Cybersecurity Project

Università di Pisa

Antonio Le Caldare, Vincenzo Consales

year 2017/2018

Contents

Chapter 1

Description of the protocol

1.1 Introduction

The protocol developed in this project has been designed to garantee secrecy, integrity and authentication. It is used by a simple client-server application wich allows clients to download files stored inside the server.
The overall protocol is based on public encrypt. Infact we suppose that the client already has the public key of the server stored on its filesystem. The public encryption scheme allows to authenticate the server. It also allows to exchange a secret master key wich is used by symmetric ciphers to encrpyt the following communications. It is also used an HMAC to garantee integrity and nonces to garantee freshness of communications.

1.2 Description