CA 1

E-Commerce

Alejandro Pérez Bueno

Oct 22, 2024

Table of Contents

Statement

The community of residents of tourist homes must prepare a document to request the City Council to carry out work on streets near their area. Since the owners of the flats do not live in the area, it is necessary to prepare and submit the text using, exclusively, telematic means. To this end, the Community Administrator has established the following procedure:

a. The Administrator prepares a first draft of the text and sends it to each neighbor.
b. Each resident may ask the Administrator to make the necessary modifications to the text.
c. Once the final text has been agreed, each neighbor will have to show their agreement with the final wording.

The system must provide, through the use of cryptography, the following security properties:

i. Residents must be sure that the first draft of the text has been prepared by the Administrator.
ii. The Administrator must be sure that each modification proposal that comes to him comes from a neighbor of the community.
iii. A neighbor who decides to propose a modification must be sure that only the Administrator will have access to the content of his message.
iv. When the City Council receives the final text, it must be able to validate, conclusively, the identity of the residents who support it.

Section 1 (80%)

Detail the content of the messages exchanged between the different actors in the system as well as the cryptographic operations necessary to carry out the following operations:

1. Generation and sending, by the Administrator, of the DRAFT document.
2. Reception and reading, by a neighbor, of the DRAFT document.
3. Generation and sending, by a neighbor, of an AMENDMENT message.
4. Receipt and reading, by the Administrator, of an AMENDMENT message.
5. Compilation, by the Administrator, of the approval of each neighbor on the FINAL text.
6. Reception by the City Council of the FINAL text and validation of the sample of conformity of each neighbor.

Yours must detail who is required to have a duly certified public key. If you find it necessary to use shared key cryptography, you must indicate how the two participants in a communication decide which key to use to communicate. solution

Answer

To solve this problem, we need to use cryptography to ensure that the messages exchanged between the Administrator and the neighbors are secure and trustworthy. Let's break down each step:

1) Generation and Sending of the DRAFT Document by the Administrator

- **Content of the Message:** The DRAFT document.
- **Cryptographic Operations:**
  - The Administrator signs the DRAFT document with their private key to ensure authenticity. This means that when the neighbors receive it, they can verify it was indeed sent by the Administrator.
  - The signed document is then encrypted with each neighbor's public key to ensure confidentiality, meaning only the intended neighbor can read it.

> **i** Note
>
> **Who needs a certified public key?** The Administrator and each neighbor need a certified public key to verify signatures and encrypt messages.

2) Reception and Reading of the DRAFT Document by a Neighbor

- **Content of the Message:** The encrypted and signed DRAFT document.
- **Cryptographic Operations:**
  - The neighbor decrypts the document using their private key to read it.
  - They verify the Administrator's signature using the Administrator's public key to ensure it was not tampered with and was indeed sent by the Administrator.

3) Generation and Sending of an AMENDMENT Message by a Neighbor

- **Content of the Message:** The AMENDMENT proposal.
- **Cryptographic Operations:**
  - The neighbor signs the AMENDMENT with their private key to prove they sent it.
  - The signed message is encrypted with the Administrator's public key to ensure only the Administrator can read it.

> **i** Note
>
> **Who needs a certified public key?** The neighbor needs a certified public key to sign the message, and the Administrator needs one to decrypt it.

4) Receipt and Reading of the AMENDMENT Message by the Administrator

- **Content of the Message:** The encrypted and signed AMENDMENT.
- **Cryptographic Operations:**
  - The Administrator decrypts the message using their private key.
  - They verify the neighbor's signature using the neighbor's public key to ensure it was sent by the neighbor and not altered.

5) Compilation of the Approval of Each Neighbor on the FINAL Text by the Administrator

- **Content of the Message:** The FINAL text and each neighbor's approval.
- **Cryptographic Operations:**
  - Each neighbor signs the FINAL text with their private key to show their agreement.
  - The Administrator collects all signed approvals.

6) Reception by the City Council of the FINAL Text and Validation of the Sample of Conformity of Each Neighbor

- **Content of the Message:** The FINAL text and the signed approvals from each neighbor.
- **Cryptographic Operations:**
  - The City Council verifies each neighbor's signature using their public keys to ensure the approvals are genuine and from the correct individuals.

> Note
>
> **Who needs a certified public key?** The City Council needs the certified public keys of all neighbors to verify their signatures.

Section 2 (20%)

Explain, in detail, how the cryptographic operations used guarantee compliance with each of the security requirements (i)-(iv).

> Indications for drafting the solution in Section 1
>
> For reasons of computational efficiency, all public-key encryption operations must be carried out using a digital envelope and all signatures must use a hash function. It is recommended to use the following notation:
>
> - AESK(M): Encrypt the message M using the AES symmetric key cryptosystem using the K key.
> - AES-1K(M): Decrypt the M message using the AES symmetric key cryptosystem using the K key.
> - H(M): Hash value of the message M.
> - RSAPriv(M): Apply the RSA public key cryptosystem to message M using the Priv private key.
> - RSAPub(M): Apply the RSA public key cryptosystem to message M using the Pub public key. Remember that before using a public key, its validity must be verified using the corresponding digital certificate. The system is intended to be as simple as possible. In this sense, the use of cryptographic operations that do not serve to guarantee any of the requirements of the statement will be assessed negatively.

Answer

Security Requirements

(i) **Confidentiality:** Only the intended recipient should be able to read the message.

- **Operation:** Use a digital envelope.
  - Generate a symmetric key (K).
  - Encrypt the message (M) using (AES_K(M)).
  - Encrypt the symmetric key (K) with the recipient's public key (RSAPub(K)).
- **Guarantee:** Only the recipient can decrypt (RSAPub(K)) using their private key to obtain (K) and then decrypt (AES_K(M)).

(ii) **Integrity:** The message should not be altered during transmission.

- **Operation:** Use a hash function.
  - Compute the hash (H(M)) of the message.
  - Include the hash with the message.
- **Guarantee:** The recipient can compute the hash of the received message and compare it with the transmitted hash to ensure the message has not been altered.

(iii) **Authentication:** The sender of the message should be verifiable.

- **Operation:** Use a digital signature.
  - Compute the hash (H(M)).
  - Sign the hash with the sender's private key (RSAPriv(H(M))).
- **Guarantee:** The recipient can verify the signature using the sender's public key, ensuring the message was sent by the legitimate sender.

(iv) **Non-repudiation:** The sender cannot deny having sent the message.

- **Operation:** Use a digital signature.
  - The signed hash (RSAPriv(H(M))) serves as proof of the sender's identity.
- **Guarantee:** The signature can be verified by anyone using the sender's public key, providing undeniable proof of the sender's involvement.