29C3: Big bugging with Cisco VoIP phones

At the 29C3 hacker congress in Hamburg, security researchers from Columbia University have demonstrated that the microphone in the receiver of internet-based Cisco phones can be turned into a remotely controlled listening device. "We'll meet at 4 pm", whispered an uninvolved member of the audience in front of a manipulated device whose handset was on the hook. A few seconds later, a specially crafted app displayed the text on an attacker's smartphone, which was paired with the compromised phone via Bluetooth.
PhD student Ang Cui, who demonstrated the principle, explained that the device was a kind of room microphone of reasonable audio quality. Apparently, all Voice-over-IP (VoIP)-based Cisco phones are vulnerable, although the company only considers the series 7900 phones to be affected. Cui said that such devices are used almost everywhere, in locations such as offices and hospitals, and particularly in the US. The researcher demonstrated that his team had also located them on photos of US President Barack Obama at the White House and on Air Force One. One of the pictures even shows former CIA director David Petraeus with three Cisco phones in the background.

According to Cui, the devices' security documentation makes a solid impression on the casual reader. For example, the researcher said that the devices use electronically signed firmware, that their encryption techniques are certified, and that their attack surfaces have been minimised. Their admin interface can only be accessed via encrypted protocols such as HTTPS or SSH, continued Cui. As is the case with many embedded systems, the devices consist of a general-purpose computer with two chips: one SoC and one Flash storage. They also have a VoIP engine and a little bit of RAM, added Cui, as well as a switch that signals whether the handset has been picked up.
Version 4.1 of CNU (Cisco Native Unix) is used as the operating system. Cui explained that the kernel of this operating system has been found to contain several vulnerabilities with particular syscall functions when called by the kernel, as the functions do not check that they are not modifying kernel memory. According to the researcher, this potentially enables attackers to control all system components, inject arbitrary code, and take control of the kernel. Cui's colleague Michael Costello added that there were a total of 364 system calls and that 173 of these have been implemented, while 60 of them caused kernel panics which shut down the operating system's kernel leaving a core dump that could be used to identify concrete attack vectors.

Cui noted that the team didn't get very far with the phone's speakerphone microphone, because an LED that can't be disabled is activated when it is in operation. However, the researcher said that they did manage to reprogram the mic in the phone's receiver. First, the researchers had to take to phone "off hook"; they did this by reprogramming the GPIO connection to the hook switch to be an output. Cui then explained that three internal software modifications had to be made: the researchers first customised the Digital Signal Processor (DSP) chip's configuration for the listening attack by setting the connections, adjusting the microphone's output to a high level, and setting up an RTP socket

connection. In the kernel, they modify the GPIO and set the hook switch. Finally they modified the display code in the Java Virtual Machine which displayed an icon showing when the phone was on or off hook.

At present, the attack requires physical access to a Cisco phone because a small connector that the researchers have named "thingp3wn3r" must be inserted into an RJ11 console port on the device. The "thingp3wn3r" can be paired with a Bluetooth-enabled smartphone which plays host to the attack software. Pressing the "Auto-pwn" button on the smartphone transfers around 900 bytes of code to the phone, runs the exploit and patches the software.

However, Cui also presented several scenarios for fully remote attacks. For example, he said that the VoIP devices are usually connected with each other and with a TFTP (Trivial File Transfer Protocol) server via a VOIP LAN. He explained that this TFTP server is used to distribute a file used to verify firmware and other configuration information, but as it is a TFTP server it would be possible to connect to the VOIP LAN through a compromised phone and advertise some other device under an attacker's control as the network TFTP server. According to the researcher, it is also conceivable that known vulnerabilities in other embedded systems such as printers could be exploited to allow attackers to execute arbitrary code on the phone.

The researchers said that they informed Cisco of the security issue on 24 October. Apparently, the California-based company responded a week later, saying that there is a patch. However, Costello criticised the patch, which is not deployed automatically, as its changes just turned the exploit into a denial-of-service and left the door open for a simple modification of the exploit to return it to usefulness.

In February 2013, the team plans to present considerably more far-reaching defensive measures for embedded computer systems, based on the US government-sponsoredSymbiote technology. A Cisco phone will be shown at the RSA security conference in San Francisco with the Symbiote technology protecting the kernel.