

Analysis of white box cryptography

MSc Research Project

Date: November 2, 2007

Introduction

The protection of sensitive information in electronic devices is generally performed with cryptography. This works fine in a black box environment, but fails in a white box environment. For instance, a PC application that uses obfuscation by code encryption with a key incorporated in the software can relatively easy be attacked by code analysis. An attacker familiar with cryptography will detect the algorithm and key applied. The attacker can then decrypt the obfuscated code and break its security.

White box cryptography aims at increasing the security level of cryptography in a white box environment (for example in a DRM context). This obfuscation technique uses the fact that algorithms can be implemented in multiple ways, and that random information can be used throughout the algorithm to hide sensitivity values. Also the key can be mixed with algorithmic elements such as substitution boxes. An application protected with white box cryptography is much more difficult to analyse. The attacker will not find any plaintext keys in the code, and may even have difficulty in recognizing the applied algorithm.

Scope

White box cryptography delivers obfuscated encryption algorithms and keys that are functionally equivalent to the original algorithm with a specific key. Conceptually it may be possible to (automatically) break the white box obfuscation by mapping the obfuscated code upon known algorithms. The research question is to evaluate the conceptual strength of white box cryptography by searching for (automated) analysis methods for de-obfuscation.

Research aspects

The following aspects should be addressed by the research:

- Study of white box cryptography theory and implementations.
- Development of a model for analysis of obfuscated code.
- Design of software prototypes for automated analysis of protected implementations.
- Implementation and test of prototype on an example white box solution.
- Write an article for a scientific conference or magazine.

Conditions

The research will be performed at Riscure in Delft. Riscure provides a monthly allowance and, if necessary, housing costs for the duration of the research. A Riscure security analyst will be available for guidance and support. The project will result in a publication and a prototype. Riscure may pose restrictions to the distribution of this material. Riscure maintains the intellectual property rights over the results.

Students with a strong background in software development and an interest in information security are invited to send their resume and a motivation to:

Amanda van den Berg
Office Manager
Email: vandenber@riscure.com
Phone: +31 152682664
Web: www.riscure.com