University of Pisa

MSc in Computer Engineering

SNCS Project

Author:
La Marra Antonio
439833

Indice

1 Application **3**

1.1 Detailed description 3

1.2 List of commands 4

1.2.1 Client 4

1.2.2 Server 4

2 Steganography **5**

3 Protocol **6**

3.1 Objectives 6

3.2 Real Protocol 6

3.3 Assumption 6

3.4 Idealized Protocol 7

3.5 Demonstration 7

3.5.1 After M2 7

3.5.2 After M3 7

1 Application

The application I had in mind is for example the communication between a person (the boss { namely the server }) and a group of people (employees { namely the clients }) that work in different cities, they share a secret (password) and they don't want that their communication is detected by a competitor, that's why further of cryptography I provide also steganography, so that, when needed, they can exchange a simple image to hide their effective communication.

Steganography Example

Let's think for example of a contest in which both the companies are involved, with steganography what the adversary sees are simple images concerning for example vacations, so he thinks that the other company is unprepared for the contest, while in the same case if he sees encrypted messages, then he may think that the other company is working harder and harder to win the competition.

1.1 Detailed description

The boss has a certain number of files and when a client asks for a file the boss sends it. It's the boss that starts the protocol and the client states the key. In my application there are some simulated part or assumptions such as:

- Login, I don't provide a secure way to do a login from one party to the other
- Steganography, instead of exchanging a message to state steganography, each part autonomously set the steganography mode, I assumed that they do that almost synchronously, for example calling each other on the phone
- hash: each message or command has been hashed, I assumed that this is a kind of *digitally signed* hash message

1.2 List of commands

1.2.1 Client

The list of available commands are:

- 'f' to request a file
- 's' to set steganography mode
- 'q' to exit the communication
- 'l' to do the login (it MUST be the first step)
- 'c' a non-command message has to be sent to the server

1.2.2 Server

The list of available commands are:

- 'p' starts the protocol
- 'q' quit
- 's' set the steganography mode
- 'k' change the couple public and private key

2 Steganography

The steganography is a technique that allows us to hide a message into an image, of every kind of format, of course to be efffective this technique has to be used on the RAW image, so before doing the compression.

One of the simplest adopted techniques in the literature involves the changing of at most the 3 least significant bits for every bytes that represents the color of a pixel. In some experiments they proved that if we use only the least significant bit, the message is practically undetectable because the human eye isn't so sensitive. Of course things change a little after the compression algorithm, because in this case they try to reduce the amount of informations carried by the image and they use the strong correlation that there is between adjacent pixels, and this correlation reduces of course if we change the values of some pixel. Other techniques exploit the trasformations that need to be done in the compression phase, but in this way the image appears a little more changed. Steganography may be used both with or without cryptography, so it's a kind of an external mechanism that allows the parties to communicate in an undetected way.

Steganography is easily detected by applying lossy compresion algorithms.

3 Protocol

3.1 Objectives

$$S \mid\equiv C \overset{K_{cs}}{\longleftrightarrow} S \tag{3.1}$$

$$S \mid\equiv C \mid\equiv (C \overset{K_{cs}}{\longleftrightarrow} S) \tag{3.2}$$

$$C \mid\equiv S \mid\equiv (C \overset{K_{cs}}{\longleftrightarrow} S) \tag{3.3}$$

3.2 Real Protocol

$$M1 : S \to C : N_s \tag{3.4}$$

$$M2 : C \to S : \{N_s, N_c, C \overset{K_{cs}}{\longleftrightarrow} S, h(Q)\}_{K_s} \tag{3.5}$$

$$M3 : S \to S : \{N_c - 1\}_{K_{cs}} \tag{3.6}$$

3.3 Assumption

$\overset{K_s}{\mapsto} S$
$C \overset{Q}{\rightleftharpoons} S$
$C \Rightarrow (C \overset{K_{cs}}{\longleftrightarrow} S)$
$C \mid\equiv (C \overset{K_{cs}}{\longleftrightarrow} S)$
$C \mid\equiv \#(N_c)$
$S \mid\equiv \#(N_s)$

3.4 Idealized Protocol

$$M1 : S \rightarrow C : N_s \tag{3.7}$$

$$M2 : C \rightarrow S : \{N_s, N_c, C \overset{K_{cs}}{\longleftrightarrow} S, C \overset{Q}{\rightleftharpoons} S\}_{K_s} \tag{3.8}$$

$$M3 : S \rightarrow C : \{N_c - 1, C \overset{K_{cs}}{\longleftrightarrow} S\}_{K_{cs}} \tag{3.9}$$

3.5 Demonstration

3.5.1 After M2

$$\frac{S \mid\equiv S \overset{Q}{\rightleftharpoons} C, S \triangleleft \langle S \overset{K_{cs}}{\longleftrightarrow} C \rangle_Q}{S \mid\equiv C \mid\sim S \overset{K_{cs}}{\longleftrightarrow} C} \tag{3.10}$$

$$\frac{S \mid\equiv \#(N_s), S \mid\equiv (C \mid\sim S \overset{K_{cs}}{\longleftrightarrow} C)}{S \mid\equiv C \mid\equiv (C \overset{K_{cs}}{\longleftrightarrow} S)} \tag{3.11}$$

One objective reached

$$\frac{S \mid\equiv (C \Rightarrow C \overset{K_{cs}}{\longleftrightarrow} S), S \mid\equiv C \mid\equiv (C \overset{K_{cs}}{\longleftrightarrow} S)}{S \mid\equiv (C \overset{K_{cs}}{\longleftrightarrow} S)} \tag{3.12}$$

Another objective reached

3.5.2 After M3

$$\frac{C \mid\equiv (C \overset{K_{cs}}{\longleftrightarrow} S), C \triangleleft \{N_c, C \overset{K_{cs}}{\longleftrightarrow} S\}}{C \mid\equiv S \mid\sim (N_c, C \overset{K_{cs}}{\longleftrightarrow} S)} \tag{3.13}$$

$$\frac{C \mid\equiv \#(N_c), C \mid\equiv S \mid\sim (N_c, C \overset{K_{cs}}{\longleftrightarrow} S)}{C \mid\equiv S \mid\equiv (C \overset{K_{cs}}{\longleftrightarrow} S)} \tag{3.14}$$

All objects reached