The Threat Is Real and Lives Among Us

By

Angela Marie Lucero

A Thesis Submitted to The Honors College

In Partial Fulfillment of the Bachelors degree
With Honors in

Cyber Operation

THE UNIVERSITY OF ARIZONA SOUTH

December 2018

Approved by:

Linda Denno, Ph.D.
Faculty Program, Cyber Operations

Abstract

The thesis focuses on the components inside the device, vulnerabilities, and interaction with the IoT device, Amazon's Echo Plus. The security of the device is addressed to help users understand how the device operates and what precautions should be in place. Many known vulnerabilities have affected the device along with the steps taken to secure the device. The interaction with the device discusses the steps taken to set up the device and the possible red flags found during this process. Also looked at is how the device can connect users near and far along with the possibility of surprise connections with friends and unknown connections where voice conversations are heard. The final piece is analyzing the packet capture of the device during three different scenarios; the device in isolation, the device in the main room with interaction happening around the device, and finally the user interacting with the device.

The Threat Is Real and Lives Among Us

While the Internet of Things (IoT) is made up of objects that were created to make lives more comfortable, it is vital that individuals understand the types of vulnerabilities they are exposing themselves to by using these devices and what potential threat these devices pose. According to Li, Tryfonas, and Li (2016), "The data security and privacy concerns are very important, but the potential risks associated with the IoT will reach new levels as interoperability, mashups and autonomous decision-making begin to embed complexity, security loopholes, and potential vulnerability" (p. 5). One of the most popular IoT devices is the Amazon Echo Plus. Even though the developers from Amazon created measures to strengthen the security in the Amazon Echo Plus, an analysis will expose some security vulnerabilities. The architecture of the product has features that can be modified to change the behaviors of the IoT device. This type of manipulation poses a risk to users' personal information. Users cannot afford to be an easy target for hackers so it is vital to know what data is received, where the recorded data goes, and who else could potentially access their information.

The Amazon Echo Plus is an IoT device that is controlled by the user's voice and allows users to get updates on traffic, the weather, to research information, listen to music, message and call friends while also controlling compatible lights, door locks, and wall switches. According to Amazon, "With seven microphones, beamforming technology, and noise cancellation, Echo Plus hears you from any direction—even while music is playing" (Amazon.com, Inc., 2018, p. 1). The Echo Plus collects information and sends it to Amazon, so it is essential to find out what information Amazon has received, where it goes, and who else could potentially have access to this information so users can be proactive in safeguarding themselves.

Li, Tryfonas, and Li (2016) discuss the four main layers in the architecture for IoT devices. These layers are essential for IoT devices and include the sensing layer, network layer, the service layer, and the application-interface layer. The sensing layer can determine the environment the device lives in. At this layer, the device interacts with the user through voice commands. The device then has to determine if authorization is correct, which in this case only a wake word is needed to execute commands. At the sensing layer, software updates take place along with any patches that could affect the how the device functions. Updates and patches are necessary as the device is exploited and voice conversations intercepted or packets of data could be intercepted. One concern about the sensing layer is who can control the device and then how the device chooses to complete the command or task. Unauthorized access, availability of the device compromised, or a malicious virus or malware could all threaten the security of the device. The network layer is what enables the device to connect with networks and other applications. There is a concern about the level of security and privacy depending on the type of network the device is on. The security and privacy of the user are at stake and could be compromised through a data breach at the network layer meaning that secure and confidential information could be stolen or a Denial of Service (DoS) attack preventing authorized users from accessing the network. These are just a few of the security threats that affect IoT devices. The service layer is where management services of the device lie that determines how the device will behave. The concern for the service layer is that the device is attacked. The application-interface layer is how the device interacts with users or other applications. The concern in this layer is the device could be misconfigured, log and key files leaked, unauthorized access, and a variety of viruses, trojans, spam, and malware. To understand how a device is susceptible to

vulnerabilities, it is essential to understand how each layer works and the security concerns that happen at each layer and the effect it has on the device and user.

Paul Dempsey (2015) reported on the teardown of the Amazon Echo by the iFixit team, and the findings show that the components are a lot more powerful than needed for a device that plays music. Texas Instruments (TI) manufactures the majority of the components along with some by Qualcomm, SanDisk, and Samsung. The parts found inside include digital media processors, memory (storage), Dynamic Random Access Memory (DRAM), Wi-Fi/Bluetooth modules, power management, audio-to-digital converters, flip-flops, Light-Emitting Diode (LED) drivers, step-down regulators, audio codecs, and amplifiers.

Dempsey (2015) goes on to list other components of the Amazon Echo Plus such as the digital media processor created by TI. The processor is a DM3725 with an Advanced RISC Machine (ARM) Cortex-A8 and C64x+DSP as the core. This chip was designed to process large amounts of data as it completes many tasks on a whim (Leyden, 2018). There is some concern about this chip, as most are fixed and resistant to being altered quickly, but this chip can be manipulated. If the wrong person has access to the device, the processor can be injected with code by anyone who has a set of instructions putting personal data in jeopardy. The digital signal processor (DSP) of the DM3725 allows for a stream of digital data where large amounts of the digital signal can be changed (Thompson, 2001). The Samsung LPDDR1 of memory uses less power than other chips while also transferring data up to 200 megabits per second (Mbps). While these components are high tech, there is a concern about how they can be tampered with while putting the user's data at risk.

John Keefer (2018) reported on several vulnerabilities related to the ARM chip such as Spectre and Meltdown. Spectre makes the program select random areas in the memory space of

the program. An attacker could access the data in the memory space and be able to read potentially sensitive data. Spectre can make changes to a process and not reveal the data. It is also easier to exploit because it can be done through C or C++ programming and also executed remotely. Meltdown vulnerability allows the memory to be obtained where data could be accessed from other applications or operating system. Variant 4 is a vulnerability that allows old memory values to be accessed in the stack of the Central Processing Unit (CPU) or other memory locations (Alert, May 2018). All of these vulnerabilities could harm an unpatched operating system.

The Samsung LPDDR1 chip along with the LPDDR2, LPDDR3, and LPDDR4 chips are susceptible to the RAMpage vulnerability (Conway, 2018). The vulnerability could be used to acquire root access on a device. This is done through Android's memory management system, Android ION memory allocator. ION was created in 2011 and provides applications the needed memory to run the program. Protected memory is now gone because ION allows malicious programs to make its way into the memory. GuardION was released to build a safeguard to stop this from happening. It is not a guarantee to stop this from happening; it only lessens the damage that could be done.

A hacker who has access to the physical device can compromise the device by opening the bottom of the Amazon Echo and attaching a Secure Digital (SD) card to the ports of the machine. Mark Barnes (2017) explains that the SD card is accessed when the device is rebooted bypassing the internal startup. The processor chip begins mapping, and the boot process is intercepted allowing access into the partition of the memory. In order to gain access to the audio files, a script was used to mount the partition to gain entry to the entire file system. Once a reverse shell is installed, root shell is used to listen to the device and commands are used to

capture the audio stream and copy it to a remote device. Barnes (2017) said that this vulnerability was found on the 2015 and 2016 Amazon Echo devices but was fixed in the 2017 devices. Navarro (2017) recommends that when the Amazon Echo Plus is not in use, it be suggested that you mute the device. At the moment, there is no known way for malware to get around the mute button unless the attacker has kernel level control and then has complete access to all functionality. Turning the device off is the surest way to safeguard personal conversations. While the attacked does need access to the device to capture the audio files, it is essential to have a secure device especially when you are not sure who may have access to it.

There are some Common Vulnerabilities and Exposures (CVE) connected to the Amazon Echo Plus. CVE-2018-11567 has been disputed, but before April 27, 2018, the reprompt feature could allow for a skill to be used allowing the conversation data to be intercepted. The reprompt feature comes in to play if the Amazon Echo does not hear anything within eight seconds, it can ask the user to repeat the request. If the device still does not hear anything, then the device turns off. CVE-2018-19187 is the Amazon PAYFORT vulnerability where a random parameter name is messed up in the success.php echo statement The MITRE Corporation. (2018). Payfort is an Amazon company that handles online payment systems so users can purchase products online. It was discovered that during the encryption process of the Software Development Kit (SDK) that handles the payments, there is a vulnerability that could allow for the processing payments to be hijacked through Cross-Site Scripting (XSS). This vulnerability allows malicious code to be injected into websites that users would generally trust. This is fixed by changing the code of the SDK. Baset (2018) said that the code needs to be updated or the SDK taken down, so the vulnerability does not hurt users. CVE-2018-19189 is another Amazon PAYFORT vulnerability that is affecting the error.php echo statement. This also affects users as their websites are at risk

for malicious code in the request. Again, the code needs to be fixed on the SDK or not used. It has been said that this vulnerability was fixed, but there has not been any official confirmation (Baset, 2018).

Along with the CVE's, there have been a variety of other security concerns with the Amazon Echo since its debut in 2014. Kumar (2018) reports that researchers have created a "skill" that turns the Amazon Echo into a device that can spy on you. This skill is called the calculator skill, which uses the API\Lambda-function. When the calculator skill is started, a second session is also initiated that allows the microphone to continue running without the user knowing. While the calculator skill would end, the second session would continue without alerting the user verbally. All of your conversations would be captured for as long as the session is open. The only way that a user would know that their device is on by the blue light that is illuminated on the Amazon Echo. Amazon knows about this skill and checks for ones like the calculator one and removes them from their store. At this moment, there are not any versions of this skill, but if a second-hand echo was purchased that has not been patched or a copy of the skill is put into the wild, the device would be vulnerable to this security flaw.

Page (2017) reveals an exploit called BlueBorne that uses the device's Bluetooth ability to take over the device. The BlueBorne attack can pair with your device without any needed permissions. In order to pair with a device, the Bluetooth setting has to be enabled (Lamb, 2017). This is extremely dangerous because once the attacker is paired to your device; they can access the network and install malicious code or malware. Two specific BlueBorne vulnerabilities affect the Amazon Echo. There is the remote code execution vulnerability in the Linux Kernel and the information leak vulnerability in the Session Description Protocol (SDP) server. The attacker can connect to the device using Bluetooth and then can run a shell script to

overtake the device. Once this happens, the device only hears the wake word, "Alexa" and instead with a reply that has been pre-programmed by the hacker (Armis, 2017). This exploit, CVE-2-17-1000250, also allows the hacker to retrieve sensitive information from the process memory (The MITRE Corporation 2018). Amazon has said that devices were automatically updated to fix this. Devices need to be checked to ensure they have the correct version installed. Users want to make sure that v591448720 or newer is installed as it has the patch to block the vulnerability.

An incident occurred where the Amazon Echo was remotely activated. The owner was not home, and the device was overtaken, and the volume was put on full blast. The music was so loud that the police were called and all that was found was the device. Amazon says that a third-party app was used to turn the volume up. While this instance shows how the device is controlled, if an attacker has access to the device it can then go in deeper to the network that the device is on. This is a concern because the personal information could be stolen or attack other networks and devices (Page, 2017).

Another vulnerability is one called Key Reinstallation AttaCKs (KRACK). This vulnerability works to create a key that can read the encrypted traffic. During the handshake of the WPA2 protocol, an attack can happen where it creates a key that is previously installed and then it is possible that the encryption does not happen. This vulnerability affected all existing Wi-Fi where data is intercepted, but the KRACK attack was more likely to be used to send malware or viruses through the network. When a Wi-Fi connection is established, there is a four-way handshake that happens. A new, unused encryption key is generated when a Wi-Fi is joined and confirmed on the third handshake, but for the attack to happen, an old key is reinstalled after the attacker makes it look like packets were dropped. It then appears to resend

the data, and that is when the reinstallation of the key happens. The attacker then has access to the encrypted key and access to all the data on the device. Public Wi-Fi should be used with great caution as anyone could attempt to access nearby device (Vanhoef, 2017).

Device Interaction

There are specific steps that need to be followed when setting up the Amazon Echo for the first time. One of the very first things the user must do is to download the Amazon Alexa app that is found in the app store. Sign in with Amazon credentials and then follow the steps in the app to connect the device to the Wi-Fi. Once the Amazon Echo is plugged in and ready for the setup, an orange ring on the top of the device will appear. The user then needs to go to the phone Wi-Fi settings and connect the phone to Amazon-XXX Wi-Fi. The largest red flag in this part of the process is that this network is open and unsecured. Even though this process takes a moment to connect the device to the Wi-Fi, the phone is now open and being used on an unsecured network. The phone could be overtaken and whatever is stored on the phone is now available for the taking. Once the device is set up, the keyword "Alexa" is used to request facts, music, weather updates, and much more.

The user can also make phone calls to other Amazon Echo users that show up in the phone list in the app. The user has to authorize others to see that they have an Amazon Echo product for someone to send them a message or call. While this is a handy feature to call your friends quickly, it does not always work as expected. The calling feature works well when the user asks "Alexa" to call someone, but the person on the other side may be caught off guard. The default when setting up the Amazon Echo is to allow others to contact the user. This feature was attempted, and the contact on the other side was quite bewildered when they heard a voice randomly talking to them. The contact was not aware that this default was on for the device.

Another instance of unknown voice calling is when the user heard conversations from the device. A person in the contact list had inadvertently said a keyword that the Echo Plus interpreted. The person's background conversation could be heard through the device. It is essential to know how the device is set up because users do not want random calls or to have personal conversations go out over the device.

Multiple packet captures were completed with the Amazon Echo Plus through three different scenarios. The device was isolated with no noise or traffic around the device, the device was in the room with regular conversations without using the "Alexa" keyword, and the final scenario was interaction with the device using the "Alexa" keyword. When the device was isolated without any noise or traffic near it, multiple packet captures showed communication from the Amazon Echo Plus to the server. The initial packet capture included a Multicast Domain Name System (MDNS) query. This was a request for all records the server has available. There were a couple of packets like this with some join group packets with an Internet Group Management Protocol (IGMPv3). This shows the device connecting into the network, and after the connection is made, there are many packets with a standard query response with an MDNS protocol. These packets show a DNS response retransmission during the packet capture. The DNS response retransmission happens because packets are lost during the transmission. This policy enables devices to stay connected with the network and the policy is also changeable based on the devices needs (NS1 – Intelligent DNS and Traffic Management, 2018). Farther in the packet capture, the device loses connection with the Wi-Fi and is established again. There have been issues with other devices disconnecting from the Wi-Fi, and this packet capture fits the pattern of previous connection issues. After this reconnection, the rest of the packets contained the same DNS response retransmission.

When the Amazon Echo Plus was in the central part of the house with conversations around the device, there was similar packet captures of that of the device in isolation. Some packets contained sleep_proxy queries. This indicates that the device went to sleep for less than an hour while users conducted regular business around it (Cheshire, 2009). The device then put out a standard query response with cache flush to provide new information and to ignore previous outputs from the device. This same cycle continues for a while without much else showing up in the packet capture.

During the interaction with the Amazon Echo Plus using the keyword "Alexa," the packets show where the device connects to the Wi-Fi and a connection is established. As soon as the keyword is used and commands are given to the Echo Plus, there are many packets sent to the Amazon server. There are many packets with a standard query response, but these are slightly different from before as they do contain the cache flush, but also has Android.local within the packet capture. When the device is in use, the cache flush is happening, but the Android.local is used due to zeroconf to allow services and systems to be discovered (Burgess, 2018). This type of packet only shows up when the device is being interacted with. When it is not in use, then packets with standard query response with cache flush come through. At one point while interacting with the device, packet captures were showing the Amazon Echo Plus trying to establish a connection to the central computer in the house. The packets show while the device is in use, a TCP Retransmission is taking place. A connection never happens, and then after a few moments it ends, and the device goes back to sending data to the Amazon server. There could have been an error in the connection between the device and server so the device went to the next device it could find. Every voice interaction is recorded, kept, and can be heard

on the phone app. The user can delete these, but there is no confirmation if they are deleted from Amazon servers.

After looking at the components of the device, the vulnerabilities, known ways hackers can access data remotely from your device, and see how the device interacts within a home, there is many red flags that consumers need to be aware of. There is an element of danger to having this item in the home, but the fun of the device will probably outweigh the risks for consumers. The Amazon Echo Plus is viewed as more of a toy than a tool, and because of this, users will probably take the chance and put it in homes. The device becomes more a risk when it is used in offices because of the level of security that businesses work to hold onto. Having this device in the workplace opens up the company to liability. Given that more and more IoT devices will enter homes and offices, there is a high level of vigilance that users need to be at. The risk will always be there, but it is how users move forward with the knowledge to protect themselves.

References

Alert (TA18-141A). (2018, May 21). Retrieved from https://www.us-cert.gov/ncas/alerts/TA18-141A

Amazon.com, Inc. (2018). Echo plus. Retrieved from https://www.amazon.com/dp/B015S1SWLO/ref=ods_mccc_sr?th=1

Aravindan, V. & James, D. (2017, April). Smart homes using internet of things. *International Research Journal of Engineering and Technology (IRJET), 4*(4), 1725-1729.

Armis (2017, December 5) BlueBorne cyber threat impacts amazon echo and google home. Retrieved from https://armis.com/blueborne-cyber-threat-impacts-amazon-echo-google-home/

Barnes, M. (2017, August 1). Alexa, are you listening? Retrieved from https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening

Baset, M. A. (2018, November 13). PAYFORT – multiple security issues and concerns in a PCI/DSS compliant payment processor SDK! Retrieved from https://www.seekurity.com/blog/general/payfort-multiple-security-issues-and-concerns-in-a-supposed-to-be-pci-dss-compliant-payment-processor-sdk/

Burgess, P. (2018). Bonjour (Zeroconf) Networking for Windows and Linux. Retrieved from https://learn.adafruit.com/bonjour-zeroconf-networking-for-windows-and-linux/overview

Champlain College. (2016, March 08). Amazon echo forensics update 2. Retrieved from https://lcdiblog.champlain.edu/2016/03/08/amazon-echo-forensics-update-2/

Cheshire, S. (2009, December). Understanding sleep proxy service. Retrieved from http://stuartcheshire.org/sleepproxy/

Conway, A. (2018, June 29). Every Android device is susceptible to a hardware vulnerability called RAMpage. Retrieved from https://www.xda-developers.com/android-hardware-vulnerability-rampage/

Davies, C. (2014, November 07). How private is amazon echo? Retrieved from https://www.slashgear.com/how-private-is-amazon-echo-07354486/

Dempsey, P. (2015, March). The teardown: Amazon echo digital personal assistant. *Engineering and Technology.* 10(2), 88-89.

Field, M. (2018, April 27). Amazon fixes alexa bug that let echo keep listening. Retrieved from https://www.yahoo.com/news/amazon-alexa-bug-let-hackers-104609600.html

Keefer, J. (2018, January 04). ARM acknowledges chip vulnerabilities, details fixes. Retrieved from https://www.neowin.net/news/arm-acknowledges-chip-vulnerabilities-details-fixes/

Kumar, M. (2018, April 26). Amazon alexa has got some serious skills-spying on users! Retrieved from https://thehackernews.com/2018/04/amazon-alexa-hacking-skill.html?m=1

Leyden, J. (2018, February 27). Malware-flingers can pwn your mobile with over-the-air updates. Retrieved from https://www.theregister.co.uk/2013/03/07/baseband_processor_mobile_hack_threat/

Li, S., Tryfonas, T., & Li, H. (2016). The internet of things: A security point of view. *Internet Research, 26*(2), 337-359.

Lumb, D. (2017, September 12). Some phones and laptops are vulnerable to 'BlueBorne' exploit. Retrieved from https://www.engadget.com/2017/09/12/blueborne-bluetooth-exploit-ios-android-windows/

Micaksica. (2017, January 02). Exploring the amazon echo dot, part 1: Intercepting firmware updates. Retrieved from https://medium.com/@micaksica/exploring-the-amazon-echo-dot-part-1-intercepting-firmware-updates-c7e0f9408b59

Navarro, F. (2017, November 09). 3 amazon echo privacy settings you should turn on now. Retrieved from https://www.komando.com/tips/426842/3-amazon-echo-privacy-settings-you-should-turn-on-now

Navarro, F. (2017, November 04). 10 amazon echo commands you have to try. Retrieved from https://www.komando.com/happening-now/427655/10-amazon-echo-commands-you-have-to-try

NS1 – Intelligent DNS and Traffic Management. (2018). DNS retransmission. Retrieved from https://ns1.com/resources/dns-retransmission

Page, C. (2017, November 16). BlueBorne: Bluetooth exploit takes aim at amazon echo and google assistant devices. *The Inquirer*. Retrieved from https://www.theinquirer.net/inquirer/news/3021179/blueborne-bluetooth-exploit-takes-aim-at-amazon-echo-and-google-assistant-devices

Rahman, A. F. A., Daud, M., & Mohamad, M. Z. (2016, March). Securing sensor to cloud ecosystem using internet of things (iot) security framework. *Proceedings of the International Conference on Internet of things and Cloud Computing* (p. 79). ACM.

The MITRE Corporation. (2018). Common vulnerabilities and exposures. Retrieved from https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=amazon%2Balexa

Thompson, T. (2001, March 12). Digital Signal Processor. Retrieved from https://www.computerworld.com/article/2591782/enterprise-applications/digital-signal-processor.html

Vanhoef, M. (2017). Key reinstallation attacks. Retrieved from https://www.krackattacks.com/

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. *IEEE wireless communications*, *24*(3), 10-16.