Talking Behind Your Back

Attacks & Countermeasures of Ultrasonic Cross-Device Tracking

Vasilios Mavroudis
Doctoral Researcher UCL

Federico Maggi
Assistant Professor POLIMI
Visiting Researcher UCSB

Who we are

Vasilios Mavroudis
PhD Student UCL

Shuang Hao
Post-doc UCSB

Yanick Fratantonio
PhD Student UCSB

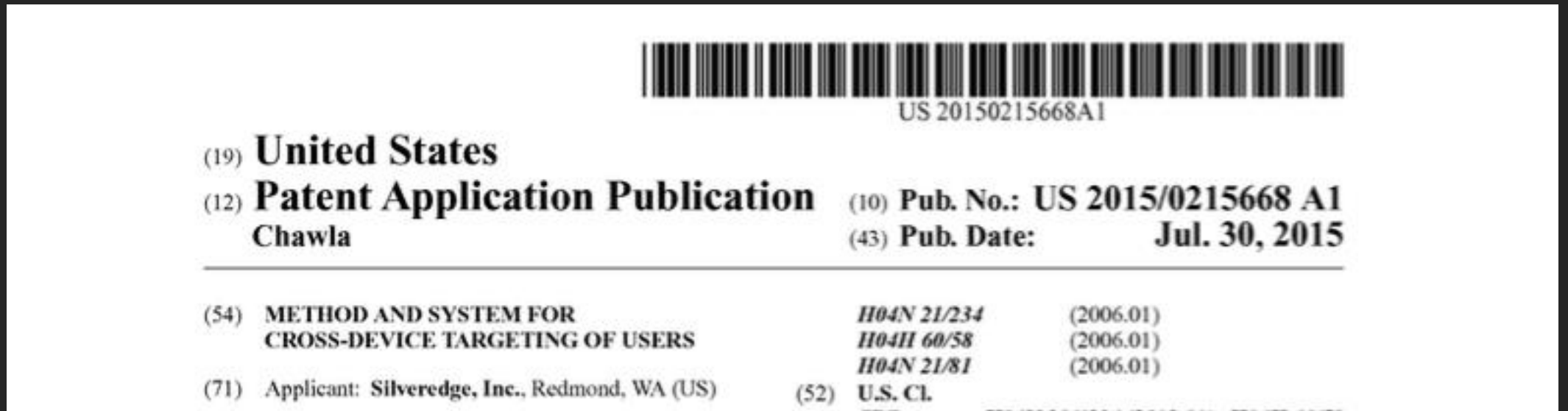
Federico Maggi
Assistant Professor POLIMI
Visiting Researcher UCSB

Christopher Kruegel
Professor UCSB
Co-founder of Lastline

Giovanni Vigna
Professor UCSB
Co-founder of Lastline

The Story of a Product

- 10/2012: SilverPush is founded
- 4/2014: SilverPush funded by Unilazer, IDG Ventures & others
- 6/2014: Articles cover the SilverPush product



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
- 4/2014: SilverPush funded by Unilazer, IDG Ventures & others
- 6/2014: Articles cover the SilverPush product
- **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
- 4/2014: SilverPush funded by Unilazer, IDG Ventures & others
- 6/2014: Articles cover the SilverPush product
- 11/2015: The security community and the press notice
- **11/2015: The Federal Trade Commission takes action**

Many of the questions raised by cross device tracking techniques are familiar. Are the new methods operating in a way that is transparent to consumers? Can consumers be given effective opt-out choices? And if not, what can be done to provide consumers with more control?

These are all steps in a positive direction. As tracking becomes more sophisticated, it's imperative that companies throughout the tracking ecosystem rise to the challenge of fostering technological solutions to inform consumers, offer choices, and honor those choices.

There's very little transparency about how those operate. I know there's some changes in how folks associated with the DAA may be reporting their use of that kind of stuff. There's very few user controls. So, for example-- and I'll show up in a second-- we'd have to essentially find a way to make browsers essentially not emit sounds that humans can't hear in order to be able to do some of this stuff.

But you're having to really get sophisticated in the technical countermeasures you employ so that that kind of activity can't happen. With some of the stuff, like the audio beaconing or the thing I made up earlier, the visual beaconing, I'm not sure we know of ways to protect against that stuff.

have, I think, a very nice approach to handling this sort of thing. So playing it out in the audio beaconing context, you fire up the app and it says this app would like to use your microphone so that it can associate-- do you allow or disallow? That seems like a pretty good motive, notice and consent.

FTC Cross-Device Tracking Workshop, Nov 16, 2015 (Washington, DC)

The Story of a Product

- 10/2012: SilverPush is founded
- 4/2014: SilverPush funded by Unilazer, IDG Ventures & others
- 6/2014: Articles cover the SilverPush product
- 11/2015: The security community and the press notice
- 11/2015: The Federal Trade Commission takes action
- **11/2015: The users react**

Unhappy

This stuff doesn't "resemble" malware. It IS malware.

This is highly invasive and should be stopped and banned immediately by the FTC. There's way too much room for abuse

Kills battery My phone usually gets about 15 hours of battery life. This runs in the background all day and I got about 6 hours yesterday

Proactive

I want an OS-level option in iOS and OS X to roll off the frequency response in the speaker output at a frequency of my choice, 18 kHz or maybe as low as 15 kHz would be fine.

Unhappy

This stuff doesn't "resemble" malware. It IS malware.

This is highly invasive and should be stopped and banned immediately by the FTC. There's way too much room for abuse

Kills battery My phone usually gets about 15 hours of battery life. This runs in the background all day and I got about 6 hours yesterday

Proactive

I want an OS-level option in iOS and OS X to roll off the frequency response in the speaker output at a frequency of my choice, 18 kHz or maybe as low as 15 kHz would be fine.

Unconcerned

Do they know how I turn off the sound during commercials?

The Story of a Product

- 10/2012: SilverPush is founded
- 4/2014: SilverPush funded by Unilazer, IDG Ventures & others
- 6/2014: Articles cover the SilverPush 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

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 the SilverPush 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

Not the End of our Story: The Tip of the Iceberg

- SilverPush was assumed to be an isolated security incident
- Very little became known about the ecosystem
- Other ultrasound-enabled products received little attention
- No scientific examination of the ultrasound-tracking frameworks
- No report on the security of the whole ecosystem

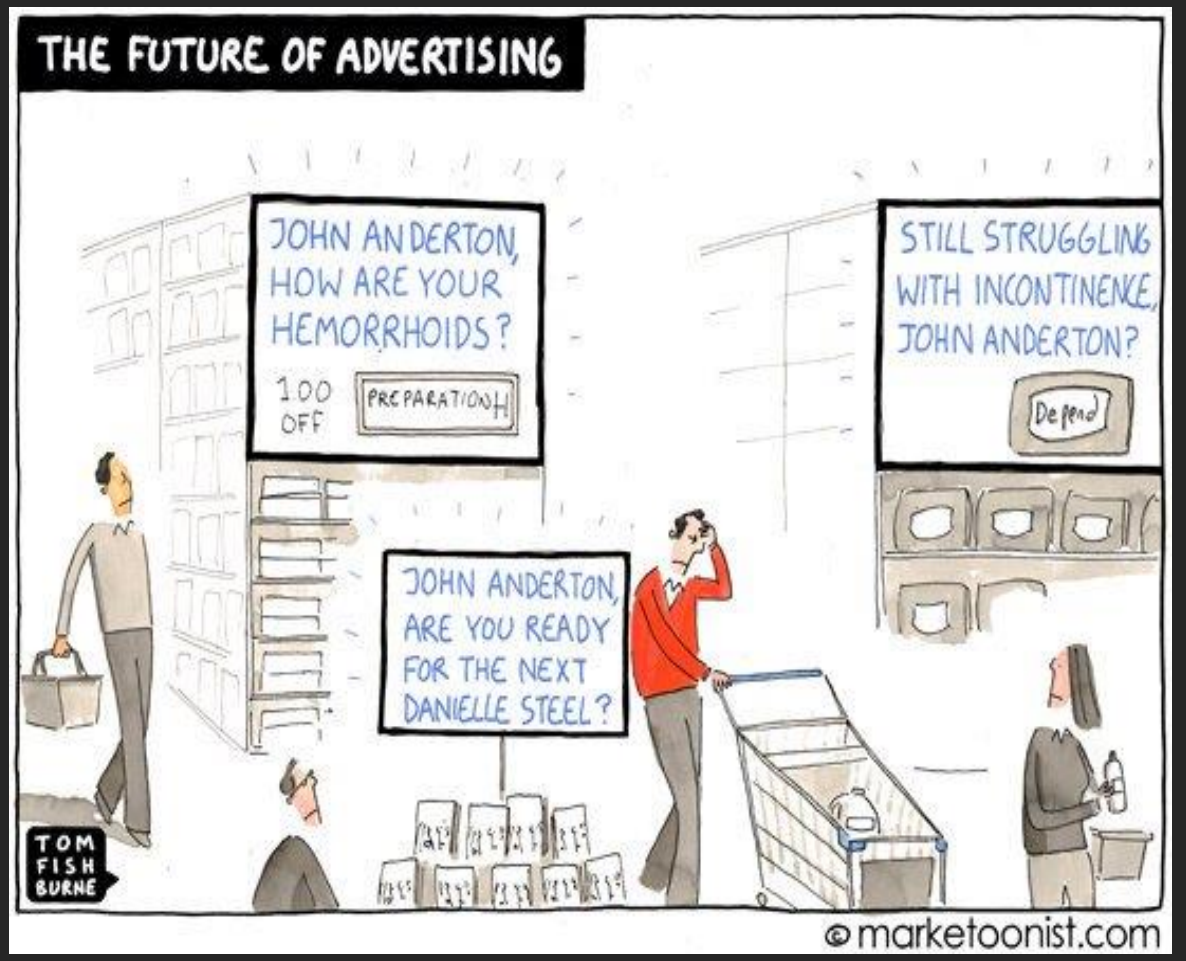
Contents

- Motivation
- What is “ultrasound tracking”?
- Exploitation & Attack Details (with DEMO)
- What went wrong?
- Where do we go from here?

THE ECOSYSTEM

The Ultrasound Tracking Ecosystem

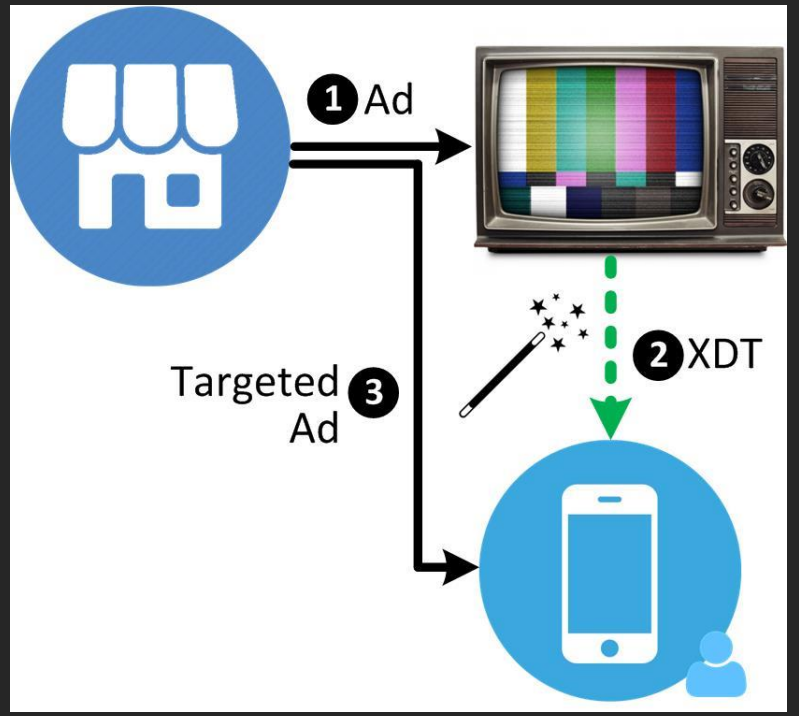
- Cross-device Tracking. XDT
- Audience Analytics
- Synchronized Content
- Proximity Marketing
- Device Pairing



Cross-Device Tracking, XDT: Overview

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, XDT: Details

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

Deterministic Example:

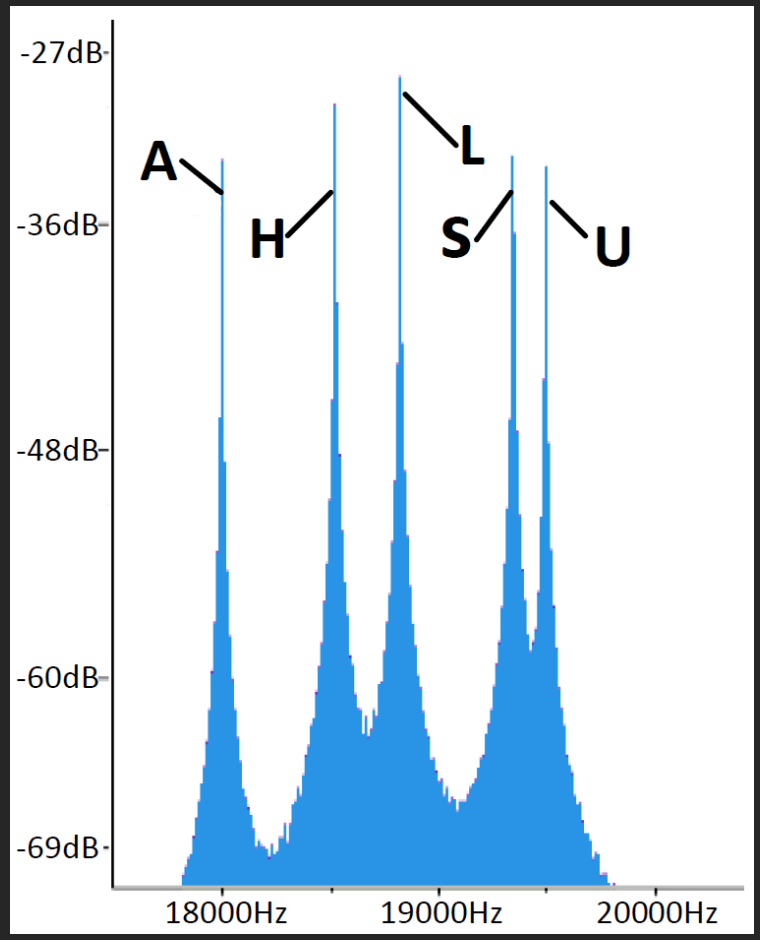
- Shared account across all devices
- Suitable for platforms, where the users are incentivized to login
- Inapplicable in most cases
- Hence alternatives are sought

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 18000Hz & 20000Hz
- Divided in smaller (~75Hz) chunks
- Each one corresponds to a symbol
- Duration of only few seconds (usually ~4)
- The exact encoding varies greatly
- No uBeacon standard
- Lots of patents



uBeacons: Practical Details

- Very low error rate in distances up to ~7 meters
- Work very well with computer speakers
- Cannot penetrate through physical obstacles (e.g., walls, doors)
- Audible by animals

XDT + uBeacons = uXDT

Ultrasound Cross-Device Tracking

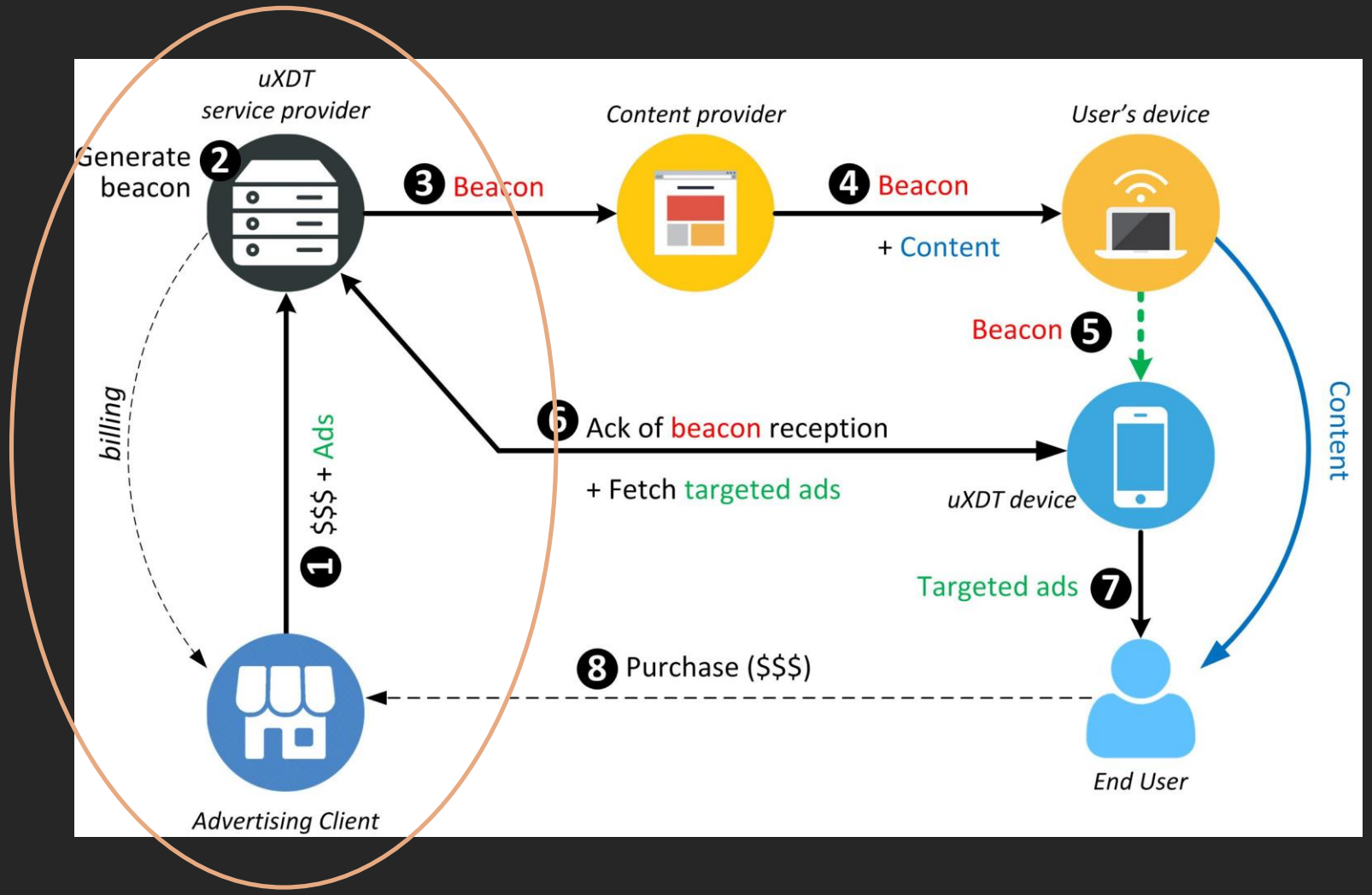
- Offers very high accuracy
- No requirement for user login
- Based on uBeacons embedded into websites or TV ads (songs?)
- Requires sophisticated backend infrastructure
- A network of publishers who incorporate uBeacons in their content
- Requires an uXDT framework installed on the user's mobile device
- uXDT Frameworks come incorporated in 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

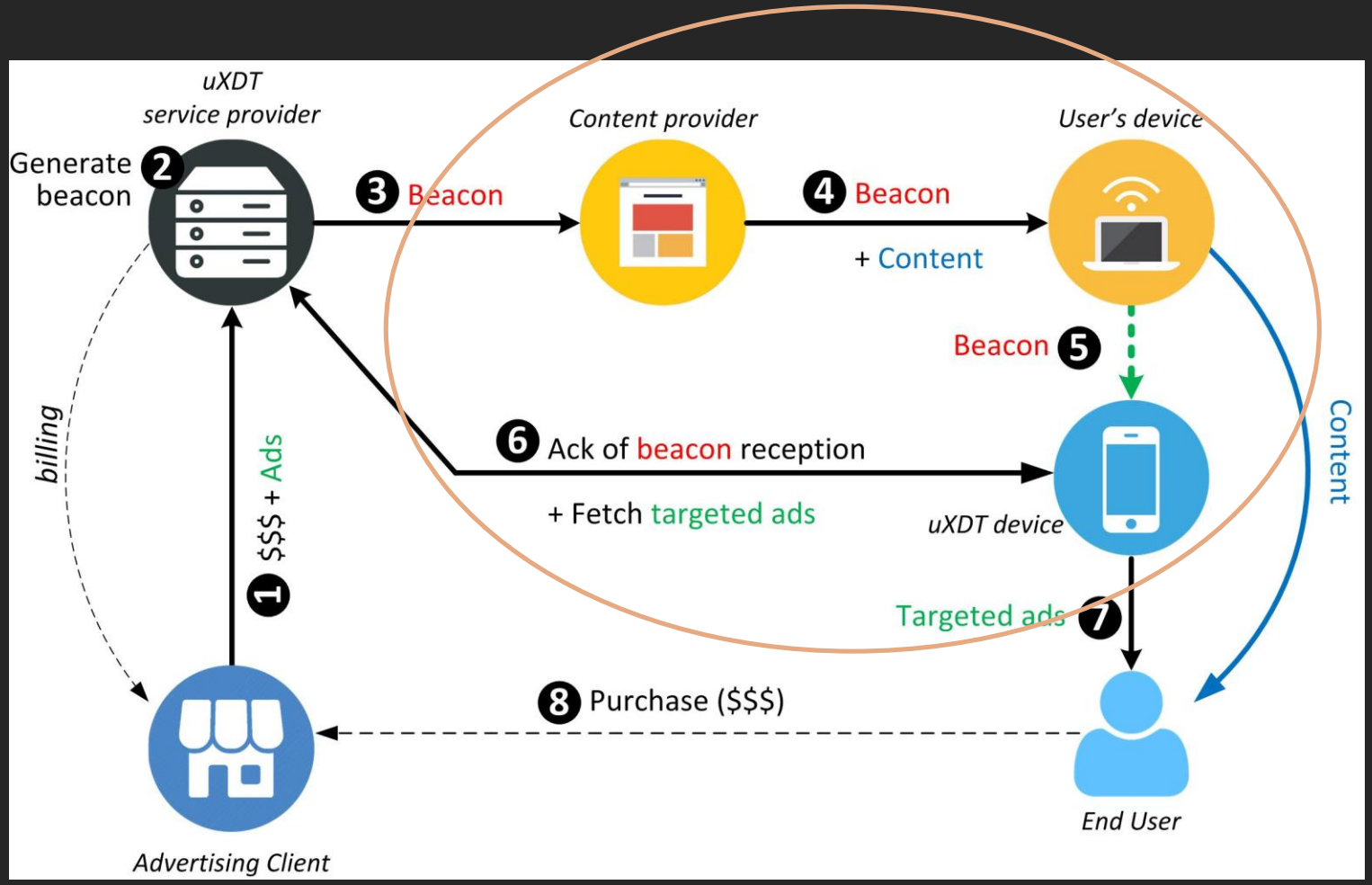


Ultrasound Cross-Device Tracking

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

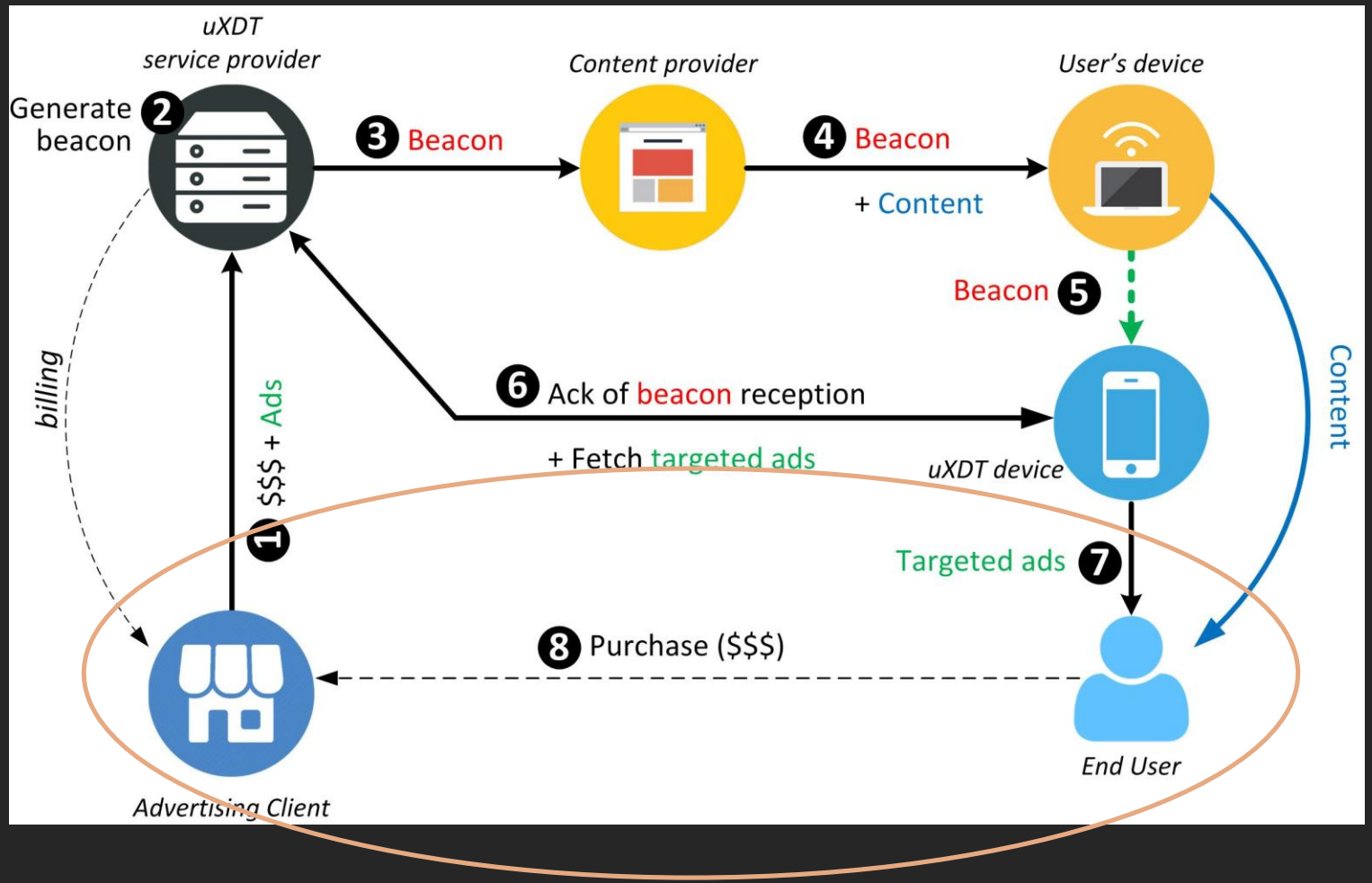


Ultrasound Cross-Device Tracking

7. The advertisement framework:

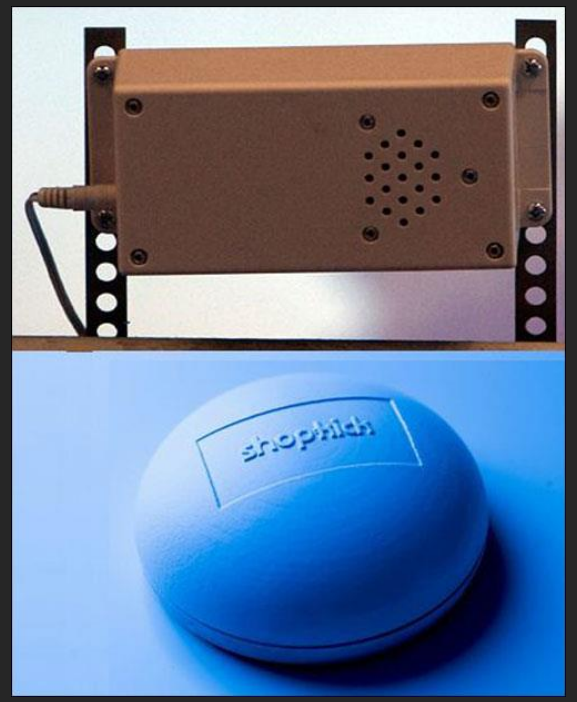
- Builds a user profile
- Pushes targeted ads to the user's device

8. Increased conversion rates for customers



Proximity Marketing

- Venues setup multiple ultrasound emitters
- An app in the customer’s phone captures the beacons up and reports them back to the company
- The data is used to:
  - Study the user's in-store behavior
  - Provide real-time notifications for products in proximity
  - Offer reward points for visiting the store



Other Use Cases

Device Pairing

- Relies on the fact that ultrasounds do not penetrate through objects
- Device A broadcasts uBeacon with random PIN
- Device B captures the uBeacon and submits a response to the PIN (usually through the Internet).
- Used to pair Google Cast (Chromecast) with mobile devices
  - Hey, it looks like Google just acquired *SlickLogin: sound-based auth for everyone!*

Audience Measurements & Analytics

- Number of viewers for a specific TV ad
- and their reactions/behavior (e.g., switching channels)

But how secure is this?

Exploitation!

Ingredients:

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

Setting the Scene

- A whistleblower wants to leak documents to a journalist
- What he 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...

LIVE DEMO

The Attacker's Toolchest

Beacon Trap
Code snippet (usually JavaScript) that, when loaded, reproduces one or more attacker-chosen inaudible beacons

The adversary attaches the trap to a resource, such as:

- An innocuous-looking web page and lures the user to visit it
- A benign website using an existing XSS vulnerability
- The users' traffic by mounting a man-in-the-middle attacks (e.g., malicious Tor exit node)
- An audio message that the attacker sends to the victim

In all these cases, when the resource is loaded, the audio beacon is captured by the ultrasound-enabled device, which would then handle it as every other valid beacon

The Attacker’s Toolchest

Beacon-injection
Pushes beacons into nearby ultrasound-enabled devices to capture and report beacons of her choice.

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 advertiser's backend.

Beacon-replay

- *V*ariation of beacon-injection
- The adversary captures and replays existing beacons

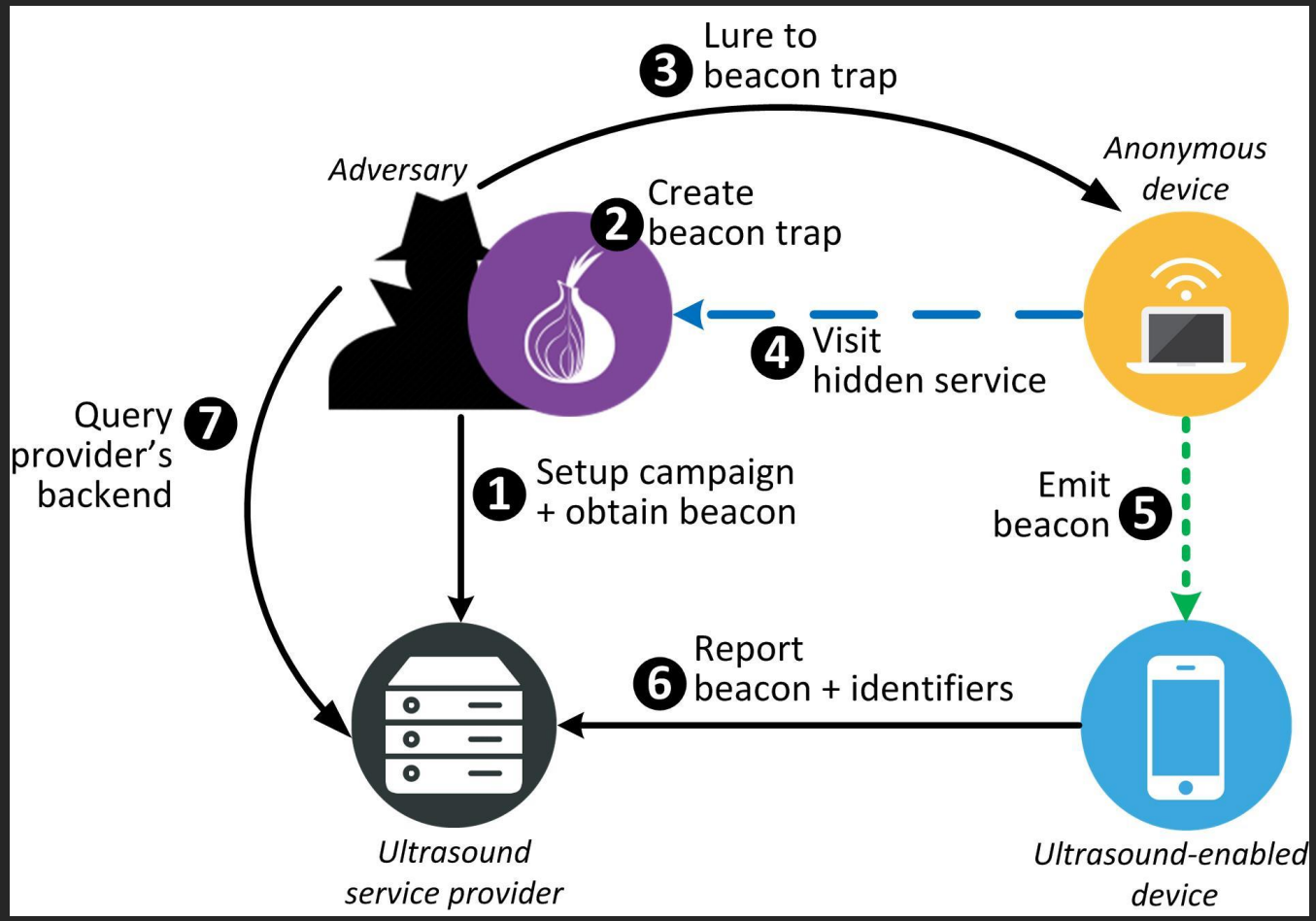
The Tor de-anonymization Attack

1. Adversary starts a campaign

2. Sets up a beacon trap on a Tor hidden service

3. Lure the user to visit it

4. User loads the resource

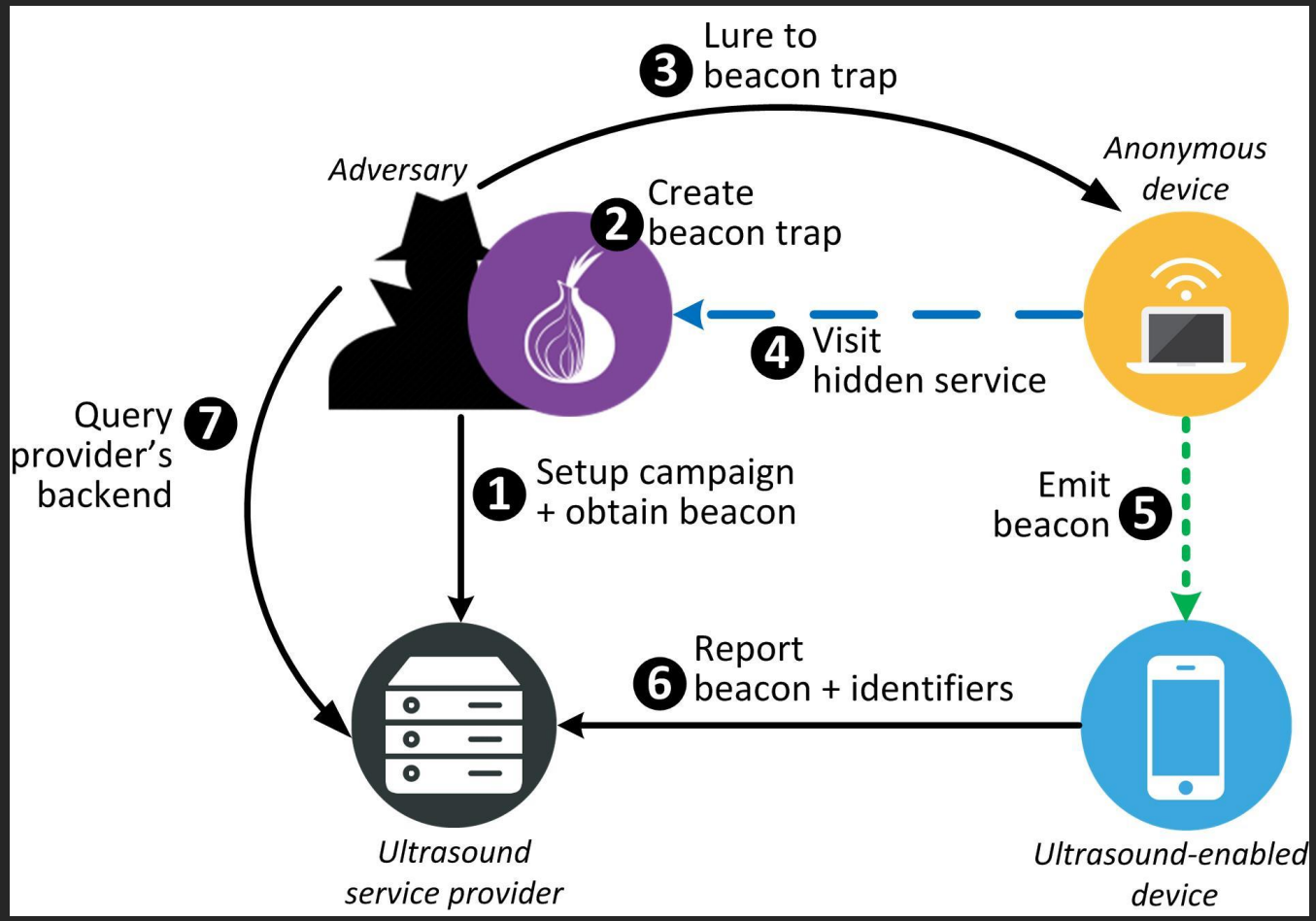


The Tor de-anonymization Attack

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



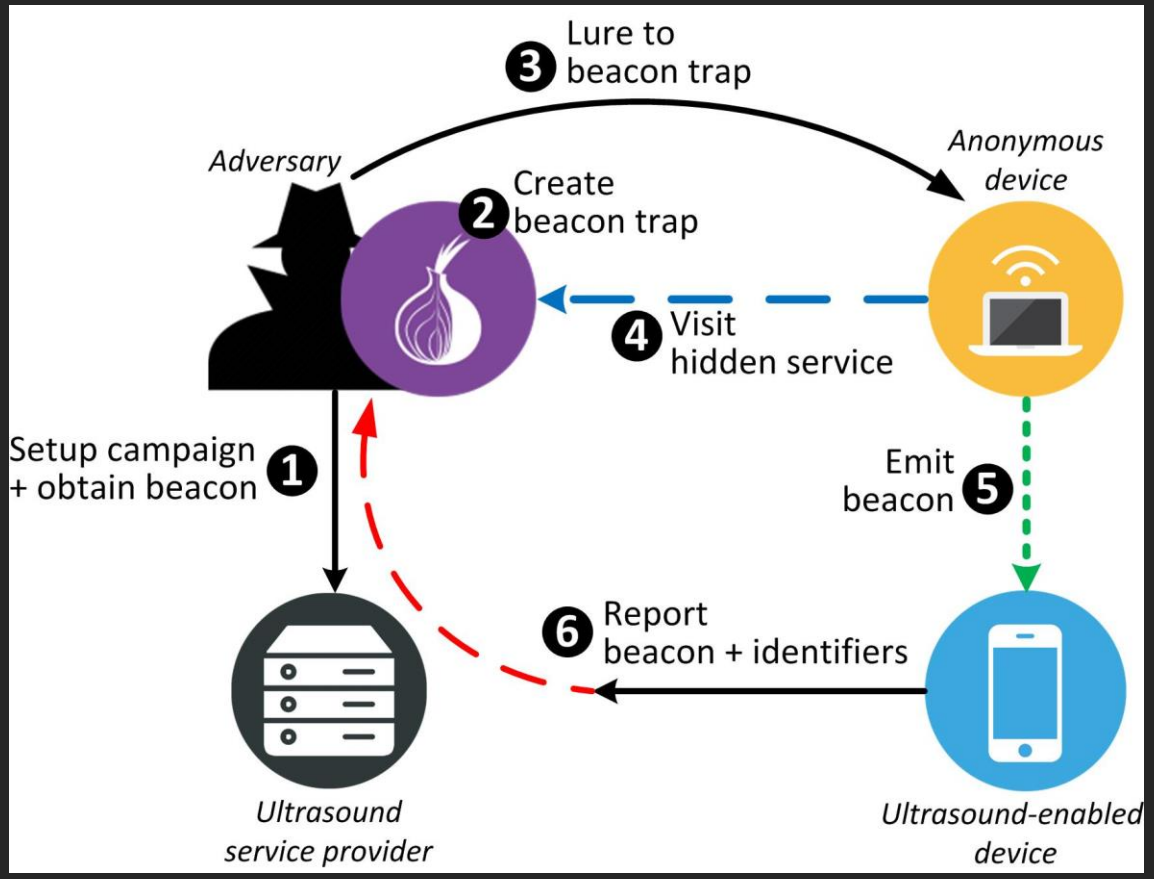
The Demo Explained

Ingredients:

- A victim with:
  - A computer with speakers & the Tor browser ✓
    - Latest version of Tor (6.0.5)
    - 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."

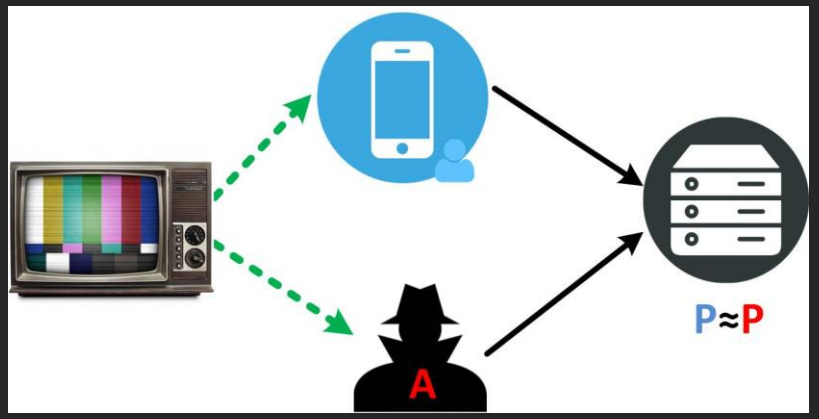
Some More Attacks

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



WHAT WENT WRONG?

Security Evaluation

- Inaccurate Threat Model
- Lack of security features in uBeacons
- Violation of a fundamental security principle
- Lack of Transparency

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: *beacon traps*

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
- No way to gain access only to the ultrasound spectrum

Repercussions:

- A malicious developers misuse their access to the mic
- Any ultrasound-enabled app can be perceived as malicious by the users

Security Evaluation

Lack of Transparency

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

Conflict of interest

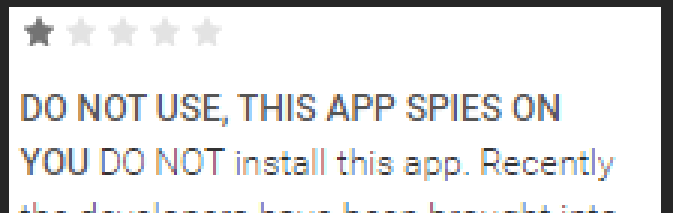
- Framework developers in many cases advice for proper practices
- But do not enforce them

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.

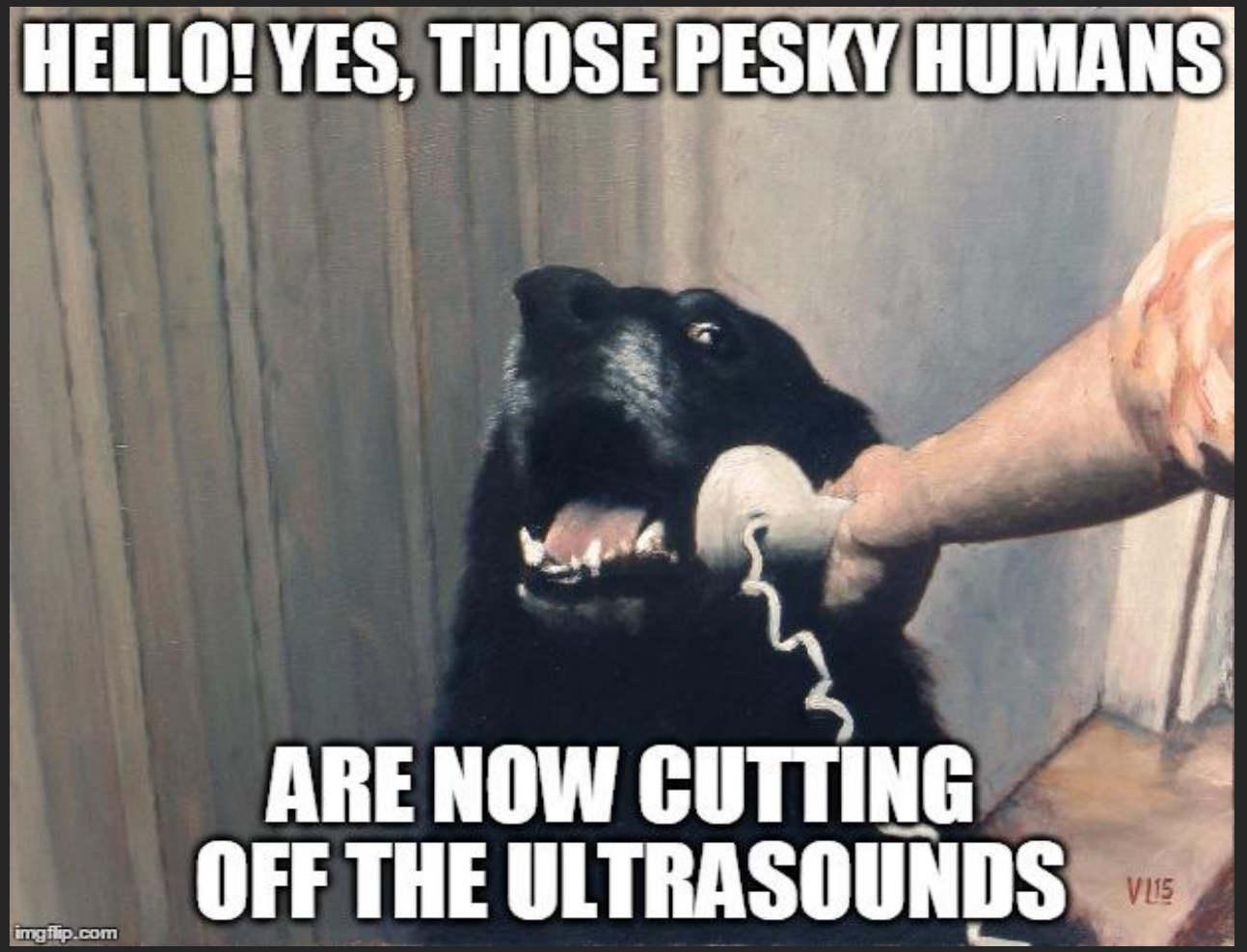
Oct 17, 2016

Market Penetration

- The ecosystem is growing fast
- New companies and products appear at a fast pace.
- Fortunately, the number of users seems to be still relatively low
- There are ~10 companies offering ultrasound-tracking products
- The great majority of them for proximity marketing
- Only one company offers an uXDT framework
  - Infrastructure Complexity
  - Backslash dis-incentivized others from joining

NOW WHAT?

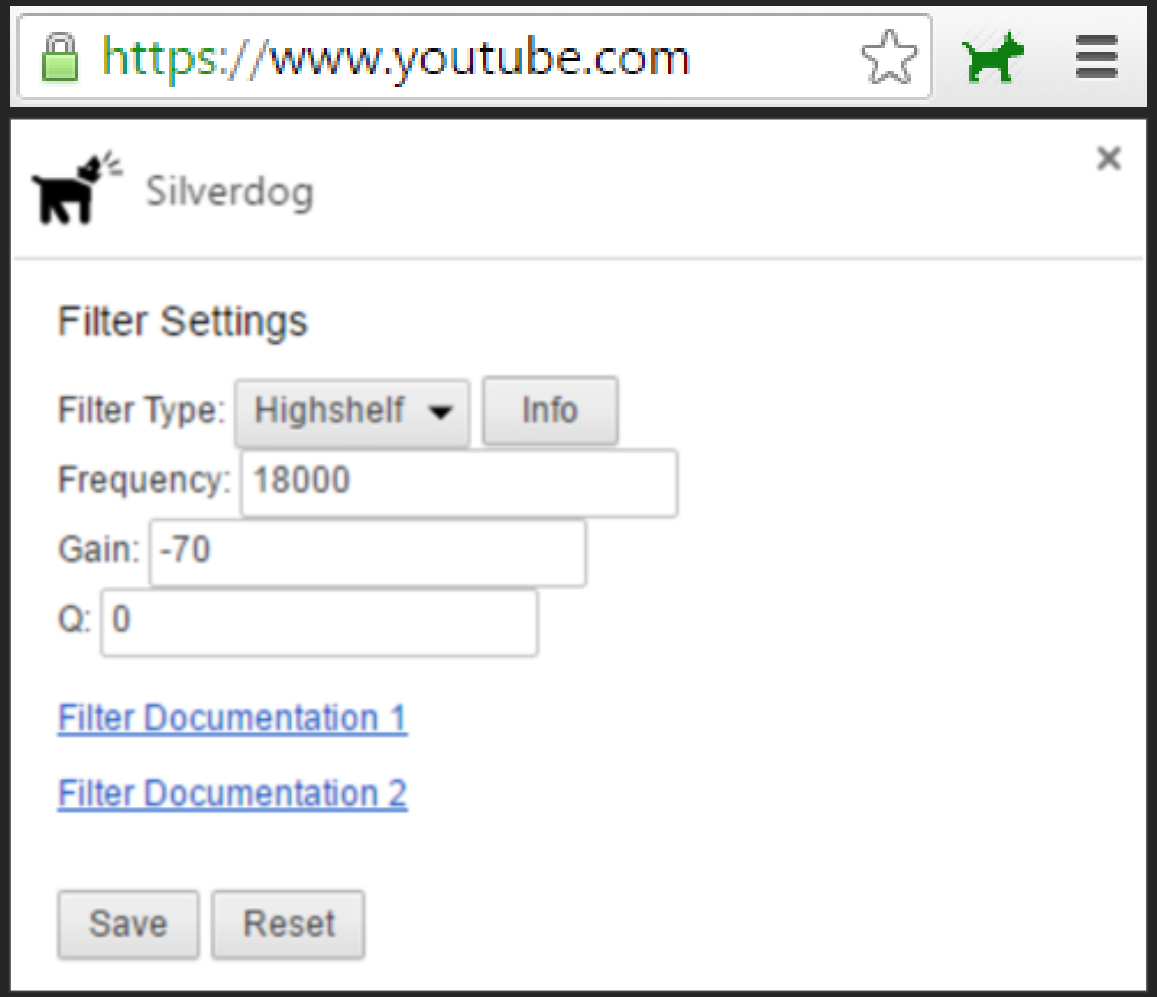
Countermeasures



Browser Extension

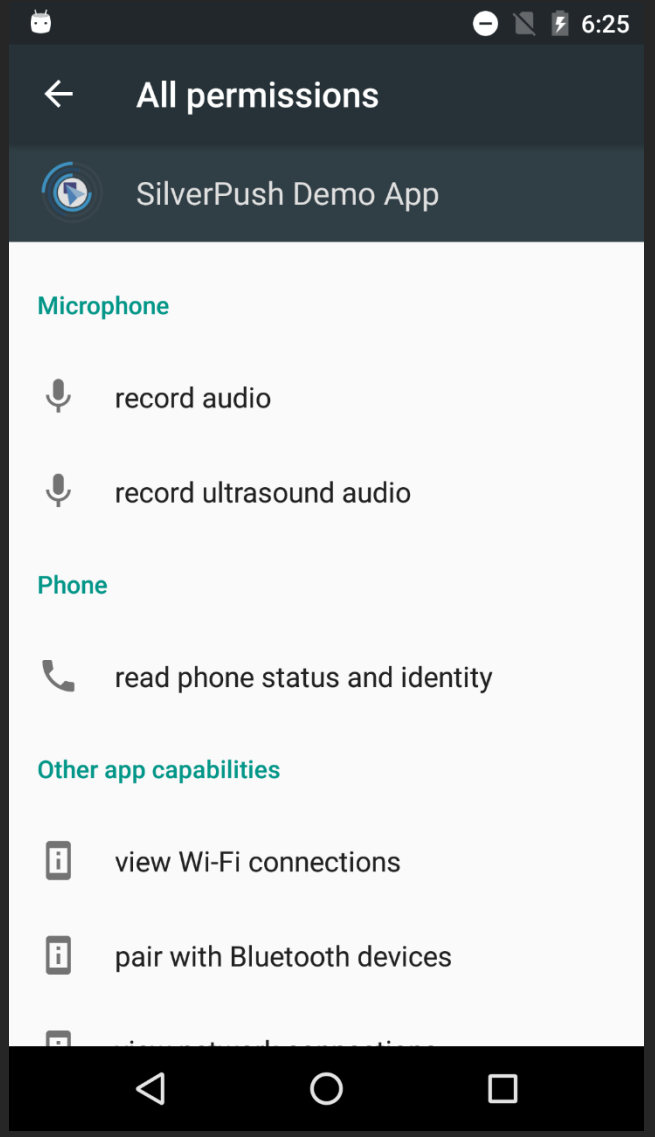
Filters all audio sources and removes all uBeacons while leaving all audible frequencies intact

- Uses the Web Audio API, HTML5
- Audio Processing Module with a Highshelf filter
- Attenuates frequencies above 18kHz
- Identifies all audio sources and destinations
- Re-wires the audio paths between them to include the filter
- Limitation: Won't work with Flash



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
- Forces applications to declare their intention to capture sound from the inaudible spectrum
- End users can selectively filter the ultrasound frequencies out



Tor Bug Tracker

#20214 new defect

Opened 4 weeks ago
Last modified 5 days ago

Ultrasound Cross Device Tracking techniques could be used to launch deanonymization attacks against some users

Reported by:	VasiliosMavroudis	Owned by:	tbb-team
Priority:	Medium	Milestone:	
Component:	Applications/Tor Browser	Version:	
Severity:	Normal	Keywords:	
Cc:	yanick@..., shuanghao@..., federico.maggi@..., gk@...	Actual Points:	
Parent ID:		Points:	
Reviewer:		Sponsor:	

Description

Emerging cross-device tracking technologies based on ultrasound could be used to fully deanonymize TOR users.

Advertisers started using ultrasounds to link multiple devices owned by the same user (i.e., perform ultrasound cross-device tracking, uXDT). For this purpose, they release advertising frameworks that can be incorporated in apps (e.g., android apps). These frameworks listen for series of tones in the ultrasonic spectrum, and once one is detected, they report it to the advertiser's servers.

It is easy to see how this could be exploited. The attacker sets up a hidden service playing such a beacon on the background and lures the victim to visit it using Tor browser. Once the victim loads the page, the tone is played through the speakers, and his/her phone picks the inaudible tone up and reports it to the advertiser's server. A state level adversary can then easily retrieve the Tor user's IP (and other unique identifiers) from the advertiser.

Since the technology is emerging, we believe that taking action now rather than later would be preferable.

One solution would be to filter-out all inaudible frequencies emitted by each visited webpage. We have developed such an extension for Chrome and a similar addon can be easily developed for the Tor browser. However, since there are similar tracking technologies using the audible spectrum: it may be a good idea to disable audio by default when using the Tor browser, or ask for user permission each time. In practice, this could be done by asking the user through popups, similarly to those used when requesting access to the user's location and the microphone.

We would be happy to provide more details and/or help in the development of a countermeasure for the Tor browser.

Securing the Ecosystem

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
- No need to access the device's microphone
- New permission for this API

Securing the Ecosystem

Benefits

- 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”

How to enforce the use of the API

- The system module handling the mic should filter out ultrasonic frequencies
- The user should be able to grant access to the spectrum on a per-app basis

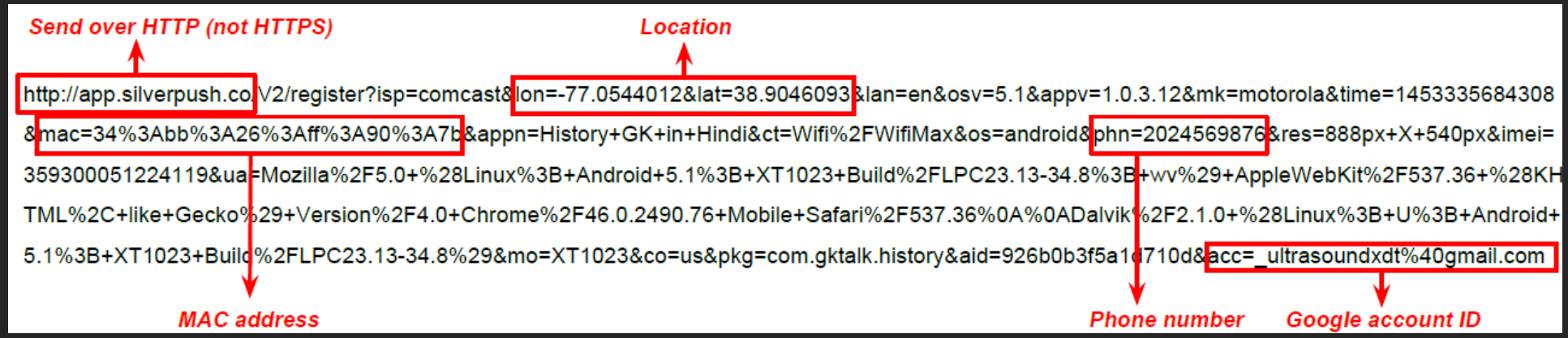
CONCLUSIONS

Conclusions: What we did

- We analyzed multiple ultrasound tracking technologies
- Reversed real-world apps and frameworks
- Identified various security shortcomings
- Introduced multiple attacks (Demo'ed one)
- Proposed and released usable countermeasures
- Initiated the uBeacon standardization discussion (hopefully)

Conclusions: What's left to do!

- What app developers should do:
  - Explicitly notify that the app will access the ultrasound spectrum
  - Improve transparency on the data collection process
  - Provide an opt-out option or better an opt-in option
  - Follow standard security practices (e.g., TLS anyone?)



Conclusions: What's left to do!

- What framework providers should do:
  - Make sure developers inform the users
  - Make sure that users' consent regularly to listening for uBeacons

- What everyone should do:
  - Standardization of uBeacons
  - Specialized API provided by the OS
  - Authentication mechanisms if technically possible

Q & A

Lara: Our Research Assistant

TALKING BEHIND YOUR BACK

ubeacsec.org

Vasilios Mavroudis - http://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/