g the Air Gap

ECHO

Jose Padilla, Jesse Lozano, Mohammed Haque, Danny Tran

ute

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.

Project Goal

The goal of this project is to demonstrate data leakage from an air-gapped computer via ultrasound. We envision an external system with WiFi for outside access that can bidirectionally communicate with the hacked computer efficiently and accurately. We hope that our ultrasound communication protocol will have other usages too.

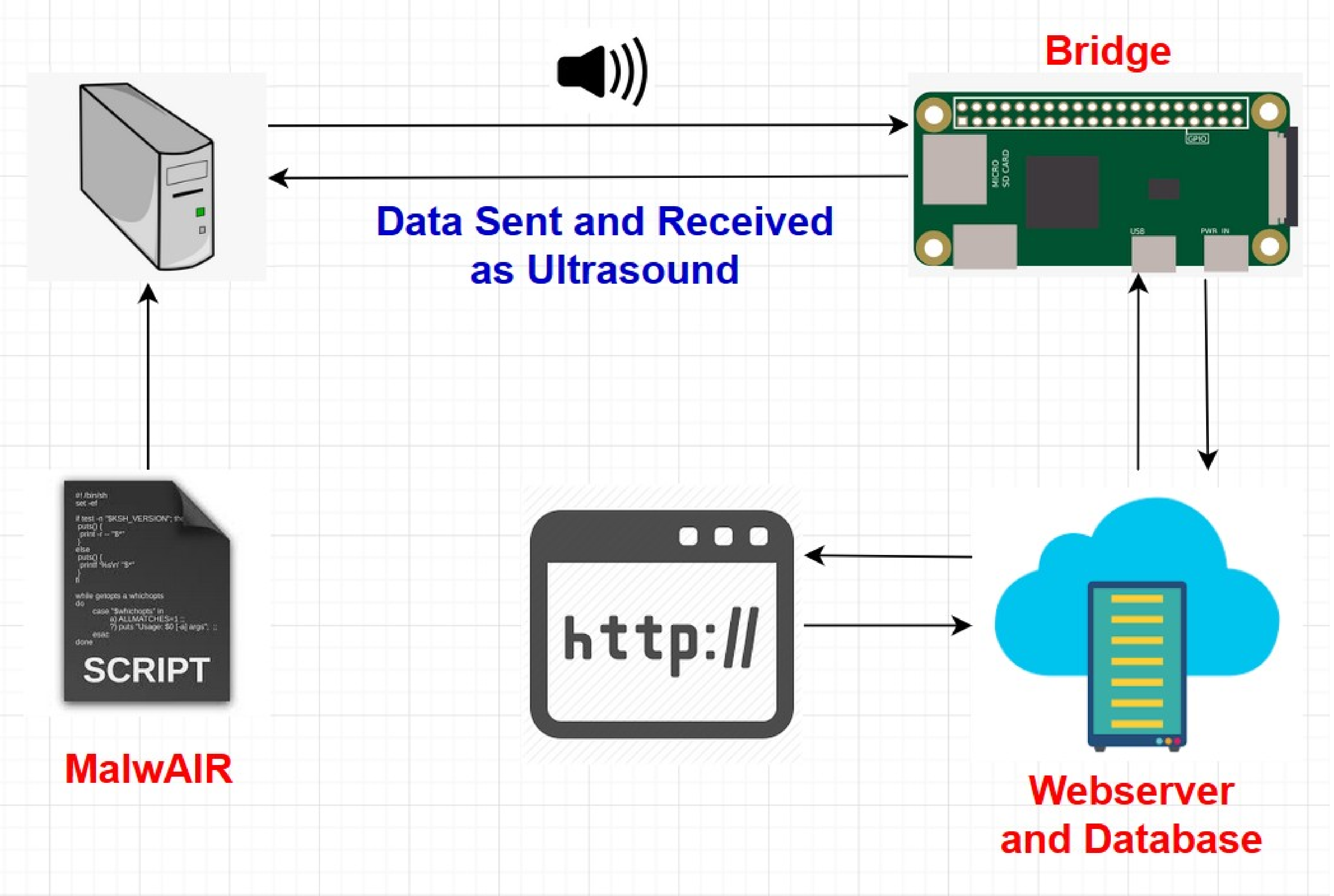

Figure 1: Flow diagram for leaking data through ultrasound and capturing it

Milestones

- MalwAIR - A C++ tool that uses RtAudio to interface with a computer’s native sound card API to transmit data by outputting pure sine waves with frequencies over 20 kHz (ultrasound)
- Bridge 1.0 - Raspberry Pi 3B+ and USB Microphone
  - Records data emitted through ultrasound and decodes it
  - Protocol: 3 frequencies for bit 0, bit 1, and separator
  - Filter noises and is fairly accurate, but slow and chunky
- Bridge 2.0 - Raspberry Pi Zero, Teensy 4.0, Electret Microphone
- New Ultrasound Communication Protocol
  - Data comes in bytes, and a byte can be broken down into 2 hex values.
  - 16 different frequencies, one for each hex value
  - Extra frequency identifying the hex value is the 4 MSBs of a byte when played simultaneously

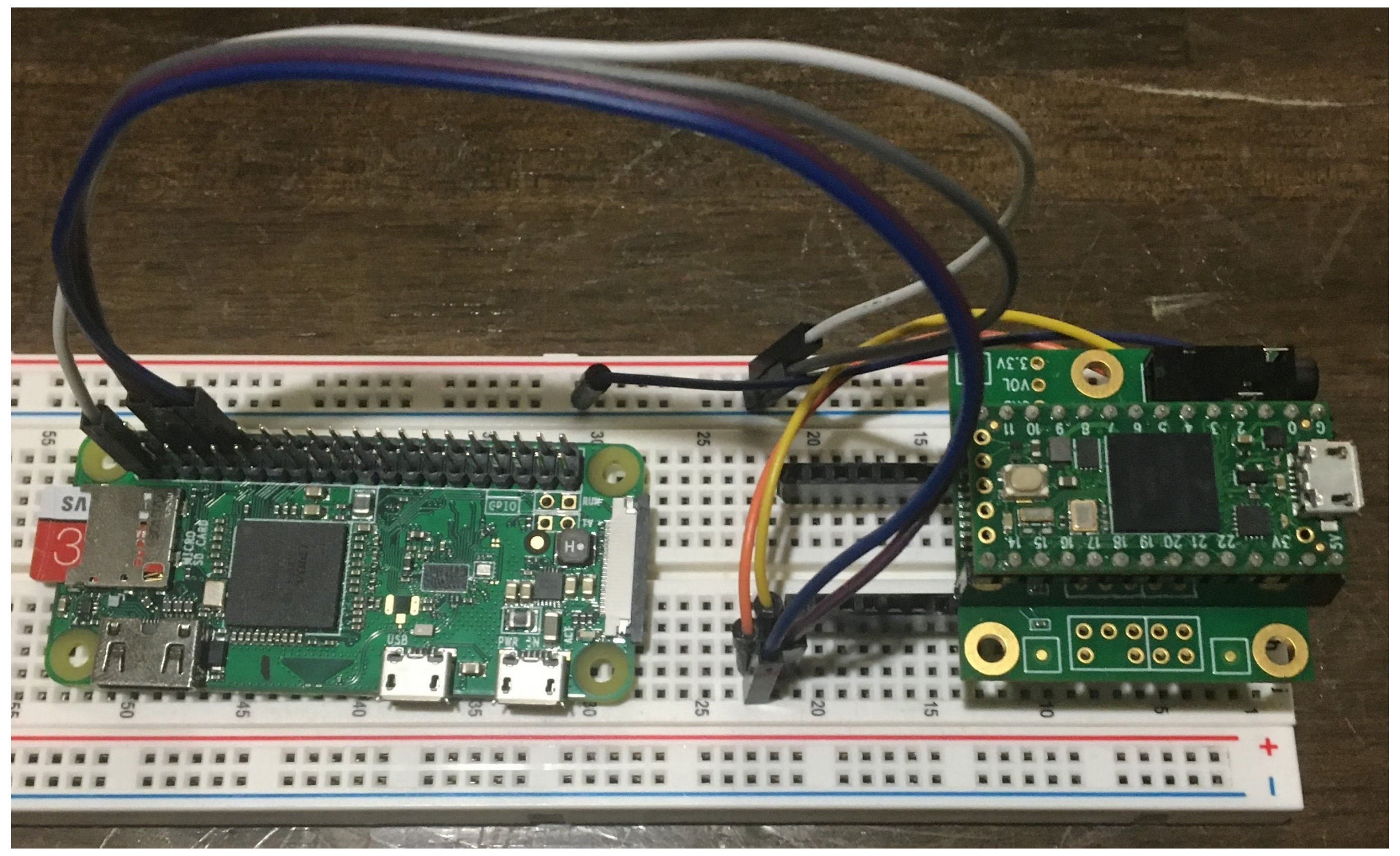

Figure 2: Bridge 2.0 Setup - Teensy 4.0 reads input from an electret microphone, does audio processing, and sends decoded data to the Raspberry Pi Zero through UART

Future Work

- New ultrasound communication protocol isn’t working well because of hardware limitations
- Bidirectional communication with hacked commuter
- Database to upload leaked data to
- Website to access leaked data and remote control RPi

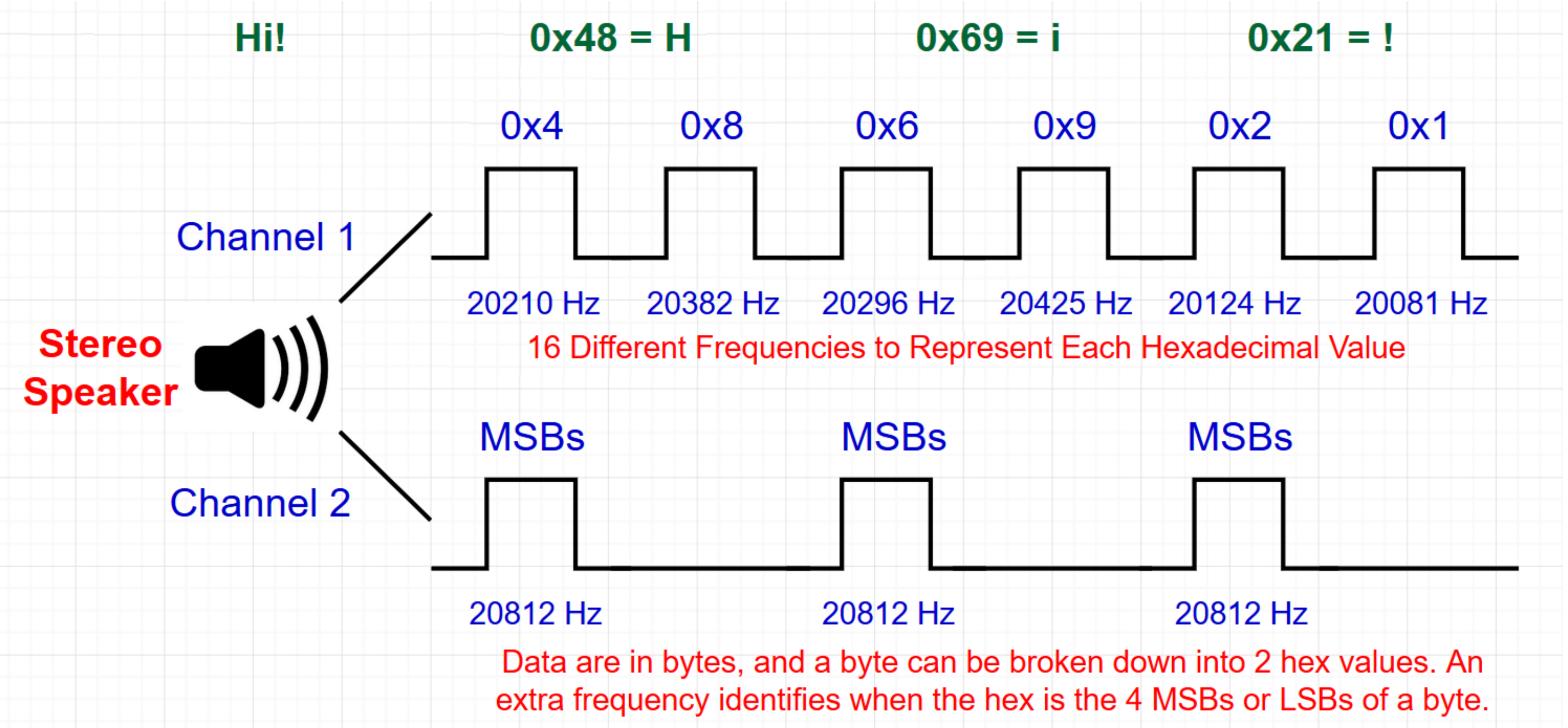
Hi!
0x48 = H
0x69 = i
0x21 = !
0x4
0x8
0x6
0x9
0x2
0x1
Channel 1
20210 Hz
20382 Hz
20296 Hz
20425 Hz
20124 Hz
20081 Hz
16 Different Frequencies to Represent Each Hexadecimal Value
Stereo Speaker
MSBs
MSBs
MSBs
Channel 2
20812 Hz
20812 Hz
20812 Hz
Data are in bytes, and a byte can be broken down into 2 hex values. An extra frequency identifies when the hex is the 4 MSBs or LSBs of a byte.

Figure 3: Ultrasound communication protocol

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