Skip to main content

> cs > arXiv:2202.08619

Search... GO

## quick links

- Login
- Help Pages
- About

**Computer Science > Cryptography and Security**

**arXiv:2202.08619** (cs)

*[Submitted on 17 Feb 2022]*

# Alexa versus Alexa: Controlling Smart Speakers by Self-Issuing Voice Commands

Sergio Esposito, Daniele Sgandurra, Giampaolo Bella

Download PDF

We present Alexa versus Alexa (AvA), a novel attack that leverages audio files containing voice commands and audio reproduction methods in an offensive fashion, to gain control of Amazon Echo devices for a prolonged amount of time. AvA leverages the fact that Alexa running on an Echo device correctly interprets voice commands originated from audio files even when they are played by the device itself -- i.e., it leverages a command self-issue vulnerability. Hence, AvA removes the necessity of having a rogue speaker in proximity of the victim's Echo, a constraint that many attacks share. With AvA, an attacker can self-issue any permissible command to Echo, controlling it on behalf of the legitimate user. We have verified that, via AvA, attackers can control smart appliances within the household, buy unwanted items, tamper linked calendars and eavesdrop on the user. We also discovered two additional Echo vulnerabilities, which we call Full Volume and Break Tag Chain. The Full Volume increases the self-issue command recognition rate, by doubling it on average, hence allowing attackers to perform additional self-issue commands. Break Tag Chain increases the time a skill can run without user interaction, from eight seconds to more than one hour, hence enabling attackers to setup realistic social engineering scenarios. By exploiting these vulnerabilities, the adversary can self-issue commands that are correctly executed 99% of the times and can keep control of the device for a prolonged amount of time. We reported these vulnerabilities to Amazon via their vulnerability research program, who rated them with a Medium severity score. Finally, to assess limitations of AvA on a larger scale, we provide the results of a survey performed on a study group of 18 users, and we show that most of the limitations against AvA are hardly used in practice.

Comments: 15 pages, 5 figures, published in Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security (ASIA CCS '22)
Subjects: **Cryptography and Security (cs.CR)**
Cite as: **arXiv:2202.08619 [cs.CR]**
(or **arXiv:2202.08619v1 [cs.CR]** for this version)
https://doi.org/10.48550/arXiv.2202.08619
ℹ Focus to learn more
arXiv-issued DOI via DataCite

## Submission history

From: Sergio Esposito [view email]
**[v1]** Thu, 17 Feb 2022 12:05:09 UTC (596 KB)
● Bibliographic Tools

# Bibliographic and Citation Tools

□ Bibliographic Explorer Toggle
Bibliographic Explorer *(What is the Explorer?)*
□ Litmaps Toggle
Litmaps *(What is Litmaps?)*
□ scite.ai Toggle
scite Smart Citations *(What are Smart Citations?)*

○ Code & Data

# Code and Data Associated with this Article

□ arXiv Links to Code Toggle
arXiv Links to Code & Data *(What is Links to Code & Data?)*
○
Demos

# Demos

□ Replicate Toggle

Replicate *(What is Replicate?)*
□ Spaces Toggle
Hugging Face Spaces *(What is Spaces?)*
○ Related Papers

# Recommenders and Search Tools

□ Connected Papers Toggle
Connected Papers *(What is Connected Papers?)*
□ Core recommender toggle
CORE Recommender *(What is CORE?)*

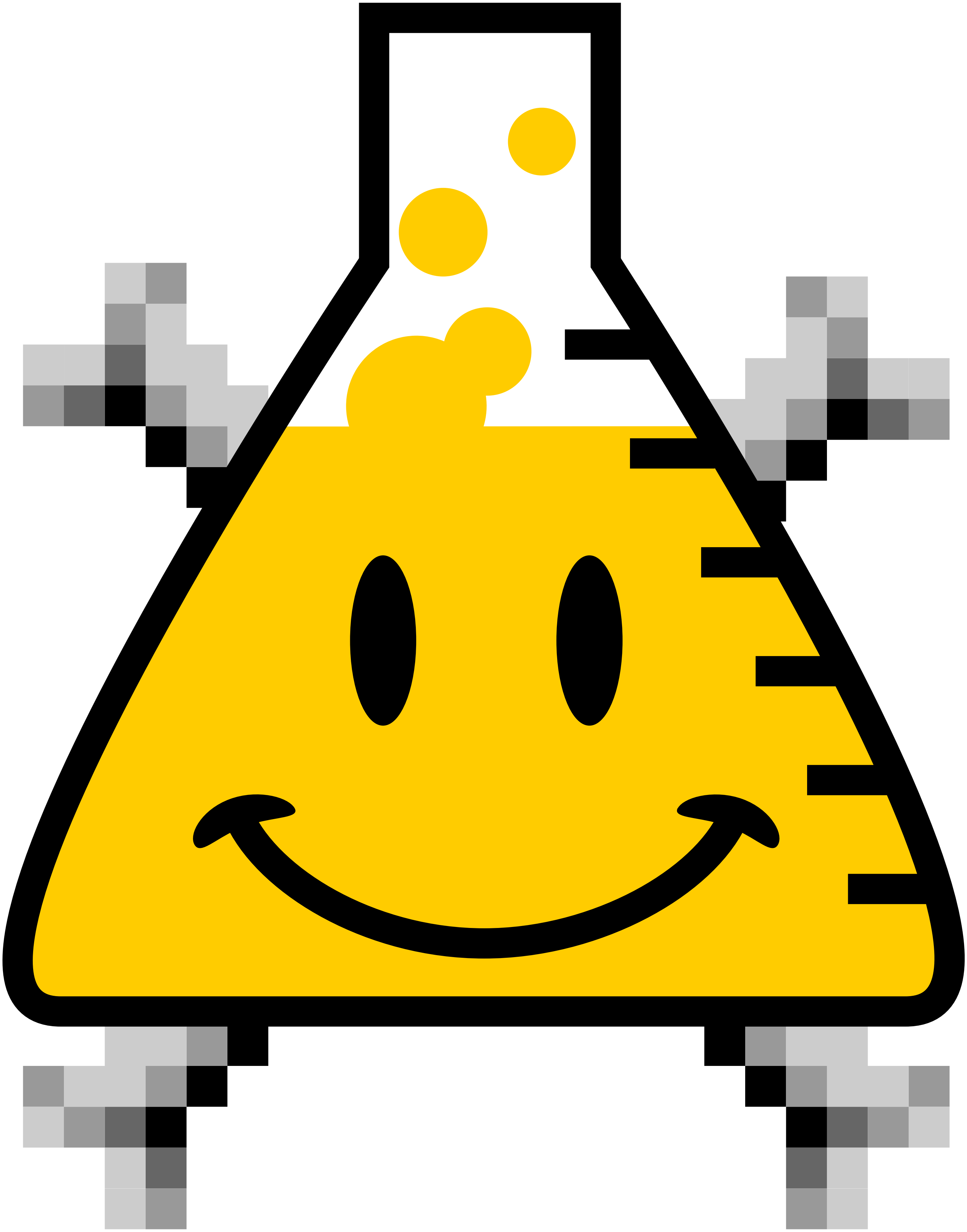
○ About arXivLabs

# arXivLabs: experimental projects with community collaborators

arXivLabs is a framework that allows collaborators to develop and share new arXiv features directly on our website.

Both individuals and organizations that work with arXivLabs have embraced and accepted our values of openness, community, excellence, and user data privacy. arXiv is committed to these values and only works with partners that adhere to them.

Have an idea for a project that will add value for arXiv's community? **Learn more about arXivLabs** and **how to get involved**.



Which authors of this paper are endorsers? | Disable MathJax (What is MathJax?)