

Network and Computer Security

1º Semester – Academic Year 2013/2014

Hirak Jyoti Kashyap, 79314 - [hirak.kashyap@ist.utl.pt](mailto:hirak.kashyap@ist.utl.pt)   
Kuganesan Srijeyanthan, 79531 - [kuganesan.srijeyanthan@ist.utl.pt](mailto:kuganesan.srijeyanthan@ist.utl.pt)   
Gayana Ranganatha Chandrasekara Pilana Withanage, 79529 - [gayana.withanage@ist.utl.pt](mailto:gayana.withanage@ist.utl.pt)  
Group 7 - Alameda

IDEA 22: **Automatic decryption directory on phone presence**

# Introduction

This report is presented in order to provide a detailed description with practical implementation results, of the project we selected to deliver for this course which is Automatic Directory Decryption on Phone Presence. We will name our application as “BT-CRYPT” for further reference in this report. Section 1 of this report will detail the components of the system and its interoperation while Section 2 will describe the Security features and justification. Possible vulnerabilities of the system will be discussed in Section 3 and Section 4 will be the appendix which will give detailed diagrams of the protocol implementation and overview of the source with user guide.

# Section 1: Components

The system consists of two components, one is an Android application which can be considered as the client and the other is a PC application which will work as the server.

Android Application (Client)

This component provide the user to search the available devices those have already been paired with the mobile phone and will to select the appropriate server device in order to establish a socket connection with the server. Moreover this provides an interface to connect to the server providing the username and the password. Once the user connected there will be a time to time communication with the server in order to keep and refresh the state of the live connection.

PC application (Server)

This component will be started and waiting for a client request to establish a socket connection and proceed. Once a client request is arrived server will create a new socket connection and start following the protocol steps in order to establish a valid connection with the client. This component also provides an interface for user registration, so user should pre-register in the server component before user the client to connect. This registration will ask the user to give a Username, Password and a Folder location to secure the files.

Component inter operation

This is the step by step message exchange between the client and the server in order to establish a proper secure connection so that the decryption of the selected folder can be proceeded by the server.

Pre Requisites

1. Server component has been started in the PC.
2. User has already registered in the server component.
3. User installed the Android application in his smart phone.
4. Mobile phone and PC is properly paired via bluetooth. (This is operating system level pairing.)
5. Client application has paired with the

Protocol

1. User provides his/her username and password in the client interface and press connect button.
2. Client will keep the hash value of the password in the application memory and send the username to the server.
3. Server check the system with username sent and if it exists, will generate a new message with a session key and a random number (Nonce), this message will be encrypted with the password hash of the user and send back to the client. If username does not exists server terminates the socket connection with the client.
4. Client will decrypt the message and keep the session key in memory. Then client increments the random value received and send to the server encrypted by the session key.
5. Server decrypt the message and validate whether the replied random number is what server expected and send a message encrypted with session key which confirm the authentication.
6. Server now decrypt all the encrypted files in the relevant folder with using password hash as the key and every 5 seconds sends a random number encrypted with session key to the client and check client properly reply.
7. If challenge was not reply within 5 seconds the relevant folder will be encrypted again and the socket connection will be closed.

# Section 2: Security overview

Authentication

First 5 steps mention in the previous protocol is used to properly authenticate the client. The authentication will be done based on the password user keeps. During the authentication process we do not send the password itself or any encrypted version of the password via the bluetooth channel and therefore password can be considered as a secure key encryption key shared between the server and the client. This will avoid User Impersonation attacks against the system.

This authentication has included the challenge response mechanism which ensure the freshness of the messages communicated between client and the server. Therefore this will eliminate the replay attacks to the system.

Encryption of the system

The messages including the session key those are passed between the server and the client will be encrypted using Advanced Encryption Standard (AES) cryptographic algorithm with block size 128 bits and key with 256 bits. This will ensure that the communicated messages are secure during the transmission.

The file encryption also uses AES cryptographic algorithm with same block size and key size as above, in Cipher Block Chaining (CBC) mode. The key generation was done with adding SALT to the password hash which will harden the identification of the encryption key even both encryption and decryption data available.

# Section 3: Vulnerability overview

# Section 4: Appendix