Towards Tamper Resistant Code Encryption: Practice and Experience

Jan Cappaert[1], Bart Preneel[1],
Bertrand Anckaert[2], Matias Madou[2], and Koen De Bosschere[2]

[1] Katholieke Universiteit Leuven
Department of Electrical Engineering, ESAT/SCD-COSIC
Kasteelpark Arenberg 10
B-3001 Heverlee, Belgium
{jan.cappaert,bart.preneel}@esat.kuleuven.be
[2] Universiteit Gent
Department of Electronics and Information Systems, ELIS/PARIS
Sint-Pietersnieuwstraat 41
B-9000 Gent, Belgium
{banckaer,mmadou,kdb}@elis.ugent.be

Abstract. In recent years, many have suggested to apply encryption in the domain of software protection against malicious hosts. However, little information seems to be available on the implementation aspects or cost of the different schemes. This paper tries to fill the gap by presenting our experience with several encryption techniques: bulk encryption, an on-demand decryption scheme, and a combination of both techniques. Our scheme offers maximal protection against both static and dynamic code analysis and tampering. We validate our techniques by applying them on several benchmark programs of the CPU2006 Test Suite. And finally, we propose a heuristic which trades off security versus performance, resulting in a decrease of the runtime overhead.

1 Introduction

In the 1980s application security was achieved through secure hardware, such as ATM terminals, or set-top boxes. Since the 1990s, however, secure software has gained much interest due to its low cost and flexibility. Nowadays, we are surrounded by software applications for online banking, communication, e-voting, ... As a result, threats such as piracy, reverse engineering and tampering have emerged. These threats are exacerbated by poorly protected software. Therefore, it is important to have a thorough threat analysis (e.g., STRIDE [10]) as well as software protection schemes. The techniques discussed in this paper protect against reverse engineering and tampering.

The goal of encryption is to hide the content of information. Originally, it was applied within the context of communication, but has become a technique to secure all critical data, either for short-term transmission or long-term storage. More recently, commercial tools for software protection have become available.