Rheinische Friedrich-Wilhelms-Universität Bonn

Master of Computer Science

Written Exam

Semester: Winter Term	Exam Period: 1
Module Name: IT Security	
Module No: MA-INF 3236	Date of Examination: 06.02.2024
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

Last Name: **Matriculation Number:**

Exercise 1 (Side Channel Attacks, 3+7 points).

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

b) What information is leaked in the padding oracle attack and what information does the attacker ultimately obtain? Based on that, what could be interesting targets for this attack?

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

a) Define the following terms and write down the name of the affected CIA-property:
Spoofing, **Elevation of Privilege**

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.

Last Name: **Matriculation Number:**

Exercise 3 (Usable Security and Privacy, 3+7 points).

a) Your colleagues are planning a survey study about computer science students' use of two-factor authentication, 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.

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

Do you use two-factor authentication (for example, Google's 2-Step-Verification or a bank's two factor authentication app) for at least one of your online accounts?

- ☐ **Yes**
- ☐ **No**
- ☐ **I don't know**
- ☐ **I don't want to answer this question**

The question is...
☐ methodologically sound ☐ methodologically problematic

Explanation of problematic aspects:

How often do you use two-factor authentication per month?

- ☐ **never**
- ☐ **fewer than once per month**
- ☐ **1-5 times per month**
- ☐ **5-10 times per month**
- ☐ **10 - 15 times per month**
- ☐ **15 times or more often per month**

The question is...
☐ methodologically sound ☐ methodologically problematic

Explanation of problematic aspects:

How usable and secure do you think the process of two-factor authentication is?

- ☐ **very usable and secure**
- ☐ **moderately usable and secure**
- ☐ **neutral**
- ☐ **somewhat usable and secure**
- ☐ **not usable and secure**

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.

___ Research in Usable Security and Privacy uses interview, survey, and experimental studies to investigate how human factors impact privacy and security.

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

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

___ Most software developers are security experts.

___ Informed consent means that study participants need to have sufficient information and understanding about a study, before deciding to take part in it.

___ In the SOUPS-paper „,...no one can hack my mind‘: Comparing Expert and Non-Expert Security practices“ by Ion et. al., security experts recommend using two-factor authentication more frequently than non-experts do.

___ In the SOUPS-paper „,...no one can hack my mind‘: Comparing Expert and Non-Expert Security practices“ by Ion et. al., security experts recommend using an antivirus program more frequently than non-experts do.

Last Name: **Matriculation Number:**

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 `execve("/bin/sh", NULL, NULL)`. **Write it into the column „Stack at Position 2" along with very brief explanations of each word.** 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 rax; ret              --   0x42
  pop rdi; pop rdx; ret     --   0x1000
  pop rsi; ret              --   0x08 0400
  syscall                   --   0xdead
String "/bin/sh\0" address: 0x7fff f7ff dab0

execve() syscall:
  rax  -- 0x3b
  rdi  -- const char *filename
  rsi  -- const char *argv[]
  rdx  -- const char *envp[]
```

You can assume that the executed code is equivalent to the following Pseudo-C snippet and that there are no stack canaries or mitigations active:

```
1 void func() {
2     unsigned long x = 42;
3
4     // Position 1
5
6     read(stdin, &x, 8 * 16);
7
8     // Position 2
9 }
```

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

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

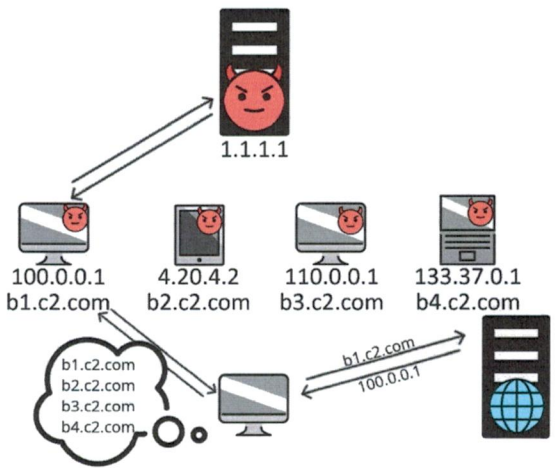
Exercise 5 (Malware Analysis, 3+4+3 points).

a) In 2-3 sentences, explain the obfuscation technique *stack strings*, what they are used for and why they work.

b) Given the following assembly instructions of the main function, conceptually explain how you would use a debugger to circumvent the anti-debugging functionality, and execute the target function `super_secret_target_func`. Use the concrete addresses and names from the example in your explanation.

```
0000000140001457 <main>:
   140001457:  push   rbp
   140001458:  mov    rbp,rsp
   14000145b:  sub    rsp,0x30
   14000145f:  call   140001560 <__main>
   140001464:  movabs rax,0x656874206d612049
   14000146e:  mov    QWORD PTR [rbp-0xe],rax
   140001472:  movabs rax,0x2e79656b206568
   14000147c:  mov    QWORD PTR [rbp-0x8],rax
   140001480:  mov    rax,QWORD PTR [rip+0x6d01]
   140001487:  call   rax                                  # calls IsDebuggerPresent
   140001489:  test   eax,eax
   14000148b:  je     140001497 <main+0x40>
   14000148d:  mov    ecx,0x1
   140001492:  call   140002628 <exit>                     # ends the program
   140001497:  call   140001450 <super_secret_target_func> # you want to execute this
   14000149c:  mov    eax,0x0
   1400014a1:  add    rsp,0x30
   1400014a5:  pop    rbp
   1400014a6:  ret
```

c) 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`.



Last Name: **Matriculation Number:**

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

a) Write down two different types of secret sharing and describe two main features for each type.

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

c) Some e-voting system uses secret sharing for trustworthy voting. Describe the four steps of the e-voting system introduced in the lecture and specify the calculations of the voter and the authorities.

Exercise 7 (Fuzzing, 3+3+4 points).

a) You want to instrument a C library for fuzzing. At what point during the build process of the library is the instrumentation being done? Describe how the instrumentation is being done.

b) Describe one kind of vulnerability that can be detected with the Address Sanitizer (ASAN). How does ASAN detect the vulnerability?

c) Given the following list of labels and the diagram with blank spaces: Write the labels into the blank spaces so that the diagram represents the Coverage Guided Fuzzing Algorithm as presented in the lecture.

Mutation

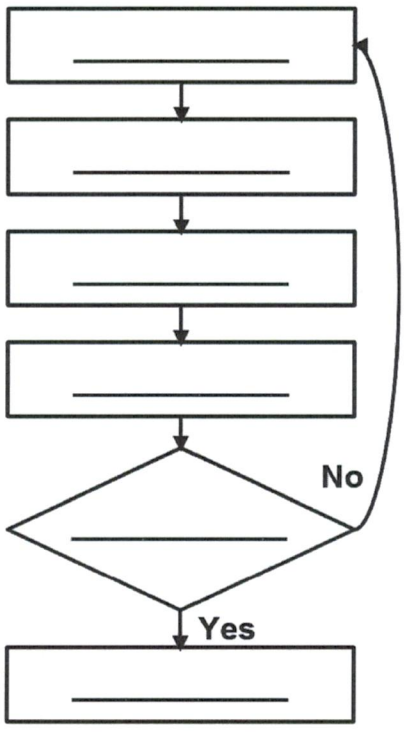
Seed Files

Done

Selection

Code Coverage

Crash (Or ASAN etc.)



Last Name: **Matriculation Number:**

Exercise 8 (Domain-Specific Automated Software Testing, 4+2+4 points).

a) Given the following parameters and test suite: Eliminate a row so that the remainder is still a 2-way test suite.

$p_1 \in \{0, 1\}$
$p_2, p_3 \in \{0, 1, 2\}$

p_1	p_2	p_3
0	0	1
0	1	0
0	1	2
0	2	1
1	0	0
1	0	2
1	1	1
1	1	2
1	2	0
1	2	2

b) Define the property *completeness* for a test oracle.

c) Consider differential testing of TLS servers which focuses only on the handshake process with a reduction function

$$R(o) = \text{raw bytes sent by the server}$$

and assume the pool of implementations contains at least one perfect reference implementation.

Prove that differential testing is not complete 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 a defensive actor as discussed in the lecture. In what way can the defensive actor use identifying data in your example?

b) Name two collectable characteristics of a wireless transmission to be used as direct device identifying data (DID) and explain why they qualify as direct DID.

c) Describe a scenario where using active device identification may be harmful to an attacking fingerprinter but passive device identification can be utilized effectively. Why can active device identification be harmful to the attacker but passive device identification is not in your given scenario?

Last Name: **Matriculation Number:**

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

a) Name and briefly explain the key concepts of information security.

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

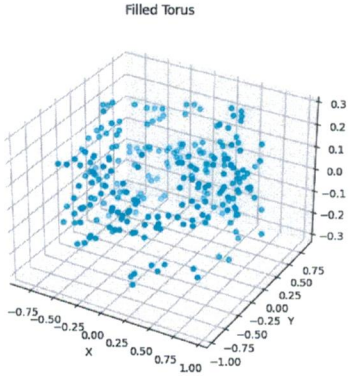
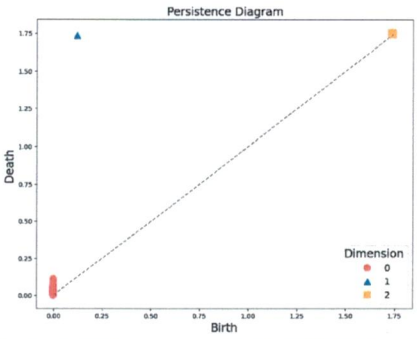
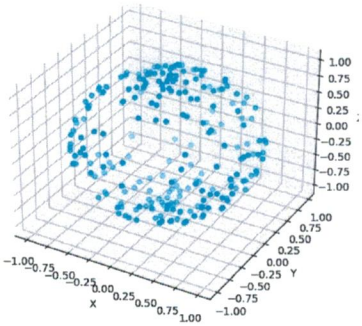
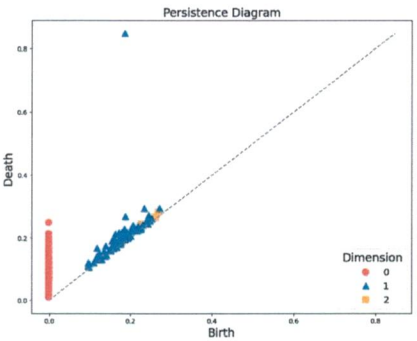
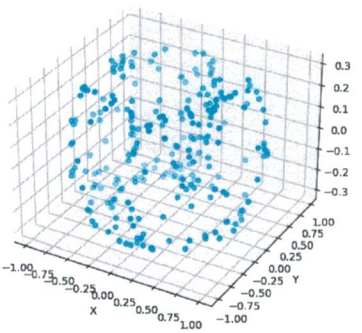
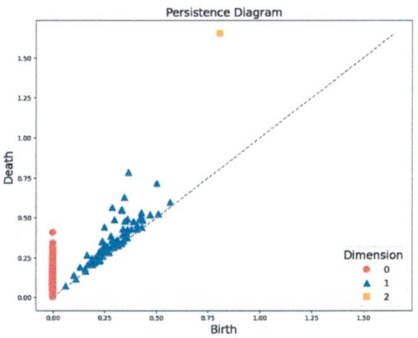
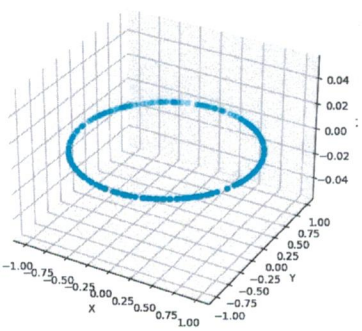
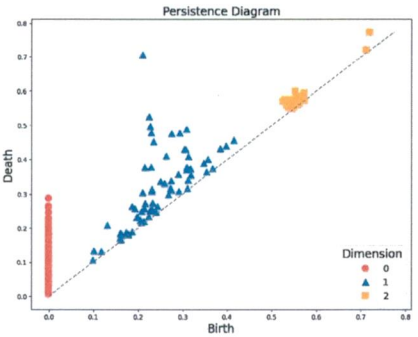
c) What is the idea behind Supply Chain Attacks?

d) What are APTs and what characterizes them?

Last Name: **Matriculation Number:**

Exercise 11 (Topological Data Analysis, 2+4+2+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 two topological spaces X and Y, define homotopy equivalence and homeomorphism.

c) Consider two topological spaces: Space X is a solid torus, and space Y is a hollow torus. Are X and Y homotopy equivalent? Justify your answer.

d) Give an example for two spaces that are homotopy equivalent, but not homeomorphic. Explain the reasoning behind your example.

Last Name: **Matriculation Number:**

Exercise 12 (Anonymization and Secure Multiparty Computation, 2+2+1+5 points).

a) Write down the similarities and differences between the prosecutor and journalist attacker.

b) Define the property *distinct l-diversity* for a dataset.

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

d) Fill in the empty lines to implement the given circuit in the Bristol Fashion Format which is used in the jigg library.

```
1
2 2 2 2
3 1 1
4
5
6
7
```