Security Overview

José Pedro Almeida Duarte (64194)
Security (47232)
Department of Electronics, Telecommunications and Informatics
University of Aveiro

Security Messaging Repository System

8th November 2017

OVERVIEW

“The objective of this project is to develop a system enabling users to exchange messages asynchronously. Messages are sent and received through a non-trustworthy central repository, which keeps messages for users until they fetch them. The resulting system is composed by a Rendezvous Point, or Server, and several clients exchanging messages.”

GOALS

1. Architecture
2. Specifications

ARCHITECTURE

1. **Server**

   Rendezvous point for all clients to connect
2. **Multiple Clients**

   Used for users to interact
3. **PKI**

   Public Key Infrastructure to define certification hierarchies, emit and distribute public key certificates and distribute revoking certificates

SPECIFICATIONS

1. Setup a session key between a client and the server prior to exchange any command/response

To setup a session key between a client and the server, a symmetric key will be generated in order to be possible for them to exchange commands and/or responses securely. This key will be valid only for that session and will be discarded when it ends.
To securely distribute the symmetric key, the Diffie-Hellman algorithm will be used.

2. Authentication and integrity control of all messages exchanged between client and server

To ensure authentication and integrity control of all messages, the “Encryption + Authentication” is used, more specifically the MAC-then-Encrypt because it’s considered to be the most secure and provides integrity for both ciphertext and plaintext.

3. Add to each server reply a genuineness warrant

To prove that the reply is the correct one for the client’s request, each command and/or reply will be authenticated using a MAC (Message Authentication Code). This MAC is produced given the symmetric key (session key) and the message.

Specify which or how to MAC
(isn’t this already done on 2. ?)
(or cipher with the symmetric key corresponding to the session key what makes sure that both request or reply can only be perceived by the intended parts ??)

4. Register relevant security-related data in a user creation process

During the user creation process, the “secdata” field will be filled with the both public key value and Diffie-Hellman value and both private asymmetric key and Diffie-Hellman value. All keys will be authenticated using the private key of the user’s Citizen Card.

5. Involve the Citizen Card in the user creation process

When an user is the user is created, his keys will be also created and authenticated using his Citizen Card.

(TODO - more specific)

6. Encrypt messages delivered to other users

To encrypt messages delivered to other users, a hybrid cryptosystem will be used in order to use the efficiency of symmetric keys allied to the convenience of asymmetric keys. The message will be then encrypted with a combined symmetric key and, therefore, this symmetric key will be signed by the (asymmetric) public key of the recipient which can access it with his private key. It is needed that the sender is able to prove the authenticity of the public key of the recipient.

(TODO - explain public key certificates)

7. Signature of the messages delivered to other users and validation of those signatures

To sign the messages delivered to other users, will be used digital signatures. These signatures will be accomplished using the private key of the sender to cipher the message. This private key is obtained from the Citizen card.
To validate the signature, the recipient can use the public key of the sender, the one

corresponding to the same pair of asymmetric keys which the secret key used to cipher the message is part of.

8. Encrypt messages saved in the receipt box

An user will encrypt all his messages in the receipt box by using his own public key what makes him the only one who can decrypt it (using the corresponding private key).

9. Send a secure receipt after reading a message

TODO

10. Check receipts of sent messages

TODO

11. Proper checking of public key certificates from Citizen Cards

TODO - Cadeias de certificados e stuff ?

12. Prevent a user from reading messages from other than their own message box

TODO

13. Prevent a user from sending a receipt for a message that they had not read

TODO