How to Phone Home with Someone Else's Phone

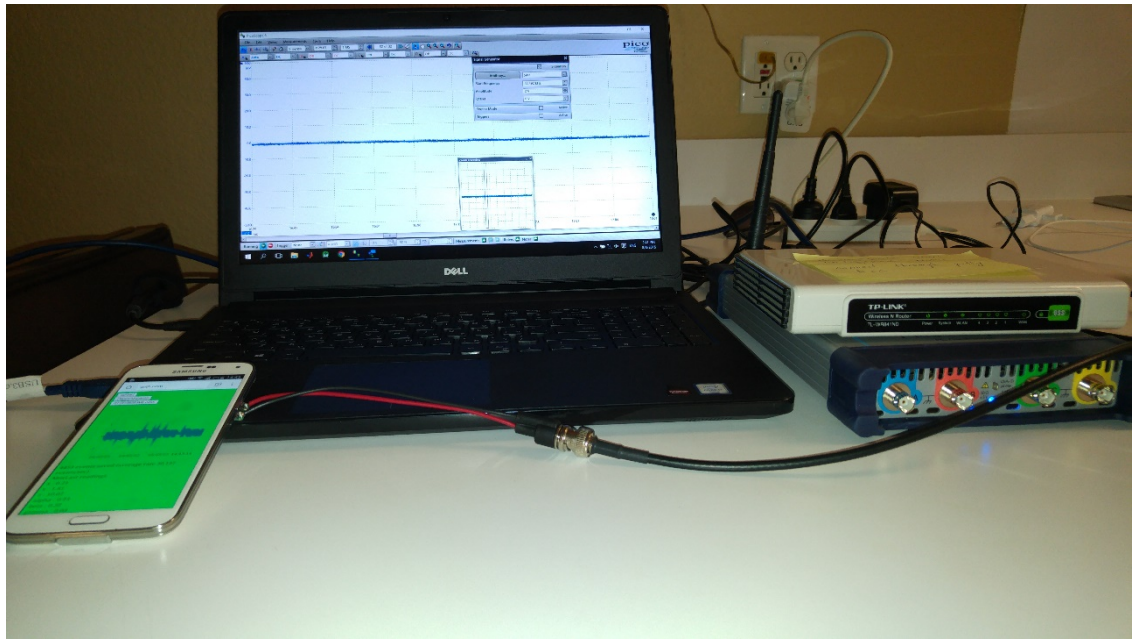


Information Exfiltration Using Intentional Sound Noise on Gyroscopic Sensors

Benyamin Farshteindiker
Nir Hassidim
Asaf Grosz
Yossi Oren

Poster Session on Thursday

Come and watch a live attack on Thursday at 18:30.



Outline

- Introduction

  Gyroscopes On Personal Devices

  The Attack

  Results

  Countermeasures

  Conclusions

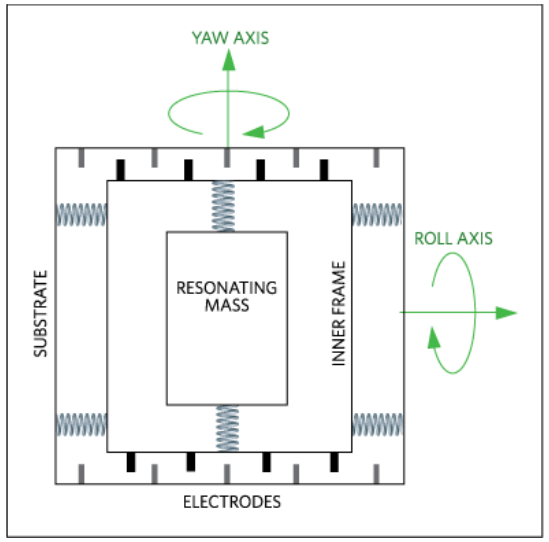
Implant Architecture

- Secret Collection – Microphone, camera, side-channel probe.
- Secret Exfiltration – RF backscatter, acoustical coupling, this work.
- Power Supply – Passive power, battery.

Outline

- Introduction
- Gyroscopes On Personal Devices
- The Attack
- Results
- Countermeasures
- Conclusions

Gyroscopes On Personal Devices



MEMS gyroscopes sense the angular rate of rotation.

Outline

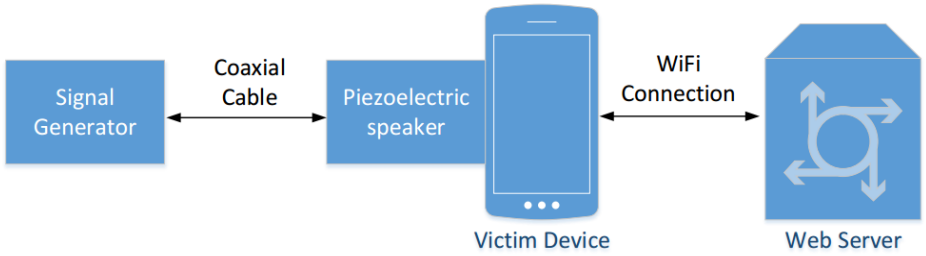
- Introduction
- Gyroscopes On Personal Devices
- The Attack
- Results
- Countermeasures
- Conclusions

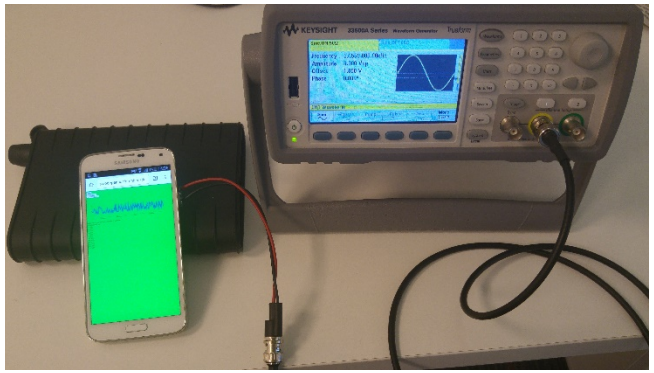
The Attack – Attack model

Base assumptions:

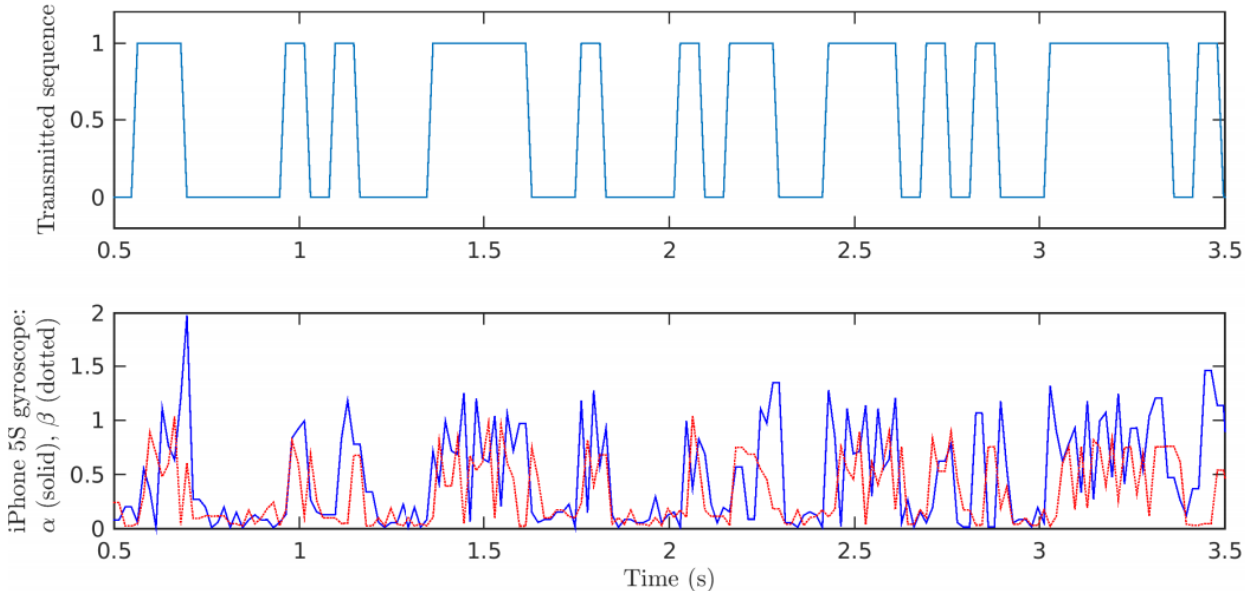
- The adversary manages to place the implant near the victim's mobile device.
- The implant has some secret it wishes to exfiltrate.
- The attacker has the ability to make the victim's mobile device display a website or run some unprivileged application.

The Attack – Evaluation Setup





The Attack – PRBS example



The Attack – Advantages

Advantages of our exfiltration scheme over traditional methods:

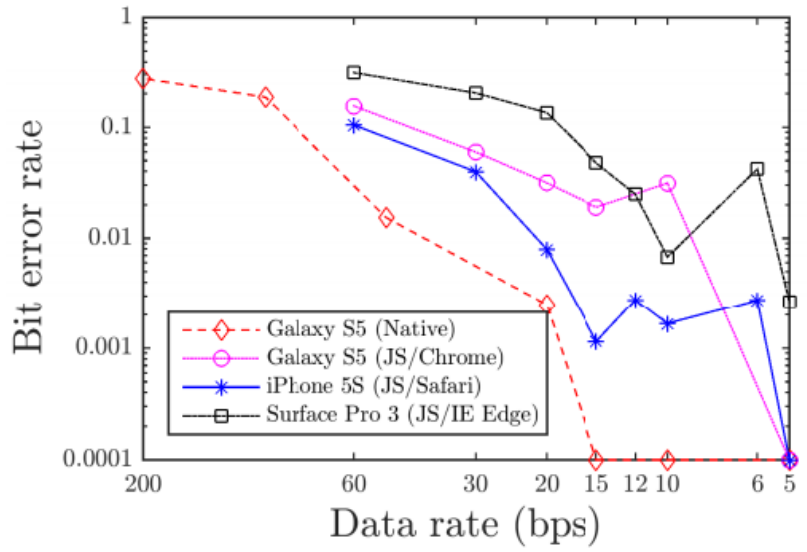
- Gyro access requires zero permissions or notifications
- Sensitivity of the sensor

Outline

- Introduction
- Gyroscopes On Personal Devices
- The Attack
- Results
- Countermeasures
- Conclusions

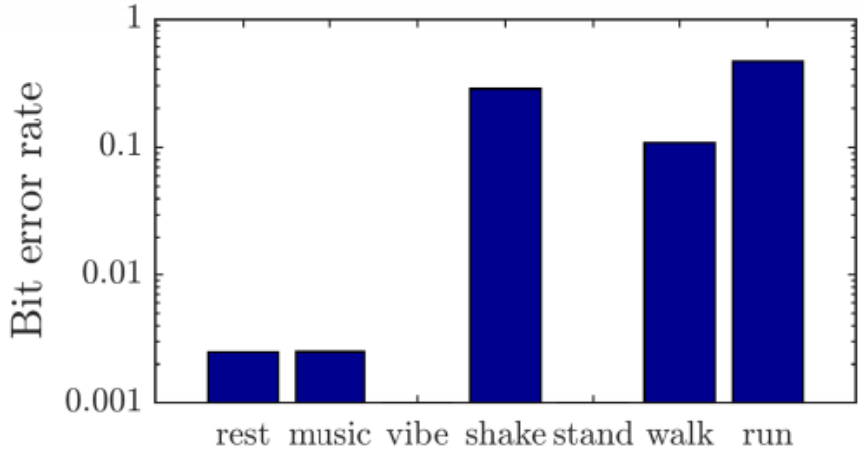
Results – Error rate

- Increasing amount of samples per data bit improve the results.
- Audio signal can't be heard by the human ear or detected as motion.
- Consumes less than 10 microwatt of power.



Results – Activity profiles

Samsung S5 results tested on different user activities running a native application.



Results – Capacity and power bounds

- Theoretical capacity of the channel is 1 Kbps with 60 Hz sampling rate.
- Can grow over 4 Kbps when increasing the sampling rate.

Outline

- Introduction
- Gyroscopes On Personal Devices
- The Attack
- Results
- Countermeasures
- Conclusions

Countermeasures

- Require permission to the gyroscope.
- Lower the sampling rate.
- Physical modification.
- Sensor fusion.

Outline

- Introduction
- Gyroscopes On Personal Devices
- The Attack
- Results
- Countermeasures
- Conclusions

Conclusions

- Low cost implants
- No exposure risk
- Undetectable bugs
- Allow monitoring many implants simultaneously

Conclusions – Two factor authentication



Questions?

Benyamin Farshteindiker
farshben@post.bgu.ac.il
https://iss.oy.ne.ro/PhoneHome



* Don’t forget to come to our poster session on Thursday.