Computer Security

Name: Daniel Silva (00201725)

Theme: Homework 2.

Exercise 1:

1. Suppose a password is chosen as a concatenation of seven lower-case dictionary of size 50,000. An example of such a password is "mothercathousefivenextcrossroom". How many bits of entropy does this have?

$E = \log_2(50000^7)$

$E = 109{,}27$ bits

R: 109,27 bits

2. Consider an alternative scheme where a password is chosen as a sequence of 10 random alphanumeric characters. An example is "dA3mG67Rrs". How many bits of entropy does this have?

$A = 26$

$a = 26$

$d = 10$

$T = A + a + d = 62$

$E = \log(62^{10})$

$E = 59{,}54$ bits

3. Which password is better, the one from 1 or 2?

The first one is better, because the entropy is higher than the second one. So, the first one is better password, it has more uncertainty.

Exercicio 2 :

1. Design a data verification system using hash functions Explain the steps involved in the process.

SHA-256

1st. It's important to choose a secure hash function. In this step, I searched information and I selected SHA-256, because it is famous for its security and collision resistance.

2nd For the dataset, we have to apply the hash fuction selected, because it's important to obtain a unique hash value. This value is secret.

3rd In this step we have to storage the original value in a secure place.

4rd We have to share the hash to the recipients.

5th When the recipients obtain the data, the recipient has to calculate the hash value with SHA-256.

6th Using the new hash value, we have to comparate both hash values: original and calculated. If both math, the data hasn't been modified.

7th If it doesn't match we decline the data.

2. Discuss the advantages and disadvantages of using hash functions for data verification.

Advantages

- Hash functions implemetation is simple.
- Security in transmission of data.
- To calculate hasha value is fast and efficient.
- Using hash functions help us to detect changes of data.

Disadvantages.

- It would be vulnerable to some attack.
- Some Hash function could generate collisions
- A hacker could modify the data and then calculate a new hash.

3. Provide an example of a real world application where data verification system using hash functions is used.

The best excample of using hash functions for data verification, is for download files from websites. In this case, developer use to use hash functions to ensure that files wich user download didn't be corrupted. Software developer make a hash of the file, usig a hash function. Then the developer publishes the hash value with the file. Next, User download the file and calculate the hash value. Then, user compare both hash values and verify if it is autentic.

Exercise 3:

1. Define what a Message Authentication Code (MAC) is and how it is used in cryptography.

A message authentication MAC is a cryptographic checksum used to detect both accidental and intentional modifications to data. A MAC requires two inputs: a message and a secret key known only the originator of the message and its intented recipients.

A MAC is used to authenticate a message. MAC values are calculated by applying a cryptographic hash function with secret key K, wich is known only tho the sender and reicipient, but not to attackers. Mathematically, the cryptographic hash function takes two arguments: a key K of fixed sized and a message M of arbitrary lenght. The result is a fixed-length MAC code: MAC= CK(M) where M is a message into a MAC value and that uses a secret key K as a parameter MAC is the value fixed length calculated MAC

2. Explain the process of generating an verifying MAC.

1st MAC generation

- Select the MAC function
- Share the secret Key
- The sender takes the original message and the secret Key and calculate the MAC message.
- Attatch the MAC to message

2nd Message transmission and MAC

- The sender sends the message along with the MAC to the receiver through the communication way.

3rd MAC Verification

- The receiver receives the message.
- The receiver calculate a new MAC.
- The receiver compares both MAC.

3. Discuss the importance of using MACs in secure communication systems.

MACs are important tool in modern Cryptography. MACs are used to verify the data integrity and detect both accidental and intentional data modifications. MAC values are calulated by applying a cryptographic hash function with secret Key, wich only to the sender and recipient, but not to the attackers. MACs are used to authenticate messages in many application, including file integrity verification, strong passwords, digital signatures and blockchain. MACs are an effective way to protect data and ensure that it has not been modified without authorization.

Exercicio 4:

Given the values of $p = 17$ and $q = 23$, generate a pair of keys for RSA.

$n = p * q = 391$

$\varphi(n) = (p-1) * (q-1) = 352$

Using:

$e = 3$

$g(3) = 235$

PuK = $(n = 391, e = 3)$

PrivK = $d = 235$

Exercise 5:

1. Design a public Key infrastructure PKI. Explain the components and their roles in system

- Certification Athority is the trusted entity that issues and manges digital certificats. Its roles include verifying identity of the requester.

- Digital certificates are electronic documents that contain the owner's public Key, identity information and the digital signature of the CA

- The validation authority verifies the validity of the digital certificads issued by the CA.

- PKI database stores and distributes information about certificads, public Keys and certificads revocation.

- Certification Policies establish the rules and the standards that govern the issuance, renewal and revocation of digital certificats

- Public and private keys that users generate a pair of them. These are included in the digital certificate

2. Discuss the advantages and challenges of implementing a PKI system.

Advantages

- Provide a high level of security for authenticates data encryption.
- Allows the authentication and verification of the identity of the pairs.
- Ensures that data has not been modified in transit.
- Facilitates the secure managment of public and private keys.

Challenges

- Implements a managing a PKI system can be expensive
- Requires advanced technical knowledge and the managment of complex policies.
- Managing a large-scale PKI can be challenging

3. Provide an example of a real-world application where PKI system is used

The security of online transactions, such as online shopping and online banking. Banks and e-commerce sites use a PKI system to ensure the security of online transactions. Users can securely authenticate using digital certecates and transactions are encrypted to protect the confidentiality and integrity of data. Digital certificates issued by a CA allow users to trust the authenticity of websites and applications, which is critical for online security

Exercise 6:

Design a system for digital signatures based on public-key cryptography. Explain the steps involved in the process and role of each component.

1st The first step is step is to generate a key pair, one public and one private. The public key is used to verify the signature, while the private key is used to create the signature

2nd Create a message digest using a cryptographic hash function. The summary is a single, compact representation of the message

3rd The private Key is then used to encrypt the messag digest. The result is the digital signature

4th The public Key is then used to decrypt, the encrypted message digest

Roles

- Public Key: to verify the digital signature
- Private Key: to create the digital signature
- Cryptographic hash functions used to create a unique digest of the message
- Message summary is a single representation of the message.
- Digital signature is the result of encrypting the messag summary using the private Key.