Compilation Integrity Assurance through Deep Code Alignment (Ramot)

code: 4-2016-1012

Lior WOLF, T.A.U Tel Aviv University, Exact Sciences, School of Computer Science

TECHNOLOGY & POTENTIAL APPLICATION

We propose a completely novel approach for detecting hardware Trojans. We obtain, from the foundry or by other means the binaries. These binaries are expected to largely match the programming code provided by the hardware designer with some unavoidable additions inserted in order to support debugging, QA, and to comply with manufacturing constraints. We then identify for every line of the binaries (viewed as assembly code) the matching line in the original C code. Following this step, we can easily identify insertions and other forms of modifications. The engineers of the supplier company or any other verifying agency can then readily track these modifications and tag each one as malicious or not.

THE NEED

Hardware Trojans are both persistent and extremely hard to detect. In this project, we address the problem of executable component addition, substitution, and re-programming in the supply chain.

PATENTS

Patent pending

Contact for more information:

Ofer Shneyour ✉, VP Business Development, ICT, +972.3.640.6496

Ramot at Tel Aviv University Ltd. P.O. Box 39296, Tel Aviv 61392 ISRAEL
Phone: +972-3-6406608
Fax: +972-3-6406675