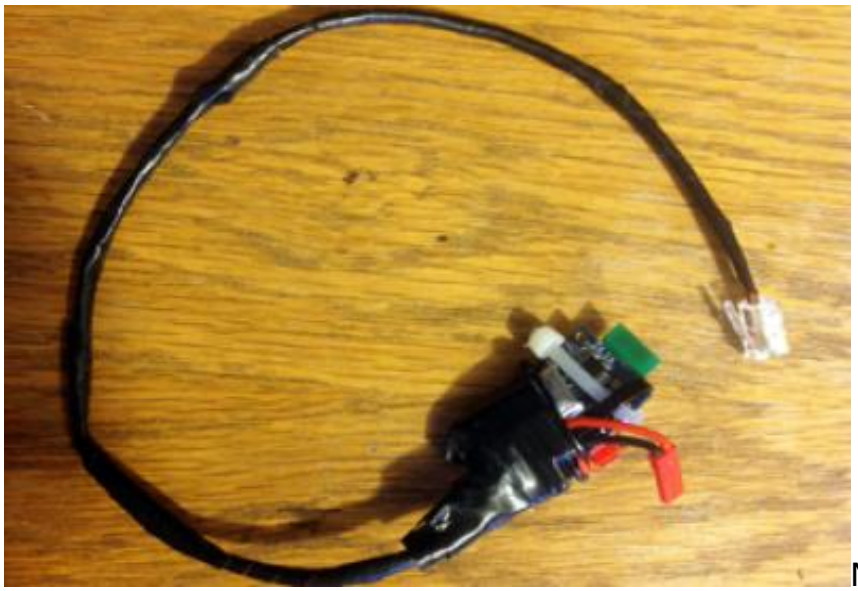
Computer scientists find vulnerabilities in Cisco VoIP phones

EurekAlert!

 New York, NY—January 7, 2013—Columbia Engineering's Computer Science PhD candidate Ang Cui and Computer Science Professor Salvatore Stolfo have found serious vulnerabilities in Cisco VoIP (voice over internet protocol) telephones, devices used around the world by a broad range of networked organizations from governments to banks to major corporations, and beyond. In particular, they have discovered troubling security breaches with Cisco's VoIP phone technology. At a recent conference on the security of connected devices, Cui demonstrated how they can easily insert malicious code into a Cisco VoIP phone (any of the 14 Cisco Unified IP Phone models) and start eavesdropping on private conversations—not just on the phone but also in the phone's surroundings—from anywhere in the world.

"It's not just Cisco phones that are at risk. All VoIP phones are particularly problematic since they are everywhere and reveal our private communications," says Stolfo. "It's relatively easy to penetrate any corporate phone system, any government phone system, any home with Cisco VoIP phones—they are not secure."

Cui and Stolfo analyzed the phones' firmware (the software running in the computer inside the phone) and they were able to identify many vulnerabilities. They are particularly concerned with embedded systems that are widely used and networked on the Internet, including VoIP phones, routers, and printers, and have focused their research on developing new advanced security technology to protect these systems.

"Binary firmware analysis is commonly used to identify faulty software by the 'white hat' hackers and security scientists and researchers like our team," Stolfo says. "We

performed this analysis to demonstrate a new defense technology, called Software Symbiotes, that protects them from exploitation."

Software Symbiotes is designed to safeguard embedded systems from malicious code injection attacks into these systems, including routers and printers.

"This is a host-based defense mechanism that's a code structure inspired by a natural phenomenon known as symbiotic defensive mutualism," Cui notes. "The Symbiote is especially suitable for retrofitting legacy embedded systems with sophisticated host-based defenses."

The researchers see these Symbiotes as a kind of digital life form that tightly co-exists with arbitrary executables in a mutually defensive arrangement. "They extract computational resources (CPU cycles) from the host while simultaneously protecting the host from attack and exploitation," explains Cui. "And, because they are by their nature so diverse, they can provide self-protection against direct attack by adversaries that directly target host defenses."

"We envision a general-purpose computing architecture consisting of two mutual defensive systems whereby a self-contained, distinct, and unique Symbiote machine is embedded in each instance of a host program," adds Stolfo. "The Symbiote can reside within any arbitrary body of software, regardless of its place within the system stack. It can be injected into an arbitrary host in many different ways, while its code can be 'randomized' by a number of well-known methods."

The Symbiote, which at runtime is required by its host to successfully execute in order for the host to operate, then monitors its host's behavior to ensure it continues to operate correctly, and, if not, it stops the host from doing harm. Removal, or attempted removal, of the Symbiote renders the host inoperable.

"The beauty of the Symbiote," says Cui, "is that it can be used to protect all kinds of embedded systems, from phones and printers to ATM machines and even cars—systems that we all use every day."

Cisco has since released a patch to repair these vulnerabilities but it is ineffective. "It doesn't solve the fundamental problems we've pointed out to Cisco," Cui observes. "We don't know of any solution to solve the systemic problem with Cisco's IP Phone firmware except for the Symbiote technology or rewriting the firmware. We plan to demonstrate a Symbiote-protected Cisco IP Phone at an upcoming conference."

Source: http://www.eurekalert.org/pub_releases/2013-01/cu-csf010713.php [1]

Links:
[1] http://www.eurekalert.org/pub_releases/2013-01/cu-csf010713.php