Exam: Secure Computer Systems 1
1DT072
2023–06–12

Teacher: Paul Fiterau-Brostean (tel. 0040720114646)
Time: 8.00–13.00

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 If there is a vulnerability with respect to *integrity* (the security property) the following is true:

A. Botnets are often used for attacking this vulnerability

B. A reasonable protection involves encryption/decryption

C. A trojan could reduce the accountability

D. Computing file hashes may be part of a mitigation

E. The threat can be controlled by proper access control

Question 2 Consider a ransomware attack – which of the basic security properties is most affected?

A. confidentiality

B. authenticity

C. availability

D. integrity

E. accountability

Question 3 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 all users should have only the minimum of privileges needed

C. *Open design* says widely accepted design patterns should be employed when implementing security mechanisms.

D. *Economy of mechanism* says you should consider the cost of implementing security

E. *Separation of privilege* says protection mechanisms should be separated from each other, to avoid unintended overlap

---

2 Web and data security

Question 4 Running a web application in an isolated environment via 'chroot' can best defend against which attack:

A. SYN flood attack

B. SQL injection

C. command injection

D. XSS

E. path traversal

Question 5 In a shell injection attack, which is **true**?

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

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

C. If shell comment characters and boolean expressions are filtered, shell attacks are impossible

D. The attack injects data which is interpreted as shell code

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

---

Question 6 The following is **FALSE** regarding XSS (cross-site scripting) and CSRF (cross-site request forgery) attacks:

A. CSRF attacks typically involve the victim performing a state-changing action

B. Disabling execution of client-side scripts prevents all XSS attacks

C. If XSS attacks are made impossible, CSRF attacks are still possible

D. An XSS attack can be used to perform a CSRF attack

E. Properly sanitizing inputs prevents all CSRF attacks

Question 7 Which of the following attacks can best leverage *homographic encodings*?

A. command injection

B. phishing

C. SQL injection

D. XSS

E. CSRF

---

3 Asymmetric Cryptography and Signatures

Question 8 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. A user would have to know more secret keys if symmetric cryptography was used

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

D. Symmetric encryption algorithms are generally faster

E. For 10 users, symmetric cryptography requires 25 fewer secret keys

---

Question 9 You are given the certificate hierarchy in Figure 1.

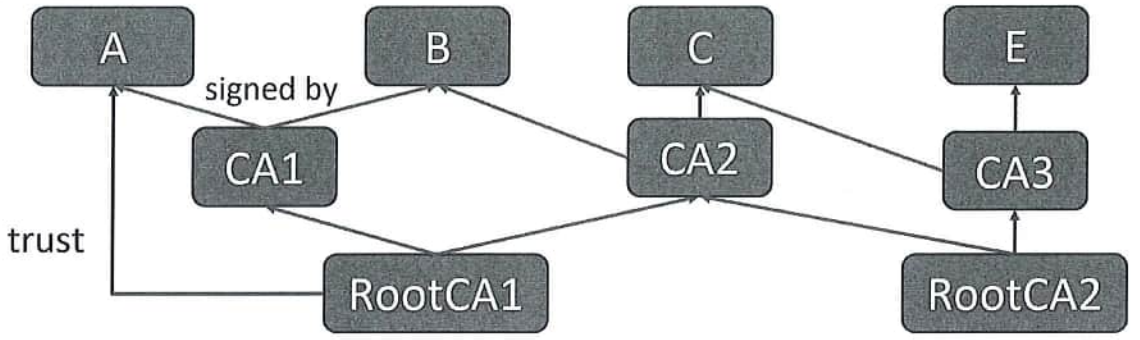

Figure 1 Certificate Hierarchy

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. $Cert_{CA3(C)}$, $Cert_{RootCA2(CA3)}$

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

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

E. $Cert_{CA3(E)}$

Question 10 In the first lab, you used S/MIME certificates for secure email. Which of the following is **TRUE**?

A. Sending a digitally signed email requires the certificate of the recipient

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

C. Verifying a digitally signed email requires the certificate of the sender

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

E. Encrypting a digitally signed email requires the certificate of the sender

---

4 Sandboxing and Virtualization

Question 11 AppArmor is used to restrict the capabilities of a program, and in doing so protect the operating system. Running a program inside AppArmor can enhance its security with respect to several design principles (by Saltzer et al). Select the principle that is not among these.

A. *Least privilege*

B. *Complete mediation*

C. *Separation of privilege*

D. *Fail-safe defaults*

E. *Least common mechanism*

Question 12 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 abstracts underlying components

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

D. Virtualization is designed to protect the system against viruses

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

---

5 Identification and authentication

Question 13 A brute-force attack uses randomly generated passwords and **does not** re-use passwords that proved invalid. Assuming the number of possible passwords is n, give the probability of cracking a password in at most k attempts, where $0 < k < n$.

A. 0

B. $1/n$

C. $2/n$

D. k/n

E. $1/n^k$

Question 14 You should of course *never* store passwords in plain text, at any time. Instead, always use *salted hashing*. How does this work – what of the following is **TRUE**?

A. The salt is used to make the password longer, but is not stored

B. It is a bad idea to save the salt you used for hashing the password

C. It is efficient and secure to use the same salt for all your passwords as long the salt is kept secret

D. The salt is hashed together with the password and the result is stored together with the salt

E. When checking an input password, you compare its hash value with the stored salt value

---

6 Information flow

Question 15 Information entropy is a measure of the uncertainty of the values of a variable, based on their probabilities. The value can be interpreted as the average size (in bits) of an optimally encoded value. Below, $H(X)$ is the entropy of the variable X, and n is the number of possible values for X. What of the following is **TRUE**?

A. If X can only have one value, then $H(X) = log_2(n)$

B. $H(X)$ can be negative in special cases

C. $0 \leq H(X) \leq log_2(n)$, with minimal value for a random distribution of X, and maximal value when X can only have a single value

D. $0 \leq H(X) \leq 1$, with maximal value for a random distribution of X, and minimal value when X can only have a single value

E. The maximum entropy is $H(X) = log_2(n)$

Question 16 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. What of the following is **TRUE** regarding the amount of information leaked by executing these programs?

A. $\boxed{x := (y + z) \bmod 4}$ leaks more information about y than $\boxed{x := (y + z) \bmod 2}$

B. $\boxed{x := y + z}$ leaks more information about z than $\boxed{x := y^z}$

C. $\boxed{x := y * z}$ leaks less information about z than $\boxed{x := y \text{ xor } z}$

D. $\boxed{x := y * z}$ leaks more information about y than it does about z

E. $\boxed{x := y/z}$ leaks no information about z

---

7 Access control

Question 17 The access control matrix can be implemented using Capability Lists (CL) or Access Control Lists (ACL). Which is better, when?

A. ACLs give a better overview of which subjects have access to a particular object

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

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

D. ACLs often allow delegation of rights between subjects

E. ACLs are better when subjects often need to have all their rights revoked

---

Question 18 Mandatory Access Control (MAC) differs from Discretionary Access Control (DAC). What of the following is **FALSE**?

A. In a MAC system, central policies define the access rights

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

C. "Classic" Linux file protection supports MAC

D. Role-Based Access Control is typically MAC

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

---

8 Software security

Question 19 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 20 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;
  }
}
```

Select the input which would give you the best chance at passing the PIN check, running the `sensitive` function, *and* terminating gracefully.

A. `111111111111111111111111`

B. `11111111`

C. `1234`

D. `1111`

E. `12345678`

---

9 Privacy and Tracking

Question 21 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 as 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 *least* useful information that an HTTP request could contain?

A. the size of the browser window

B. the universal time (UTC) when doing the request

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

A. disabling script execution

B. using highly customized parameters in HTTP requests

C. making your browser appear indistinguishable from many others

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 23 Suppose the attacks: SQL Injection, IP Spoofing, SYN Flooding, and MAC-address Spoofing. The layers, from left to right, these attacks target are:

A. Application Layer, Network Layer, Transport Layer, Link Layer

B. Transport Layer, Application Layer, Link Layer, Transport Layer

C. Application Layer, Transport Layer, Network Layer, Link Layer

D. Transport Layer, Network Layer, Application Layer, Link Layer

E. Application Layer, Network Layer, Transport Layer, Network Layer

---

Question 24 A security mechanism provides different forms of protection. What is **FALSE** of the following?

A. TLS provides confidentiality of data exchanged between applications

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

C. S/MIME can hide all the information in an email from an eavesdropper

D. SYN Cookies protects availability in the transport layer

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

---

11 Ethics in Security

Question 25 (2 points) You're leading a team developing a banking application for a major bank. Due to the nature of the application, security is critical. Tomorrow is the planned date for the next major release which will add support for two-factor authentication. However, regression testing is only 70% done, with no chance of finishing by tomorrow. Testing has not revealed any bugs and has exercised all the parts of the code judged to be security-sensitive.

Make a decision about whether to release the software or delay its release. 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: 2023–06–12**
	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 25 (please write LEGIBLY and only write inside the box):