

# RSA<sup>®</sup>Conference2018

San Francisco | April 16 – 20 | Moscone Center



#RSAC

SESSION ID: MBS-T07

## THE GOOD, THE BAD, AND THE UGLY OF THE ULTRASONIC COMMUNICATIONS ECOSYSTEM

**Vasilios Mavroudis**

Doctoral Researcher  
University College London  
@mavroudisv



**Giovanni Vigna**

Professor UC Santa Barbara  
Lastline Co-founder  
@giovanni\_vigna



# Who We Are



## **Vasilios Mavroudis**

Doctoral Researcher, UCL

## **Shuang Hao**

Assistant Professor, UTDallas

## **Yanick Fratantonio**

Assistant Professor, EURECOM

## **Federico Maggi**

Senior Researcher, Trend Micro

## **Christopher Kruegel**

Professor UCSB

Co-founder of Lastline

## **Giovanni Vigna**

Professor UCSB

Co-founder of Lastline

## **Lara**



# How it All Started



- 10/2012: SilverPush is founded
- 04/2014: SilverPush funded by Unilazer, IDG Ventures & others
- 06/2014: Articles cover their tracking framework



US 20150215668A1

(19) **United States**

(12) **Patent Application Publication**  
**Chawla**

(10) **Pub. No.: US 2015/0215668 A1**  
(43) **Pub. Date: Jul. 30, 2015**

(54) **METHOD AND SYSTEM FOR  
CROSS-DEVICE TARGETING OF USERS**

*H04N 21/234* (2006.01)  
*H04H 60/58* (2006.01)  
*H04N 21/81* (2006.01)

(71) Applicant: Silveredge, Inc., Redmond, WA (US)

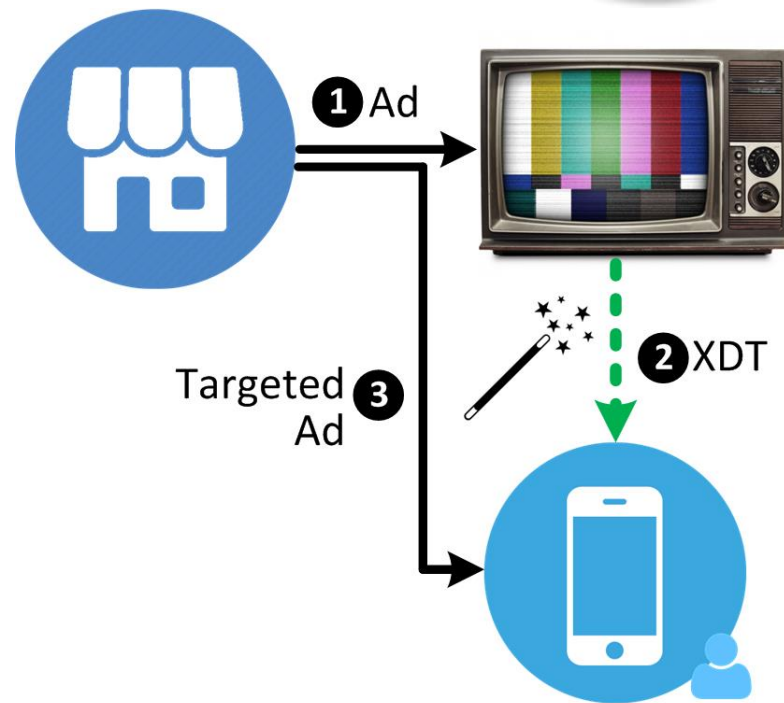
(52) **U.S. CL.**

# Cross-Device Tracking



*John has just watched a TV ad and is now browsing the Internet from his smartphone. The advertiser now is pushing relevant (e.g., follow up) ads to his smartphone.*

*Holy grail of marketers, allows them to track the user's activities across different devices.*





# How It All Started



- 10/2012: SilverPush is founded
- 04/2014: SilverPush funded by Unilazer, IDG Ventures & others
- 06/2014: Articles cover their “ultrasound” tracking framework
- **11/2015: The security community and the press notice**

# How It All Started



**From:** Lukasz Olejnik (W3C) <[lukasz.w3c@gmail.com](mailto:lukasz.w3c@gmail.com)>

**Date:** Thu, 12 Nov 2015 21:18:06 +0000

**Message-ID:** <CAC1M5qqt21Ddw0U8EmbikYNE42DBYjN-pjqERYiOSQsBGdBPDQ@mail.gmail.com>

**To:** "public-privacy (W3C mailing list)" <[public-privacy@w3.org](mailto:public-privacy@w3.org)>, [public-audio@w3.org](mailto:public-audio@w3.org)

Dear all,

I would like to raise the current issue of tracking using ultrasound audio beacons/markers.

**SilverPush** PRISM [1] is a program/method enabling cross-device tracking. In short, it is the association of users of desktops/laptops with devices such as smartphones. The intention is to enhance tracking and profiling, so users can experience more rich Web content, of course.

It supposedly uses ultrasound beacons via speakers, emitted by scripts on websites. These can then be detected by smartphone apps.

It is, however, bringing some transparency issues. Users are unaware of this, can't provide consent, and can't configure their browsers according to their expectations.

The current privacy considerations of Web Audio API [4] are not addressing these concerns. Possibly we should ask for an update?

We might consider investigating, and deciding - if possible - should Web Audio:

- be subject of permissions
- limit the output to filter out infra/ultrasound, if possible (?)
- have an additional note

Thanks and regards  
Lukasz

# How It All Started



Beware of ads that use inaudible sound to link your phone, TV, tablet, and PC

**Startup uses ultrasound chirps to covertly link and track all your devices**

ADVERTISERS ARE USING INAUDIBLE NOISE TO FIGURE OUT WHAT DEVICES ARE YOURS

Cross-Device Tracking: a privacy invasive tracking method

Ad tracking tech uses high-frequency audio to communicate between devices

# How It All Started



- 10/2012: SilverPush is founded
- 04/2014: SilverPush funded by Unilazer, IDG Ventures & others
- 06/2014: Articles cover their “ultrasound” tracking framework
- 11/2015: The security community and the press notice
- **03/2016: The Federal Trade Commission takes action**



# How It All Started



#RSAC



Bureau of Consumer Protection

UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION  
WASHINGTON, D.C. 20580

[date]

BY ELECTRONIC MAIL

[App Developer]

Dear Sir or Madam:

You currently offer a mobile application for download in the Google Play store. We are writing to you today because of code included in the application that may allow third parties to monitor consumers' television viewing for ad targeting or analytics.

We recently discovered that your mobile application “ ” includes a software development kit created by the company Silverpush. Silverpush makes available for application developers a “Unique Audio Beacon” technology that enables mobile applications to listen for unique codes embedded into television audio signals in order to determine what television shows or advertisements are playing on a nearby television. This functionality is designed to run silently in the background, even while the user is not actively using the application. Using this technology, Silverpush could generate a detailed log of the television content viewed while a user’s mobile phone was turned on.

# How It All Started



- 10/2012: SilverPush is founded
- 4/2014: SilverPush funded by Unilazer, IDG Ventures & others
- 6/2014: Articles cover their ultrasound tracking product
- 11/2015: The security community and the press notice
- 3/2016: The Federal Trade Commission takes action
- **3/2016: SilverPush claims no active partnerships in the US**

# How It All Ended



- Assumed to be an isolated security incident
- A “poor” company that believed security is optional
- Very little became known about the technology used
- Press moved on
- People went quiet



**RSA**Conference2018



#RSAC

**WHY THIS TALK IS NOT OVER**



# Open Questions



- Why ultrasounds? NFC, Bluetooth, BLE, Wifi?
- How did the Silverpush app work?
- Other ultrasound-enabled products?
- How about Security?
- How about Privacy?

# Ultrasonic Communications Use Cases



- Device Onboarding
- Realtime Group Building
- Realtime Data Sharing
- Proximity Verification
- Third Screen Interactivity
- Offline Connectivity
- Vehicle Connectivity
- Authentication
- P2P Payments
- App to App Connectivity
- Embedded IoT Connectivity
- Machine 2 Machine Connectivity
- Internet Of Sound\*

# Why Use Ultrasounds?



- Inaudible to humans
- Can be emitted by most commercial speakers
- Captured by most commercial microphones



# Ultrasonic Packets & Beacons



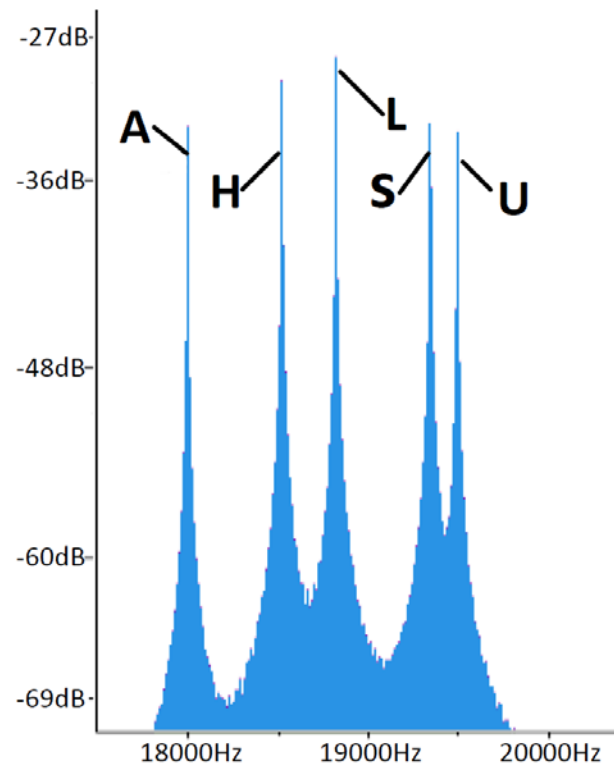
- Lie at the core of all ultrasound-enabled products
- Max reported bitrate 1kbps (unknown distance)
- Common frequency spectrum 18-20kHz
- No uBeacon or uPacket standard
- Encoding varies between companies
- Lots of patents



# Silverpush Beacons





- 5-6 Characters-long
- Spectrum: 18-20kHz
- Divided in smaller ( $\sim 75\text{Hz}$ ) chunks
- Each one corresponds to a symbol
- Duration of only few seconds ( $\sim 4$ )

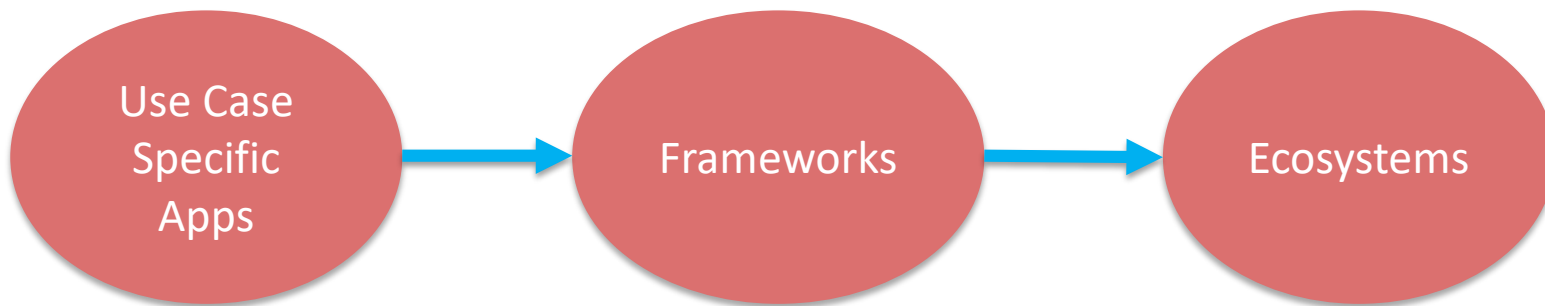




- Focused on sending messages directly over near-ultrasonic audio
- The payload can be an arbitrary array of bytes
- Max length is 10 Bytes
- Used by Google Nearby
- Native Android support

1. Open your device's Settings app .  
2. Tap **Google** > **Nearby** > Settings .

# Evolution



# Use Case-Specific Apps



- Silverpush, Cross-device Tracking (Not in US/EU)
- Shopkick, Shopping rewards (BLE now)
- CUE Audio, Ultrasonic Synchronization
- Signal 360, Proximity Marketing

## Security Key Points:

- Novel Use Cases → No best practice consensus
- Highly competitive timeframes → No time for security
- Limited Emission range → “No need for security” fallacy





- *Lisnr*: Near-ultrasonic Protocol
- *Chirp*: Data over Sound

## Security Key Points:

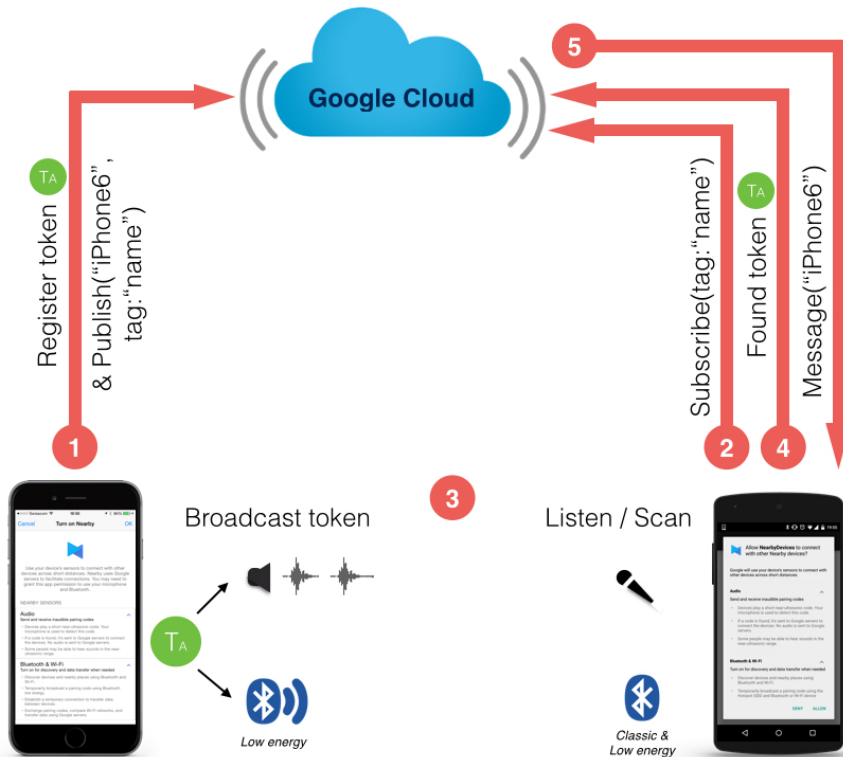
- Replay attack protection
- Ciphers, Techniques etc not public
- We bring the bitrate-Bring your own security

# Ecosystems



One to rule them all:

- Google Nearby
  - ❖ Nearby Messages
  - ❖ Nearby Connections
  - ❖ Nearby Notifications
- Pre-installed with Android
- Also uses Bluetooth and Wifi
- Ultrasounds as beacons



*How Google Nearby.Messages works?*



## SECURITY?



**Beacon-injection:** Pushes beacons into nearby ultrasound-enabled devices

*Example*

Attacker equipped with a simple beacon-emitting device (e.g., smartphone) walking into Starbucks at peak hour. As a result, all customers with an ultrasound-enabled app installed on their devices will be receiving the beacons and unknowingly forward them to the service provider's backend.

**Beacon-replay**

- Variation of beacon-injection
- The adversary captures and replays existing beacons



# The Shopkick Incident





## PRIVACY ATTACK DEMO

# Setting a Surveillance Scene



- A whistleblower wants to leak documents to a journalist
- The journalist is coerced to de-anonymize him
- The whistleblower takes precautions and uses only Tor
- The journalist asks the whistleblower to upload the documents to a Tor hidden service that he owns
- The whistleblower fires up Tor and loads the page...

A person is sitting at a wooden desk in a dimly lit room, possibly a cafe. They are holding a smartphone in their right hand and a coffee cup in their left hand. A laptop is open on the desk to their right, displaying a webpage. The background is blurred, showing shelves with various items.

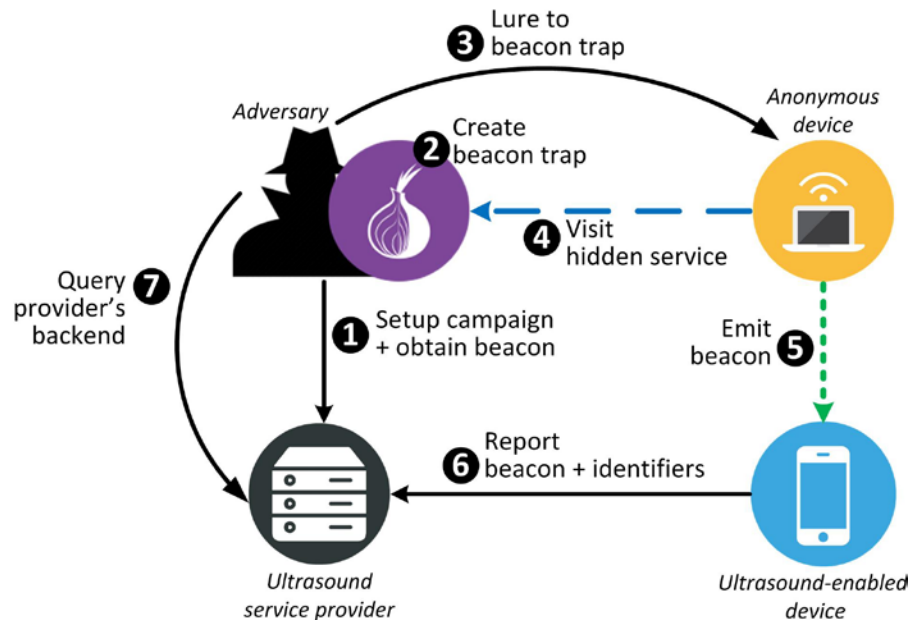
# Tor Deanonimization

with ultrasound beacons

# The Tor De-Anonymization Attack



1. Adversary starts a campaign
2. Embeds the uBeacon in a Tor hidden service
3. Lures the user to visit it
4. User loads the resource

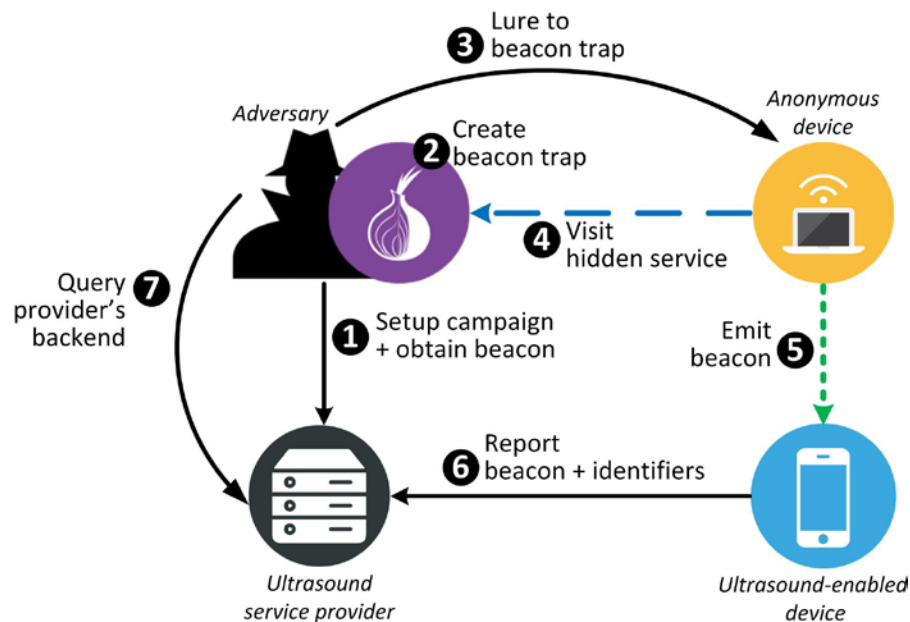




# The Tor De-Anonymization Attack



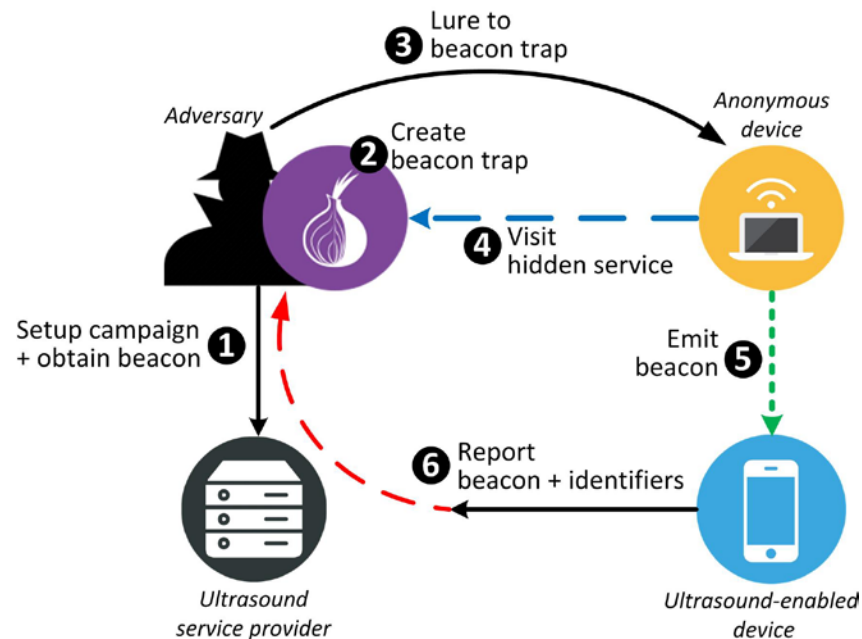
5. His laptop emits the uBeacon
6. His smartphone picks it up and reports it back to the tracking provider
7. State level adversary simply subpoena's the provider for the IP or other identifiers



# The Tor De-Anonymization Attack



- We didn't have a state-level adversary handy
- Redirected traffic from steps 6 to the adversary's backend



# The Tor De-Anonymization Attack



## AT&T SPYING PROGRAM IS ‘WORSE THAN SNOWDEN REVELATIONS’

To gain access to the Hemisphere program, authorities pay anything between \$100,000 and millions of dollars. Only an administrative subpoena is required to access it, which does not need to be obtained by a judge.

In response to this week’s revelations, AT&T issued the following statement: “Like other communications companies, if a government agency seeks customer call records through a subpoena, court order or other mandatory legal process, we are required by law to provide this non-content information, such as the phone numbers and the date and time of calls.”

# More Attacks



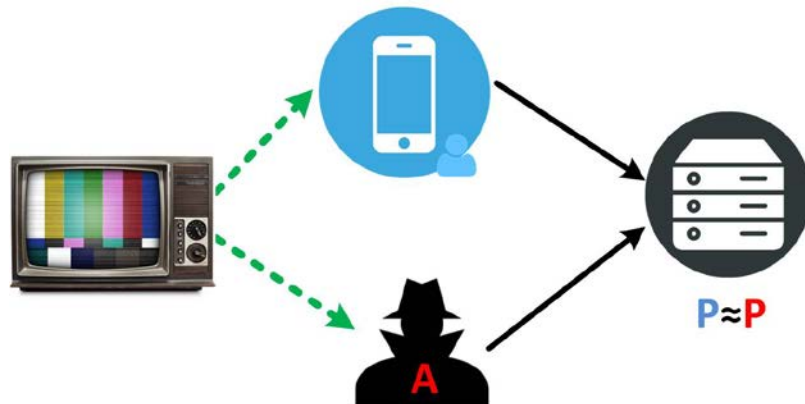
## *Profile Corruption*

- Advertisers love user profiling (e.g., on interests, behavior)
- *Beacon-injection* can be used to pollute the ad profile of the users



## *Information Leakage Attack*

- Make his profile identical to the victim's
- Causes a leakage of the victim's interests
- Depends on the profiling techniques used by the tracking provider







## POST-MORTEM





## *Inaccurate Threat Model*

- Security relies on the limited transmission range of ultrasounds
- Assumes no physical proximity of an attacker
- Assumes no one would be able to capture and replay beacons

However:

- Ultrasounds can travel reliably for a few meters
- There are ways to get “virtually” close

# Security Evaluation



## *Authentication and Encryption*

- Replay and Injection attacks
- No documentation on algorithms used

## Use Case Constraints:

- Relatively low bandwidth
- Limited time
- Noisy environment



## *Violation of the principle of least privilege*

- Ultrasound-based apps need full access to the microphone
- Unnecessary access to all audible frequencies
- Malicious developers could misuse their access to the mic
- Ultrasound-enabled apps can be perceived as malicious by the users

## *Lack of Transparency*

- Large discrepancies in informing the users
- Opt-out options vary too

**RSA**Conference2018



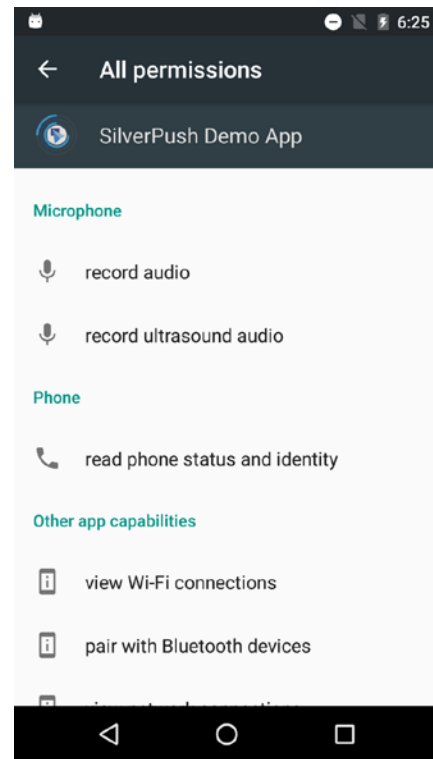
#RSAC

## MITIGATION

# Android Permission



- Patch for the Android permission system
- Finer-grained control over the audio channel
- Separate listening permissions for the audible and ultrasonic spectrum
- Selectively filter out ultrasound frequencies out





# Browser Extension



*Filters all audio sources and removes all ultrasounds while leaving all audible frequencies intact*

- Uses the Web Audio API, HTML5
- Attenuates frequencies above 18kHz



SilverDog



## Filter Settings

Filter Type:

Highshelf ▼

Frequency:

18000

Gain:

-70

Q:

0

[Filter Documentation 1](#)

[Filter Documentation 2](#)

Save

Reset

# We Need Standards!



Immediate benefits:

- OS-level APIs (manufacturer independent!)
- Functionality for discovery, processing, and emission
- New permission for this API
- No need to access the microphone
- Ultrasound-enabled apps will not risk being considered as “spying”

**RSA**Conference2018



#RSAC

## TAKEAWAYS

# Takeaways



- Ultrasounds is another communication channel
- No standards to comply with
- No common packet format (“proprietary technology”)
- You’ll have to do your own audits
- It’s becoming popular, and you’ll likely encounter it



If your product designers want to use it:

- Make sure they really need it
- Consider your adversarial model carefully
- Try to see if an ecosystem (e.g., Nearby) works for you
- If not, pick a framework and use proven crypto



# Takeaways



## Sanity-Checks for everyone:

- Do we have any air-gapped systems that could be affected?
- Any PCs with disabled USBs?
- Users can use ultrasounds to transfer data in-and-out of the system
- Any privacy attacks that may affect your users?

**RSA**Conference2018



#RSAC

**THANK YOU!**