Justification for inclusion in NSPW

"Cryptomorphic Programming: Towards White-box Security"

Willard Thompson and J. Todd McDonald

Category 1: *Research papers should be of a length commensurate with the novelty of the paradigm and the amount of novel material that the reviewer must assimilate in order to evaluate it.*

Our justification for including this research paper in NSPW is not only its novelty but it is also a shift in the direction of program encryption research. Our new proposed paradigm is called the Cryptomorphic Programming Model. This new paradigm is much needed theoretical work for program encryption with the notion of advancing provable security to a new level. The concept of a random program, expressed in the notion of a random oracle model, does not exist before our work. It is important to set the bar for what it means for a program to be tamper resistant and hide proprietary algorithms under the concept of a random program.

There are two main existing areas for encrypting programs, code obfuscation and mobile cryptography. Code obfuscation alters the syntax of a program into a less readable format with the goal of making the program's instructions unintelligible to human and mechanized analysis. Code obfuscation does not change the I/O relationship of the program. Unfortunately, it is difficult to measure the security of code obfuscation, thus it is not provably secure. On the other end of the provably secure spectrum is mobile cryptography. Mobile cryptography aims to secure functions such as polynomials using homomorphism. However, mobile cryptography is extremely limited and not applicable towards programs in general.

Our work departs from these existing notions of program encryption by not only combining the best properties of code obfuscation and mobile cryptography, but by also using primitive data encryption techniques such as permutations and substitutions on program constructs or more precisely memory cells. These cryptographic properties can lead to provable security.