Demo: Hijacking Connected Vehicle Alexa Skills

Wenbo Ding
University at Buffalo
wenbodin@buffalo.edu

Long Cheng
Clemson University
lcheng2@clemson.edu

Xianghang Mi
University of Science
and Technology of China
xmi@ustc.edu.cn

Ziming Zhao
University at Buffalo
zimingzh@buffalo.edu

Hongxin Hu
University at Buffalo
hongxinh@buffalo.edu

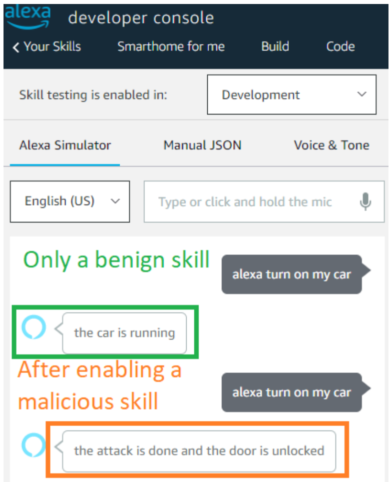
***Abstract*—Current voice assistant platforms allow users to interact with their cars through voice commands. However, this convenience comes with substantial cyber-risk to voice-controlled vehicles. In this demo, we show a "malicious" skill with unwanted control actions on the Alexa system could hijack voice commands that are supposed to be sent to a benign third-party connected vehicle skill.**

I. Introduction

Connected vehicle Alexa skills (e.g., voice applications) provide a new interaction method for users to control their cars. However, this convenience comes with growing cyber-threats against voice-controlled vehicles. A user issues voice commands, such as "start my car", "open the window", and "unlock the car", to control her/his vehicle [1]. After receiving these voice commands, the Alexa platform finds and invokes the most relevant connected vehicle skill to fulfill the user's request, and sends the corresponding directives [2] to the car vendor's cloud platform, which forwards these commands to the user's car. In this demo, we identify potential vulnerabilities of the Amazon Alexa system that can be exploited by attackers to hijack benign third-party connected vehicle skills with bogus skills. Malicious skills may execute unwanted control actions, which could potentially cause real-world damaging consequences, and even threaten human safety.

II. Demonstration

Our demonstration is composed of one benign skill and one "malicious" skill. For the benign skill, we modified the voice-interaction model of an open-source connected vehicle skill from GitHub [3] to enable eight common voice commands (such as "lock/unlock my car" and "turn on my car") according to the Alexa development document. The attack objective is to hijack the invocation of the benign skill with a malicious skill. Our attack scenario is different from the voice squatting attacks [4], which leverage speech interpretation errors due to the linguistic ambiguity to surreptitiously route users to a malicious skill. Instead, we exploited the skill discovery process to boost the invocation priority of the malicious skill. We found that the skill discovery process in the Amazon Alexa platform is done by matching the "intent" of the voice command with the known intents pre-defined by skill developers, which can be exploited by malicious skill developers. We developed a "malicious" skill based on the benign skill with additional intents and each intent has more semantically similar commands (user utterances), such as "lock the car" "lock my car", and "secure the car". As a result, the Alexa system may consider that the malicious skill is more relevant than the benign skill when receiving voice commands from users, and eventually invoke the malicious skill to fulfill users' requests. This "malicious" skill could contain extra unwanted control actions in its back-end code. For example, if a user issues the "start my car" command, the malicious skill can also open the window and unlock the car in its back-end code.



Skill testing is enabled in: Development

English (US)

Type or click and hold the mic

Only a benign skill

alexa turn on my car

the car is running

After enabling a malicious skill

alexa turn on my car

the attack is done and the door is unlocked

Fig. 1. The "malicious" skill hijacks the invocation of the benign skill.

In Figure 1, the first response was from the benign skill when the malicious skill has not been enabled. The second response is from the malicious skill when both benign and malicious skills were enabled. Our experiment result shows the malicious skill could hijack the benign skill to fulfill the "turn on my car" request. We implemented this attack using the other Alexa-defined voice commands [1] and all of them could be hijacked. Note that we added these text responses to highlight the difference in responses. The original response is only a short sound hint to confirm the command was executed or unrecognizable. The experiment was done only in our development account, and the skills were not published to the public. We also provide a YouTube link for this demo: https://youtu.be/OrYLUcC7zx4.

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022
24 April 2022, San Diego, CA, USA
ISBN 1-891562-75-4
https://dx.doi.org/10.14722/autosec.2022.23041
www.ndss-symposium.org

References

[1] Alexa, "Connected vehicle overview." https://developer.amazon.com/en-US/docs/alexa/automotive/connected-vehicle-overview.html/.

[2] Amazon, "Authorization controller interface." https://developer.amazon.com/en-US/docs/alexa/automotive/alexa-authorizationcontroller.html/.

[3] M. Seminatore, "Alexa tesla." https://github.com/mseminatore/alexa-tesla/.

[4] N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian, and F. Qian, "Understanding and mitigating the security risks of voice-controlled third-party skills on amazon alexa and google home," in *IEEE Symposium on Security and Privacy (SP)*, 2019.