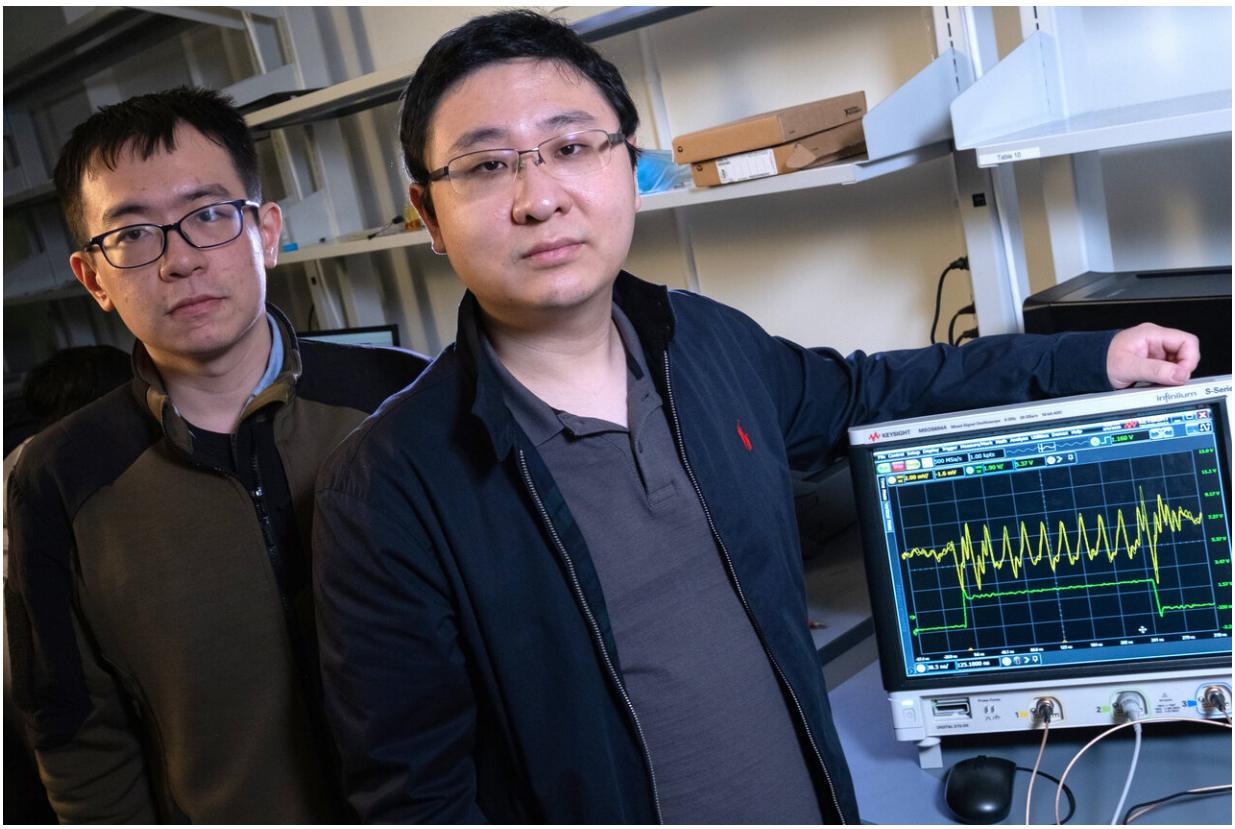
Engineers' custom circuits would make IoT systems 14,000 times harder to crack than current tech

February 19 2020, by Mike Williams



Rice University graduate student Yan He, left, and Kaiyuan Yang, an assistant professor of electrical and computer engineering, will demonstrate their enhanced security strategy for the "internet of things" at the International Solid-State Circuits Conference in San Francisco. Credit: Jeff Fitlow/Rice University

Rice University engineers have one-upped their own technique to increase security for the "internet of things."

In truth, their upping is far greater than one.

Kaiyuan Yang, an assistant professor of electrical and computer engineering at Rice's Brown School of Engineering, and graduate student Yan He have introduced a technique to make security more than 14,000 times better than current state-of-the-art defenses while using far less energy.

The Rice team's technique, introduced with a paper and presentation at the International Solid-State Circuits Conference in San Francisco, is a hardware solution centered in the power management circuitry found in most central processing chips.

The "internet of things" (IoT) allows devices—kitchen appliances, security systems, wearable technologies and many other applications—to communicate with each other through networks. With the world on the verge of adopting them by the billions, the best possible security is paramount, Yang said.

Unfortunately, he said, any IoT device may become vulnerable to thieves, who could use it to gain access to entire households.

"Once they've found a hole, there are so many things they can do," Yang said. "And they don't need to get into a computer system or a cell phone. For instance, a thermostat connected to the network can become an access point to a home, a company, a hospital or a city."

Last year's breakthrough by the lab generated paired security keys based on fingerprintlike defects unique to every computer chip. "This year, the story is similar, but we are not generating keys," Yang said. "We are

looking at defending against a new type of attack that is specifically for IoT and mobile systems.

"In power and electromagnetic side-channel attacks, the attackers can figure out a secret key when your device is running without opening up the device," he said. "Once they have your key they can decrypt everything, no matter how good your security software is.

The new strategy leverages the power regulators to obfuscate the information leaked by the power consumption of encryption circuits, Yang said. "Every system-on-a-chip has multiple modules powered by the power management circuits, so the interfaces we need are already there.

"By replacing existing power management circuitry with our unit, we not only provide a much better way to defend against powerful threats, but also provide a much more energy-efficient solution," he said.

Yang said the circuit should take no more room on a chip than current power management units, and as a side benefit will provide state-of-the-art power regulation. "I think it's going to be a very promising solution thanks to its minimal performance and design overheads," he said.

Yang said encryption-cracking hardware and software leveraging power and electromagnetic side-channel leakage are far too easy to find, "and there are YouTube videos to show you how to do this," he said. "This is a real threat, and we're in a fight to make it much more difficult and expensive for attackers to succeed."

While Rice's protective circuitry is improving with every iteration, he said it will take time for manufacturers to design it into their fabrication processes. "There's all the interface and engineering stuff," Yang said. "In terms of the concepts and principles, they're all proven. It's just

going to be a long engineering effort."

Provided by Rice University

Citation: Engineers' custom circuits would make IoT systems 14,000 times harder to crack than current tech (2020, February 19) retrieved 4 May 2024 from https://techxplore.com/news/2020-02-custom-circuits-iot-harder-current.html