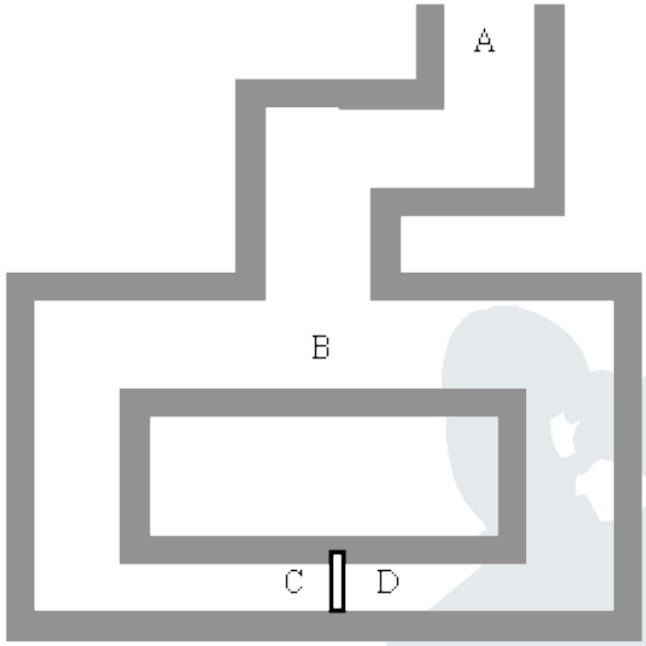
- Alice wants to prove to Bob that she knows the secret words that will open the portal CD, but she does not wish to reveal the secret to Bob. In this scenario, Alice's commitment is to go to A or B. She should show that she can pass from C to D without telling Bob the secret.
- A typical round in the 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% 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

4: Ali Baba's Cave ZK (2)

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



Ali Baba's Cave

mobile business

Solution to Exercise 4:

- 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%.
- Let p be the chance that Alice can guess right the secret:
  - After *one* round the probability of a ***false*** authentication is 50%:

$$p_1 = 0.5$$

  - After two rounds, $p_2 = 0.5^2 = 0.25$
  - ...
  - After n rounds, $p_n = 0.5^n$

- We need

$$p_n < 0{,}01$$
$$\Rightarrow 0.5^n < 0.01$$
$$\Rightarrow n > \log_{0.5} 0.01 \approx 6.67$$

- Therefore, *n* must be no smaller than 7.

mobile business

Exercise 5: Types of authentication

5: Types of authentication

- Q: 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!

5: Types of authentication Solution

What you know	Password
What you have	Smart card, token, etc.
What you are	Biometric features (voice, fingerprint, gait, etc.)
Where you are	e.g. accessing the university resources from the campus.

Exercise 6: Biometrics

6: Fingerprint recognition system

- 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* (FRR) of 10% and a *false-accept rate (FAR)* 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?

6: Fingerprint recognition system
Solution a)

- 6a) Explain what false-accepts and false-rejects are. Are the above-mentioned rates suitable for this kind of application?
- 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 FAR and the FRR are 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.

6: Fingerprint recognition system
Solution b)

- 6b) 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?
- 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)

- 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.

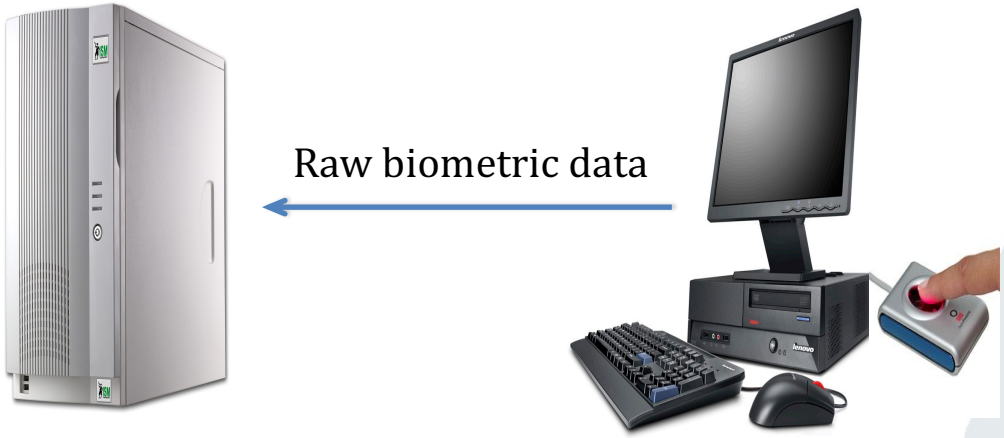
a. The biometric hardware is directly connected to the system, and the authentication software is loaded onto the system.

Solution to Exercise 7(a)

- When the authentication module is directly connected to the server, it provides the most secure way.
- The only way to spoof/attack this authentication is to spoof the authentication server and replace it with something else. This is in practice less feasible.
- In practice, data servers are located somewhere else, so the users need to communicate through a network.

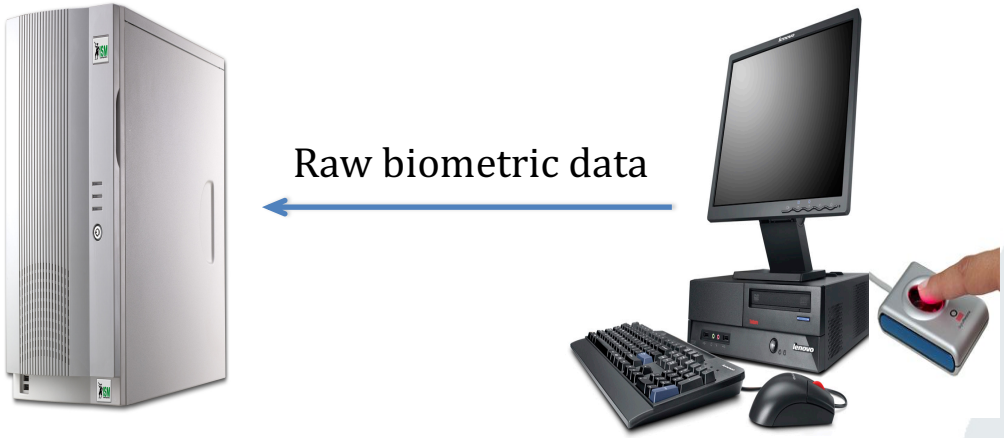
Exercise 7(b)

- 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 on a stand-alone computer connected to the system through the Internet.
  - The authentication software on the stand-alone computer reads the raw biometric data from the user and sends them to the server, which then decides whether or not the user can be authenticated.



Solution to Exercise 7(b)

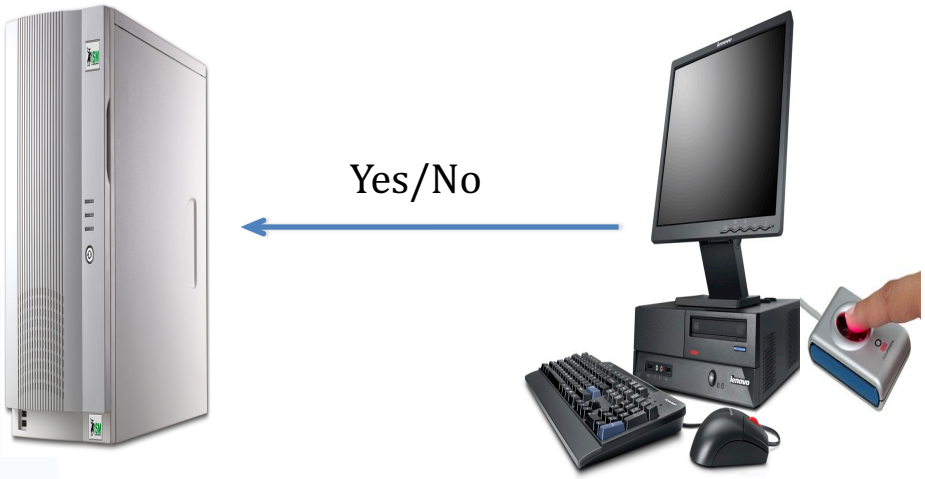
- This case gives a more flexible access to the end users.
- On the other hand, an attacker can spoof the communication channel.
- In order to proceed with the spoofing attack, the attacker needs to somehow get the biometric data of a valid user, provide it to the server through the intercepted link and then get access to the server.



Exercise 7(c)

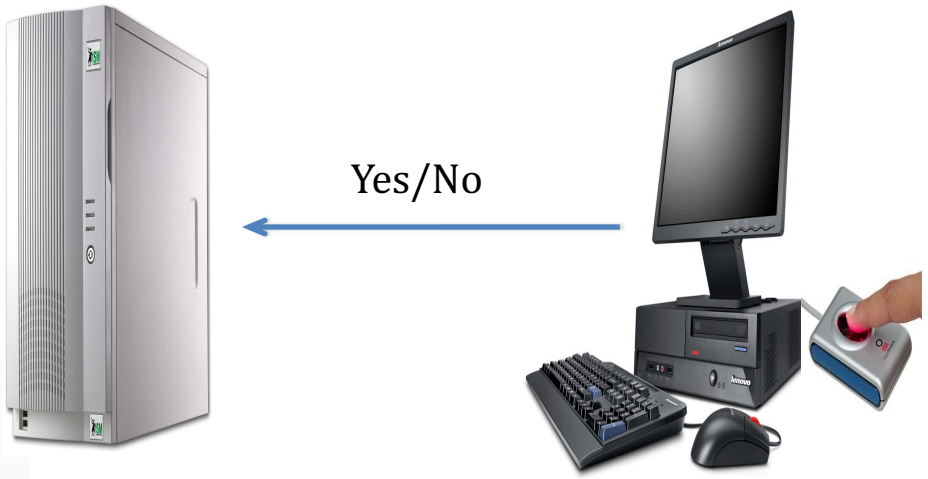
- A computer system uses biometrics to authenticate users. Discuss ways in which an attacker might try to spoof the system under each of the following conditions.

c. The biometric reader is connected to the computer, which is connected to the authentication system via the network. The authentication software on the computer sends sends a "Yes" or "No" message to the server, depending on whether or not the user can be authenticated.



Solution to Exercise 7(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.
- On the other hand, personal computers may be more vulnerable to attacks, so manipulating the computer to send a „yes“ can be easier than manipulating the server, which is usually more secured.

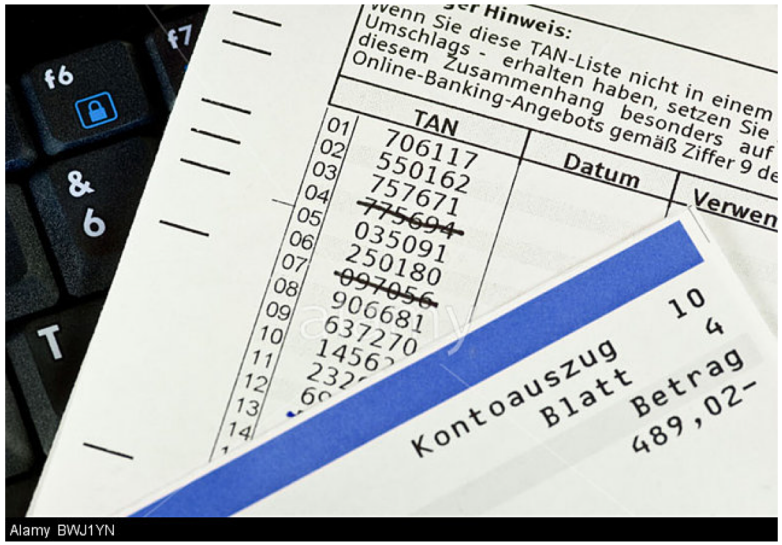


8: Your experiences with authentication

- As an everyday example of authentication is the use of e-banking.
  - What experiences do you have with your bank? What kind of authentication scheme does the bank use?
  - What are the possible attacks on the authentication scheme of the bank?
  - What are the drawbacks of the given scheme? Think about *usability*, *convenience*, *and ease of use*.
  - Can there be improvements to the security of the authentication scheme? If yes, what?

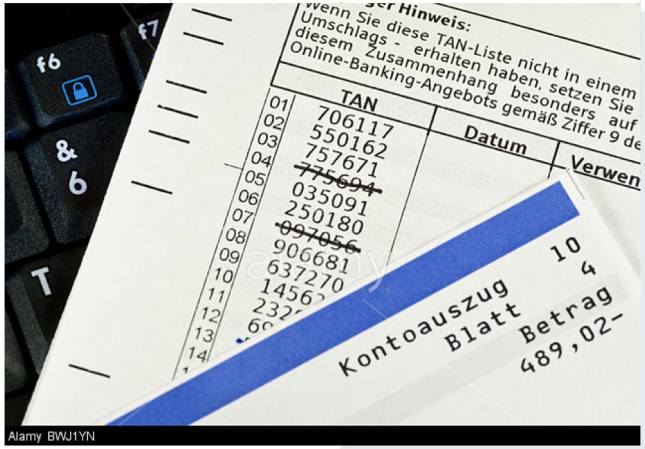
mobile business

Examples: TANs



8: Your experiences with authentication

- What kind of authentication scheme does the bank use?
- What are the possible attacks on the authentication scheme of the bank?
- What are the drawbacks of the given scheme? Think about *usability, convenience, and ease of use*.
- Can there be improvements to the security of the authentication scheme? If yes, what?



mobile business

Thanks for your attention!

- For questions, feedback, suggestions:
  - security@m-chair.de
  - abtin.shahkarami@m-chair.de
  - welderufael.tesfay@m-chair.de

References

- **[Bi05] Bishop, Matt.** *Introduction to Computer Security*. Boston: Addison Wesley, 2005. pp. 171-198.
- [Dict16] **Dictionary.com**, "authenticate," in Online Etymology Dictionary. Source location: Douglas Harper, Historian. http://dictionary.reference.com/browse/authenticate. Available: http://dictionary.reference.com. Accessed: Apri 18, 2016.