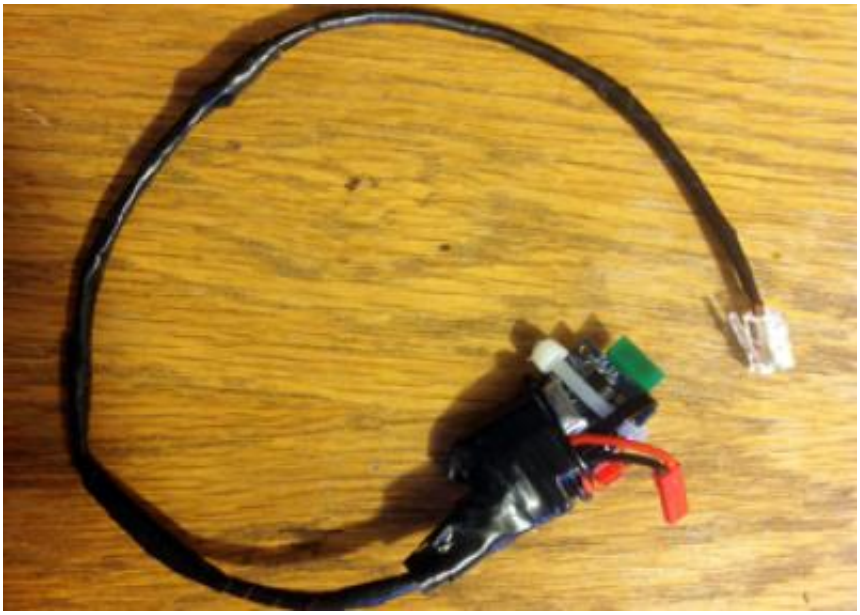
Security researchers find vulnerability in Cisco VoIP phones

December 19 2012, by Bob Yirka



Columbia Engineering's computer science Ph.D. candidate Ang Cui designed this device to plug into a Cisco phone and download malware, showing the vulnerabilities of the phone. Credit: Columbia Engineering

(Phys.org)—Ang Cui a fifth year PhD student at Columbia University, has given a demonstration at this year's Amphion Forum in San Francisco, showing a security vulnerability he and colleagues have discovered in Cisco VoIP phones. The vulnerability, he said, allows an intruder to place an electronic device into an on-premise VoIP phone that can be controlled by a nearby smartphone – allowing the "Off Hook

Switch" to be manipulated in such as way as to effectively turn the phone into a two-way walkie-talkie. He noted also that once a single phone had been breached all others on the same network could be breached as well though the single device.

Cui's demonstration was part of an overall theme – that embedded devices are vulnerable to attack by people bent on espionage or who wish to cause harm. He noted that devices such as network printers are quite often installed without adequate protection, leaving them open to attack by those outside of the system who wish to get in. VoIP phones, he says, use roughly the same type of technology and thus are equally vulnerable.

VoIP phones are normal looking phones that make and receive telephone calls using the Internet instead of the traditional phone network. Many large corporations have installed them because of their increased utility. Governments use them as well, Cui demonstrated, by presenting pictures of them sitting in several different governmental offices, including that of the Director of the CIA. In his demonstration, he affixed a simple circuit board (he calls it the Thingp3wn3r) to a VoIP phone that he said could just as easily have been in someone's real office – in just minutes. Next, he demonstrated the effectiveness of the Thingp3wn3r by accessing it via a smartphone app. Words he spoke in the vicinity of the phone, despite the receiver being down – the traditional mode of putting a phone offline – were picked up by the circuit board and transmitted to the smarthone app and played for all to hear. The end result is an ability to place a bug in an office using a simple circuit board and available hardware.

Cui and his professor, Salvatore Stolfo notified Cisco of the vulnerability prior to the demonstration and Cisco has responded by creating a patch that prevents the vulnerability from occurring. Those who are concerned about the vulnerability of their own systems are urged to contact Cisco for support.

More information: ids.cs.columbia.edu/sites/defa … iles/paper-acsac.pdf

Press release