Study reveals extent of privacy vulnerabilities with Amazon's Alexa

March 4 2021, by Matt Shipman

Credit: Unsplash/CC0 Public Domain

A recent study outlines a range of privacy concerns related to the programs that users interact with when using Amazon's voice-activated assistant, Alexa. Issues range from misleading privacy policies to the

ability of third-parties to change the code of their programs after receiving Amazon approval.

"When people use Alexa to play games or seek information, they often think they're interacting only with Amazon," says Anupam Das, co-author of the paper and an assistant professor of computer science at North Carolina State University. "But a lot of the applications they are interacting with were created by third parties, and we've identified several flaws in the current vetting process that could allow those third parties to gain access to users' personal or private information."

At issue are the programs that run on Alexa, allowing users to do everything from listen to music to order groceries. These programs, which are roughly equivalent to the apps on a smartphone, are called skills. Amazon has sold at least 100 million Alexa devices (and possibly twice that many), and there are more than 100,000 skills for users to choose from. Because the majority of these skills are created by third-party developers, and Alexa is used in homes, researchers wanted to learn more about potential security and privacy concerns.

With that goal in mind, the researchers used an automated program to collect 90,194 unique skills found in seven different skill stores. The research team also developed an automated review process that provided a detailed analysis of each skill.

One problem the researchers noted was that the skill stores display the developer responsible for publishing the skill. This is a problem because Amazon does not verify that the name is correct. In other words, a developer can claim to be anyone. This would make it easy for an attacker to register under the name of a more trustworthy organization. That, in turn, could fool users into thinking the skill was published by the trustworthy organization, facilitating phishing attacks.

The researchers also found that Amazon allows multiple skills to use the same invocation phrase.

"This is problematic because, if you think you are activating one skill, but are actually activating another, this creates the risk that you will share information with a developer that you did not intend to share information with," Das says. "For example, some skills require linking to a third-party account, such as an email, banking, or social media account. This could pose a significant privacy or security risk to users."

In addition, the researchers demonstrated that developers can change the code on the back end of skills after the skill has been placed in stores. Specifically, the researchers published a skill and then modified the code to request additional information from users after the skill was approved by Amazon.

"We were not engaged in malicious behavior, but our demonstration shows that there aren't enough controls in place to prevent this vulnerability from being abused," Das says.

Amazon does have some privacy protections in place, including explicit requirements related to eight types of personal data—including location data, full names and phone numbers. One of those requirements is that any skills requesting this data must have a publicly available privacy policy in place explaining why the skill wants that data and how the skill will use the data.

But the researchers found that 23.3% of 1,146 skills that requested access to privacy-sensitive data either didn't have privacy policies or their privacy policies were misleading or incomplete. For example, some requested private information even thought their privacy policies stated they were not requesting private information.

The researchers also outline a host of recommendations for how to make Alexa more secure and empower users to make more informed decisions about their privacy. For example, the researchers encourage Amazon to validate the identity of skill developers and to use visual or audio cues to let users know when they are using skills that were not developed by Amazon itself.

"This release isn't long enough to talk about all of the problems or all of the recommendations we outline in the paper," Das says. "There is a lot of room for future work in this field. For example, we're interested in what users' expectations are in terms of system security and privacy when they interact with Alexa."

The paper, "Hey Alexa, is this Skill Safe? Taking a Closer Look at the Alexa Skill Ecosystem," was presented at the Network and Distributed Systems Security Symposium 2021, which was held Feb. 21-24.

More information: Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem. Network and Distributed Systems Security (NDSS) Symposium 2021.
dx.doi.org/10.14722/ndss.2021.23111

Provided by North Carolina State University