Homework 2 José Luis Santillán

Monday, October 16, 2023

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?

   Total number of combinations = 50000^7

   $Entropy\ =\ \log_2(50000^7)$

   $Entropy\ = 7\ \times 16.61$

   $Entropy\ = 109\ bits$

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?

   $Possible\ characters = 26 + 26 + 10$

   $Possible\ characters = 62$

   $Total\ number\ of\ combinations = 62^{10}$

   $Entropy = 10 \times \log_2(62)$

   $Entropy = 59.5\ bits$

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

   The first one is better due to its higher entropy, is implies that more combinations are possible, so it is harde to guess or apply some brute-force algorithm

Exercise 2:

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

   a. Select cryptographic hash function like SHA-256 and be sure it is a collision resistant function

b. Accept the data that is going to be verified.
c. Time to compute the hash and produce the output.
d. Store the hash output alogin with the data input. It either can be with the data or in metadata. It depends on the implementation.
e. Time to verify, by hashing the input again with the same hash function.
f. Compare the new hash with the transferred. If both hashes match means that the data has not been altered.

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

   This functions play a critical role in ensuring data integrity. Here are some advantages and disadvantages of using these functions

   Advantages:
   - Data integrity: Any minor change in the data results in a different hash value.
   - Non reversibility: It is not possible tod retrieve the original input data from its hash value
   - No collision: A good hash function ensures that two inputs produce the same hash value

   Disadvantages
   - Not so fast: The most secure hash functiones can be slower, and dependendin on the data input it may take more time.Might be an issue for real time applications
   - No recovery: One the data is hashed. the original data can not be recovered. It depends on the context, but it may be a disadvantge at some point.
   - Need to be in constant updates: Since technology is evolving fast as well as computational capabilities, new attack methods are discovered and hash functions need to be replaced and updated to provide more security.

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

   The example I can think of where hash functions are applied in a real word application is on digital signatures. They are used to verify the authencity and the integrity of the dats, such as documents. When a document is digitally signed, a hash function is applied. On the receving end, the process is reversed, it computes a new hash and decrypt the digital signature using the public key to obtain the original hash. It the two hashes match, it verifies de document.

Exercise 3:

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

   Is a code that provides a way to verify that a message has not been altered and that it comes from a legitimate source. It takes a secret key and an input, it produces an output which is the MAC tag, it is sent with the original message, and the receiver can cmompute the MAC value with the secret key that also knows. If they MAC Code matches, then is considered verifies and unaltered.

It is used in cryptography for example for data transfer, when to agents communicate over an inscure or public channel and want to ensure authencity and integrity. Also MAC codes can be used in password verification systems, it is a versatile technique in this context.

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

   a. Key agreement: Both parties agree upon and share a secret key
   b. Message preparation: The sender prepares the content he want to send
   c. MAC Algorithm: One we have the message, the MAC Algorithm is applied, This coould be and specific MAC function or a hash based on MAC. The output is a MAC tag
   d. Transmission: The sender receives both the original message and the MAC value
   e. Reception: The receiver gets the message and MAC value
   f. Recomputing MAC: The receiver computes again the MAC Algorith to calculate a new MAC Code
   g. Compare: If the two MAC codes match, it means that the message has not been altered.

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

   MACs play an vital role in maintaining the integrity and authencity of the data that is transmited, especially through insecure channels and information that need to be verifies such as documents. It is a faster technique than digital signatures, are more effcient. It is ideal for real time apllications or real time commuinications such as streaming servcies. Also it is flexible with the algorithm you want to apply, whether is a SHA-256 or HMAC. So in conclusion, it gives a lot of benefits and on this days where a lot ofo information is sent through the internet, it is very important.

<u>Exercise 4:</u>

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

$n = p \times q$

$n = 17 \times 23$

$n = 391$

$\emptyset(n) = (p-1) \times (q-1)$

$\emptyset(n) = (17-1) \times (23-1)$

$\emptyset(391) = 16 \times 22$

$\emptyset(391) = 352$

Lets choose $e = 13$

$d \times e = 1\; mod\; 391$

$d \times 13 = 1\; mod\; 391$

$d = 325$

Public and private key

$Public = (391, 13)$

$Private = (391, 325)$

Exercise 5:

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

   PKI uses a dual-key mechanism: a public key and a private key, with the public key being openly available while the private key remains confidential to its owner.

   a. The pair of keys. The public key is distributed openly, while the private key is confidentila and onli known to the owner.
   b. The digital certificat ethath binds a public key to an entity. It contains the key and other relevant information. It confirms the identity of the certificate holder.
   c. The certification authority. The third party entity responsible for issuing, renewing and revoking digital certificates
   d. The registration authority. It is the verifier of the certification authority beofre the digital certificate is issued to the end user.
   e. The certificate revocation list. It is a list of certificates thath have been revoked by the certification authority before the expiration date.
   f. The digital signatures. Provides a proof of the origin, identity and the status of data. It is created using the private kkey and can be verifies using the public key.
   g. The hardware security modules. The physical hardware that ensures and provides cryptoprocessing. They safeguard private keys.
   h. The PKI policies. It defines the framework and procesdures within which all entities in the PKI System operate. It is the standar the the roles.
   i. The end entites. The entities or users thath employ certificates for secure communication.
   j. The certificate repositories. It is where all the certificates are stores and the certificate revocation list are held and be queried by the entities.

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

   Implementing a PKI System offers a range of advatges but also comes some challenges that are the following

   Advantages
   - Provides a robist security for data in transit ensuring that the message was not altered.
   - Can me scaled to support a lot of users
   - Provides strong authentication mechanisms with digital certificates
   - PKI Standards are widely used and recognized so it can be used across different systems and softwares.

   Disadvantages
   - Management of a PKI can be costly, especially for large organizations
   - A compromised private key can undermine the security of the entire PKI
   - Users may need training on how to request certificates or use the digital signatures.
   - The hardware and server that host the PKI need to be physically secured to prevent unauthorized access.

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

   After doing somre research, the PKI system is applied in Secure Sockets Layer and Transport Layer Security. This is particularly vital for websites that hanlde sensitive information, perfetc examples of real word applications where PKI systems are applied are on major platforms such as Amazon, or online banking sites. They used it to secure user data and of course transactions.

Exercise 6:

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

A digital signature system based on public-key cryptography provides integrity regarding the origin, identity, and status of an electronic message or document. The principal components are the following:

a. Key pairs: The private key is kept secret by the user and used to sign messages. The public key is shared and used by others to verify signatures.
b. Digital Siganture algorithm: Provides the mathematical foundation for creating and verifying digital signatures.
c. Hash function: Ensures that even a tiny change in the message will produce a different hash.
d. Digital certificate: Assures the recipient that the public key used to verify the signature truly belongs to the sender
e. Certification authority: The third party entity responsible for issuing, renewing and revoking digital certificates

Now the steps:

1. The key generation, both the private key and the public key
2. The user sends a request to the CA for a digital certificate, usually by providing their public key
3. The CA verifies the users identity, issues a digital certificate that binds the user's public key to their identity. The CA signs the certificate with its own private key.
4. The sender of the message creates a hash of the message using a hash function.
5. The sender then encrypts this hash using their private key, creating the digital signature.
6. The original message and its digital signature are sent together to the recipient.
7. The recipient receives the message and the digital signature.
8. The recipient decrypts the digital signature using the sender's public key, retrieving the original hash.
9. The recipient computes a new hash of the received message, if it matches then it is verified.