Universidad San Francisco de Quito

Computer Security

Homework 2

Name: Mateo Ruiz

Banner: 00212195

Exercise 1:

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

To develop this exercise, we will use the entropy formula in bits: $Log_2(N^L)$

Where N will be the number of letters found in the alphabet (26), L the length of the password (7), E the size of the dictionary (50000).

$$\text{Entropy} = 7\ x\ Log_2(50000) = 109.27\ bits$$

2. Consider an alternative scheme where a password is chosen as a sequence of 10 random alphanumeric characters (including both lower-case and upper-case letters). An example is "dA3mG67Rrs". How many bits of entropy does this have?

N = 26 for lower cases + 26 for up cases + 10 for characters

L = 10

$$\text{Entropy} = Log_2(62^{10}) = 59.54\ bits$$

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

   The first one because it has a higher entropy than the second one, and that's its better in terms of security

Exercise 2:

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

These are the steps for a data verification system:

First, we start with the creation of data, then we proceed to create the hashing. In the third step, the original data is sent to a container with its respective hash value, so that the recipient then receives both the original data and the hash values.

In the fifth step, the recipient re-hashes the received data to generate a new hash value again. In the sixth step, the recipients compare the generated hash values with those received, if

they match, the data is considered valid. In the seventh step, the recipient ensures that there has not been any type of change or manipulation in the data, this is simple, since any type of change would end up giving a different hash value. Now if the hash value is different, then it is reported that the data has undergone changes.

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

The advantages of using hash functions are that they allow the integrity of the data to be guaranteed, thanks to the use given to hash values. Likewise, hash functions are much faster and more efficient when calculating. Another of its advantages is that the hash values have a size independent of that of the original data.

Among the disadvantages of using hash functions is that they do not have authentication, they are capable of verifying the integrity of the data but it does not guarantee who generated the data, likewise, there may be the case that two different sets of data may have the same hash value, thus causing a collision. Finally, hash functions can be very vulnerable to attacks if they are not designed well enough.

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

As a real example we can put the websites that are responsible for distributing different files or software to their respective users. In this case, the company must always be sure that the files have not been corrupted, mistaken or manipulated during their download, so This way, they can verify its integrity using hash functions.

Exercise 3

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

The message authentication code or MAC is a block of data that has a fixed size, which is sent with a message to determine its origin and integrity.

In cryptography, the mac can be generated in different ways, but generally it is used to detect any modification or corruption of data during transmissions, in the same way it allows authenticating senders, in addition to having security protocols such as TLS/SSL

2. **Explain the process of generating and verifying a MAC.**

To generate a MAC, the sender must want to send a message and see that the receiver is able to verify the integrity, likewise, both parties must have a shared key to generate the mac, then the sender must take the message and shared key to apply it to a MAC function such as HMAC, in this way a MAC value can be created, finally, with the created MAC value you only have to attach the message and send it to the receiver

To verify the MAC, the receiver receives the MAC sent by the sender. Since it has the same key, it must only apply it to a MAC function to obtain its own MAC value. In this way, the

receiver compares its MAC value with the sender's MAC value. and if they match, it means that the message is authentic.

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

The importance of using MAC lies in the fact that it allows us to guarantee that messages are not altered or come from an illegitimate source. This allows us to maintain and protect the integrity and authenticity of the information, something that allows us to combat and prevent online fraud.

Exercise 4

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

$$n = p*q$$

$$n = 17*23$$

$$n = 391$$

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

$$= (17-1)*(23-1)$$

$$= 352$$

In this case, to choose our value we can take any integer smaller and coprime of (n), so we will use the number 3

On the other hand, for d we will use the modular inverse of e with respect to (n), therefore $d * e \equiv 1 \pmod{\varphi(n)}$, however to calculate this we use the function pow, so that pow (3, -1, 352) = 235

So, our peers are:

Public key:

n = 391

e = 3

Private key:

d = 235

Exercise 5

1. Design a public key infrastructure (PKI) system. Explain the components and their roles in the system.

To design a PKI we must consider a series of sets of components, procedures and policies.

<u>We start with the Certificate authority CA:</u>

Its role is to issue and sign digital certificates, it verifies the identity of the sender, in addition to associating it with its public address, and then issuing the digital certificate.

Registration Authority RA:

This will be in charge of verifying the various identities of the entities that request certificates just before the CA issues them, authenticates and guarantees that everyone complies with the measures before continuing.

Digital certificate:

This is a file digitally signed by the CA, it contains the key and the data of the entity, it is used to authenticate and guarantee the integrity of the data

Public and private key:

Each holder has a pair of keys, this is used to encrypt data and verify signatures

Database:

Container that stores and distributes digital certificates

Security politics:

Policies that allow controlling and guaranteeing the security of how the PKI system operates

Certificate Revocation List CRL:

Repository that stores all the certificates that have been issued by the CA in addition to the revocation lists of those certificates that are no longer valid, this is where users can verify if their certificates are still valid

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

The advantages of implementing a PKI system range from providing a solid basis for authentication and encryption, it also guarantees that data is not modified during any transmission, its authentication system is reliable and it also helps comply with privacy and security regulations.

The challenges when implementing a PKI system begin with the fact that they have a relatively high level of complexity, implementing and maintaining it can have a high cost, since it must have the ability to be scalable, in addition to key management being critical.

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

In real life we can see that PKIs are used in banks, since they allow them to issue digital certificates to their clients, relating them to their respective public keys, in this way users can use their keys to authenticate with the banking system, in addition, the PKI ensures and protects the integrity of transactions, thus avoiding the fraud rate and reducing the response time to different security incidents.

Exercise 6:

To design a digital signature system based on cryptography we need the following steps.

Key generation:

First you need a pair of keys, the public and private. Their respective role is to sign certificates for the private and verify the signatures for the public.

Digital signature:

This occurs when a user wants to make a signature, the role of this is the generation of a unique signature that is attached to the document.

Signature verification:

This allows us to verify the validity of the signature, its role is to decrypt it with the public key and compare it with the new signature. If both agree, the signature is authentic.

Document integrity:

This is responsible for ensuring that the document has not been modified after being signed.

Digital certificate:

Implementation of a CA, these will allow users to be associated with their respective public keys.

PKI:

This allows us to guarantee the security and trust of the digital signature process, since it manages, issues and revokes certificates.

Security and audit:

This is responsible for guaranteeing the security of the system in accordance with its security policies, complying with legal requirements, in addition to guaranteeing the protection of your keys.