Jonathon Everatt, Piero Puccini, Lynn Weyn, Chelsea Van Coller

EVRJON003,PCCPIE001,WYNLYN004,VNCCHE001

Abstract

A PGP cryptosystem that combines shared key encryption, public-key encryption and certificates to send image files and captions between two clients.

Network and Internetwork security

Practical Assignment

Contents

[Communications Implementation 2](#_Toc74776995)

[Documentation on communication process 2](#_Toc74776996)

[Keys Exchange process 2](#_Toc74776997)

[Security Implementation 2](#_Toc74776998)

[Message Integrity 2](#_Toc74776999)

[Message Authentication 2](#_Toc74777000)

[Message Confidentiality 2](#_Toc74777001)

[System Design and Functionality 2](#_Toc74777002)

[Compression 2](#_Toc74777003)

[Shared Key Usage 2](#_Toc74777004)

[Ordering of System 2](#_Toc74777005)

[Testing Procedure 2](#_Toc74777006)

# Communications Implementation

## Documentation on communication process

## Keys Exchange process

We used a key distribution centre (KDC) for authentication and key exchange. Both Alice and Bob have a master key that they share with the KDC that is used for authentication. First a request is sent for communication. That request is replied to with a nonce encrypted with the master kay shared with the KDC.

*For the key exchange process we used a Key Distribution Center (KDC) to set up and authenticate a session key between the two clients: Bob and Alice.*

# Security Implementation

## Message Integrity

Message integrity is maintained during the communication process using hash functions. The message or block that is being sent is hashed and that hash is concatenated to the sent block and is encrypted with the recipients public key. The recipient will then decrypt the hash with their private key and calculate their own hash of the (decrypted) message and if those two hashes match then the message integrity has been maintained. This also means that if the message is intercepted, the recipient would know if it’s changed due to the changes hash.

*We sent an encrypted hash of the message contents using the other clients public key to prove message integrity.*

## Message Authentication

We initially authenticated the communication session between Alice and Bob using a KDC. At the end of this authentication process a session key was set up between the two which was used for encryption of their communication data.  
*Carry on with how the session key evolved and if security functions has any authentication in it*

*We authenticated the communication session at the beginning with the kdc and then every X messages(?).P*

## Message Confidentiality

*We used this encryption on our messages to keep them confidential and we used this because of the good reasons that will be listed.*

# System Design and Functionality

## Compression

*Lynn and Chelsea talk about the compression.*

## Shared Key Usage

*Jonno, Lynn and Chelsea talk about setting up and continued usage of the shared key(s) during the system including the master shared keys with the kdc(?).*

## Ordering of System

*How does the system run, how do we execute the events. Once the system is integrated the person who integrates it needs to make the structure and everyone else can fill in the blanks*

# Testing Procedure