# Hey, Alexa, who else is listening right now?

April 28 2020

University of Cincinnati computer scientists are looking at ways to improve security of smart speakers. Credit: Joseph Fuqua II/UC Creative Services

Voice-activated speakers like Amazon's Alexa, Apple's Siri and Google Home are becoming ubiquitous in homes, cars and offices.

These digital assistants make it easy to get travel directions, find a

restaurant's phone number or do a myriad of other daily hands-free tasks. These devices can adjust a home's heating or air conditioning, open locked doors remotely or link to security cameras or baby monitors.

But computer scientists at the University of Cincinnati are investigating potential security weaknesses that hackers could exploit.

"We have millions of smart speakers in our homes these days," said Boyang Wang, assistant professor in UC's College of Engineering and Applied Science.

"People use them every day. It's convenient. On the other hand, we don't have a good understanding of the vulnerabilities they have."

Wang was awarded a two-year National Science Foundation grant for $175,000 to investigate one particular gap that malicious actors could exploit in smart speakers.

"This technology is relatively new. Everyone has the devices, but there hasn't been a lot of research to understand the privacy issues," Wang said.

Wang is an expert in applied cryptography and teaches network security, data security and privacy. He holds several patents on encrypted data and has published extensively on the topic.


More than 157 million smart speakers are in use in U.S. households, according to Mobile Marketer. Credit: Joseph Fuqua II/UC Creative + Brand

In UC's Department of Electrical Engineering and Computer Science, Wang and his students are investigating ways hackers could exploit the devices and potentially steal financial or personal information stored online.

They presented some of their findings last year at the Institute of Electrical and Electronics Engineers' annual conference on communications and network security.

The UC researchers examined a new passive attack on home speakers, called "voice command fingerprinting," in which hackers can eavesdrop

on data transferred between the smart speaker and the cloud server to learn what questions or commands the user gives the device.

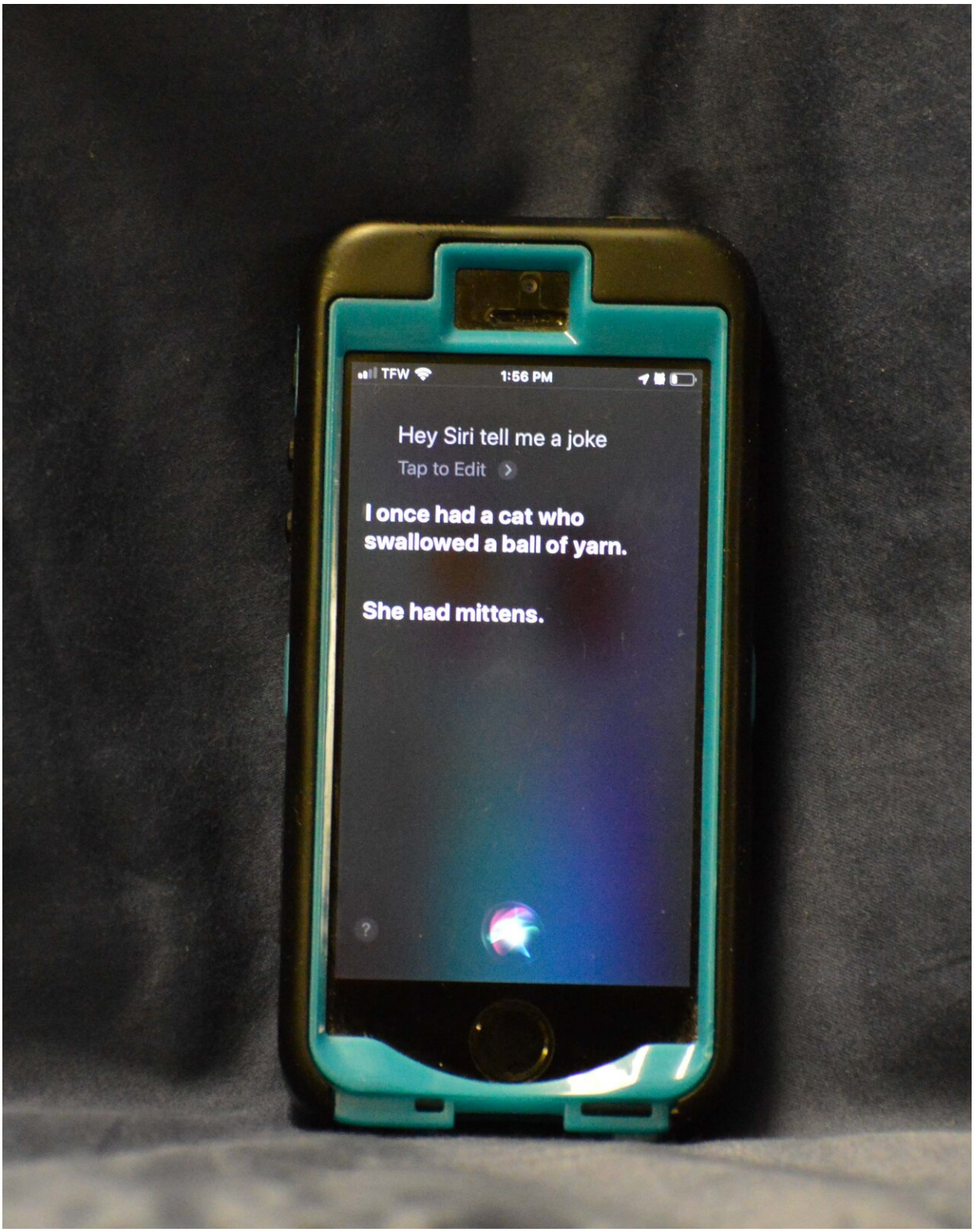
Using machine-learning algorithms, they calculated that with this information alone hackers could correctly infer about one-third of voice commands by eavesdropping on the encrypted network packets the device sends to and receives from the cloud.

## How do they do it?

UC graduate Sean Kennedy and his co-authors built 1,000 traces on an Amazon Echo for 100 common voice commands. The information sent to the cloud each time you ask Alexa for the weather are encrypted. But this data, called a network packet, from each voice command includes predictable traffic patterns like a digital fingerprint, Kennedy said.

"If someone is asking for the weather, that doesn't reveal a lot," Kennedy said. "But if you were able to string together other things someone asks a smart speaker, you could use that to do something else like open a garage door."

Knowing what questions or commands people give can establish a pattern that someone could exploit, Kennedy said.




Smart speakers offer hands-free convenience for consumers. Computer scientists at the University of Cincinnati are looking to improve their security. Credit: UC

"You could imagine a scenario where you would know when someone was leaving their house," Kennedy said.

Kennedy graduated with a master's degree last year. Now he conducts research for Fortune 500 company Leidos at the Air Force Research Lab at Wright-Patterson Air Force Base.

UC researchers found that knowing the size of the encrypted packets alone could help them correctly infer what the user is asking 33% of the time. Wang said their latest study this year using deep learning can improve this predictive accuracy by 81 percent. Pretty sneaky.

Wang said one solution is to disguise these packets by artificially padding all of them with extra harmless but useless data. It's a solution that works well to fool the eavesdroppers, except it creates considerable lag in response time. And nobody wants that, he said.

With the increasing reliance on the internet to manage everything from what's in your refrigerator to what time your alarm clock goes off, security is paramount, Wang said.

Perhaps tellingly, while Wang keeps six or seven smart speakers to study in his UC lab, he doesn't take any home.

"The intentions are good: to provide more services to users to make our lives easier and more convenient," he said. "But from a security and privacy perspective, since we have more devices that are connected, it introduces more challenges and more vulnerabilities."

Provided by University of Cincinnati