Alexa, check my security settings

May 10 2018, by David Bradley

Credit: CC0 Public Domain

Do you trust the Internet of Things? More to the point, do you trust "Alexa" the voice-activated software in the Amazon Echo and related IoT devices? There is not necessarily any particular reason not to trust Alexa and Amazon, although one must always remember that data held by any company on its servers may be compromised by hackers or malware. In addition, might your "conversations" with Alexa and the Echo's recordings of your voice while it is in seemingly passive mode might be exploited by third parties or perhaps even used as evidence in a court of law.

Writing in the *International Journal of the Internet of Things and Cyber-Assurance*, Catherine Jackson and Angela Orebaugh of the School of Continuing and Professional Studies, at the University of Virginia, in Charlottesville, Virginia, highlight several issues and offer some advice for users. The same problems and how to address them might equally apply to any other voice-activated IoT device.

Problem 1: Alexa trusts and responds to requests from anyone, including those on TV or passing by an open window. This means that it will respond to a command from a passerby or a personality on the TV. The team suggests that without adequate security measures, unauthorised users might order items from Amazon, unlock the doors of the house, control thermostats, locate phones, and control devices such as ovens and other domestic appliances.

Recommendation 1a: Users worried about problem 1 should assign another wake word, such as "echo", "computer", or "Amazon" instead of using "Alexa". This will preclude radio and television advertisements, news broadcasts, and films and television programmes with characters named Alexa from activating the device.

Recommendation 1b: Users should enable a request notification sound at the start and end of a request to know when the device has been triggered. This might alert the user to an accidental or malicious activation.

Recommendation 1c: Users should keep their Amazon Echo device away from windows, doors, and out of "earshot" of their telephone answering machine, television or other audio device.

Problem 2: There are many benefits to having an "intelligent" digital assistant, but voice activation requires the device to be constantly alert to its wake word. However, there may be times when you might not want any device to "hear" your conversation.

Recommendation 2a: Engage the mute button so that your Amazon Echo stops listening. The LED indicator for the mute button will turn red to indicate that Alexa will no longer hear you as the microphone circuit has been disconnected by this action.

Recommendation 2b: Instead of only temporarily muting the Echo, you can leave it in mute mode perpetually and use the app or remote control.

Recommendation 2c: Disconnect the power supply when you are away from your device or not using it for extended periods of time. Not only does this save the trickle of standby electricity, but ensures privacy.

Problem3: Alexa stores a log of requests on Amazon's cloud servers, which are linked directly to the Amazon account associated with the [device](#).

Recommendation 3: Review your stored history periodically to check for unexplained or unauthorised actions and delete stored recordings when you feel the need.

Problem 4: Voice-activated purchases from Amazon are enabled by default.

Recommendation 4: disable voice purchasing or add a 4-digit PIN for purchases through the Alexa app to preclude third-parties, including children, friends, relatives, and visitors to your home from ordering items on your account.

"While these recommendations can improve consumer security and privacy for the Amazon Echo, similar actions should be taken for other intelligent personal assistants. Additionally, it is important to raise overall consumer awareness of security and privacy," the team concludes.

Jackson, C. and Orebaugh, A. (2018) 'A study of security and privacy issues associated with the Amazon Echo', Int. J. Internet of Things and Cyber-Assurance, Vol. 1, No. 1, pp.91–100.

Provided by Inderscience