Language Based Security For Cryptographic Software

Ph.D. Thesis Proposal

Manuel Bernardo Barbosa, Manuel Alcino Cunha
DI/CCTC, Universidade do Minho

January 2008

Context

This thesis proposal results from the participation of the Cryptography and Information Security group at CCTC in the FP7 European Project titled *Computer Aided Cryptography Engineering* (CACE). The project duration is three-years and kick-off will take place in February 2008.

The goal of the CACE project is to design, develop and deploy a toolbox that will support the specific domain of cryptographic software engineering. Ordinarily, development of cryptographic software is a huge challenge: security and trust is mission critical and modern applications typically use sophisticated cryptographic techniques. The proposed toolbox will allow non-experts to develop high level cryptographic applications (and business models) using cryptography-aware high level programming languages and tools. The description of such applications in this way will allow automatic analysis and transformation of cryptographic software to detect security critical implementation failures (e.g. software and hardware based side-channel attacks) when realizing low level cryptographic primitives and protocols.

This thesis will be integrated into *WP5 (VERIF): Formal Validation and Varification* which addresses the adaptation of previous results in applying formal methods to the development of secure software to the domain-specific languages and tools developed within the CACE project. In particular, this

thesis will focus on adapting language based security techniques to the CACE toolbox, addressing security policies such as secure information and control flow, access control to security-critical resources, stack and memory access safety, etc.

The project funding includes a 3 year Ph.D. grant to support the student taking on this thesis proposal. The Ph.D. student will also be working in close collaboration with a Post-Doctoral researcher allocated full-time to the project for a period of 2 years.

The project work plan includes visits to partners in the project, to ensure that integration of different components in the CACE toolbox is successful.

Objectives

- To explore the state-of-the-art in Language Based Security technology.
- To identify a subset of the cryptographic software security policies established in the CACE project that can be addressed using Language Based Security techniques.
- Extend CACE language definitions and CACE tools to include support for said Language Based Security techniques.
- Validate the results using concrete examples of cryptographic software implementations.

References

[1] Rushby, J.: Critical system properties: Survey and taxonomy. Reliability Engineering and System Safety **43** (1994) 189–219

[2] Sabelfeld, A., Myers, A.: Language-based information-flow security (2003)

[3] Pavlova, M., Burdy, L., Barthe, G., Huisman, M., Lanet, J.: Enforcing high-level security properties for applets (2004)

[4] Barthe, G., Rezk, T., Warnier, M.: Preventing timing leaks through transactional branching instructions. Electr. Notes Theor. Comput. Sci. **153** (2006) 33–55