Highly Dependable Systems

Sistemas de Elevada Confiabilidade

Project 2: Extending the file system to support smartcard authentication

Goals

The goal of this stage of the project is to extend your implementation of the previous stage with smartcard-based authentication. To this end, we will be making use of the cryptographic capabilities of the Portuguese national ID card ("cartão de cidadão").

In particular, your file system interface and semantics will be modified in two main ways:

1. Instead of using the key pair generated by the application to sign public key blocks, these will be signed by the smart card (using an "authentication signature", and never with a "qualified digital signature" – see warning below).
2. Instead of clients sharing their public keys using an out of band mechanism, the block server will also become a key server, the FS_init call will register the public key certificate associated with the card in the block/key server, and a new FS_list call will enable clients to look up the existing public keys. To make the file system interface more coherent, FS_read will also be modified to pass a public key as an argument to identify the file. More precisely:

- FS_list( ) → returns list of <public_key>
  Specification: retrieves the list of all public key certificates of the clients that have previously registered in the system.
- FS_init( ) → returns void
  Specification: Initializes all file system structures, and registers with the key server the public key certificate of the client (present in its smartcard).
- FS_read(public_key pk, int pos, int nbytes) → returns contents
  Specification: Same as in stage 1 of the project, except that the file is identified by a public key.

Design and implementation requirements

To add the above mentioned functionality, you need to modify the way in which signatures for public key blocks are generated, to invoke the authentication signature capability of the ID card.
Warning: you must be careful to always use the authentication signature ("autenticação") and never use the qualified digital signature ("assinatura digital qualificada"), because the latter has a legal equivalence to a manual signature.

To be prudent, we advise you not to use your own id card in case you have activated the “assinatura digital qualificada”.

The second functionality will require you to add two new RPCs between the client and the block/key server. The first RPC (called storePubKey) passes a digital certificate as an argument and stores it in the key server, returning only an acknowledgement. The second RPC (called readPubKeys) has no arguments and returns a list of public keys present in the server.

Continuing to work after incomplete submissions for stage 1

The evaluation for stage 2 will focus only on the features requested in this stage, and not on any aspects of stage 1. Therefore, in case your stage 1 submission was not fully functional, you must add the bare minimum fixes so that it implements the requested functionality, even if it does not work perfectly in terms of performance or dependability.

Submission

Submission will be done through Fénix. The submission shall include:

- a self-contained zip archive containing the source code of the project and any additional libraries required for its compilation and execution. The archive shall also include a set of tests for the new functionality, and dependability tests showing how the system tolerates or breaks under specific types of faults or attacks. (Please include a README file explaining how to run the tests).
- a concise reports of up to 3,000 characters addressing:
  - explanation of the new features;
  - explanation of the new integrity guarantees that are provided.

The deadline is April 1, at 17:00. More instructions on the submission will be posted in the course page.