On the Privacy and Security of the Ultrasound Ecosystem

Vasilios Mavroudis
Doctoral Researcher UCL

uBeacSec.org

The Story of a Product

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

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

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

(52) **U.S. Cl.**

The Story of a Product

- 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**

From: Lukasz Olejnik (W3C) <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>, 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

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

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

Cross-Device Tracking: a privacy invasive tracking method

The Story of a Product

- 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**

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

Bureau of Consumer Protection

[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.

The Story of a Product

- 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
- 11/2015: The Federal Trade Commission takes action
- 11/2015: The users react
- 3/2016: The Federal Trade Commission takes action
- **3/2016: SilverPush claims no active partnerships in the US**

The end of our Story?

- It was assumed to be an isolated security incident
- Very little became known about the technology used
- Press moved on
- People went quiet

Wait! What was that?!

- Why they were using ultrasounds?
- How do such tracking frameworks work?
- Other ultrasound-enabled products?
- How about Privacy and Security?

Who we are

Vasilios Mavroudis
PhD Student UCL

Shuang Hao
Post-doc UCSB

Yanick Fratantonio
PhD Student UCSB

Federico Maggi
Assistant Professor POLIMI
Visiting Researcher UCSB

Christopher Kruegel
Professor UCSB
Co-founder of Lastline

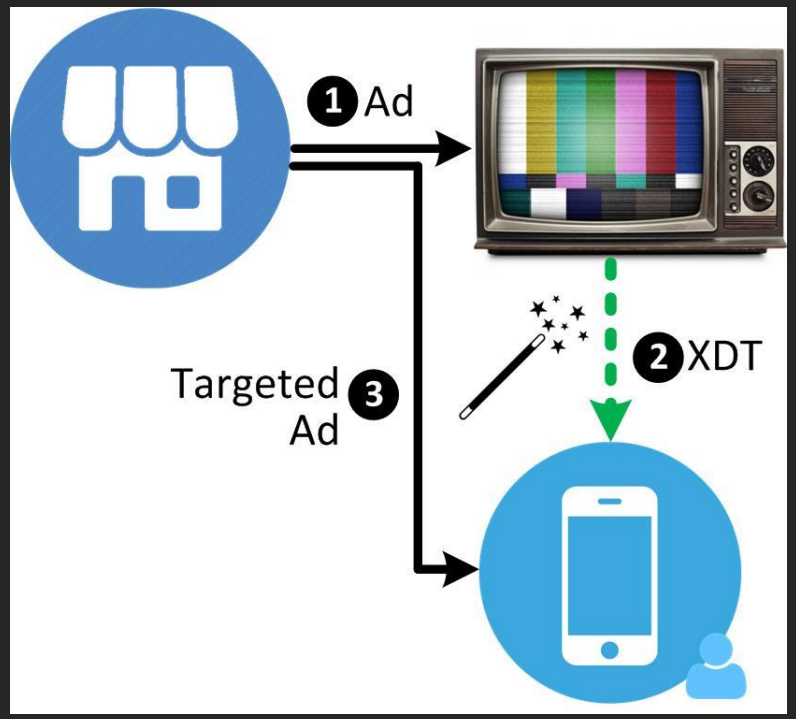
Giovanni Vigna
Professor UCSB
Co-founder of Lastline

Vasilios is supported by H2020 PANORAMIX Grant (ref. 653497)

Cross-Device Tracking

Example:

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.

Cross-Device Tracking

- Employed by major advertisement networks
- Varying degrees of precision: Deterministic or Probabilistic

Deterministic Example:

- Shared account across all devices
- Suitable for platforms where users are incentivized to login
- Inapplicable in most cases
- Hence alternatives are sought

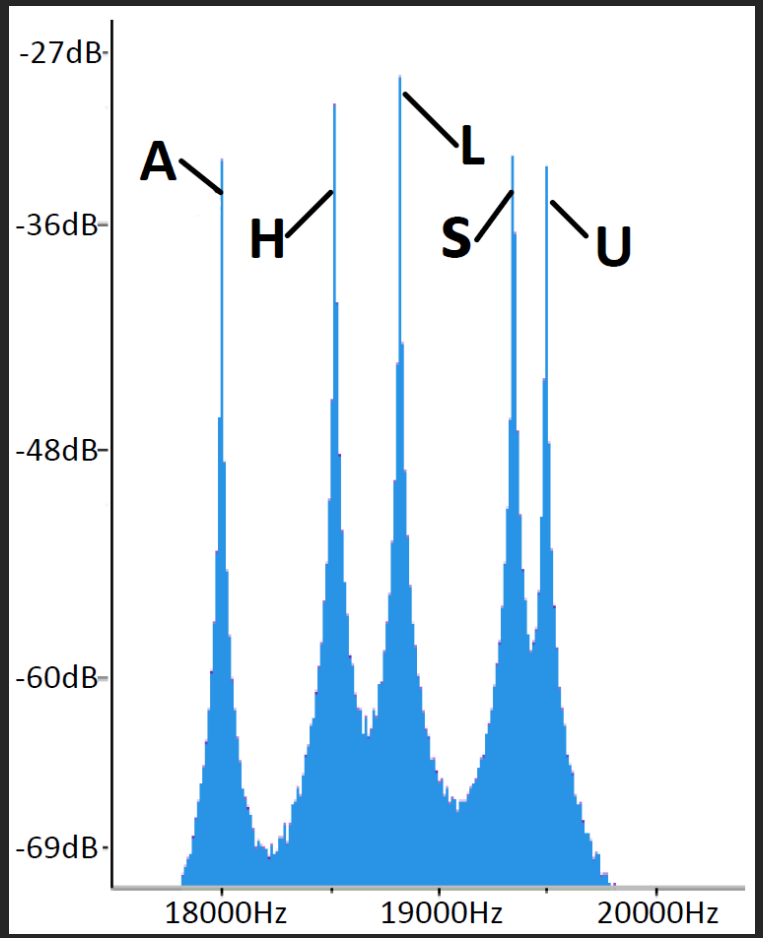
Ultrasound Beacons: uBeacons

- uBeacons lie at the core of all ultrasound tracking products
- High-frequency audio “tags”
- Encode a small sequence of symbols

- Can be emitted and captured by most commercial speakers and microphones
- Inaudible by humans

uBeacons: Technical Details

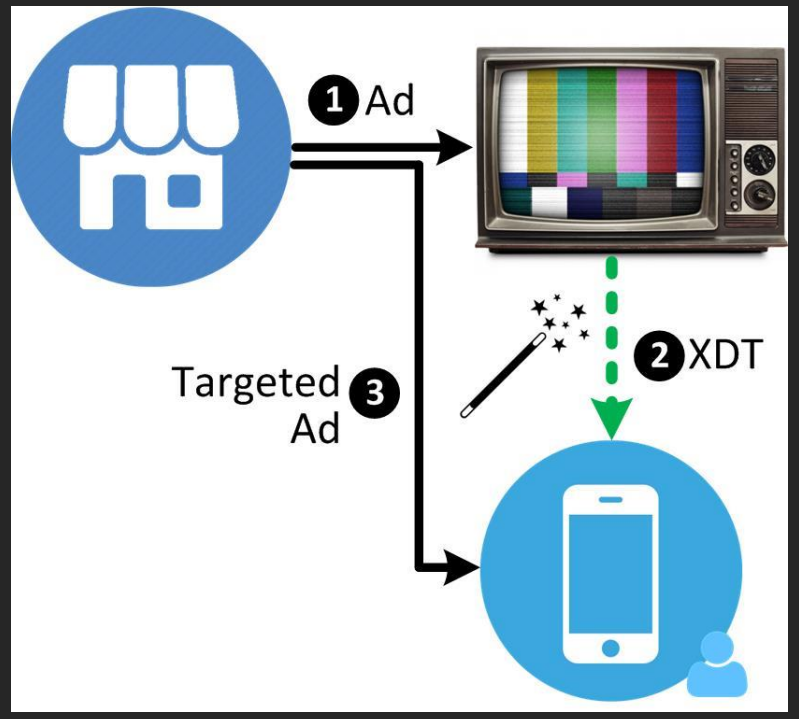
- The spectrum between 18kHz & 20kHz
- Divided in smaller (~75Hz) chunks
- Each one corresponds to a symbol
- Duration of only few seconds (usually ~4)
- No uBeacon standard
- Encoding varies between companies
- Lots of patents



XDT + uBeacons = uXDT

Ultrasound Cross-Device Tracking

- Offers very high tracking accuracy
- Based on uBeacons embedded into websites or TV ads
- Requires an uXDT framework installed on the user's mobile device
  - Loyalty/Brand apps
  - Advertising SDKs

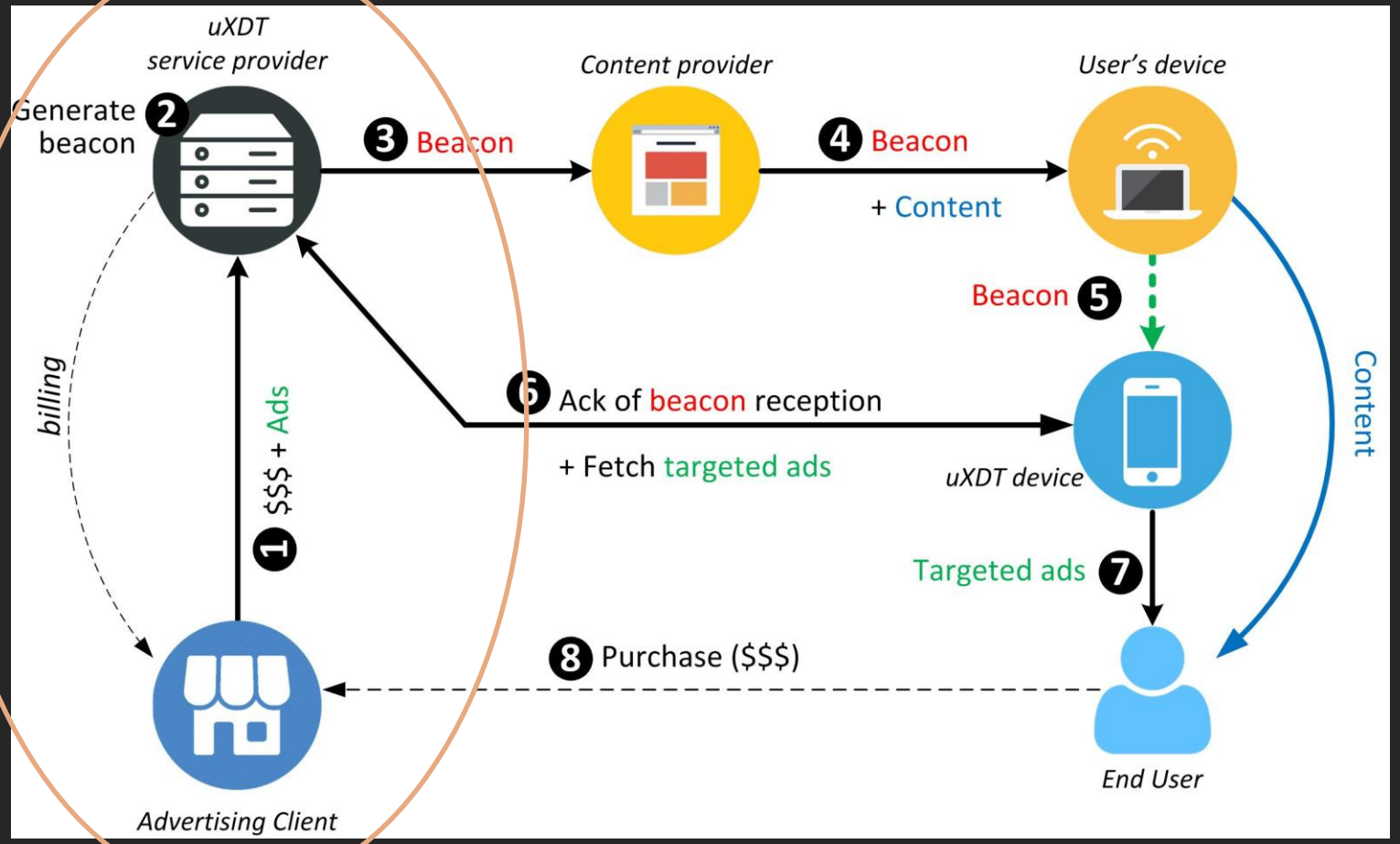


Ultrasound Cross-Device Tracking

1. The *advertising client* starts a new advertising campaign with the *uXDT provider*

2. The uXDT provider generates a unique u*Beacon* and associates it with the client's campaign

3. uBeacon is incorporated in the publishers' content

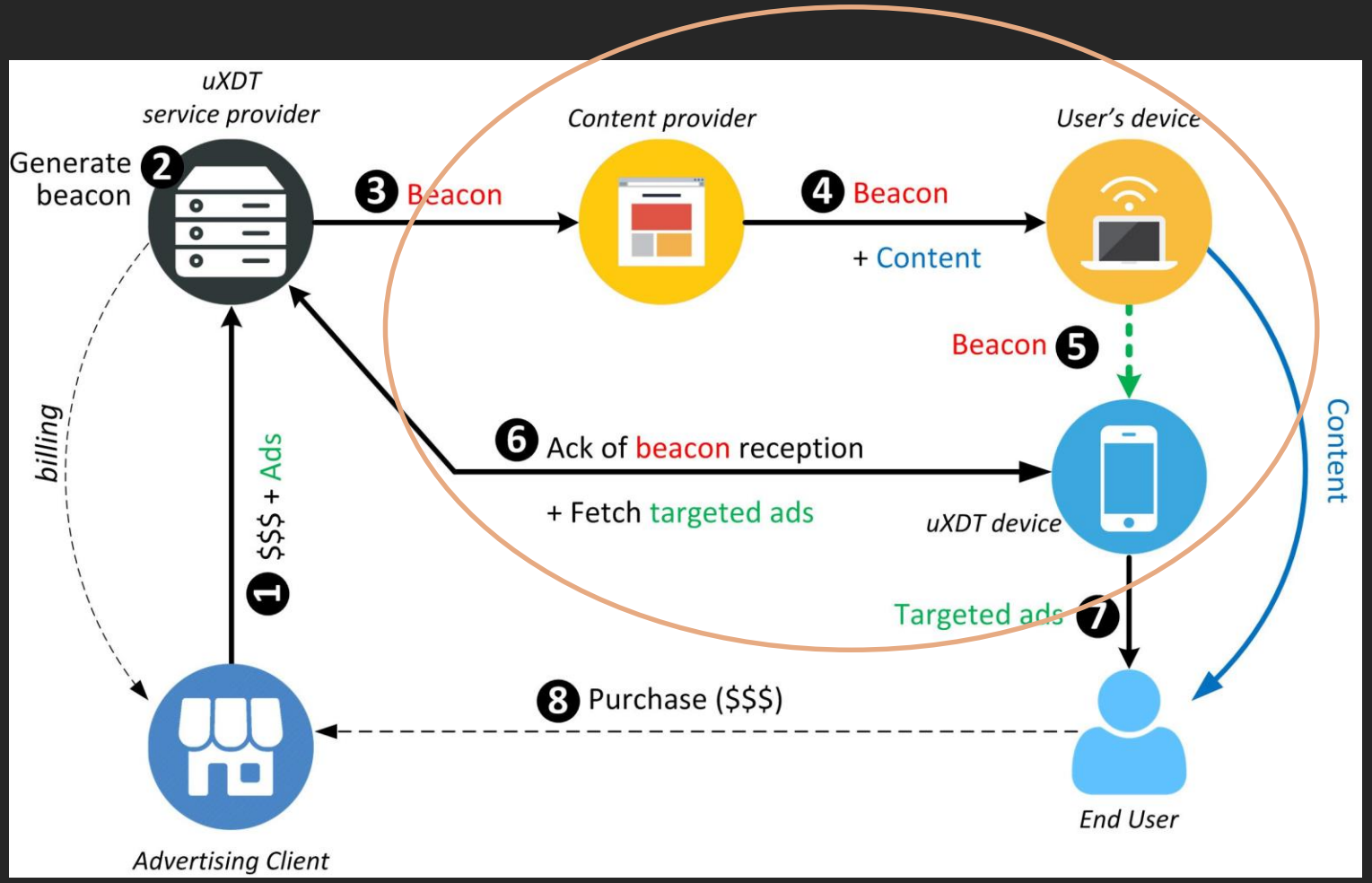


Ultrasound Cross-Device Tracking

4. The user accesses the content using one of his devices

5. Once the content is loaded the beacon is emitted through the device's speakers

6. The uXDT framework reports the beacon to the uXDT service provider

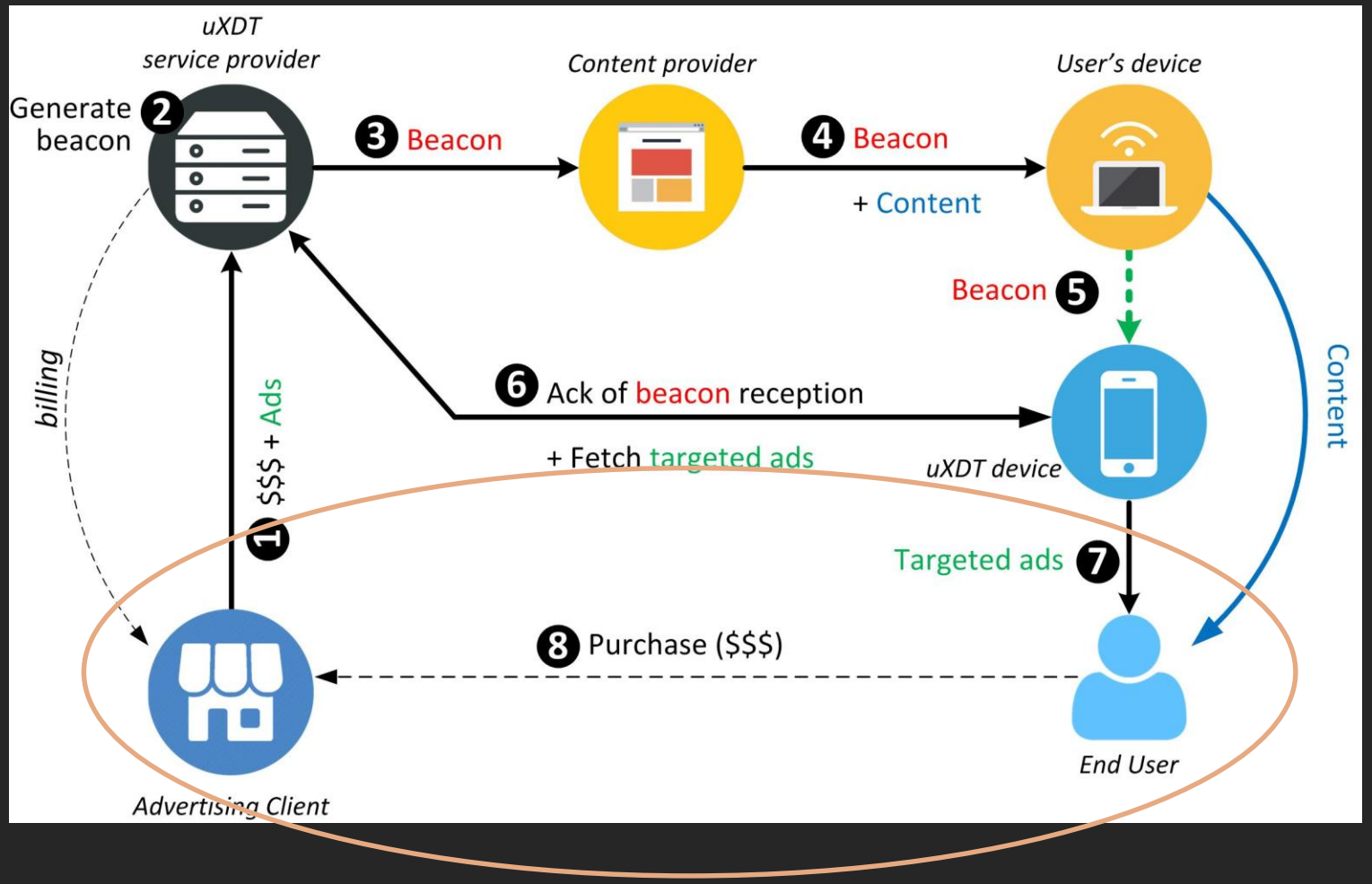


Ultrasound Cross-Device Tracking

7. The advertisement framework:

- Builds a user profile
- Pushes targeted ads to the user's device

8. Increased conversion rates for customers



The Ultrasound Ecosystem

- Cross-device Tracking
- Audience Analytics
- Synchronized Content
- Proximity Marketing
- Device Pairing

But how secure is this?

Exploitation!

Ingredients:

- A victim with:
  - A computer with speakers & the Tor browser
  - A smartphone with an uXDT-enabled app
- A state-level adversary

Setting a Surveillance Scene

- A whistleblower wants to leak documents to a journalist
- Whistleblower doesn't know is that:
  1. The journalist works with the repressive government
  2. Intends to de-anonymize him
- 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…

DEMO

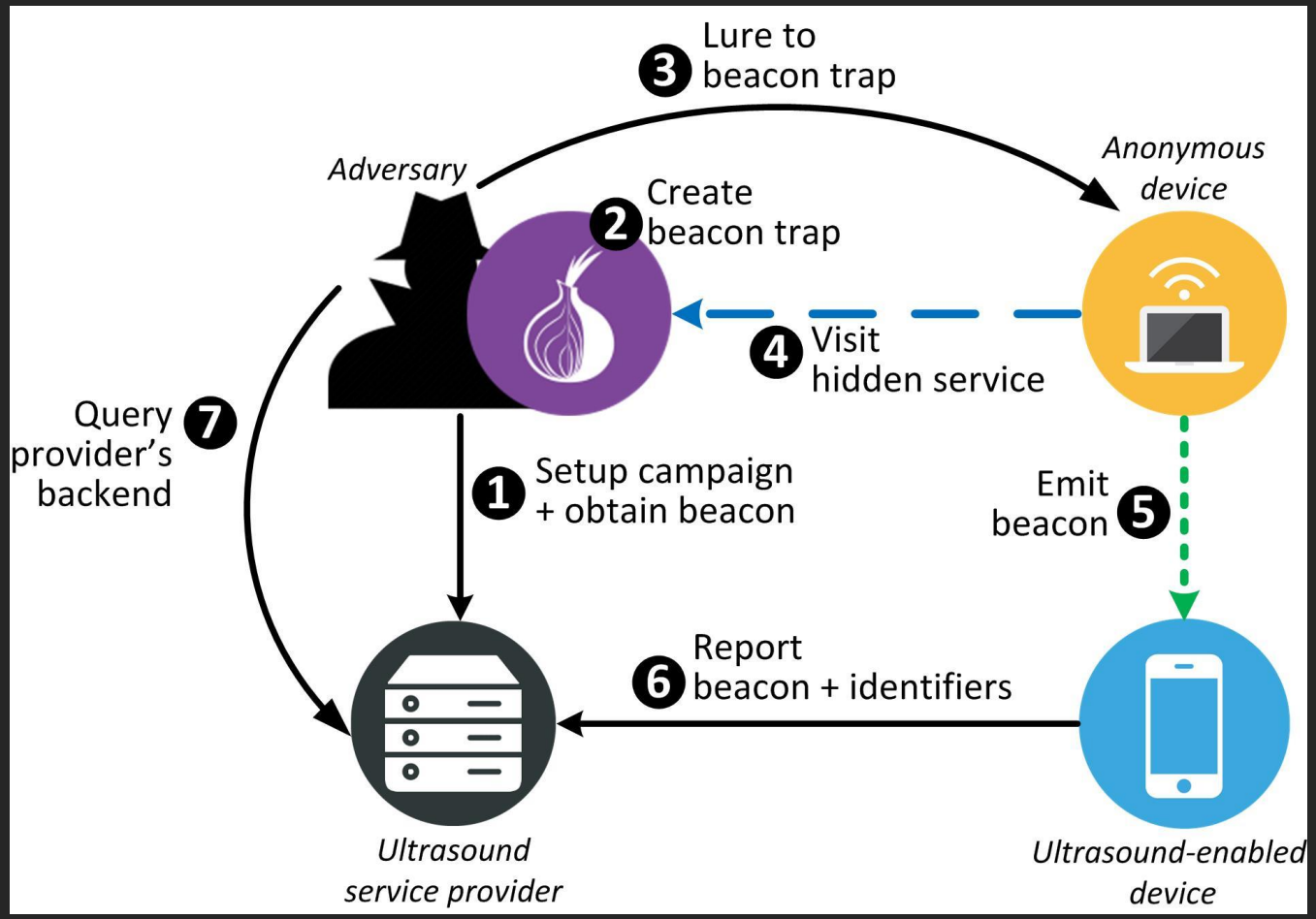
The Tor de-anonymization Attack

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

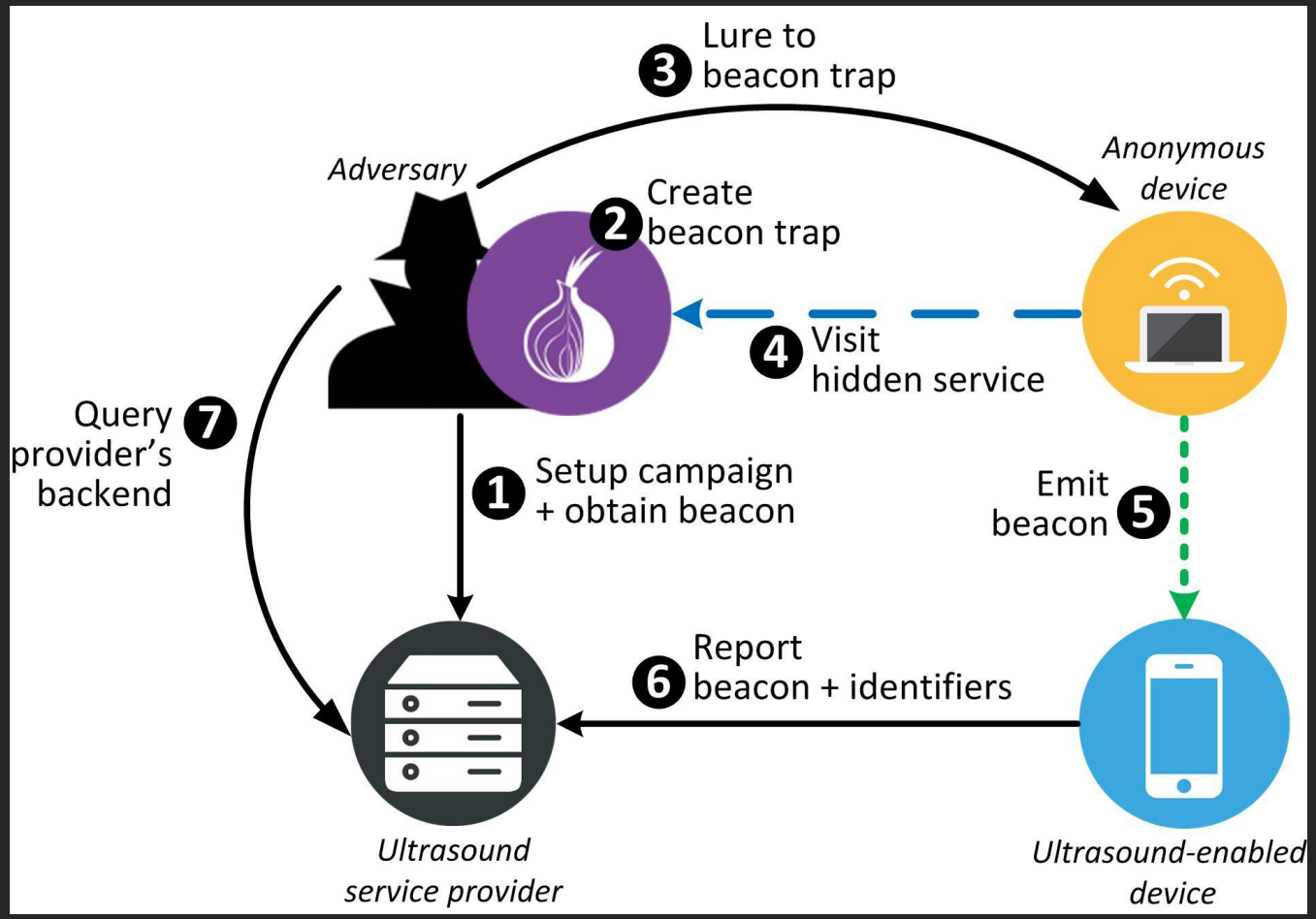


The Tor de-anonymization Attack

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



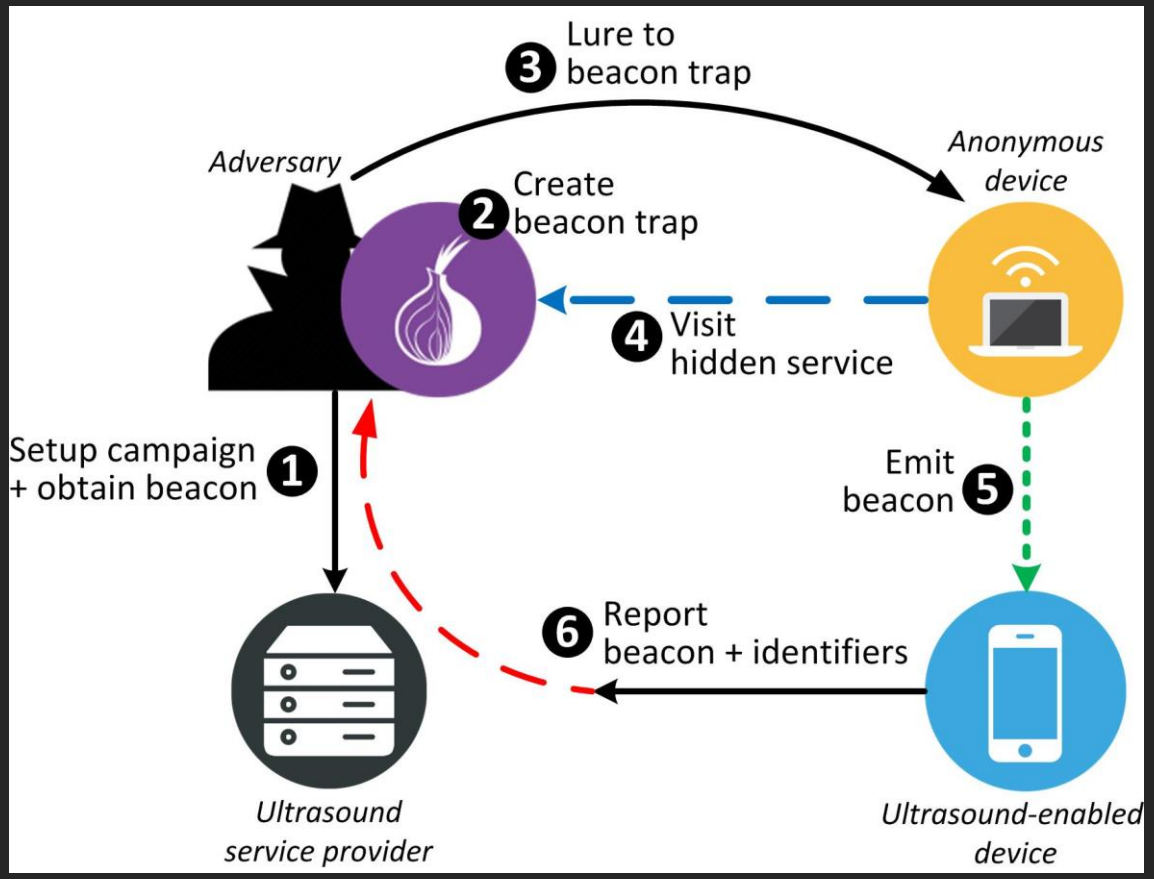
The Demo Explained

Ingredients:

- A victim with:
  - A computer with speakers & the Tor browser ✓
    - Latest version of Tor
    - Default security settings
  - A smartphone with a uXDT-enabled app ✓
- A state-level adversary ✗

The Demo: Simulated State-level Adversary

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



The Demo: Simulated State-level Adversary

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."

WHAT WENT WRONG?

Security Evaluation

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

Lack of authentication and encryption capabilities

Use Case Constraints:

- Relatively low bandwidth
- Limited Time
- Noisy environment

Resulting in:

- Replay and Injection attacks

Security Evaluation

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

Signal360 Is Bringing Sponsor Messaging To NBA Teams And Here's How To Get Creative With It

May 10, 2016

Golden State Warriors, Signal360 And App Developer Sued Over 'Eavesdropping' Allegations

Aug 31, 2016

★☆☆☆☆

DO NOT USE, THIS APP SPIES ON YOU DO NOT install this app. Recently

She acknowledges in the complaint that the app asks people for permission to access their devices' microphones, but says users aren't given enough information to understand the reason for the request.

Colts To Begin Using LISNR Technology To Reach Fans' Mobile Devices At Games, Events

July 19, 2016

Indianapolis Colts' app records audio, suit filed in Pittsburgh claims

However, the app is "systematically and surreptitiously intercepting consumers' oral communications," the lawsuit says.

Specifically, when the Colts played the Bears at Lucas Oil Stadium on Oct. 9, the app activated the microphones on all the users' phones from 11:30 a.m. to 12:15 p.m. and 2:30 p.m. to 3:30 p.m., the lawsuit says.

The app turned on the microphones regardless of whether the user was in the stadium, "in church, in their cars, at work, or in their homes," the lawsuit says.

Oct 17, 2016

NOW WHAT?

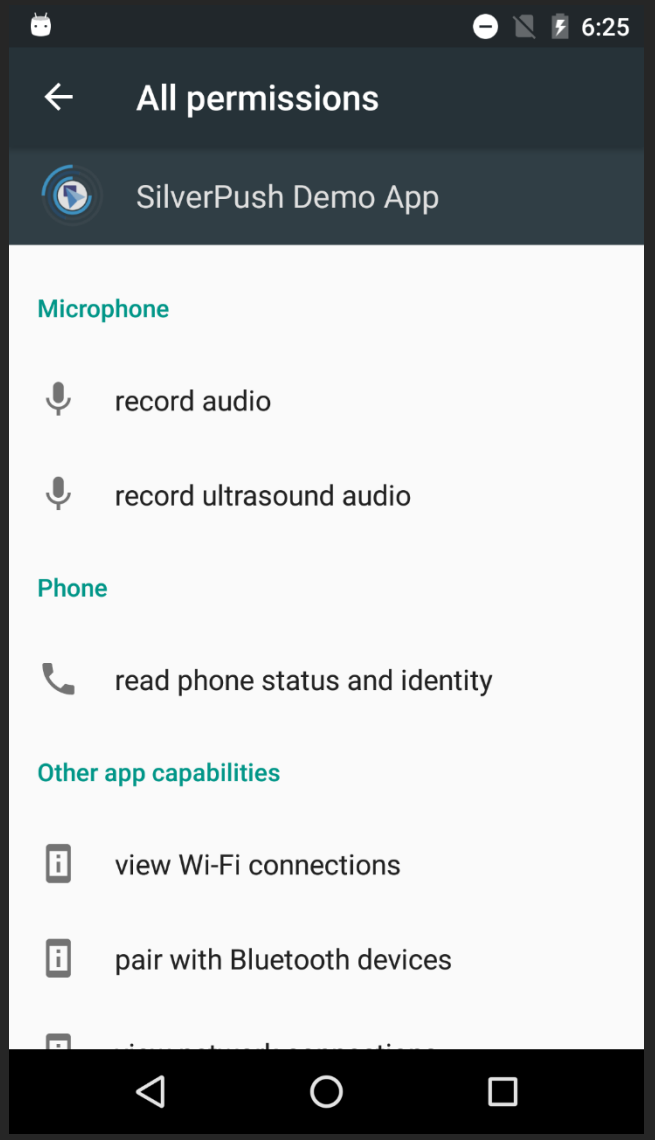

KILL IT WITH FIRE

How to fix an Ecosystem

1. Understand what's wrong with it
2. Provide some quick fixes
3. And some medium-term solutions
4. Advocate for long-term changes
5. Involve the community

Android Permission

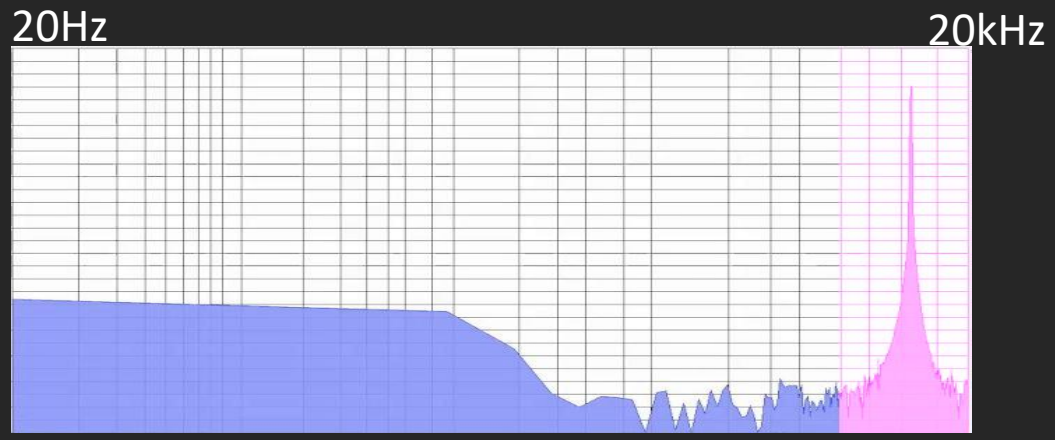
- Patch for the Android permission system
- Allows finer-grained control over the audio channel
- Separates the permissions for listening to audible sound and the ultrasonic spectrum
- End users can selectively filter the ultrasound frequencies out

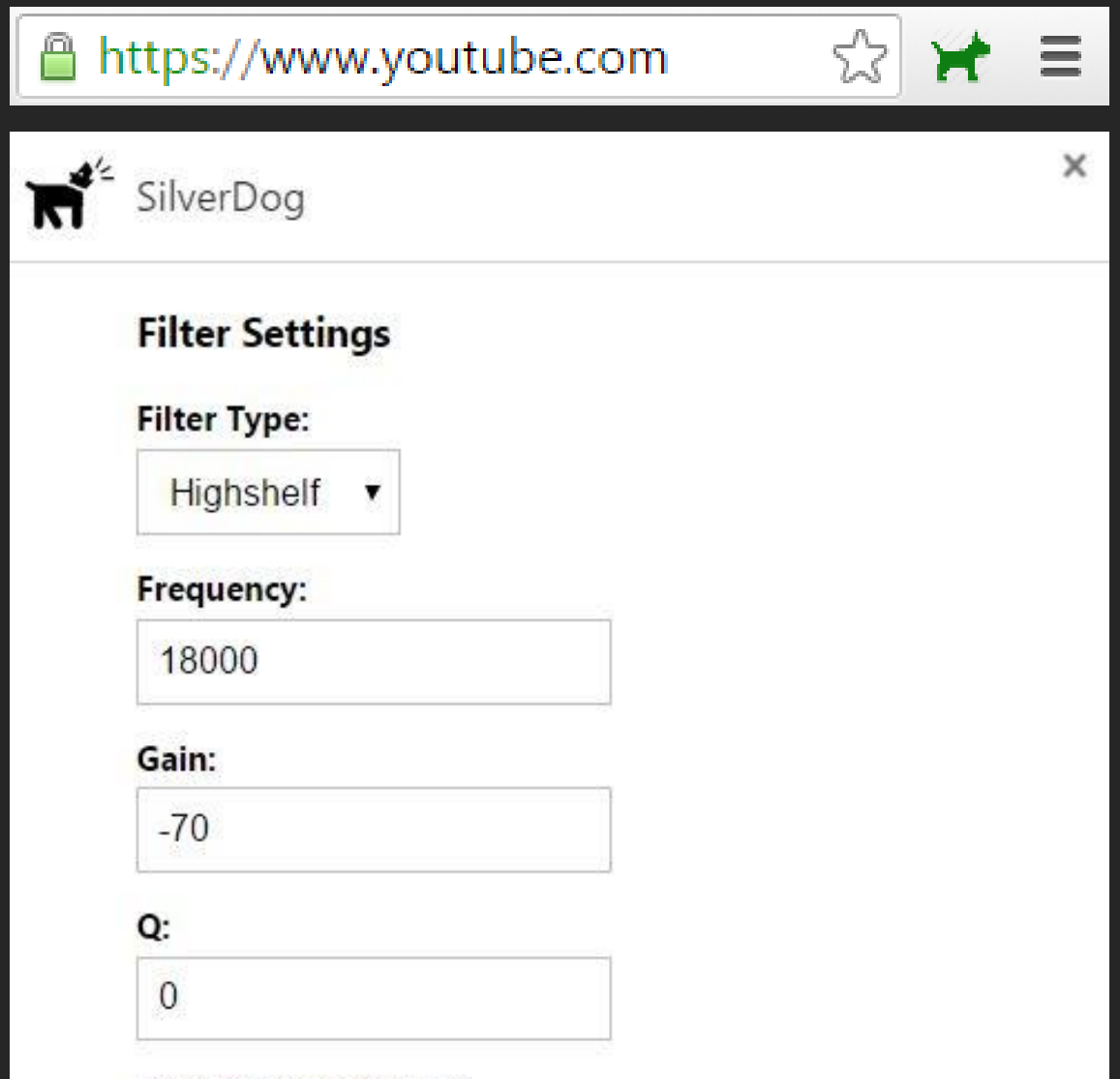


Browser Extension

Filters all audio sources and removes all uBeacons while leaving all audible frequencies intact

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





Long-Term Solutions

Standardization

- Agree on an uBeacon format
- Decide if/what security features uBeacons will have

OS-level APIs

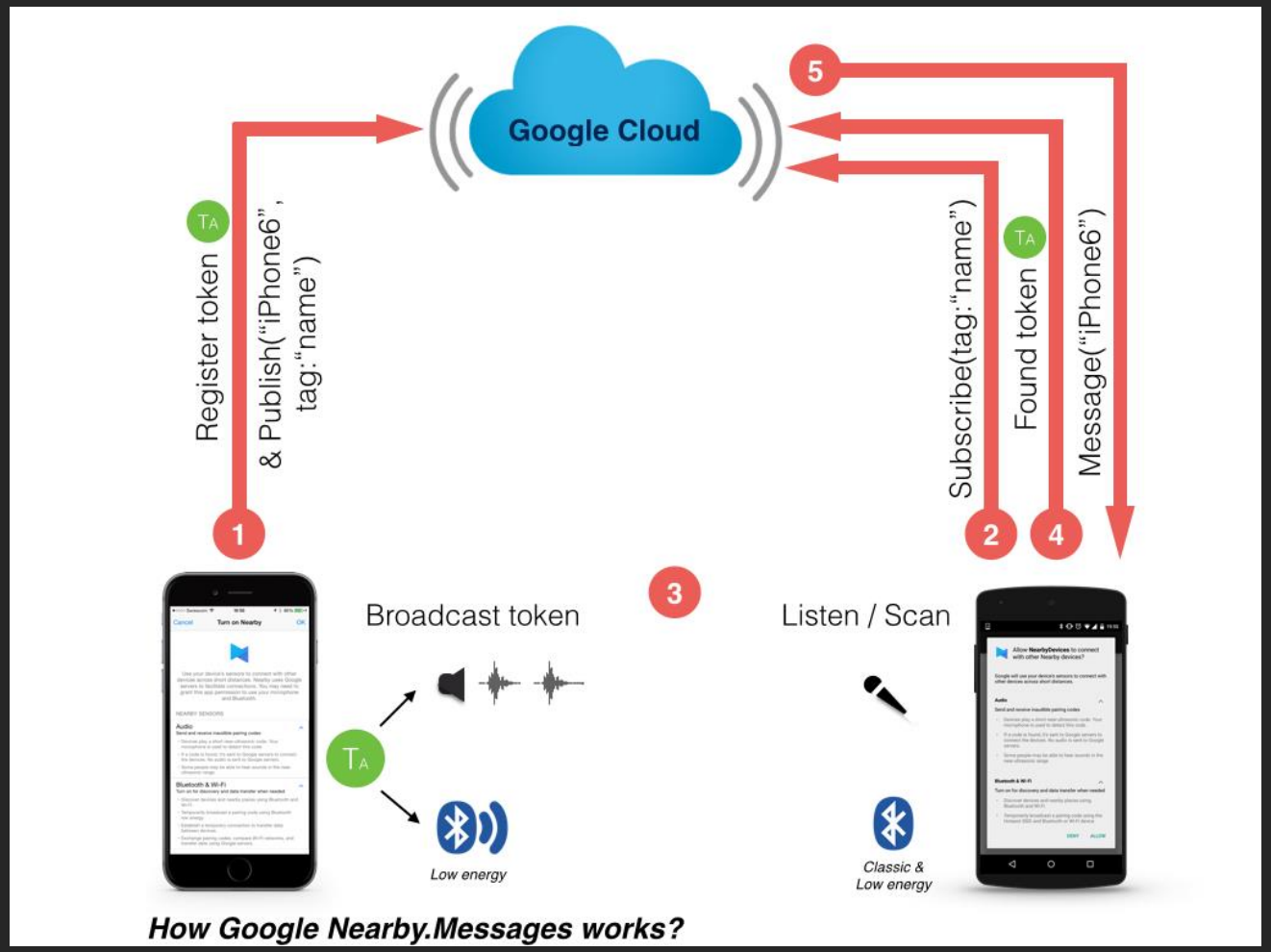
- Methods for uBeacon discovery, processing, generation and emission
- New permission for this API

Long-Term Solutions

Benefits of the API:

- Solves the problem of over-privileged apps
- No need to access the microphone
- Ultrasound-enabled apps will not risk being considered as “spying”
- Resolves the problem of “microphone locking”

It's happening!



Interact with places & devices close to you

Interact with places near you

When you're close to a place that works with "Nearby links available:"

If you have notifications turned on

1. You'll get a silent notification of what your device can do for you there.
2. To launch the offered action, tap the notification.

If you have notifications turned off

1. Open your device's Settings app ⚙.
2. Tap **Google** > **Nearby**.
3. To launch the offered action, tap the entry.

CONCLUSIONS

Conclusions: Lessons Learned

- **Inform the users**

  Improve transparency on the data collection process
- **Ask the users**

  Notifications when the app is about to take any action
- **Enable the users**

  Provide an opt-out option or better an opt-in option

- Standards are a friend of security & privacy

uBeacSec.org

Q & A

Lara: Our Research Assistant

On the Privacy and Security of the Ultrasound Ecosystem

uBeacSec.org

ubeacsec.org

Vasilios Mavroudis - https://mavroud.is

Shuang Hao - http://cs.ucsb.edu/~shuanghao

Yanick Fratantonio - http://cs.ucsb.edu/~yanick

Federico Maggi - http://maggi.cc

Giovanni Vigna - https://www.cs.ucsb.edu/~vigna/

Christopher Kruegel - http://www.cs.ucsb.edu/~chris/