INSTITUTO SUPERIOR TÉCNICO

HIGHLY DEPENDABLE SYSTEMS

SISTEMAS DE ELEVADA CONFIABILIDADE

MEIC

Project 2: Extending the file system to support smart card authentication

Report

Group: 9

2015/2016

Ricardo Filipe Fonseca Silva
Rui Filipe do Rosário Galão Ribeiro
João Daniel Jorge Machado

1 Introduction

For the second stage of this course's project, we were asked to further develop upon the file server, by enabling authentication based on smart cards, using the cryptographic capabilities of the Portuguese citizen ID card *("Cartão de Cidadão")*

In this report, we will go over the new additions made to the FS, as well as the new integrity guarantees they enable.

2 New Features

With the use of the ID card, we are now able to use its authentication signature capabilities to generate signatures that tie the citizen (client), to the corresponding public key block (file) assigned to him. There's no longer a need to generate key pairs, or use the java cryptographic capabilities to sign the blocks (although they are still used for the purpose of signature validation).

In addition to this, the FS also now functions as a basic Key Server, by storing the public key certificates of the users when they first connect to the server. Users can also query the server for a list of all the public keys of all the clients, making it easy to see which files are available for reading (since file reading is now also tried to a client's Public Key, instead of being tied to the file's identification).

3 New Integrity Guarantees

One of the Integrity improvements stage 2 brings, is the thwarting of integrity breaches related to replay attacks, by making use of time-stamps, to guarantee that no unauthorized requests are sent to the server, by replaying a previously sent, legal request.

In this stage, we are also validating the digital certificates in the citizen ID card, by comparing them to the certificates issued by the ID card's certification entity (which are stored in the server), to guarantee the authenticity of a client of the FS. This verification prevents an attacker from impersonating a legitimate user, by using expired certificates, and signing/sending fake requests in that client's name.