Research initiative to enhance integrity of integrated circuits

April 27 2011

A consortium of hardware security experts from four major universities around the country has received a $1.2 million federal grant to conduct wide-ranging research aimed at enhancing the integrity of integrated circuits (ICs), the computer chips that are used in virtually all electronic devices today, from cell phones and medical instruments to laptop computers and flat-screen TVs.

The consortium, which is made up of experts from the University of Connecticut, the Polytechnic Institute of New York University, Rice University and the University of California, Los Angeles, has developed a web-based, dynamic exchange network dubbed Trust-Hub, a website where members of the IC hardware security community can share their discoveries and other information that accelerates hardware security research and developments. Trust-Hub serves as a clearing house and community-building tool where researchers can exchange papers, benchmarks, hardware platforms, source codes and tools.

The Trust-Hub consortium aims to establish criteria for determining the "trustworthiness" of integrated circuits. It also hopes to develop trust benchmarks for the hardware security community along with common hardware platforms for the validation of solutions. A central feature of the project is the web-based Trust-Hub repository, which will help to ensure widespread access to the latest tools and knowledge in hardware security and trust.

Trustworthy Computing Program Officer Samuel Weber of the National

Science Foundation, which funded the Trust-Hub project, said “NSF’s Trustworthy Computing and Computing Research Infrastructure Programs are pleased to award this grant. Malicious computer hardware is a difficult and growing problem and one that poses new research challenges. This project promises to build and support a community of researchers to tackle this challenge by providing much needed infrastructure.”

The grant’s principal investigator is Mohammad Tehranipoor, associate professor of electrical and computer engineering at the University of Connecticut. Co-principal investigators include Farinaz Koushanfar, assistant professor of electrical and computer engineering at Rice University; Ramesh Karri, professor of electrical and computer engineering at the Polytechnic Institute of New York University; and Miodrag Potkonjak, professor of computer science at UCLA.

“The objective of the Trust-Hub project is to lead a community-wide movement toward stronger assurances in the hardware industry,” Tehranipoor said. “The Trust-Hub is a means for information-sharing between researchers and practitioners to accelerate the development of defenses against hardware-level attacks.”

The Trust Hub website is a resource for research, education and collaboration among hardware security experts and also includes information about activities such as technical events, workshops, seminars, and news stories in addition to online courses and tutorials.

“We believe the Trust-Hub can provide opportunities to synchronize research activities in this community and help accelerate research and development by providing baselines for examining various methods developed by researchers in academia and industry,” Koushanfar said. “This will help establish a sound basis for the ‘hardness’ of each design instance, and it will result in common platforms that can enable effective

implementation of methodologies. We will make all benchmark circuits, tools and common platforms available to the public."

Another important capability available on the Trust-Hub website is simulation tools that can be accessed from a local web browser, enabling researchers to explore and also simulate a specific science area.

The researchers will develop benchmark circuits – "trust benchmarks" – infected with hardware Trojans with the aim of creating hardware platforms to validate trust. Karri explained that in the last decade, researchers have made important advancements in hardware security and trust. However, the effectiveness of these methods is not universally accepted and some are applicable only to specific designs, platforms and technologies. The lack of universal solutions for IC security is an underlying premise for the Trust-Hub collaboration, whose partners aim to develop effective trust benchmark circuits, tools and hardware.

"This project will greatly impact the research and development in the security community and has the potential of coordinating research among various institutions and government agencies," Potkonjak said. "In addition, it helps facilitate technology transfer to industry since the methodology and implementation becomes repeatable in practice."

More information: trust-hub.org/

Provided by University of Connecticut