CONTENTS

Vol. 3. Issue 3 (2018)

Ultrasonic Tracking (User's Activity), Detection and Forensics

Airgap has long been used to protect the data leakage but with the advancement in technology the same has been proved to be a myth. There are multiple ways to break the airgap barrier. One of them is by using ultrasound waves to transmit the data. This article outlines the conceptual framework for using ultrasonic sound waves for data stealing and transmission along with a few ways of detection.

-Ummed Meel

Introduction:

In today's scenario, people use smart phones for various purposes such as e-transactions, quick messaging, social media connectivity, entertainment purposes, etc. Users are regularly being tracked and monitored through the microphones of their devices. Nowadays, "Ultrasonic Detection" is being used to convert inaudible beacons in sound which are used to monitor user's activity.

This technology has raised alarms since an individual's privacy is at stake. A third person can remotely access your microphone without your knowledge and permission. There are lots of android applications that are capable of processing ultrasonic signals silently. This technology is able to identify the location of the user, habits to watch TV (distance from TV and the exact name of the channel that one is watching), health issues and much more. When a user is watching TV at home sitting on the sofa, someone might be monitoring him remotely and having information about everything such as the distance between the user and TV, the program being watched and the total time span of the TV being watched. Based on analytics drawn by ultrasonic tracking technology application, the application owner can suggest user many medical treatments or check-ups, habitual guidance and products to buy. Ultrasonic detection can also detect nearby electronic devices and the distance between the devices.

Fig: Ultrasonic tracking

Including Google and Facebook, various advertising platforms provide corresponding services to their customer for targeted advertising. Now technology has been upgraded and companies have switched to a new way to track their users. Companies are embedding these inaudible beacons in the ultrasonic frequency range between 18 to 20 kHz in order to track their user with the regular mobile application.
As per our observation, this might be a sigh of relief that ultrasonic tracking is not widely being used anywhere as of now but this technology is already deployed with several platforms and applications and this might be a privacy threat in the near future.

Technical background

The audio can be described in different ways based on frequency.

1. Infrasound (<=20 Hz) - This is a long wavelength signal that isn't audible to human beings.
2. Audible Sound (20 Hz to 20 kHz) - frequency between 20 Hz to 20 kHz is audible to human beings. Frequency above 18 kHz is difficult to hear by old age people.
3. Ultrasound (>=20 kHz) - This is a small wavelength and high-frequency signals that aren't audible to human beings.

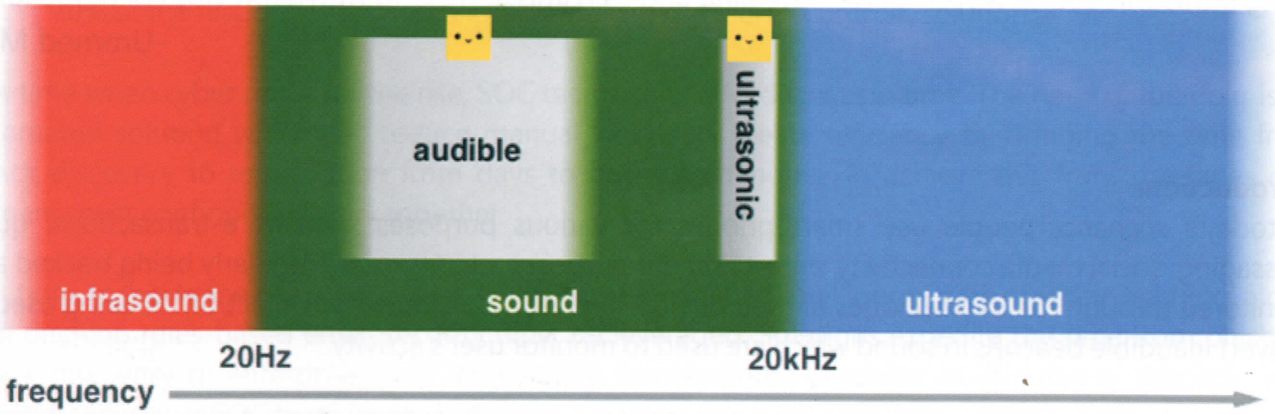
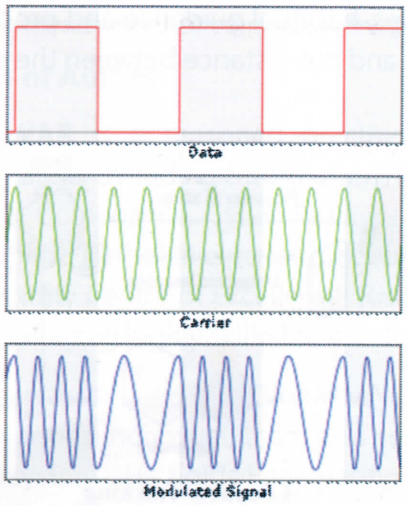


Fig: Sound Wave Classification

Encoding and Transmission of Information

We have selected frequency band 18 kHz to 20 kHz for the inaudible communication but still, the thing to note is the process to encode the information on the channel. We have several modulation techniques in signal processing but frequency shift keying (FSK) fulfills our entire requirement to make sure that no frequencies outside the selected band occurs. Other modulation techniques like (phase shift keying) PSK can introduce high distortion and discontinuity that can produce an audible sound.



In the image, we can observe that carrier signal get modified according to the data signal before processing. A high value (1) of data signal generates a high-frequency signal and on the other side, low value (0) data generates a low frequency (not zero).

Android platform provides a dedicated java class name as "AudiRecord" for recording audio from the microphone without compression. It is very easy to access this class and is sufficient enough to record audio signal without compression because compression technique may cut off inaudible beacons. To record the audio signals from this class, we also require RECORD_AUD permission from the user. Most of the times, people blindly allow this permission to the installed application and thus the app can listen to the inaudible beacons.

Detecting Ultrasonic beacons

We need a broad detection that can detect ultrasonic beacons on a large scale and need to ensure that the detection algorithm detects zero or a very few false positive which can later be manually verified. This filter detects signals only between 18khz to 20 KHz signals which include TV streams, environmental sound and echo sound in the mall etc.

For example, let's take 20 audio samples from different sources and plot a frequency distribution chart. Comparison of the frequency distribution with an arbitrary signal with distribution signal shows the anomalies in reflected files. The figure below shows a sample audio frequency plot that contains ultrasonic beacons. The detector alerts when it crosses the previously selected threshold value of near-ultrasonic frequency.

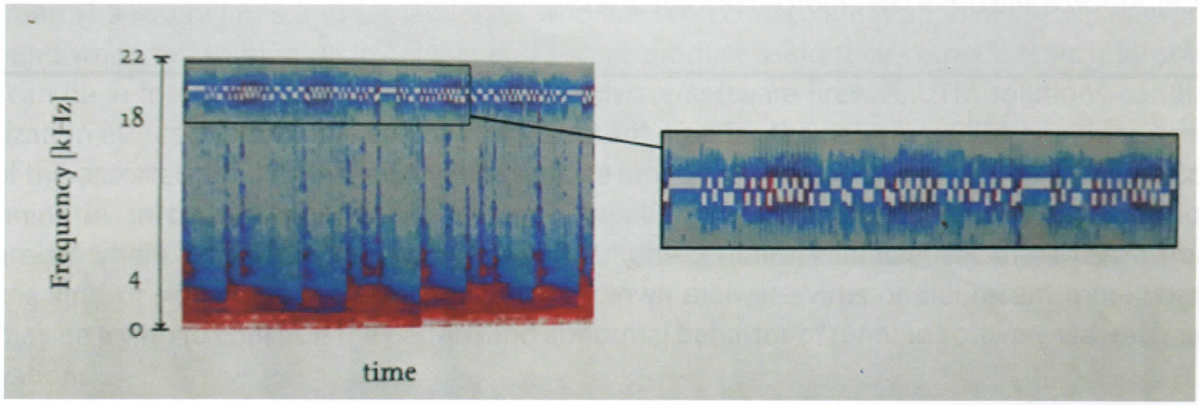


Fig: Ultrasonic detection

Many applications are using three commercial technologies namely Silverpush, Shopkick and Lisnr to detect and send the ultrasonic sounds. Researcher and forensics experts found several android applications those are using ultrasonic technologies to track user's activities continuously.

Forensics

Most of the applications which use inaudible beacons do not disclose its presence as it may lead to privacy issues and potential risk. The user can be fingerprinted by malicious applications using camera, accelerometer, proximity, and microphone of the mobile device. Kirin and Drebin are two popular methods for the static analysis of malicious Android applications that use ultrasonic tracking facility. Both methods detect the combination of malicious permission and source code of the application but generate more false positives, thus they are not useful for large collection of application.

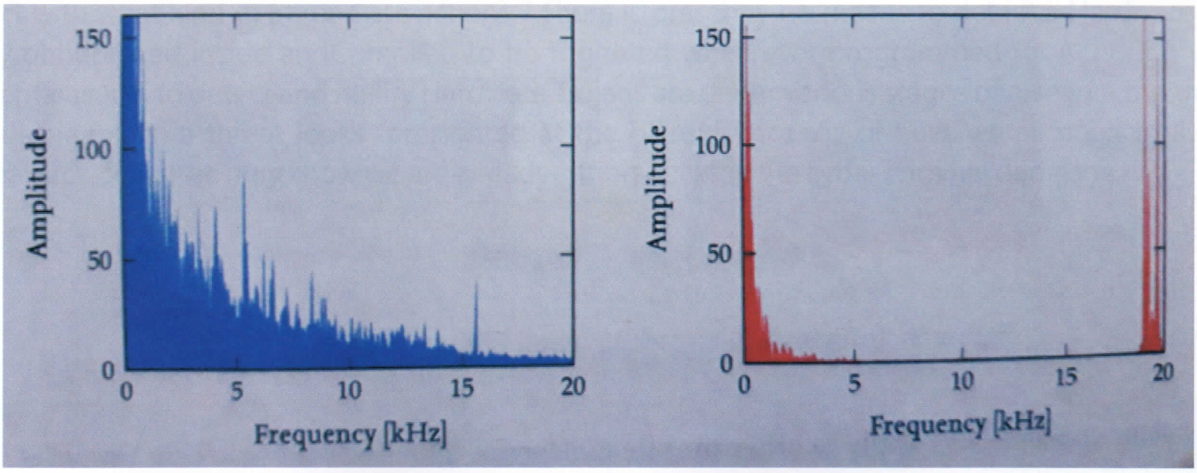


Fig: Ultrasonic tracking forensics

For effective analysis and detection of a maliciousapplication, we can use TaintDroid or CopperDroid methods. These methods analyze the targeted application during runtime and generate a behavioral analysis report. This can also monitor and detect the data leakage by third-party application. To protect our personal data and ultrasonic data we should never allow AUDIO_Record permission to the suspected application.

Introduction of Author

UMMEDMEEL has been working with several law enforcement agencies in and around NCR. He has helped and trained officers from the Police department of Rajasthan, Delhi, Haryana etc, CBI, Airforce and other law enforcement agencies.