UC SANTA BARBARA

THE Current

April 25, 2018
Sonia Fernandez

An Ionic Black Box

While we embrace the way the Internet of Things already is making our lives more streamlined and convenient, the cybersecurity risk posed by millions of wirelessly connected gadgets, devices and appliances remains a huge concern. Even single, targeted attacks can result in major damage; when cybercriminals control and manipulate several nodes in a network, the potential for destruction increases.

UC Santa Barbara electrical and computer engineering professor Dmitri Strukov is working to address the latter. He and his team are looking to put an extra layer of security on the growing number of internet- and Bluetooth-enabled devices with technology that aims to prevent cloning, the practice by which nodes in a network are replicated and then used to launch attacks from within the network. A chip that deploys ionic memristor technology, it is an analog memory hardware solution to a digital problem.

“You can think of it as a black box,” said Strukov, whose new paper, “Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors,” appears on the cover of Nature Electronics. Due to its nature, the chip is physically unclonable and can thus render the device invulnerable to hijacking, counterfeiting or replication by cyber criminals.

Key to this technology is the memristor, or memory resistor — an electrical resistance switch that can “remember” its state of resistance based on its history of applied voltage and current. Not only can memristors can change their outputs in response to their histories, but each memristor, due to the physical structure of its

material, also is unique in its response to applied voltage and current. Therefore, a circuit made of memristors results in a black box of sorts, as Strukov called it, with outputs extremely difficult to predict based on the inputs.

“The idea is that it’s hard to predict, and because it’s hard to predict, it’s hard to reproduce,” Strukov said. The multitude of possible inputs can result in at least as many outputs — the more memristors, the more possibilities. Running each would take more time than an attacker may reasonably have to clone one device, let alone a network of them.

The use of memristors in today’s cybersecurity is especially significant in light of machine learning-enabled hacking, in which artificial intelligence technology is trained to “learn” and model inputs and outputs, then predict the next sequence based on its model. With machine learning, an attacker doesn’t even need to know what exactly is occurring as the computer is trained on a series of inputs and outputs of a system.

“For instance, if you have 2 million outputs and the attacker sees 10,000 or 20,000 of these outputs, he can, based on that, train a model that can copy the system afterwards,” said Hussein Nili, the paper’s lead author. The memristive black box can circumvent this method of attack because it makes the relationship between inputs and outputs look random enough to the outside world even as the circuits’ internal mechanisms are repeatable enough to be reliable.

“It has to look random, but it should also be deterministic,” he said.

In addition to the variability embedded in these memristor circuits, other features include high throughput, speed and economy of energy use, making them an ideal component in the tight energy budget of the Internet of Things. Then there is the fact that this is already a semi-practical technology which can be used to both secure device identity and encrypt information.

“If we scale it a little bit further, it’s going to be hardware which could be, in many metrics, the state-of-the-art,” Strukov said.

As they continue to refine this technology, Strukov and his team are investigating whether there will be any drifts in the characteristics over time. They also are developing “strong” security paths that require larger memristive circuits and additional techniques (suitable for sensitive military equipment or highly classified

information), and “weak” paths geared more toward consumer electronics and everyday gadgets — situations in which it would likely not be worth an attacker’s time to spend hours or days hacking into a device.

Tags
Artificial Intelligence

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.