Securing electronic devices by creating 'digital fingerprints'

Cisco grant provides funding for hardware security research at Virginia Tech

Computers and internet connectivity continue to become vital across industries, from communications to transportation, medicine, energy, manufacturing, defense, finance and many more. But while this technology has enhanced the features and capabilities of everything from household appliances and cars to medical devices and the electrical grid, there are also serious concerns about the vulnerability of all of this hardware.

Finding ways to improve the security of such devices is the focus of research being conducted in the Bradley Department of Electrical and Computer Engineering at Virginia Tech, led by Patrick Schaumont, an associate professor there since 2005.

> "We design electronics for their functionality, but security is an afterthought or even simply absent. Our research focuses on finding ways to ensure the integrity and security of these types of hardware."

"Traditionally we think of computers as devices with a keyboard and a display, but that is rapidly changing given the sheer quantity of computers required within so many different types of devices and in various industries," Schaumont says, citing cars as one example. "There may be over 100 interconnected microcontrollers—essentially a network of tiny computers—in a modern car."

All of this technology is rapidly advancing, but research and development on the security of these devices has lagged behind. "Addressing the security of the computers in all these different types of devices turns the traditional IT security model on its head," says Schaumont. "Rather than focusing on securing a server, for example, you now have a device with a computer inside of it that is vulnerable. When these embedded computers are hacked, serious physical harm may result," he says. "In addition, there are safety concerns that emerge when we consider the risk of counterfeit embedded electronics. We design electronics for their functionality, but security is an afterthought or even simply absent. Our research focuses on finding ways to ensure the integrity and security of these types of hardware."

The research at Virginia Tech is supported in part by a grant awarded in June 2015 by Cisco, whose Advanced Security and Research team provides grants and expertise to guide and advance cybersecurity research at higher education institutions. "Cisco has been a true partner to us," Schaumont says. "They are not only providing us with funding through this grant, but we are also in regular contact and they offer us expert insights and a big-picture industry perspective that have been very helpful to guide the direction of our research."

Schaumont's research specializes in what is known in the industry and academia as Physically Uncloneable Functions, or PUF. "The best way to describe PUF is to compare it with fingerprints," he says. "The goal is to create what are essentially digital fingerprints for these devices, which are unique to each device and cannot be duplicated. These digital fingerprints could then be matched to a database record, providing authentication. This would ensure that the device is genuine, and has not been hacked or counterfeited."

While perfect IT security does not exist, Schaumont says if this research is able to create these digital fingerprints, it will make hacking or counterfeiting very difficult. "This would be an extremely robust solution. It would be a big first step to ensuring these devices are secure, and would minimize the risk of tampering."

Going forward, Schaumont says the research is making significant progress, and an engineering step by industry will take the concept to the next level in terms of embedding this authenticating technology into real-world electronics. "By enabling us to develop a prototype as a model of how the industry could create these digital fingerprints and build much more secure devices, this grant from Cisco has helped our research come a long way."

CISCO™

For more information on applying for a grant, visit http://research.cisco.com and visit the Trust and Transparency Center at http://trust.cisco.com.