Rheinische Friedrich-Wilhelms-Universität Bonn

Master of Computer Science

Written Exam

Semester: Winter Term	Exam Period: 2
Module Name: IT Security	
Module No: MA-INF 3236	Date of Examination: 18.03.2024
Examiner: Prof. Dr. Michael Meier	

To be filled out by the Student:

Last Name:	Matriculation Number:
Given Name:	

Case of Study

Computer Science □ Cyber Security □ Secondary Subject □ Other □

To be filled by the examiner:

1	2	3	4	5	6	7	8	9	10	11	12	Σ
10	10	10	10	10	10	10	10	10	10	10	10	120

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

Exercise 1 (Side Channel Attacks, 5+5 points).

a) In the Rowhammer attack, an attacker flips a bit at some memory address, without the computer noticing. Give two examples where flipping a single bit compromises the security of the system and describe how the security is compromised.

b) Compared to brute forcing a cryptographic algorithm, what advantage do side channels provide? Give two examples of cryptographic algorithms, where side channels make the attacks feasible.

Exercise 2 (Secure Software Engineering, 4+6 points).

a) Define the following terms and write down the name of the affected CIA-property: **Tampering, Information Disclosure**

b) Name one abuse and one misuse case for the following scenario and define the affected CIA-properties: A company has set up a vending machine for softdrinks on the university campus, where the purchase process works as follows:

(1) Hold your prepaid card on the machine.

(2) Choose your drink.

(3) Take the drink.

(4) Payment amount is debited from your card.

Exercise 3 (Usable Security and Privacy, 4+6 points).

a) Your colleagues are planning a survey study about peoples' attitudes towards clientside scanning, and have asked for your feedback. For the following questions in bold font below, apart from self-reporting bias, judge which questions are methodologically sound, and which are problematic enough, that you would recommend your colleagues to improve the question, before publishing and distributing their survey.

At the beginning of the survey, your colleagues present a neutral definition of clientside scanning: „There is software that allows comprehensive automated searches for files relevant to criminal activities on devices such as smartphones or laptops. Law enforcement authorities are informed if the software finds suspicious material."

If you judge a question or its answers to be problematic, briefly explain the problematic aspects.

How much privacy do you think there is on the internet right now?

□ **There is much privacy**

□ **There is some privacy**

□ **There is not much privacy**

□ **There is no privacy at all**

□ **I do not know**

□ **I would rather not say**

The question is...
□ methodologically sound □ methodologically problematic

Explanation of problematic aspects:

How concerned are you about possible misuse of clientside scanning?

□ **Extremely concerned**

□ **Highly concerned**

□ **Very concerned**

□ **Strongly concerned**

□ **Moderately concerned**

The question is...
□ methodologically sound □ methodologically problematic

Explanation of problematic aspects:

Would you approve or disapprove of clientside scanning to prosecute terrorism?

□ **I disapprove**

□ **I somewhat disapprove**

□ **I neither approve nor disapprove**

□ **I somewhat approve**

□ **I approve**

The question is...
□ methodologically sound □ methodologically problematic

Explanation of problematic aspects:

How privacy-preserving and crime-exposing do you think clientside scanning is?

- □ **very privacy-preserving and crime-exposing**
- □ **moderately privacy-preserving and crime-exposing**
- □ **neutral**
- □ **somewhat privacy-preserving and crime-exposing**
- □ **not privacy-preserving and crime-exposing**

The question is...
□ methodologically sound □ methodologically problematic

Explanation of problematic aspects:

b) Decide for each statement, whether it is true (**T**) or false (**F**) by marking it with the corresponding letter.

___ Software developers are the root cause of most IT security problems.

___ Using snowball sampling to recruit participants leads to an unbiased, random sample.

___ Most software developers are not security experts.

___ From an ethical point of view, study participants need to have sufficient information and understanding about a study, before deciding to take part in it.

___ In the SOUPS-paper „Replication: No One Can Hack My Mind: Revisiting a Study on Expert and Non-Expert Security Practices and Advice“ by Busse et. al., security experts recommend not sharing private information more frequently than non-experts do.

___ In the SOUPS-paper „Replication: No One Can Hack My Mind: Revisiting a Study on Expert and Non-Expert Security Practices and Advice“ by Busse et. al., security experts recommend using password managers more frequently than non-experts do.

Exercise 4 (Applied Binary Exploitation, 10 points). Given the following information, prepare the payload to overflow the local variable `x` to exploit a program with a ROP chain which calls libc's `system("/bin/sh")`. **Write the bytes of the payload correctly into „Stack at Position 2“ and briefly explain each stack word on the right.** The exploit should be designed for a little-endian x64 architecture with System V calling convention.

```
Base Address of library: 0x7fff 4000 0000
Gadget offsets:
  pop rdx; ret             --    0x1000
  mov rdi, rsp; ret        --    0xdead
  add rdi, rdx; ret        --    0x001e
system() offset            --    0x01 00e8

system():
  rdi  -- const char *command
```

You can assume that the executed code is equivalent to the following Pseudo-C snippet and that there are no stack canaries active. **However, the position of the stack is randomized, so you cannot use absolute stack addresses.**

```
void func() {
    unsigned long x = 42;

    // Position 1

    read(stdin, &x, 8 * 16);

    // Position 2
}
```

You may write a dash (–) instead of a 00.

Address	Stack at Position 1	comment	Stack at Position 2	Your Explanation
7fff ???? dc50	42 -- -- -- -- -- -- --	x		
7fff ???? dc58	50 dd ff ff ff 7f -- --	saved rbp		
7fff ???? dc60	23 51 55 55 55 55 -- --	ret addr		
7fff ???? dc68	...	...		
7fff ???? dc70	...	...		
7fff ???? dc78	...	...		
7fff ???? dc80	...	...		
7fff ???? dc88	...	...		
7fff ???? dc90	...	...		
7fff ???? dc98	...	...		
7fff ???? dca0	...	...		
7fff ???? dca8	...	...		
7fff ???? dcb0	...	...		
7fff ???? dcb8	...	...		
7fff ???? dcc0	...	...		
7fff ???? dcc8	...	...		

Exercise 5 (Malware Analysis, 2+3+2+3 points).

a) Given the parts of a PDF file shown in the listing below, answer the following questions in at most one sentence each:

   i. What is the ID of the action that is executed when the PDF is opened?

   ii. What happens when the action is invoked?

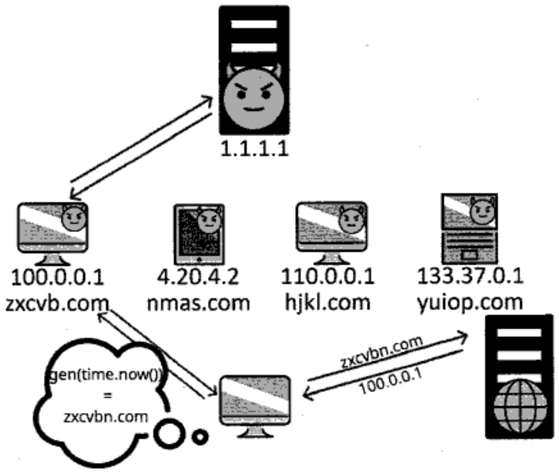
```
1 0 obj
<<
  /Type /Catalog
  /Pages 2 0 R
  /OpenAction 3 0 R
>>
endobj

2 0 obj
  /Type /Pages
  /Kids 8 0 R
  /Resources 4 0 R
endobj

3 0 obj
<<
  /Type /Action
  /S /Launch
  /F ('/usr/bin/shutdown')
>>
endobj

4 0 obj
<<
  /Type /Action
  /S /JavaScript
  /F ("console.log('Hello, world!');")
>>
```

b) In 2-3 sentences, describe one file-system-based anti-sandboxing technique discussed in the lecture, and why the underlying artifact is specific to sandboxes.

c) Name the obfuscation technique displayed in the listing below, and in one sentence each, explain the general concept of it, what it's used for, and why it works.

```
void some_func() {
  unsigned char e0 = 0x00;
  unsigned char e1 = 0x6f;
  unsigned char e2 = 0x6c;
  unsigned char e3 = 0x6c;
  unsigned char e4 = 0x65;
  unsigned char e5 = 0x68;
  printf("%s", e5); // prints "hello"
}
```

d) Given the following diagram of communication between an infected client and a C&C server, explain the characteristic technique of this approach, and two advantages compared to the naive approach of directly communicating with the hardcoded IP `1.1.1.1`.



Exercise 6 (Security of Distributed Systems, 1+6+2+1 points).

a) What is the purpose of the distributed ledger technology?

b) Describe the six steps of a blockchain-based distributed ledger operation.

c) Name two mechanisms to realize a n-of-m wallet for a distributed ledger.

d) Briefly describe a mechanism to reduce the storage space of a Blockchain-based distributed ledger.

Exercise 7 (Fuzzing, 3+3+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) Match the excerpts of the command line commands related to fuzzing to the respective explanations, by inserting the correct numbers into the boxes on the left.

□	`-Lcalculation`	1	Tell the compiler to generate a LibFuzzer executable
□	`-fsanitize=fuzzer`	2	Instrument an object for fuzzing
□	`-Icalculation`	3	Instrument an object for address sanitization
□	`CXX=afl-clang`	4	Use afl-clang as the C++ compiler
□	`-lcalculation`	5	Use afl-clang as the C compiler
□	`-fsanitize=address`	6	Look for libraries in a folder named calculation
□	`-fsanitize=fuzzer-no-link`	7	Link against a library named calculation
□	`CC=afl-clang`	8	Look for headers in a folder named calculation

Exercise 8 (Domain-Specific Automated Software Testing, 3+3+2+2 points).

a) Give a formal definition of a t-way test suite as discussed in the lecture.

b) Explain an advantage and a disadvantage of combinatorial testing compared to domain-specific fuzzing in one sentence each.

c) Define the property *soundness* for a test oracle.

d) Consider differential testing of the X.509 certificate validation with a reduction function

$$R(o) = \begin{cases} 1 & \text{certificate is considered to be valid,} \\ 0 & \text{else} \end{cases}$$

Prove that differential testing is not sound by giving a counter-example with a short explanation.

Exercise 9 (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) Assume you want to know, whether a target device is still sending and in range of your receiver. It is communicating to one specific receiver that is always accessible and responsive and does not move. Its communication is completely encrypted, however, so you have no access to the header or content of the sent packets.

Explain a passive device identification technique presented in the lecture that you could be using in that scenario. Why does it work? What drawbacks does your suggested technique have?

c) Explain the goal of MAC address randomization. Describe two different forms of MAC address randomization that can be found on modern smartphones and explain the differences. Explain, how these forms can be attacked using device identification techniques.

Exercise 10 (Supply Chain Attacks, 1+2+2+3+2 points).

a) What is the *Intrusion Kill Chain* used for?

b) Briefly explain one step (of your choosing) of the *Intrusion Kill Chain.* Name the step before and after.

c) What is the idea behind Supply Chain Attacks?

d) Name the main motivation for each Threat Actor type.

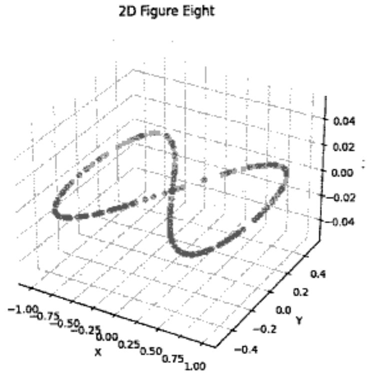
e) Is scanning the target's public servers for open ports a suitable technique for footprinting? Why?

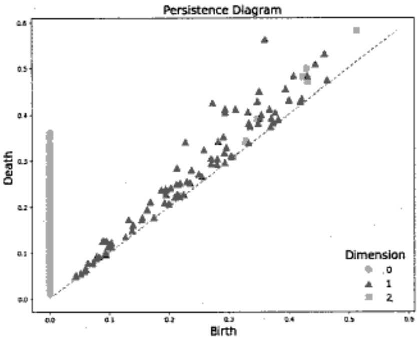
Last Name: **Matriculation Number:**

Exercise 11 (Topological Data Analysis, 2+3+3+2 points).

a) Match the persistence diagrams to the captioned point clouds by writing the numbers in corresponding box. Briefly justify your answers.

1

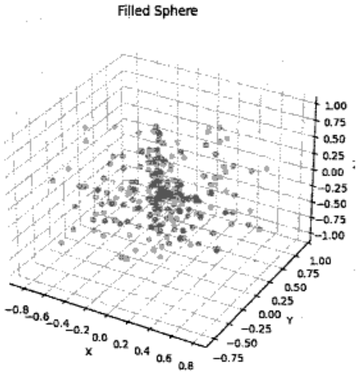


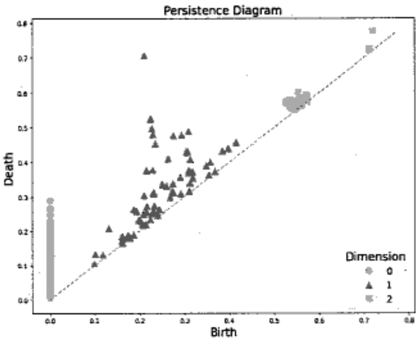


□

Justification:

2

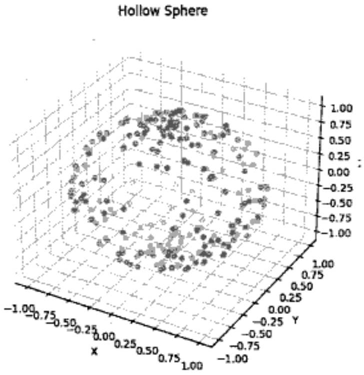


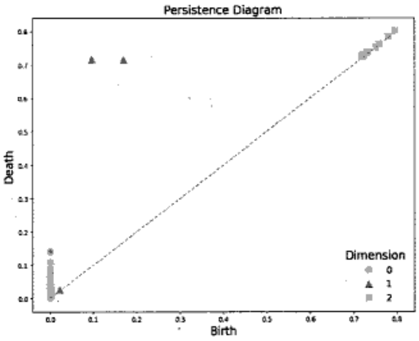


□

Justification:

3

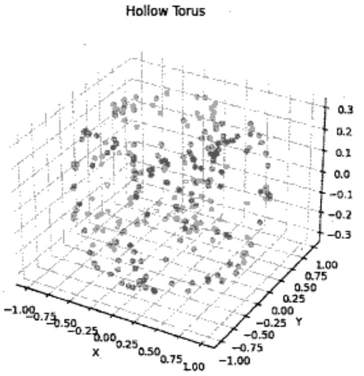


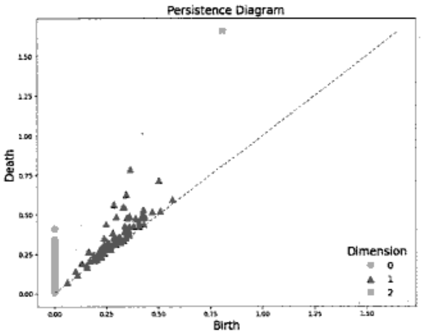


□

Justification:

4





□

Justification:

b) Given a topological space X define the concepts of homology as well as filtration. Given these two concepts, explain persistent homology.

c) Consider the abstract simplicial complex K given by

$$\begin{aligned}K = \{&\emptyset, \{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{0,1\}, \{0,2\}, \{1,3\}, \{2,3\}, \{2,4\},\\ &\{3,4\}, \{3,5\}, \{4,5\}, \{2,3,4\}, \{3,4,5\}\}.\end{aligned}$$

Draw its geometric realization. What are the homology groups of K?

d) Given two homotopy equivalent topological spaces X and Y, how do their homology groups relate to each other? Briefly justify your answer.

Exercise 12 (Anonymization and Secure Multiparty Computation, 2+1+1+6 points).

a) Define the marketer attacker model.

b) Define *k-anonymity.*

c) Describe the advantage of point-and-permute over the raw garbled circuits technique and how it is achieved.

d) List the six steps needed to create a garbled circuit.