Inaudible Sound as a Covert Channel in Mobile Devices

Luke Deshotels
Gist:

Leaking Data → 18kHz-19kHz Audio Waves → Oblivious Humans → 17kHz Max → Malicious Receiver
Two Types of Inaudible Sound

- **Isolated Sound**
  - Vibrator and Accelerometer
  - Felt but not heard
  - Discussed in paper

- **Ultrasonic Sound**
  - Speaker to Microphone
  - Dog Whistle
  - Focus of Presentation
Sound vs. Radio

● Radio (4G, Wi-Fi, Bluetooth, etc.)
  ○ Requires permissions
  ○ Security extensions monitor network connections
  ○ Often disabled by careful users

● Sound (Speakers)
  ○ No permissions
  ○ Often ignored by security extensions and users
  ○ Preventing detection is non-trivial
Ultrasonic Sound Assumptions

- Victim cannot hear 18khz or higher
- Only intended frequencies are produced
Ultrasonic Sound Proof of Concept

Dog Whistle Free App on iOS

FrequenSee App on Android
Prior Knowledge

Frequency Shift Keying

- Data
- Carrier
- Modulated Signal
Research Questions

- Transmission speed?
- Recorder/attacker proximity?
- Pockets?
- Practical Attacks?
Experiments

● Constants
  ○ Low Frequency 0: 18khz
  ○ High Frequency 1: 19khz
  ○ Device: Nexus 7 2013 Edition

● Variables
  ○ Bitrate
  ○ Distance
  ○ Fabric
Optimization

- Audible Clicks on Phase Shifts
- Amplitude Bias Against Phase Shifts
Bitrate Results*

Bitrate Limit ~345 bits/sec

*Plots are for illustration, but are not real data
Error Rate Evaluation

- Multiple Decoding Scheme
- Parity Numbers
- Transmission: 0s1t2r3a4w5b6e7r8r9y
- Received: 0t1t2r3a4w5b6e7r8r9y
  rs6tzaya4w5b6e7r8r9y
  *&(lasfn20981hn4029x

- Error Rate: 3.75% (3 bit errors out of 80)
Distance Results

Distance Limit
- ~100 feet

Device in pocket still leaks data at 20 feet.

*How did we get a Nexus 7 in a pocket?
Abuses

Used to bypass information flow security.

- PasswordManager leaks data to other app
- PasswordManager leaks data to other device
Large Scale Abuse Scenario

- Devices emit unique identifiers
- Recorders in entrances forward IDs to tracking systems
- Tracks devices with disabled networking (GPS, 4G, Wi-Fi, etc.)
Solutions

● Hardware solutions
  ○ Embed limits or use physical filters
  ○ Indicator light

● Software solutions
  ○ App to detect or log ultrasonic activity

● Train dogs to destroy ultrasonic devices
Future Work

● Higher frequencies on other devices
● Alternatives to frequency shift keying
● More sophisticated recording devices
● Implement solutions
Questions?
Source code available: https://bitbucket.org/ladeshot/ultrasonicfsk
alecdeshotels@gmail.com
Speaker Frequency Limits

Related Accelerometer Attacks

Tapprints

(a) \( \delta > \beta \)

(b) \( \delta \leq \beta \)

(Sp)iPhone
Isolated Sound Proof of Concept

VibrationX App

Accelerometer Monitor App on Touching Device
Quiet Sound Assumptions

- No drum-like surfaces
- Not touching user
- Not near user’s ear
- No animals
Inspiration

● Covert Channels
  ○ Forbidden communication between processes
  ○ For example: bank app talking to game app

● Limits of Human Perception

● Mobile Devices
Demonstrations

Follow along:
- FrequenSee for Android
- Dog Whistle Free for iOS

Demos
- Clicks
- Without Clicks