You Said What? The Threat of "Always-Listening" Digital Assistants

Overview

Voice-enabled home assistants may expose your personal data and conversations to hackers, government agencies, and other third-party actors. Digital assistants collect expansive information about your habits and lifestyle, and many create an opportunity for adversaries to surreptitiously eavesdrop on your private conversations.

The prevalence of digital home assistants equipped with microphones has rapidly expanded in recent years as voice-assisted devices improved to allow for a broader array of functionalities. What was originally a niche feature in phones through Apple's Siri and Microsoft's Cortana is now embedded in standalone digital assistants that listen for conversations throughout your house.

- Strategy Analytics, a marketing research firm, estimated that two percent of US households—more than 2.8 million—owned a voice-activated digital assistant by the end of 2016. The firm expects this to rise to 11.5 percent of households by 2020.

Threats to Your Privacy from Digital Assistants

The presence of voice-enabled devices throughout your home creates a network of "hot mics"—listening systems that key into your conversations. Some of these devices, like Amazon Echo and Google Home, may only be listening for their "wake-up" words; however, a device may mistake an innocuous phrase for its "wake-up" phrase and begin recording. There is also a risk that the product could be constantly storing and transmitting your speech for use by the corporation.

- Digital assistants record your requests, and can use this data for targeted advertisements and for sale to third parties.
- Samsung faced backlash in 2015 when it came to light that its Internet-connected SmartTV, which includes voice-activation, was programmed to listen to your every word. The privacy policy for the devices stated, "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party."

Do You, Alexa, Swear to Tell the Truth, the Whole Truth…

Police in Bentonville, Arkansas served a warrant to Amazon in 2016 that requested audio recordings from the Echo in a murder suspect's residence. The affidavit stated that the police department had "reason to believe

that Amazon.com is in possession of records related to a homicide investigation being conducted by the Bentonville Police Department." Amazon does record and store transcription of the audio from user requests on its servers at remote locations—users can delete these recordings manually from the Alexa app. Police have routinely seized computers and cell phones in criminal investigations, and the Bentonville case has generated questions surrounding the expectation of privacy—particularly regarding "always listening" devices.

The personal data and recording logs compiled by your virtual assistant are also susceptible to attacks from hackers. The data stored by devices like Amazon Echo and Google Home can provide adversaries with important data about your interests, your habits, and your schedule that could be used for malicious purposes. For example, these devices will log your requests to add appointments to your personal calendar—a clear indication for potential criminals as to when you will be away from your residence.

- This data is vulnerable at two points—stored on the physical device and in transit to off-site servers. While Amazon states that it transmits data with secure HTTPS, the company has not publicized its precise security protocols, thus making it difficult to assess the security of these transmissions.
- Virtual assistant devices also have some local storage to record these logs. This data is vulnerable to both a remote hack or compromise by a hacker with physical access to the device.
- You can manually delete your data logs from both Amazon Echo and Google Home through the devices' apps.

"Always listening" devices could also be exploited by hackers to access your phone's microphone and discretely record your conversations. The presence of the microphone in these voice-assisted devices creates the potential for hackers to turn your virtual assistant into a bug without your knowledge. While incidents of adversaries co-opting devices in this way have not been documented, you should assume the same vulnerabilities apply to these devices as cell phones, which have historically been used as remote listening devices for hackers, according to one of our cyber security partners.

- Researchers from Georgetown University and the University of California, Berkeley released a proof of concept in 2016 on the ability to infect devices running Okay Google software with malware using covert voice commands hidden in YouTube videos.
- Devices from large technology companies—such as Amazon, Google, and Apple—are more likely to have strong security measures that vastly reduce the risk of hacker attacks than those produced by less established manufacturers.

The more interconnected your listening device is to your other home systems, the more vulnerable it becomes. Digital assistants are specifically designed to be a central control hub for a number of other "smart home" devices—such as lights, refrigerators, and security cameras—which are part of the interconnected "Internet of Things" (IoT). However, all of these devices—many of which have weaker security protocols than the virtual assistants—can be potential points of vulnerability where hackers could penetrate your network, compromise your digital assistant device, and access data logs or install malware to use the microphone.

- According to an information technology consultancy, there were more than six billion connected devices in use at the end of 2016; this number is expected to more than double by 2020.
- A teenager in the UK hacked 150,000 internet-connected printers across the world on 4 February 2017. While the attacker only used the devices to print messages, the printers provided easy points of access that could be used for other malicious activities.
- Attackers hacked at least 100,000 IoT devices—including cameras and DVRs—and used them to carry out a massive denial-of-service attack that disrupted internet access on the east coast of the US in October 2016. The compromised devices all had weak default passwords that allowed hackers to access and upload malware to them.

Mitigation Measures

While the most effective way to avoid the compromise of your personal data and conversations due to a virtual assistant is not to use one, there are a number of steps that can be taken to reduce associated risks. These methods will help you limit your exposure to hackers and reduce the amount of personal data available for compromise:

- ***Purchase a virtual assistant with a mute button and use it during sensitive discussions.*** Many virtual assistants have mute features that will disable the passive listening function in which it monitors for its wake phrase. However, hackers could unmute the device without your knowledge, so for truly confidential discussions, unplug the device.
- ***Hold sensitive discussions in a room from which the device cannot pick up your voice.*** Most digital assistant devices are designed with the ability to hear a voice from a substantial distance. Establish a location, such as a home office or bedroom, to be used for sensitive discussions and position the device in a location where it cannot hear statements in that room.
- ***Regularly delete the logs of your requests from your digital assistant.*** If your device provides the ability to delete these logs, use the feature regularly to limit the amount of personal information available for compromise.

- ***Ensure strong security on all of your connected devices.*** Change the passwords on every device that you connect to your home network so that it no longer uses the default, and regularly update these passwords. Install software patches as they become available—these are updates released by the manufacturer to address bugs and vulnerabilities discovered in the software.