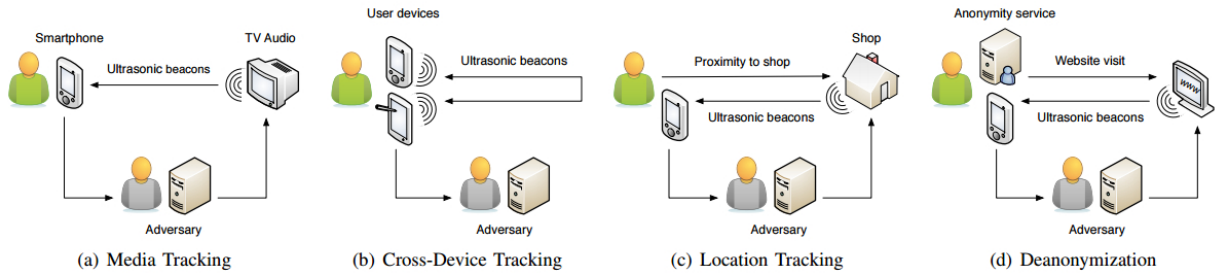
Researchers discuss findings on tracking smartphone user habits, activities with ultrasonic beacons

May 6 2017, by Nancy Owano



(a) Media Tracking (b) Cross-Device Tracking (c) Location Tracking (d) Deanonymization

Examples of different privacy threats introduced by ultrasonic side channels. (a) Ultrasonic beacons are embedded in TV audio to track the viewing habits of a user; (b) ultrasonic beacons are used to track a user across multiple devices; (c) the user's location is precisely tracked inside a store using ultrasonic signals; (d) visitors of a website are de-anonymized through ultrasonic beacons sent by the website. Credit: Daniel Arp, et al.

(Tech Xplore)—Are some Android mobile applications listening surreptitiously for ultrasonic beacons embedded in audio? Are they being used to track users and present targeted advertising?

Researchers are concerned about their findings. Academics from Technische Universitat Braunschweig,Brunswick, Germany have written a paper about their work, "Privacy Threats through Ultrasonic Side Channels on Mobile Devices."

Daniel Arp, Erwin Quiring, Christian Wressnegger and Konrad Rieck wrote that "A recent practice embeds ultrasonic beacons in audio and tracks them using the microphone of mobile devices."

What is an ultrasonic beacon, anyway?

Pedro Umbelino in *Hackaday*: "An ultrasonic beacon is an inaudible sound with encoded data that can be used by a listening device to receive information on just about anything. Beacons can be used, for example, inside a shop to highlight a particular promotion or on a museum for guided tours where the ultrasonic beacons can encode the location."

Now for the part that raises privacy concerns: they can also be used to track consumers.

Ars Technica also ran it down. "The apps silently listen for ultrasonic sounds that marketers use as high-tech beacons to indicate when a phone user is viewing a TV commercial or other type of targeted audio."

As Michael Mimoso in *Threatpost* and other sites reported, the researchers found this behavior in 234 Android apps. How can users tell if this is going on? They cannot.

Mimoso and other sites pointed out that the mobile user has no knowledge this is happening. Phones with such apps installed could listen for ultrasonic sounds without the owner knowing.

The authors discussed this. "Sound can be formally described as a sum of waves with different frequency. While natural sound is usually composed of a wide spectrum of these frequencies, humans are only able to perceive a particular range, where frequencies outside of this range remain inaudible. For designing an inaudible side channel it is thus essential to first pick an appropriate frequency band for transmission."

The beacons are in the 18kHz to 20kHz range. "So far, we have identified the frequency band 18 kHz to 20 kHz as a promising channel for designing inaudible communication."

While the range is inaudible to most people, it can be detected by most phone microphones, said Dan Goodin in *Ars Technica*.

The authors discussed their findings.

"We spot ultrasonic beacons in various web media content and detect signals in4 of 35 stores in two European cities that are used for location tracking. While we do not find ultrasonic beacons in TV streams from 7 countries, we spot 234 Android applications that are constantly listening for ultrasonic beacons in the background without the user's knowledge."

All in all, ultrasonic tracking poses a potential threat to privacy if carried out without the consent or knowledge of the user. The researchers stated in their paper that "Our findings strengthen our concerns that the deployment of ultrasonic tracking increases in the wild and therefore needs serious attention regarding its privacy consequences."

Beyond media tracking, another possibility posing privacy concerns could be de-anonymization. "The side channel through ultrasonic codes makes the de-pseudonymization of Bitcoin and de anonymization of Tor users possible," they wrote.

Dan Goodin in *Ars Technica*, meanwhile, talked about what may be done in the future about this kind of tracking.

"Longer term, antivirus providers may be able to add features that detect the tracking during routine scans of installed apps. Another long-term solution is to lobby government regulators, Google, Apple, and other companies to strictly enforce clear and prominent disclosure of all

ultrasonic-based tracking."

More information: Privacy Threats through Ultrasonic Side Channels on Mobile Devices, christian.wressnegger.info/con … nels/2017-eurosp.pdf