The Final Project

INTRODUCTION TO COMPUTER SCIENCE FALL 2016

CECILIE UPPARD

Abstract

My family acquired an Amazon Echo, or commonly known as Alexa, over the summer and I found it very amusing. Shortly after, however, I heard of and became aware of several possible security holes in the product. Firstly, while Alexa is idle it listens for its "wake call". Amazon claims that the information which the device processes while it is idle is not used for anything. However, it might be interesting to try to find out what happens to the data it accumulates during this process. Secondly, the device learns to better understand commands and queries by storing previous queries. It may be interesting to look into how safely this data is stored and how it is used. Thirdly, Alexa holds on to several usernames and passwords and grants direct access to some accounts of third party applications. It would be interesting to look into what the risks associated to third party apps are. For instance, you can control entire home security and smart home systems through Alexa.

Introduction

Amazon Echo is a voice controlled device developed by Amazon.com. The device has seven microphones to capture commands and has a wide skill set including voice interaction, playing music, providing live news and setting alarms. The most useful feature, however, is its support for third party applications. Amazon Echo can connect to several other services, which allows one to control regular applications through voice commands. These services vary from controlling your lights, sprinkler system, home security system and thermostat, to browsing Spotify and making appointments in Google Calendar. While the device has been very well adopted by the public and has received great reviews, there exist concerns about the security

risks that Echo poses. This paper will try to convey three aspects of security in Amazon Echo; the consequences of always listening for its "wake word", processing commands in the cloud and possible risks of third party apps.

To the Community

The Internet of Things is rapidly developing. As there is a race to develop and release devices that make use of the cloud and can be incorporated into the public's lives, corporations down prioritize privacy and security. Convenience, efficiency and design are all aspects of products that keep improving, while the requirements to protect the user's privacy and the security of the data are minimal. I was curious if this trend would affect Amazon's Echo, now that the product has caught on to the public and has inspired several other technology companies to release similar products. Thus, the implications of a possibly insecure device like Echo would be big. I chose to research the security risks of Amazon Echo because the device is an IoT device that also utilizes other IoT devices. This way, even if Echo is implemented in an acceptably secure way, the lack of security in other IoT devices and applications makes Amazon Echo still pose a threat. Ultimately, such a device possibly carves a path for a wide range of malicious actions.

Alexa listens for your "wake call"

While Amazon Echo is turned on it will at any time light up and become responsive if the "wake call" is detected. The wake call is by default "Alexa", but can be changed to be "Echo" or "Amazon". Followingly, to detect the wake call Alexa must listen in on conversations. Thus, although the device is idle and supposedly not responsive, it must also be constantly processing noise that it picks up. Concerns have been expressed regarding this behavior, as to many it is unclear what happens to the data that Alexa processes while attempting to detect its wake call. In other words, Alexa is eavesdropping on conversations. Where does the information go?

It seems that the device records commands and requests and sends them to the cloud. In other words, the device does not process any sound locally, rather, processing is executed on Amazon's servers. "Like Siri, Amazon Echo works in the 'cloud,' running on Amazon Web Services."[1] Like any technology, most security risks are introduced once networks are joined.

At this point, it remains unclear exactly how Echo transmits its information, whether it is encrypted or not and which ports and protocols are utilized. I found only one source that addressed this question, and it states that the traffic is indeed encrypted.[2] So, even assuming that information is transmitted responsibly, the device will be prone to the regular risks associated to networks, like scanning, sniffing and man-in-the-middle attacks. Although these risks are something we all have to deal with on a regular basis, it may not be apparent to the general

[1] http://cybercrimenews.norton.com/toshibaweb2/expertqa/how-private-is-new-amazon-echo/index.html
[2] http://blog.zfeldman.com/2014-12-28-using-amazon-echo-to-control-lights-and-temperature/

public that these also exist with voice controlled devices, especially if the devices listen in on conversation without being invoked. So, how much does Alexa actually listen in?

"The tech giant says it does not listen to or record private conversations in the home."[3] The official Amazon FAQ for echo devices states that, "Amazon Echo and Echo Dot use on-device keyword spotting to detect the wake word. When these devices detect the wake word, they stream audio to the Cloud, including a fraction of a second of audio before the wake word." [4] Another source states that Amazon replied to his question about the wake call with, "the audio stream includes a few seconds of audio before the wake word, and closes once Amazon Echo has processed your question or request."[5] It therefore seems unclear how much of a command or request Echo actually sends to its servers. Whether it is a fraction of a second or a few seconds might not matter for most people, but for some, personal privacy is highly prioritized. Parts of private conversations that are unwillingly recorded, transmitted and stored in commercial servers therefore makes for a security risk in Amazon Echo.

Regardless of how much of our conversations is sent to the Amazon drivers, Robert Graham at Errata Security claims that the biggest security risk associated with Alexa's constant listening is related to the police. "The always listening feature is primarily a threat from the police, who could get a court order to secretly eavesdrop on you," says Graham. "I doubt it's a security concern from harm by hackers or harm by Amazon." [6] Additionally, he claims that this is actually a right that the police obtain. "According to 18 U.S. Code 2516, the Attorney General's office can petition a federal judge to 'intercept wire, oral or electronic

[3] http://www.yoursecurityresource.com/expertqa/how-private-is-new-amazon-echo/
[4] https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230
[5] https://www.slashgear.com/how-private-is-amazon-echo-07354486/
[6] http://www.cepro.com/article/amazon_echo_always_listening_feature_worries_security_experts#

communications.' Given the Echo is both electronic as well as oral, it is within this statute's purview." [7] Furthermore, media can apply for a right to publish the activity that Amazon collects from Echo. "Media outlets like *CE Pro* can file Freedom of Information acts to see exactly what sites and services the Justice Department and others are asking information from." The reason that queries to the Amazon servers are at risk is that Amazon stores previous queries to better understand future ones. The data that is stored is not anonymous, unlike the information Siri or Google Home stores, with the intent to make a personal device work better for the owner. This information gathering itself, is a security risk that should be addressed as servers and databases generally are hacked on a regular basis. Information stored by Echo will be related to purchases, conversations, questions, location and possibly Amazon account name and information. Thereby, in case of an attack on these servers, personal information is at risk.

Alexa Utilizes Third Party Applications

The biggest security threat associated with Amazon Echo, however, is posed by the connectivity to third party applications. "'This is the big security concern,' adds Graham, 'Even if the Echo is secure, many IoT devices are not.' As you connect your Amazon Echo to other devices, make sure to verify the security of those devices."[8]

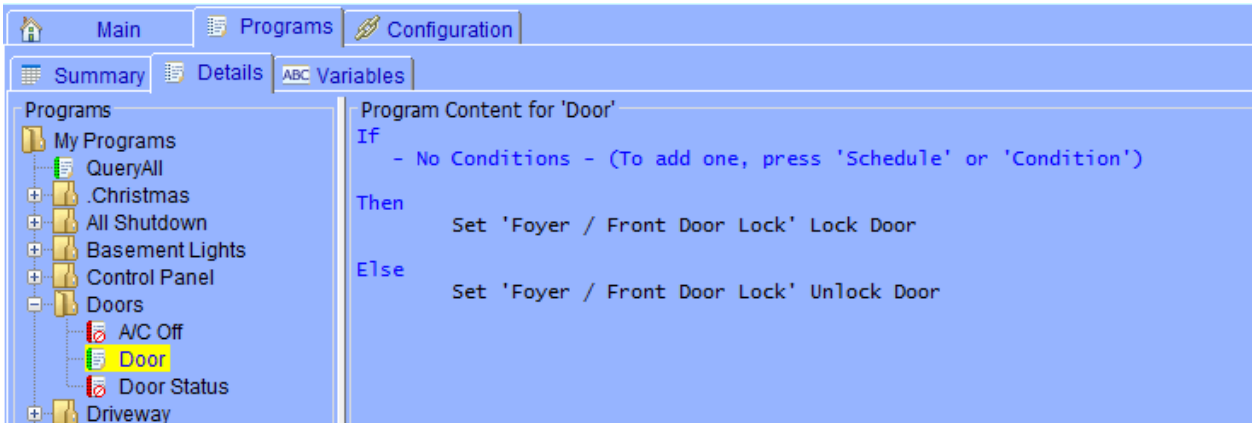
The first threat is username, password and possibly credit card information stored in third party applications. It remains unclear how well Echo protects this information when invoking actions related to them.

[7] http://www.cepro.com/article/amazon_echo_always_listening_feature_worries_security_experts#
[8] http://www.raifindia.org/robozine/2016/08/21/amazon-echo-the-new-home-assistant/

The most prominent threat, however, is posed by the group of home security system applications one can pair with Echo, including Nest and Scout.

With a paired Alexa and a Scout system it is possible to arm and disarm alarms, lock and unlock doors, ask for status of alarm and doors and alert the system.[9] The Scout system asks for a special Alexa PIN code when performing these actions to prevent intruders from exploiting the system. However, one could question the security of this code as the PIN has to be spoken out loud to Alexa.

Furthermore, Alexa supports an ISY integration that allows one to write programs to incorporate systems that are not already supported by the device, like Philips Hue and Samsung Smart Things. Using this integration, Matt Chiste writing for homeautomationguru.com wrote a program to lock and unlock his front door.



"What that means is that you can map a device called 'Open Door' to the program, allowing you to unlock the door with 'Alexa, turn on Open Door' and lock it with 'Alexa, turn off Open

[9] https://www.cnet.com/news/scouting-out-a-security-system-that-talks-to-amazons-alexa/

Door'."[10] Furthermore, Chiste demonstrates that placing the amazon Echo by the window and giving this command would unlock his front door from the outside. "The problem is that Alexa is a bit "too good" at what it does – always listening REALLY WELL for commands. Even… Through… Closed… Doors. And therein lies the problem: depending on the position of the Echo in your home, someone could just walk up from the outside and ask the door to unlock through a door or window!" Unlike Scout, this action does not require a PIN code or any form of authorization, and is thus a great security risk.

Two sub problems cause this action to be possible; Firstly, Alexa does not have any form of authorization of whomever speaks to it and secondly, there is a general lack of knowledge of the risks that follow the opportunities of third party applications.

Tackling the latter first, Amazon Echo has an endless number of opportunities to utilize applications by way of voice commands. If not supported by Echo, Matt Chiste just demonstrated that one can program applications to be supported. This is a trend that is spiraling upward and many have expressed interest in an Echo API that makes this programming more accessible to the people. However, most are not aware of the security issues that come with this liberty. Most applications have a hard enough time to handle authorization and security with the interfaces and portals they provide. If it is possible for a voice command device to access these based on either stored credentials or none at all, the authorization and verifications of logins and different actions are taken entirely out of the hands of the applications and left in the responsibility of Amazon Echo developers. Although this ultimately might be a good solution, today's Echo does not sufficiently support such behavior and it therefore poses a great security

[10] http://homeautomationguru.com/amazon-echo-door-lock-security/

risk. This brings us to a final security issue related to Amazon Echo; Echo does not authorize its user.

Echo Does Not Authorize Its User

When you set up Alexa you are given the following warning: "When you connect devices and services to Alexa, anyone speaking to Alexa can operate those products. This includes products such as garage doors, locks, and appliances." [11] Such a service is also Amazon's marketplace. There are recorded incidents of placement of orders from Amazon made by others than the owner of the account.[12] Thereby, Alexa practically grants every guest access to purchase anything from Amazon's marketplace. Furthermore, anyone can control the music that is playing, set off the sprinklers, turn off the lights and so on and so forth. Evidently, with support for more third party applications in store, the need for authorization before use of Alexa is highly needed.

What Can Be Done to Fill These Security Holes?

Firstly, Amazon must start working on developing some form of voice recognition or other means of authorization of users. Amazon Echo has huge potential to become an incredibly useful device both in our homes and in workplaces or for corporations. It is a device as taken out of a futuristic movie, however, the devices featured in such naturally do not perform any action for just anyone. Thereby, the lack of authorization currently stands in the way of further

[11] https://www.amazon.com/gp/help/customer/display.html?nodeId=201819970
[12] https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud

development as the product may become so unsafe at some point that it is an irresponsible device to own.

Secondly, the device can have some sort of location detection, either via phone or some small device, to detect the presence of eligible users. This way, if no one is home, intruders cannot activate Alexa, unauthorized users cannot use the services offered by the device without the presence of an eligible user and the system can generally be unavailable for unwanted guests or users.

Thirdly, personal information privacy must be improved. It is generally not safe to store personal information, as any server or database is prone to attacks, although there have not yet been recorded any such attacks.

Finally, the public must be educated on computer security. This measure is something that applies to any technology and computer security in general, as technology is rapidly interfering with our privacy. Especially now that the sphere of IoT is expanding, the public must be aware of the implications of bringing such devices into their homes and lives. The standards for security in Internet of Things are currently too low, and the vulnerabilities are many, as the software and technology implemented in them are limited compared to more advanced technology like laptops and servers. This final measure is a responsibility not only for developers of technology, but also for governments to enforce higher computer security requirements.

Conclusion

Amazon Echo poses big potential security risks that need to be handled before the device can live up to its full potential. Ranging from information storage and command transmission, to

third party app loop holes and lack of authorization, security risks may stand in the way of development of one of the most interesting products in future markets.

Sources:

- http://cybercrimenews.norton.com/toshibaweb2/expertqa/how-private-is-new-amazon-echo/index.html
- http://blog.zfeldman.com/2014-12-28-using-amazon-echo-to-control-lights-and-temperature/
- http://www.yoursecurityresource.com/expertqa/how-private-is-new-amazon-echo/
- https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230
- https://www.slashgear.com/how-private-is-amazon-echo-07354486/
- http://www.cepro.com/article/amazon_echo_always_listening_feature_worries_security_experts#
- http://www.cepro.com/article/amazon_echo_always_listening_feature_worries_security_experts#
- http://www.raifindia.org/robozine/2016/08/21/amazon-echo-the-new-home-assistant/
- https://www.cnet.com/news/scouting-out-a-security-system-that-talks-to-amazons-alexa/
- http://homeautomationguru.com/amazon-echo-door-lock-security/
- https://www.amazon.com/gp/help/customer/display.html?nodeId=201819970
- https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud