Issued 5/30/18

How Hackers can Exploit Devices Used at Home

Experts say the expanding ecosystem of internet-connected devices such as smart thermostats, home security systems and electric door locks are increasingly susceptible to hackers, including those trying to leverage voice-command devices. This risk is further compounded if an individual stores sensitive data on certain internet-connected products, like a credit card number or mailing address, which a hacker may be able to gain access to through other connected devices. One incident that drew particular attention this week highlighted some of the privacy fears surrounding voice-controlled devices and how they can operate seemingly independently of their owners' intentions. A woman in Portland, Ore., said her Amazon Echo recorded a private conversation she had with her husband and then sent an audio file of the recording to someone in the couple's contact list. The incident added to renewed scrutiny over how voice-controlled devices can operate outside their owners' intent and how they might be exploited by hackers. A group of researchers at the University of California, Berkeley, detailed in a paper earlier this month how they could embed hidden commands into text or music recordings, which could then get picked up by smart devices that have their microphones enabled. “Attackers can create a completely silent audio that you wouldn’t hear at all,” said Tavish Vaidya, a researcher at Georgetown University, noting that the audio could then “inject malicious commands onto any device that has a personal voice assistant." As an example, Vaidya described a situation where a hacker could try to embed a directive into a YouTube video that would in turn issue a command to a device using a digital assistant like Amazon's Alexa without the user ever knowing. Experts note that

there also appears to be an inverse relationship between security and connectivity, with products becoming increasingly less secure as they are hooked up to other online devices and applications. “The second you use some software to link everything to your house to some online account to something else, then it becomes valuable — in ways we don’t necessarily see, but hackers can definitely find those connections and try to figure out a way to exploit it," King said. "The fridge or the door lock, or any other home device, are all using software designed to communicate with the web and deliver one or other types of functionality," said Amit Ashbel, the director of marketing at application security company Checkmarx. “Each of these devices can be seen as a potential entry point into your home network and from there potentially to different types of data, whether personal, financial or business data,” he said. Vaidya said most devices currently do not have the ability to differentiate between the voices of their owner and a third party issuing a command. Thus, he noted that a hacker could theoretically send a hidden command to an Alexa-enabled security system asking it to unlock a door, as an example. Authorities have also raised concerns over the threats facing routers, devices that collect personal data including the internet sites visited by a household. While some internet-connected devices produced overseas or from unknown companies may be more affordable, experts warn that the manufacturers are often held to a less demanding security standard, allowing them to potentially leave out protective measures. “Major software manufacturers are still vulnerable to hacking, but they will be probably less so than the smaller, mostly Asian-made devices that have no security in them at all or very little,” King said. Experts also urge users to be cautious about what and how much information they share with their internet-connected devices. “If it is asking for your mailing address, then I would be suspicious,” Vaidya said, adding that he turns off devices when they are not in use.