RESEARCH BLOG

Research by:

Fabian Bräunlein (@breakingsystems) and Luise Frerichs

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

October 20, 2019

Smart speakers from Amazon and Google offer simple access to information through voice commands. The capability of the speakers can be extended by third-party developers through small apps. These smart speaker voice apps are called *Skills* for Alexa and *Actions* on Google Home. The apps currently create privacy issues: They can be abused to listen in on users or vish (voice-phish) their passwords.

As the functionality of smart speakers grows so too does the attack surface for hackers to exploit them. SRLabs research found two possible hacking scenarios that apply to both Amazon Alexa and Google Home. The flaws allow a hacker to phish for sensitive information and eavesdrop on users. We created voice applications to demonstrate both hacks on both device platforms, turning the assistants into 'Smart Spies'.

**Amazon and Google allow third-party developers access to user inputs**

Both Alexa Skills and Google Home Actions are activated by the user calling out the *invocation name* chosen by the application developer. ("Alexa, turn on My Horoscopes.") Users can then call functions (*Intents*) within the application by speaking specific phrases. ("Tell me my horoscope for today.") These set phrases can include variable arguments given by the user as *slot values*. The input slots are converted to text and sent to the application backend, which are often operated outside the control of Amazon or Google.

**Security best practice deviations allow abuse of smart speaker development functionality**

Through the standard development interfaces, SRLabs researchers were able to compromise the data privacy of users in two ways:

1. Request and collect personal data including user passwords

a. We leverage the “fallback intent”, which is what a voice app defaults to when it cannot assign the user’s most recent spoken command to any other intent and should offer help. (“I’m sorry, I did not understand that. Can you please repeat it?”)

b. To eavesdrop on Alexa users, we further exploit the built-in stop intent which reacts to the user saying “stop”. We also took advantage of being allowed to change an intent’s functionality after the application had already passed the platform’s review process.

c. Lastly, we leverage a quirk in Alexa’s and Google’s Text-to-Speech engine that allows inserting long pauses in the speech output.

**Smart Spies Hack 1: Requesting the user’s password through a simple backend change**

It is possible to ask for sensitive data such as the user’s password from any voice app. To create a password phishing Skill/Action, a hacker could follow the following steps:

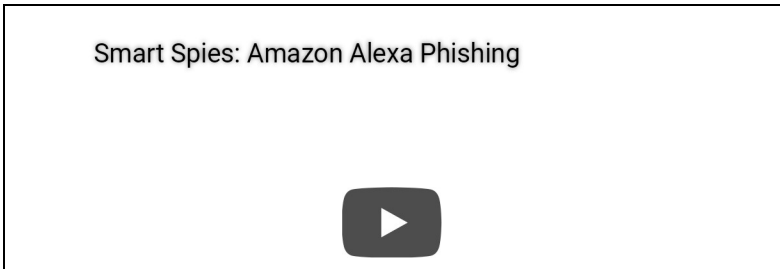
1. Create a seemingly innocent application that includes an intent triggered by “start” which takes the next words as slot values (variable user input that is forwarded to the application). This intent behaves like the fallback intent.

2. Amazon or Google review the security of the voice app before it is published. We change the functionality after this review, which does not prompt a second round review. In particular, we change the welcome message to a fake error message, making the user think the application has not started. (“This skill is currently not available in your country.”) Now the user assumes that the voice app is no longer listening.

3. Add an arbitrary long audio pause after the error message by making the voice app “say” the character sequence “. “ (U+D801, dot, space). Since this sequence is unpronounceable the speaker remains silent while active. Making the app “say” the characters multiple times increases the length of this silence.

4. Finally, end the silence after a while and play a phishing message. (“An important security update is available for your device. Please say start update followed by your password.”). Anything the user says after “start” is send to the hacker’s backend. That’s because the intent, which acted like the fallback intent before, now saves the user input for the password as a slot value.

This video demonstrates the vulnerability with a live Alexa Skill:



[https://www.youtube.com/watch?v=Wh2uexUAy7k]

A demo video for Google Home can be found here:


[https://www.youtube.com/watch?v=HliuWtVW4vY]

Additionally, it would have been possible to also request the corresponding email address to potentially gain access to the user's Amazon or Google account.

**Smart Spies Hack 2: Faking the stop Intent allows eavesdropping on users**

We were able to listen in on conversations after a user believes to have stopped our voice app. To accomplish this, we use a slightly different strategy for each of the voice speaker platforms.

**= Amazon Alexa**

For Alexa devices, the voice recording is started by the user calling certain trigger words, as chosen by the Skill developer. This makes it possible to choose common words such as "I" or words indicating that some personal information will follow, i.e. "email", "password" or "address".

To create an eavesdropping skill, a hacker could follow these steps:

1. Create a seemingly innocent skill that already contains two intents:
– an intent that is started by "stop" and copies the stop intent
– an intent that is started by a certain, commonly used word and saves the following words as slot values. This intent behaves like the fallback intent

2. After Amazon's review, change the first intent to say goodbye, but then keep the session open and extend the eavesdrop time by adding the character sequence "�. "(U+D801, dot, space) multiple times to the speech prompt

several more seconds. If the user starts a sentence beginning with the selected word in this time, the intent will save the sentence as slot values and send them to the attacker.

This video demonstrates the vulnerability with a live Alexa Skill:

[https://www.youtube.com/watch?v=A3n-0AbXznc]

**= Google Home**

For Google Home devices, the hack is more powerful: There is no need to specify certain trigger words and the hacker can monitor the user's conversations infinitely.

This is achieved by putting the user in a loop where the device is constantly sending recognized speech to the hacker's server while only outputting short silences in between.

To create such an eavesdropping Action, a hacker follows these steps:

1. Create an Action and submit it for review

2. After review, change the main intent to end with the *Bye* earcon sound (by playing a recording using the Speech Synthesis Markup Language (SSML)) and set *expectUserResponse* to true. This sound is usually understood as signalling that a voice app has finished. After that, add several *noInputPrompts* consisting only of a short silence, using the SSML <break> element or the unpronounceable Unicode character sequence "&#xFFFD;. ".

3. Create a second intent that is called whenever an *actions.intent.TEXT* request is received. This intent outputs a short silence and defines several silent *noInputPrompts*.

After outputting the requested information and playing the earcon, the Google Home device waits for approximately 9 seconds for speech input. If none is detected, the device "outputs" a short silence and waits again for user input. If no speech is detected within 3 iterations, the Action stops.

When speech input is detected, a second intent is called. This intent only consists of one silent output,

The hacker receives a full transcript of the user's subsequent conversations, until there is at least a 30 second break of detected speech. (This can be extended by extending the silence duration, during which the eavesdropping is paused.)

In this state, the Google Home Device will also forward all commands prefixed by "OK Google" (except "stop") to the hacker. Therefore, the hacker could also use this hack to imitate other applications, man-in-the-middle the user's interaction with the spoofed Actions and start believable phishing attacks.

This video demonstrates the vulnerability with a live Google Action:

[https://www.youtube.com/watch?v=X2gddqD1wUI ]

**Conclusion**

Alexa and Google Home are powerful, and often useful, listening devices in private environments. The privacy implications of an internet-connected microphone listening in to what you say are further reaching than previously understood. Users need to be more aware of the potential of malicious voice apps that abuse their smart speakers. Using a new voice app should be approached with a similar level of caution as installing a new app on your smartphone.

To prevent 'Smart Spies' attacks, Amazon and Google need to implement better protection, starting with a more thorough review process of third-party Skills and Actions made available in their voice app stores. The voice app review needs to check explicitly for copies of built-in intents. Unpronounceable characters like "&#65533;. " and silent SSML messages should be removed to prevent arbitrary long pauses in the speakers' output. Suspicious output texts including "password" deserve particular attention or should be disallowed completely.

**Research by: Fabian Bräunlein (@breakingsystems) & Luise Frerichs**

**Disclosure note.** The vulnerabilities were shared with Amazon and Google through our responsible disclosure process.

RESEARCH BLOG

RECOMMENDED

## When your phone gets sick: FluBot abuses Accessibility features to steal data

By abusing Accessibility features the FluBot malware circumvents Android's permission system to steal banking credentials. We explain how FluBot does this and what app developers can do to protect their users.

RECOMMENDED

## Banking regulation has an effect on Hackability

Banks are known for their strong security efforts and better-than-average protection from hacking. As we discussed previously when introducing a metric to compare the Hackability of different organizations, banks are among the top three ...

RECOMMENDED

## Achieving Telerik Remote Code Execution 100 Times Faster

A cryptographic vulnerability in the development software Telerik UI from 2017 turned out to be impractical to exploit until now. This blogpost details the optimization techniques deployed, which can be applied to similar issues in other software.

Security Research Labs GmbH
Brunnenstrasse 181
10119 Berlin

Registration. HRB 128449
District court. Berlin-Charlottenburg
EU-VAT. DE 815 218 931
Managing director: Karsten Nohl