APRIL 10, 2018

RISK ASSESSMENT REPORT

514 K

RAVNEET KAUR

RISK ASSESSMENT OF AMAZON ALEXA

Executive Summary

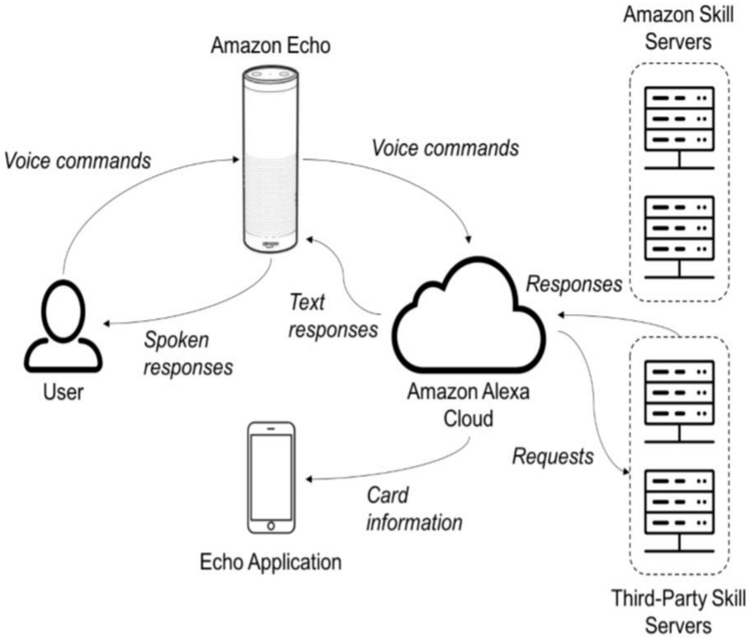
Date: March 25,2018- April 10, 2018

Home automation is exactly what sounds like controlling your house virtually, using a single button or with a single voice command. These devices allow you to control everything from lights and temperature to locks and security of the home. These devices can be operated from anywhere and function even when the person is not present in the home. Every big company is putting thousands of researchers and resources to create such easy-to-use devices with whom people can talk with, namely Apple, Samsung, Google, Microsoft, Amazon etc. These devices are equipped with sensors, actuators, processors, and transceivers, each of which performs individually to provide an integrated intelligent system. One such popular device introduced in 2017 is Alexa, which is virtual assistant developed by Amazon and is first used in Amazon echo and Amazon echo Dot speakers introduced in November 2017. It is capable of music playback, recognizing owner's voice, check the weather, setting alarms, making a to-do list and what not. Its default facilities can be further extended using the third-party app.

This small piece of intelligent technology is a beautiful thing, but like all good things, there are risks. These devices have machine learning algorithms combined with NLP(Natural Language Processing), which are capable of understanding and learning human language. They obviously listen to every command that user gives them, but what else these are listening to? Moreover, Alexa echo doesn't have an activation button to press and is switched on with a single command('echo', 'Alexa', 'Amazon', or, 'Computer'). Alexa is not a complete smart home hub, rather it is an additional interface for your smart home that provides functionality without actually using(virtually). But the number of functionalities it can perform are enormous. These smart home devices are the current interest to the attackers, the adversaries want to hear any personal information so that they can use it to benefit themselves. Anyone who chooses to use this technology has to be extra cautious while operating it.

Many users don't have knowledge regarding the threats these devices possess, along with the ease they provide. Managing the risks associated with Amazon Alexa requires an understanding of the basic understanding of the assets, threats, and vulnerabilities associated with them, along with the identification of countermeasures and mitigation strategies to ensure the security according to CIA(Confidentiality, Integrity, and Availability) traid.

Architecture of Amazon Alexa



The figure specifies the components and the interactions among them, which are discussed as:
2.1 Amazon Alexa: this device accepts user commands and processes the information and gives back the desired results. The request from the user is firstly sent to the cloud from where the response is made to user's query.

2.2 Alexa Cloud: The Alexa cloud receives the audio request from the user and responds back with the results. The cloud is further connected to the server which may be operated by Amazon or any other third- party, to which the cloud communicates to satisfy the user query.
2.3 Amazon Skill Servers: 'Skills' are the tasks that Alexa performs for the user like ordering a pizza, paying credit card bills, checking weather forecast etc. requests are made to these servers by the cloud and follows request-response protocol.

2.4 Third-Party Skill Servers: Other skills are offered by third-party developers, such as a food-ordering application or ride-sharing applications, which are the third-party application with which the functionality of the Alexa is integrated. These are not handled by Amazon and works in a similar manner as Amazon servers.

2.5 Alexa Application: This is an app offered on Android and IOS by the Amazon, through which users can do their Alexa settings, give the feedback and may even give commands to it.

DETAILED ASSESSMENT

1. Introduction

1.1 Purpose

This document provides the various threats posed to smart home device Amazon Alexa, virtual assistant, which is a perfect example of an intelligent system capable of understanding and processing human language. The vulnerabilities, exploits and its countermeasures, security practices/controls that can be adapted to mitigate the risks.

1.2. Scope of this risk assessment

This risk assessment can benefit the targeted audience using the device, the people planning to buy one, and the company 'Amazon' itself so that the threats posed can be reduced. The threats and risks associated with Alexa can be reduced with further upgrades to the device's software, which is based on the correct identification of threats.

1.3. Assumptions and Constraints

The risk assessment of Amazon Alexa requires making certain assumptions about the environment in which it operates.

a. An assumption could be that the cloud stores data in an unencrypted way.

b. The functionality of the third-party servers are unknown.

c. The system under investigation is easily approachable to an adversary.

The major constraint faced is that the detailed architecture and the protocols adopted by the system are unknown.

1.4. Risk Tolerance inputs to Risk Assessment

Risk tolerance is the amount of risk the system can tolerate and still keep functioning. Reversing or mitigating the risk can reduce the damage that would have been there otherwise in case of successful attack. If the risk is not mitigated, the attack vector can cause the loss of reputation and goodwill to the company. The clear functionality of the system is not available and how much risk Alexa can withstand without failure is unknown. Until and unless Alexa starts taking the adversary's commands, it can be assumed that it can withstand any risks until then.

1.5. Rationale for risk-related decisions during the risk assessment process

The rationale behind the risk assessment is done according to the viewpoint of the user of Alexa.

1.5. Uncertainties within the risk assessment process

The risk assessment is done as a part of the academic assignment. The report does qualitative analysis and does not includes quantitative data. The report can serve as the initial step in accessing the risks related to the system where security controls are not effective and the vulnerabilities of the system can be exploited.

2. Risk Assessment Approach

The focus of the approach is to find the adversarial and non-adversarial threats associated with smart home equipment Amazon Alexa. Adversarial threats targets the individuals who aim to exploit the vulnerabilities of the system for their own mean purpose.

2.1 Techniques Used

The initial risk assessment is done using NIST 800-30 guide for conducting risk assessment along with this, the qualitative approach will be used for the purpose of this study assigning nonnumerical categories or levels to the risks encountered (e.g., very low, low, moderate, high, very high). Risks are determined based on adversarial and non-adversarial threats, the likelihood of that threat occurring, known system vulnerabilities and mitigation factors.

Threat Likelihood/Probability

High: The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.

Medium: The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

Low: The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Magnitude of Impact

Very High: The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.

High: The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Moderate: The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Low: The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Very Low: The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

2.2. Assets determination

a. Information collected by the device

b. the owner's location
c. the card information(Debit/Credit)
d. logs information
e. information resource(Music, to do list)
f. stored conversations
g. third- party app data

2.3 Risk Model

NIST publication SP-800-30 proposed risk model is used to perform the risk assessment of Amazon Alexa.

Step 1: Prepare for Assessment
Step 2: Conduct Assessment

- Identify threats
- Identify vulnerabilities
- Determine likelihood and impact to threat
- Determine risk

Step 3: Communicate results
Step 4: Maintain assessment

2.4 Risk Assessment Results

S.No.	Threat	Description	Probability	Impact	Overall	Mitigation
1.	Network Sniffing	Adversary can access the wireless channel from which the Alexa communicated with the cloud to gain sensitive information.	HIGH	HIGH	VERY HIGH	Implementing end-to-end encryption can mitigate this attack
2.	Phishing Attack	Adversary can pretend to be the owner by replaying the messages and gain access to private data	LOW	HIGH	HIGH	Setting up the password with which the Alexa awakes can help fighting this threat.
3.	Insert counterfeit or tampered hardware The Barne's Hack [1]	Wiring the SD card in the Alexa records everything on the device that adversary accesses.	LOW	HIGH	HIGH	Mute the Alexa every time you say something confidential.

4.	Blueborne Attack	Information leak in Android’s Bluetooth Stack	HIGH	HIGH	VERY HIGH	Turn off the Bluetooth when Alexa not in use
5.	Denial of Service	While connected to the internet, this may result in device being temporarily unusable.	HIGH	HIGH	HIGH	Updating the firmware and turning off when not in use can help in mitigating this attack.
6.	Access Permissions	Alexa allows anyone to interact with it, can act upon commands from everyone.	LOW	LOW	VERY LOW	Turn off device when not in use, not allowing everyone to interact with it.
7.	Data loss	Adversary may delete the important notes or data.	HIGH	HIGH	HIGH	Backup of data on other storage medium could prevent data loss.

8.	Data shared with third parties	User’s data is stored and accessed by third-party servers.	HIGH	LOW	LOW	Data should be stored in encrypted form.
9.	Tampering	Attacker may tamper with the data stored on the servers, and may modify it.	HIGH	HIGH	HIGH	Restricted access to the servers help to solve it.
10.	Elevation of Privileges	The attacker is able to access and process and data sent over the network.	LOW	LOW	LOW	Restricted access mechanisms should be implemented.
11.	Information disclosure	An attacker can read the network communication and may use the information against the owner.	HIGH	HIGH	HIGH	End-to-End encryption should be implemented
12.	Data Scavenging attack	Adversary obtains data used and then deleted by organizational	LOW	HIGH	MEDIUM	Restricted access mechanisms may prevent

		processes running in a cloud environment.				this attack
13.	Theft	Stealing the Alexa give full access to user’s information.	MEDIUM	LOW	LOW	Restricted access to the physical boundaries of the device prevents this attack.
14.	Share the location	Alexa is capable of accessing the location where it is placed and once hacked, it can share this information with an adversary	HIGH	HIGH	VERY HIGH	Turning off the location services stops Alexa from accessing the location
15.	Use camera without user’s consent	Alexa can be integrated with third-party camera, and is capable of switching it on and off.	HIGH	HIGH	HIGH	Using third-party apps in integration with Alexa wisely, only the ones that are needed most.

16.	Insecure API’s	The cloud services are accessible from anywhere on the internet, attacker may use it to compromise confidentiality and integrity of user’s data.	HIGH	HIGH	HIGH	Passwords and other integrity controls on the API’s
17.	Identity and credential theft	Alexa stores user’s credit card information and many other sensitive data, which once compromised may incur big financial loss to the user.	HIGH	HIGH	HIGH	Implementing multi-factor authentication adds various layers of security.
18.	Airborne attack	The severe threat posed to Alexa is via airborne attack, using the wi-fi to which it connects to. Adversary may hack or intercept the Wi-Fi communication to carry out attacks.	MEDIUM	MEDIUM	MEDIUM	By setting up password on Wi-Fi, and doing end-to-end encryption can help.

19.	Access to information logs	Alexa stores historical data, which may contain system configuration of various devices integrated with Alexa. Once compromised, attacker may possess control of all the home automation devices integrated with Alexa	HIGH	HIGH	HIGH	Either the user may avoid logging information or protect the logs with cryptographic mechanisms

The results of the risk assessment are summarized below. The overall risk of Amazon Alexa is **HIGH**.

1.	VERY HIGH	3
2.	HIGH	10
3.	MEDIUM	2
4.	LOW	3
5.	VERY LOW	1

REFERENCES

[1] https://www.the-ambient.com/features/weird-ways-echo-can-be-hacked-how-to-stop-it-231

[2] https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/amazon-echo.htm

[3] https://www.coursehero.com/file/p7ieu7vi/The-primary-goals-of-a-security-risk-assessment-are-to-minimize-the-possibility/

Other Sources of Information

[1] Appendix K from NIST 800-30 for conducting Risk Assessment

[2] Tables D1-D8 from NIST 800-30

[3] Tables E1-E5 from NIST 800-30

[4] Tables F1-F8 from NIST 800-30

[5] Tables G1-G5 from NIST 800-30

[6] Tables H1-H4 from NIST 800-30