Question 1 **[Supway]** To avoid long queues, Supway wants to use shared files where clients, sandwich makers, and cashiers can communicate.
There are three kind of files:

- `order_X.txt` where `client_X` can write their order. Sandwich makers use these files to prepare the required sandwiches;
- `bills.txt` contains all paid orders. This file is used by cashiers to verify if a client has paid for their order, before giving them the sandwich(es); and finally
- `payment.py` a payment script which runs the payment operation, and, upon successful payment confirmation, logs the payment in the `bills.txt` file. This file is used by clients to pay for their order.

Which of the following permissions ensure that Supway can function correctly without allowing any adversarial behavior:

☒
```
-rw-rw-r-- supway client_X order_X.txt
-rw-r----- supway cashiers bills.txt
-rwsr-x--- supway clients payment.py
```

☐
```
-rw-rw-r-- supway client_X order_X.txt
-rw-r----- supway cashiers bills.txt
-rwsrwx--- supway clients payment.py
```

☐
```
-rw-rw-r-- supway client_X order_X.txt
-rw-r----- supway cashiers bills.txt
-rwxr-x--- supway clients payment.py
```

☐
```
-rw-r--r-- supway client_X order_X.txt
-rw-r----- supway cashiers bills.txt
-rw-r-x--- supway clients payment.py
```

Question 2 **[MAC]** Which of the following statements are true:

☐ The Chinese wall model is a form of discretionary access control.

☐ For labels **U**nclassified < **S**ecret < **T**op Secret, level (S, {Finances, Software}) dominates level (U, {Hardware})

☒ The Bell-Lapadula model is used to protect the confidentiality of objects.

☒ The BIBA model is used to protect integrity of objects.

Question 3 **[Crypto]** Which of the following statements are true:

☐ The output of a secure hash function is unique for every possible input.

☒ In asymmetric cryptography, a user decrypts a message with their secret key.

☐ The size of the hash function output depends on the size of the input.

☐ In asymmetric cryptography, a user encrypts a message with their public key.

Question 4 **[Authentication]** When storing passwords in a database, which of the following statements about salts are true:

- [x] The salt is stored in the clear next to the hash of the password.
- [ ] We use salts because they are large numbers, so concatenating them with the password will result in hashes that are very long.
- [x] Salts increase the cost of brute force attacks because users often select common passwords from dictionaries
- [ ] Salts increase the cost of brute force attacks because calculating the hash of the concatenation of two strings is very costly.

Question 5 **[CWE]** While you are logged into your bank's website (`https://creditbank.com`) in your browser, you receive an email with the following subject: *"Job opportunity at Appgle! Apply now"*, and open it right away in the same browser. In the email, there is an image attachment with the following HTML image tag:

```
<img src="https://creditbank.com/enabletransaction?account=ATTACKERACCOUNT&amount=10000">
```

As soon as you are done reading the email, you find that your bank account is missing 10000 CHF.
Which of the following CWE was exploited here?

- [x] Cross-site request forgery, because the code that loads the image takes advantage of an existing `creditbank.com` session cookie to execute the request on your behalf.
- [ ] Cross-site scripting, because the arguments to the URL to access the bank's website are not properly sanitized.
- [ ] Cross-site request forgery, because the arguments to the URL to access the bank's website are not properly sanitized.
- [ ] Cross-site scripting, because the code that loads the image takes advantage of an existing `creditbank.com` session cookie to execute the request on your behalf.

Question 6 **[Software Security I]** The HelloUserBank identifies customers with a username that has a maximum length of 13 characters. The HelloUserBank server runs the following login program with the username as first argument, and with standard output returned back to the user. Since this bank is very confident their system is secure, the program was compiled without any stack protection.

```
1  #include <stdio.h>
2  #include <string.h>
3  int main(int argc, char** argv){
4      int is_valid_user = 0;
5      int secret_key = 11111111;
6      char username[13];
7      strncpy(username, argv[1], 13);
8      printf("\%s", "Hello user: ");
9      printf("\%s", username);
10     if (is_valid_user){
11         strcpy(username, argv[1]);
12         /* Let user access his bank account. */
13         /* ... */
14     }
15     return 0;
16 }
```

Note:

- argv[1] refers to the first argument received by the program, in this case the username entered by the user.
- The function `strcpy(dst,src)` copies `src` to `dst`.
- The function `strncpy(dst,src,n)` copies at most `n` bytes from `src` to `dst` and does not guarantee that `dst` is null-terminated.

Which of the following statements are true:

- ☒ This code may allow a malicious user to recover the secret key.
- ☐ The use of a strict W^X policy would prevent a malicious user from exploiting the security bug in this program.
- ☐ This code may allow a malicious user to overwrite `is_valid_user` using a buffer overflow attack.
- ☐ The use of ASLR would prevent a malicious user from exploiting the security bug in this program.

Question 7 **[Software Security II]** Which of the following statements are true:

- ☒ The W^X policy, when strictly enforced, prevents code injection attacks.
- ☒ Canaries aims to protect from both code injection and control flow hijacking attacks.
- ☒ Control flow hijacking attacks are possible even when the adversary does not know the addresses of the system functions.
- ☐ A fuzzing testing framework must choose between attempting to test all control flows or test all data flows.

Question 8 **[Network security]** Which of the following statements are true:

- ☒ Unless IPSEC is used, IP headers contain source and destination IP addresses in clear.
- ☐ DNS hijacking is an attack where a router A tells other routers that A has fast routes.
- ☐ In ARP, the receiver can check the authenticity of a sender upon receiving a packet.
- ☒ ARP associates MAC addresses of given IP addresses.

Question 9 **[Privacy]** WeDoNotChat is a popular chat application with the following architecture.

WeDoNotChat complies with local law and uses TLS 1.3 to protect messages. When Client A sends a message to Client B, Client A establishes a TLS connection with Server A; Server A connects to Server B over another TLS connection; and then Client B establishes a TLS connection with Server B to fetch the message from Client A.
Assuming that WeDoNotChat traffic cannot be differentiated from other traffic, which of the following statements are true?

- ☐ Law enforcement that observes network traffic traversing the Magic Internet (3) can filter WeDoNotChat messages by matching certain keywords.
- ☒ Law enforcement that has access to the server A can filter WeDoNotChat messages by matching certain keywords.
- ☒ WeDoNotChat protects content of the conversations from the local Internet service providers.
- ☐ WeDoNotChat provides antisurveillance privacy.

Question 10 **[Malware]**
You downloaded the file free-photoshop.exe, a highly reputable open-source software, from an untrusted website on your laptop and you are worried that it is a virus/malware. Which of the following statements are true:

- ☒ If free-photoshop.exe includes a virus, the virus is able to propagate itself to your printer connected over a USB port even if the printer is not connected to the internet.
- ☒ If free-photoshop.exe is a ransomware, you are protected if you always open it from within an empty VM with restricted access to your computer and the network.
- ☐ If free-photoshop.exe is a ransomware, you are protected if no program on your laptop is susceptible to buffer overflows.
- ☒ To check whether there is a backdoor in free-photoshop.exe, the best practice is to compare the checksum published on the official website with the checksum of free-photoshop.exe after downloading it from the untrusted website.

[SHA? shhh. . .]
SHA3 is a hash function that takes a message m as input and outputs a fixed-length result h. We use the notation `SHA3(m) = h`. It is known that SHA3 is collision resistant, pre-image resistant, and second pre-image resistant.
Your friend ignores the advice that was given in the COM-301 lecture and decides to design a new hash function MYHASH where:
`PREFIX(m)` = the first 32 bytes of `m` (padded with "`0`" if `len(m) < 32`)
`MYHASH(m) = SHA3(m) || PREFIX(m);`
where `||` denotes the concatenation.

Question 11 Is MYHASH collision resistant? Justify.

☐ 0 ☐ 0.5 ☐ 1

.....

Question 12 Is MYHASH pre-image resistant? Justify.

☐ 0 ☐ 0.5 ☐ 1

.....

Question 13 Is MYHASH second pre-image resistant? Justify.

☐ 0 ☐ 0.5 ☐ 1

.....

[Geletram II] Geletram is happy to present their newest protocol.
Let (x, X) be the long-term (private, public) key pair of Alice, and (y, Y) be the long-term key pair of Bob. Geletram protocol works as follows:
Alice and Bob start a session by exchanging a session key:

SessionKeyExchange :

Alice :		Bob :
$a = random()$		
$X = g^x$		
$X' = X \cdot g^a$		$Y = g^y$
	$\xrightarrow{X'}$	
	$\xleftarrow{Y}$	
$SK = Y^{(x+a)}$		$SK = (X')^y$

Then, Alice and Bob use Symmetric Encryption (Enc) using the symmetric key SK to exchange messages for the rest of the session. For example for Alice to send m to Bob:

MessageExchange :

Alice :		Bob :
$c = Enc(m, SK)$		
	$\xrightarrow{c}$	
		$m = Dec(c, SK)$

All operations are done in Z_p (a group modulo p) where p is a well known prime number.
Every week, the current session is closed and Alice and Bob start a new session.

Geletram stores long-term secret keys of Alice and Bob: x and y, as well as the key exchanges and conversation logs: X', Y, and c in a database. Neither a nor SK are logged anywhere.
This full database leaked on New Year's Eve (i.e. 31st December 2022).

Question 14 Using the leaked database, can someone recover plaintext messages (m) exchanged by Alice and Bob during Christmas time? If they can recover the messages, describe how and propose a fix. If they cannot, justify why.

☐ **0** ☐ **0.5** ☐ **1** ☐ **1.5** ☐ **2** ☐ **2.5** ☐ **3**

.....

.....

.....

.....

[How-To MFA] The LFPE university now requires multi-factor authentication using Google Authenticator. During enrollment, the user receives 10 backup codes, which can each be used only once. Each backup code is a random 10-character sequence of upper-case letters (i.e. there are 26^{10} possibilities). Normally, Google Authenticator (on the phone) provides the second factor. If the user has temporarily or permanently lost access to their phone, they pick a fresh backup code from the list as the second factor.

Question 15 LFPE keeps the backup codes in a database on a server. How should the backup codes be stored to mitigate the impact of the database being leaked ?

☐ **0** ☐ **0.5** ☐ **1**

.....

.....

.....

[Google Maps] A user of Google Maps noticed in late 2022 that the URL changed from "`https://maps.google.com`" to "`https://google.com/maps`". A redirection from the original URL to the new URL was also added for backward compatibility.

Question 16 Will this change increase, decrease or have no impact on this user's privacy? Justify.

☐ **0** ☐ **0.5** ☐ **1** ☐ **1.5** ☐ **2**

.....

.....

.....

[DoReal] In the Computer Security class, many students use the social network app DoReal. Every minute the DoReal app on their phone connects to the `doreal.com` server with **HTTP** and checks if there's a notification for the student's account. If there is a notification, the app displays an alert and the student has one minute to take a picture of themselves and post it on the social network. The notifications are programmed to happen at a random time, including during the Computer Security lecture, which then disturbs the whole class. If there is no notification, the app doesn't show anything. If the request to the server times out, the app shows an alert saying that something went wrong, which also disturbs the lecture!
Edward, the professor, is very annoyed and wants to ensure that students are not distracted by DoReal while he is teaching.

Question 17 As a professor with good connections with the DSI team which controls the local network, he sets up a DNS hijacking attack to ensure that all student phones remain quiet during his lecture (at least when it comes to DoReal notifications). Describe how he sets up the attack, and specify which infrastructure (servers, switches, routers, etc.) needs to be either modified or added.

☐ 0 ☐ 0.5 ☐ 1

.....

.....

.....

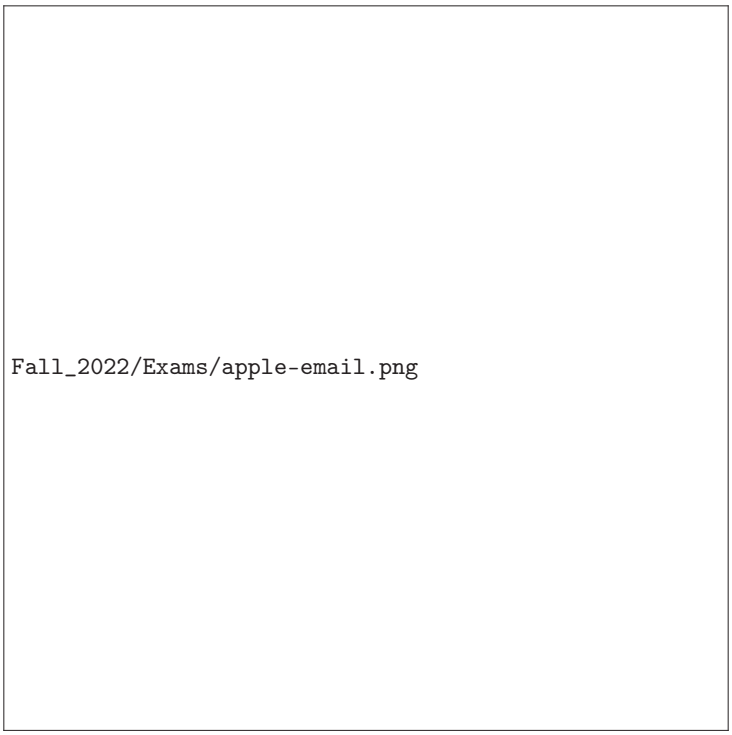
Question 18 The DoReal company then makes a software improvement to use HTTPS instead of HTTP. What are the consequences of this change on the DNS hijacking attack setup by the professor. Justify.

☐ 0 ☐ 0.5 ☐ 1

.....

.....

[Apple Mail Privacy]



Apple recently introduced a new feature, called Apple Mail Privacy Protection for its email client "Mail". The feature works as follows :
When a sender sends an email to an Apple Mail user, Apple caches on its proxy servers all content referenced via URL by that email. When doing so, Apple downloads all images, including tracking pixels. Tracking pixels are invisible images fetched via the HTTPS protocol that allow the sender of the mail to know when the email has been opened. Apple's caching action looks like an "email open" to the email service provider – even though the end user may not have opened the email.
When the user chooses to open the email themselves, Apple Mail downloads the remote content from the Apple proxy servers, not from the sender's web host or a server belonging to the sender's email service provider.

Question 19 What are the privacy implications for users of Apple Mail that enable this new feature? Justify.

☐ **0** ☐ **0.5** ☐ **1**

. . . . . .

. . . . . .

Question 20 Mailchimp is one of the world's most popular email marketing providers, making it easy for Mailchimp's customers to send legitimate commercial emails to their own customer base. For example, for a winery to announce its next wine tasting event. Mailchimp uses tracking pixels.
What are the implications of this new feature from Apple for the winery? Justify.

☐ 0 ☐ 0.5 ☐ 1

.....

.....

[Thesis Theft] Ariel has been working hard on her master's thesis, due in a few days, and which contains valuable and sensitive information. One morning when she turns on her laptop, she realizes that the Microsoft Word document that contains her entire thesis is missing. Furthermore, she notices a pop-up that says "*Want your thesis back? It'll cost you $1000*". Given the situation, she starts worrying and decides to come to you.

Question 21 What kind of malware is Ariel's laptop infected with? How can an adversary prove that they have not just destroyed the document from Ariel's laptop but hold a copy of it (without sending a copy to Alice as otherwise she would not have incentives to pay the adversary)? Justify.

☐ **0** ☐ **0.5** ☐ **1**

.....

.....

Question 22 To avoid this situation in the future, Ariel decides to back up her documents everyday using the university's backup system without installing any anti-malware software on her own computer. Name one security property preserved by this strategy. Name one security property that is not preserved by this strategy. Justify.

☐ **0** ☐ **0.5** ☐ **1**

.....

.....

.....