Rheinische Friedrich-Wilhelms-Universität Bonn

Master Course Computer Science

Written Exam

Semester: Winter 2022	Exam Period: 1. x 2. ☐
Module Name: IT Security	
Module Number: MA-INF 3236	Date of Exam: 13.02.2023
Examiner: Prof. Dr. Michael Meier	

To be filled by the Student:

Last name:	Matriculation number:
First name:	
Course of Study	
Master in Computer Science ☐ Master in Education ☐ secondary subject ☐ other ☐	

To be filled by the Examiner:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Σ
10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	150

To be filled by the Examiner:

Grading:

***Grades: very good (1,0; 1,3) good (1,7; 2,0; 2,3) satisfactory (2,7; 3,0; 3,3) sufficient (3,7; 4,0) not sufficient (5,0)**

Date:

Signature of Examiner

Name: _____ *Matriculation number:* _____

Task 1: (Wireless Security – Basics and Jamming) 4+4+2 points

a) What influences the choice of antenna used by an attacker aiming to attack a wireless communication? Explain on an example.

b) Why is security by proximity a flawed security strategy? Explain on an example.

c) Name a protocol aware jamming attack and explain how the attack works against OFDM as used in 802.11a Wi-Fi. Why is it protocol aware?

Task 2: (Wireless Security – Wi-Fi Security) 3+5+2 points

a) What weakness of RC4 does the FMS attack exploit?

b) You are eavesdropping all nearby Wi-Fi packets. You notice a WEP encrypted communication between two devices. What packets can you use to perform the FMS attack as presented in the lecture? Explain what makes these packets usable and why.

c) What makes the WPA2 handshake vulnerable?

Name: _____ ***Matriculation number:*** _____

Task 3: (Wireless Security – Device Identification) 3+3+4 points

a) Give an example for why utilizing device identification techniques can benefit an offensive actor as discussed in the lecture. In what way can the target device and/or its holder be compromised in your example?

b) Describe the difference between direct and indirect device identifying data. Give one example each.

c) Describe a scenario where passive device identification fails but active device identification can be utilized effectively. Why does passive device identification fail but active device identification does not in your given scenario?

Task 4: (Side Channel Attacks) 3+3+4 points

a) Describe the difference between the side channels and covert channels.

b) In the library example of a meltdown-type attack, how was the attacker able to gain information?

c) What information is leaked in the timing side channel attack on the standard implementation of RSA?

Name: _____ ***Matriculation number:*** _____

Task 5: (Fuzzing) 2+4+4 points

a) Name one property that whitebox testing and blackbox testing have in common and one property that is different between the two testing methods.

b) Describe a method, presented in the lecture, that has been used to perform robustness testing on computers in the 1950s.

c) Connect the excerpts of the command line commands related to fuzzing with the respective explanations, by inserting the according number.

	`-Lcalculcation`
	`-fsanitize=fuzzer`
	`-Icalculation`
	`CXX=alf-clang`
	`-lcalculation`
	`-fsanitize=address`
	`-fsanitize=fuzzer-no-link`
	`CC=afl-clang`

1	Tell the compiler to generate a LibFuzzer executable
2	Instrument an object for fuzzing
3	Instrument an object for address sanitiziation
4	Use afl-clang as the C++ compiler
5	Use afl-clang as the C compiler
6	Look for libraries in a folder named calculation
7	Link against a library named calculation
8	Look for headers in a folder named calculation

Task 6: (E-Voting System) 2+8 points

a) Write down the basic mechanisms of an e-voting system.

b) Describe the four steps of an e-voting system.

Name: _____ ***Matriculation number:*** _____

Task 7: (Centralized Group Key Management) 2+4+4 points

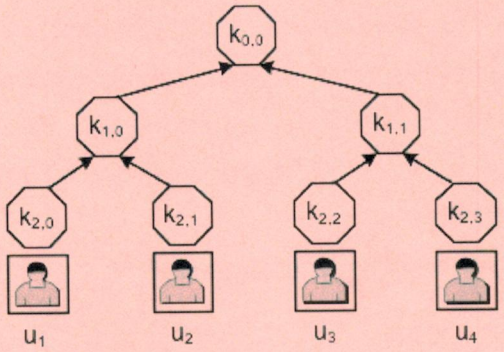

Figure 1: Key tree of the LKH protocol

A group controller (GC) uses the LKH protocol with the key tree in figure 1 for the key management of the group G with the user u_i $i \in \{1,2,3,4\}$. The members of the group are associated with the leaves of the key tree. The key $k_{0,0}$ stored in the root of the tree is the group key.

a) The user u_5 joins the group. Add the new user to the key tree and draw the modified tree. List the keys known by user u_1.

A group controller uses the LKH method for the key update. Assume that the key $k_{3,1}$ is established by the Diffie-Hellman algorithm in advanced.

b) Specify the group controller messages to the new user and to previous users for group oriented rekeying. All members should be able to calculate the new group key.

c) Specify the group controller messages to the new user and to previous users for user oriented rekeying. All members should be able to calculate the new group key.

Task 8: (Secret Sharing) 2+4+2+2 points

a) Write down two different types of secret sharing and describe their main features.

b) Write down the operation to restore the secret. Assume that a dealer uses Shamir`s secret sharing and gives every user u_i a share $(i, s_i=f(i) \bmod p)$

c) Write the additional operation of the dealer in order to enable the users to check the consistency of the secret sharing.

d) How can a user verify the consistency of his share?

Name: _____ ***Matriculation number:*** _____

Task 9: (Public Key Infrastructure) 9+1 points

Serial Number	1
Issuer	P
NotBefore	16/08/2017
NotAfter	30/05/2022
Subject	P

Serial Number	3
Issuer	P
NotBefore	16/10/2017
NotAfter	31/11/2018
Subject	N

Serial Number	4
Issuer	N
NotBefore	15/11/2017
NotAfter	30/08/2020
Subject	A

Table 1: Certificates of a PKI

The user A signs a document at 01/12/2017, 16/10/2018 and 15/02/2019. More details about the certificates is given in table 1.

a) Determine the result of the verification on 20/10/2019 based on the shell, hybrid and chain model.

b) What is the reason for the distribution of certificate revocation lists?

Task 10: (Threat Intelligence) 3+1+1+2+2+1 points

a) Name the key concepts of information security and define each in one sentence.

b) What does IoC stand for? Give an example.

c) What does APT stand for? What makes them so special?

d) What does the "Pyramid of Pain" model?

e) What is the "Intrusion Kill Chain" used for? Name and explain one stage.

f) What is footprinting?

Name: _____ *Matriculation number:* _____

Task 11: (Web Security) 2+2+3+2+1 points

a) Explain the threat model of a web adversary in two sentences.

b) What parts of a URL does the origin consist of?

c) What are the rules of the Same-Origin Policy (SOP)?

d) Name and briefly explain a single-phase SSO attack.

e) Against which of the attacks discussed in the lecture does HSTS help?

Task 12: (Privacy)

2+1+1+6 points

a) Explain the difference between a perturbative and a non-perturbative anonymization technique.

b) Define quasi-identifier as discussed in the lecture.

c) Define identity disclosure as discussed in the lecture.

d) Decide for each of the following statements, which are true and which are false. Mark them accordingly using 'T' for true and 'F' for false.

_ In local recoding all occurences of a specific value are replaced with the same value.
_ Pseudonymous data is not excempt from the GDPR.
_ Using attribute disclosure the attacker discloses which attributes are sensitive attributes.
_ Mathematical operations are not executable on pseudonymous data.
_ Univariate Microaggregation ensures k-anonymity.
_ Considering the GDPR, data minimization must be ensured.

Name: _____ ***Matriculation number:*** _____

Task 13: (Privacy Enhancing Technologies) 2+6+2 points

a) Define the semi-honest adversary.

b) Describe the six steps needed to create a garbled circuit.

c) Describe the advantage of point-and-permute and how it is reached.

Task 14: (Anomaly Detection) 2+5+3 points

a) Decide for each of the following statements, which are true and which are false. Mark them accordingly using 'T' for true and 'F' for false.

__ An anomaly is an observation that is distinctly different from all other observations.
__ Local Outlier Factor (LOF) is a neighborhood-based anomaly detection method.
__ In Hartigan's kMeans, the centroids are updated every time a point is reassigned.
__ Anomaly detection employing an Autoencoder requires the anomalies to be clearly in the minority.

b) Give the algorithm for Hartigan's kMeans. Clearly state inputs and outputs of the algorithm.

c) Draw an example of a 2D dataset, where the anomalous data points are easily distinguishable and visually separated from the normal data points, but Hartigan's kMeans algorithm would struggle to establish a clear separation. Explain why.

Name: _____ ***Matriculation number:*** _____

Task 15: (Statistics) 4+6 points

a) Decide for each of the following statements, which are true and which are false. Mark them accordingly using 'T' for true and 'F' for false.

__ Given positive ratios $x_1,\ldots, x_n$, their harmonic mean is $H(x_1,\ldots, x_n) = \frac{n}{\frac{1}{x_1}+\ldots+\frac{1}{x_n}}$

__ The Spearman Correlation Coefficient computes the correlation of a nominal feature.

__ The Principle Component Analysis embeds a given point cloud into a space of higher dimension.

__ In the t-test, we have to assume that the two given groups are approximately normally distributed.

b) A new virus scanner detects malware with a recall Rec = TP/(TP+FN) of 100% and a specificity Spec = TN/(TN+FP) of 99.9%. A cloud service provider operates a server with 10,050,000 unencrypted files. We assume that 50,000 files are infected. The virus scanner scans all unencrypted files.

Fill out the confusion matrix **and** compute the accuracy of the virus scanner.

	File is infected	File is not infected
File is reported by the scanner	T_P	F_P
File is not reported by the scanner	F_N	T_N