IT-Sikkerhed, Assignment 1

ITS - 2021

Department of Computer Science
University of Copenhagen

M. Ali
M. Chleih

April 2, 2022

Review Questions

3.1 In general terms, what are four means of authenticating a user's identity?

- Something the individual knows, this includes a password, a PIN or answers to a prearranged set of security questions.
- Something the individual physically possess. This could be electronic key cards, smart cards and physical keys. This type of authentication medium is referred to as a token.
- Static bio-metrics, which are unique physical characteristics that an individual possess. This includes recognition by fingerprints, face or retina.
- Dynamic bio-metrics which are unique behavioural characteristics that an individual exhibits. This includes voice pattern recognition, handwriting characteristics and typing rhythm.

3.2 List and briefly describe the principal threats to the secrecy of passwords.

- **Offline dictionary attack:** The attacker obtains the system password file and compares the password hashes stored within the password file against hashes of commonly used passwords that the attacker is in possession of. If a match is found, the attacker can gain access by that ID/password combination.
- **Specific account attack:** The attacker targets a specific account and by the use of a brute-force approach, submits password guesses until the correct password is discovered.
- **Popular password attack:** A variation of the preceding attack is to use a popular password and try it against a wide range of user IDs.
- **Password guessing against single user:** Through various means including social engineering, the attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password.

- **Workstation hijacking:** The attacker waits until a logged-in workstation is unattended.
- **Exploiting user mistakes:** The user might be inclined to write down passwords because they are difficult to remember due to a strict password policy. An attacker may trick the user or an account manager into revealing a password. Also not changing pre-configured passwords for system administrators are a threat.
- **Exploiting multiple password use:** If different network devices share the same or similar password, security breaches become more damaging and effective.
- **Electronic monitoring:** If a password is communicated across a network to log on to a remote system, it is vulnerable to eavesdropping.

3.4 Explain how the proactive password checker approach can improve password security.

During the creation process the systems checks to see if the password meets certain requirements, if it does, it will be allowed otherwise rejected.
Since users have a tendency to create guessable and not-so-secure passwords, this scheme aims to alleviate that problem by providing specific guidelines for users to help them in the creation of a secure password that is unlikely to be guessed in a dictionary attack. This can be done using different approaches.
One approach is a system for rule enforcement, for instance, a password must have at least sixteen characters (basic16). Another approach is to have a blacklist of certain words, such that when the user selects a password, the system checks to make sure that it does not include a blacklisted word.

4.1 What is the difference between authentication and authorization?

Authentication involves verifying the credentials of a user, to determine whether or not said user is allowed to access the system.
Authorization on the other hand involves granting the right or permission to a verified user to access a system resource. For instance, an *authenticated* user is allowed access to a database with read-only privileges, therefore lacking the *authorization* to modify the content.

4.2 How does RBAC relate to DAC and MAC

In the DAC policy, access is based on the identity of the user and on access rules stating what users are or are not allowed to do. This closely relates to the RBAC policy in which access is based on the roles that users have within the system and on user privileges. The same goes for the MAC policy with its usage of security clearances that indicate which subjects are eligible to access which resources.

Problems

2.5

a.

- **DS**: Bob **will be** able to detect this since if the message was altered during the transmission, the hash value for the forged message will be different and when given as input to the verification algorithm alongside Alice's public key, the result is an invalid signature.
- **MAC**: Following the same logic from above, Bob **will be** able to detect this since the MAC will be different upon comparison.

b.

- Bob **will not** be able to detect by either DS or MAC, since the DS and MAC will be successfully validated.

c.

- **DS**: Bob **will be** able to detect this since all he has to do is, verify the message using the public key from both to find the alleged signer.
- **MAC**: Bob **will be** able to detect this. For this technique both communicating parties share a common secret key. Since Bob knows the secret key, he can ask both Alice and Oscar to reveal the key.

d.

- **DS**: Alice can obtain a copy of the message and signature and attempt to verify it with her public key to prove whether or not she has sent the message. Alternatively, she can attempt to verify the signature with Bob's public key. If the signature is valid then Bob himself must have written the message.
- **MAC**: Alice can not disprove Bob's claim, since they both have the same secret key thus, the MAC will be valid upon comparison.

2.6

Assuming that the hash function H has no second pre-image resistance and neither weak or strong collision resistance, the security requirements are as follows:

1. H can be applied to a block of any data size.
2. H produces a fixed-length hash.
3. $H(x)$ is easy to compute within hardware and software limitations.
4. Given a hash code, it is impossible to find the original message.

We assume that H is pre-image resistant, otherwise the function is pointless. Since H is only pre-image resistant it takes 2^n tries to find a collision:

$$2^{16} = 65536 \text{ random message would be require to find a collision}$$

SEED Lab

Task 2

The following encryption standards and modes of operation were used:

- **DES-ECB**: The plain text consisted of the same character repeated multiple times. We observed a pattern in the cipher text. This is due to the way ECB works.
- **AES-128-ECB**: The same plain text was used, however, we did not notice a pattern at first. We then figured out that this is because the plain text was considered a single block since it did not have a length that exceeded 128 bits. We then added more of the same character to end up with a string of length 32 bytes, i.e two blocks. Encrypting this, resulted in a pattern.
- **DES-CBC**: The same plain text was used, but no pattern was detected.

Task 3

When using **ECB** we were easily able to see the the different geometrical shapes. The reason for this is that, when encountering the same plain text/data, the ECB mode encrypts in the same manner resulting in the same cipher text. This is also what we experienced in the previous task.

With **CBC** however, we were not able to deduce any information regarding the original picture. This is because in CBC mode, each block of plain text is XORed with the previous cipher text block before being encrypted. This way, each cipher text block depends on all plain text blocks processed up to that point, ensuring that even if the plain data is the same, it will be have different ciphers, effectively creating pseudo-randomness.

Task 5

ECB

Before conducting the task: If a single bit of the cipher block is corrupted then only the corresponding plain test block will be corrupted the rest of the plain text will not get corrupted due to how the ECB scheme works.
After conducting the task: Our initial deduction is correct.

CBC

Before conducting the task: By virtue of the self-healing property in the CBC mode, if one block of cipher text is altered, the error will propagate for at most two blocks including the plain text block that is associated with the corrupted cipher text block itself. Thus, only two plain text blocks will be corrupted since the third block takes a "clean" cipher text at input.
After conducting the task: Our initial deduction was mostly correct. The corrupted cipher block resulted in corrupting the corresponding plain text, moreover, the same corrupted cipher block is XORed with the next decrypted cipher block, where only the corresponding byte in the decrypted block would be corrupted and not entire the block.

CFB

Before conducting the task: This mode is similar to CBC. The corrupted cipher text is XORed with the plain text, then the same cipher text is passed to the block cipher encryption which in turn gets XORed with another an un-corrupted cipher text, so the erroneous bit will propagate throughout the entire plain text.
After conducting the task: The plain text block that was associated with the corrupted cipher block was the one mostly affected. Then when the same corrupted cipher is XORed with the block cipher encryption is underlying corrupted bit is also corrupted in the plain text, similar to CBC.

OFB

Before conducting the task: When a bit is corrupted, only the corresponding bit in the plain text would be corrupted. The corruption will not propagate, since the corrupted block is not used by other encryption blocks.
After conducting the task: Our initial assumption is correct. The corrupted block is isolated from the rest of the process.