Dissertação de Mestrado em Engenharia Informática (2017/2018)

Title : Study of the quality of cryptographic key material.

Supervisor: Prof. Paul Crocker Email: crocker@di.ubi.pt

Co-Supervisor : Prof. Dr. Simão Melo de Sousa

Description

The main aim of the thesis is to study the quality of the cryptographic key material contained in the Portuguese Electronic Identify (E-ID) card, or Cartão de Cidadão (CC), in particular the key material for digital signatures. Although there is no known general attack on the RSA signature system It's well known that badly designed systems for generating RSA key material can lead to unsafe situations. Currently newly issued CC cards use RSA key sizes of 2048 bits however many identity cards based on RSA key sizes of 1024 bits are still in use and will still be in use for many years to come, this dissertation will study these older cards.

In this project a review of attacks on the RSA system will be undertaken, such the use of low public or private exponents but excluding hardware attacks such as timing attacks. This will be followed by a systematic implementation of a benchmark for auditing the quality of sampled public signature key.

Work Plan

1 Literature and State of the Art Review concerning e-id cards and rsa attacks
2 Study of the characteristics, algorithms and architectures to be used.
3 Implementation, Testing and Evaluation of the proposed solution
4 Publication of the results
5 Writing of the Dissertation.

References

- Twenty Years of Attacks on the RSA Cryptosystem, D Boneh - 1999
- A graduate course in applied cryptography, D. Boneh and Victor Shoup, online at http://toc.cryptobook.us/