Microsoft RSLN

Ars Technica
28 novembre 2016

Smartphones : comment lutter contre le tracking des signaux ultrasonores ?

Si le smartphone est devenu pour beaucoup un outil indispensable au quotidien, le fait qu'il puisse envoyer, en toute indépendance et dans le plus grand secret, des signaux ultrasonores à des annonceurs pourrait bien bousculer ce constat. Ars Technica fait le point sur la situation.

Stiller Beobachter via Flickr CC BY 2.0

Ces dernières années, les signaux ultrasonores ont évolué pour devenir très faciles à déployer, n'ayant que peu de besoins pour exister. Un micro, un haut-parleur, et le tour est joué, rapporte Ars Technica.

Actuellement, lorsqu'une application vous demande la permission d'utiliser votre micro et votre haut-parleur, il existe la possibilité qu'elle utilise des *trackers* ultrasonores pour récupérer… tout ce que transmet votre micro, et pas simplement au moment de l'utilisation de l'application en question. Le tout, sans que vous n'en soyez forcément informé. Ce qui ne va pas sans poser des questions en termes de vie privée et d'utilisation des données personnelles.

Cela peut également poser un problème de sécurité : il n'existe actuellement aucun standard industriel de légitimation de l'interopérabilité des balises avec un smartphone, *via* des protocoles comme Bluetooth. Idéalement, ces balises devraient pouvoir s'authentifier avec l'application de réception de façon à éviter qu'un hacker ne crée de fausses balises pour intercepter et manipuler le contenu des informations transmises. Toutefois, les balises n'ayant qu'un laps de temps très court pour effectuer leur travail de transmission, il est délicat de rajouter un processus d'authentification dans ces quelques secondes.

Une piste, actuellement explorée par le Centre pour la Démocratie et la Technologie, en réponse à une étude de la Federal Trade Commission (FTC) consacrée à ces signaux et datée de 2015, préconise d'"accroître la transparence ainsi qu'un système opt-out à la fois robuste et significatif", avant d'ajouter :

> "Si les sociétés spécialisées dans le cross-device tracking ne peuvent pas offrir de garanties suffisantes aux utilisateurs en termes de détection et de contrôle, alors elles ne doivent pas s'engager dans cette voie."

La FTC avait justement rédigé une première lettre à l'intention des développeurs, à propos d'une certaine marque de balises audio pouvant potentiellement tracer l'ensemble des programmes télévisés consommés par un utilisateur, sans même qu'ils ne le sachent… Cette société a depuis abandonné le tracking *via* les signaux ultrasonores, signalant néanmoins que le courrier de la FTC n'avait rien à voir avec sa décision.

Plus d'informations ci-dessous (en anglais)
Risk Assessment
Lily Hay Newman,
wired.com
11/3/2016

How to block the ultrasonic signals you didn't know were tracking you

Your phone can talk to advertisers beyond your back, beyond your audible spectrum.

Dystopian corporate surveillance threats today come at us from all directions. Companies offer "always-on" devices that listen for our voice commands, and marketers follow us around the web to create personalized user profiles so they can (maybe) show us ads we'll actually click. Now marketers have been experimenting with combining those web-based and audio approaches to track consumers in another disturbingly science fictional way: with audio signals your phone can hear, but you can't. And though you probably have no idea that dog whistle marketing is going on, researchers are already offering ways to protect yourself.

The technology, called ultrasonic cross-device tracking, embeds high-frequency tones that are inaudible to humans in advertisements, web pages, and even physical locations like retail stores. These ultrasound "beacons" emit their audio sequences with speakers, and almost any device microphone—like those accessed by an app on a smartphone or tablet—can detect the signal and start to put together a picture of what ads you've seen, what sites you've perused, and even where you've been. Now that you're sufficiently concerned, the good news is that at the Black Hat Europe security conference on Thursday, a group based at University of California, Santa Barbara will present an Android patch and a Chrome extension that give consumers more control over the transmission and receipt of ultrasonic pitches on their devices.

Beyond the abstract creep factor of ultrasonic tracking, the larger worry about the technology is that it requires giving an app the ability to listen to everything around you, says Vasilios Mavroudis, a privacy and security researcher at University College London who worked on the research being presented at Black Hat.

> "The bad thing is that if you're a company that wants to provide ultrasound tracking there is no other way to do it currently, you have to use the microphone," says Mavroudis. "So you will be what we call 'over-privileged,' because you don't need access to audible sounds but you have to get them."

This type of tracking, which has been offered in some form by companies like Silverpush and Shopkick, has hardly exploded in adoption. But it's persisted as more third party companies develop ultrasonic tools for a range of uses, like data transmission without Wi-Fi or other connectivity. The more the

technology evolves, the easier it is to use in marketing. As a result, the researchers say that their goal is to help protect users from inadvertently leaking their personal information.

> "There are certain serious security shortcomings that need to be addressed before the technology becomes more widely used," says Mavroudis. "And there is a lack of transparency. Users are basically clueless about what's going on."

Currently, when Android or iOS do require apps to request permission to use a phone's microphone. But most users likely aren't aware that by granting that permission, apps that use ultrasonic tracking could access their microphone—and everything it's picking up, not just ultrasonic frequencies—all the time, even while they're running in the background.

The researchers' patch adjusts Android's permission system so that apps have to make it clear that they're asking for permission to receive inaudible inputs. It also allows users to choose to block anything the microphone picks up on the ultrasound spectrum. The patch isn't an official Google release, but represents the researchers' recommendations for a step mobile operating systems can take to offer more transparency.

To block the other end of those high-pitched audio communications, the group's Chrome extension preemptively screens websites' audio components as they load to keep the ones that emit ultrasounds from executing, thus blocking pages from emitting them. There are a few old services that the extension can't screen, like Flash, but overall the extension works much like an ad-blocker for ultrasonic tracking. The researchers plan to post their patch and their extension available for download after their Black Hat presentation.

Ultrasonic tracking has been evolving for the last couple of years, and it is relatively easy to deploy since it relies on basic speakers and microphones instead of specialized equipment. But from the start, the technology has encountered pushback about its privacy and security limitations. Currently there are no industry standards for legitimizing beacons or allowing them to interoperate the way there are with a protocol like Bluetooth. And ultrasonic tracking transmissions are difficult to secure because they need to happen quickly for the technology to work. Ideally the beacons would authenticate with the receiving apps each time they interact to reduce the possibility that a hacker could create phony beacons by manipulating the tones before sending them. But the beacons need to complete their transmissions in the time it takes someone to briefly check a website or pass a store, and it's difficult to fit an authentication process into those few seconds. The researchers say they've already observed one type of real-world attack in which hackers replay a beacon over and over to skew analytics data or alter the reported behavior of a user. The team also developed other types of theoretical attacks that take advantage of the lack of encryption and authentication on beacons.

The Federal Trade Commission evaluated ultrasonic tracking technology at the end of 2015, and the privacy-focused non-profit Center for Democracy and Technology wrote to the agency at the time that

> "the best solution is increased transparency and a robust and meaningful opt-out system. If cross-device tracking companies cannot give users these types of notice and control, they should not engage in cross-device tracking."

By March the FTC had drafted a warning letter to developers about a certain brand of audio beacon that could potentially track all of a users' television viewing without their knowledge. That company,

called Silverpush, has since ceased working on ultrasonic tracking in the United States, though the firm said at the time that its decision to drop the tech wasn't related to the FTC probe.

More recently, two lawsuits filed this fall—each about the Android app of an NBA team—allege that the apps activated user microphones improperly to listen for beacons, capturing lots of other audio in the process without user knowledge. Two defendants in those lawsuits, YinzCam and Signal360, both told WIRED that they aren't beacon developers themselves and don't collect or store any audio in the spectrum that's audible to humans.

But the researchers presenting at Black Hat argue that controversy over just how much audio ultrasonic tracking tools collect is all the more reason to create industry standards, so that consumers don't need to rely on companies to make privacy-minded choices independently.

> "I don't believe that companies are malicious, but currently the way this whole thing is implemented seems very shady to users," says Mavroudis.

Once there are standards in place, the researchers propose that mobile operating systems like Android and iOS could provide application program interfaces that restrict microphone access so ultrasonic tracking apps can only receive relevant data, instead of everything the microphone is picking up.

> "Then we get rid of this overprivileged problem where apps need to have access to the microphone, because they will just need to have access to this API," Mavroudis says.

For anyone who's not waiting for companies to rein in what kinds of audio they collect to track us, however, the UCSB and UCL researchers software offers a temporary fix. And that may be more appealing than the notion of your phone talking to advertisers behind your back—or beyond your audible spectrum.

Correction 11/3/2016 6:20pm EST: An earlier version of this article stated that the cross-device tracking companies 4Info and Tapad use ultrasonic tracking. Both companies say they don't use the form of tracking the researchers describe.