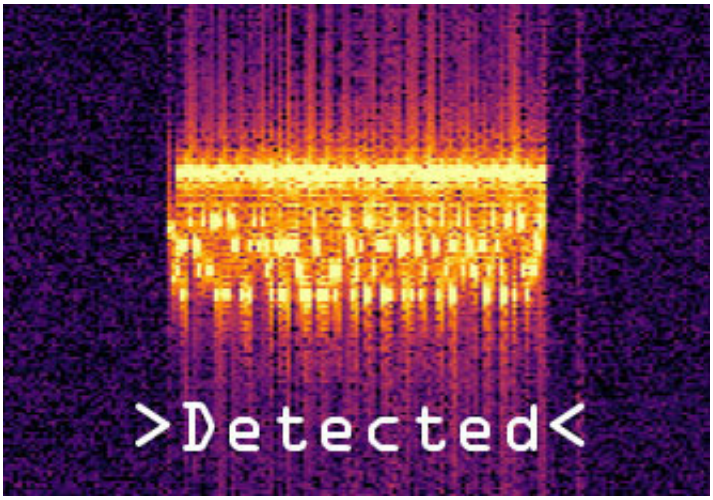
Ultrasound-firewall for mobile phones

May 25 2018



Ultrasound-firewall for mobile phones. Credit: St. Poelten UAS / Matthias Zeppelzauer

The permanent networking of mobile devices can endanger the privacy of users and lead to new forms of monitoring. New technologies such as Google Nearby and Silverpush use ultrasonic sounds to exchange information between devices via loudspeakers and microphones (also called "data over audio").

Devices increasingly communicate via this inaudible communication channel. Ultrasonic communication allows devices to be paired and information to be exchanged. It also makes it possible to track users and their behaviour over a number of devices, much like cookies on the Web. Almost every device with a microphone and a loudspeaker can

send and receive ultrasonic sounds. Users are usually unaware of this inaudible and hidden data transmission.

The SoniControl project of St. Pölten University of Applied Sciences has developed a mobile application that detects acoustic cookies, brings them to the attention of users, and if desired, blocks the tracking. The app is thus, in a sense, the first available ultrasound firewall for smartphones and tablets. "The most challenging part of developing the app was to devise a method that can detect existing ultrasound-transmission techniques reliably and in real time," said Matthias Zeppelzauer, head of the project and senior researcher in the Media Computing research group of the Institute of CreativeMedia/Technologies at St. Pölten UAS.

Determining interests and location

Such ultrasonic signals can be used for so-called "cross-device tracking." This makes it possible to track the user's behaviour across multiple devices, and relevant user profiles can be merged with one other. In this way, more accurate user profiles can be created for targeted advertising and filtering of internet content.

Up until now, it has not been possible to block acoustic cookies. "In order to accept voice commands, the mobile phone microphone is often permanently active. Every mobile application that has access to the microphone as well as the operating system itself can at any time without notice activate the microphone of a mobile device, listen to it, detect acoustic cookies and synchronise it over the Internet," said Zeppelzauer. Users are often not informed of this information transmission during operation. Only a permanent deactivation of the microphone would suffice, rendering the device unusable as a telephone.

Masking of ultrasound cookies

In the SoniControl project, Zeppelzauer and his colleagues Peter Kopciak, Kevin Pirner, Alexis Ringot and Florian Taurer have developed a procedure to expose the cookies and inform device users. For masking and blocking the ultrasonic data transfer, interference signals are transmitted via the loudspeaker of the mobile device. Thus, acoustic cookies can be neutralized before operating systems or mobile applications can access them. Users can selectively block cookies without affecting the functionality of the smartphone.

The masking of the cookies occurs by means of ultrasound, which is inaudible to humans. "There is currently no technology on the market that can detect and block acoustic cookies. The application developed in this project represents the first approach that gives people control over this type of tracking," said Zeppelzauer.

All project results and the application have been made publicly available. The system is therefore directly usable and expandable for everyone. All project results have been released under Creative-Commons license.

Data exchange via ultrasound in the Internet-of-Things

The technology is now being further developed in a follow-up project, SoniTalk. Through Internet-of-Things (IoT) technologies an increasing number of devices are communicating with one another. Ultrasonic communication is increasingly used for data exchange between mobile phones and devices. Thus, ultrasonic communication is an alternative technology for ad-hoc data exchange, near-field communication (NFC) and as a channel for two-factor authentication that proves the identity of users by combining two different and independent components.

The new project SoniTalk wants to give users full control over what is

allowed to be sent by which app and should effectively help to protect user privacy. The goal of SoniTalk is an open source, transparent and fully private-sphere oriented protocol for ultrasonic communication. SoniTalk seeks to lay the groundwork for a new free standard in the field of ultrasonic communication that enables secure communication and protects user privacy.

More information: Project website: sonicontrol.fhstp.ac.at

Project results: www.netidee.at/sonicontrol

SoniControl App in the Google Play Store: play.google.com/store/apps/det … ac.fhstp.sonicontrol

Source Code: git.nwt.fhstp.ac.at/m.zeppelzauer/SoniControl

Provided by St. Poelten University of Applied Sciences