Exam: Secure Computer Systems 1
1DT072
2023–01–05

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 *authenticity* (the security property) the following is **TRUE**:

A. Botnets are often used for attacking this vulnerability

B. A reasonable protection involves signatures

C. A trojan could reduce the accountability

D. Computing file hashes provide a mitigation

E. The threat can be controlled by proper access control

Question 2 Some network attacks can leverage *botnets*. Which security property do these attacks often target?

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

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

C. *Separation of privilege* says multiple conditions should be met before access is granted.

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

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

---

2 Web and data security

Question 4 Escaping the character '-' provides some protection against which attack:

A. XSS

B. SQL injection

C. path traversal

D. command injection

E. CSRF

Question 5 The following is **FALSE** regarding XSS (cross-site scripting) and CSRF (cross-site request forgery) attacks:

A. Disabling execution of client-side scripts prevents CSRF attacks

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

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

D. If all input is properly treated as data, XSS attacks can be stopped

E. CSRF attacks may be conducted via phishing

Question 6 To protect yourself against a XSS (cross-site scripting) attack, which method is **most** effective?

A. Disabling cookies in your web browser

B. Visiting only web servers that use HTTPS

C. Not clicking on suspicious links

D. Disabling script execution in your web browser

E. Visiting only web servers with trusted certificates

Question 7 Which statement is **FALSE** regarding homographs and multiple UTF-8 encodings of a string?

A. homographs are leveraged to perform phishing attacks

B. UTF-8 encodings are used to evade web filters

C. homographs look similar to the user, but mean different things

D. UTF-8 encodings are used to impersonate domain names

E. UTF-8 encodings are leveraged to perform XSS attacks

---

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 public-key cryptography. Which of the following statements is **TRUE**?

A. A user would have to remember more secret keys if public-key cryptography was used

B. Symmetric cryptography requires fewer keys in total

C. Public-key encryption algorithms are generally faster

D. Leakage of a secret key would compromise more secure channels if public-key cryptography is used

E. Adding a new user to the group is easier for public-key cryptography (i.e., it entails generating fewer keys)

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

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

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

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

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

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

---

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. *Open design*

B. *Complete mediation*

C. *Least escalation*

D. *Psychological acceptability*

E. *Least common mechanism*

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

A. Sandboxing is meant to protect 'sandboxed' applications from viruses affecting the system

B. Virtualization necessarily incurs a significant overhead

C. Virtualization is (mainly) a software feature, and not helped much by hardware support

D. Sandboxing enables running applications on different operating systems

E. Virtualization abstracts underlying components

---

5 Identification and authentication

Question 12 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 at exactly the k-th attempt, where $0 < k < n$.

A. k/n

B. 0

C. $1/n$

D. $2/n$

E. $1/n^k$

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. It requires a more secure hashing algorithm

C. Cracking the password of a user does not expose other users' passwords

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

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

6 Information flow

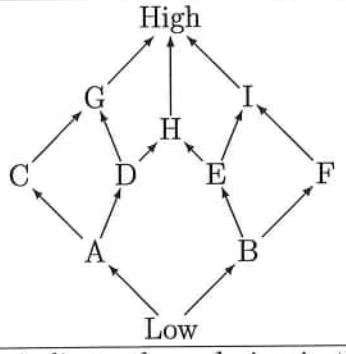

Figure 1 BLP lattice. Arrows indicate the ordering in the lattice.

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 1, using the rules of the Bell-LaPadula model?

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

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

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

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

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

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, and the entropy of the variable X is often written $H(X)$.

When reasoning about quantitative information flows, we can use *conditional entropy*. The entropy of X given Y is often written $H(X|Y)$. What of the following is **FALSE**?

A. The conditional entropy of a variable is at most its non-conditional entropy

B. The conditional entropy calculations are based on the conditional probabilities of the values of variables

C. The conditional entropy $H(x|y)$ can be used to find out about the amount of information which flows from y to x by a program

D. For the program `x := y*z;` the conditional entropy $H(x|y)$ is less than $H(y)$ if $H(y) = H(z) = 4$ and all the values of `y` and `z` are equally probable

E. For the program `x := xor(y,z);` the conditional entropy $H(x|y)$ is less than $H(y)$ if $H(y) = H(z) = 4$, $0 \leq y, z \leq 15$ and all the values of `y` and `z` are equally probable

---

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 subjects often need to have all their rights revoked

B. CLs are better for settings where 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. CLs give a better overview of which subjects have access to a particular object

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 **NOT** true?

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

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

C. Role-Based Access Control is typically MAC

D. "Classic" Linux file protection supports DAC

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

---

8 Software security

Question 18 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 `strcmp` with a safer alternative (e.g. `strncmp`)

B. enabling address randomization

C. compiling for a 64-bit architecture

D. increasing the size of the array `input`

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

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*.
Which of the following statements is **TRUE**?

A. The exploit is chosen based on the payload

B. The exploit uses the payload to exercise the vulnerability

C. The payload depends on the vulnerability

D. There is exactly one exploit for each vulnerability

E. The vulnerability is chosen based on the exploit

---

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 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 time zone

D. the language preferences in the browser

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

Question 21 Suppose you want to avoid being tracked when surfing the web. Which of the following measures has the potential of making you more trackable?

A. disabling script execution

B. changing the user agent string to a common one (e.g. Edge)

C. disabling third-party cookies

D. using Tor Browser

E. using different browsers

---

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. Which protection is NOT provided by the mentioned security mechanism in the following?

A. IPsec in tunnel model provides confidentiality of IP addresses

B. TLS supports authentication between applications

C. SYN Cookies protects integrity in the transport layer

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

E. Using SMTP over TLS ensures confidentiality between mail servers.

---

11 Ethics in Security

Question 24 (2 points) A recent article in The Guardian (Jan 4, 2020)[1] describes an "explosive leak" of thousands of documents from Cambridge Analytica, the now defunct data firm which misappropriated 87 million Facebook profiles and used them to influence voters in the 2016 US election. The recent leak reveals they were also involved in elections in Malaysia, Kenya and Brazil, as well as working to manipulate voters in 65 more countries. This rises fears that e.g. voters in the upcoming 2020 election in the US will be manipulated (not by Cambridge Analytica which is defunct, but by other similar companies).

Computer science (including data science, machine learning and artificial intelligence) is of course necessary to analyse and use these masses of data. Suppose one of your friends told you they had been offered a job at a company (lets call it Oxbridge Analytica) which specialises in analysing personal profiles and video from surveillance cameras. The purpose specified is to find people with mental problems and quickly give them help. The job is to further develop the methods used and make them more efficient and precise.

How could you help your friend to make a decision about whether to take the job or not? 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 think". 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 think" is not enough for any score at all.

Good luck!

[1] https://bit.ly/37Bfe5O

Exam: Secure Computer Systems 1 (1DT072)
Date: 2023–01–05

Score:

Your 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

Question	Answer				
12	A	B	C	D	E
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

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