Embedded Security

EECE 5698-08: Special Topics: Cyber-Physical Security of IoT Systems in the Age of AI

Lecture 4: Transduction Attacks and EMI

Prof. Kevin Fu

September 18, 2025

https://spqrlab1.github.io/emsec/

Last Time: Signals and Systems Refresher

- **Frequency domain:** Fourier transform, frequency response, spectrogram/waterfall plot
- **Filters:** low-pass, high-pass, band-pass, and band-stop/notch filters shape signals for desired applications such as hearing, radios, and speakers.
- **Resonance:** systems amplify at natural frequencies, for example train wheel squeal.
- **Sampling (Shannon–Nyquist):** must sample at least twice the signal frequency to avoid aliasing.
- **Signal-to-noise ratio:** determines survival of meaningful signals in noise, with real-world path loss limiting attacks.

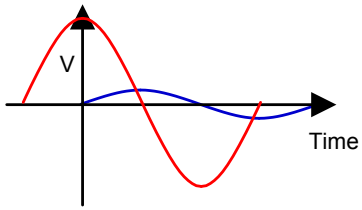
Today's Learning Goals

- Gain experience with transduction attacks and the underlying physics of modulation.

Pop Quiz #2

- Write your name on paper

Analog Side Channels



Analog

Digital

"Read"
Property: Confidentiality
Example: Power Analysis

"Read"
Property: Confidentiality
Spectre, Meltdown, …

"Write"
Property: Integrity
Example: Sensors

Sensor Signal Conditioning Path

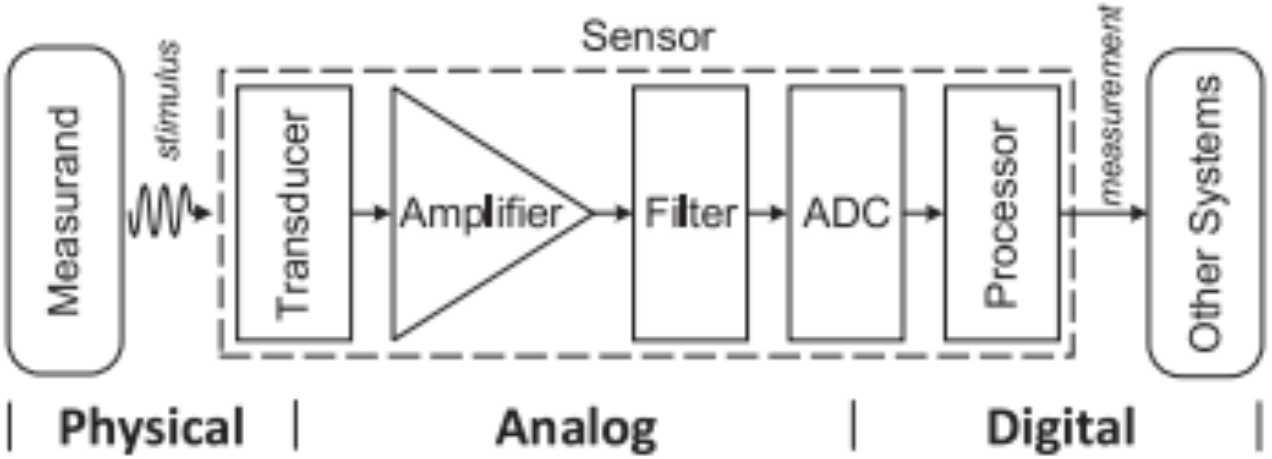
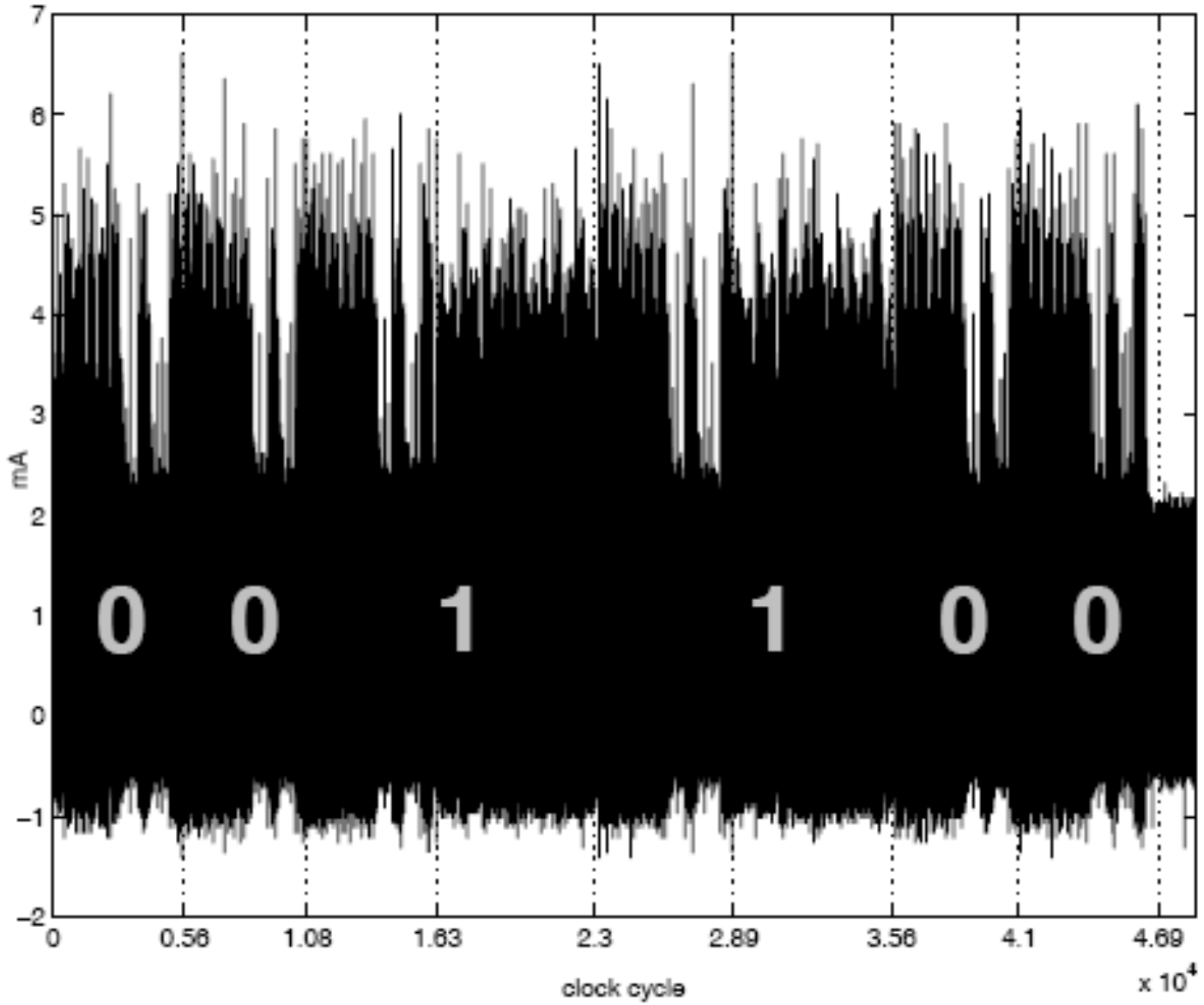


Figure 2.1: A general signal conditioning chain of sensors. Signals flow from left to right through each component and transform from the physical stimulus (input) to an analog intermediate and finally to a digital representation (output). Depending on the specific design, variations to this schematic may include multiple amplifiers or filters, no filters, filters before the transducer (e.g., CMOS) or amplifier, other circuits (e.g., comparators), etc.

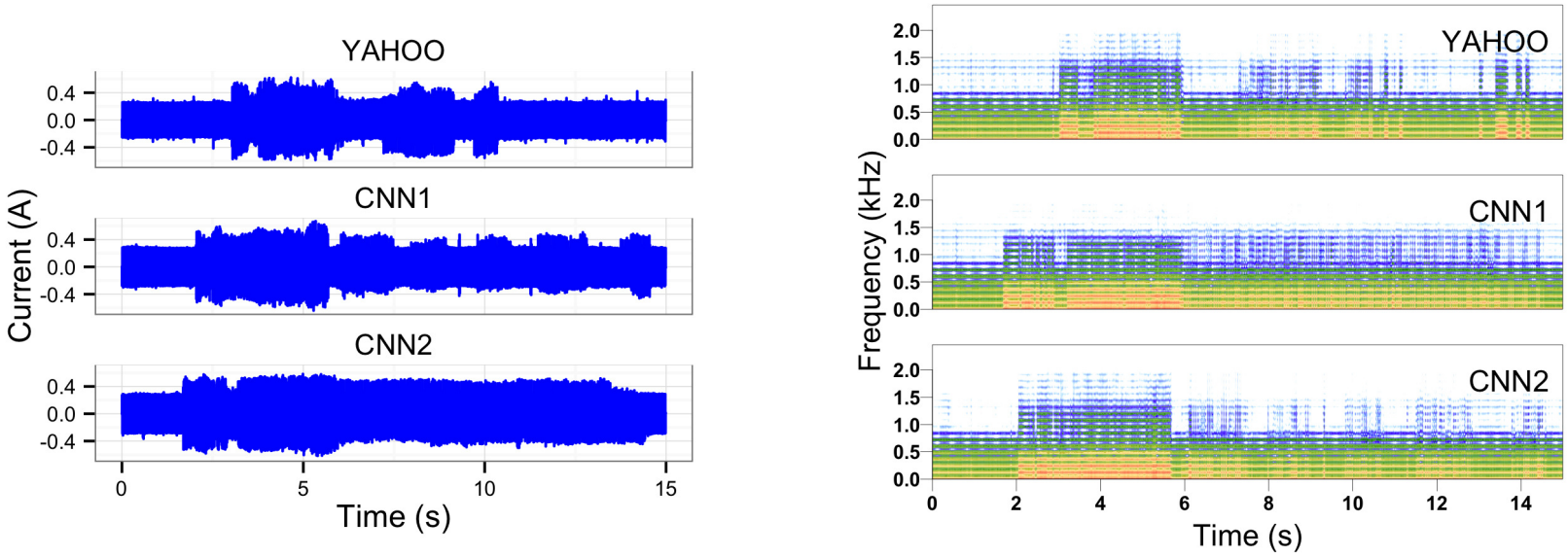
["Protecting the Security of Sensor Systems" by Connor Bolton, Ph.D. Thesis, University of Michigan, 2022]

Analog Side "Read" Channels: Confidentiality

Power Analysis



Review: Power Spectrum



(a) Time-domain plots

(b) Spectrogram plots

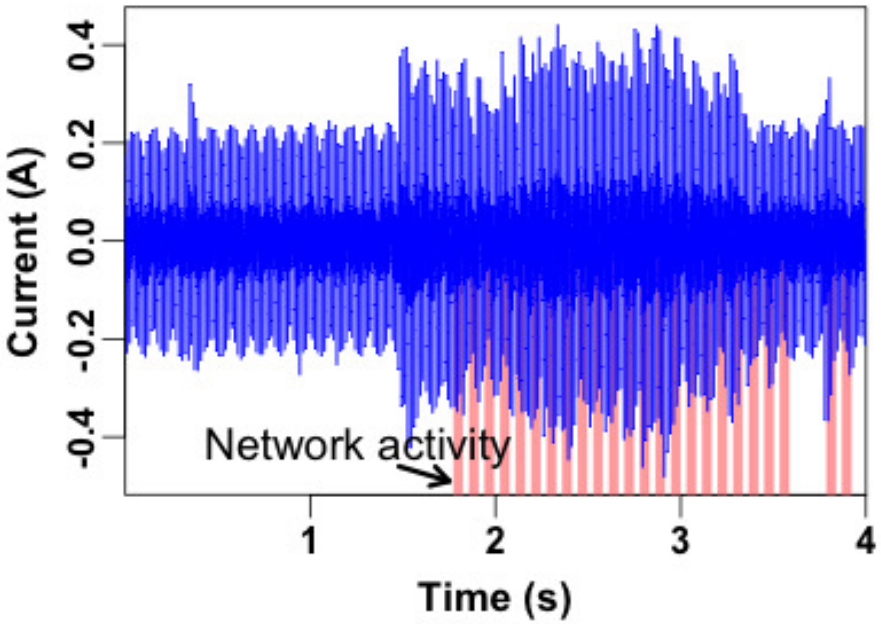
Fig. 1: Time- and frequency-domain plots of several power traces as a MacBook loads two different pages. In the frequency domain, brighter colors represent more energy at a given frequency. Despite the lack of obviously characteristic information in the time domain, the classifier correctly identifies all of the above traces.

"Current Events: Identifying Webpages by Tapping the Electrical Outlet" by Clark et al, ESORICS 2013

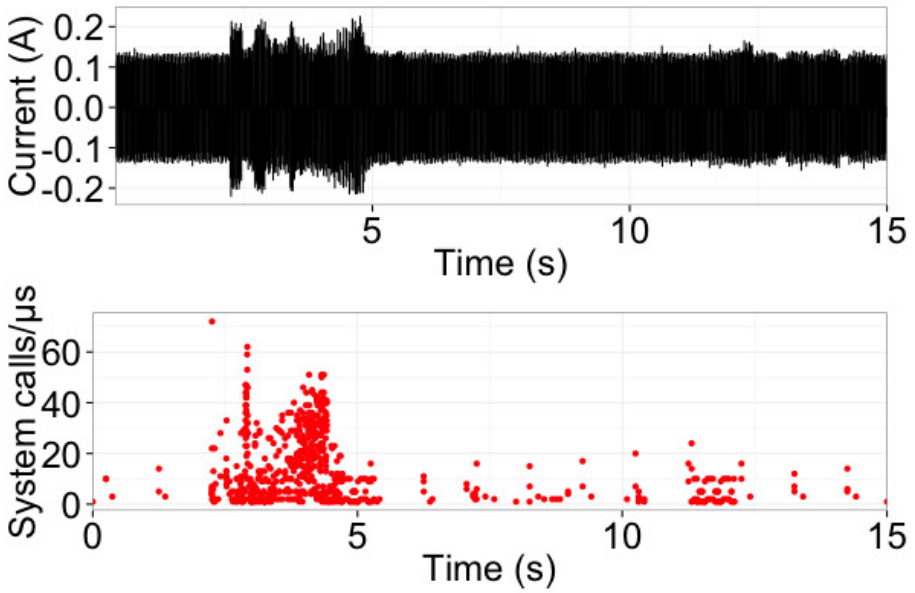
Condition	Power (W) vs. Baseline
Baseline (idle, screen off)	**8**
One core at 100%	+7
Two cores at 100%	+11
GPU at 100%	+11
Wired network saturated	+2
Wireless network saturated	+3
File copy, SSD to SSD	+6
Screen at maximum brightness	+6

Table 1: MacBook power consumption under various types of load. Numbers beginning with + are relative to the baseline of 8 W.

"Potentias est Scientias" by Clark et al, USENIX HotSec 2012



(a) The network activity is correlated with high current consumption, but is not the only cause. Spikes before and after network activity show that local computation dominates the consumption.

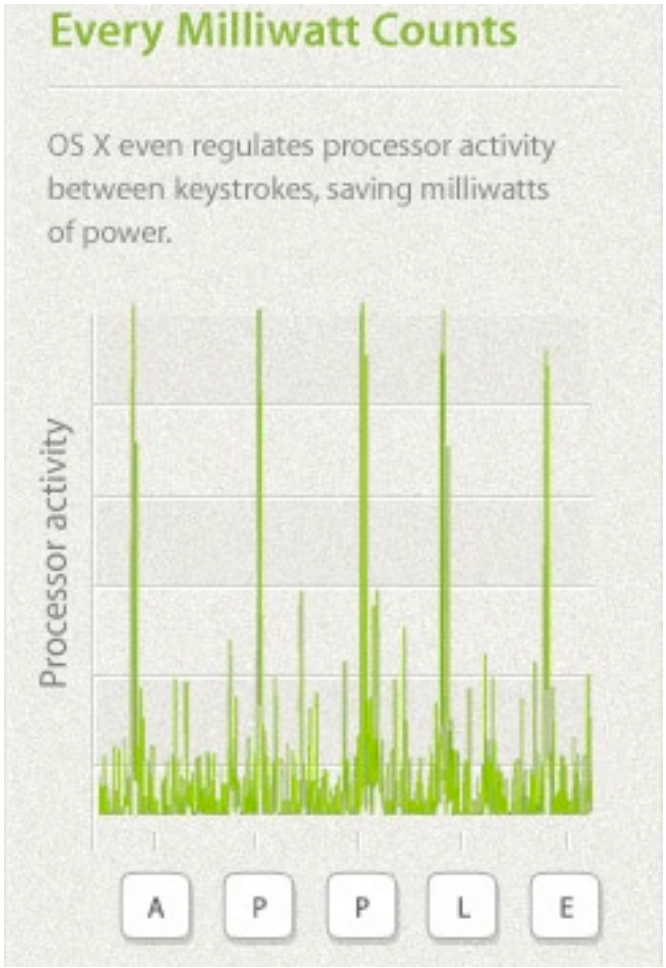


(b) The system call activity (as measured by DTrace) is also correlated with high current consumption, and our results suggest that systems exercised by system calls are a major cause of consumption.

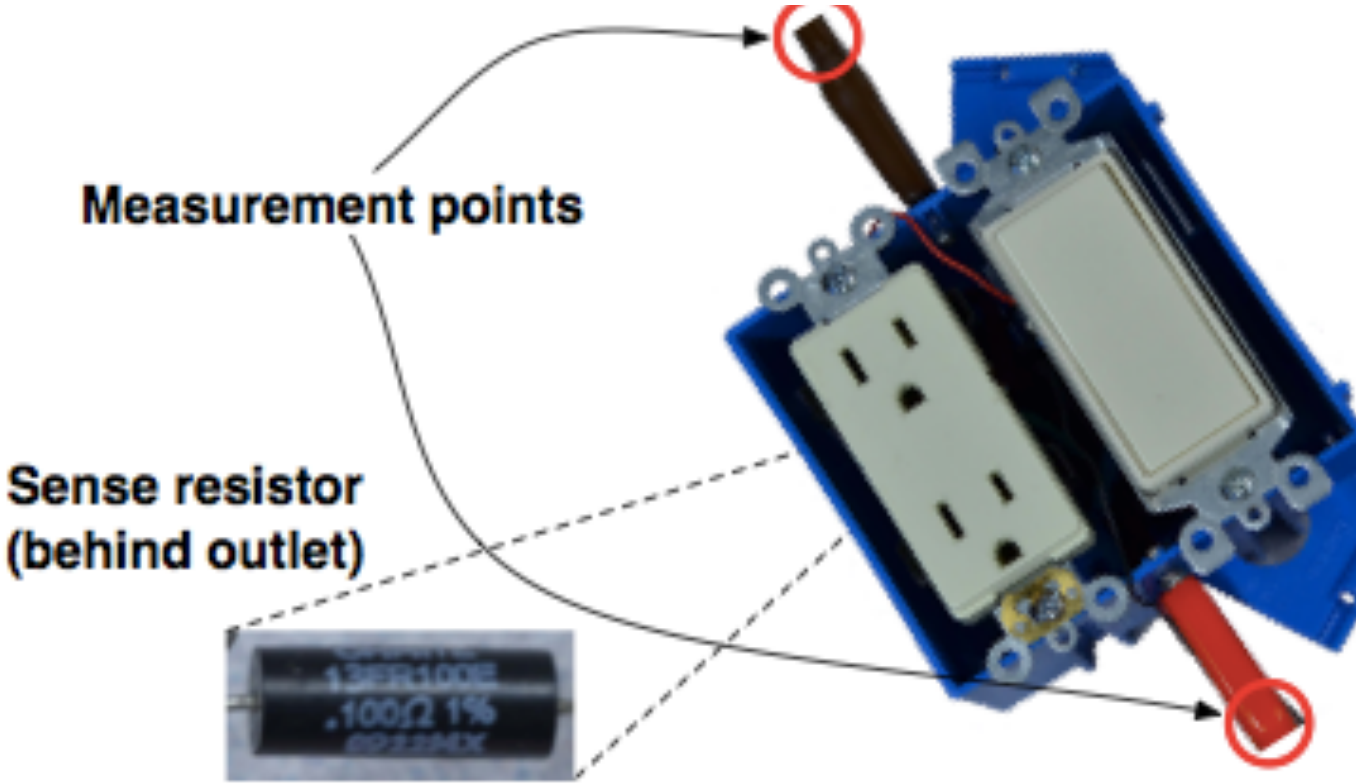
Fig. 2: Time-domain plots as a MacBook loads webpages. Both network activity and system calls appear to correlate with energy consumption.

Analog Cybersecurity: Using Read Side Channels for Defense

Detecting Malware at Power Outlets

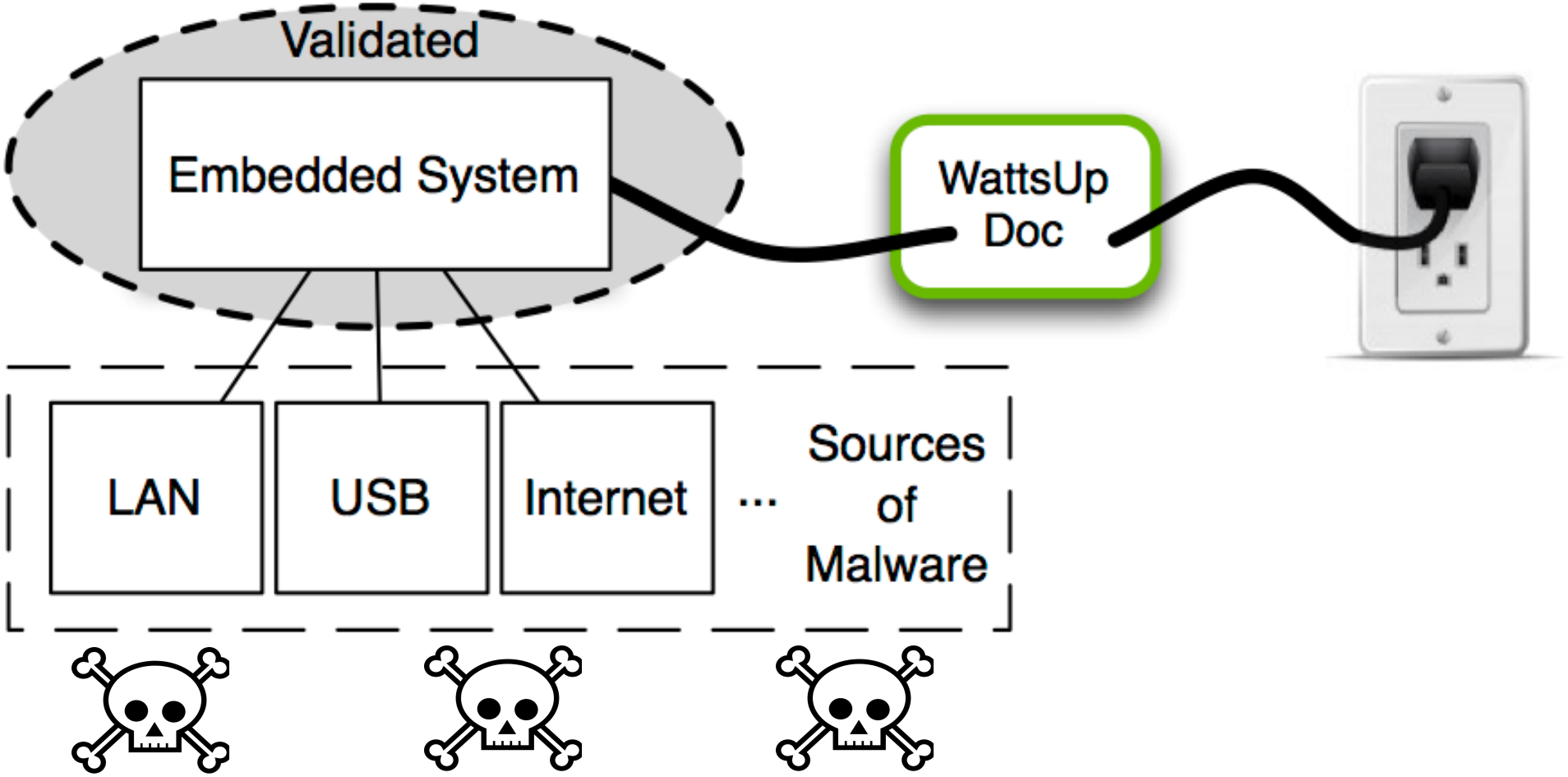


(a) An Apple advertisement from 2009 [6] touts energy-efficiency gains that also happen to reveal keystrokes in power traces.



- "Potentia est Scientia: Energy Proportionality Enables Whole-System Power Analysis" by Clark et al. In USENIX HotSec, 2012.

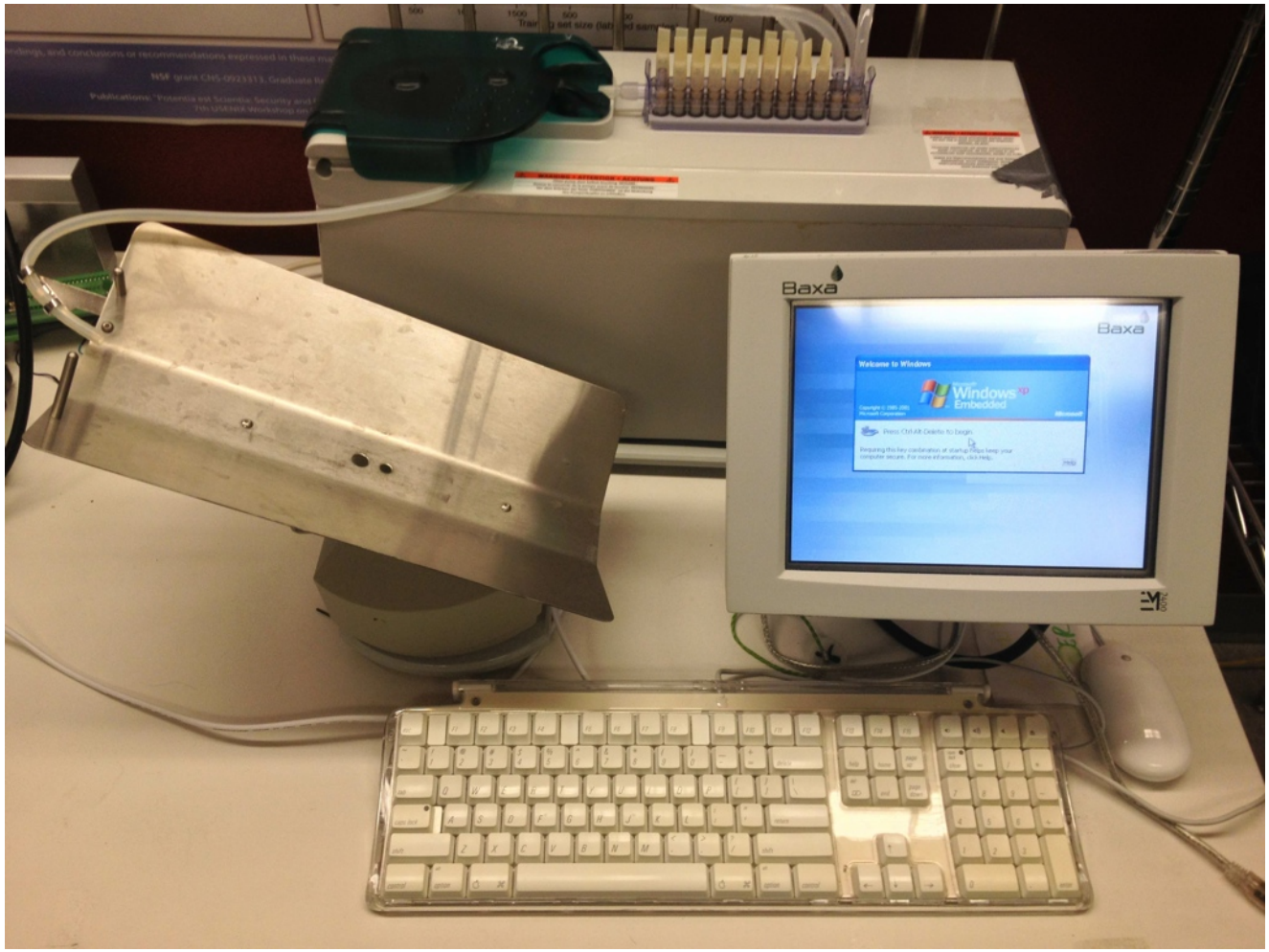
WattsUpDoc



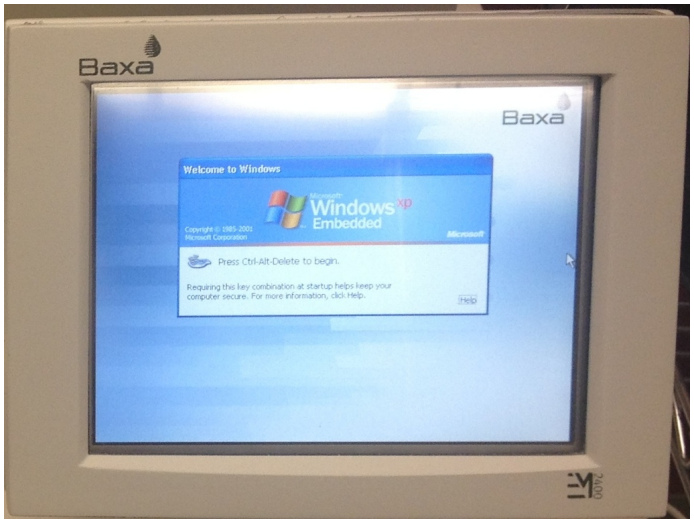
- "WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices" by Clark et al. In USENIX HealthTech, 2013.

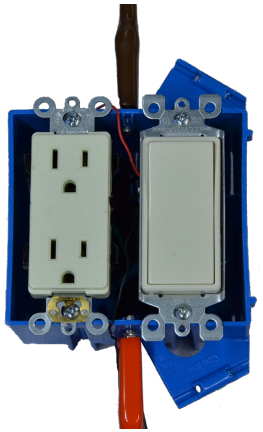
Pharmaceutical Compounder

- Mixes solutions, verifies output
- Flushes inputs
- Idles

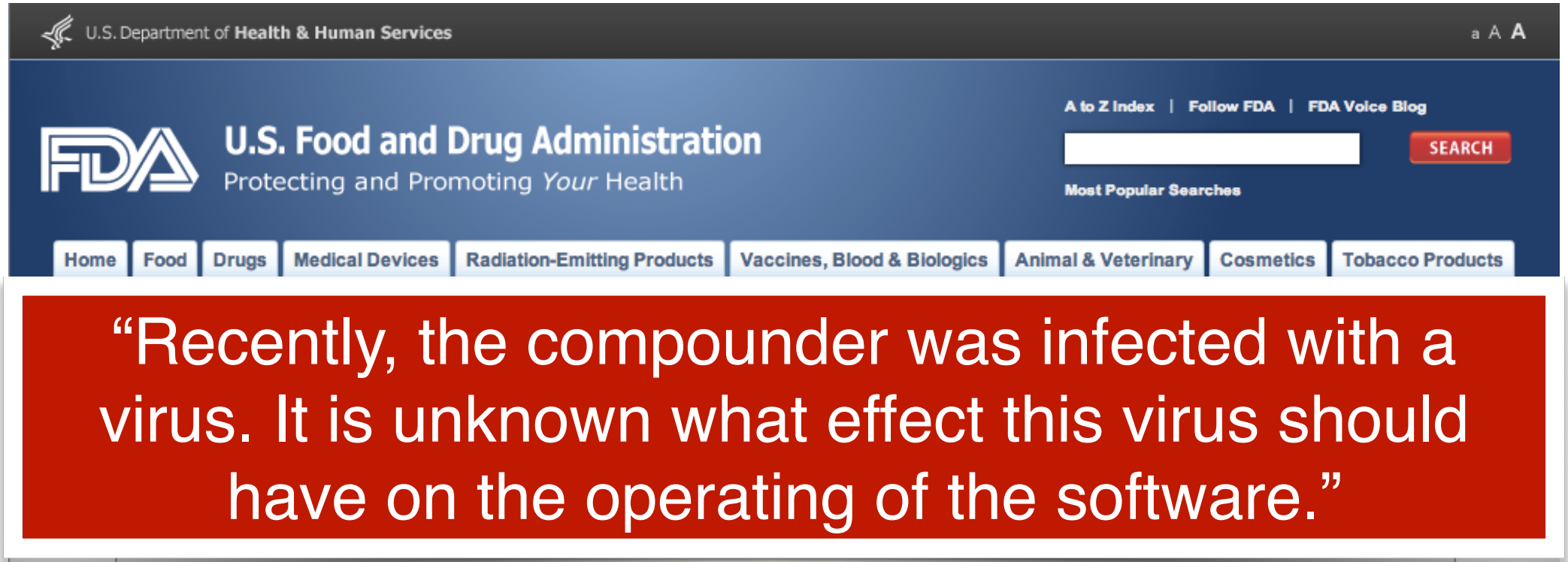


Power Analysis of Medical Devices





The Problem…



"Recently, the compounder was infected with a virus. It is unknown what effect this virus should have on the operating of the software."

BAXA CORPORATION BAXA EM2400 COMPOUNDER Back to Search Results

Event Type Malfunction

Event Description

The (b) (6) pharmacy department uses a baxa em2400 compounder to make tpn's and other admixtures. Recently, the compounder was infected with a virus. The virus has been contained on the em2400 compounder. It is unknown what effect this virus should have on the operating of the software. (b) (6) information systems department together with the pharmacy has requested that baxa provide a microsoft security patch to prevent this infection from occurring again. Baxa is unwilling to allow these patches to be applied to the baxa em2400. Instead baxa has recommend that we place a router with the functionality for a firewall between the compounder and the network (b) (4) as protection. In a single case, this may be a possible solution. (b) (6)'s manager indicates that if this was the routine solution, (b) (6) would then have to procure and maintain over 1000 routers institution wide. That approach is not sustainable by (b) (6) nor the marketplace. I am interested to hear about fda's requirement for medical devices to have security patches that protect the device from contamination.

The Problem

- Malware infects medical devices
- Solutions in the consumer space **do not readily apply**

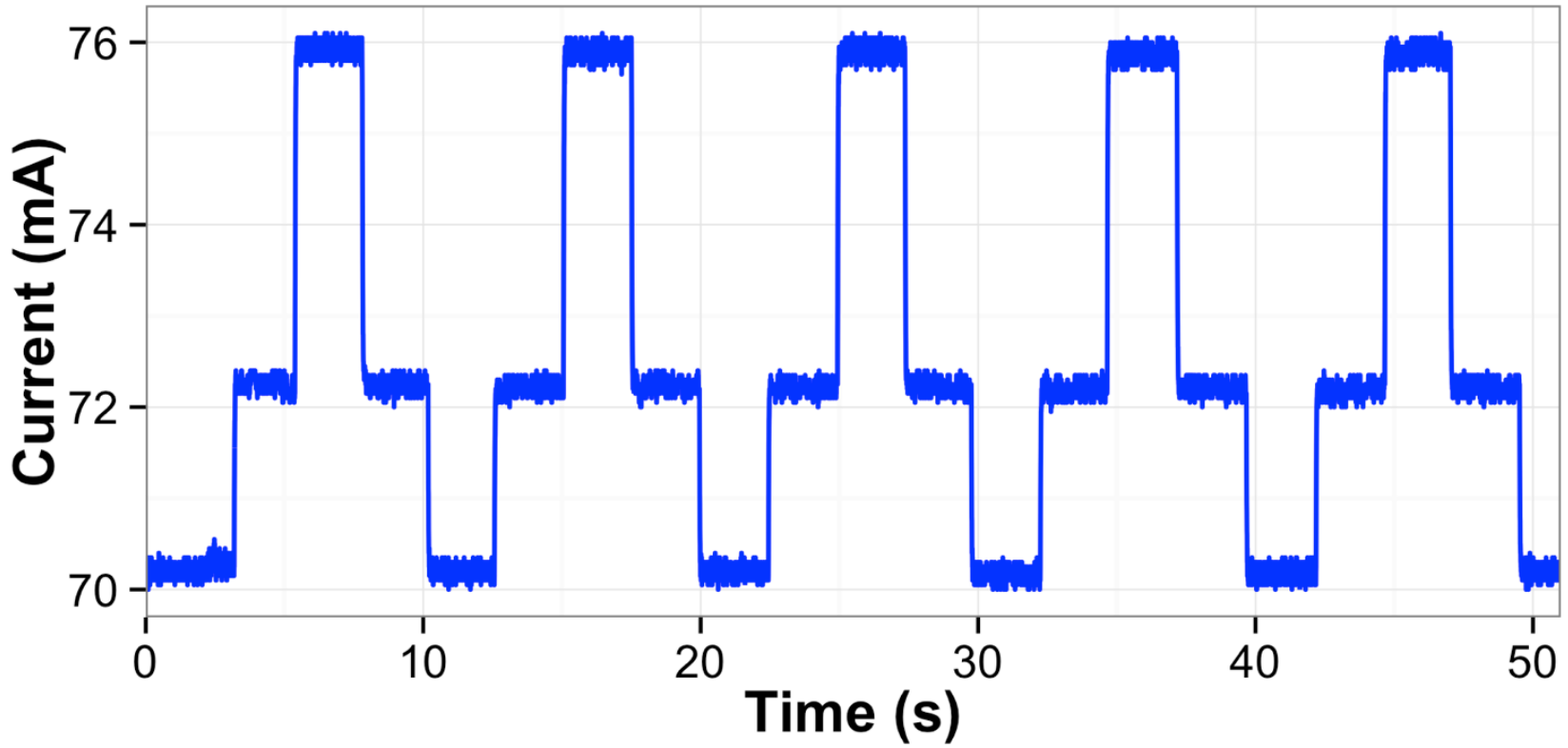
"Less than **1%** of our devices are network-connected."

-Lynette Sherrill, this morning

Properties

	No software changes	No updates	No manual configuration	No network connection
Antivirus	x	x	✓	✓
Firewall	✓	✓	x	x
NIDS	✓	x	x	x
WattsUpDoc	✓	?	✓	✓

Power Analysis

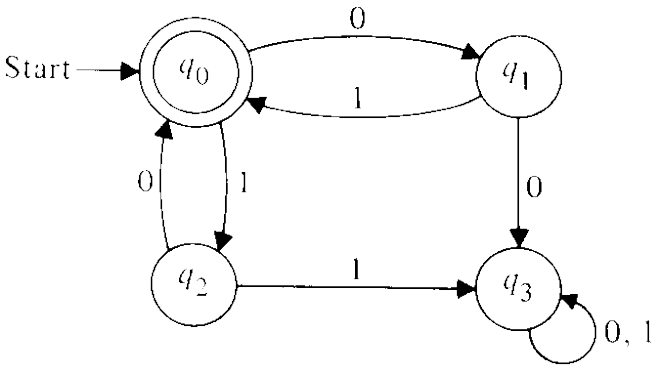


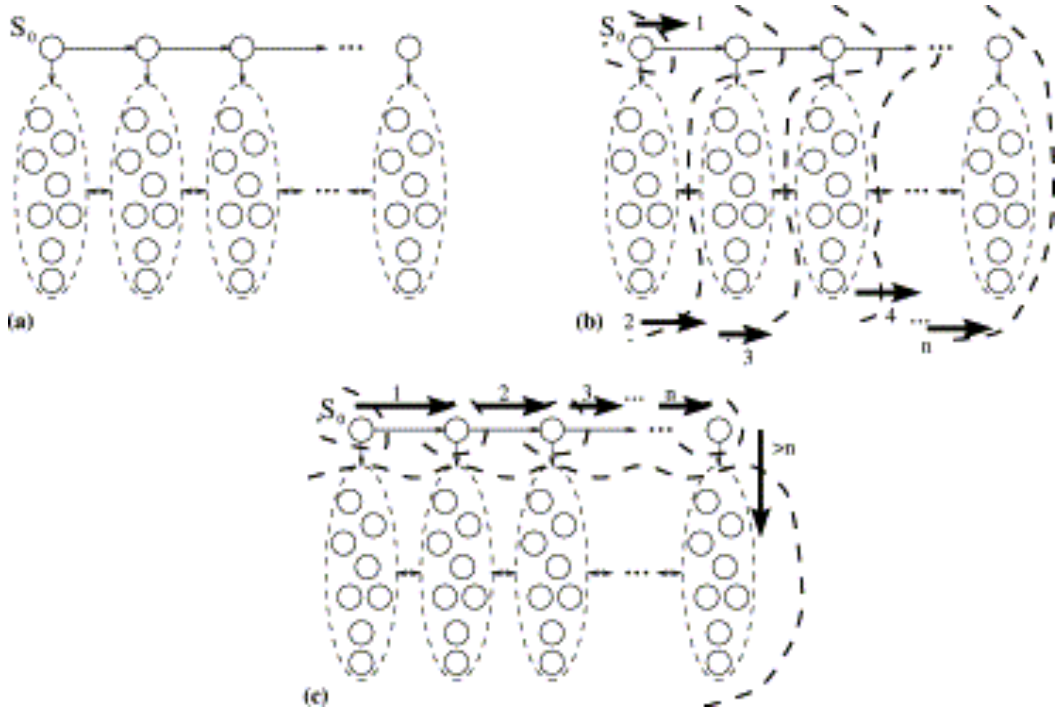
[Barisani CanSecWest09, Enev CCS11, Gandolfi CHES01, Hart IEEE89, Kocher CRYPTO99, Patel Ubicomp07]

Intuition

Embedded

General-purpose





Devices Tested

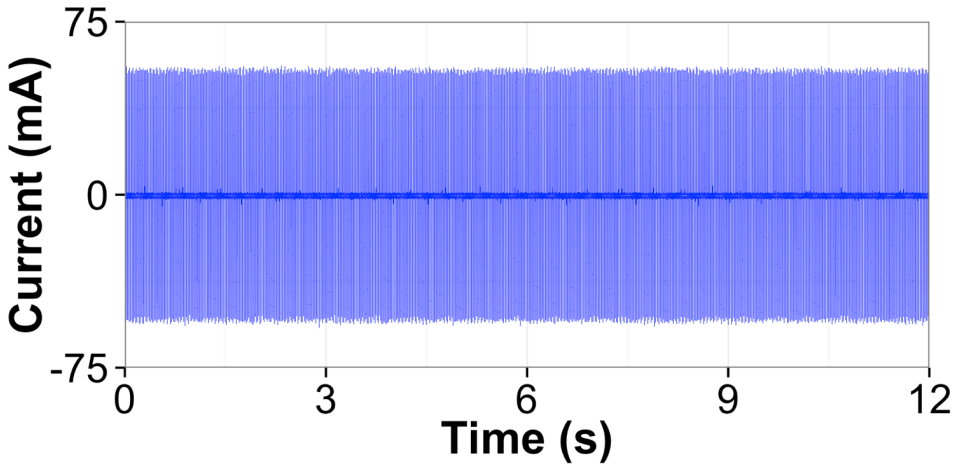
Device	Configuration
Baxa ExactaMix 2400 compounder	WinXP Embedded, Via 664 MHz , 512 MB RAM
Schweitzer SEL3354 substation computer	WinXP Embedded, Athlon 2600+, 2 GB RAM

Trace Collection

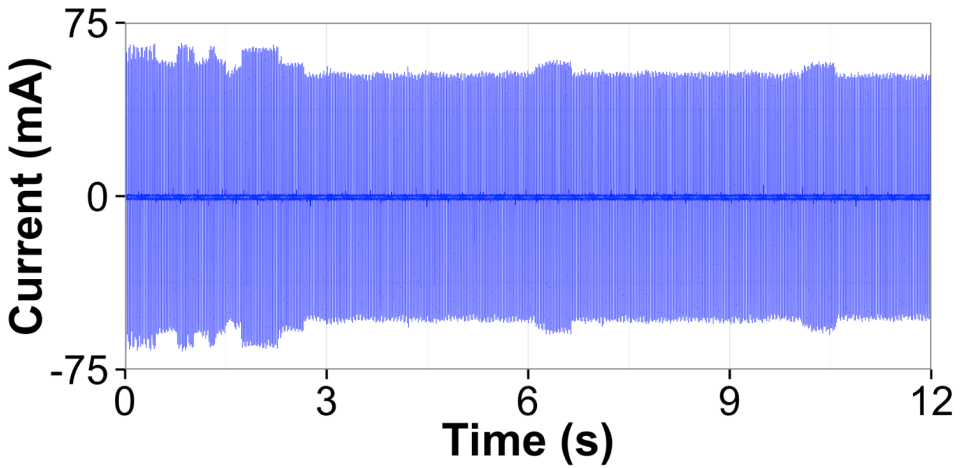
- Gather traces in "normal" and "abnormal" conditions
  - Normal included idle, mixing chemicals, etc
  - Abnormal included emulated and real malware
  - ~2500 traces for each device
- Look at frequency domain, not time domain

Compounder Traces

- AC traces are sinusoidal.
- Changes in power consumption create changes in amplitude.

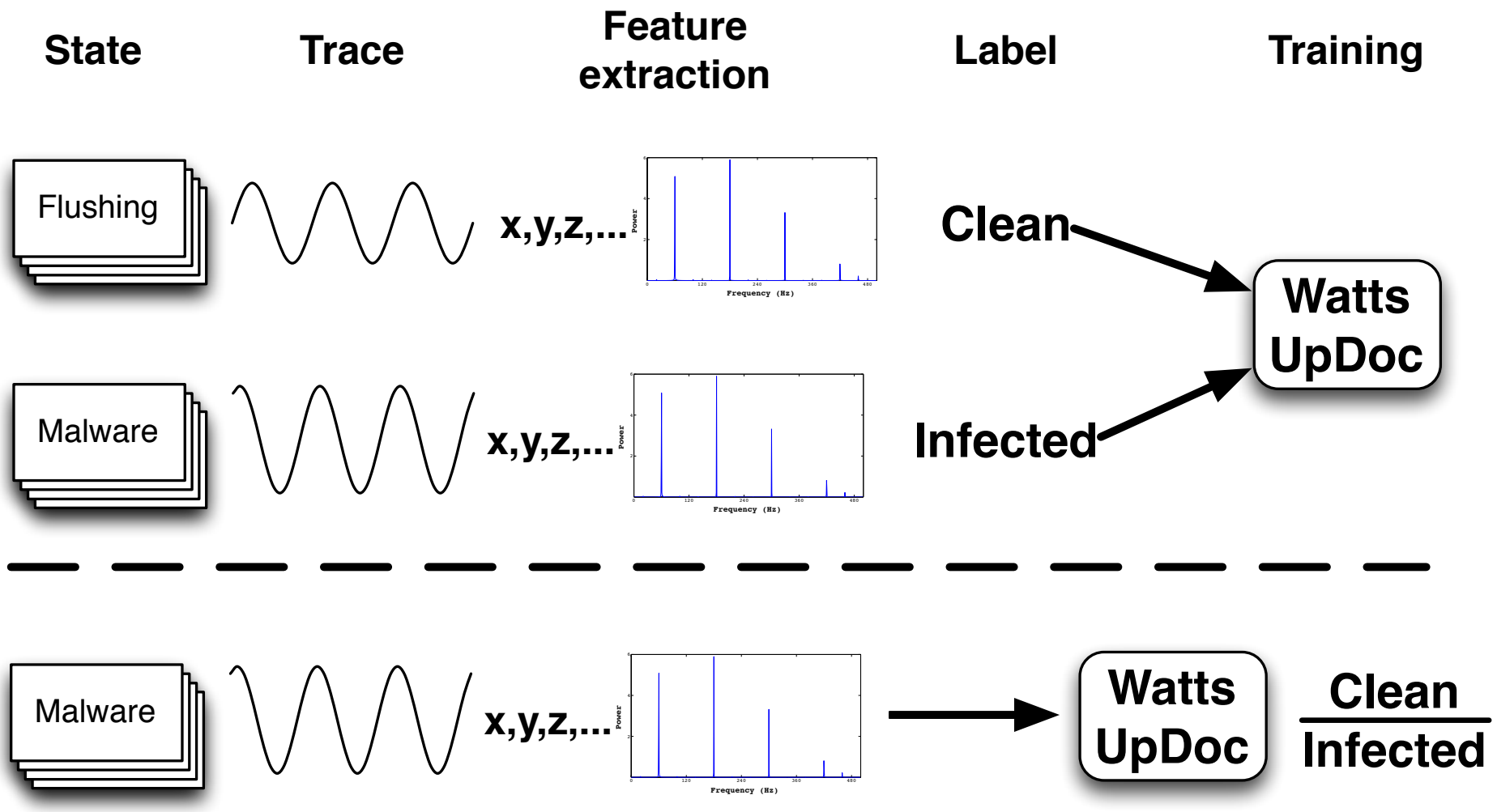


Idle



Infected

Building a Classifier

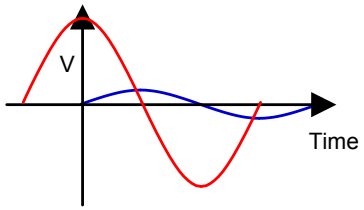


Related Work

- NILM [Hart IEEE89]
- Differential power analysis [Kocher CRYPTO99]
- Identifying videos, webpages [Enev CCS11, Clark ESORICS13]
- Power-based malware detection on smart phones [Kim Mobisys08, Liu RAID09]
- Sensor node failure detection [Khan IPSN10]


120VAC 15A MAX
PowerGuard
VirtaLabs
VIRTA LABORATORIES, INC.
HW1.0
VIRTA LABS

Analog Side Channels

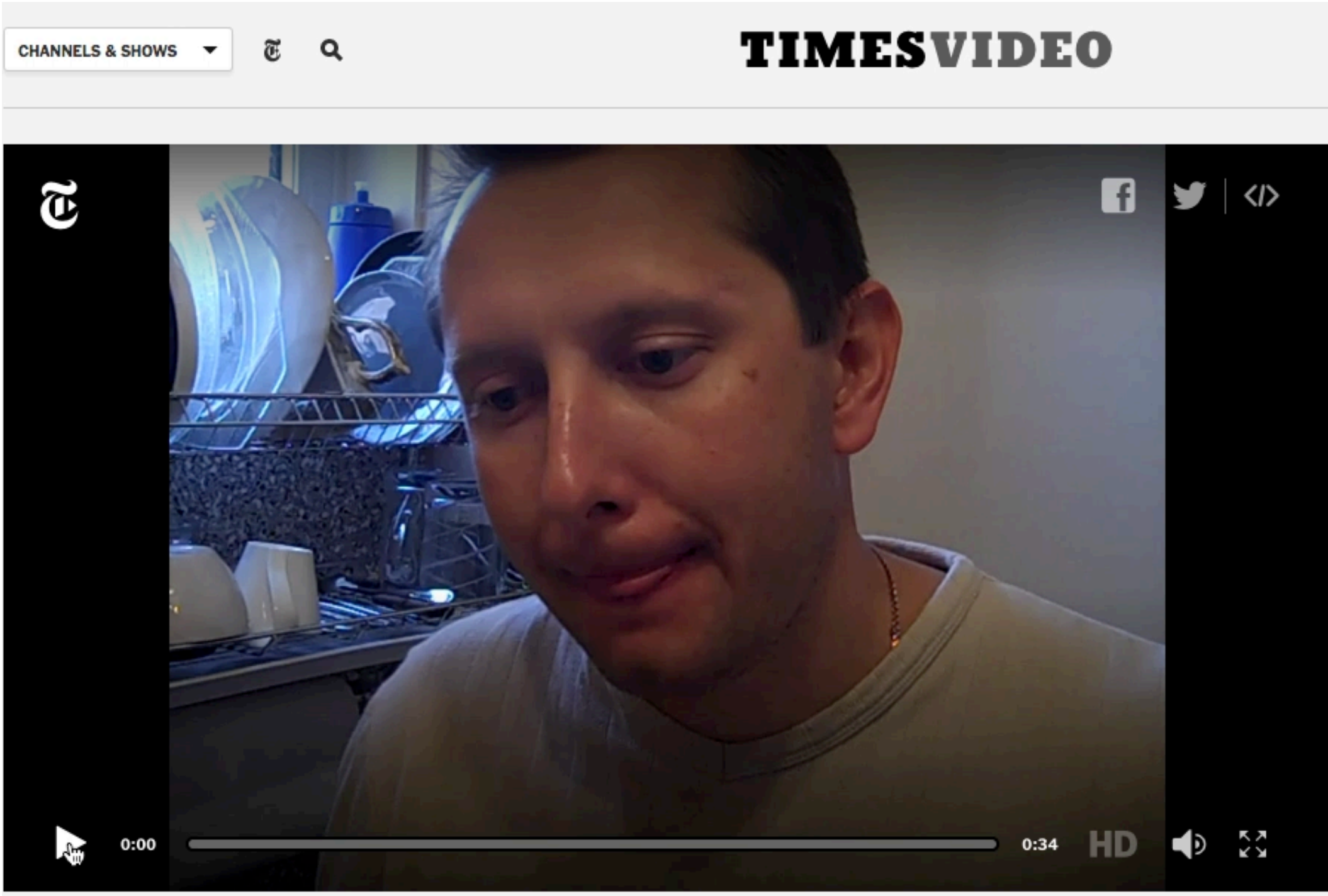


Analog **Digital**

"Read"
Property: Confidentiality
Spectre, Meltdown, …

"Read"
Property: Confidentiality
Example: Power Analysis

"Write"
Property: Integrity
Example: Sensors



https://www.nytimes.com/video/multimedia/1247464146747/mobile-phone-turns-on-oven.html

Review: Fault Injection

- Given a smart card that uses CRT to compute $m = D(c) = c^d \bmod n$
- Inject a fault in the CRT portion of the algorithm with a chosen ciphertext **c** such that the output is **m'**
- Compute a regular decryption without a fault with output **m**
- WLOG, $p = GCD(m - m', n)$

Handout 6: "On the Importance of Checking Cryptographic Protocols for Faults" by Boneh et al., EuroCrypt 1997.

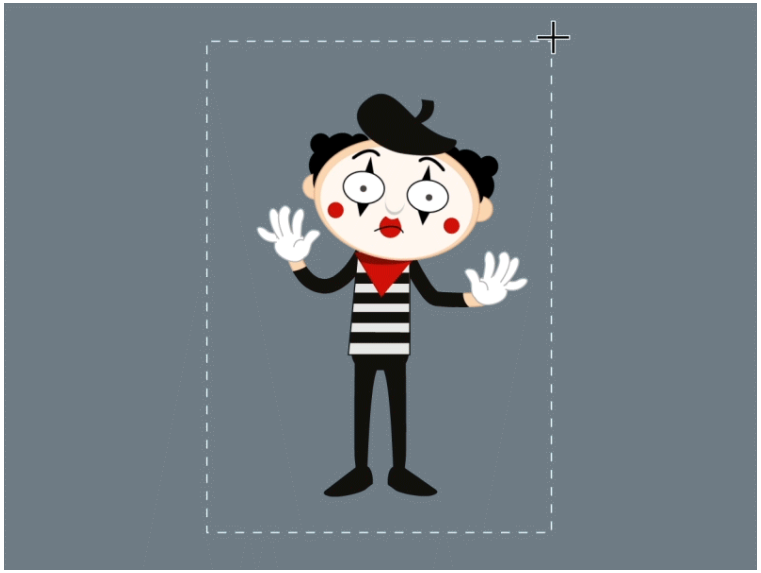
Transduction Attacks [CACM '18]

- Sensors are transducers
  - Translate the physical into the electrical
  - Computer software interprets and operates on binary representations rather than direct physical or electrical quantities

- Transduction attack
  - Exploits a vulnerability in the physics of a sensor to manipulate its output or induce intentional errors
  - Think of it as violating the "requires" clause of mechanical or electrical engineering, and no exception is thrown at the software

Digital Abstraction != Force Field

intentional interference violates assumption of **sensor output integrity**



- Vibration
- Acoustics
- RF
- Light
- Heat

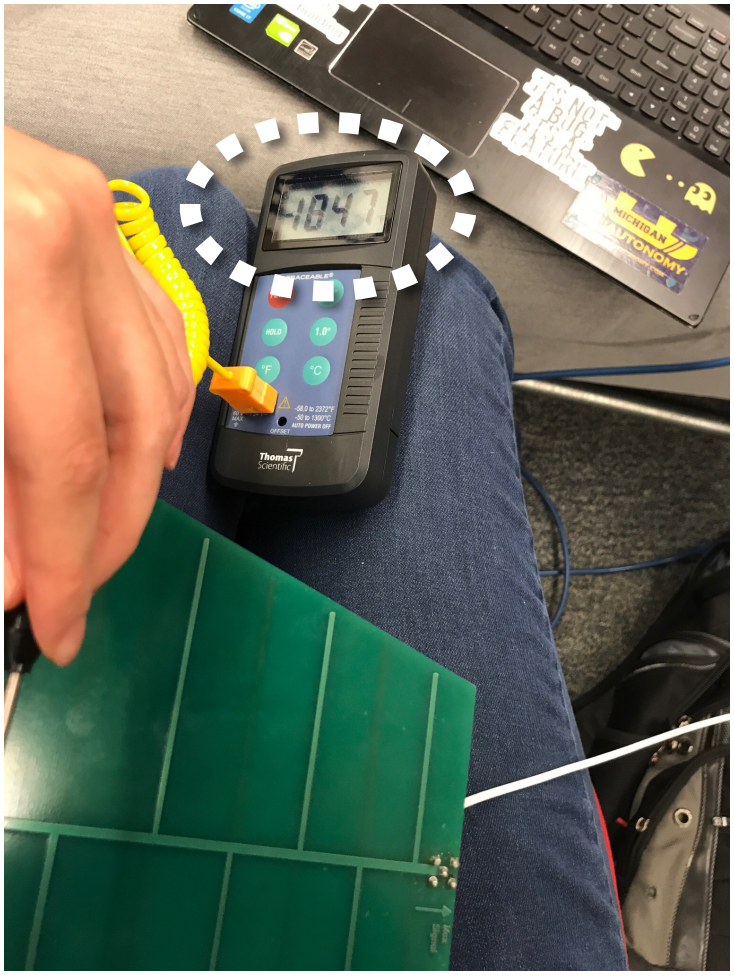
$\Rightarrow$ Sensor spoofing

https://dribbble.com/shots/2281625-Marquee-Tool-Mime

Do Not Blindly Trust Sensors

Sensors are a proxy for reality

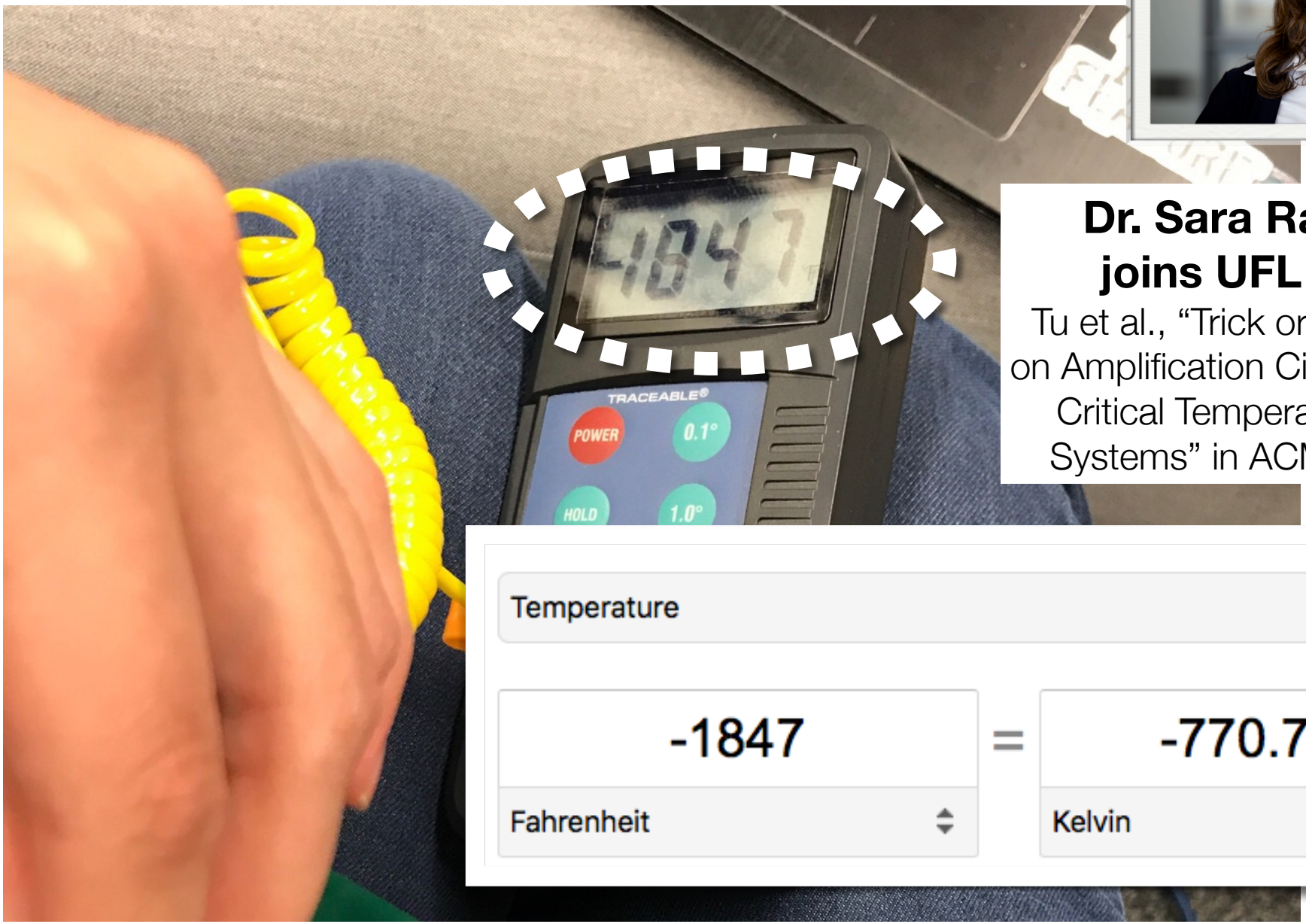
- **Thermocouple interpolates from a voltage potential**
- **Not necessarily temperature**



Absolute Zero Day Attack

Dr. Sara Rampazzi joins UFL faculty

Tu et al., "Trick or Heat? Attack on Amplification Circuits to Abuse Critical Temperature Control Systems" in ACM CCS 2019



Where Do Thermocouples Matter?

The New York Times

How to Ship a Vaccine at –80°C, and Other Obstacles in the Covid Fight

Developing an effective vaccine is the first step. Then comes the question of how to deliver hundreds of millions of doses that may need to be ...

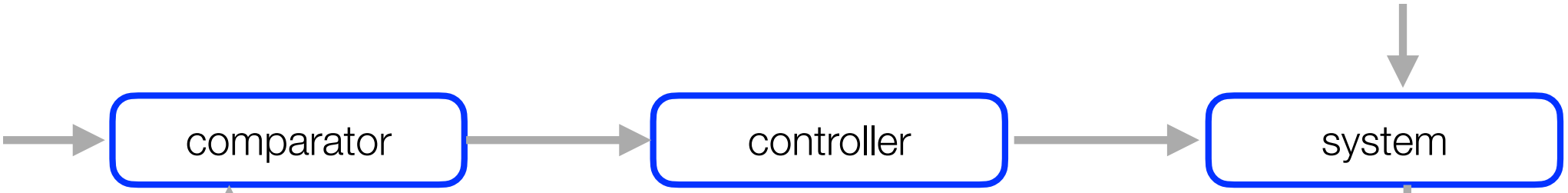
Blog / Temperature measurements and temperature control in the IVF lab are crucial for your results

Temperature measurements and temperature control in the IVF lab are crucial for your results

Posted by Jaco Geyer, Jan 26, 2016 6

At Risk: Closed-Loop Feedback Systems

Photos: NYTimes, NBC Today, ABC News5 Cleveland



Problem:

How to protect medical devices and cyberphysical systems from emerging threats to

analog sensor integrity?

Outline: Protecting Sensor Integrity

Today: taste of sensor security research across three modalities:

- Defending against **radio-based attacks** on sensors

Coming weeks:

- Defending against **sound-based attacks** on sensors
- Defending against **light-based attacks** on sensors

Intentional Electromagnetic Interference (Or Don't Trust Your Sensors)

"Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors" by Foo Kune et al.
In Proc. IEEE Symposium on Security and Privacy, 2013.

Joint work with Denis Foo Kune (U. Michigan),
John Backes (U. Minnesota), Shane Clark (U. Mass Amherst),
Dr. Dan Kramer (Beth Israel Deaconess Medical Center),
Dr. Matthew Reynolds (Harvard Clinical Research Institute),
Yongdae Kim (KAIST), Wenyuan Xu (U. South Carolina)

Supported in part by NSF CNS- 1035715, CNS-0845671, CNS-0923313, GEO-1124657, S121000000211, HHS 90TR0003/01, the Sloan Research Fellowship, the University of Minnesota Doctoral Dissertation fellowship, the Korean MEST NRF 2012-0000979, the Harvard Catalyst/Harvard Clinical and Translational Science Center MeRIT career development. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the HHS or NSF.

Many reports of accidental

Cellphone
+
Oven

New York Times
Aug 21 2009

Ambulance comm
+
Life support system

Armstrong, Hutley
2007

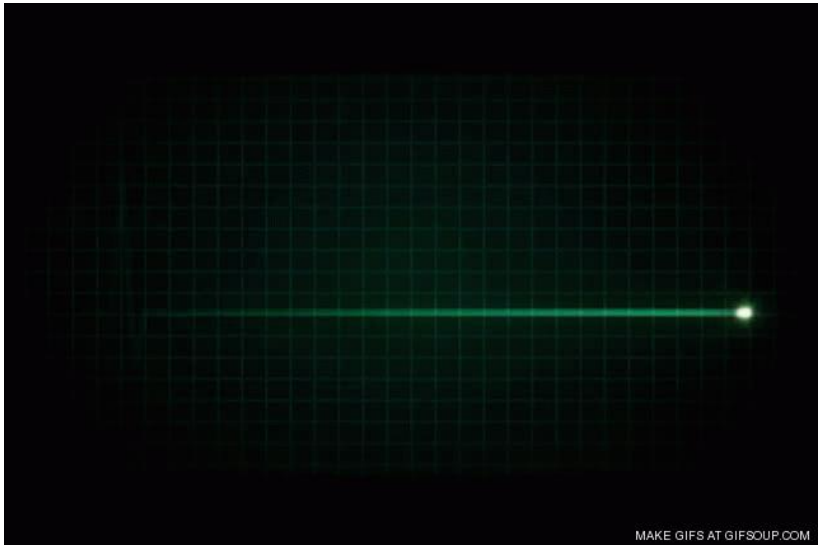
EMI
+
Anti-lock brakes

NASA pub 1374
1995

Which one is the real cardiac signal?

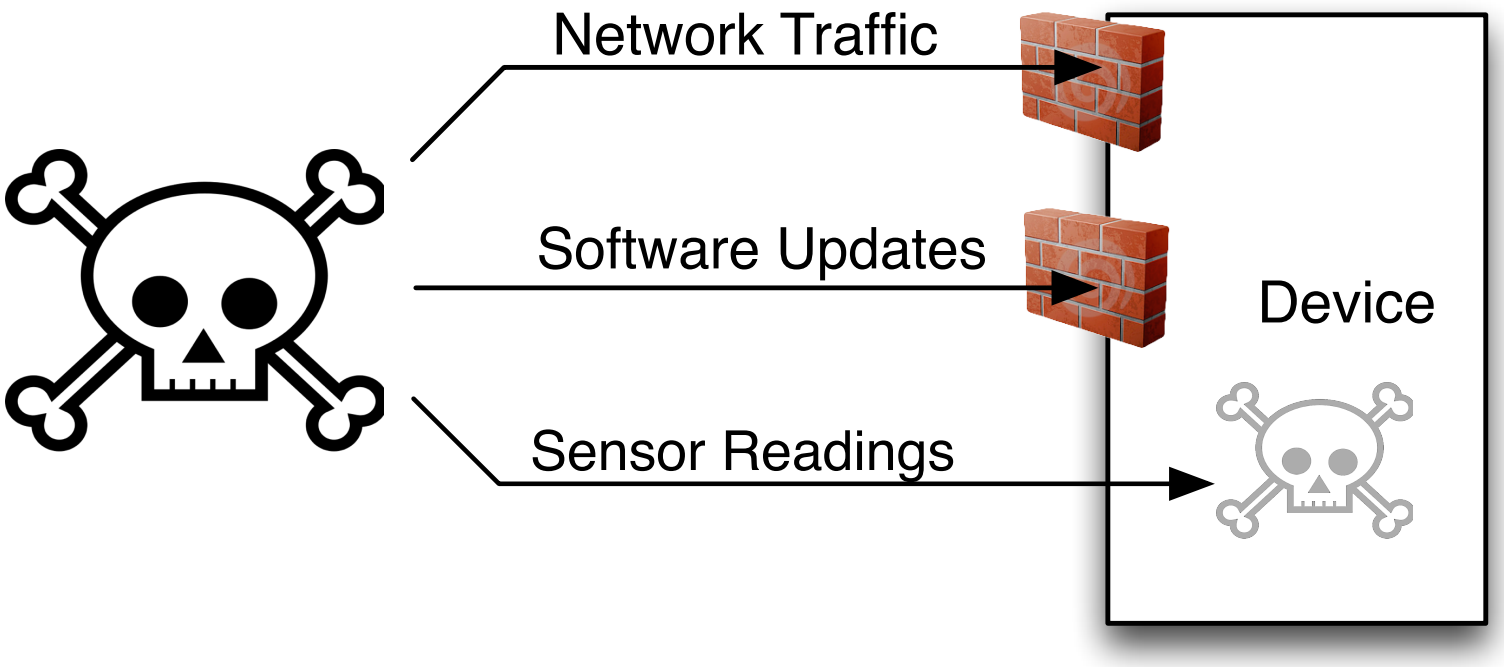
A

B



["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

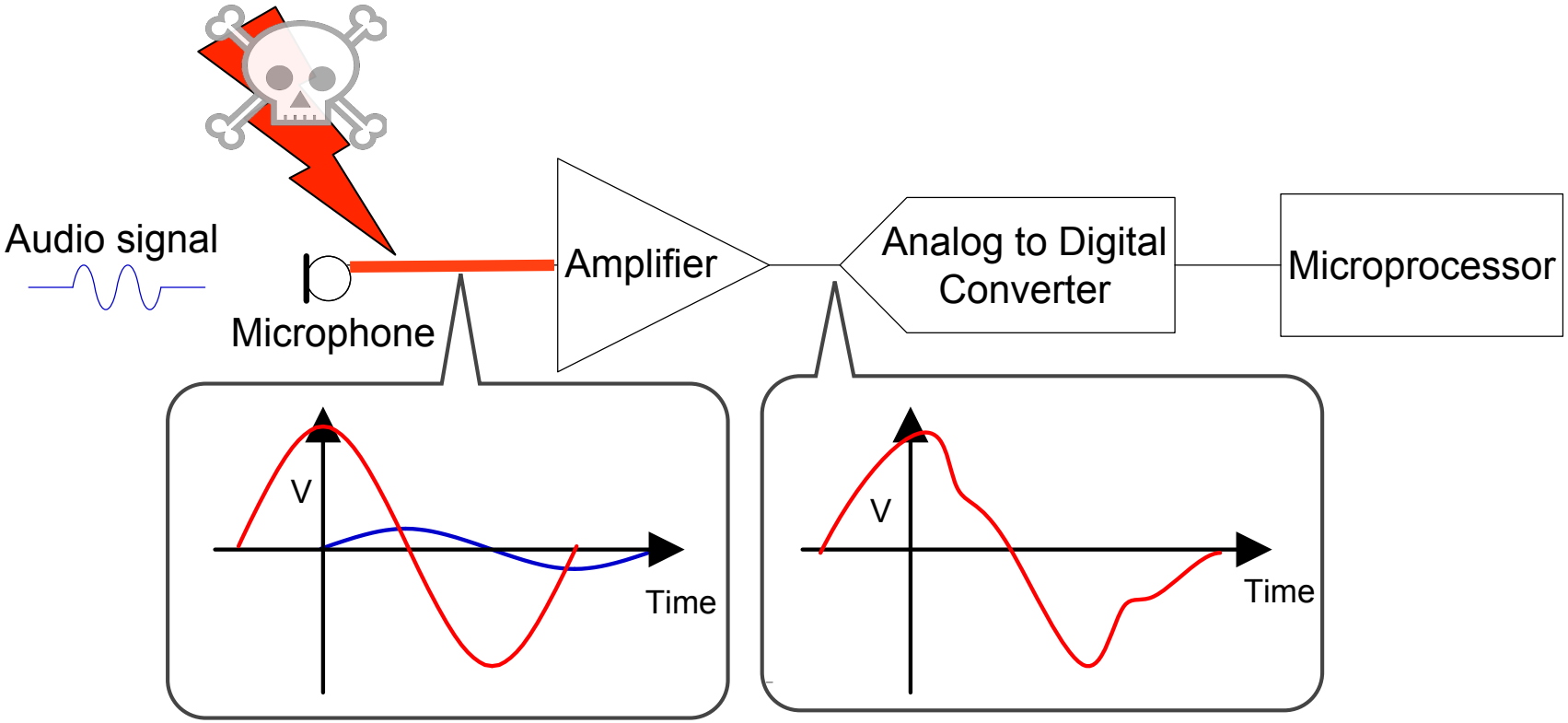
Inputs may not be trustworthy



["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

Ghost Talk: Intentional interference

- Conducting traces can couple to EMI (back-door).
- Sensitive analog sensors can be affected.



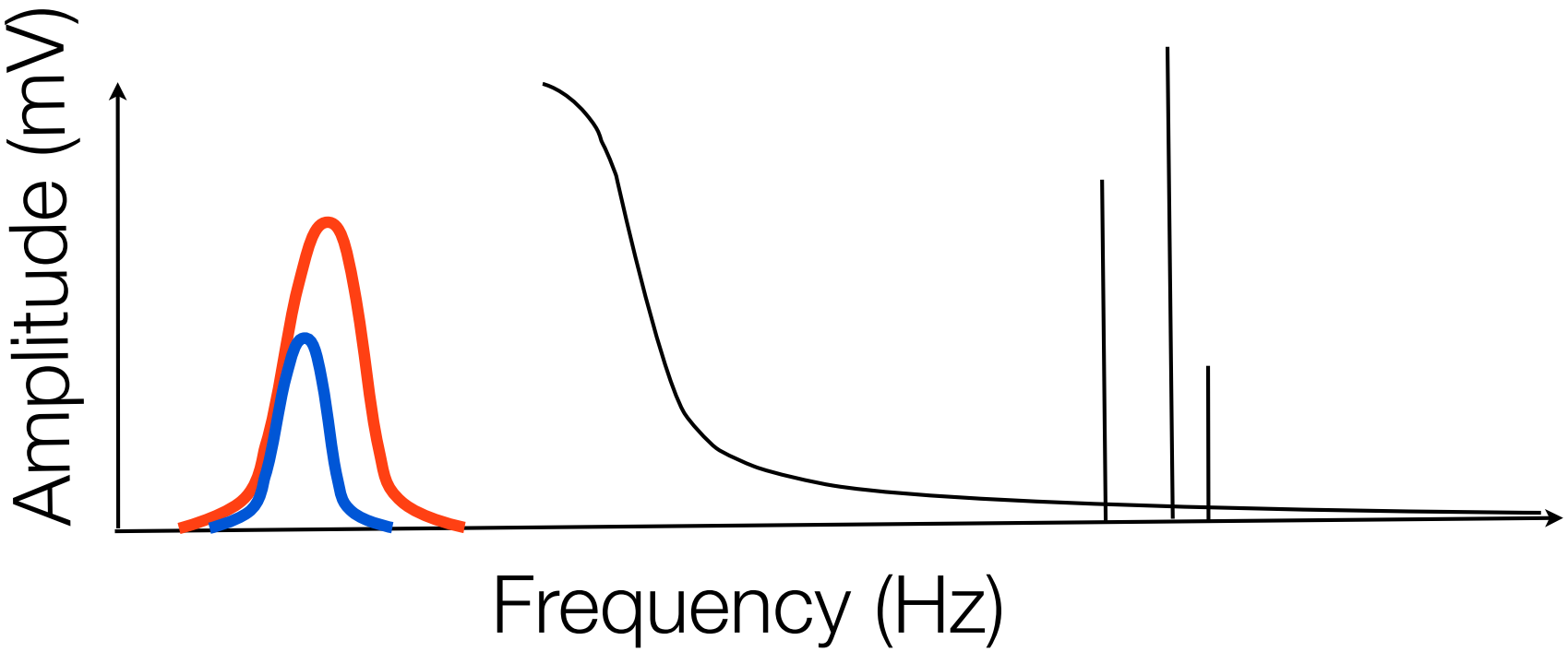
["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

The Max Headroom incident

- Max Headroom
  - Front-door coupling
  - Overwhelm legitimate radio signal with another radio signal
- Ghost Talk
  - Back-door coupling
  - Overwhelm legitimate acoustic signal with radio signal

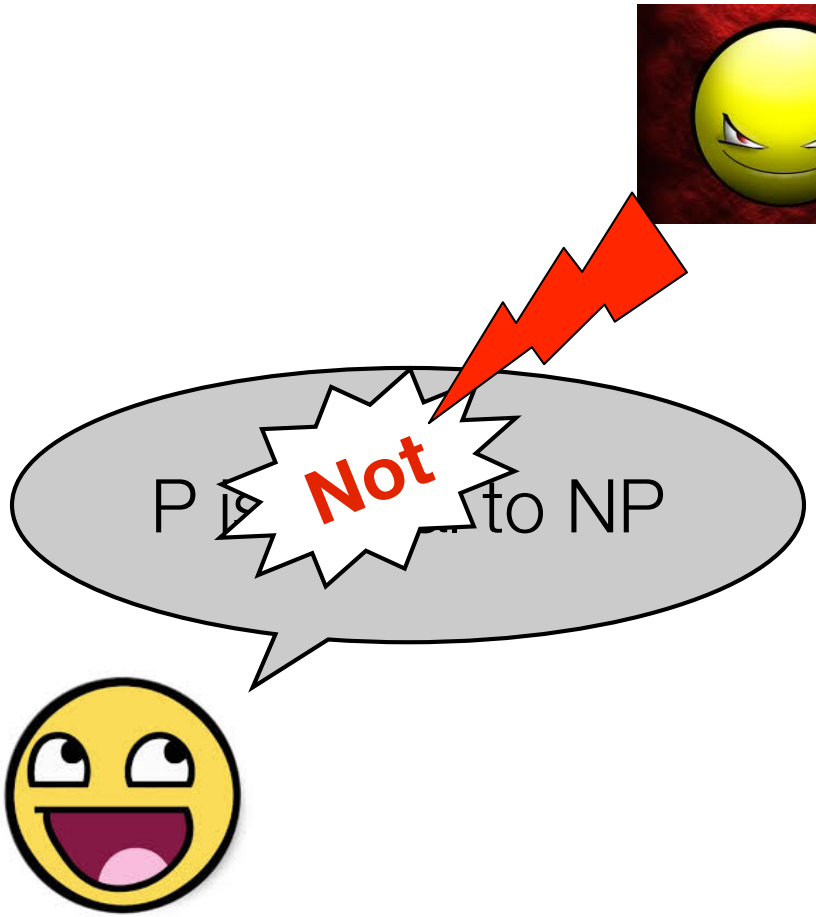
Fundamental Problem: Baseband

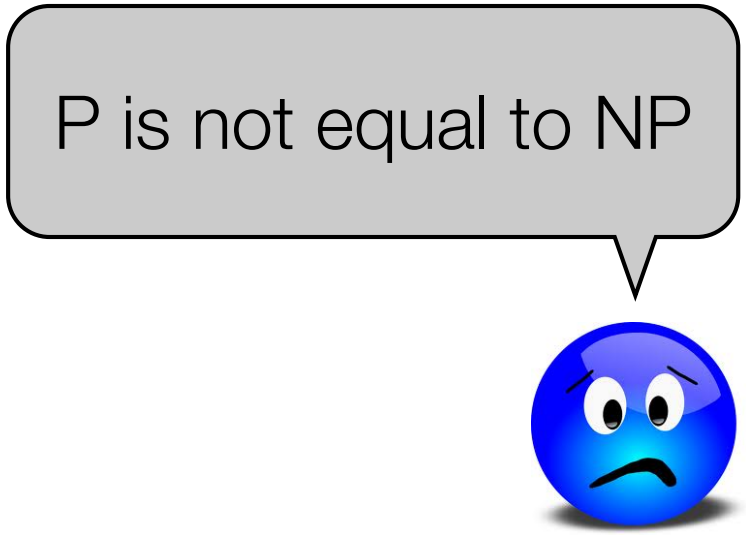
- Baseband: frequency range of desired signals.
- Interference outside the baseband is easy to filter.
- Interference in the baseband is hard to remove.



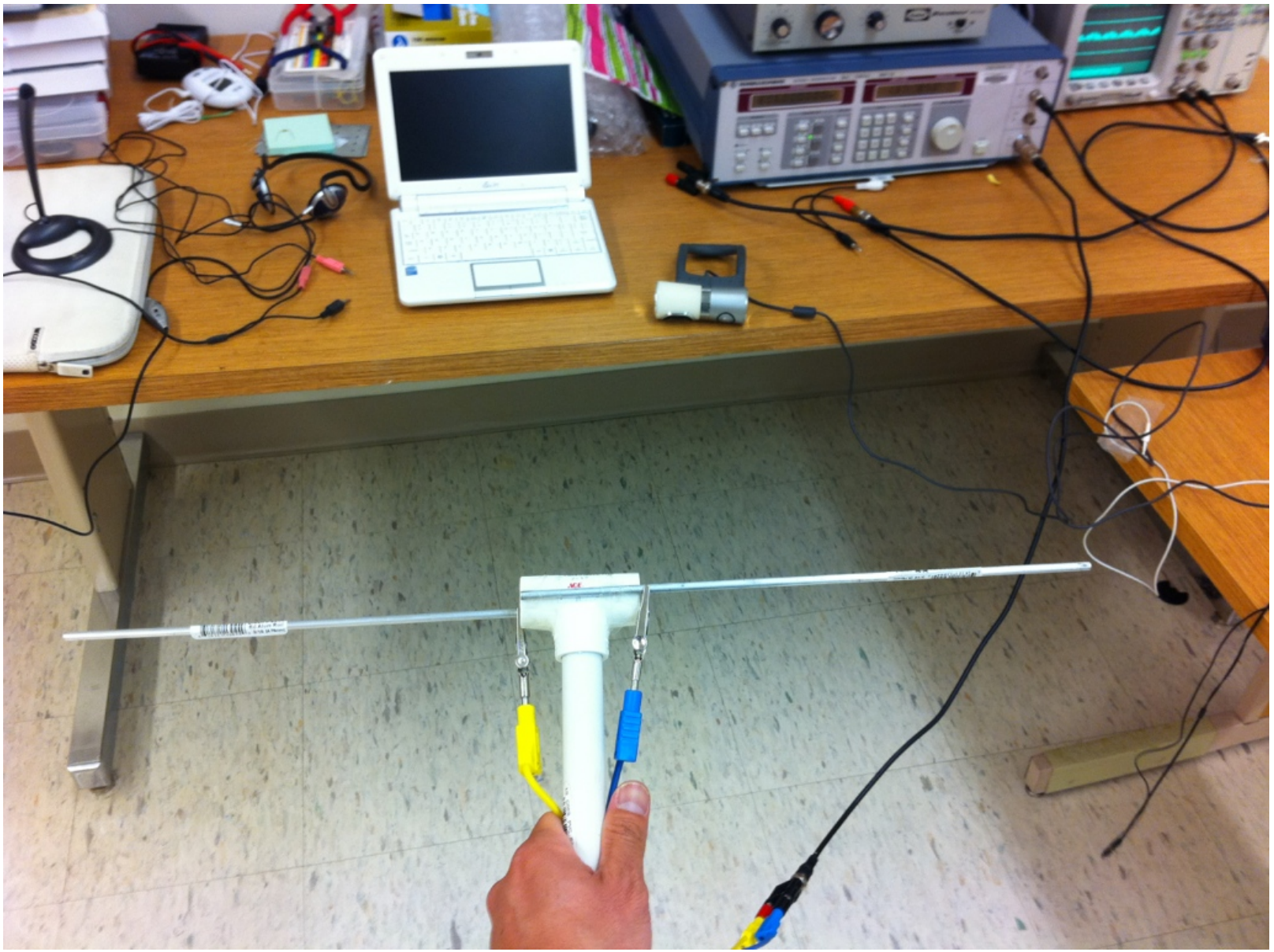
["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

Example: Adding audio waveform



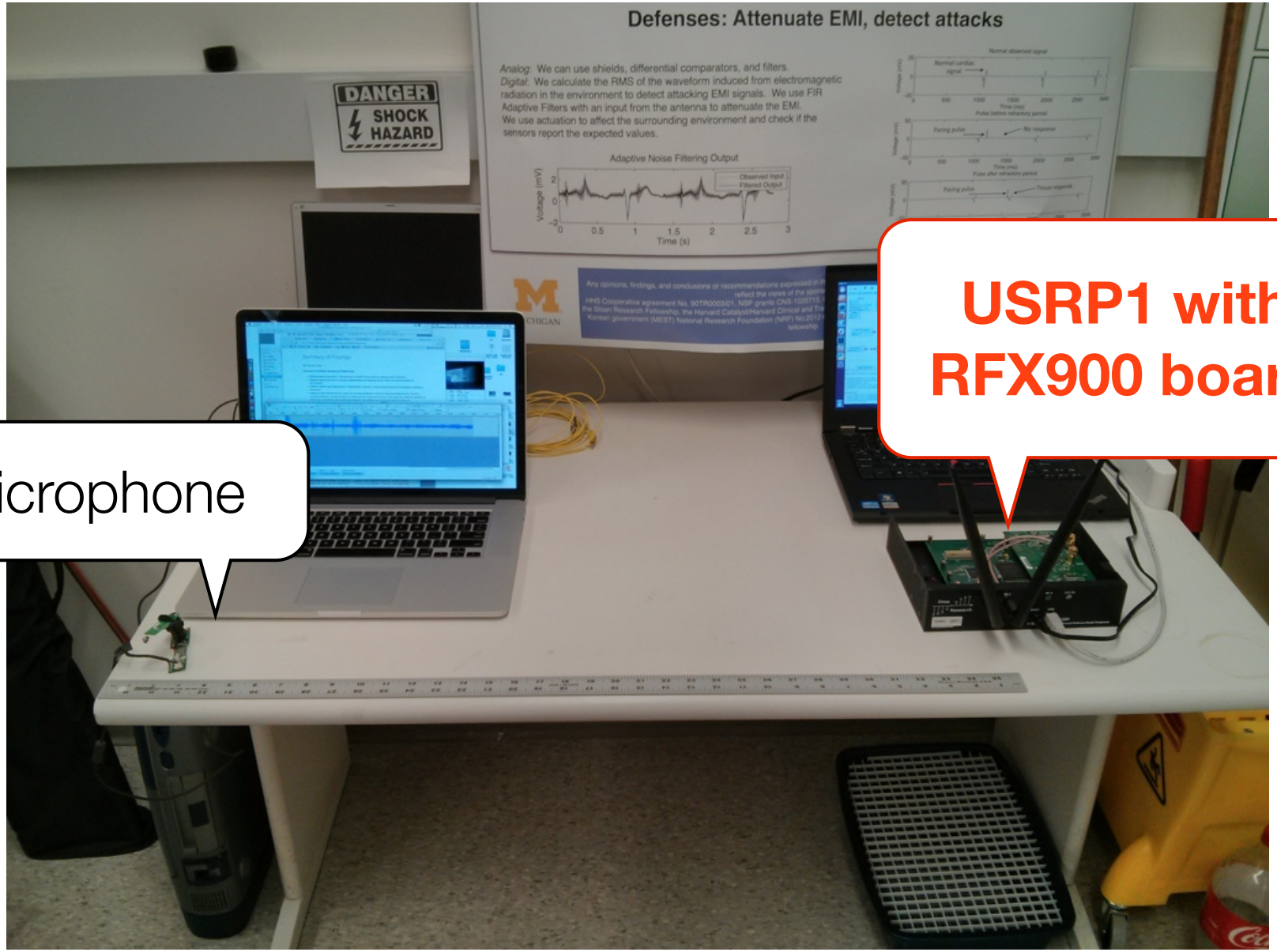


Mic and dipole antenna



["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

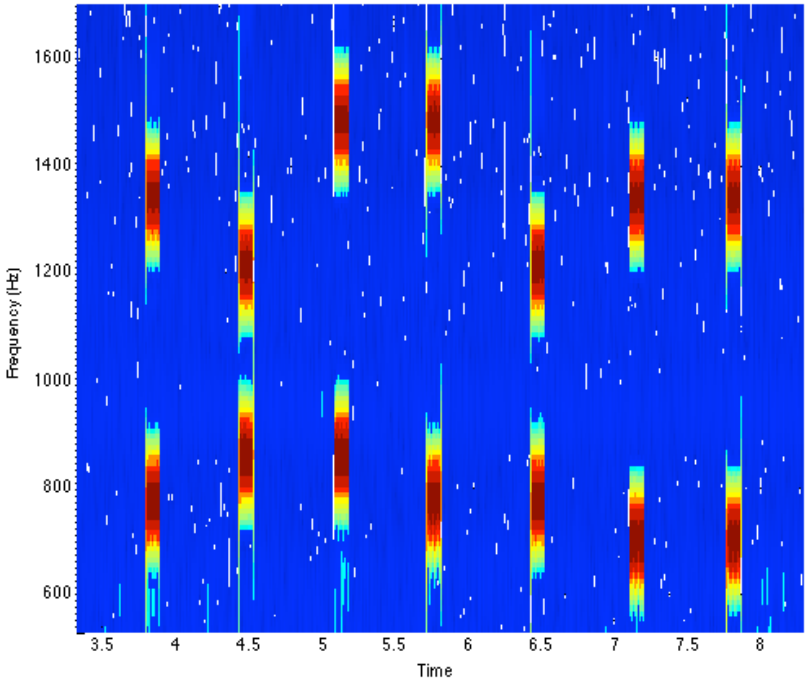
Microphone Interference with RF



["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

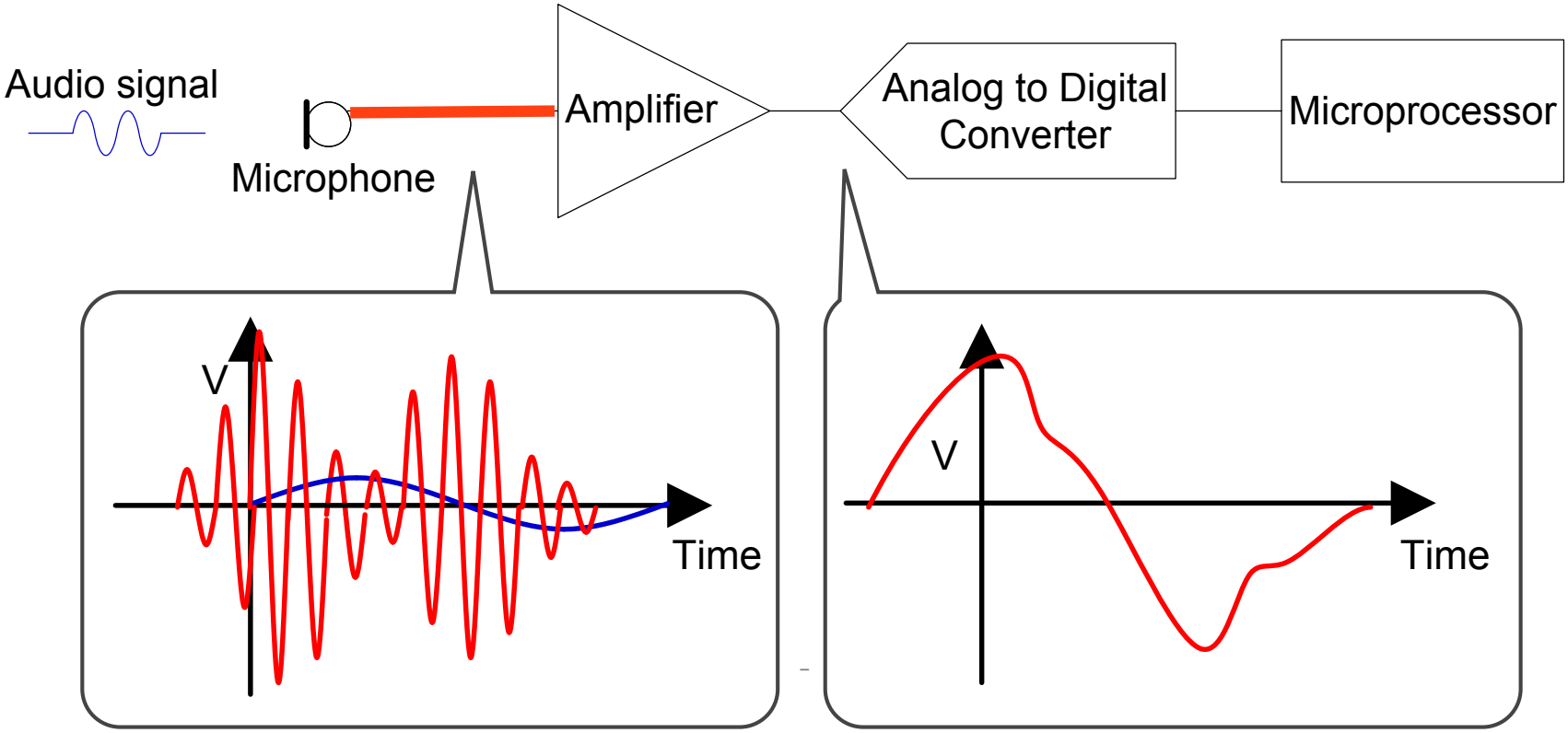
DTMF tones can be transmitted over EMI

- Setup: Phone with bluetooth device dialed a bank
- Transmitted: credit card number over EMI
- Consequence: remote bank logged us into the system



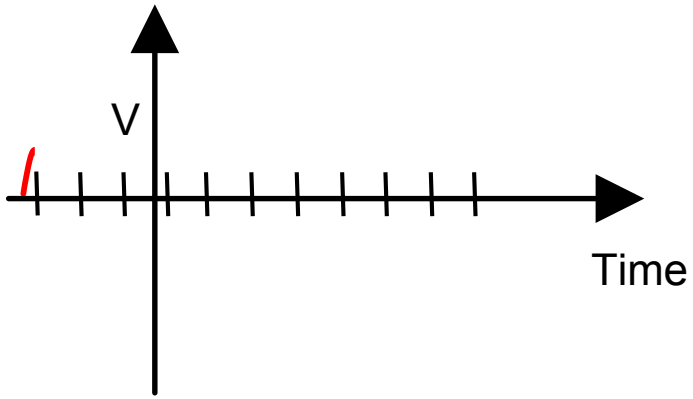
Operational challenges for intentional EMI

- Transform emitted interference to match circuit.
- Reduce transmission power with high frequency carrier

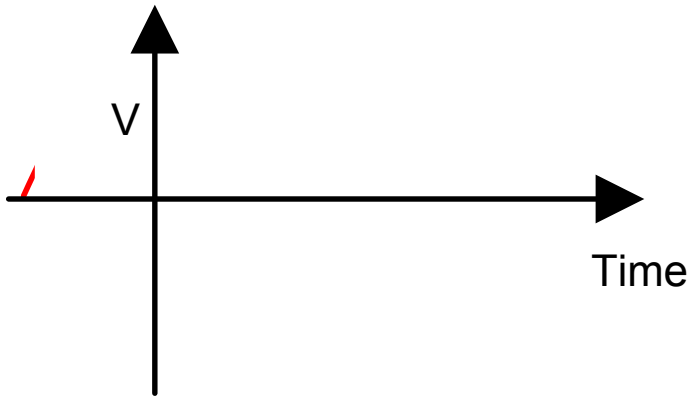


Sampler can demodulate signal

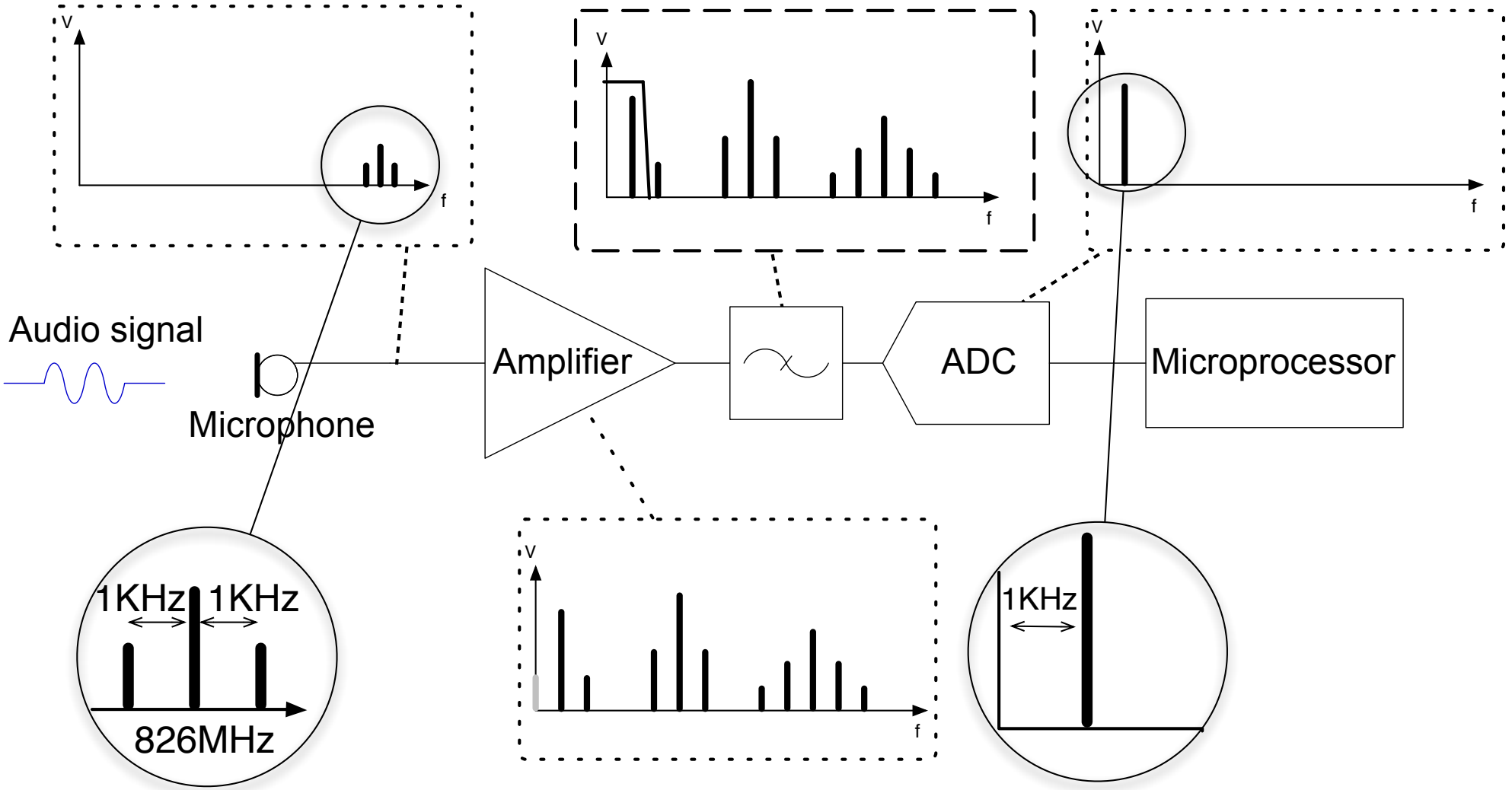
Induced interference



Resulting sampled signal



Non-Linearity: Self Demodulation

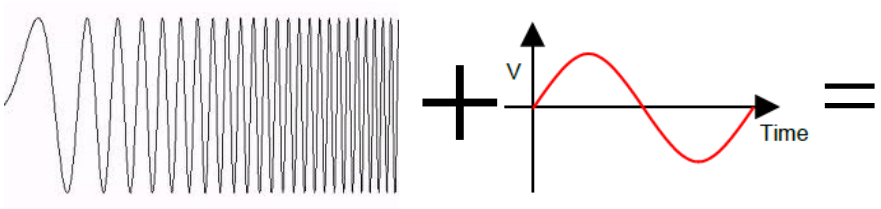


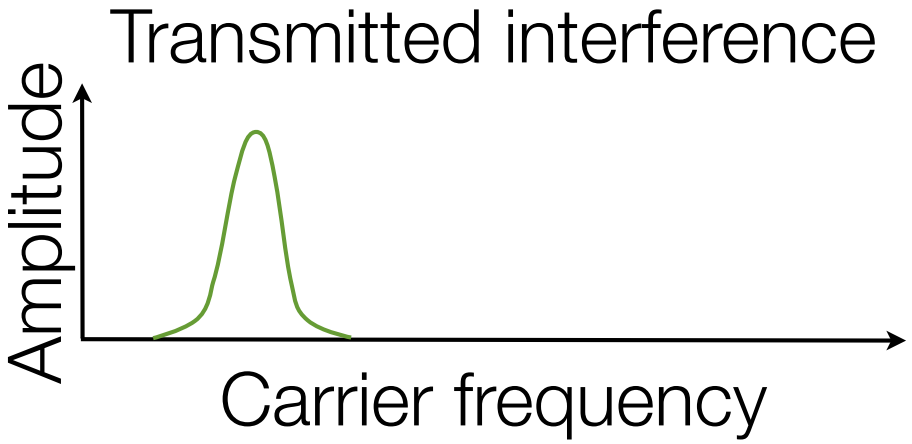
["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

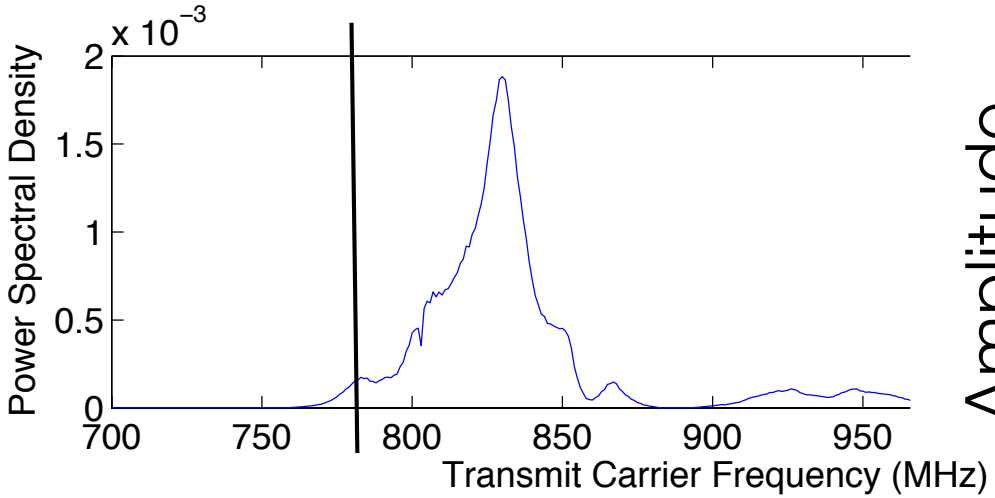
intermodulation distortion…

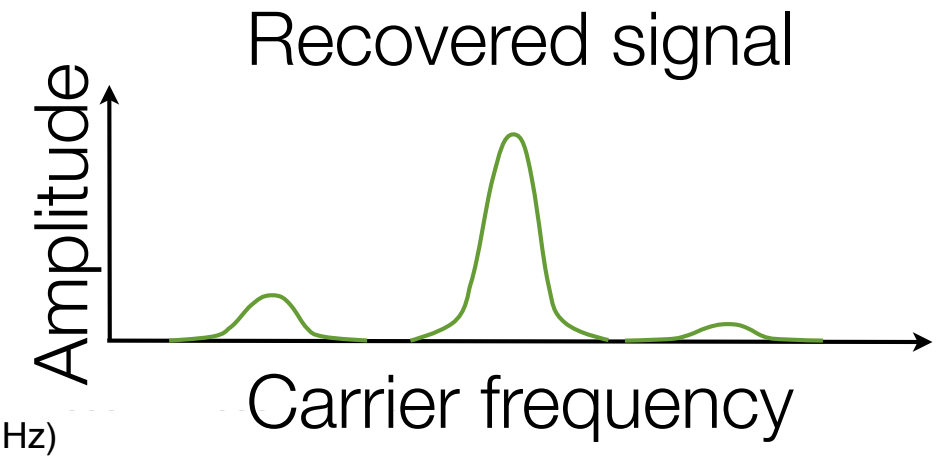
Reverse tuning: Finding a good frequency

- The receiver acts as a fixed circuit.
- Tune the transmitter

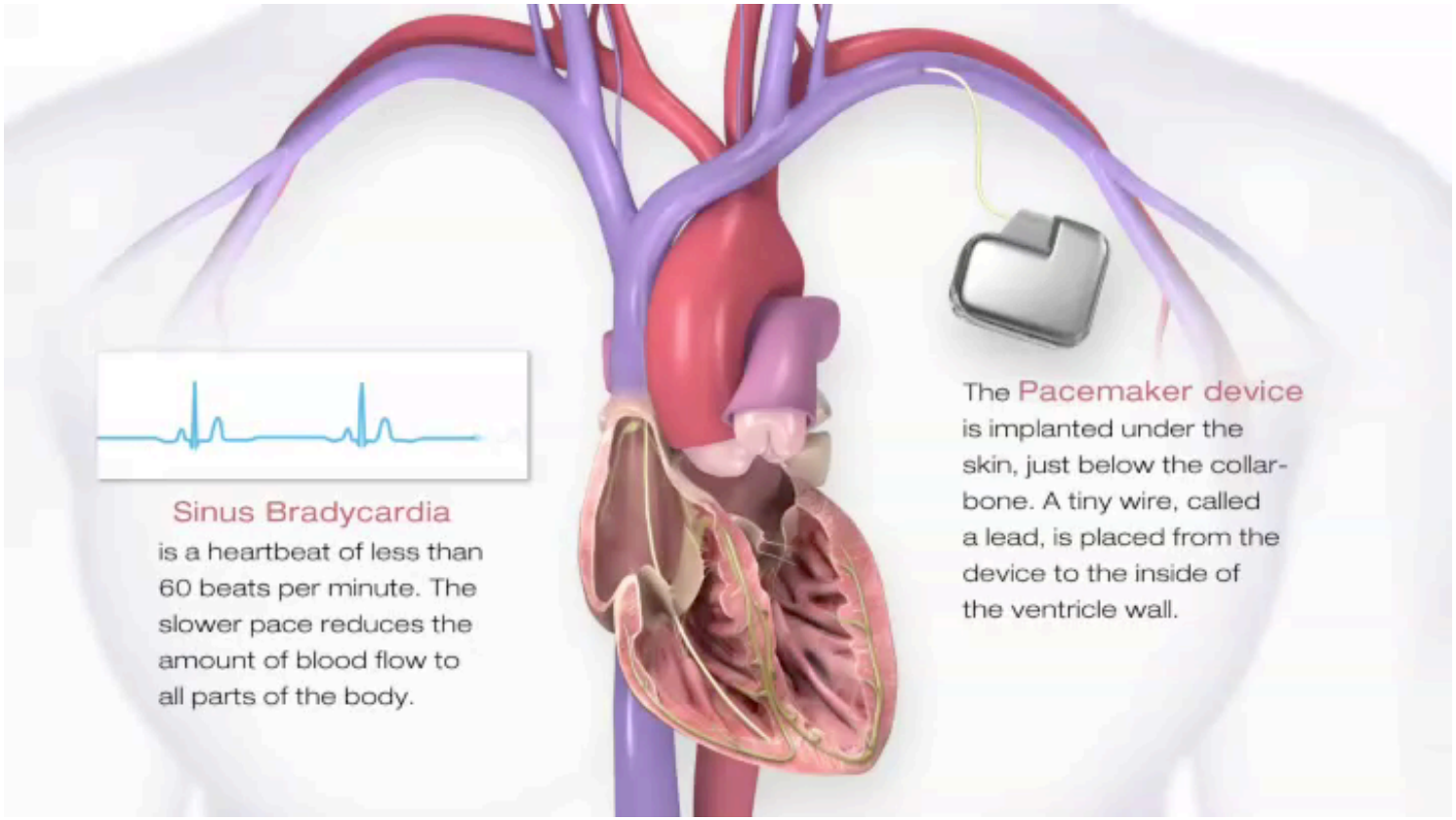








The Cardiac Cycle

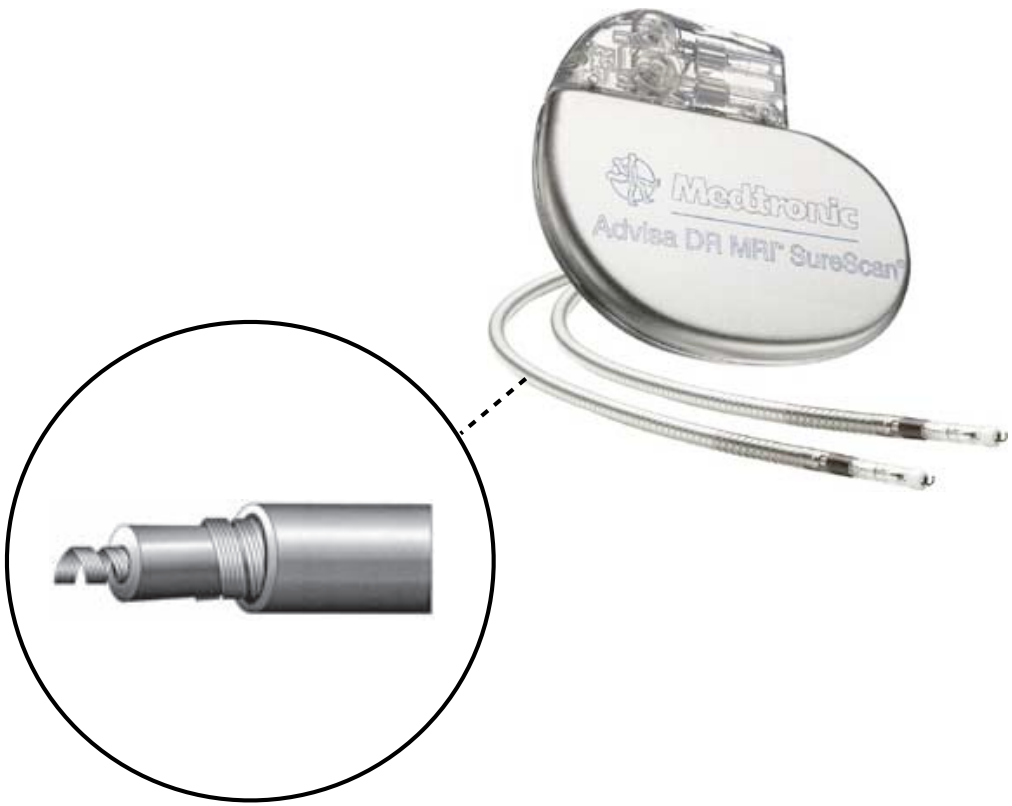


American Heart Association, August 2012

["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

Intentional EMI on cardiac devices

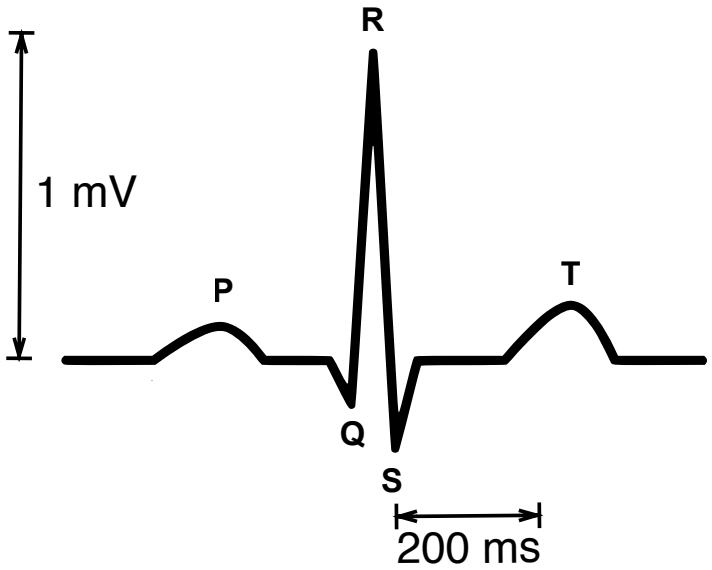
- Pacemakers, defibrillators
- Electrocardiogram machines

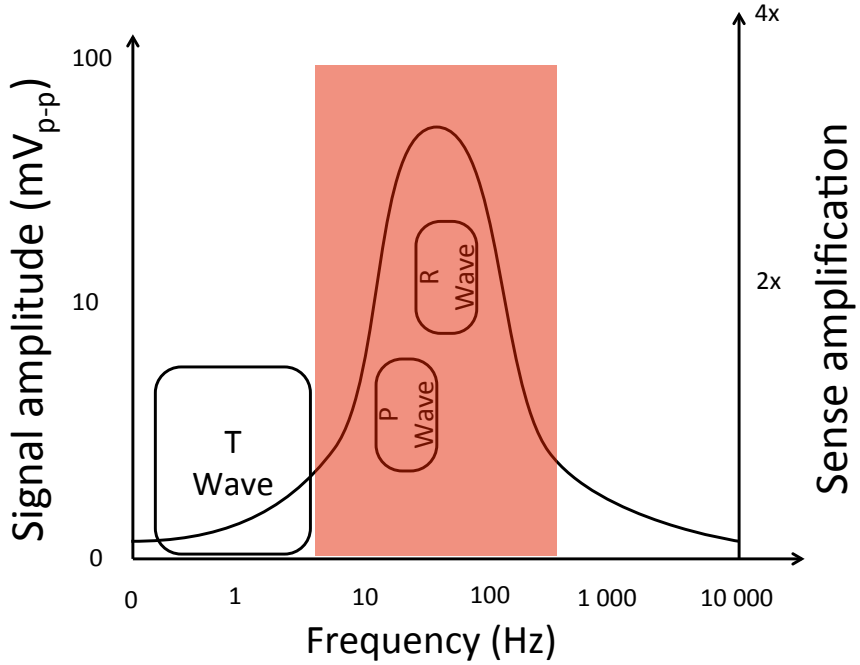


["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

Cardiac devices vulnerable to baseband EMI

- Filter high frequency
  - 800MHz and GHz range: attenuation of up to 40dB
- Can't filter baseband



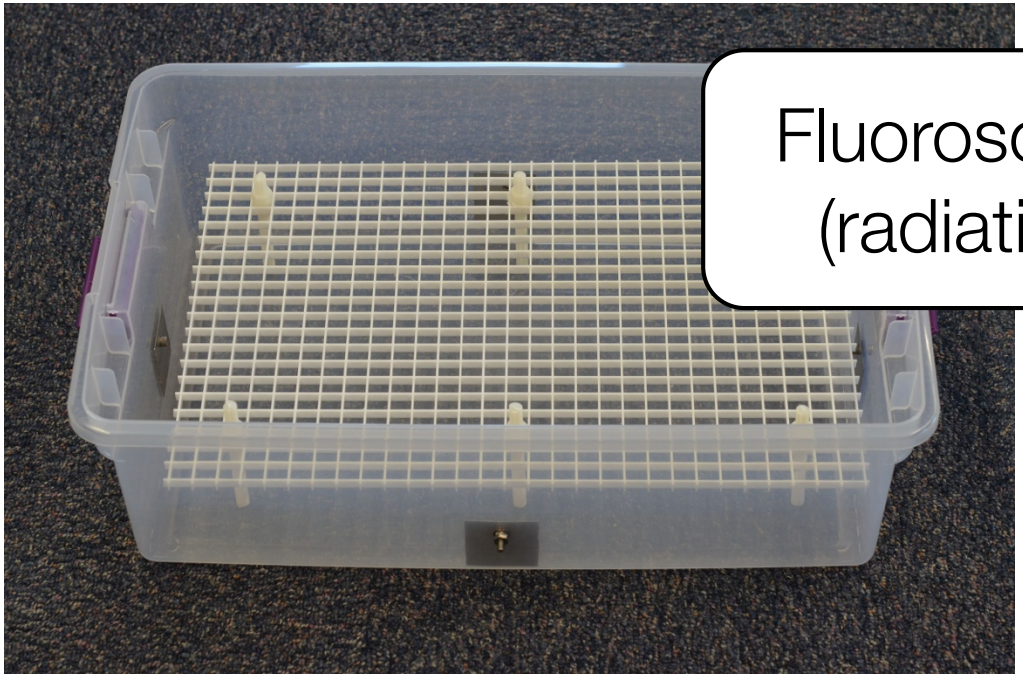


Cohan et al, 2008

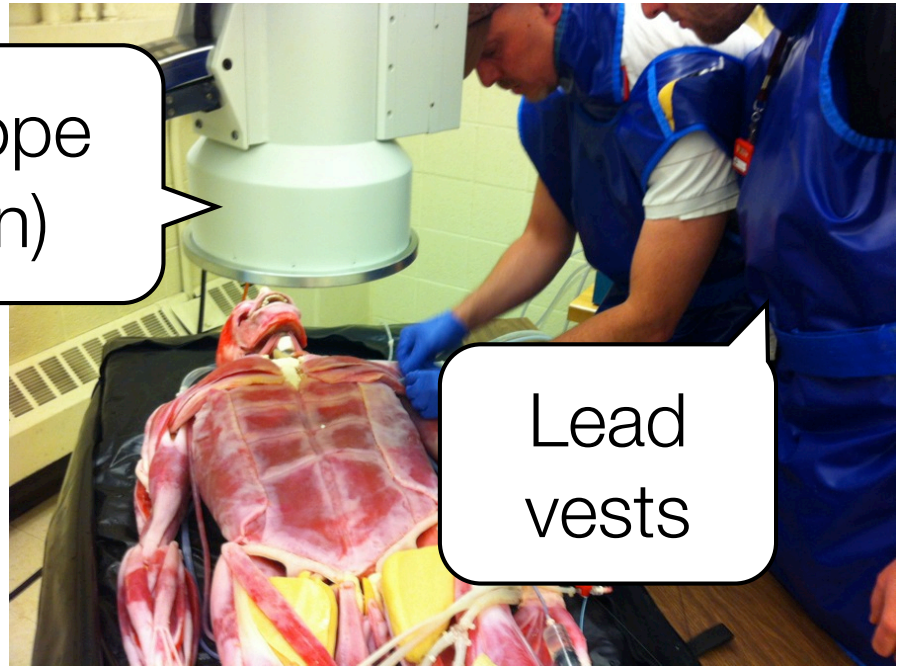
["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

Experimental setup: Simulators

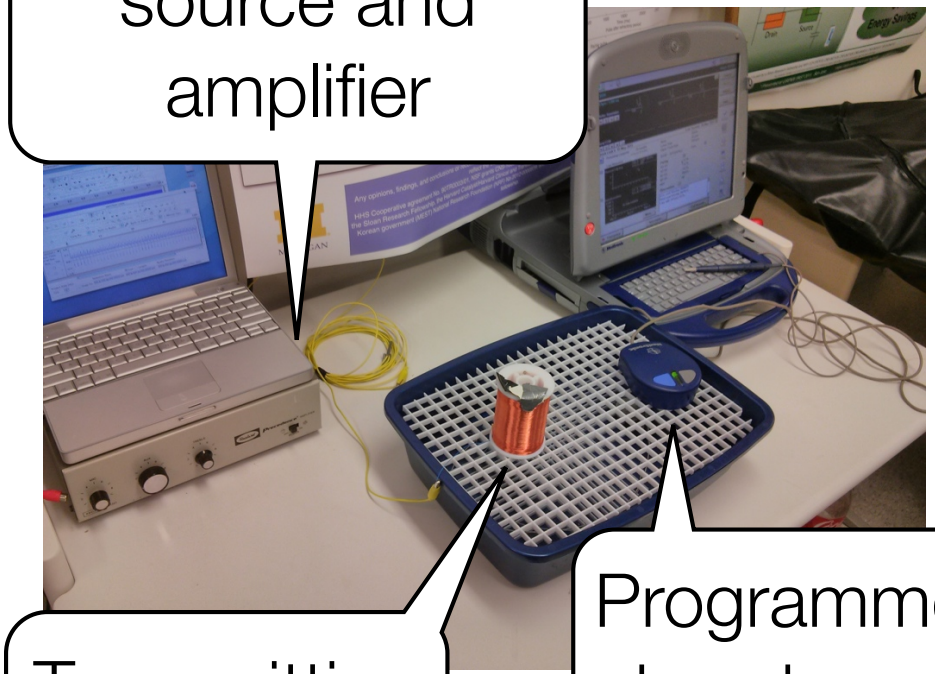
Saline bath

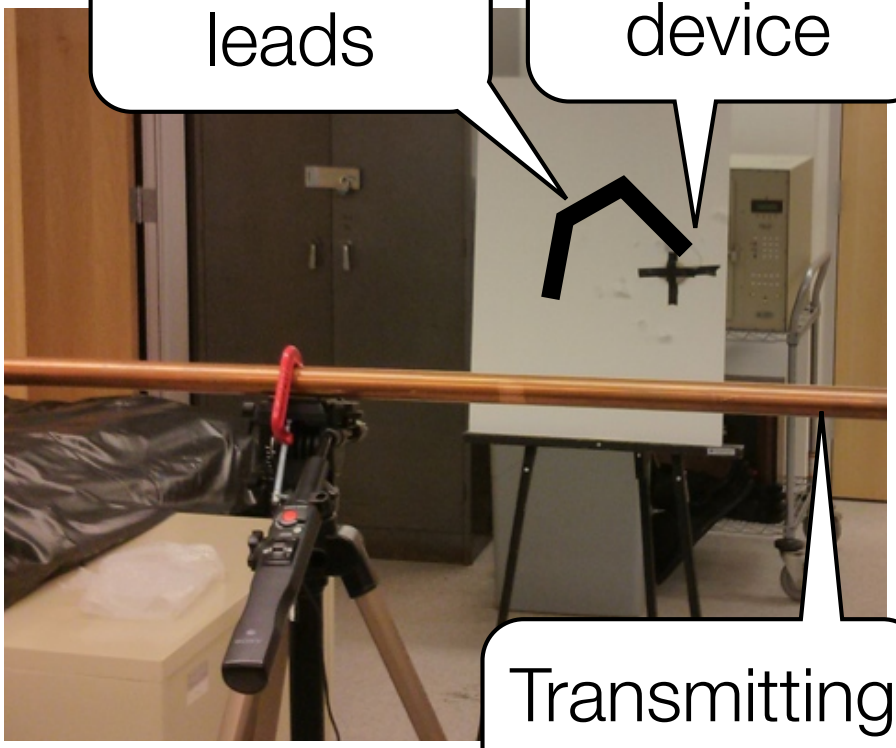


Synthetic human



Experiment: Implants & Emitters

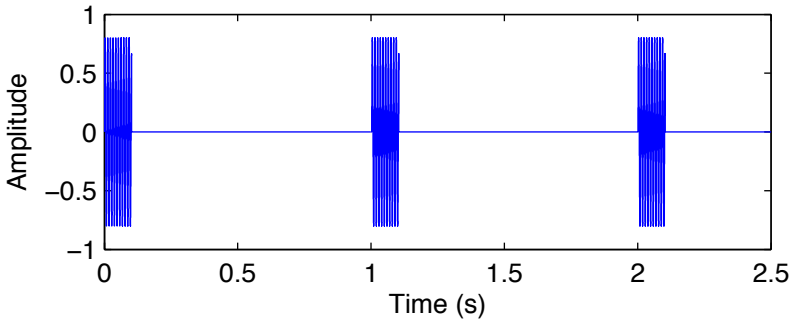


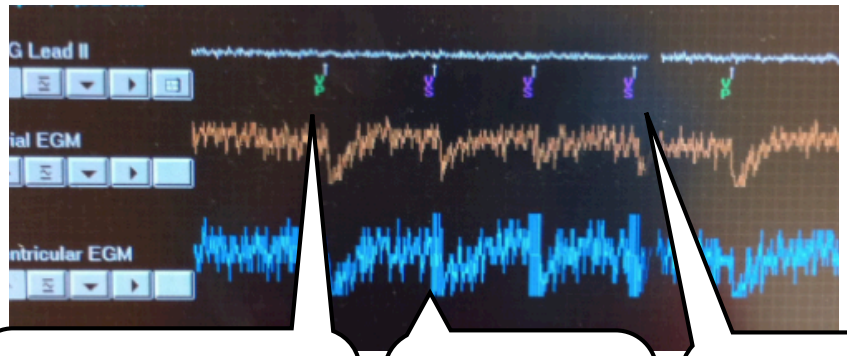


["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

Results: Waveforms & Responses

Pulsed sinusoid



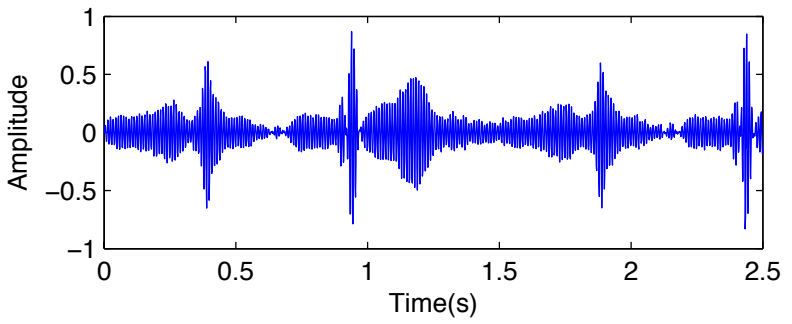


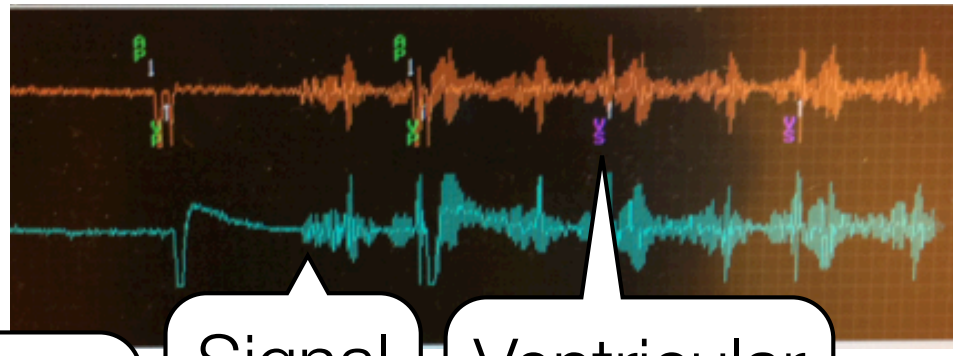
Ventricular pace

Signal onset

Ventricular sense

Modulated heart beat





Signal onset

Ventricular sense

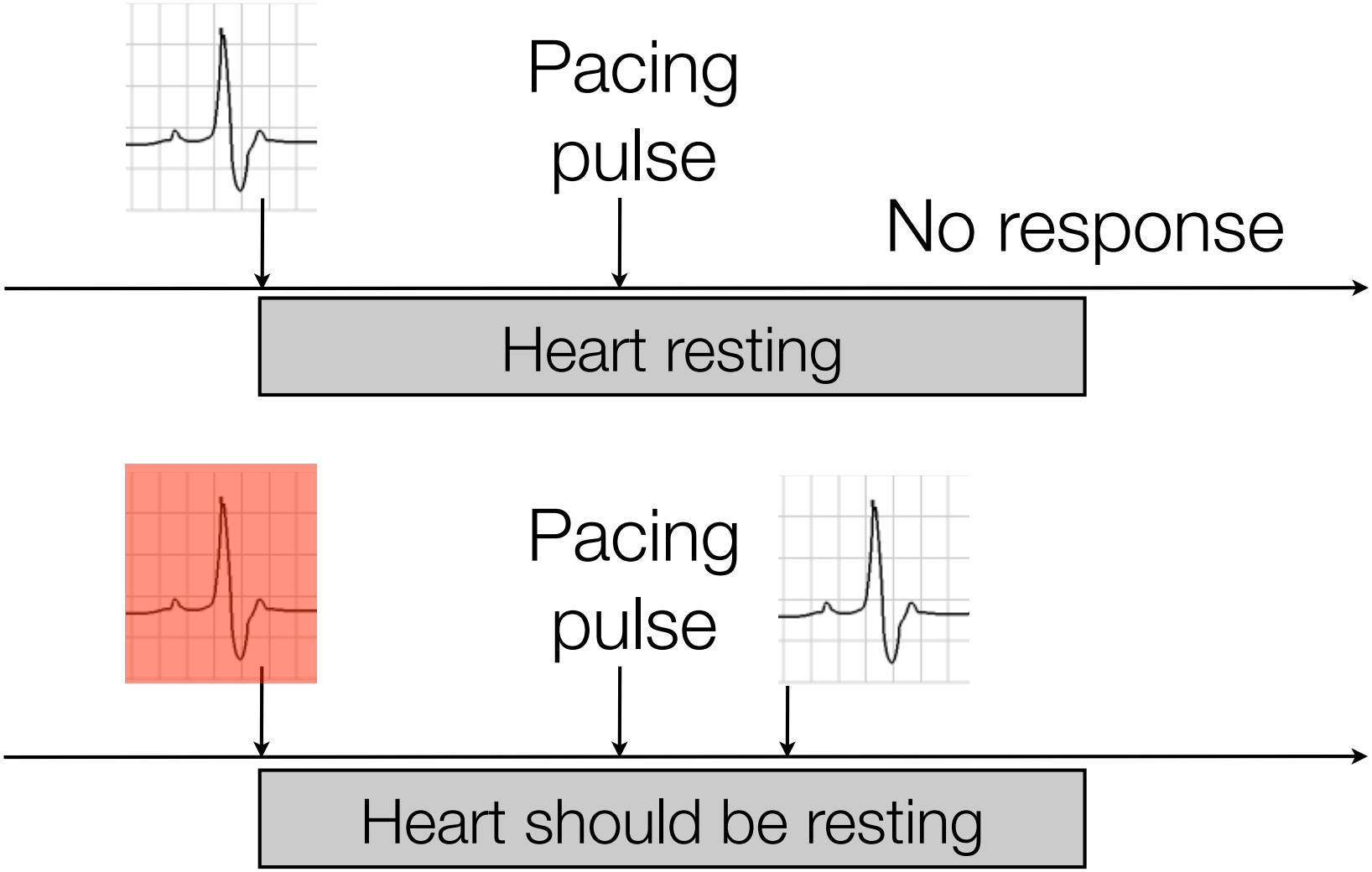
["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

Good News: Distance

Device	Open air pacing	Open air Defib	Saline tips only	SynDaver
Medtronic Adapta	1.40m	NA	**3cm**	Untested
Medtronic InSync Sentry	1.57m	1.67m	**5cm**	**8cm**
Boston Scientific Cognis	1.34m	No defib	Untested	Untested
St. Jude Promote	0.68m	No defib	Untested	Untested

["Ghost Talk" by Foo Kune et al., IEEE S&P 2013]

Pacemaker defense: application-level filter



Homework and Next

- Homework
  - ➡ Lab #1: Due Mon, Sep 22
  - ➡ Prelab #2: Due Thu, Sep 25
  - ➡ Essay #1: Due Mon, Sep 29
  - ➡ **In-class midterm: Monday October 27**

- Next
  - Monday: Sound and Sensors
  - Read for Monday: Trippel et al. “WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks,” in IEEE European Symposium on Security & Privacy, April 2017.
  - Thursday: Lab #2 time in class