Hacking the Air Gap

Jose Padilla (CpE), Jesse Lozano (CpE), Mohammed Haque (CpE), Danny Tran (CSE)
Professor Zhou Li
Department of Electrical Engineering and Computer Science
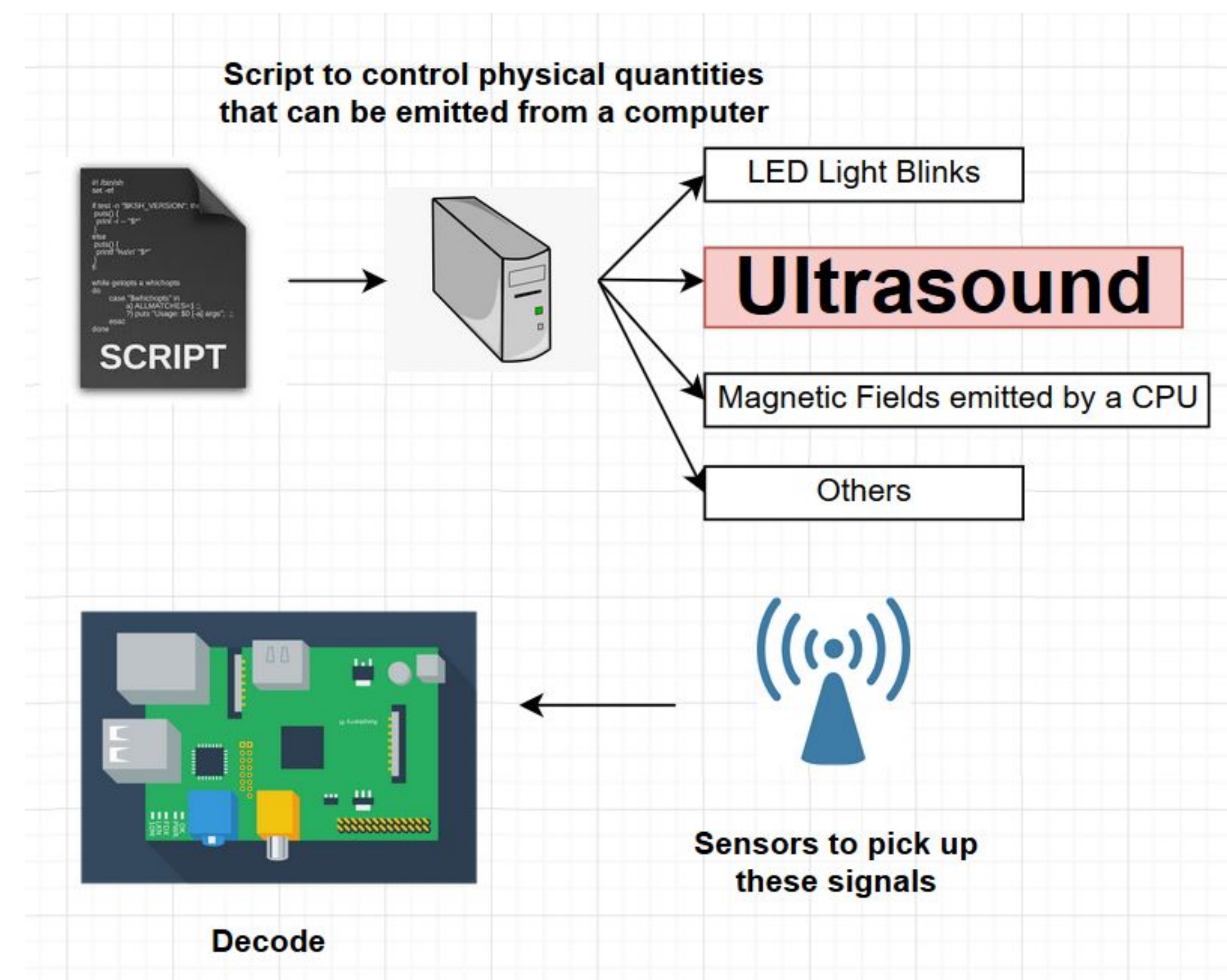
Background

In today's digital ecosystem, malicious 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.

Project Goal

The goal of this project is to successfully 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. By demonstrating the different ways a computer can be attacked, we can create signal blockers/jammers to protect sensitive data.

Script to control physical quantities that can be emitted from a computer

SCRIPT → [computer] →
- LED Light Blinks
- **Ultrasound**
- Magnetic Fields emitted by a CPU
- Others

Sensors to pick up these signals

Decode

Milestones

1. Write a keylogger that is able to output data by ultrasound or other means.
2. Set up a raspberry pi with necessary sensors and transmitters (ultrasound, magnetometer, camera, etc.).
3. Write python code for the pi to decode transmissions from hacked computer.
4. Find ways of stopping attacks either by physically blocking transmissions or by jamming them with a transmitter.
5. Repeat steps 2 to 4 with other means of transmission or attempt to increase attack range.

Progress

- Keylogger complete
- Can detect and log frequencies
- Wrote a high-level class that uses the system's native sound card API to output different binary tones

Materials Needed

- Raspberry Pi / Arduino
- Ultrasound sensor
- Magnetometer
- Camera
- Computer to hack

References

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

THE HENRY SAMUELI SCHOOL OF ENGINEERING
UNIVERSITY of CALIFORNIA · IRVINE