LeakyPick

IoT Audio Spy Detector

Richard Mitev, Markus Miettinen, Ahmad-Reza Sadeghi
Technical University of Darmstadt, Germany
William Enck
North Carolina State University, USA
Anna Pazii
University of Paris Saclay, France

Voice Activated Devices?

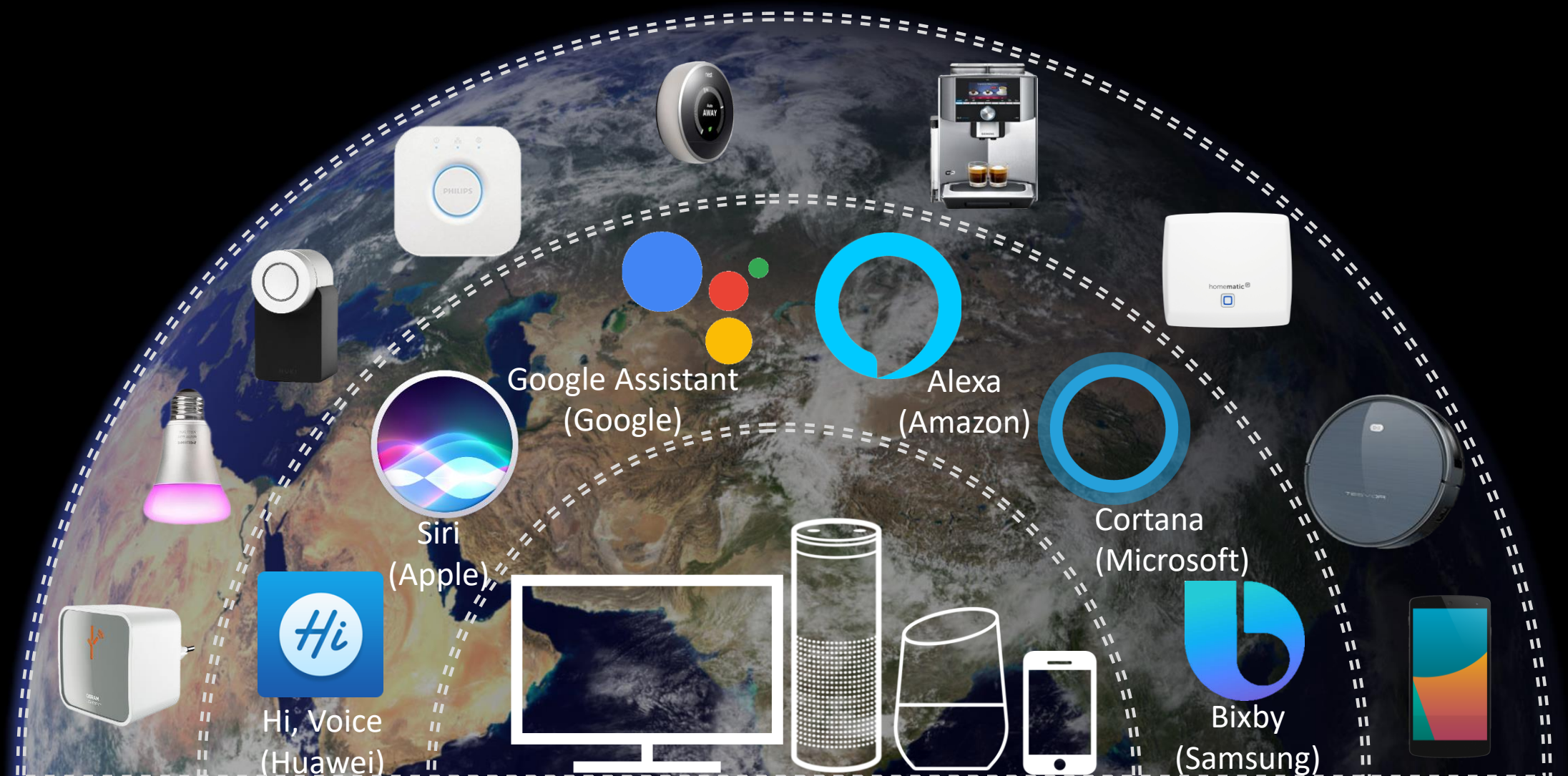
- Amazon alone sold 100M smart speakers equipped with voice assistants
- Assistants can be integrated into any device, e.g., TV, Car, Freezer
- Smart cameras reacting to audio, e.g. start recording
- Smart security systems warning the user of dog barking or glass shattering sounds

Echo Dot

Welcome

360 Hub

Ecosystem of Voice Assistants



Do devices only record when needed?

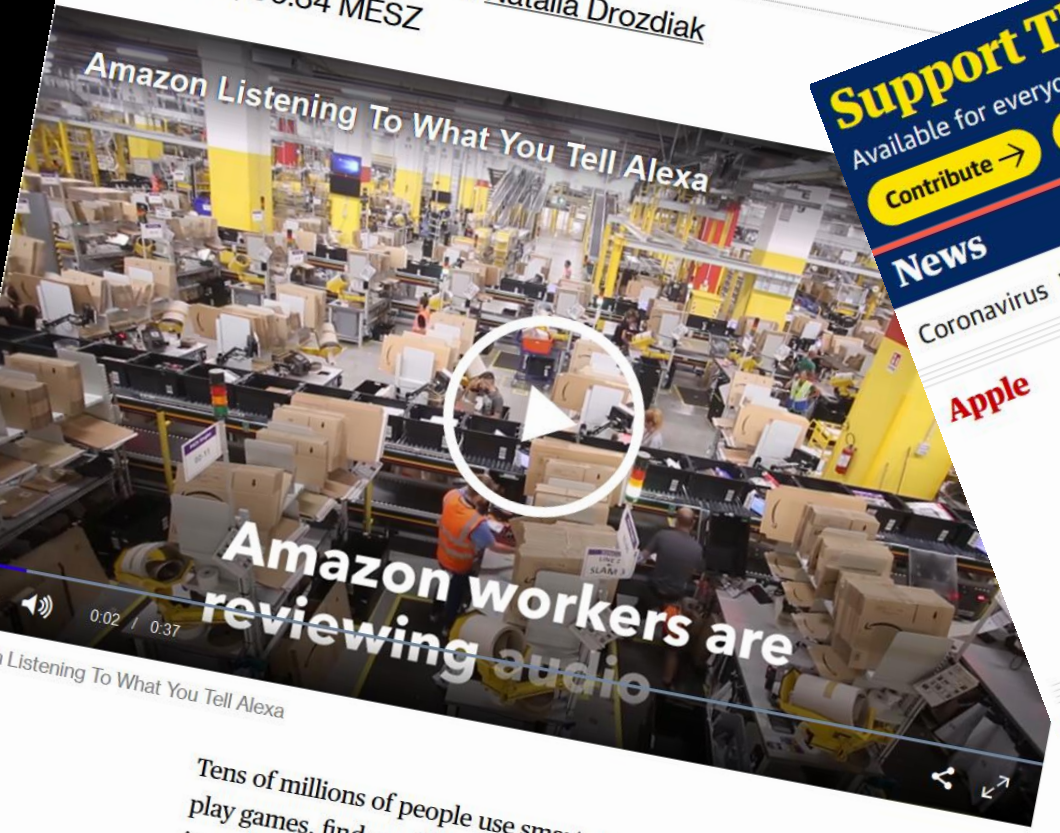
Technology

Bloomberg

Amazon Workers Are Listening to W
You Tell Alexa

A global team reviews audio clips in an effort to help
assistant respond to commands.

By Matt Day, Giles Turner, and Natalia Drozdiak
11. April 2019, 00:34 MESZ



Listening To What You Tell Alexa

Tens of millions of people use smart speakers and their voice software to
play games, find music or trawl for trivia. Millions more
invite the devices and their powerful
concern that someone

Support The Guardian
Available for everyone, funded by readers
Contribute → Subscribe →

Search jobs | Sign in | Search | The Guardian

News | Opinion | Sport | Culture | Lifestyle | More

Coronavirus World UK Environment Science Global development Football Tech Business Obituaries

Apple

This article is more than 1 year old

Apple contractors 'regularly hear confidential details' on Siri recordings

Workers hear drug deals, medical details and people having sex, says whistleblower

rol for Apple's Siri voice assistant. Photograph: Oli

Alex Hern
@alexhern
Fri 26 Jul 2019 17.34 BST

4,006

formation, drug
oviding

Wake Words?

Alexa
Echo
Computer
Amazon

Known Wake-Words

Voice Assistant

Conversation

???
???
???
???

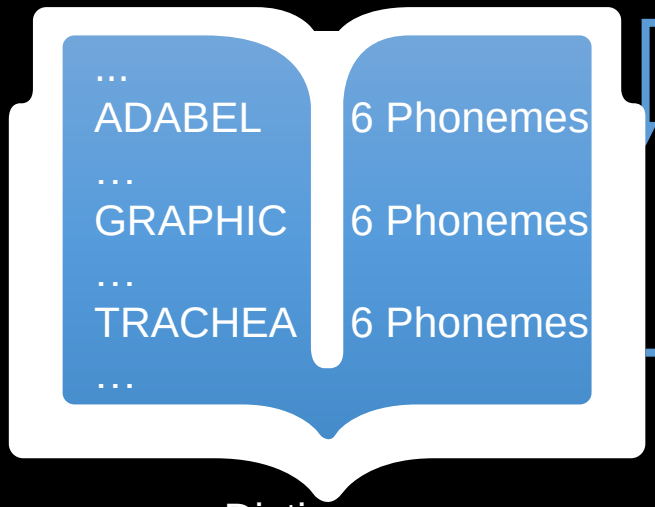
Unknown Wake-Words

Are there other words voice assistants react to?

Wake Words!

ALEXA – 6 Phonemes

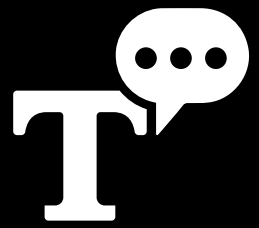
Standard Wake-Word



Dictionary

1. Search for words with similar phoneme count

2. Convert words to audio



Text to Speech

3. Play audio to voice assistant

Cloud

Wake-word detector

4. Model mistakenly recognizes word as wake-word

Voice Assistant

LETTER
GRAPHIC
LECTERN
HYPER

Unknown Wake-Words

Conversation

4. Assistant erroneously starts recording

Why does this happen?

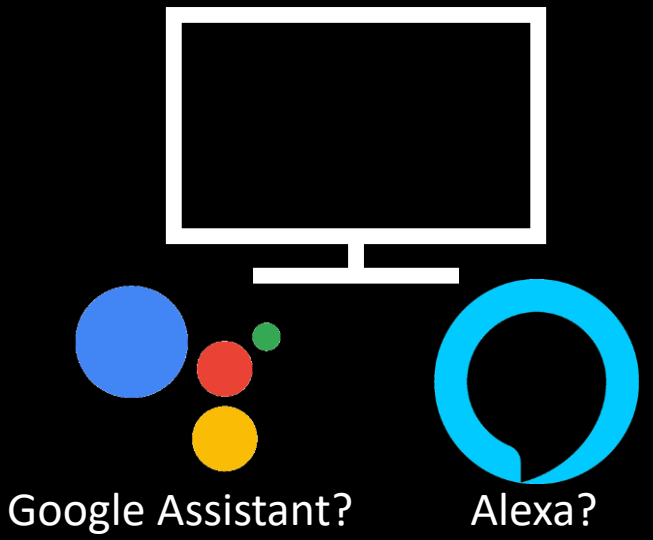
- Voice assistants should be able to activate by everyone regardless of their accent (usability > privacy)
- Wake-word detector is trained using labelled data, which can be erroneous (wrong training data)
- Features of two different sounding words can be similar (feature extraction)

Threat model for our Spy Detector

- Benign IoT devices streaming audio to the cloud in response to a wake-word (e.g., Alexa Smart Speaker)
- “Hidden” or unknown voice assistants incorporated into commodity hardware (e.g., Alexa in a TV)
- Voice assistants also reacting to different wake-words as the one they are intended to

LeakyPick Capabilities

- Identify which devices incorporate a voice assistant reacting to audio
- Identify to which wake-words a voice assistant reacts to by utilizing audio fuzzing
- Detect when a device sends audio to the cloud and warn the user of a possible attack or misrecognized wake-word



Challenges

How can we …

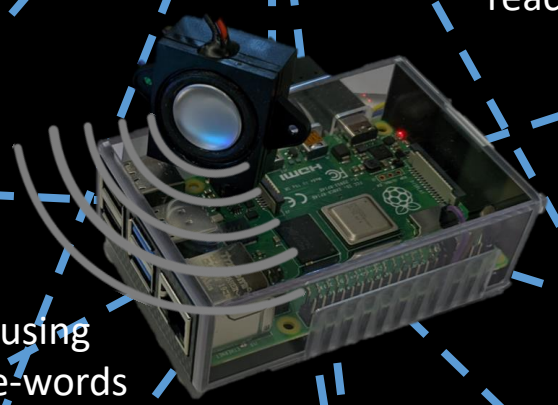
… detect a device reacting to audio if the traffic is encrypted?

… detect reaction to audio in all sorts of previously unseen devices?

Leaky Pick

Home Pod

1. Record statistics from idle traffic using meta data



Leaky Pick Device

2. Audibly probe devices using known and possible wake-words

4. LeakyPick can then inform the user that this device is reacting to audio

Google Home

3. If a device reacts to the word it starts streaming audio to the cloud changing its traffic pattern which will be detected using the t-test

Welcome

Echo Dot

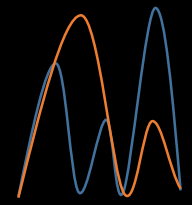
Nest Protect

360 Hub

Presence

t-test on traffic

Extract features (size, time) over time



Idle traffic of devices

Devices changes network behavior when probed

Leaky Pick Device

Warn the user

Compare time series using t-test

Evaluation

- Evaluated on multiple variants of Alexa Smart Speaker, Netatmo, Google Home, Siri Home Pod, Nest and Hive devices.
- Identified 89 words that could unknowingly trigger an Amazon Echo Dot to transmit audio to the cloud
- Accuracy of 94% in detecting audio transmissions from eight different devices equipped with microphones without any a priori training

Leaky Pick Device