A self-healing and self-concealing silicon chip 'fingerprint' for stronger, hardware security

April 15 2020

NUS researchers Prof Massimo Alioto (left) and Mr Sachin Taneja (right) testing the self-healing and self-concealing PUF for hardware security. Credit: National University of Singapore

A team of researchers from the National University of Singapore (NUS)

has developed a novel technique that allows Physically Unclonable Functions (PUFs) to produce more secure, unique 'fingerprint' outputs at a very low cost. This achievement enhances the level of hardware security even in low-end systems on chips.

Traditionally, PUFs are embedded in several commercial chips to uniquely distinguish one silicon chip from another by generating a secret key, similar to an individual fingerprint. Such a technology prevents hardware piracy, chip counterfeiting and physical attacks.

The research team from the Department of Electrical and Computer Engineering at the NUS Faculty of Engineering has taken silicon chip fingerprinting to the next level with two significant improvements: firstly, making PUFs self-healing; and secondly, enabling them to self-conceal.

Self-healing PUFs

In spite of their remarkable evolution in the last decade, existing PUFs still suffer from limited stability and periodically incorrect fingerprint identification. Often designed as stand-alone circuits, they provide hackers with obvious points of physical attacks on the chip.

The instability is conventionally counteracted through overdesign, such as designing error-correcting codes margined for the very worst case, which substantially increases both chip cost and consumption. In addition, before proceeding to commercialization, chips with unstable PUFs must first be identified and discarded through extensive testing on a very wide set of environmental conditions, further increasing cost.

To address the gaps, the team of NUS engineers introduced a novel adaptation technique that uses on-chip sensors and machine learning algorithms to predict and detect PUF instability. This technique

intelligently adjusts the tuneable level of correction to the minimum necessary, and produces a more secure, stable PUF output. In turn, the novel approach brings consumption back to the minimum possible, and is able to detect anomalous environmental conditions such as temperature, voltage or noise that are routinely exploited by hackers in physical attacks.

An added benefit is that the traditional testing burden and cost are dramatically reduced by narrowing down the test cases required. This eliminates overdesign and unnecessary design costs, as most of the testing effort can be delegated to the available on-chip sensing and intelligence throughout the device's lifetime.

"Our approach utilizes on-chip sensing and machine learning to enable accurate prediction, detection and adaptive suppression of PUF instability events. The ability to self-heal without stability degradation over the entire chip's lifetime assures reliable generation of secret keys at the highest level of security, while avoiding the burden of designing and testing for the very worst case, even if the latter is actually infrequent and unlikely. This reduces the overall cost, shortens the time to market, and cuts down on system power to extend the battery lifetime," shared Professor Massimo Alioto, who leads the Green IC Group that is behind this breakthrough in hardware security.

The reduction in the cost of chip design and testing is key in enhancing hardware security even in very low-cost and low-power silicon systems, such as sensor nodes for the Internet of Things (IoT), wearable devices and implantable biomedical systems.

Prof Alioto elaborated, "On-chip sensing, as well as machine learning and adaptation, allow us to raise the bar in chip security at significantly lower cost. As a result, PUFs can be deployed in every silicon system on earth, democratizing hardware security even under tight cost

constraints."

Creation of self-concealing PUFs using innovative immersed-in-logic design

The PUFs invented by the researchers also exhibit a first-of-its-kind ability to be fully immersed and hidden within the digital logic that they actually protect. This is enabled by the mostly-digital nature of the PUF architecture, which allows the placement, routing and integration of digital standard cells, similar to conventional digital circuits. This reduces the design cost as conventional digital automated design methodologies supported by commercial software design tools can be applied to design the PUF.

In addition, the PUF digital design allows the generation of secret keys to be interspersed within the very logic that uses such keys, such as cryptographic units protecting data and the microprocessors handling the data to be encrypted. The immersed-in-logic approach scatters the PUF standard cells among the cells used for the digital logic, thereby "hiding" or concealing any explicit points of attack for hackers trying to probe specific chip signals to physically reconstruct the keys.

This self-concealing ability increases the attack effort by approximately 100 times. It also raises the cost of attacking typical chips to millions of dollars with state-of-the-art tools, as opposed to tens of thousands in conventional stand-alone PUFs.

The innovation has been supported by leading semiconductor companies (such as TSMC), the Ministry of Education, and the National Research Foundation in Singapore through the national-level "SOCure" research program.

Next steps

The NUS research team will continue to look into the convergence of computer architecture, physical security and machine learning to develop next-generation secure systems on chips. This technological innovation is driven by the growing need for privacy and information security, in view of the increasingly pervasive adoption of systems on chips that sense and process personal and sensitive information.

The team is also pursuing ubiquitous and ultra-low-cost enablement of hardware security through tight physical co-integration of architectures and security primitives with circuitry that is generally available in any system on a chip, ranging from logic, memory, intra-chip data communication and accelerators. Ultimately, the team's newest breakthrough is expected to enable hardware security at the granularity of every silicon chip, even within individual sub-systems on a chip.

Provided by National University of Singapore