Tencent Blade Team pair talk about smart speaker hack

August 14 2018, by Nancy Owano

Security researchers turned themselves into hackers this month to demo the way a smart speaker could be turned into a spy. The researchers took their story to DefCon 2018. They said they achieved remote eavesdropping. Both are Tencent Blade Team researchers. Conference notes described Wu HuiYu as a bug hunter and said Qian Wenxiang's

focus was on security research of IoT devices.

Meanwhile, *Wired* was provided with a description of the hackers' work. "After several months of research, we successfully break the Amazon Echo by using multiple vulnerabilities in the Amazon Echo system, and [achieve] remote eavesdropping," read the description.

Paul Lilly, *HotHardware*, was one of several tech watchers taking a look at how far they got and what it all suggests. First off, we need to get it straight what they were able to do, before you lose sleep over your smart speakers.

Wu Huiyu and Qian Wenxiang explored attacks to compromise a speaker considered fairly secure.

No observer though found their method at all trivial. There was little need to warn amateurs not to try it at home as their work was, well, oh please. Jon Fingas in *Engadget*: "It sounds nefarious, but it requires more steps than would be viable for most intruders."

Their attack, said *HotHardware*, "required acquiring and physically modifying an Echo speaker by removing the embedded flash chip so the hackers could write their own custom firmware to it, and then soldering it back into place." Also, there were conditions. "The modified Echo has to be on the same Wi-Fi network as the target speaker," Lilly said.

Tech watchers remarked that there was little reason to fret that their method would be used in the wild. "As it stands," said Jon Fingas in *Engadget*, "the likelihood of a real-world attack was small. A would-be eavesdropper would have to know how to disassemble the Echo, identify (and connect to) a network with other Echos and chain multiple exploits."

As for Echo, the researchers presented their findings to Amazon, which pushed out fixes to patch the security holes that made this type of attack possible.

So what are the lessons learned, then, if Amazon already pushed out fixes? One lingering thought shared by several writers on the incident is that the presence of smart speakers is very much in the line of sight of security hounds concerned over the way speakers tap into smart home devices, and security systems. Eyes are smart speakers as yet another point of entry for people with criminal intent.

Wrote Lilly: "What the attack does demonstrate, however, is that persistent hackers can find ways of attacking Internet-connected speakers like the Echo, even if the methods require a lot of work."

Fingas: "If there's a larger concern, it's that this demonstrates a snooping exploit is possible in the first place—no matter how unlikely it may be."

In the notes to their talk at DefCon, the two said they sought to present using multiple vulnerabilities to achieve a remote attack on some smart speakers.

"Our final attack effects include silent listening, control speaker speaking content and other demonstrations." They mentioned root privileges by modifying firmware content and re-soldering Flash chips. "Finally, we will play several demo videos to demonstrate how we can remotely access some Smart Speaker Root permissions and use smart speakers for eavesdropping and playing voice."

More information: Breaking Smart Speakers: We are Listening to You. www.defcon.org/html/defcon-26/ … -speakers.html#HuiYu