Researchers safeguard hardware from cyberattack

February 28 2019, by Brandon Pytel

University of Cincinnati professor Ranga Vemuri works with students in his Digital Design Environments Laboratory. Vemuri closed a security loophole that makes hardware susceptible to cyberattack. Credit: Corrie Stookey/UC College of Engineering and Applied Science

Researchers have developed an algorithm that safeguards hardware from

attacks to steal data. In the attacks, hackers detect variations of power and electromagnetic radiation in electronic devices' hardware and use that variation to steal encrypted information.

Researchers with the University of Wyoming and the University of Cincinnati recently published their work in the *Institute of Engineering and Technology Journal*.

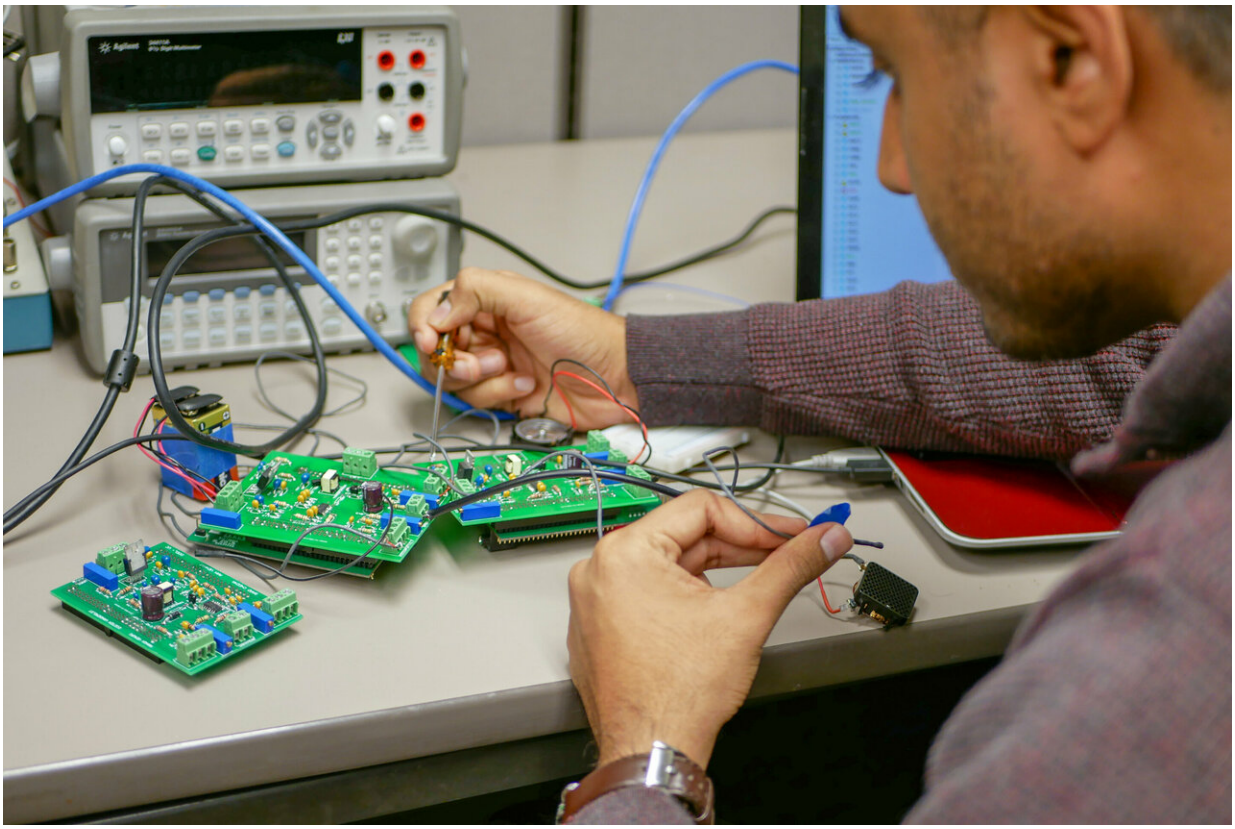
Electronic devices appear more secure than ever before. Devices that used to rely on passwords now use Touch ID, or even face recognition software. Unlocking our phones is like entering a 21st century Batcave, with high-tech security measures guarding the entry.

But protecting software is only one part of electronic security. Hardware is also susceptible to attacks.

"In general, we believe that because we write secure software, we can secure everything," said University of Wyoming assistant professor Mike Borowczak, Ph.D., who graduated from UC. He and his advisor, UC professor Ranga Vemuri, Ph.D., led the project.

"Regardless of how secure you can make your software, if your hardware leaks information, you can basically bypass all those security mechanisms," Borowczak said.

Devices such as remote car keys, cable boxes and even credit card chips are all vulnerable to hardware attacks, typically because of their design. These devices are small and lightweight and operate on minimal power. Engineers optimize designs so the devices can work within these low-power constraints.



A University of Cincinnati student works on hardware in UC's Digital Design Environments Laboratory. Credit: Corrie Stookey/UC College of Engineering and Applied Science

"The problem is if you try to absolutely minimize all the time, you're basically selectively optimizing," Borowczak said. "You're optimizing for speed, power, area and cost, but you're taking a hit on security."

When something like a cable box first turns on, it's decoding and encoding specific manufacturer information tied to its security. This decoding and encoding process draws more power and emits more electromagnetic radiation than when all of the other functions are on. Over time, these variations in power and radiation create a pattern unique to that cable box, and that unique signature is exactly what

hackers are looking for.

"If you could steal information from something like a DVR early on, you could basically use it to reverse engineer and figure out how the decryption was happening," Borowczak said.

Hackers don't need physical access to a device to take this information. Attackers can remotely detect frequencies in car keys and break into a car from more than 100 yards away.

To secure the hardware in these devices, Vemuri and Borowczak went back to square-one: these devices' designs.

Borowczak and Vemuri aim to restructure the design and code devices in a way that doesn't leak any information. To do this, they developed an algorithm that provides more secure hardware.

University of Cincinnati professor Ranga Vemuri closed a security loophole that makes hardware susceptible to cyberattack. Here he works with students in his Digital Design Environments Laboratory at UC. Credit: Corrie Stookey/UC College of Engineering and Applied Science

"You take the design specification and restructure it at an algorithmic level, so that the algorithm, no matter how it is implemented, draws the same amount of power in every cycle," Vemuri said. "We've basically equalized the amount of power consumed across all the cycles, whereby even if attackers have power measurements, they can't do anything with that information."

What's left is a more secure device with a more automated design.

Rather than manually securing each hardware component, the algorithm automates the process. On top of that, a device created using this algorithm only uses about 5 percent more power than an insecure device, making the work commercially viable.

Software and hardware security is an ongoing game of cat and mouse: As security technologies improve, hackers eventually find ways around these barriers. Hardware security is further complicated by the expanding network of devices and their interactivity, also known as the Internet of Things.

Innovative research like the work by Vemuri and Borowczak can give people an extra layer of safety and security in a world of connected devices.

More information: Mike Borowczak et al, Mitigating early-boot information leakage using S*FSM, *IET Computers & Digital Techniques* (2019). DOI: 10.1049/iet-cdt.2018.5186

Provided by University of Cincinnati