Computer scientists claim security vulnerabilities in Cisco VoIP phones allowed them to eavesdrop on calls and turn devices into bugging equipment.

Ang Cui has demonstrated how malicious code injected into 14 of the networking vendor's Unified IP Phone models could be used to record private conversations - and not just those held over the compromised telephone itself: the malware can also pick up any sound within the vicinity when the handset is not in use. The discovered flaws effectively turn the network-connected phones into bugging devices.

Cisco VoIP phones are widely used in offices - small and large - across the world, creating a massive opportunity for potential mischief especially if the equipment is accessible from the public internet.

"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," said Professor Salvatore Stolfo of Columbia University who is supervising Cui's computer science PhD research.

"It's relatively easy to penetrate any corporate phone system, any government phone system, any home with Cisco VoIP phones — they are not secure."

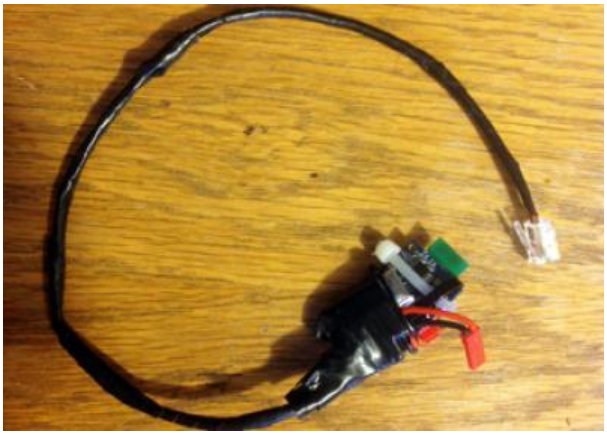
The New York university pair found that the operating system kernel in the vulnerable phones was not correctly validating data supplied by applications, meaning it trusted software to act responsibly. An attack could be launched by logging into the device over SSH, although this requires a suitable username and password, or by plugging into the Aux port of the phone to gain local access. Once inside the phone, miscreants could abuse kernel system calls to run their own code or crash the gadget.

But Cisco played down the academics' work, and said an attacker would need to be able to physically plug a line into the phone to download the malware to the device. And SSH logins are typically disabled in office environments.

Cui and Prof Stolfo dedicated several months to probing the security of internet-protocol phones, and this is far from their first advisory on problems with the widely used technology. The boffins argue that Cisco has only addressed the reported bugs rather than tackle fundamental design flaws of the hardware giant's Unix-like phone operating system.

Cisco issued an advisory on the uncovered security issues last year. It followed this up with a furtheradvisory on Wednesday, and another document providing more comprehensive and detailed mitigation advice.

"We issued a release note to customers at the end of last year (also crediting Mr Cui), but Wednesday's release of the advisory and mitigation bulletin provides more public information and the consolidated mitigation options," a Cisco spokesman explained.



Cui's makeshift tool to inject malware into Cisco phones

Credit: Columbia University

The pair of academics reckon either a complete rewrite of the firmware or a new type of security defence technology is needed.

"Cisco's recent advisory does not solve the problem unless and until they succeed in rewriting and releasing the rewritten kernel (promised in a few months) without harbouring any vulnerabilities," Prof Stolfo told *El Reg*.

"We really wish them luck. However, they can fix the immediate holes, but that does not protect the phone against other bugs the software might have. What they really need is independent security software running on the phone, just like what is available and provided by a mature security software industry for general-purpose computers."

In a separate statement, Cisco said it was continuing to investigate the reported flaws and working towards developing a more comprehensive fix. The networking giant said it has no evidence that the security shortcomings have actually been exploited. Cisco said the flaw would be hard to abuse and limited to Cisco 7900 series IP office phones:

Our engineering teams are actively working on a permanent fix, and we have released very detailed, step-by-step customer guides on identifying and preventing this vulnerability from being exploited. We are not aware of this vulnerability being used against any of our customers. We encourage customers with related questions to contact the Cisco TAC, or read the Security Advisory and Applied Mitigation Bulletin posted at www.cisco.com/go/psirt.

Cisco works closely with the IT security community and we view this as vital to helping protect our customers' networks. We thank Cui and Salvatore Stolfo for reporting this vulnerability to Cisco.

The vulnerability affects some of Cisco 7900 series IP office phones. In addition to specialist technical skills, a successful exploitation requires physical access to the phone's serial port or the combination of authenticated remote access and non-default

network settings. No default account exists for remote authentication and devices configured for remote access must use administrator-configured credentials.

Killing the spy who bugged me

Cui and Prof Stolfo found the exploitable security weaknesses after analysing the firmware binaries of VoIP phones. The research was part of an attempt to develop security technologies for embedded systems, such as network-connected phones, routers and printers. They christened this prototype technology Software Symbiotes.

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

The Symbiote runs on the embedded hardware and monitors its host's behaviour to ensure the device behaves itself and operates as expected. If not, the Symbiote stops the host from doing any harm. Removal, or attempted removal, of the Symbiote renders the device inoperable - a factor that could create a means for launching denial-of-service attacks against equipment but this has not blunted the enthusiasm of the computer scientists.

Cui said the Symbiote system could be used to protect all kinds of embedded systems, from phones and printers to ATM machines and even cars. The Symbiote design reads a bit like a science-fiction plot element* so it's no surprise that the computer scientists' research was partially funded by war tech boffins at DARPA - the US military's Defense Advanced Research Projects Agency. IARPA (Intelligence Advanced Research Projects Activity) and the Department of Homeland Security also bankrolled the research.