Exam: Secure Computer Systems 1
1DT072
2023–08–23

Teacher: Paul Fiterau-Brostean (tel. 0040720114646)
Time: 14.00–19.00

Instructions: The exam has 11 sections. To pass the exam you need to get approximately 2/3 of the possible total score.

Hand in **only the answer sheet**, with your answers clearly marked. If you make mistakes, ask for another answer sheet. If you mark more than one answer to a question, you will get no score. **Please also read** the instructions on the answer sheet!

Good luck!!

---

1 Foundations

Question 1 Consider a DNS water torture attack – which of the basic security properties is most affected?

A. confidentiality

B. authenticity

C. availability

D. integrity

E. accountability

Question 2 Which of the following is **TRUE** about the classic design principles of Saltzer and Schroeder?

A. *Fail-safe default* says default access should be configured in a safe way

B. *Least privilege* says one user must have fewer privileges than the others

C. *Open design* says security should not be ensured through secrecy

D. *Economy of mechanism* means to use security mechanisms economically, to minimize overhead

E. *Least common mechanism* means you should use the least common, i.e. most unusual, security mechanism

---

2 Web and data security

Question 3 Escaping the character ';' provides some protection against which attack:

A. XSS

B. SQL injection

C. path traversal

D. command injection

E. CSRF

Question 4 In an SQL injection attack, which is **true**?

A. The attack can be best prevented by the use of *parameterized queries*

B. Race conditions are fundamentally important to protect against SQL injections

C. Filtering SQL comment characters makes the attack impossible

D. Client-side protections are necessary to defend against the attack

E. The attacker can inject machine code in the SQL query through a stack overflow

---

Question 5 To protect against a XSS (cross-site scripting) attack, which method is **most** effective?

A. Treating user input as data

B. Disabling cookies in your web browser

C. To trust only web servers that use https

D. That the web server runs in an isolated environment

E. That the web server follows the HTML5 standard

Question 6 Which of the following attacks can best leverage *homographic encodings*?

A. SQL injection

B. command injection

C. phishing

D. CSRF

E. XSS

---

3 Asymmetric Cryptography and Signatures

Question 7 A group of 10 users want to establish secure channels among themselves. This means, every two users should be able to communicate in a way that is indecipherable by the other users. For this purpose, they are deciding between using either symmetric or asymmetric cryptography. Which of the following statements is **FALSE**?

A. Leakage of a secret key would compromise more secure channels if asymmetric cryptography is used

B. Each user would have to know a single secret key if asymmetric cryptography was used

C. Adding a new user to the group is easier for asymmetric cryptography (i.e., it entails generating fewer keys)

D. Asymmetric encryption algorithms are generally faster

E. Symmetric cryptography requires 35 more secret keys

Question 8 You are given the certificate hierarchy in Figure 1.

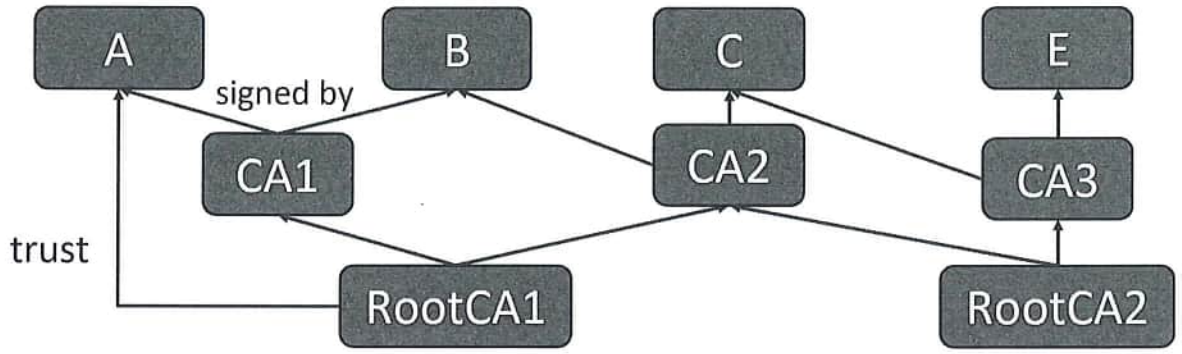

Figure 1 Certificate Hierarchy

Entity A's trust store contains **only** RootCA1's self-signed certificate ($Cert_{RootCA1(RootCA1)}$). Select the certificate chain that A will be able to successfully validate. Note that $Cert_{X(Y)}$ can be interpreted as a certificate containing Y's public key that has been signed by X.

A. $Cert_{CA1(B)}$

B. $Cert_{CA3(E)}$

C. $Cert_{CA2(B)}$, $Cert_{RootCA2(CA2)}$

D. $Cert_{CA3(C)}$, $Cert_{RootCA1(CA2)}$

E. $Cert_{CA2(C)}$, $Cert_{RootCA1(CA2)}$

Question 9 In the first lab, you used S/MIME certificates for secure email. Which of the following is **TRUE**?

A. Encrypting a digitally signed email requires the certificate of the receiver

B. Decrypting a digitally encrypted email requires the certificate of the sender

C. Sending a digitally signed email requires the certificate of the receiver

D. Sending a digitally encrypted email requires the certificate of the sender

E. Verifying a digitally signed email requires the certificate of the receiver

---

4 Sandboxing and Virtualization

Question 10 AppArmor is used to restrict the capabilities of a program, and in doing so protect the operating system. Which of the following is the design principle (by Saltzer et al) does AppArmor **most specifically** address?

A. *Least common mechanism*

B. *Open design*

C. *Least escalation*

D. *Psychological acceptability*

E. *Complete mediation*

Question 11 The terms sandboxing and virtualization can be easy to confuse. What is **TRUE** of the following?

A. Virtualization is mainly a software feature, and not helped much by hardware support

B. Sandboxing may limit an application's access to system resources

C. Sandboxing protects 'sandboxed' applications from viruses affecting the system

D. Virtualization is designed to protect the system against viruses

E. Sandboxing enables running applications on different operating systems

---

5 Identification and authentication

Question 12 In the attack on LinkedIn in 2012 resulted in the leak of 177.5 million password hashes, which appeared in a data dump in 2016. The passwords were stored with plain hashing using the SHA1 algorithm. About 98% of them were cracked within 6 days from the release of the dump.

In an attack on MySpace in 2013, 362 million accounts and their password hashes were leaked, which appeared in a data dump also in 2016. These passwords were also hashed with SHA1, but after being converted to lowercase and truncated to max 10 characters.

What is the **most relevant** statement?

A. Since only the password hashes were leaked, the passwords themselves were safe

B. Using the MD5 hash algorithm would have been even worse

C. Using the SHA1 algorithm is a bad idea since it is fast

D. Using the same password on both sites would not have been a problem if they had used different hash algorithms

E. Converting and truncating passwords makes it unfeasible to find the original password

---

Question 13 *salted hashing* protects against a dictionary attack most importantly because:

A. Both the password and the salt are unknown to the attacker

B. The attacker cannot pre-compute the dictionary used to crack the passwords

C. It requires a more secure hashing algorithm

D. It is slower to compute than regular hashing, causing attacks to take more time

E. The entropy of the password is increased, making it more difficult to crack

---

6 Information flow

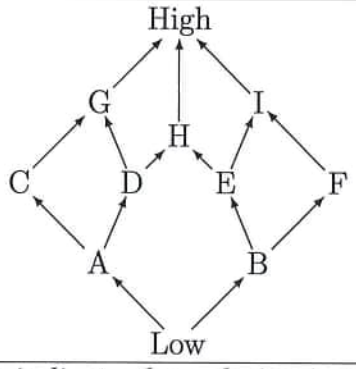

Figure 2 BLP lattice. Arrows indicate the ordering in the lattice.

Question 14 The Bell-LaPadula model (BLP) deals with security levels and categories, typically ordered as a lattice. What is **TRUE** for subjects and objects in the lattice in Figure 2, using the rules of the Bell-LaPadula model?

A. A subject with level A can read an object with level B

B. A subject with level B can write an object with level H

C. A subject with level B can read an object with level I

D. A subject with level G can write an object with level D

E. A subject with level H can write an object with level B

Question 15 y and z are variables, such that $y, z \in \{0, ..., 15\}$ with equal probabilities. The variables are secret, and used in programs whose execution produces the non-secret output x. Select the program whose execution leaks the least amount of information regarding y.

A. $\boxed{x := (y + z) \bmod 4}$

B. $\boxed{x := y^z}$

C. $\boxed{x := y \text{ xor } z}$

D. $\boxed{x := y * z}$

E. $\boxed{x := y/z}$

---

7 Access control

Question 16 The access control matrix can be implemented using Capability Lists (CL) or Access Control Lists (ACL). Which is better, when?

A. CLs are better when the owner of an object often needs to revoke access rights to it

B. CLs are better for settings where objects have owners, who can quickly see who has access to their objects

C. CLs give a better overview of which subjects have access to a particular object

D. CLs are better when subjects often need to have all their rights revoked

E. ACLs often allow delegation of rights between subjects

Question 17 Mandatory Access Control (MAC) differs from Discretionary Access Control (DAC). What of the following is **FALSE**?

A. On a standard Linux system, the root user can read and write any file

B. Role-Based Access Control is typically MAC

C. "Classic" Linux file protection supports DAC

D. In a DAC system, central policies define the access rights

E. When using DAC, all objects typically have an owner

---

8 Software security

Question 18 In Lab 3, you used Metasploit to attack the different systems. For a successful attack, you needed a *vulnerability*, an *exploit* and a *payload*. What is the relationship between an exploit and a vulnerability?

A. An exploit is a type of vulnerability

B. A vulnerability is a type of exploit

C. An exploit is used to expose a vulnerability

D. A vulnerability is the result of an exploit

E. Exploits and vulnerabilities are unrelated

Question 19 The C program (below) executes a `sensitive` function only if the user provides a correct 3-digit number. The constant `PIN` stores the correct PIN, but its contents are unknown, other than the fact that it is a 4-byte string in which a 3-digit number is stored. The binary is compiled for a 32-bit architecture.

```
#define PIN "..." // 4-byte string storing 3-digit number
void sensitive () {
  // . . .
}
int main() {
  char secret[] = PIN;
  char input[4]; // make room for end of string char '\0'
  printf("Input 3-digit PIN: \n");
  gets(input);
  if (strcmp(input, secret) == 0) {
    printf("Authenticated successfully\n");
    sensitive();
    return 1;
  } else {
    printf("PIN is incorrect\n");
    return 0;
  }
}
```

What is the measure that best would address the buffer overflow vulnerability in the given program.

A. replacing `gets` with a safer alternative (e.g. `fgets`)

B. making the stack non-executable

C. enabling address randomization

D. increasing the size of the array `input`

E. compiling for a 64-bit architecture

---

9 Privacy and Tracking

Question 20 A web server can find out a lot of information about the clients visiting its web pages, e.g. by sending Javascript code which gets executed in the web browser. (Note that this is not an XSS attack, since the information is sent back to the same web server who sent the Javascript code.)

Suppose you run a web server and want to keep track of your clients. Which of the following would be the *most* useful information that an HTTP request could contain?

A. the size of the browser window

B. a browser cookie

C. the list of installed system fonts

D. the language preferences in the browser

E. user agent string (which describes the web browser to the server)

Question 21 Tor browser protects you from being tracked when surfing the web primarily by:

A. making your browser appear indistinguishable from many others

B. disabling script execution

C. using highly customized parameters in HTTP requests

D. sending a Do-not-track header to tell web services not to track

E. launching threads for separate websites in separate containers

---

10 Network security

Question 22 Protecting against DDoS (distributed denial of service) attacks *based on address spoofing* can be very hard. What is **most often** an efficient protection?

A. Upgrading from IP version 4 to version 6

B. Having endpoint routers filter packets with spoofed addresses when they exit the local network, as they enter the Internet

C. Supporting HTTPS instead of HTTP

D. Upgrading your network interface to handle more incoming traffic

E. Having endpoint routers filter packets with spoofed addresses when they enter the local network, as they arrive from the Internet

---

Question 23 A security mechanism provides different forms of protection. What is **FALSE** of the following?

A. IPsec in tunnel model provides confidentiality of IP addresses

B. TLS provides confidentiality of application ports

C. Using IMAP over TLS ensures confidentiality between mail server and the connecting mail client

D. TCP Syn Cookies protect availability in the transport layer

E. NAT helps hide the IP addresses used by applications running behind it

---

11 Ethics in Security

Question 24 (2 points) Below is an excerpt from a recent article in Reuters (August 10, 2023).

> British technology minister Michelle Donelan defended plans to require messaging apps to provide access to encrypted private messages when needed to protect children from abuse, which major platforms say would undermine the privacy of their users.

Some of the messaging apps in question are WhatsApp and Signal. Give your take on whether parents of young children should support or oppose the plans. Analyse the issue by applying *more than one* ethical aspect (e.g. consequences, duties, virtues, freedom, fairness, or relations). Do not simply state "this is what I would do". Answer in the box at the bottom of the answer sheet. (You may want to think and formulate an answer before you write it there.)

Note: For 1 point, you need to show reflection and use basic ethical argumentation. For 2 points, you need to argue showing (relevant) understanding of ethical principles. Just stating "this is what I would do" is not enough for any score at all.

Good luck!

Score

Exam: Secure Computer Systems 1 (1DT072)
Date: 2023–08–23

Exam code: | | | | | | | | | | | | | |

Instructions: Mark clearly in the table below ***no more than one*** answer per question, by checking or covering the letter for your choice. ***Hand in only this page.*** If you find one of the questions strange or want to clarify your answer, mark ***the question box*** with a $\star$ and explain ***on the back of this sheet***, e.g, what you think is the problem and what assumptions you had to make to answer the question.

Question	Answer				
1	A	B	C	D	E
2	A	B	C	D	E
3	A	B	C	D	E
4	A	B	C	D	E
5	A	B	C	D	E
6	A	B	C	D	E
7	A	B	C	D	E
8	A	B	C	D	E
9	A	B	C	D	E
10	A	B	C	D	E
11	A	B	C	D	E
12	A	B	C	D	E

Question	Answer				
13	A	B	C	D	E
14	A	B	C	D	E
15	A	B	C	D	E
16	A	B	C	D	E
17	A	B	C	D	E
18	A	B	C	D	E
19	A	B	C	D	E
20	A	B	C	D	E
21	A	B	C	D	E
22	A	B	C	D	E
23	A	B	C	D	E
24	A	B	C	D	E

Answer to question 24 (please write LEGIBLY and only write inside the box):

Answers page.
Only answers circled here will be graded.

0. Optional anonymous background questions

0.1. A B C
0.2. A B C
0.3. A B C D
0.4. Program: _____

1. ISA 1

1.1. A B C D
1.2. A B C D
1.3. A B C D
1.4. A B C D
1.5. A B C D
1.6. A B C D

2. ISA 2

2.1. A B C D
2.2. A B C D
2.3. A B C D
2.4. A B C D
2.5. A B C D
2.6. A B C D

3. Computer Arithmetic

3.1. A B C D
3.2. A B C D
3.3. A B C D
3.4. A B C D
3.5. A B C D
3.6. A B C D

4. Logic

4.1. A B C D
4.2. A B C D
4.3. A B C D
4.4. A B C D
4.5. A B C D
4.6. A B C D

5. Processor Control and Datapath

5.1. A B C D
5.2. A B C D
5.3. A B C D
5.4. A B C D
5.5. A B C D
5.6. A B C D

6. Pipelining

6.1. A B C D
6.2. A B C D
6.3. A B C D
6.4. A B C D
6.5. A B C D
6.6. A B C D

7. Hazards

7.1. A B C D
7.2. A B C D
7.3. A B C D
7.4. A B C D
7.5. A B C D
7.6. A B C D

8. Branch Prediction and Exceptions and Interrupts

8.1. A B C D
8.2. A B C D
8.3. A B C D
8.4. A B C D
8.5. A B C D
8.6. A B C D

9. Input/Output

9.1. A B C D
9.2. A B C D
9.3. A B C D
9.4. A B C D
9.5. A B C D
9.6. A B C D

10. Caches

10.1. A B C D
10.2. A B C D
10.3. A B C D
10.4. A B C D
10.5. A B C D
10.6. A B C D

11. Virtual Memory

11.1. A B C D
11.2. A B C D
11.3. A B C D
11.4. A B C D
11.5. A B C D
11.6. A B C D

12. Parallelism

12.1. A B C D
12.2. A B C D
12.3. A B C D
12.4. A B C D
12.5. A B C D
12.6. A B C D

Feel free to detach the remaining pages of the exam and turn in only your answers.