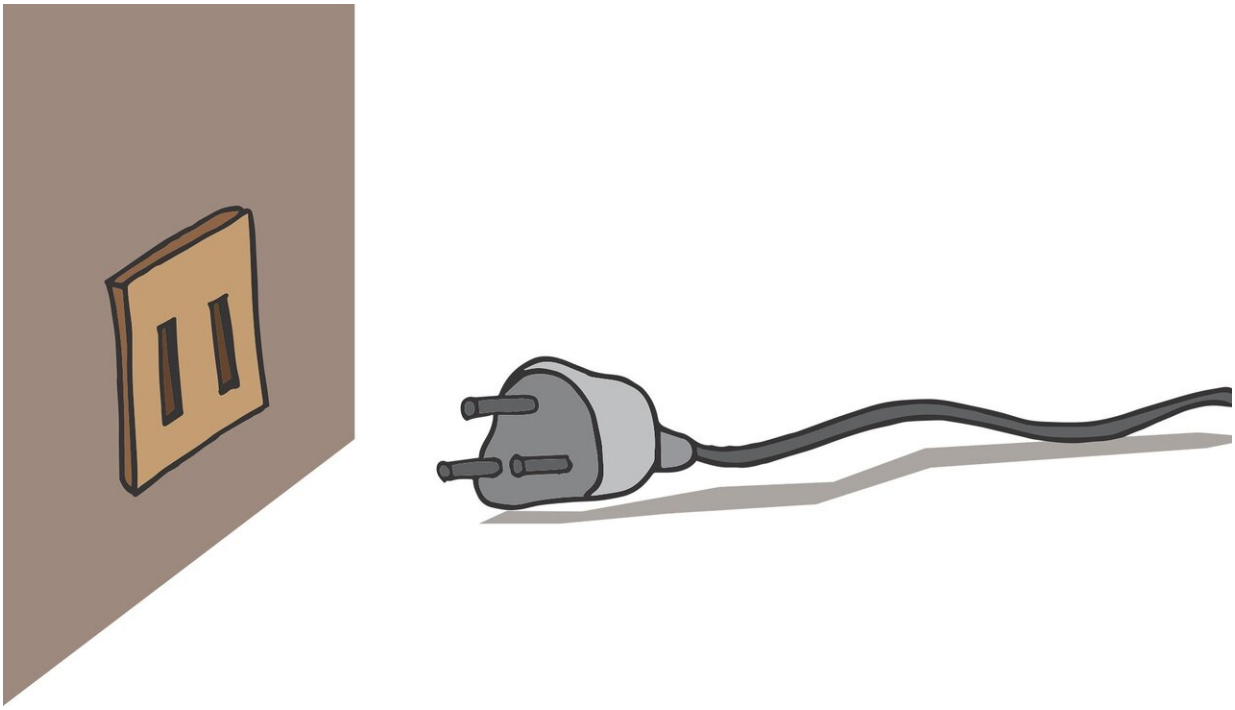
New technique uses power anomalies to ID malware in embedded systems

April 25 2019, by Matt Shipman



Credit: CC0 Public Domain

Researchers from North Carolina State University and the University of Texas at Austin have developed a technique for detecting types of malware that use a system's architecture to thwart traditional security measures. The new detection approach works by tracking power fluctuations in embedded systems.

"Embedded systems are basically any computer that doesn't have a physical keyboard – from smartphones to Internet of Things devices," says Aydin Aysu, co-author of a paper on the work and an assistant professor of electrical and computer engineering at NC State. "Embedded systems are used in everything from the voice-activated virtual assistants in our homes to industrial control systems like those used in power plants. And malware that targets those systems can be used to seize control of these systems or to steal information."

At issue are so-called micro-architectural attacks. This form of malware makes use of a system's architectural design, effectively hijacking the hardware in a way that gives outside users control of the system and access to its data. Spectre and Meltdown are high-profile examples of micro-architectural malware.

"The nature of micro-architectural attacks makes them very difficult to detect – but we have found a way to detect them," Aysu says. "We have a good idea of what power consumption looks like when embedded systems are operating normally. By looking for anomalies in power consumption, we can tell that there is malware in a system – even if we can't identify the malware directly."

The power-monitoring solution can be incorporated into smart batteries for use with new embedded systems technologies. New "plug and play" hardware would be needed to apply the detection tool with existing embedded systems.

There is one other limitation: the new detection technique relies on an embedded system's power reporting. In lab testing, researchers found that – in some instances – the power monitoring detection tool could be fooled if the malware modifies its activity to mimic "normal" power usage patterns.

"However, even in these instances our technique provides an advantage," Aysu says. "We found that the effort required to mimic normal power consumption and evade detection forced malware to slow down its data transfer rate by between 86 and 97 percent. In short, our approach can still reduce the effects of malware, even in those few instances where the malware is not detected.

"This paper demonstrates a proof of concept. We think it offers an exciting new approach for addressing a widespread security challenge."

The paper, "Using Power-Anomalies to Detect Evasive Micro-Architectural Attacks in Embedded Systems," will be presented at the IEEE International Symposium on Hardware Oriented Security and Trust (HOST), being held May 6-10 in Tysons Corner, Va. First author of the paper is Shijia Wei, a Ph.D. student at UT-Austin.

More information: "Using Power-Anomalies to Detect Evasive Micro-Architectural Attacks in Embedded Systems" Presented: May 6-10, IEEE International Symposium on Hardware Oriented Security and Trust, Tysons Corner, Va.