UC San Diego
UC San Diego News Center

August 12, 2016 | By Tiffany Fox

Nowhere to Hide: UC San Diego Researchers Devise New Method for Detecting Hardware Trojans

San Diego, Calif., Aug. 11, 2016 — Modern computer chips are made up of hundreds of millions – often billions – of transistors. Such complexity enables the smartphone in your back pocket to perform all manner of powerful computations, but it also provides lots of places for tiny malicious circuits, known as hardware Trojans, to hide. Magnifying this security risk is the increasingly distributed and globalized nature of the hardware supply chain, which makes it possible for a Trojan to be introduced at any point along the way.

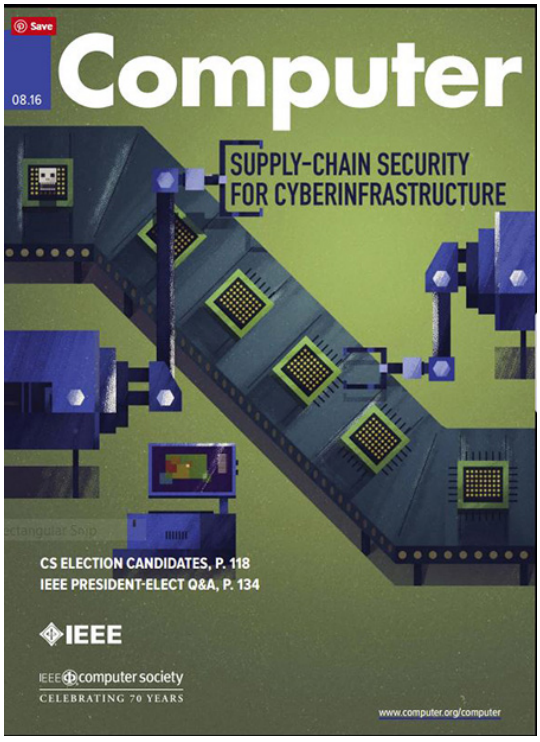
Ryan Kastner

To prevent, detect and combat these hardware Trojans, computer scientists from the University of California San Diego, together with their collaborators, have devised a new technique that tracks information flow through a circuit's logic gates, much the way one would track traffic as it flows through an intersection while obeying a series of traffic signals. If information unexpectedly moves to a part of the chip where it shouldn't be, the method will determine that a security violation occurred, and whether or not a Trojan was the root cause.

The technique is described in a paper titled "Detecting Hardware Trojans with Gate-Level Information-Flow Tracking," which is the cover story in the August 2016 edition of IEEE Computer. The paper's authors are Computer Science and Engineering (CSE) Postdoctorate

Wei Hu of UC San Diego, Computer Science and Technology Ph.D. candidate Baolei Mao of Northwestern Polytechnical University, Tortuga Logic CEO Jason Oberg and CSE Professor Ryan Kastner, also of UC San Diego.

“Trojans are designed specifically to avoid activation during testing,” explains Kastner, who is head of the Kastner Research Group at UC San Diego and an affiliate of the university’s Qualcomm Institute. “Hardware designs are complex and often consist of millions of lines of code. The standard rule is to expect one ‘bug’ per five lines of code. People with bad intentions – say, a disgruntled employee – can insert these special ‘bugs’ into sequence patterns that are very unlikely to be tested, where they lie dormant and wait for a rare input to happen and then they trigger something malicious, like draining your phone’s battery or stealing your cryptographic key,” (i.e. the key that encrypts sensitive information to keep it secure).



August 2016 Cover of IEEE Spectrum

“The concern these days is that chips are designed and manufactured all over the world, and sometimes in countries that might have a reason to steal intellectual property or other information,” Kastner says. This concern is so great in the United States, in fact, that government-sensitive technologies are fabricated in trusted foundries (semiconductor fabrication plants) that require security clearance.

But, notes Kastner, “typically these foundries are not as advanced and not as cheap as those in other countries. Sometimes they’re using technologies that are three- or four-generations old. The hope is that we can continue to send hardware to be manufactured at any foundry, and that this method will make the process more secure.”

The method uses a technique called GLIFT (gate-level information flow tracking), which works by assigning a label to important data in a hardware design. If the goal, for instance, is to understand where information about a cryptographic key is flowing, a “confidential” label would be assigned to bits of the key. The test engineer would then write a formal property that asserts that any confidential information (in this case the key) will be constrained to stay in secure part of the chip. If the key flows outside of that secure area, then the hardware is capable of being compromised.

Kastner says the previous methods for finding Trojans were mostly statistical and tried to pinpoint inconsistencies and variations in measurable properties in the circuit that would indicate a Trojan, such as how much time it should take to complete a function or how much power it should consume. Because these methods are statistical, they are also susceptible to noise. Smaller Trojan circuits, therefore, are easier to hide in large designs. “It’s like trying to find a needle in a haystack,” says Kastner.

“The state of the art right now is teams at Qualcomm or Intel, for example, manually inspecting hardware code and the physical characteristics of the chip to determine what they think could happen,” he adds. “It’s a terribly imprecise process, and you could easily overlook a small error which could have large consequences.”

Tortuga Logic – an offshoot of Kastner and Oberg’s research – offers a set of commercial products (including its “Prospect” software), that leverage the GLIFT technology. These commercial products can be used to implement a security team’s Trojan-detection techniques.Kastner notes that the techniques are automated, proactive and “can be conducted at design time, before a chip is even sent to a foundry.

“If potentially you can detect a Trojan in an earlier stage in the supply chain, it’s more cost-effective,” he adds. “Whereas before you might have a vague idea that something is wrong, with our method you’re able to prove it. Our method can find design flaws – often these are subtle, unintentional design flaws – and tell you that there is an issue even if it isn’t caused by a Trojan. This should give chip makers a lot more confidence when integrating IP created outside of their company, which is commonplace nowadays.”

MEDIA CONTACT

Tiffany Fox, 858-246-0353, tfox@ucsd.edu