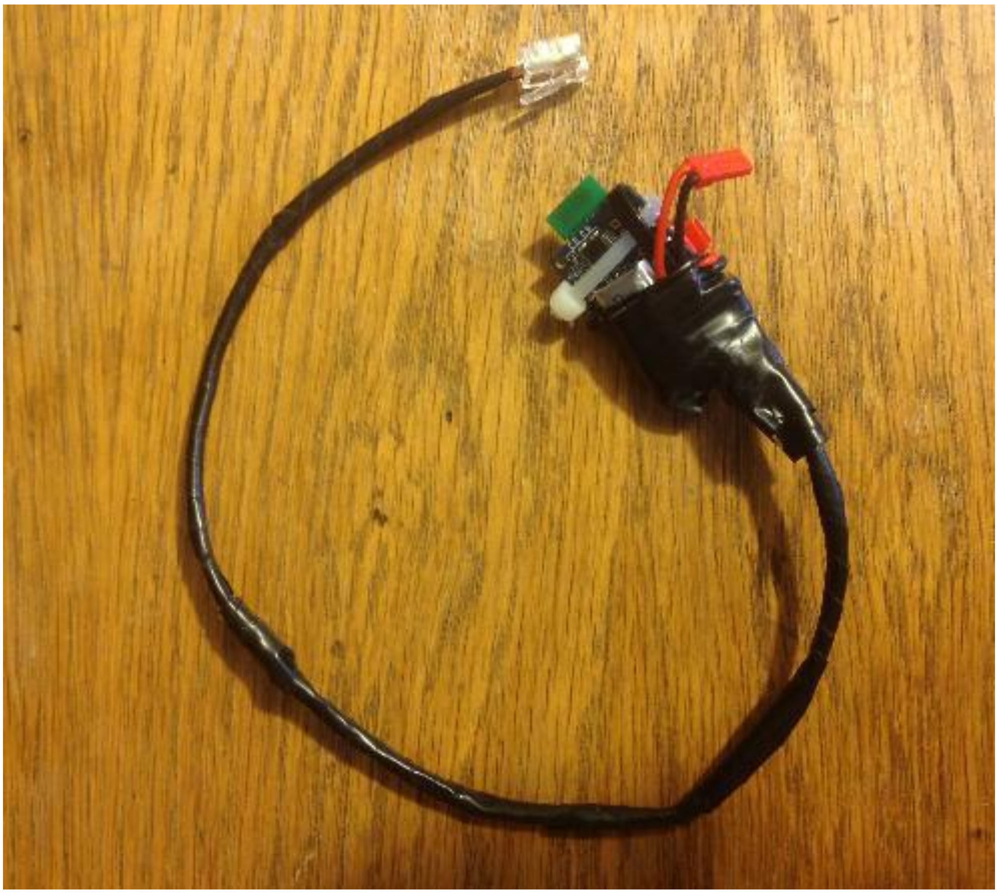
Popular office phones vulnerable to eavesdropping hack, researchers say



Columbia University

This small gadget can be attached to a single Cisco IP phone and turn an entire company's network into a sophisticated bugging device within seconds, researchers say.
By Bob Sullivan

High-tech telephones common on many workplace desks in the U.S. can be hacked and turned into eavesdropping devices, researchers at Columbia University have discovered.

The hack, demonstrated for NBC News, allows the researchers to turn on a telephone's microphone and listen in on conversations from anywhere around the globe. The only requirement, they say, is an Internet connection.
Doctoral candidate Ang Cui and Columbia Professor Sal Stolfo, who discovered the flaw while working on a grant from the U.S. Defense Department, say they can remotely order a hacked telephone to do anything they want and use software to hide their tracks. For example, they said they could turn on a webcam on a phone equipped with one or instruct the phone's LED light to stay

dark when the phone’s microphone has been turned on, so an eavesdropping subject wouldn’t be alerted that their phone has been hacked.

The flaw involves software running on Cisco’s popular Internet Protocol telephones. Cisco acknowledged the flaw in a statement to NBC News, but wouldn’t say how many of its phones were impacted. In a blog post earlier this year, the company — the leading IP phone maker, with about one-third of the market – said it had just surpassed 50 million in phone sales.

In a vulnerability announcement sent to paying customers in December, Cisco listed 15 phone models impacted by the problem.

“You can imagine the implications of this,” Stolfo said of the vulnerability. “Anything that is said behind closed doors isn’t private, no matter how sensitive the conversation is. There is no privacy. How can you conduct business like that?”

Cisco’s statement indicated that the company is working on a fix, and the firm told NBC News that it planned to issue a security bulletin next week. But Stolfo said he is “very worried about the speed with which Cisco is handling this.”

In a demonstration of the phone hack at the Chaos Communications Conference Dec. 29 in Germany, Cui showed examples of Cisco phones being used in government and military applications, though he noted there is no way to know if those phones were vulnerable to the attack.

“On the dark side, these phones are sold worldwide,” Stolfo said. “Any government that would like to peer into the private lives of citizens could use this. This is a great opportunity to create a low-cost surveillance system that is already deployed. It’s a monitoring infrastructure that’s free, when you turn these into listening posts.”

The research was conducted under a grant from the Defense Advanced Research Projects Agency (DARPA), an arm of the Defense Department devoted to computer security, and conducted at the Computer Science Department of Columbia University’s School of Engineering and Applied Science. **The same lab caused a global stir in 2011 when it published a hack of Hewlett Packard printers**.

“We consider this to be much more dangerous than the printer hack,” Stolfo said, “because of what you can do with the phone.”

In a demonstration conducted last week for NBC News, Cui showed how a small device pre-loaded with software and plugged into a port on the Cisco phone could rewrite the IP phone’s software within seconds. In the scenario he described, a would be hacker would need to access a phone for only a few moments – a phone on a secretary’s desk, for example – to conduct the attack.

Full technology and science coverage from NBC News

The Columbia lab focuses on so-called “embedded devices” — computer chips in non-PC gadgets, such as televisions, thermostats or telephones. Increasingly, all these gadgets are networked and connected to the Internet, and therefore can be hacked remotely.

“These phones are really general purpose computers jammed into a plastic case that makes you think it’s a phone,” Cui said. “Just because it doesn’t have a keyboard doesn’t make it less of a computer.”

Cisco’s IP phones — and other models that use the same chipset — are open to attack because they routinely connect to a central server looking for updated instructions, according to Cui. That creates an avenue for a hacker to insert rogue code, he said.

The phones run a proprietary adaptation of the popular Unix operating system called CNU, but any programmer familiar with Unix could write code for the phone and tell it to perform any function, Cui said.

“The phones are listening to a network waiting for a command. They are actively saying, ‘Does anybody have any code for me to run?’” said Stofo.

In an initial statement to NBC News, Cisco said that all Cisco IP phones “feature a hard-wired light that will alert the user whenever the microphone is active,” meaning it would warn any users that their phone’s microphone had been turned on. But the Columbia researchers dispute that, and showed NBC News a hacked phone that showed no evidence the microphone had been activated while they were eavesdropping on a conversation.

“There is no hard-wired light,” Cui said. “Everything is controlled by the software.”

After viewing Cui’s demonstration in Germany, Cisco issued an updated statement to NBC News backing away from its disagreement on the LED light issue, saying it “wasn’t directly relevant.”

But the researchers and Cisco still disagree about potential methods of attack.

Cisco said hackers would generally need physical access to a telephone in order to begin an attack, with rare exceptions.

“(Remote attack would require) the combination of authenticated remote access and non-default device settings,” Cisco said. “No default account exists for remote authentication and devices configured for remote access must use administrator-configured credentials.”

Stolfo said, however, that a hacker would need physical access to only a single phone on the network — a receptionist’s phone, for example, or a phone at the home or a remote worker — to gain access to a company’s entire phone network.

But he also maintained that there are multiple scenarios that would allow for a remote attack.

Escalation would be one way: An outsider could trick a worker into clicking on a virus-laden email attachment, infect the worker's computer and then use that computer to attack a phone from inside a company's network, he said. But the researchers say other flaws exist that would allow the phone to be attacked directly from outside the company.

"It also works the other way," Cui added. "You could attack the network, and then attack a single person's phone. Say, the CEO, at home."

Officials at DARPA said they couldn't comment on specific research, but praised Columbia's work generally.

"DARPA's program is concerned … with exploring what kinds of vulnerabilities are present in current systems so that we can determine architectural principles that will rule out such vulnerabilities in future systems," Dr. Howard Shrobe, DARPA Program Manager, said in a statement. "Computers often are at the core of many devices that most people do not think of as computers (e.g. phones, printers, power meters, cars and airplanes, for example) but which inherited the vulnerabilities of their embedded computer components. These devices have enormous impact in our everyday lives and in our critical infrastructures and are therefore a core concern."
Stolfo said it was critical to come forward with the Cisco flaw now because the company isn't working fast enough to fix it.

"What we're doing is trying to alert the manufacturer to not provide the opportunity to hackers to break into our phones," he said. "What we're asking them to do is like asking automakers to put seatbelts into cars to save lives."

The researchers have not released their attack code, so would-be criminals cannot simply copy their work and attack Cisco phone systems today, and there is no evidence that a hacker has exploited this vulnerability in the real world. They do believe others will successfully — and independently — duplicate their research, however, placing Cisco is in a race with hackers, and Cui thinks it's possible that has already happened.

"I'd be surprised if someone else hasn't already done this," Cui said.