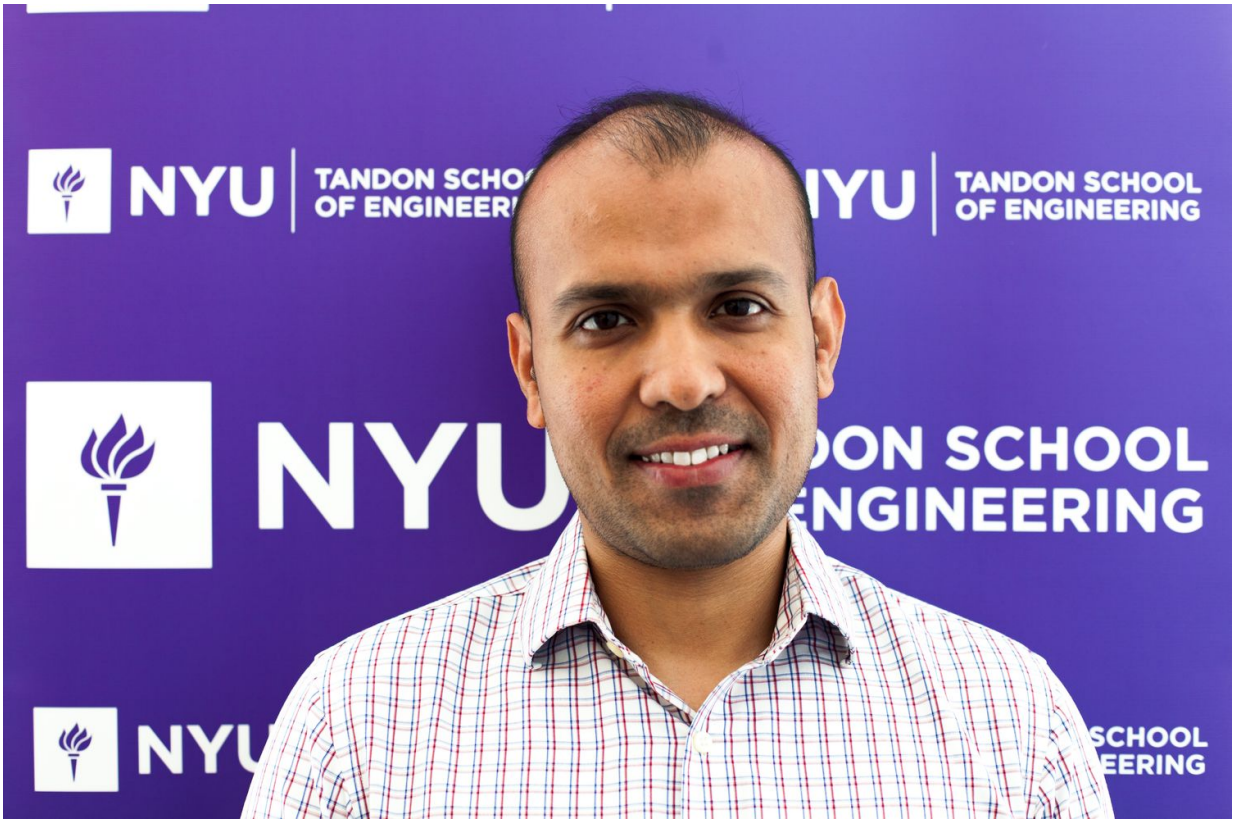
Cybersecurity researchers design a chip that checks for sabotage

August 23 2016



NYU Tandon Assistant Professor Siddharth Garg. Credit: NYU Tandon

With the outsourcing of microchip design and fabrication worldwide, a $350 billion business, bad actors along the supply chain have many opportunities to install malicious circuitry in chips. These "Trojan

horses" look harmless but can allow attackers to sabotage healthcare devices; public infrastructure; and financial, military, or government electronics.

Siddharth Garg, an assistant professor of electrical and computer engineering at the NYU Tandon School of Engineering, and fellow researchers are developing a unique solution: a chip with both an embedded module that proves that its calculations are correct and an external module that validates the first module's proofs.

While software viruses are easy to spot and fix with downloadable patches, deliberately inserted hardware defects are invisible and act surreptitiously. For example, a secretly inserted "back door" function could allow attackers to alter or take over a device or system at a specific time. Garg's configuration, an example of an approach called "verifiable computing" (VC), keeps tabs on a chip's performance and can spot telltale signs of Trojans.

The ability to verify has become vital in an electronics age without trust: Gone are the days when a company could design, prototype, and manufacture its own chips. Manufacturing costs are now so high that designs are sent to offshore foundries, where security cannot always be assured.

But under the system proposed by Garg and his colleagues, the verifying processor can be fabricated separately from the chip. "Employing an external verification unit made by a trusted fabricator means that I can go to an untrusted foundry to produce a chip that has not only the circuitry-performing computations, but also a module that presents proofs of correctness," said Garg.

The chip designer then turns to a trusted foundry to build a separate, less complex module: an ASIC (application-specific integrated circuit),

whose sole job is to validate the proofs of correctness generated by the internal module of the untrusted chip.

Garg said that this arrangement provides a safety net for the chip maker and the end user. "Under the current system, I can get a chip back from a foundry with an embedded Trojan. It might not show up during post-fabrication testing, so I'll send it to the customer," said Garg. "But two years down the line it could begin misbehaving. The nice thing about our solution is that I don't have to trust the chip because every time I give it a new input, it produces the output and the proofs of correctness, and the external module lets me continuously validate those proofs."

An added advantage is that the chip built by the external foundry is smaller, faster, and more power-efficient than the trusted ASIC, sometimes by orders of magnitude. The VC setup can therefore potentially reduce the time, energy, and chip area needed to generate proofs.

"For certain types of computations, it can even outperform the alternative: performing the computation directly on a trusted chip," Garg said.

The researchers next plan to investigate techniques to reduce both the overhead that generating and verifying proofs imposes on a system and the bandwidth required between the prover and verifier chips. "And because with hardware, the proof is always in the pudding, we plan to prototype our ideas with real silicon chips," said Garg.

To pursue the promise of verifiable ASICs, Garg, abhi shelat of the University of Virginia, Rosario Gennaro of the City University of New York, Mariana Raykova of Yale University, and Michael Taylor of the University of California, San Diego, will share a five-year National Science Foundation Large Grant of $3 million.

Verifiable ASICS by Riad S. Wahby of Stanford University, Max Howald of The Cooper Union, Garg, shelat, and Michael Walfish of the NYU Courant Institute of Mathematical Sciences, earned a Distinguished Student Paper Award at the IEEE Symposium on Security and Privacy, one of the leading global conferences for computer security research, held in May in Oakland, California. The authors were supported by grants from the NSF, the Air Force Office of Scientific Research, the Office of Naval Research, a Microsoft Faculty Fellowship, and a Google Faculty Research Award.

Provided by NYU Tandon School of Engineering