CY 5770 – Spring 2021
Alexander Semaan

HW1 – Security Review

1. Technology Summary

With the rise of IoT and smart devices, the number of interconnected devices in the average person's home has increased exponentially. In order to manage this growth and enhance the user's experience, virtual assistant AI technologies such as Amazon Echo's Alexa were developed. This security review's goal is to convey a security risk analysis for the Amazon Echo suite of products.

Amazon Echo's Alexa is considered an AI assistant that can understand over 8 natural language voice commands including English, German, French, Spanish, Japanese and Hindi, in order to perform tasks for the user. These tasks can vary widely in nature: you can ask Alexa to order you an uber, to tell you more about the weather or the news, to read you your emails, to play you specific songs on specific smart speakers, to turn on the lights or the TV, and so much more. A note to keep in mind is that this AI assistant technology is software, but it is enabled by a multitude of hardware devices known as Amazon Echo devices.

2. Assets and Security Goals

The way Amazon Echo is setup makes it a gateway that every online transaction and local interaction has to go through, making it a very attractive target to malicious actors and hackers. That is why its main security goal would be confidentiality and integrity of the data that traverses through the device.

In fact, this security goal stems from the assets that Amazon Echo devices bring to the table. And that is its innate feature of being a centralized hub for a person's home and personal needs. As previously mentioned, Amazon Echo devices can be used for a great number of things, such as setting up meetings, alerts, phone calls, or even turning on the A/C or enabling the hot water.

In turn, Amazon Echo devices have the ability to gather so much data, aside from all the sounds that it captures from its surroundings. Some argue that it is a pervasive monitoring device that listens to everything that is being said or done in one's home, and that it pretty much is a surveillance tool for governmental agencies that you yourself paid for. This has created a lot of issues and many debates regarding privacy, which emphasizes the need for information and confidentiality assurance to users.

3. Potential Threats

First, it is always good to consider natural threats as well as accidents such as a fire, earthquake and something as simple as kids, pets or anyone that accidentally breaks device or pushes it over the edge of the shelf.

Now, although the appetite for a malicious threat actor to compromise a particular person's home network might be small, there certainly is a lot to gain from compromising a popular device or service like Amazon Echo. Some malicious threat actors to consider are hacker groups, state-sponsored hackers, terrorists or criminals, as well as Amazon Echo developers. To expand on that last one, the developers have a lot of insights on the technology and might roll out software that contains code vulnerabilities. This might happen due to human error, which is considered a threat, or because the employee is disgruntled or took a bribe to introduce a vulnerability.

Another threat agent could be your neighbor, or anyone that might have access to your home or device.

4. Potential Weaknesses

The most common weakness and the source of most hacks on devices or systems is outdated software. Unpatched systems can usually be easily exploited by attackers, especially in a non-commercial setting where Echo devices would most likely be used.

Additionally, a network intrusion can lead to Amazon Echo devices being compromised, although that would be the least of your concerns if your home network was compromised.

By default, Amazon Echo devices do not have voice recognition capabilities enabled. This allows any person within proximity of your Echo device to give Alexa commands that could potentially be malicious in nature, especially if you have a lot of smart appliances in your home.

5. Potential Defenses

Some defenses require a bit more computer knowledge than others. First, it is of paramount importance to keep all interconnected IoT or smart devices' software and firmware updated. This allows for any unpatched or recently discovered security issues or bugs to be fixed, which reduces the likelihood of exploitation.

Another more advanced defense mechanism would be to subnet your home network by creating a DMZ, and connect all IoT or smart devices, including Echo devices to it. This is considered a risk response strategy, so that in the event a device is compromised, the propagation of any malware or damage is limited to this subnet and does not affect perhaps more important devices. It goes without saying that the networks should be protected by at least WPA2 authentication for passwords that meet best security practices standards.

Additionally, make sure to setup a voice profile in the Alexa app so that you can control who can give Alexa commands.

From a data privacy perspective, the best you can do is go through the Alexa App on your phone and disable any data sharing options and fine-tuning any privacy settings to protect yourself. Aside from that, there evidently is personal data that is stored by the developers of the product (Amazon in this case) on their servers, and it is their responsibility to ensure its confidentiality, integrity and availability.

6. Conclusion

At the end of the day, nothing really is bulletproof from a security perspective, but that doesn't mean you shouldn't wear any Kevlar if there is a chance you might get shot. This analogy entails that there will always be malicious actors looking to leverage and exploit vulnerabilities in IoT or smart devices. However, there are many mechanisms, tasks and strategies that can be employed to minimize security risks. Nonetheless, things can get more complicated when it comes to controversial topics like data privacy, and there are no right answers on how to go about it, just different perspectives and opinions.