g the Air Gap

Jose Padilla, Jesse Lozano, Mohammed Hague, Danny Tran
oute

Background

In today's digital ecosystem, hackers are a concerning threat. It is widely known that any system connected to the Internet is vulnerable. But what about an "air-gapped" computer? One that is not directly connected to the Internet or any other system that is connected to the Internet.

Objective

- Hack an air-gapped computer by investigating the ways of capturing data that can be leaked through physical quantities such as LED lights, sound, and magnetic fields emitted by a CPU.
- Create signal blockers/jammers to protect sensitive data.

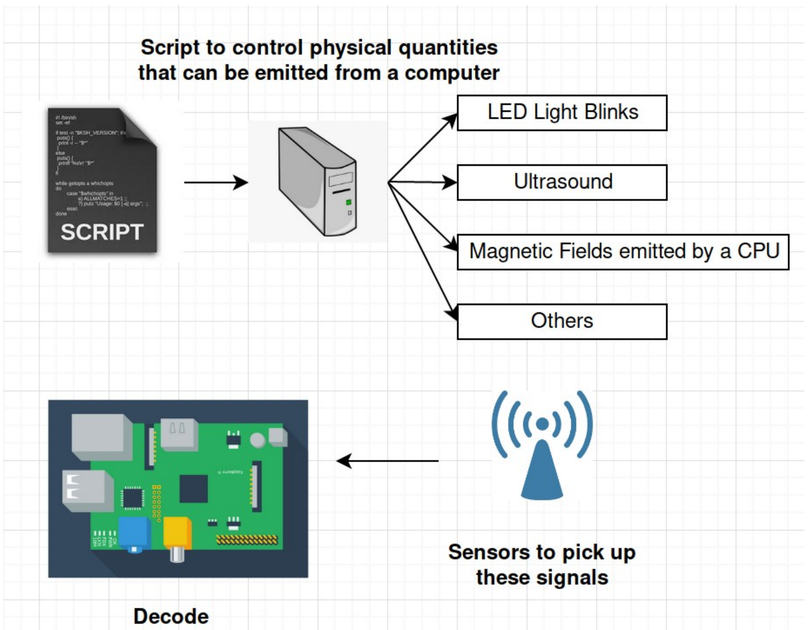

Figure 1: Flow diagram for leaking data and capturing it

Accomplishments

- Focus on leaking data through ultrasound for Fall Quarter.
- High-level C++ class to interface with a system's native sound card API to output different tones for different frequencies of a sine wave.
- Script that converts files into binary data and uses class described above to output two different tones, one for binary 1 and one for binary 0.
- Raspberry Pi with microphone to pick up data emitted through ultrasound and decode it.
- Raspberry Pi with speaker to output random ultrasound noise for jamming.

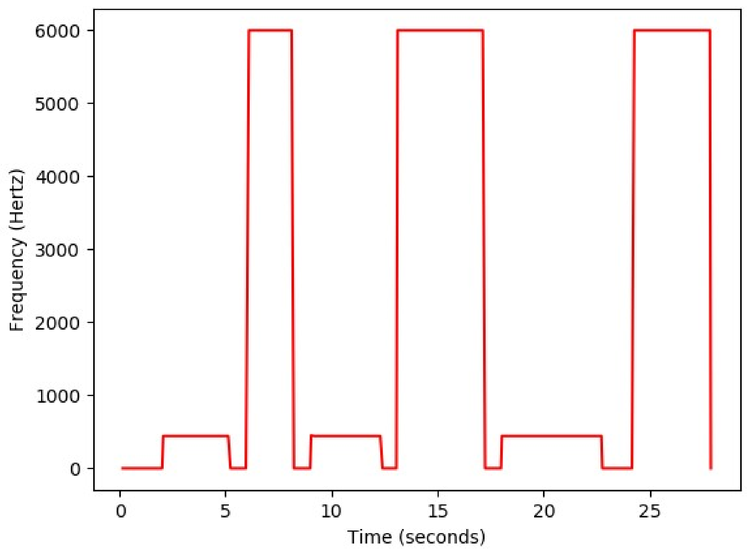

Figure 2: Decoding - 00100011 10000111

Future Goals

- Filtering out noises when decoding ultrasound.
- Decoding in real-time through multithreading.
- Research building microphone to reduce size and lower cost.
- Transmit data through other physical quantities.

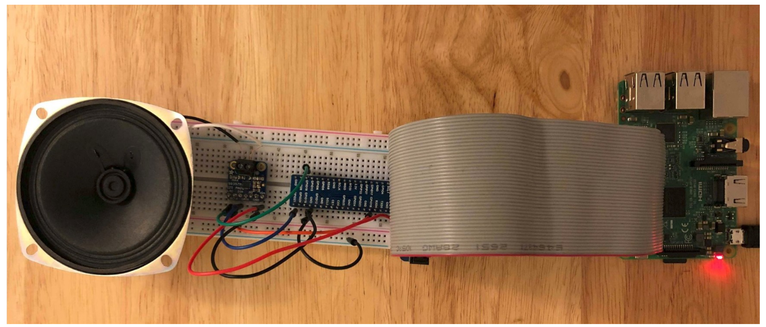

Figure 3: Jammer outputting random ultrasound noise

References

Adams, Carrara. "On Acoustic Covert Channels Between Air-Gapped Systems." SpringerLink, 5 Apr. 2015 https://link.springer.com/chapter/10.1007/978-3-319-17040-4_1

Greenberg, Andy. "This Researcher Steals Data With Noise and Light." Wired, Conde Nast, 7 Feb. 2018, https://www.wired.com/story/air-gap-researcher-mordechai-guri/.

Kovacs, Eduard. "Stealthy Data Exfiltration Possible via Magnetic Fields." SecurityWeek, 8 Feb. 2018, https://www.securityweek.com/stealthy-data-exfiltration-possible-magnetic-fields.

The Henry Samueli School of Engineering
University of California · Irvine