Cryptology ePrint Archive: Report 2011/099

Can Code Polymorphism Limit Information Leakage?

Antoine Amarilli and Sascha M\"uller and David Naccache and Daniel Page and Pablo Rauzy and Michael Tunstall

Abstract: In addition to its usual complexity assumptions, cryptography silently assumes that information can be physically protected in a single location. As one can easily imagine, real-life devices are not ideal and information may leak through different physical side-channels. It is a known fact that information leakage is a function of both the executed code F and its input x.\smallskip

In this work we explore the use of polymorphic code as a way of resisting side channel attacks. We present experimental results with procedural and functional languages. In each case we rewrite the protected code code F_i before its execution. The outcome is a genealogy of programs $F_0,F_1,\ldots$ such that for all inputs x and for all indexes $i \neq j \Rightarrow F_i(x) =F_j(x)\mbox{~and~}F_i\neq F_j$. This is shown to increase resistance to side channel attacks.\smallskip

Category / Keywords: cryptographic protocols / side channels, polymorphism

Date: received 28 Feb 2011, last revised 2 Mar 2011

Contact author: david naccache at ens fr