4-hour Written Exam in IT-Security

Department of Computer Science (DIKU)

Date: November 11 2022

Preamble

This is the exam set for the 4 hour written exam in IT-Security, B1-2022. This document consists of 19 pages including this preamble; make sure you have them all. Read the rest of this preamble carefully. Your submission will be graded as a whole on the 7-point grading scale, with internal censoring.

- You can answer in either Danish or English.
- Write your exam number on all pages.
- You do not have to hand-in this preamble.

This is an individual, open-book exam. You may use the course book, notes and any documents printed or stored on your computer, but you may not search the Internet or communicate with others to answer the exam.

The exam set is divided into sub-parts that each are given an estimate of the time needed. However, your exact usage of time can differ depending on prior knowledge and skill.

The exam is a digital exam. Write your answers to the questions in the exam PDF document. All questions include trailing white space for in-line answers. The available spaces are intended to be large enough to include a satisfactory answer of the question; thus, full answers of the question does not necessarily use all available space. You may also choose to write your answers in a separate text or Word file and create and submit a PDF file from the text or Word file. Be sure to clearly note which question you are answering.

In the event of errors or ambiguities in the exam text, you are expected to state your assumptions as to the intended meaning in your answer. Some ambiguities may be intentional.

Write your exam number on all pages you hand in.

A. Short Answer Questions (40 minutes)

Answer the following with just a few sentences.

Question 1: Briefly explain the security principle of least surprise.

Question 2: What is STRIDE?

Question 3: What is multi-factor authentication?

Question 4: How can Internet Service Providers (ISPs) help defend against IP

source address spoofing?

Question 5: True or false: anomaly-based IDS are superior to signature-based IDS in detecting compromised user accounts under attacker control. Explain your answer.

Question 6: Suppose an attacker knows a document and its corresponding hash value and wants to find another document that hashes to the same value. Which desired property would we want the cryptographic hash function to have to withstand the attacker's attempts to find such a document?

Question 7: Why would you cryptographically hash a document before signing

it using your RSA private key?

Question 8: Would you rather slow down offline password guessing using password salts or iterated hashing? Briefly explain your answer.

Question 9: How can you defend against replay attacks?

Question 10: If an attacker compromises a user's browser in a drive-by download attack, would you expect the attacker to need to do privilege escalation to run

code as an administrator or root user? Why, why not?

Question 11: True or false: if a web server is vulnerable to a XSS attack, the web server itself is at risk of compromise. Explain your answer.

Question 12: DDoS attacks are often mounted using DNS. Why?

B. Security Principles (20 minutes)

Question 1: Suppose you want to wake up at 7:00AM tomorrow at the latest and you set not one but two alarms on your smartphone (for 7:00AM and 7:15AM) and ask your friend to call you (at 7:30AM). Which security principle are you following?

Question 2: If you were to place your car keys behind the left rear wheel of your car for your friend to pick up later, which security principle are you breaking?

Question 3: When entering a car parking lot, you arrive at a boom gate or bar that block access until you press a push button at the entry ticket machine and get a ticket. To exit the lot, you enter the same ticket in the ticket machine and pay the amount displayed, after which the the boom gate opens. Which security principle being followed here?

Question 4: If you regularly use your administrator or root account for tasks

where regular user privileges suffice, you are breaking which security principle?

Question 5: Disabling unused services on a server before placing the server on the Internet follows which security principle?

C. TLS (60 minutes)

An attacker is trying to attack KU and its users. Assume that users always visit KU's website with an HTTPS connection, using RSA and AES encryption (no Diffie-Hellman).

Question 1: Briefly explain how a TLS connection is set up when a user browses KU's website.

Question 2: If the attacker obtains a copy of the certificate for KU's website, the attacker could (choose all that apply):

1. Impersonate the KU web server to a user
2. Discover some of the plaintext sent in past HTTPS sessions to the server
3. Discover all of the plaintext sent in past HTTPS sessions to the server
4. Replay data that a user sent to the server over a previous HTTPS session
5. None of the above

Question 3: If the attacker obtains the private key of a certificate authority

(CA) trusted by users of KU, the attacker could (choose all that apply):

1. Impersonate the KU web server to a user
2. Discover some of the plaintext sent in past HTTPS sessions to the server
3. Discover all of the plaintext sent in past HTTPS sessions to the server
4. Replay data that a user sent to the server over a previous HTTPS session
5. None of the above

Question 4: Suppose the attacker obtains the private key that was used by KU's server during a past session, but not the current private key. Also assume that the certificate corresponding to the old key has been revoked. This attacker could (choose all that apply):

1. Impersonate the KU web server to the user
2. Discover all of the plaintext sent in past HTTPS sessions (encrypted with the old key)
3. Discover all of the plaintext sent in future HTTPS sessions (encrypted with the current key)
4. None of the above

Question 5: Suppose KU's web server instead of RSA relies on Diffie-Hellman to exchange keys to be used with AES.

Does that change your answer to the previous question? Explain your answer.

Question 6: Suppose the administrators of KU's network wants to decrypt and examine all HTTPS traffic originating *from* its internal network going through its gateway *to* the Internet. To do so they create a CA public/private key pair and installs the CA public-key on all employee computers, so that employee browsers will trust certificates issued by this CA. The gateway has the corresponding CA private key.

Explain the process by which the gateway eavesdrops on an HTTPS connection established by a browser inside the company and connecting to an external HTTPS web site.

Question 7: How can a KU user tell that a connection to, say `https://dr.dk`,

is being intercepted as described in your answer to the previous question? Please confine your answer to the browser user inferface.

D. Firewall, VPN and IDS (40 minutes)

Question 1: Briefly explain the difference between a stateful and stateless packet-filter firewall.

Question 2: Suppose a user on the internal network is infected with malware that can *i)* either open a port to listen on and provide an interactive shell to anyone who connects to that port, or *ii)* connect to a static IP address on the Internet where a Command and Control-server is ready to accept the connection and send back commands for the malware to execute.

If the network is protected by a stateful packet-filter firewall, which of the approaches *i)* or *ii)* would you expect the attacker would succeed with, if any?

Question 3: Suppose your network is compromised of a DMZ and an internal network. A gateway firewall that sits between the Internet and the DMZ, and an additional firewall sits between DMZ and the internal network.

The DMZ contains external servers and a NIDS. The internal network is for user

laptops and internal servers.

Suppose you want set up a remote access VPN for your users to work from home. Where would you want the VPN to terminiate in your network?

Question 4: Suppose a new wormable zero-day exploit has been released on the Internet. The affected software runs on port 445 on end-user computers. How could a network and host firewall, respectively, help to mitigate the situation until a patch is released, given that the software has to remain in function until then?

Question 5: The IP protocol supports fragmentation, which allows a packet to be broken into smaller fragments as needed and re-assembled when the fragments reach their destination.

The IP payload contains the next-layer protocol (e.g., TCP, UDP, ICMP). If this is a TCP packet, for example, then the TCP header and its data is contained in the IP payload.

Is fragmenting a problem to packet-filter firewalls? Explain your answer.

E. AES and Modes of Operations (40 minutes)

In this question, E_k denotes AES block cipher encryption and D_k denotes AES block cipher decryption with key k.

Question 1: Alice and Bob share a symmetric key k, known only to them. Alice sends Bob a message m = "I owe you \$100" and attaches a AES-CBC-MAC tag t computed using k and m. Bob can use m and t to prove to a third party that Alice sent m. True or false? Explain your answer.

Question 2: Recall that for AES-CBC encryption, $c_i = E_k(m_i \oplus c_{i-1})$, where c_i and m_i are the ith ciphertext and plaintext blocks, respectively. c_0 is the Initialization Vector (IV).

What is the purpose of the IV?

Question 3: Recall that for AES-CBC decryption, $m_i = D_k(c_i) \oplus c_{i-1}$.

Which parts of the ciphertext, if any, can the receiver decrypt, if the IV is modified by an attacker during transmission (so the correct IV was used during

encryption, but the receiver receives the modified value)?

Question 4: What is authenticated encryption?

F. SQL Injection (40 minutes)

Consider the following server-side code fragment with an SQL injection vulnerability:

```
$username = $_GET["username"];

$sql = "SELECT firstname, lastname FROM MyUsers
        WHERE username = '$username'";

$result = $conn->query($sql); // issue SQL query
if ($result->num_rows > 0) {
    print("Welcome back") // if matching record found
} else {
    print("User not found") // otherwise
}
```

Here `$_GET["username"]` is the username provided by the browser in the HTTP request. `print` writes its argument to the web page sent back to the browser.

The `SELECT` statement is used to select data from a database. The `WHERE` clause is used to filter records.

The following subset of operators may be used in the `WHERE` clause:

Operator	Example	Meaning
`=`	`username='alice'`	return records for 'alice'
`AND`	`1=1 AND 2=2`	return records if all conditions hold
`OR`	`1=1 OR 2=2`	return records if any conditions hold
`LIKE`	`username LIKE 'ali%'`	find values that starts with 'ali'
`--`	`--;`	comment out text after `--`
`SLEEP()`	`SLEEP(5)`	pause execution for 5 seconds
`NULL`	`NULL`	do nothing
`IF(x,y,z)`	`IF(1=1,NULL,NULL)`	if `x` then return `y` else `z`

Question 1: Explain why a URL where `username` is set to `' OR '1'='1` will

result in a succesful login.

Question 2: List and briefly explain one or more common prevention techniques against SQL injection attacks.

Question 3: Suppose the `MyUsers` table has a `password` column, in addition to the three columns referenced in the code above.

Describe how an attacker can extract the password of any user by exploiting the code fragment above.

Question 4: Consider another example server-side code fragment.

```
$username = $_GET["username"];

$sql = "SELECT firstname, lastname FROM MyUsers
        WHERE username = '$username'";

$result = $conn->query($sql); // issue SQL query
if ($result->num_rows > 0)
    $found = true; // record result
// Prepare web page without referencing $found
```

Here the response sent to the browser is oblivious to the SQL query results.

Describe how even now an attacker can extract the password of any user.