

## i Instructions

To pass the exam you need to get points from most sections, and approximately 2/3 of the possible total score.

### ☑ Code of honour

**You may not ask for, or receive, help from other people when answering the exam.**

You should answer the exam individually, and answer the questions on your own. It is OK to read the course material and other resources, but not to ask a friend, your group, or an online forum etc, for help.

By handing in the exam, you certify that you have followed these rules.

**Select all options**

- ☐ I confirm that I will not seek assistance from anyone else to answer the exam questions.
- ☐ I confirm that I will not use unauthorized resources to answer the exam questions.

## 1 Principles

Which of the following is **true** about the classic design principles of Saltzer and Schroeder?

**Select one alternative:**

- ☐ *Separation of privilege* says protection mechanisms should be separated from each other, to avoid unintended overlap
- ☐ *Economy of mechanism* means to weigh the economic cost of introducing security against the gains in security
- ☐ *Complete mediation* says every possible situation should be considered (mediated) when implementing the secure kernel
- ☐ *Least common mechanism* means you should use the least common, i.e. most unusual, security mechanism
- ☐ *Least privilege* says every user must the fewest privileges needed for their job

---

Maximum marks: 1

## 2 Authenticity

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

**Select one alternative:**

- ☐ Botnets are sometimes used for attacking this vulnerability
- ☐ The threat must be controlled by proper access control
- ☐ Signing the hashes is a good choice for prevention
- ☐ A reasonable protection must involve encryption/decryption
- ☐ A trojan could reduce the accountability

---

Maximum marks: 1

## 3 Integrity

If there is a vulnerability with respect to *integrity*, the following is true:

**Select one alternative:**

- ☐ Signing the hashes is a good choice for prevention
- ☐ The threat must be controlled by proper access control
- ☐ A trojan could reduce the accountability
- ☐ Botnets are often used for attacking this vulnerability
- ☐ A reasonable protection must involve encryption/decryption

---

Maximum marks: 1

## 4 XSS & CSRF

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

**Select one alternative:**

- ☐ If all input is properly treated as data, XSS attacks can be stopped
- ☐ An XSS attack can be used to perform a CSRF attack
- ☐ CSRF attacks are possible even if you follow the HTML5 standard
- ☐ If Javascript is disabled, all CSRF attacks are stopped
- ☐ If CSRF attacks are made impossible, XSS attacks are still possible

---

Maximum marks: 1

## 5 XSS

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

**Select one alternative:**

- ☐ To trust only web servers that use using https
- ☐ To sanitize your input before using it
- ☐ To use nonces in web forms
- ☐ That the web browser disallows Flash media
- ☐ That the web server follows the HTML5 standard

---

Maximum marks: 1

## 6 Shell injection

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

**Select one alternative:**

- ☐ Race conditions are fundamentally important to protect against shell injections
- ☐ The attack injects data which is interpreted as shell commands
- ☐ If shell comment characters and boolean expressions are filtered, shell attacks are impossible
- ☐ The attacker can inject machine code in the shell command through a stack overflow
- ☐ The attack can be avoided by the use of *parameterized queries*

---

Maximum marks: 1

## 7 Hash properties

A common mechanism to detect integrity attacks is using cryptographic hash values. What is **most** important for cryptographic hash algorithms?

**Select one alternative:**

- ☐ That the hash algorithm is only known to the implementers, to make it harder for the attacker to hack it
- ☐ That the hash algorithm has unpredictable collisions
- ☐ That the hash algorithm is slow, to make hacking it take more time
- ☐ That the hash algorithm has predictable collisions
- ☐ That the hash algorithm is fast, so the user doesn't have to wait

---

Maximum marks: 1

## 8 Authenticity protocols

A simple protocol for detecting modifications of a message  $m$  while transported between **A** and **B**, is to attach a hash code  $H(m)$  to the message:

1. **A** sends both  $m$  and  $H(m)$  to **B**
2. when **B** receives the two parts (call them  $x$  and  $y$ ), **B** can compute  $H(x)$  and check that it matches  $y$ .

What if the following is **FALSE**?

Select one alternative:

- ☐ An attacker **C** can fabricate data which is accepted by **B** by simply creating a new message  $n$  and sending it with its hash code  $H(n)$  to **B**.
- ☐ The protocol can be fixed by using a fresh random nonce  $n$  in step 1, sending the three parts  $m$ ,  $H(m+n)$ , and  $n$ , and in step 2 verifying that  $y$  is  $H(x+z)$  where  $z$  is the third part of the received message.
- ☐ The protocol can be fixed by using a digital signature  $S(m, sk_A)$  in place of  $H(m)$  in step 1, and signature verification  $V(y, pk_A)$  in step 2, where  $(sk_A, pk_A)$  is the key pair of **A**.
- ☐ The protocol can be fixed by using a shared key  $k$  known only by **A** and **B**, which is hashed together with  $m$  in step 1 (when sending) and step 2 (when checking), i.e. using  $H(m+k)$  in place of  $H(m)$ .
- ☐ The protocol does not work, in the sense that an attacker can modify  $x$  (replacing the message) and modify  $y$  (the hash code) to match it, and this is not detected by **B**.

---

Maximum marks: 1

## 9 Certificates

In one of the labs, you used S/MIME certificates for secure email. Which of the following is correct?

**Select one alternative:**

- ☐ Sending a digitally signed email requires the certificate of the recipient
- ☐ Sending a digitally encrypted email requires the certificate of the recipient
- ☐ Verifying a digitally signed email requires the certificate of the recipient
- ☐ Decrypting a digitally encrypted email requires the certificate of the sender
- ☐ Digitally encrypting an email requires the certificate of the sender

---

Maximum marks: 1

## 10 Sandboxing

Sandboxing is more and more often used in e.g. web browsers.

Which of the following design principles (by Saltzer et al) is **most specifically** addressed by sandboxing?

**Select one alternative:**

- ☐ Economy of mechanism
- ☐ Defense in depth
- ☐ Complete mediation
- ☐ Psychological acceptability
- ☐ Least common mechanism

---

Maximum marks: 1

## 11 S & V

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

**Select one alternative:**

- ☐ Sandboxing is (mainly) a software feature, and not helped much by hardware support
- ☐ Sandboxing can lead to large overheads in execution time
- ☐ Virtualization can protect the system against viruses
- ☐ Virtualization abstracts underlying components
- ☐ Virtualization can allow a macOS computer to run Windows, or vice versa

---

Maximum marks: 1

## 12 Salted hashing

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**?

**Select one alternative:**

- ☐ It is efficient and secure to use the same salt for all your passwords as long as you keep the salt a secret
- ☐ The size of the salt varies, and is used to make all passwords in the system the same length
- ☐ The salt is a nonce, and should never be saved after using it
- ☐ The salt is hashed together with the password and the result is stored together with the salt
- ☐ When checking an input password, you compare its hash value with the stored salt value

---

Maximum marks: 1

## 13 Lock entropies

Compare the entropies of different locks: a standard 3-digit combination lock, a standard 4-digit combination lock, and the Birthday lock.



Assume the following:

- the birthday lock can be set for years 00-99, months Jan-Dec, and dates 00-99.
- 3- and 4-digit locks have random codes, while Birthday locks use the birthdate of their owner,
- but you do not know who is the owner of the Birthday lock.

Which of the following is **FALSE**?

Select one alternative:

- ☐ The entropy of the 4-digit lock is approximately 3.5 bits higher than the entropy of the Birthday lock.
- ☐ The entropy of the 4-digit lock is less than 4 bits higher than that of the 3-digit lock.
- ☐ The difficulty of breaking the code of the Birthday lock is about the same as that of breaking the code of the 4-digit lock.
- ☐ The entropy of the 3-digit lock is lower than the entropy of the Birthday lock.
- ☐ For well-constructed locks, it takes about 10 times more time to break the code of the 4-digit lock than that of the 3-digit lock.

Maximum marks: 1



## 14 CL & ACL

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

**Select one alternative:**

- ☐ CLs are better when the owner of an object often needs to revoke access rights to it
- ☐ ACLs always have a more compact representation than CLs
- ☐ CLs are better when subjects often need to have their rights to all objects revoked
- ☐ CLs are better for settings where objects have owners, who can quickly see who has access to their objects
- ☐ ACLs often allow delegation of rights between subjects

---

Maximum marks: 1

## 15 MAC&DAC

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

**Select one alternative:**

- ☐ Role-Based Access Control is typically DAC
- ☐ "Classic" Linux file protection always supports MAC
- ☐ When using DAC, all objects typically have a specific owner
- ☐ In a DAC system, central policies define the access rights
- ☐ On a Linux system with MAC, the root user can read and write any file

---

Maximum marks: 1

## 16 On wool and sheep

```
void wool(void) { // no argument, no value
    char buf[12];
    gets(buf); // read input
    if (strncmp(buf, "wool", 4)) == 0)
        // if the first 4 characters of input are "wool",
        // give a nice response
        printf("sheep!\n");
}
```

Above is the definition of the program procedure **wool**, which is vulnerable to a stack overflow attack.

What is the main problem with the procedure, which causes the vulnerability?

Select one alternative:

- ☐ The problem is the use of "strncmp" with the argument 4, which is off-by-one since strings in C are terminated by a null character. Given a longer input can still perform a stack overflow attack.
- ☐ The stack overflow is caused by the "void" argument declaration, and if **wool** is called with a suitable argument the attacker can inject arbitrary code.
- ☐ The "printf" procedure is used, which is known to have format string vulnerabilities. Instead, "puts" should have been used.
- ☐ The "gets" procedure is used, which is known to be unsafe. Instead, "fgets" should have been used.
- ☐ Allocating only 12 bytes for the "buf" variable, when it should be 4 times the length of the string "wool", i.e. 24.

---

Maximum marks: 1

## 17 Attacks

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 is **true** about those?

**Select one alternative:**

- ☐ The payload enables the exploit, allowing the vulnerability to act
- ☐ The vulnerability always depends on the exploit
- ☐ The exploit depends on the vulnerability
- ☐ The exploit is used to stop the payload from being executed
- ☐ Which payload to select always depends on the vulnerability

---

Maximum marks: 1

## 18 Spoofing

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

**Select one alternative:**

- ☐ Upgrading from IP version 4 to version 6
- ☐ All endpoint routers filter packets with spoofed addresses when they exit the local network, as they enter the Internet
- ☐ Strictly implementing IPsec at DNS servers
- ☐ Upgrading your network interface to handle more incoming traffic
- ☐ All endpoint routers filter packets with spoofed addresses when they enter the local network, as they arrive from the Internet

---

Maximum marks: 1

## 19 Layered security

Having security mechanisms in more than one layer is a good choice. What is **true** of the following?

**Select one alternative:**

- ☐ Using "ssh tunnels" to connect to web services is preferable to using https
- ☐ When S/MIME is used to encrypt all email, you must still consider confidentiality attacks from the layers above
- ☐ It is often a good idea to combine TLS with SSL in the transport layer, and WPA2 with WEP for Wifi.
- ☐ When Wifi is protected by WPA2 and the network cables are physically protected, no additional encryption is necessary
- ☐ Protecting both the network layer and the transport layer (e.g. using both IPsec and TLS) always gives enough protection

---

Maximum marks: 1

## 20 Clinical trials

One of your friends takes part in a medical study at a university hospital. The data collected in the studio is going to be publicly available after it finishes, but in a  $k$ -anonymous database. Your friend isn't sure what this means - please help! What is true?

**Select one alternative:**

- ☐ A person can be identified in the data only if at least  $k$ -many different properties about the person are known
- ☐ With additional information about a person, it may be possible to identify the person in the collected data
- ☐ If  $k$  is sufficiently large,  $k$ -anonymity ensures that even with additional information about the persons in the data, we cannot learn anything new about them from the database
- ☐ A  $k$ -anonymous database does not allow to identify individuals at all
- ☐ One can identify maximally  $k$  many individuals in a  $k$ -anonymous database

---

Maximum marks: 1

## 21 Epsilon vs k

The course dealt with two types of formal anonymity/privacy:  $k$ -anonymity and differential privacy ( $\epsilon$ -DP for some  $\epsilon \geq 0$ , or simply DP).

Which of the following does **NOT** hold?

**Select one alternative:**

- ☐ Any kind of data can be made  $k$ -anonymous (for some  $k$ ) or differentially private ( $\epsilon$ -DP for some  $\epsilon \geq 0$ )
- ☐ Combined with additional information, differentially private data can still reveal information
- ☐ Anonymity is quantified, and thus limited, in both  $k$ -anonymity and DP
- ☐  $k$ -anonymity and DP both provide *forward secrecy*
- ☐  $k$ -anonymity always has fewer privacy guarantees than DP

---

Maximum marks: 1



Words: 0

Maximum marks: 10

## ☒ Certification

By handing in the exam, I certify that

### Select all options

- ☐ I have answered the exam individually
- ☐ I have not received help from other people
- ☐ I have answered the questions on my own.

If you have any comments on the exam, please write them below:

**Write here**