ECE 518 Project 2

Topic Selected: Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping

Over the recent years, Smart Home appliances have started to take a rise. Of the multiple companies, Amazon and Google are few of the prominent ones which introduced the smart speakers which are often used as communication devices to get information from internet. The devices continue to update through various applications created by different developers. This makes the companies consider the privacy implications since an internet-connected microphone is listening in private environments. There is a potential of malicious voice applications that can abuse the smart speakers using third-party applications similar to installing applications on your smartphone.

Both Amazon Alexa and Google Home are devices that are activated with user invocation after which the specific function is called forth. The research from SRLabs, simulates how 'Smart Spies Attacks' can take place. For third-party voice applications, they show how the companies Review process are limited for the privacy protection. The voice application goes through an initial explicit review process where the application is validated for consumers. After the initial review, the companies did not follow through during application updates. This is a security threat that SRLabs also discuss as a third-party developers and hackers who want to collect personal data cam exploits the initial review process of voice applications with later updates to create their 'Smart Spies.' SRLabs researchers display how the privacy of the user's data can be compromised in two major ways which are eavesdropping and data collection request. The Eavesdropping is leveraged by exploiting the built-in stop intent which reacts to the user's 'Stop' command along with the 'fallback intent' that takes place when the voice application cannot assign the user's spoken command. The data collection is leveraged using the smart speaker's Text-to-Speech that allows inserting long pauses in the speech output. The display how a simple message like "There is an update. Your password is required to install the update." This uses both the exploits mentioned above. While a lot of the exploit does depend on the user's response, with the voice application storing the data in unpronounceable characters like "�. " and silent SSML messages to transfer the data collected back to the hacker/developer.

The security policy for the companies can be improved regarding the data privacy protection. While to prevent spy attacks, the company need to implement a better protection using thorough review process for third-party applications needs to be reviewed during every update and not have the user's data tied to the application. Another approach that can take place is for the voice applications to be processed in a separate voice model which can go through the communications between the third-party application's data request including texts like "password" deserve particular attention or should be disallowed. While the proposed solutions are quick security solutions, I believe there will always be new ways for hackers to try and collect data. I for

one think, hackers trying to decrypt data from application sign-up and for the company to improve its data security can be increasing its data encryption, have the users only use company's domain for confidential data, and have more data monitoring models between third-party applications.