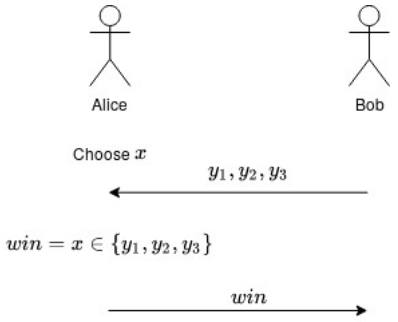
CS-301 Fall 2020 Mini-Exam 2

September 15, 2021

1 Guess My Number

Alice and Bob have decided to play a game called "Guess my number". In this game, Alice chooses one number between 0 and 100. Then, Bob has 3 chances to guess the number. Bob wins if he guesses the number correctly. How can Alice cheat? Bob thinks that using a Message Authentication Code (MAC) can prevent cheating. Can you integrate MAC into this game in a way that allows Bob to publicly show that Alice has cheated? What if Alice and Bob have a trusted friend called Charlie and Bob only cares about Charlie's opinion? Justify your answers.



2 Poetry Competition

Com-301 TAs have decided to hold a poetry competition in the class. Since TAs believe in transparency, they decided that all submissions must be public. However, this creates an unfair advantage for late submissions as students can read earlier poems. To fix this, TAs asked students to publicly submit their names and the hash of their poems during the competition and publish the full text after the deadline. Find a security threat in this competition and write the minimal requirement for the hash function to prevent any harm from these threats. Justify your answer.

3 Diffie-Hellman

Alice and Bob want to derive a shared secret using the Diffie-Hellman protocol. Alice will use this shared secret as a key to symmetrically encrypt a message m to Bob so that no one but Bob knows what she says to him. All in all, their protocol goes as follows. The public parameters are the modulus p and the generator g. Alice chooses a large secret number x and sends $g^x(modp)$ to Bob. Bob chooses a large secret number y and sends $g^y(modp)$ to Alice. After deriving the shared secret $sk = g^(xy)(modp)$, Alice uses it as a key to encrypt the message m to a ciphertext $c = Enc(sk, m)$, and sends c to Bob. What Alice and Bob are not aware of is that Mallory eavesdrops on all their communication, and can tamper with the messages they send to each other (Mallory can substitute any of their messages with an arbitrary string). Describe an attack in which Mallory achieves both of the following goals: (1) learns Alice's message m, and then (2) makes sure that instead of Alice's message, Bob reads another message m' of Mallory's choosing. Both (1) and (2) have to be done in such a way that Mallory is not detected (that is, from the point of view of Alice and Bob, the protocol goes normally).

4 Password updates

AcmeCorp forces all employees to come up with new passwords every three months. Provide at least one advantage and one disadvantage of such policy. Justify using the security principles.

5 Adversarial thinking

The TAs for COM-301 are frequently meeting in their coffee lounge to discuss the upcoming quizzes for the class and their solutions. To prevent curious students from listening to their conversations, the TAs have set up a simple authentication scheme to control who can enter the lounge. The TAs have a WhatsApp group and every morning send around the name of a new song to the group. To get entry to the lounge, you have to sing the first few lines of the current day's song. The people in the room will listen and if it is the correct melody you will be let in.?"

Is this a secure way to prevent students from entering the lounge? If you think the scheme is secure, justify what properties make it a secure authentication scheme. If you think the scheme could be broken, describe how and make a suggestion about how the TAs could prevent this attack from happening. The TAs also discussed adding a second step to the authentication process where you would not only have to sing the correct song but also name the title of the song before entry. Would adding this second step change anything about your answer to the first part of the question? Justify.

6 HMAC password

AcmeCorp is using HMAC without a salt to store MACs of passwords in their database. Represented as table, every row in the database reads:

```
Spock, HMAC(k, "VulcanRocks")
Kirk, HMAC(k, "Iampretty")
...
```

Where k is a secret key. Explain how AcmeCorp can verify that a user's password is correct and discuss the security of this storage method assuming that the database can be breached.

7 Collision resistance

Your cryptographer friend Bob has designed a new very efficient hash function he calls MD56. It satisfies pre-image resistance, but, unfortunately, does not satisfy second pre-image resistance. He says he will use it for signing a message m in which he commits to pay for your lunch at EPFL for the rest of the year: $sign(sk, H(m))$, where $H(m)$ is the MD56 hash of m. Is accepting this proposal from Bob a good idea? Justify.

8 Unix permissions Dave

Dave owns a business and has decided to develop a program to keep track of the shop inventory and manage his employees. However he's not an expert in Unix permissions and has asked you to give him a hand in configuring the access control. Give a good configuration of the access control, using the Unix format, ensuring the following system requirements (e.g. *-rwxrw-r– user1 group2 'file3'*):

Users:

1. Dave is the owner of the business
2. Alice, Bob and Charlie are employees

Files:

1. Employees schedules are written in f1.txt
2. f2 is a directory containing files for each employee's CV.
3. Inventory is written in f3.csv
4. f4 is a program to update the inventory (run everytime an item is bought by a client)

Requirements:

1. Employees should be able to read their schedules but not modify them, only Dave should be able to.

2. Only Dave should have permission to access or modify the inventory file.

3. Both employees and Dave should be able to run the *f4* program. This program requires read and write access to *f3.csv* to work correctly.

4. Only Dave can delete or rename CV files from the *f2* directory but both employees and Dave can add CVs to the directory

9 BLP

AcmeCorp is a software company. AcmeCorp is releasing a new software next month, and its engineering department is busy developing the software. Since AcmeCorp is highly secretive, it does not want the source code of its software to be leaked to anyone that does not need access to it. In the meantime, the marketing team prepares a functionality document, outlining the functionality of the software. They send it to the engineers to read. Once the engineers read and send a confirmation email that the document is correct, the marketing department prepares a new document called marketing campaign. They adjust the security level of the marketing campaign document such that everyone in AcmeCorp can view it but not make changes to it. Assume that AcmeCorp uses the Bell-LaPadula security model. Assign security levels (this includes clearance and categories) to the principals and objects in AcmeCorp, such that all the mentioned constraints are satisfied. Justify your decisions.

10 Biba

You are hired by Migoop, a new supermarket, to help them building their accounting system. For correct functioning, Migoop needs its managers to be able to get monthly balance reports, and accountants need to be able to audit the day to day operations. One problem Migoop managers and accountants are worried about is malicious cashiers reporting wrong earning and ruining their monthly balance. Explain this scenario in terms of the Biba model and assign security levels to principals and objects, explaining how the Biba rules can prevent those harms. Hint: Remember that principals are the subjects in the system that can perform actions on objects in the system. Consider that the system only covers elements in the question.

11 Covert Channels

As you liked COM-301 so much, you have asked to be Assistant Étudiant in 2021 and you got the job. While preparing the exam, the professor is worried that one of the TAs is leaking information about the questions to the students in

their Moodle answers. Thus, the professor asks you to think about one possible mechanism by which TAs may be leaking this information and devise a method to reduce the chance that this mechanism succeeds. Explain the leaking method and your proposed mitigation and argue its security.