Security in Organizations (SIO)

Assignment 2 - 2021-2022

Goal:

- Assess the risks for a two-factor authentication digital service.

Instructions:

- This assignment must be completed by a team of two students.
- The assignment must be written with the Times New Roman font, in size 12pt, with normal spacing. The subtitles are in bold, and the margins must be all of size 2.5cm.
- The original numbering of the questions must be indicated for each answer.
- State your answers in a succinct and clear manner.

Deadline:

- Submit the assignment in a PDF document through Brightspace before **2021/10/21 23:59.**

If and only if you do not have a Brightspace access, you can submit your assignment by email to Anna Guinet (see SIO website) in a PDF document.

Tiqr is a two-factor authentication application developed by Surfnet that makes use of QR codes. A demo is available at [1] where the fictive bank “Piggy Bank” uses Tiqr as an authentication mechanism. Henceforth, you assume that the Piggy Bank is real, and it uses Tiqr. Additional resources are listed below.

- The enrolment page of this demo is available on [2].
- The logon page on [3] can be used after the enrolment through Tiqr.
- The technical and cryptographic details of Tiqr are reported in [4].
- The results of a penetration test on Tiqr conducted are presented in [5].
- The source code of the Tiqr app for Android and IOS is available in [6].

A. Describe at least five vulnerabilities that you found in the Tiqr enrolment setup [2].

B. For each vulnerability that you have found in the question A, describe a scenario where a malicious user exploits the vulnerability.

C. From the potential risks that you have described in the question B,

   a. would you rate the risks as acceptable for a bank? Motivate your answer.

   b. If the risks are not acceptable, present the most relevant security measures that would compensate such risks.

D. After the creation of a bank account at Piggy Bank, the balance is set to zero euro by default. Does that imply that the risks that you have identified in the question B are negligible? Motivate your answer.

E. The EU regulation of authentication mechanisms is described in [7]. Do the enrolment and the usage of the Tiqr app on the demo site [1] comply with this regulation? Motivate your answer.

F. According to the EU regulation [7], which aspect(s) of the life-cycle of an authentication mechanism is(are) lacking on the demo site [1]?

G. Once the customers are logged in to their accounts in the Piggy Bank, they can transfer money by using the Tiqr app. When transferring money, we suppose that the amount and the beneficiary account number are displayed to the users. Which incident(s) would occur if that information would not be not shown to the sender?

H. The Raboscanner from Rabobank [8] is also a two-factor authentication mechanism that is based on QR codes. Mention three main differences between the security of the Tiqr authentication mechanism and the one of the Raboscanner.

I. Identify a fundamental vulnerability in the use of Tiqr by the Piggy bank that is not present during the use of the Raboscanner. *Hint: actually look at the use of the Raboscanner.*

J. From the vulnerability that you have found in the question I, describe a scenario where a malicious user exploits this vulnerability.

K. From the potential risk that you have described in the question J,

a. would you rate the risk as acceptable for a bank? Motivate your answer.

b. If the risk is not acceptable, present the most relevant security measure that would compensate such a risk.

L. On p. 6 of [5], it is mentioned that “tiqr is no more or less vulnerable to phishing than any other two-factor authentication system based on challenge/response (such as e.g. the OTP tokens currently in use by banks or for instance SMS authentication).’ Do you think that this statement is true? Motivate your answer.

The assignment should be four pages at most.

CALCULATION OF THE GRADE	
Question	Max. points
A. Tiqr Vulnerabilities	2
B. Tiqr scenarios	1
C. Tiqr Risks	1
D. Balance risk	1
E. EU regulation	1
F. Life-cycle	1
G. Money transfer incident	2
H. Authentication mechanism	2
I. Fundamental vulnerability	3
J. Fundamental vulnerability scenario	1
K. Fundamental vulnerability scenario risk	1
L. Phishing	1
SUM	**17**
Grade = (1 + 9*(sum_of_points / 17)) rounded to the nearest 0,5 point.	

#	**URL**
[1]	https://tiqr.org/demo/
[2]	https://demo.tiqr.org/simplesaml/module.php/authTiqr/newuser.php
[3]	https://demo.tiqr.org/v1/
[4]	https://tiqr.org/wp-content/uploads/2012/01/tiqr-usenix-lisa-1.1.pdf
[5]	https://tiqr.org/wp-content/uploads/2011/11/tiqr-security-audit-report-v1.1.pdf
[6]	https://github.com/SURFnet
[7]	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002
[8]	https://www.rabobank.com/en/products-and-solutions/wholesale-banking/corporate-connect/new-log-in-procedure/rabo-scanner/index.html