Side Channels and Fault Injection

What is a side channel

- Any observable side effect of computation that an attacker could measure and possibly influence.
  - Timing
  - Light
  - Power
  - RF
  - Sound
  - Vibration
  - Heat

Vulnerable computations:

- Caches
- Data-dependent algorithms
- Branch prediction units

Classic Side Channels: RSA square-and-multiply algorithm

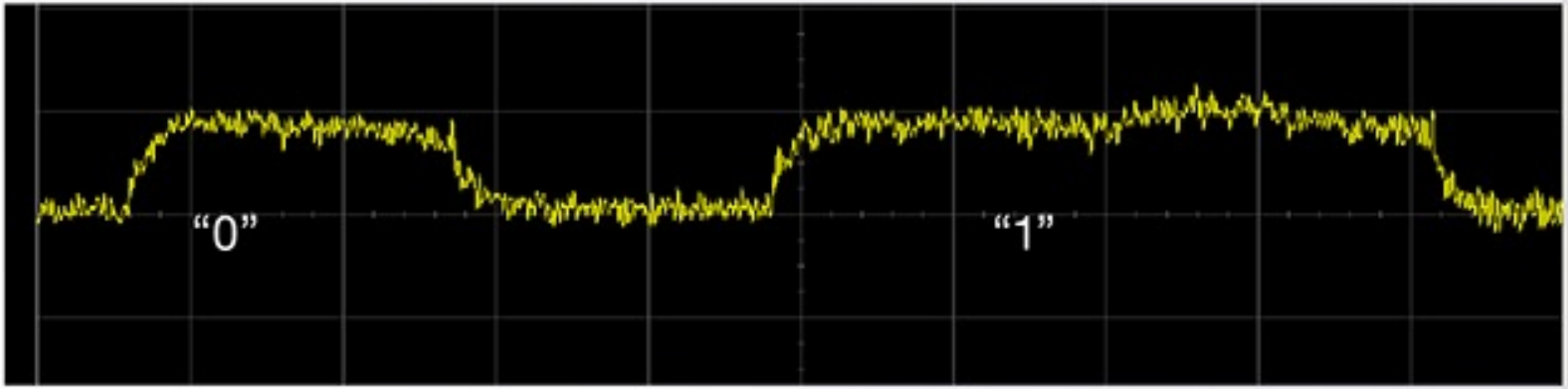
- **Simple power analysis (SPA) attack**
  - Just read the bits off an oscilloscope!
- **Timing attack**
  - More complicated, chosen ciphertext attack

SPA Intuition: Recursive version of RSA modular exponentiation

RSA Timing/Power Attack

$$c = m^e \pmod{n}$$

$$x^n = \begin{cases} x\ (x^2)^{\frac{n-1}{2}}, & \text{if } n \text{ is odd} \\ (x^2)^{\frac{n}{2}}, & \text{if } n \text{ is even.} \end{cases}$$



SPA in practice: Iterative version of RSA modular exponentiation

- $m = c^d \bmod n$ (d is k bits)
  example: $4^9 = 4^{1001} = (4^8)^1 \times (4^4)^0 \times (4^2)^0 \times (4^1)^1$

- m = 1
  while d > 0
    if (d is odd) // lsb-to-msb
      m = (m * c) mod n // slow
    shift d right 1 bit
    $c = c^2 \bmod n$ // slow

SPA side channel attack on iterative modexp

- $m = c^d \bmod n$ (d is k bits)

```
m = 1
while d > 0
    if (d is odd)
        m = (m * c) mod n        // extra slow
    shift d right 1 bit
    c = c^2 mod n                // slow, but less slow
```

- Intuition: Squaring less slow because = special case of multiplication. Dynamic programming tricks reuse internal computations and use left “shift” operator << for fast doubling that are not applicable to generic multiplication

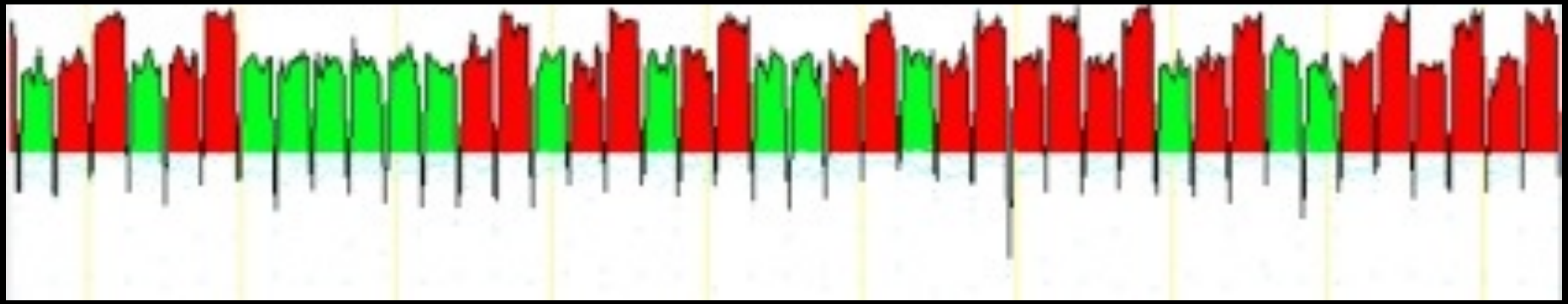
Square-and-multiply

- Example: $4^{13} \bmod 497$
- $4^1 \bmod 497 = 4$, $4^2 \bmod 497 = 16$, $4^4 \bmod 497 = 256$, $4^8 \bmod 497 = 429$

  $13_{10} = 1101_2$, result = $4^{1000} * 4^{100} * 4^1$
- result = $429 * 256 * 4 \bmod 497 = 445$

SPA Exercise: Find the RSA exponent

Note: Red pulses backwards



https://partners.nytimes.com/library/tech/98/06/biztech/articles/22card.html
https://www.rambus.com/differential-power-analysis/

RSA modexp timing attack

- **Chosen ciphertext** timing attack: recover private RSA exponent d of m = c^d mod n
- Intuition: Trick victim into performing decryptions of chosen ciphertexts, observe time for decryption to reveal MSB of exponent
- Method: Adversary chooses many pathological ciphertexts to illicit unusual behavior and performance of textbook modexp algorithm

https://www.rambus.com/timing-attacks-on-implementations-of-diffie-hellman-rsa-dss-and-other-systems/

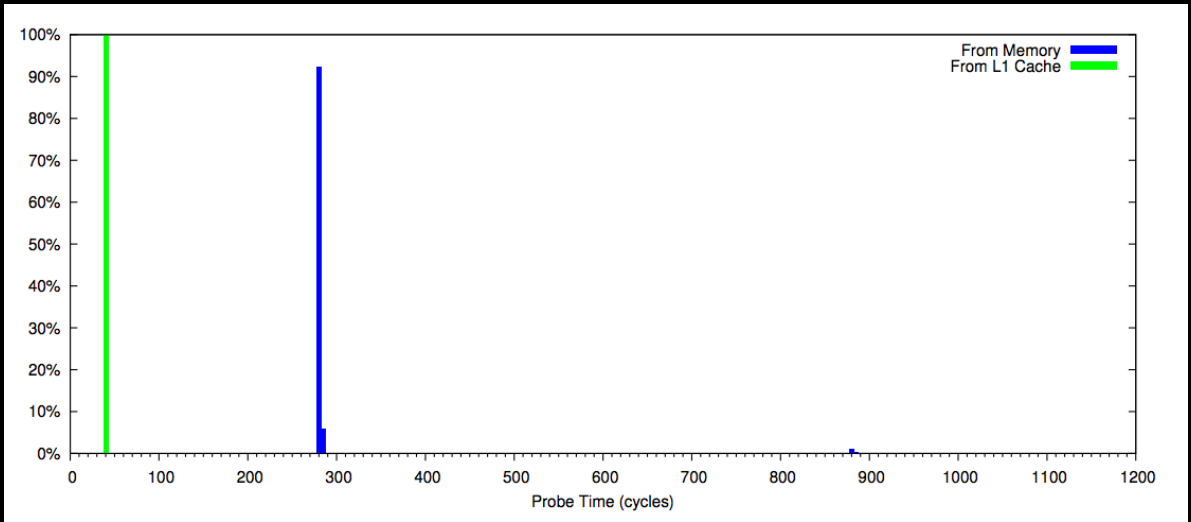
RSA modexp timing attack

- Assume: Modular **multiplication** usually fast, but occasionally a ciphertext causes multiplication to be slower than an entire modular **exponentiation**
- If mult step slow, but total decryption fast, we know the next LSB exponent bit **must** be 0
- If mult step fast, but total decryption slow, the next LSB exponent bit was **probably** 1
- Iterate on each bit of exponent from LSB to MSB (dynamic programming)

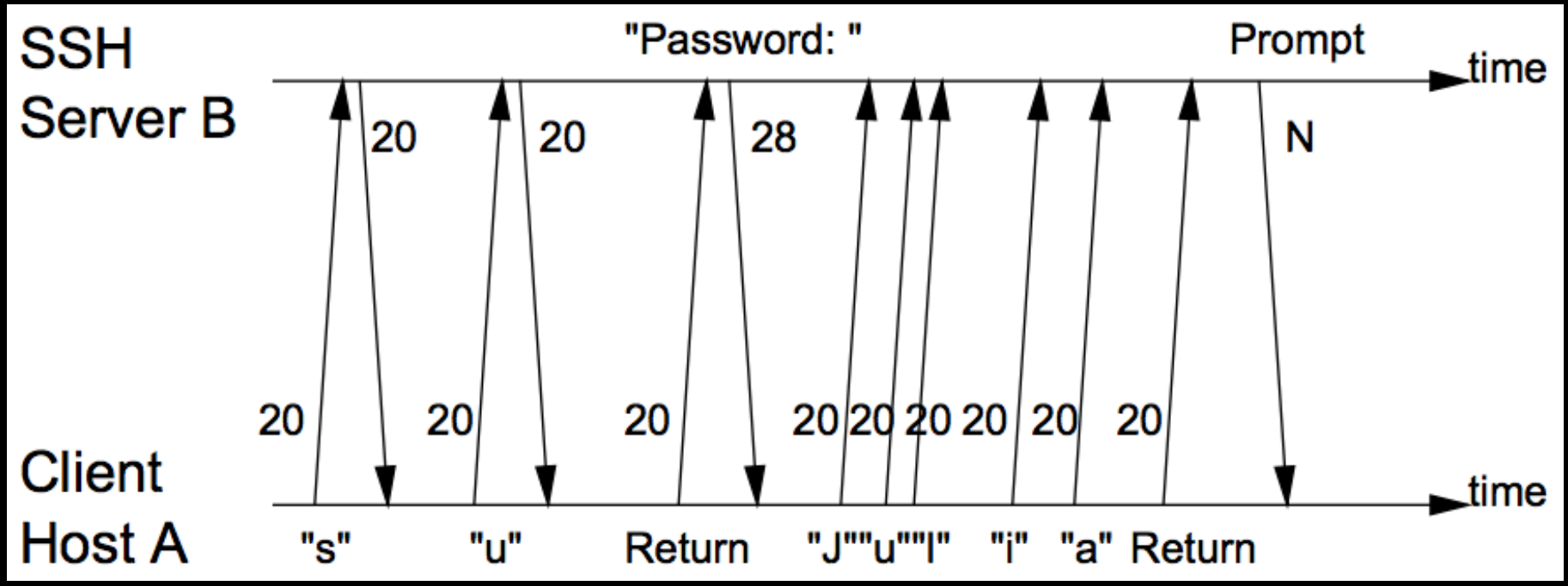
https://www.rambus.com/timing-attacks-on-implementations-of-diffie-hellman-rsa-dss-and-other-systems/

Cache timing attack

- Assume shared bignum library
- Repeatedly:
  measure access time to shared code
  flush shared code from cache
  while modexp is running

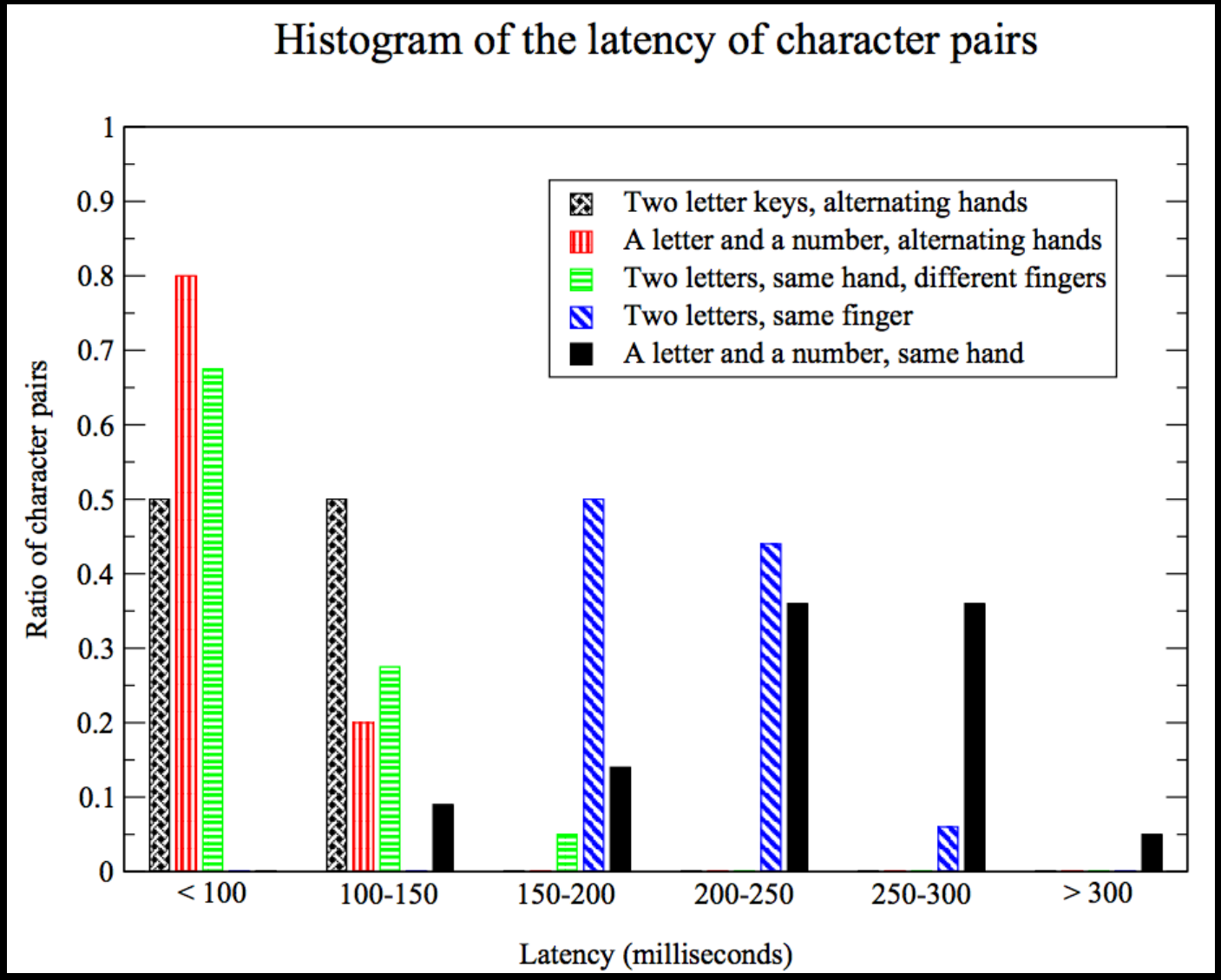


Timing attack on SSH passwords



https://people.eecs.berkeley.edu/~daw/papers/ssh-use01.pdf

Timing attack on SSH passwords



Modem light side channel

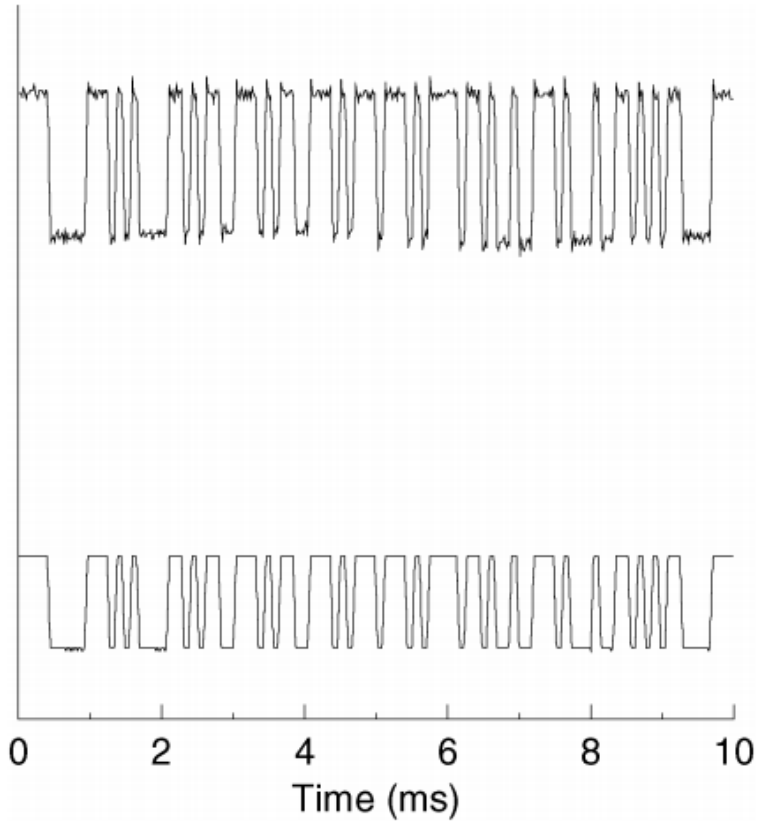


Fig. 1. Compromising optical emanations. The lower trace shows the ±15 V EIA/TIA-232-E input signal (at 9600 bits/s); the upper trace shows optical emanations intercepted 5 m from the device.

Acoustic side channel

- Different keys sound different; same keys sound the same
  - Speed up brute force attack
- Printer acoustics reveals printer output
  - 3-D printer acoustics, too

Data remanence

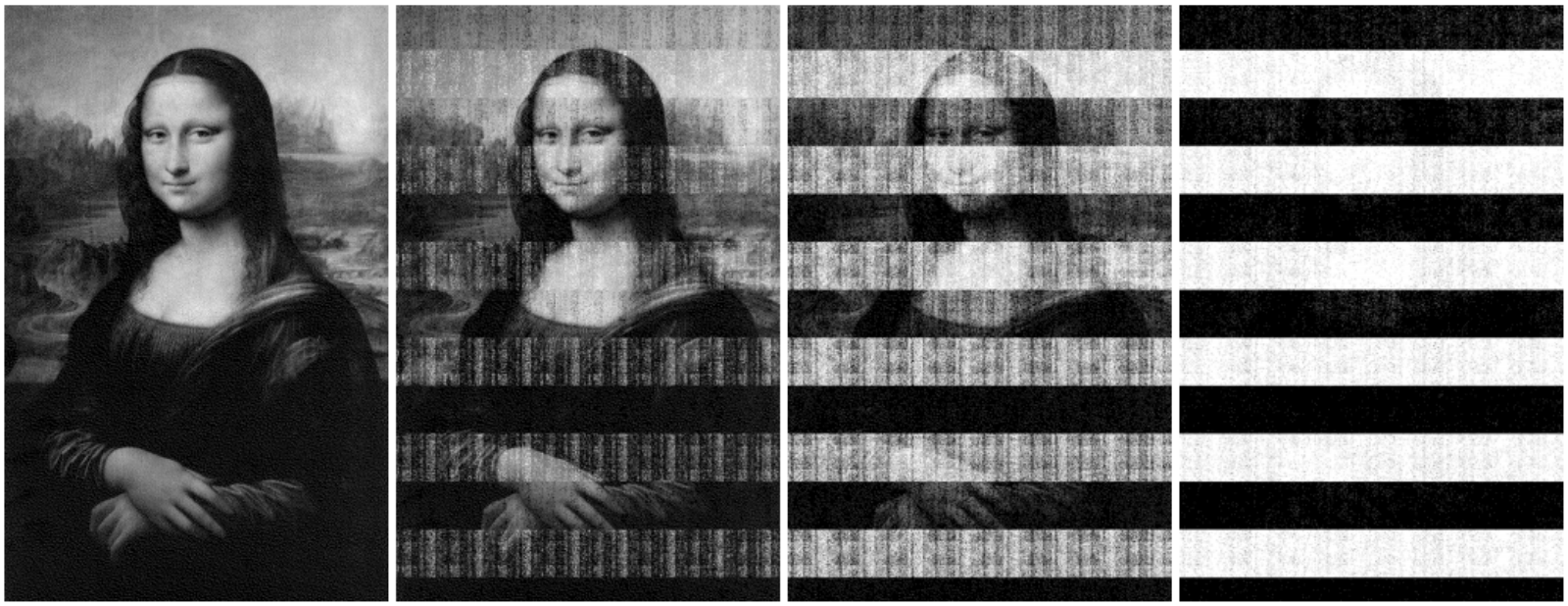
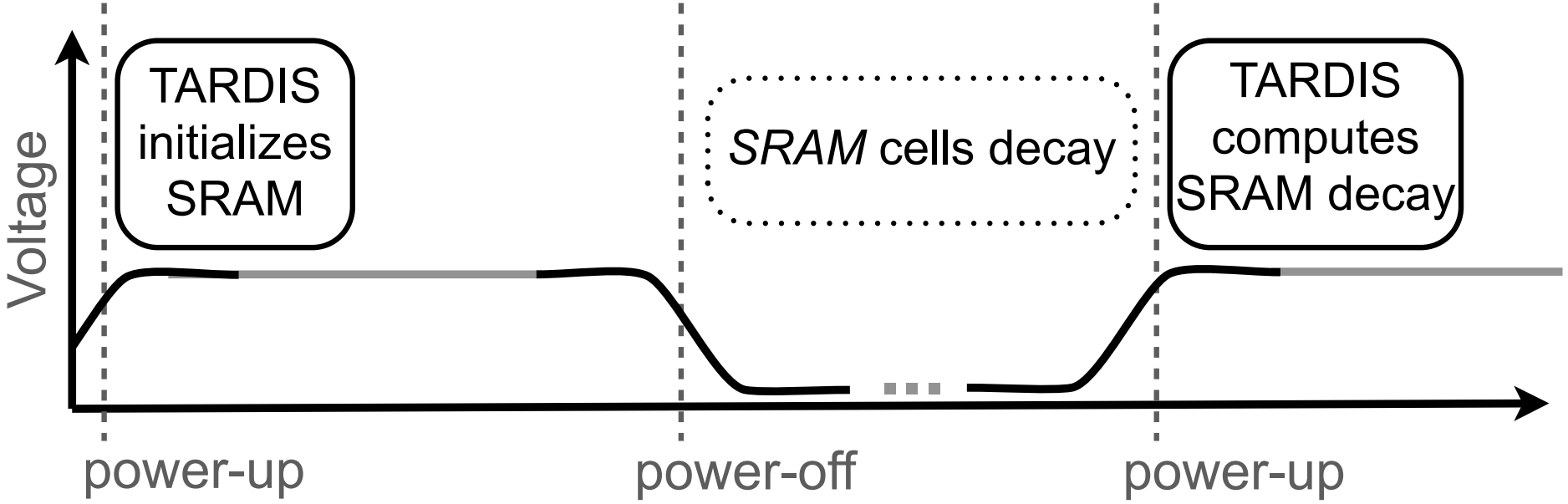
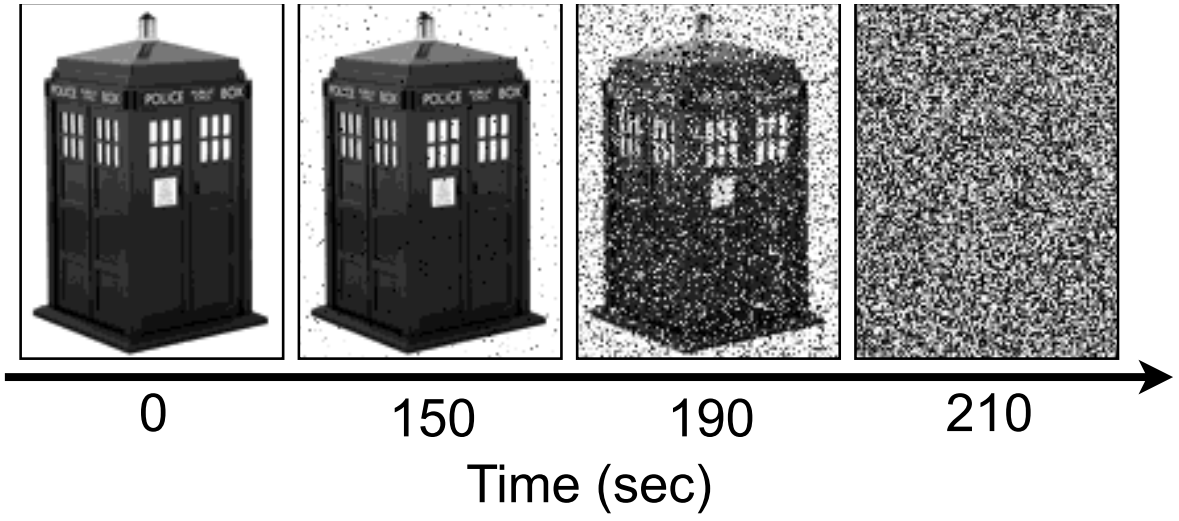


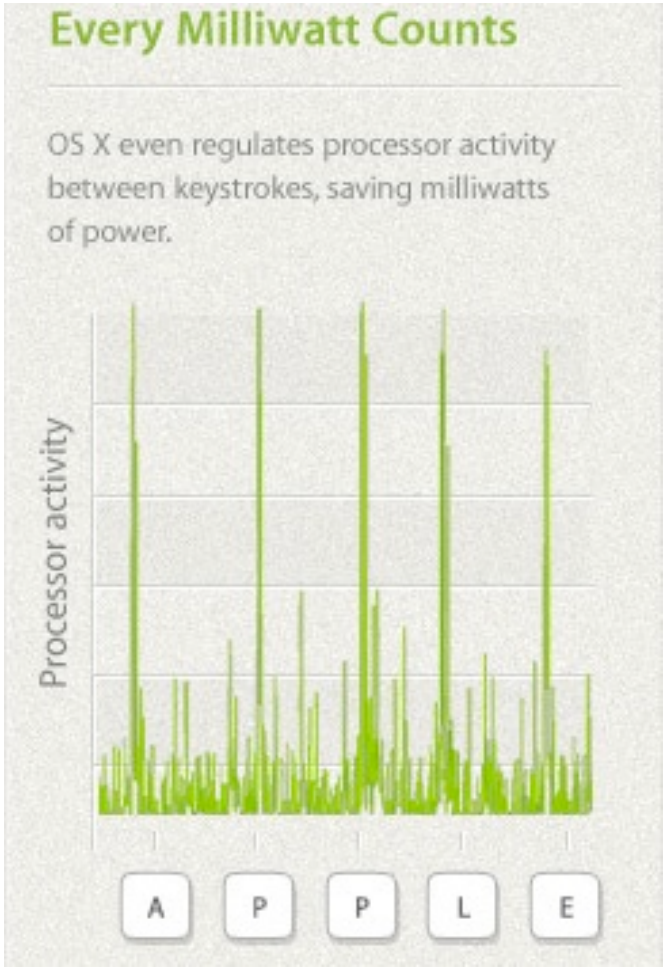
Figure 4: We loaded a bitmap image into memory on Machine A, then cut power for varying lengths of time. After 5 seconds (left), the image is indistinguishable from the original. It gradually becomes more degraded, as shown after 30 seconds, 60 seconds, and 5 minutes.

Time and Remanence Decay in SRAM

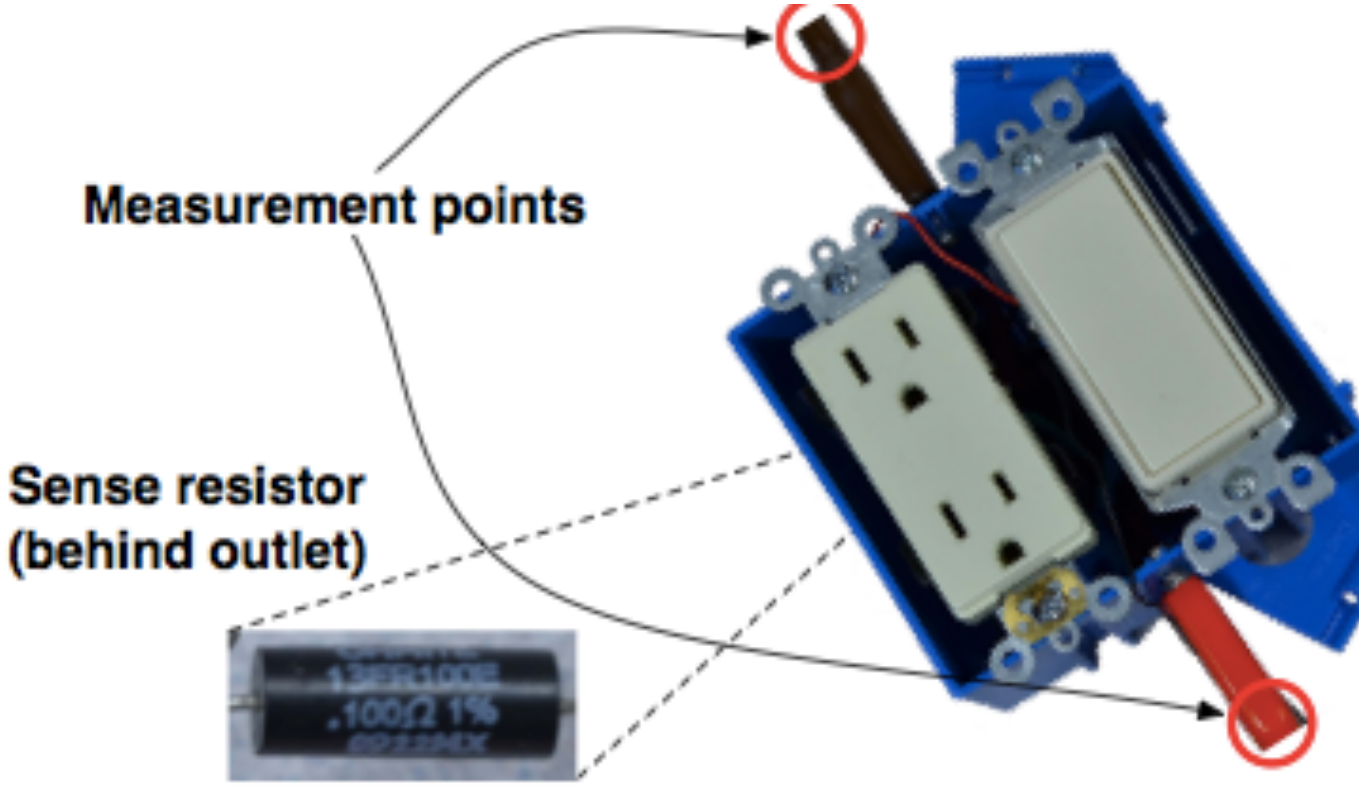


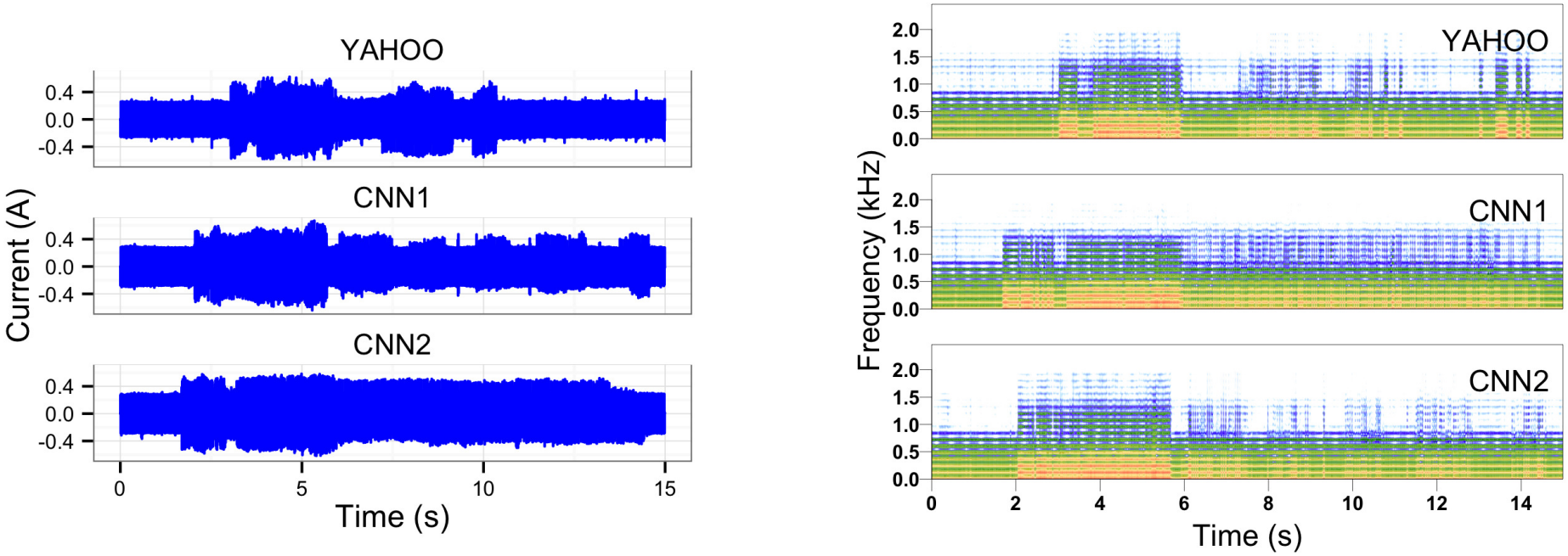


Detecting Malware at Power Outlets



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



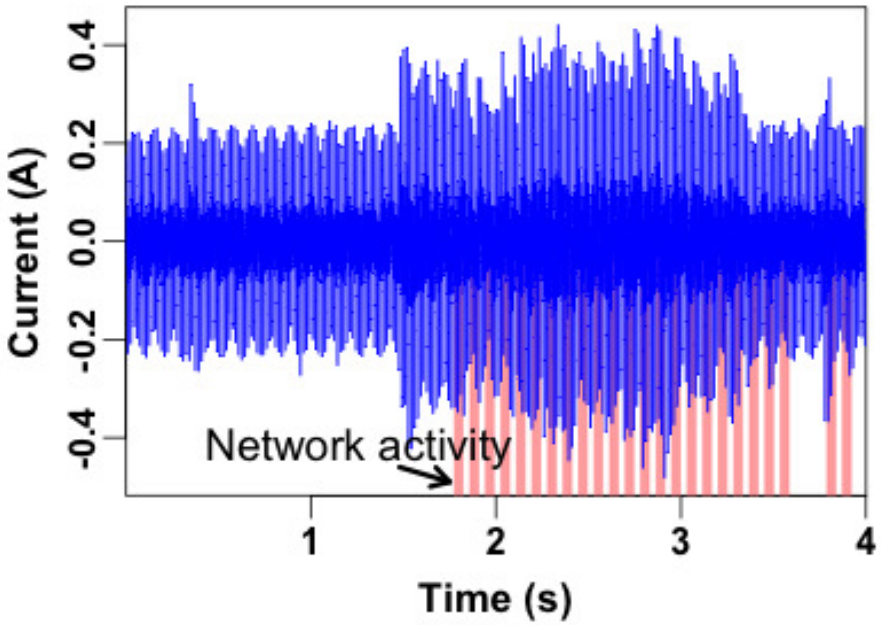


(a) Time-domain plots

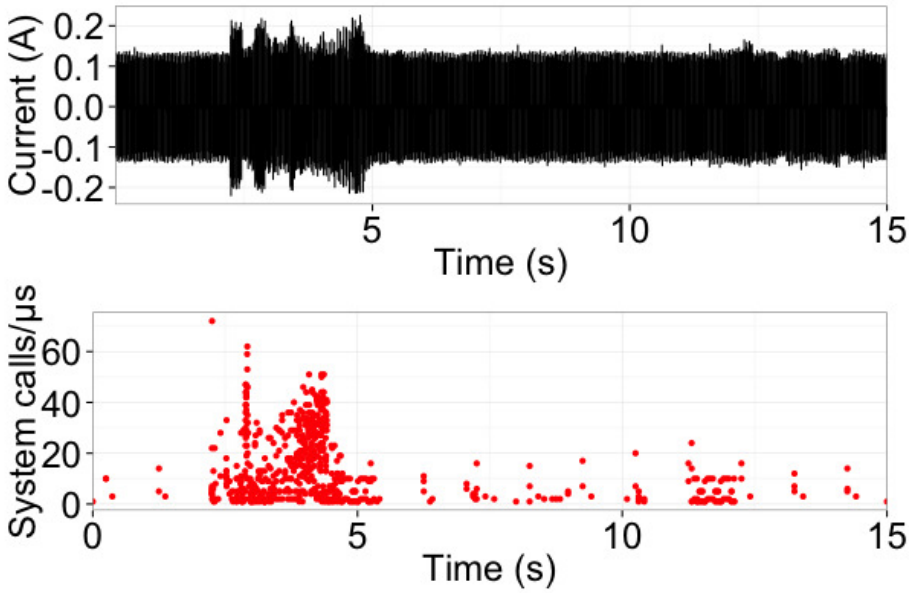
(b) Spectrogram plots

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



(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.

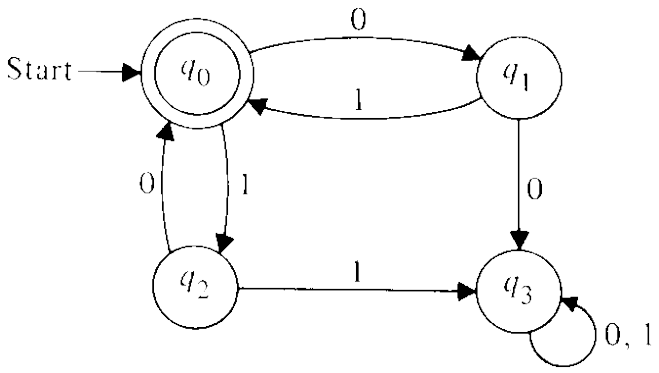


(b) The system call activity (as measured by DTrace) is also correlated with high current consumption, and our results suggest that systems exercised by system calls are a major cause of consumption.

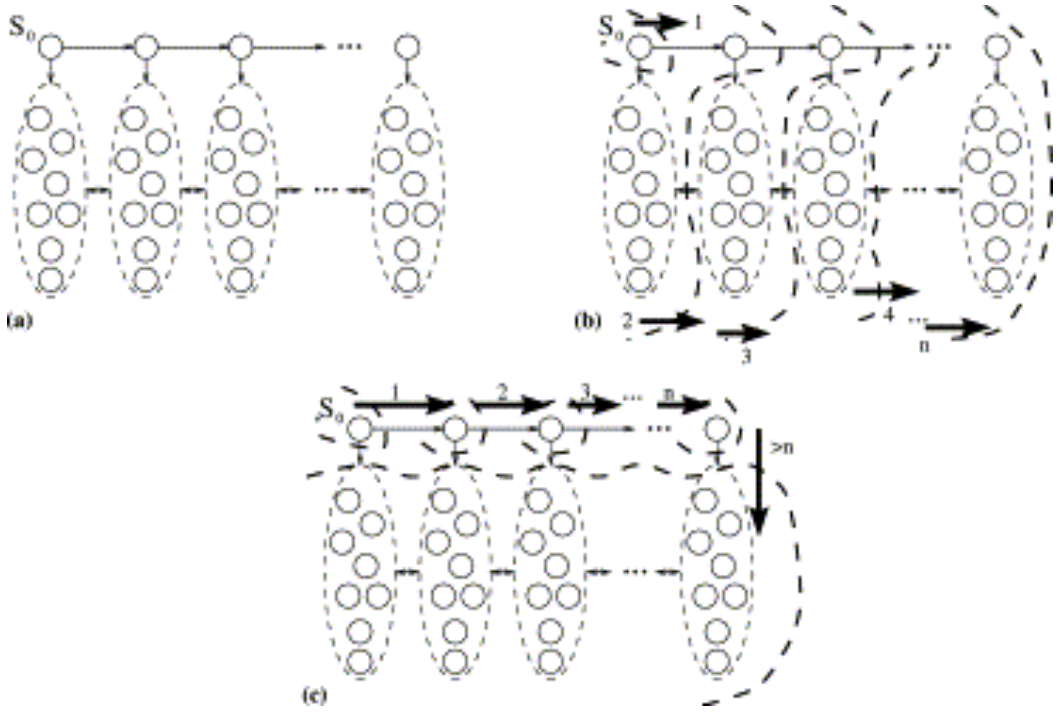
Fig. 2: Time-domain plots as a MacBook loads webpages. Both network activity and system calls appear to correlate with energy consumption.

Intuition

Embedded



General-purpose




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

Side channel defenses

- Ciphers with bounded side channel leakage
  - Fixed-time algorithms (no data-dependent delays, branches)

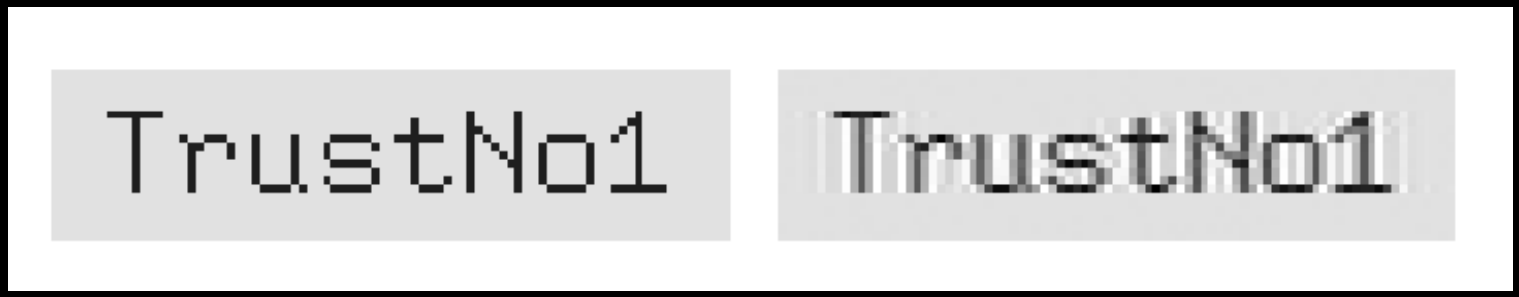
From GnuPG:

```
/* To mitigate the Yarom/Falkner flush+reload cache
 * side-channel attack on the RSA secret exponent, we
 * do the multiplication regardless of the value of
 * the high-bit of E.
 …

/* To mitigate the Yarom/Falkner flush+reload cache side-channel
 * attack on the RSA secret exponent, we don't use the square
 * routine but multiplication.
 …
```

Side channel defenses

- TEMPEST fonts



Side channel defenses

- TEMPEST fonts
- Masking and blinding with random nonces
- Differential matching (flip 0 and 1) to mask transitions
- Pre-charging registers and busses to reduce predictable transitions
- Add amplitude or temporal noise

RF side channel & injection

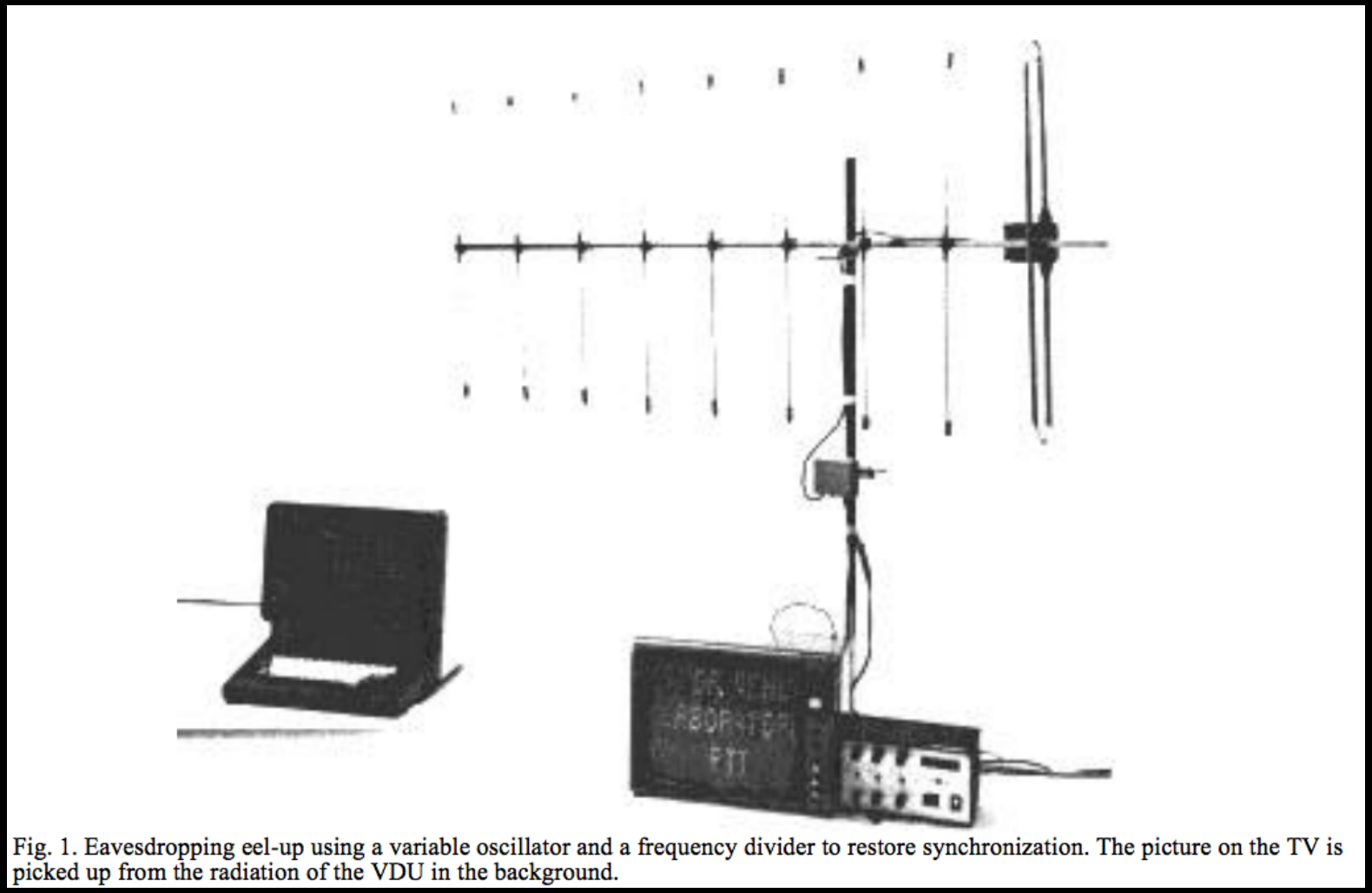


Fig. 1. Eavesdropping eel-up using a variable oscillator and a frequency divider to restore synchronization. The picture on the TV is picked up from the radiation of the VDU in the background.

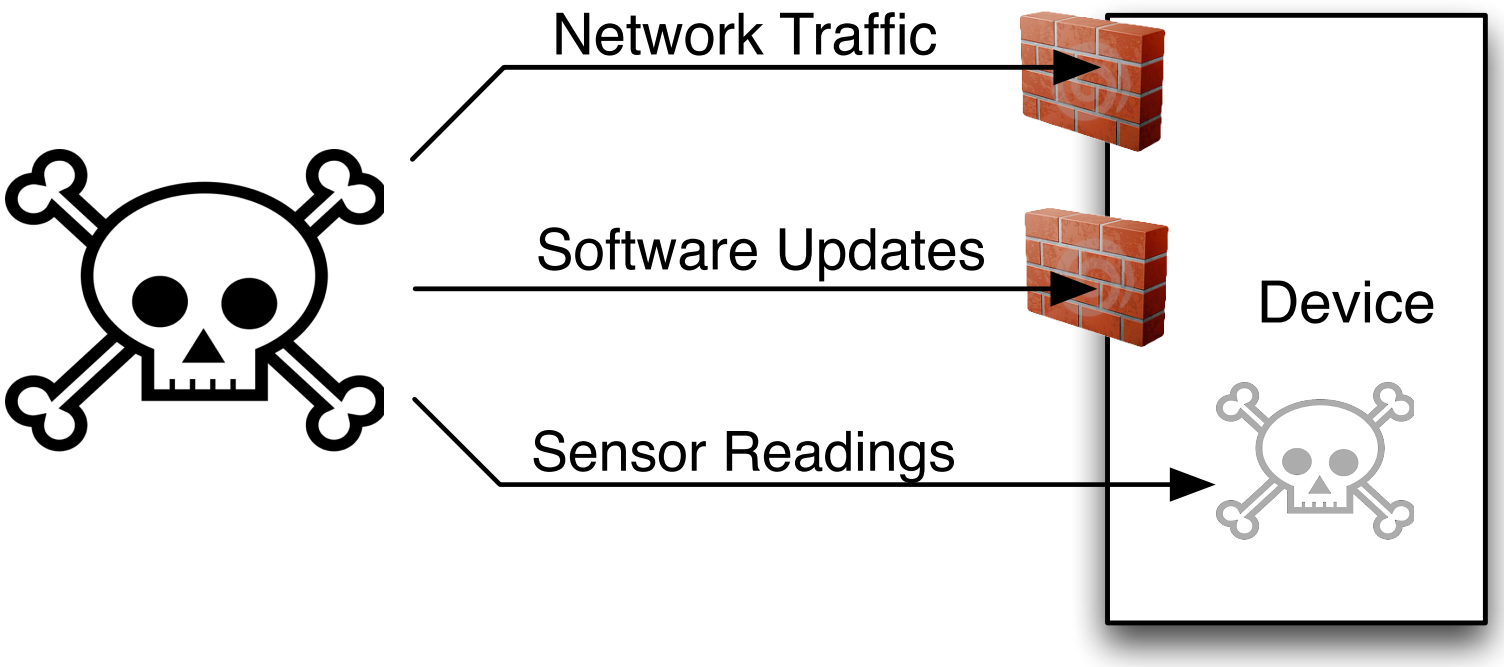
Intentional Electromagnetic Interference (Or Don't Trust Your Sensors)

"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.

Inputs may not be trustworthy



Many reports of accidental interference

Cellphone
+
Oven

New York Times
Aug 21 2009

Ambulance comm
+
Life support system

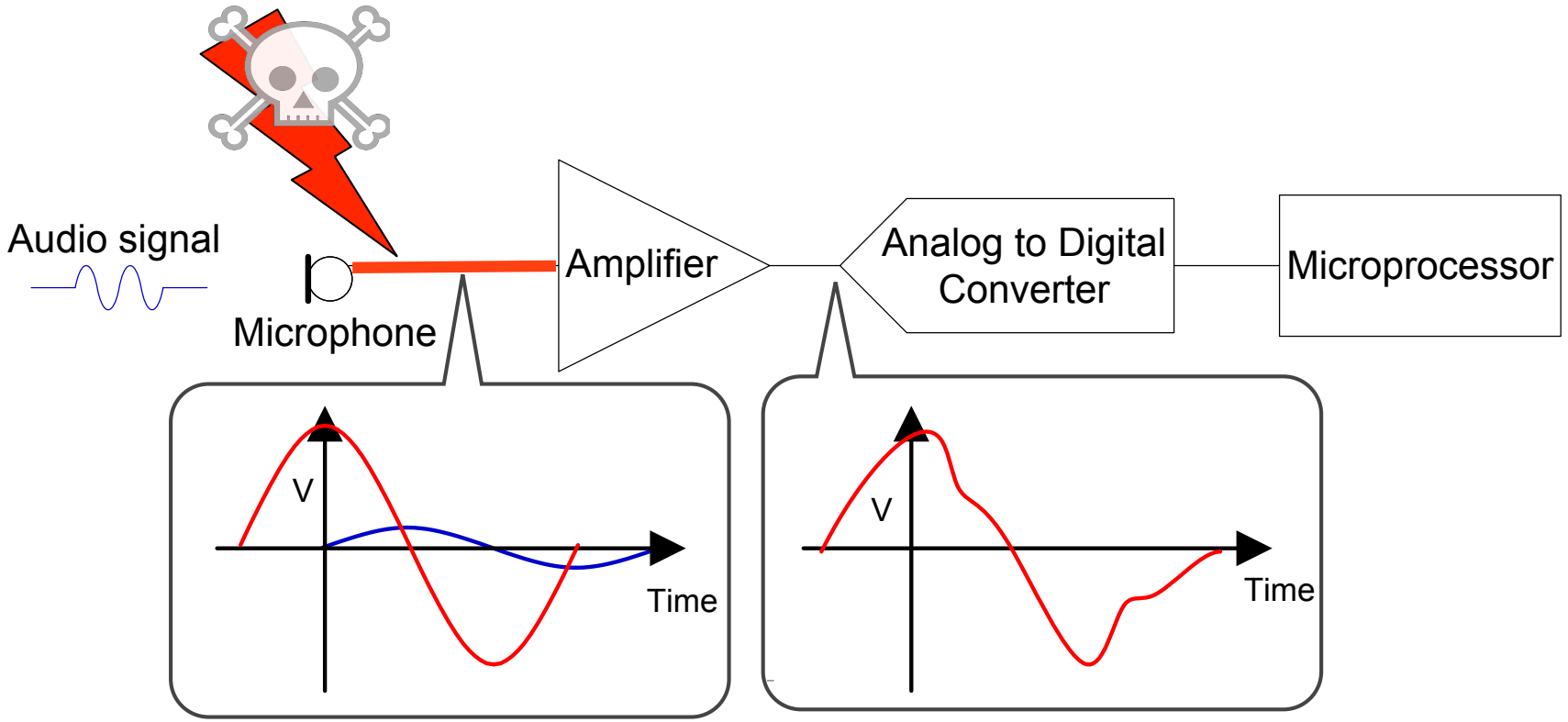
Armstrong, Hutley
2007

EMI
+
Anti-lock brakes

NASA pub 1374
1995

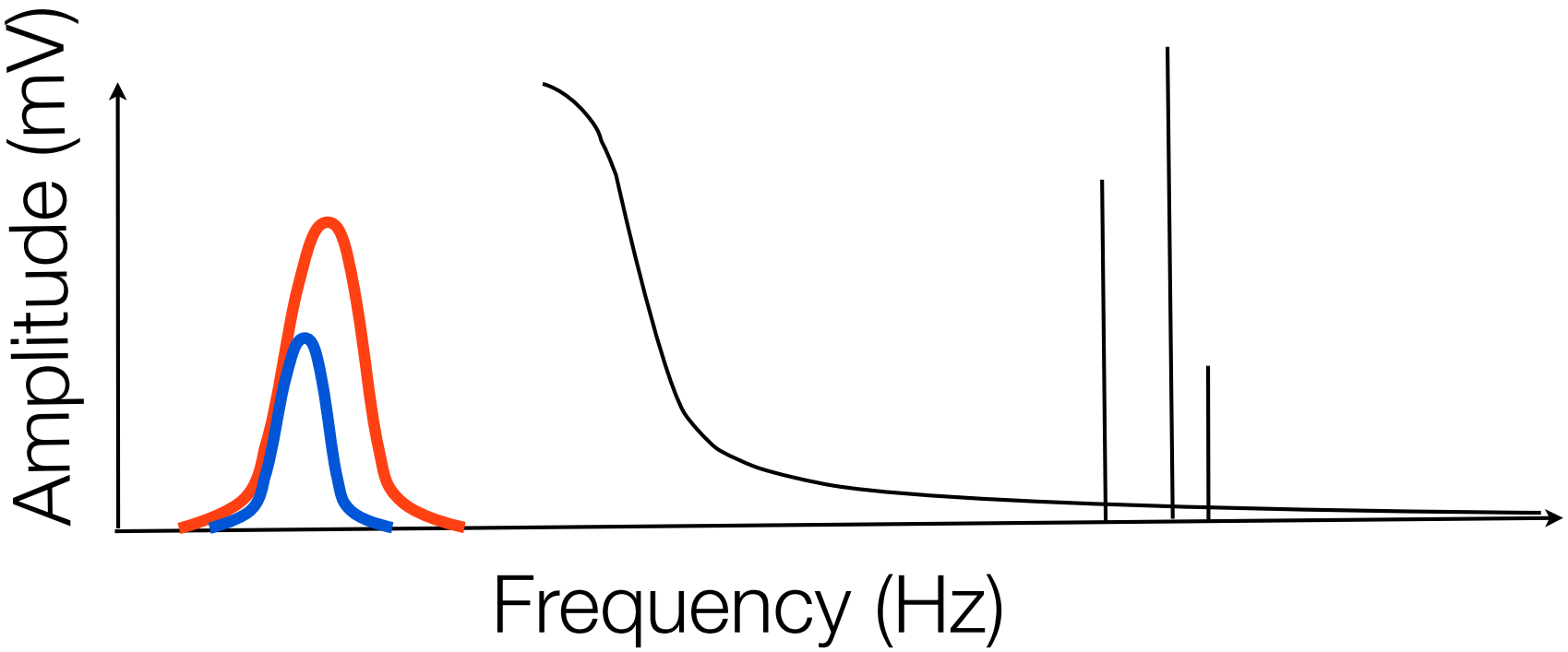
Ghost Talk: Intentional interference

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

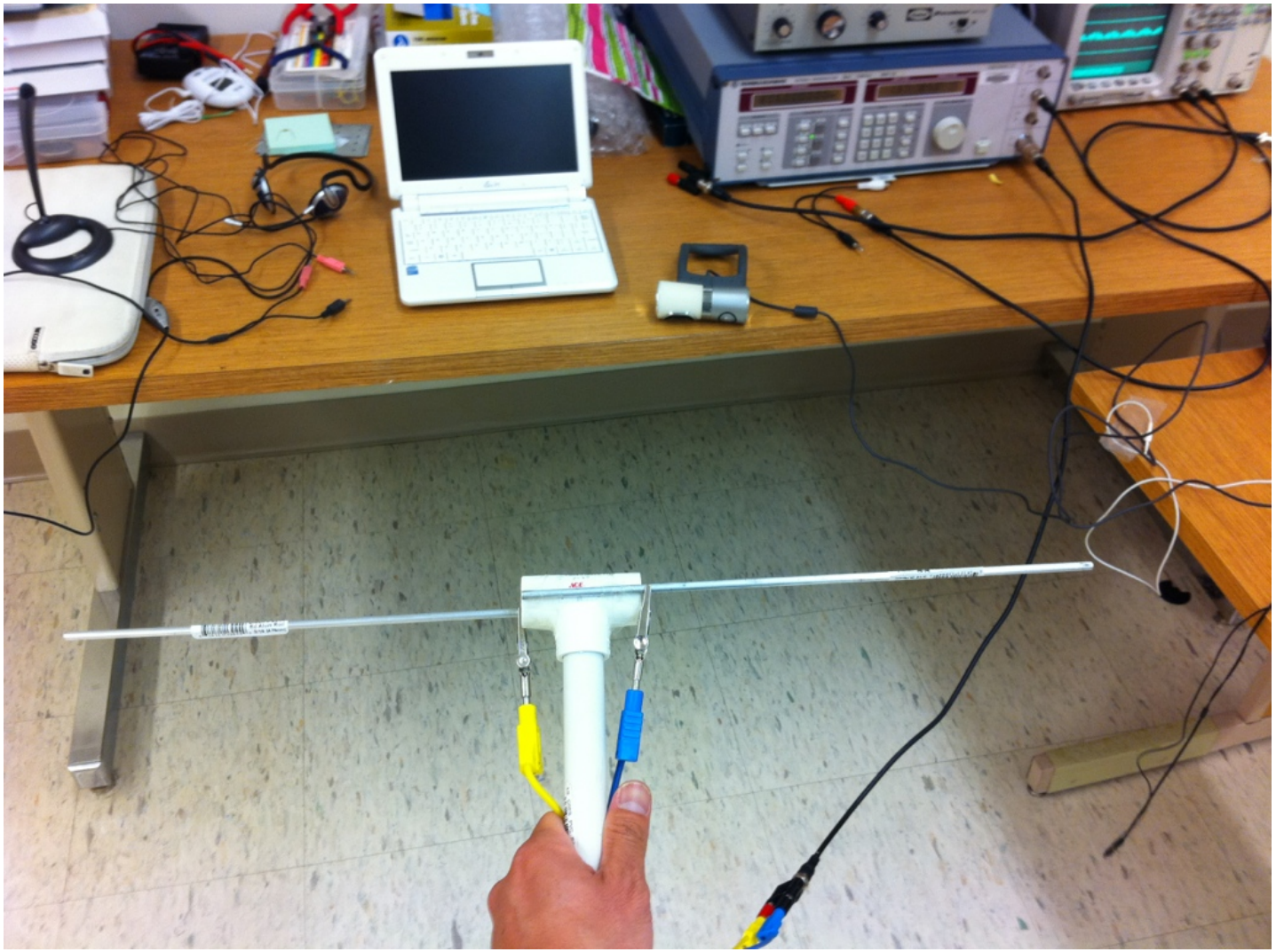


The fundamental problem: It's the baseband

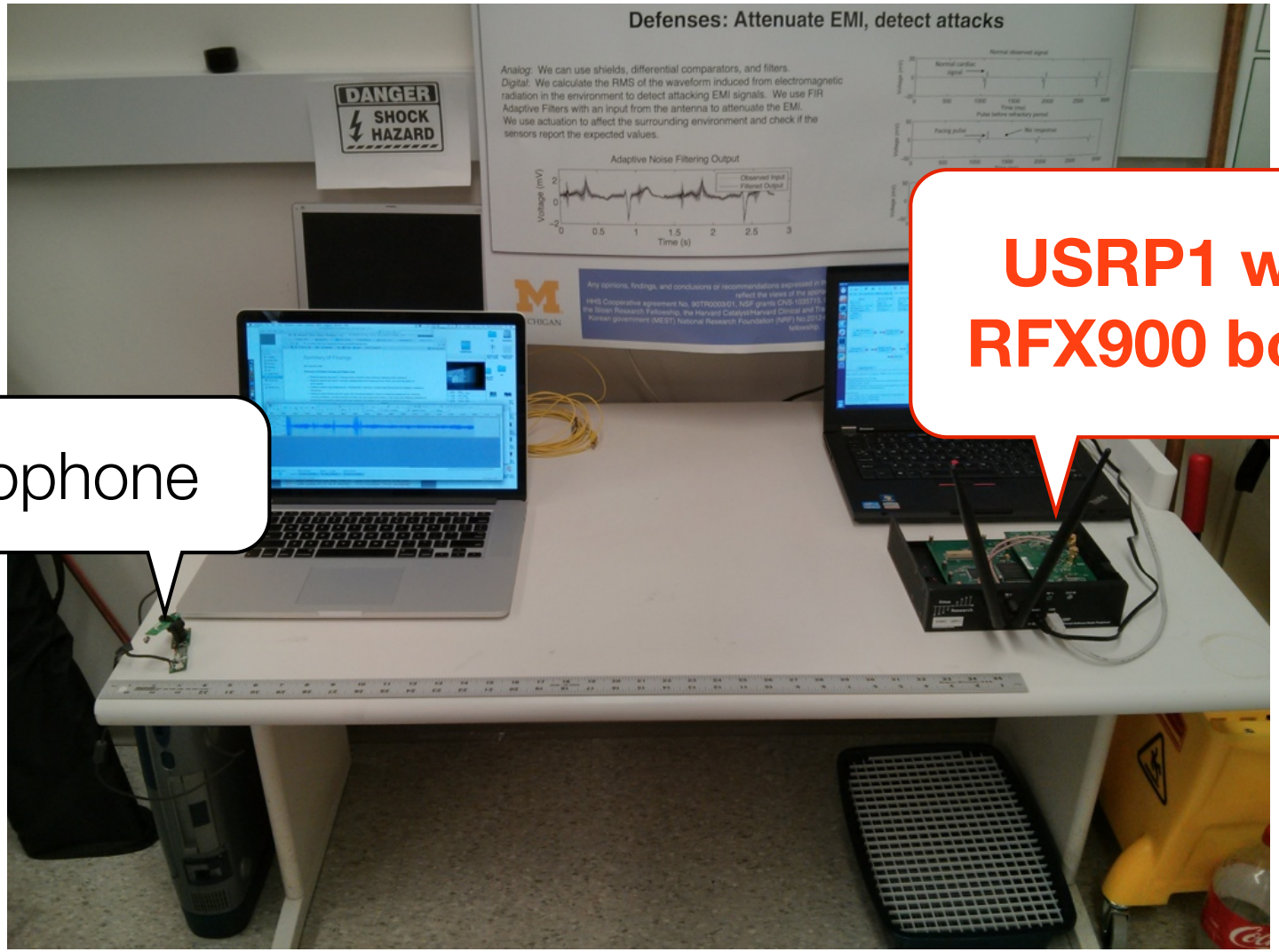
- Baseband: frequency range of desired signals.
- Interference outside the baseband is easy to filter.
- Interference in the baseband is hard to remove.



Mic and dipole antenna

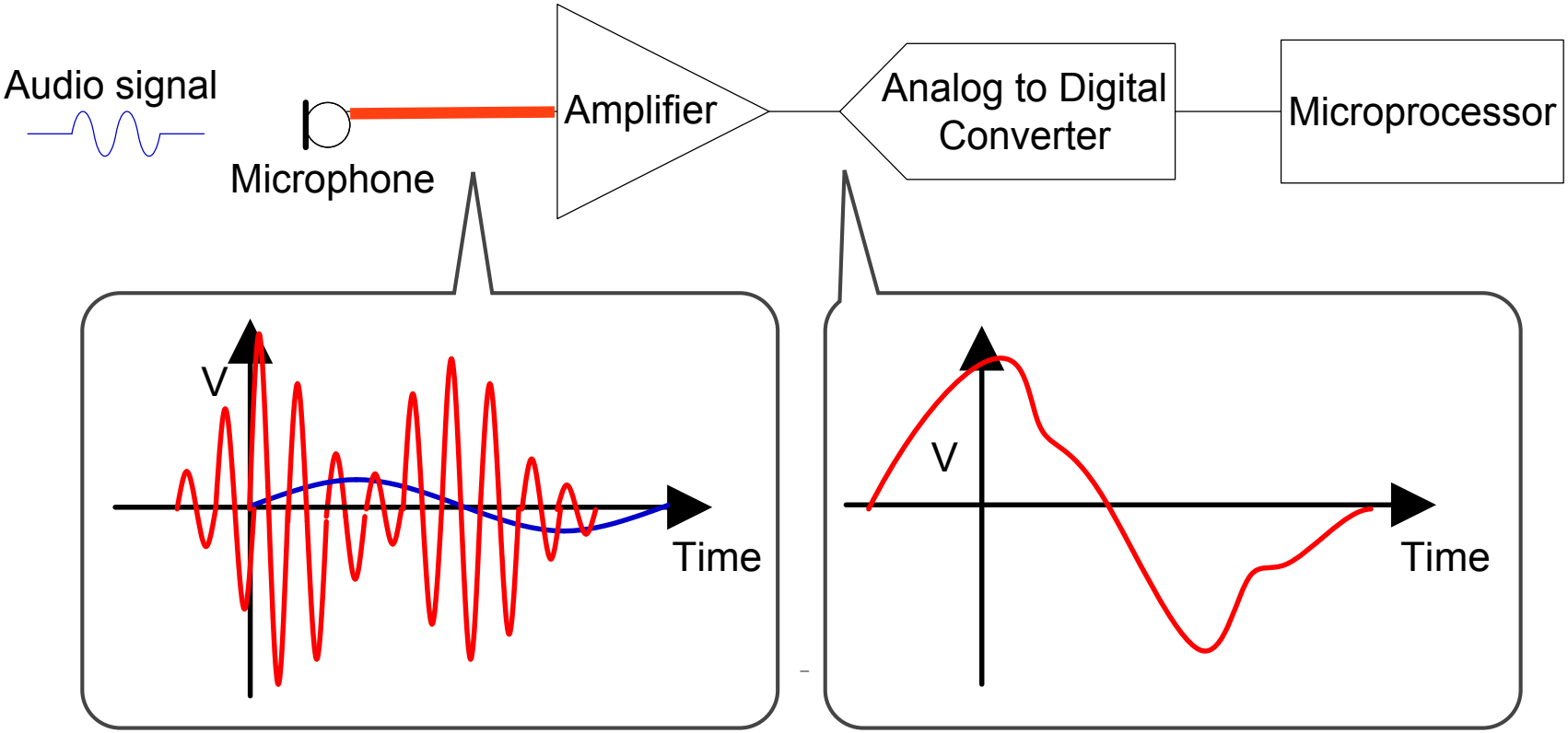


Microphone interference with USRP



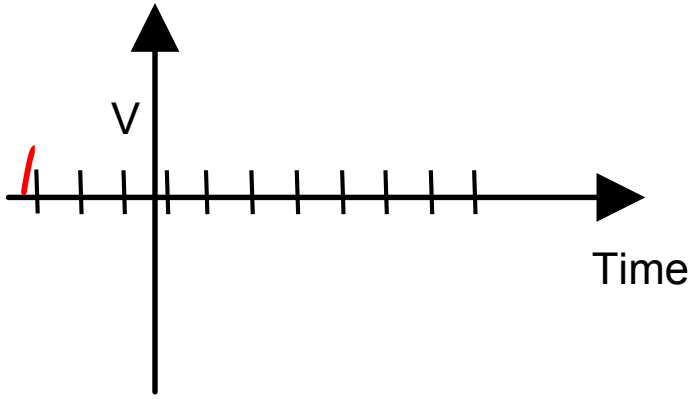
Operational challenges for intentional EMI

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

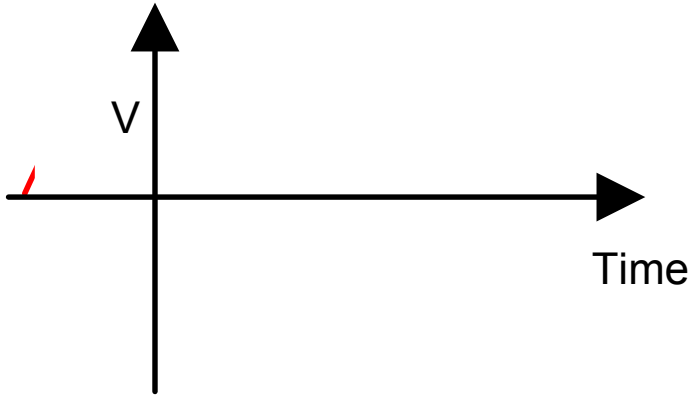


Sampler can demodulate signal

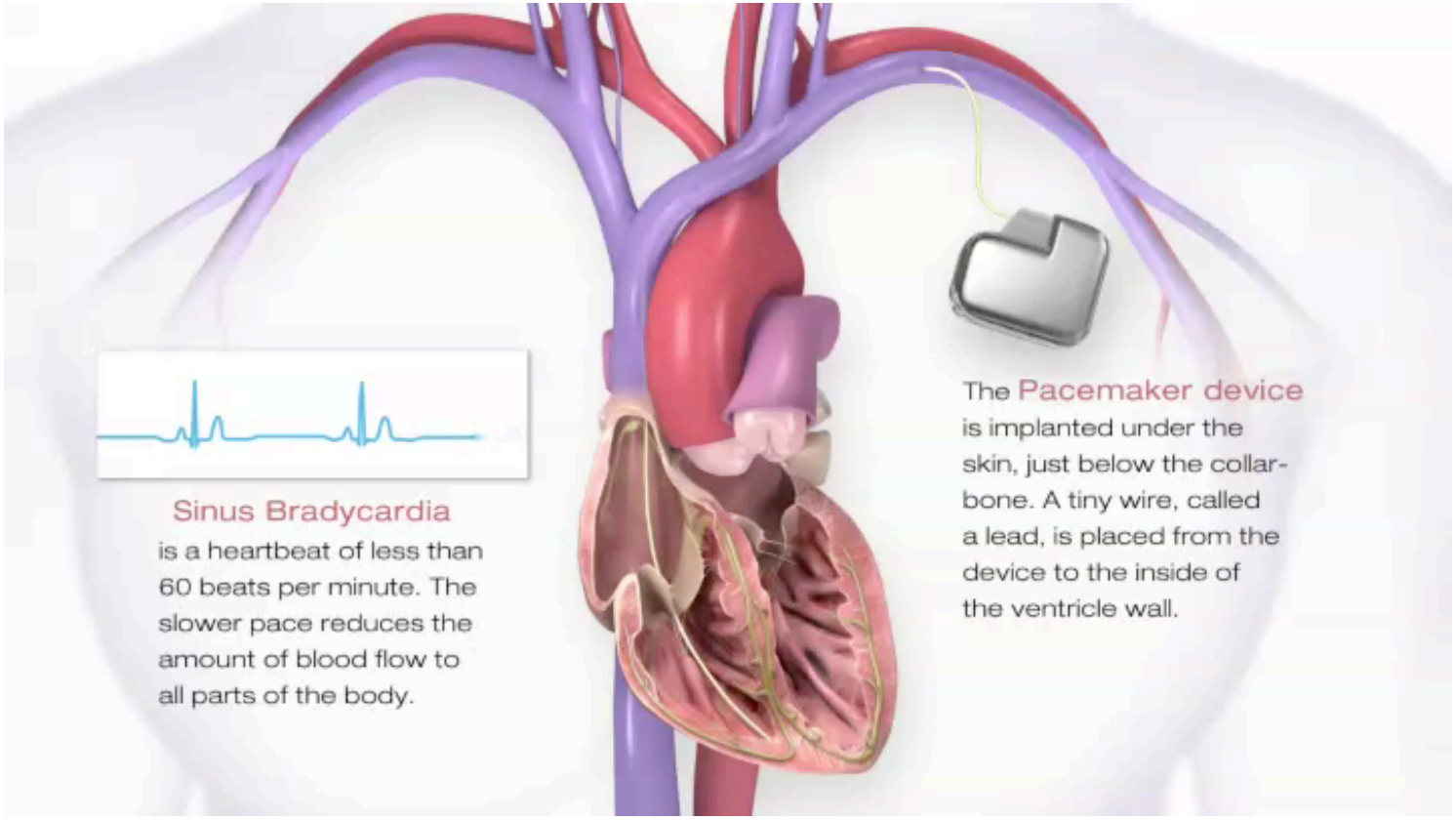
Induced interference



Resulting sampled signal



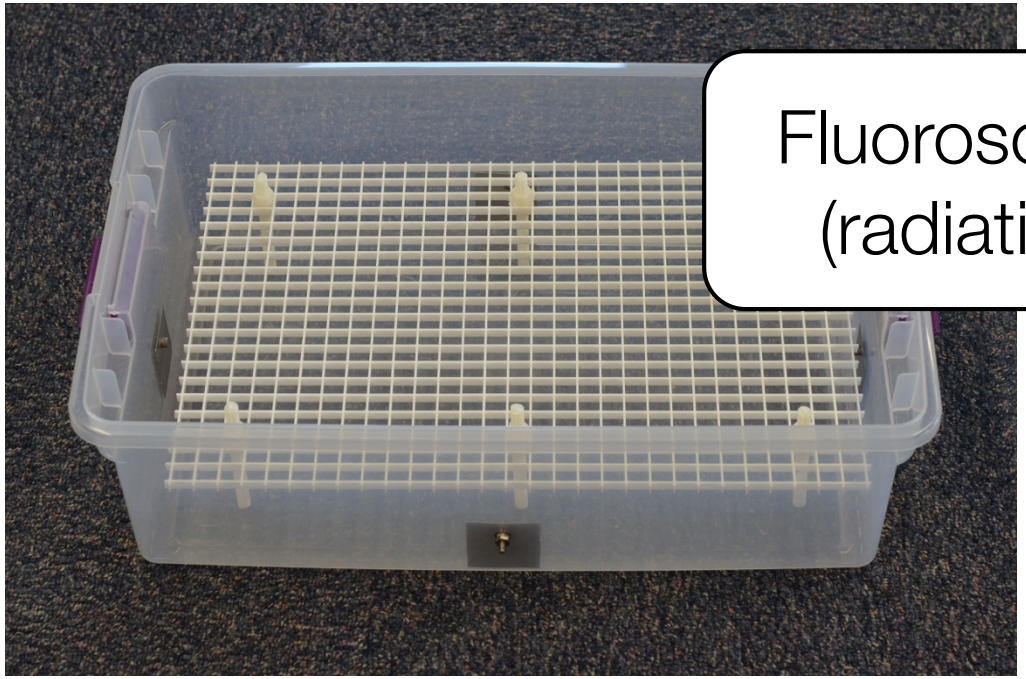
The cardiac cycle



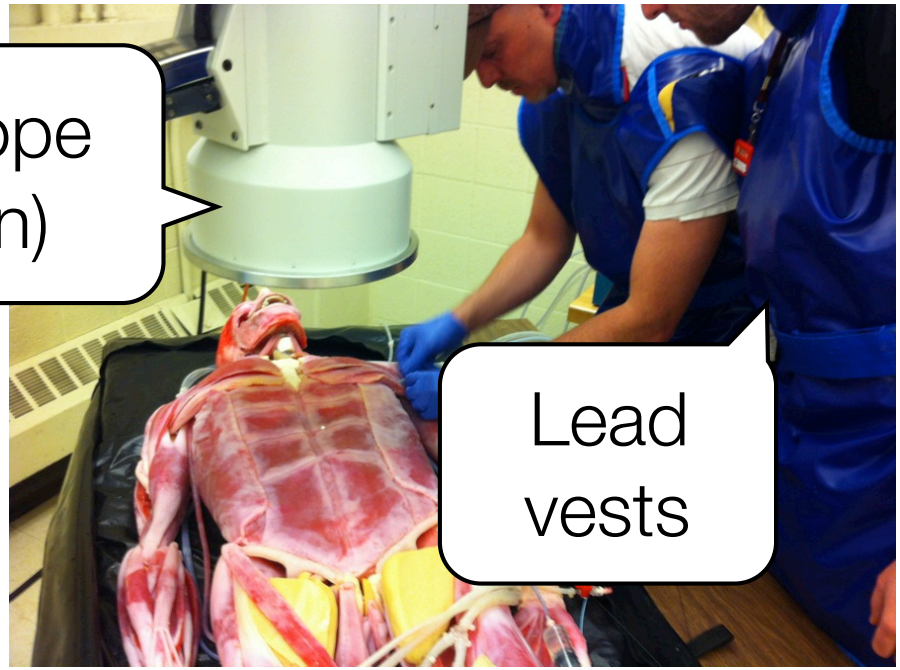
American Heart Association, August 2012

Experimental setup: Simulators

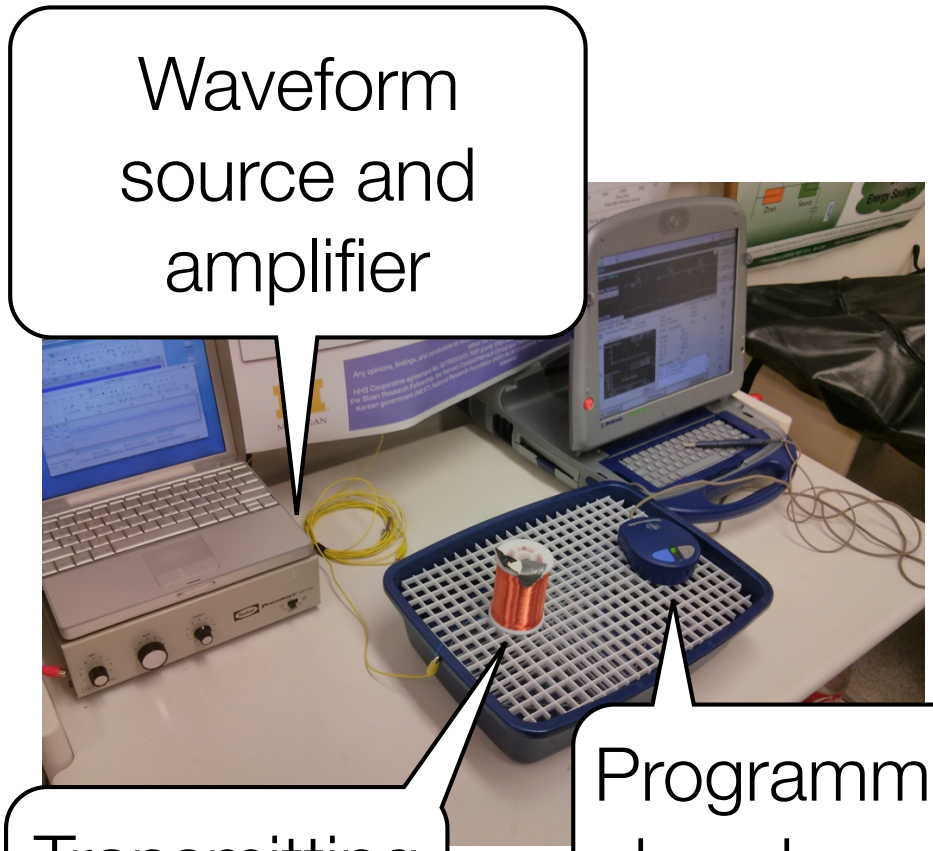
Saline bath

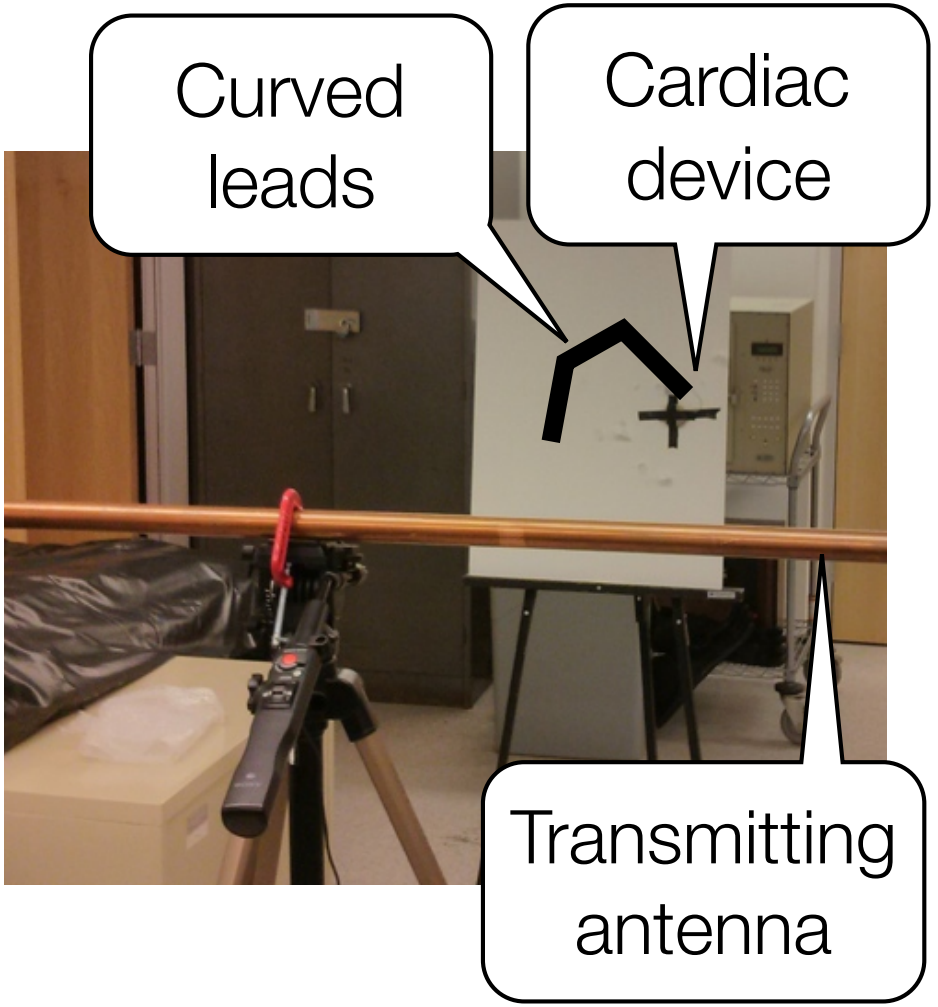


Synthetic human



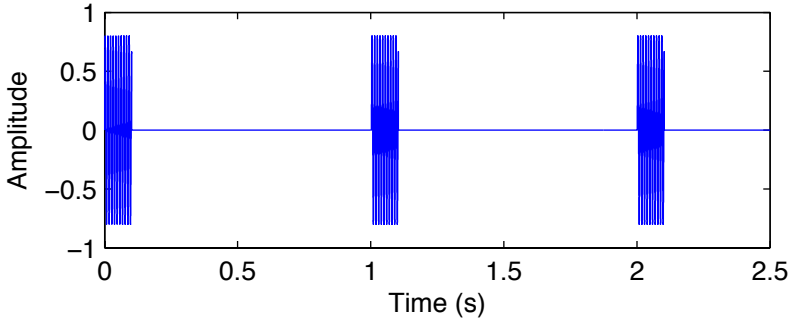
Experimental setup: Devices and emitters

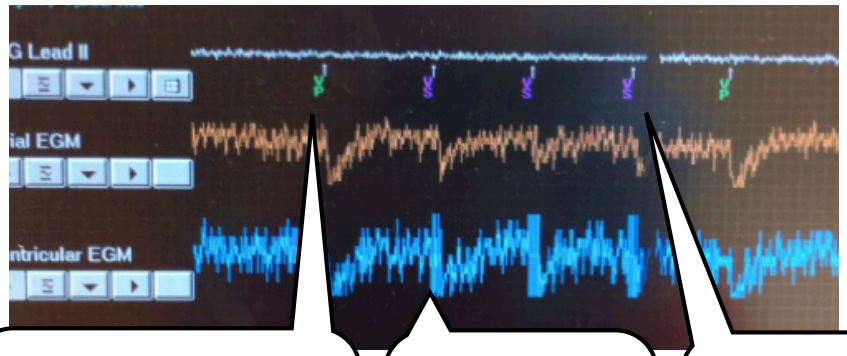




Results: Waveforms and responses

Pulsed sinusoid



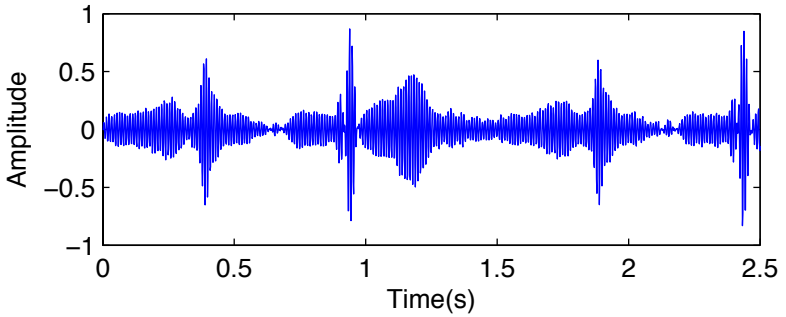


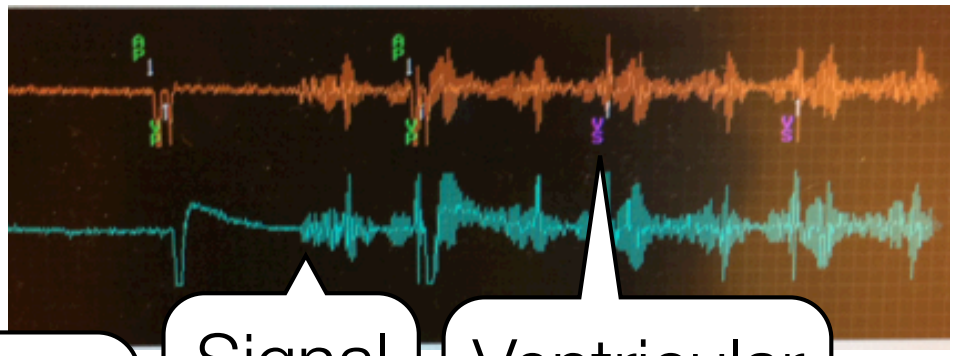
Ventricular pace

Signal onset

Ventricular sense

Modulated heart beat





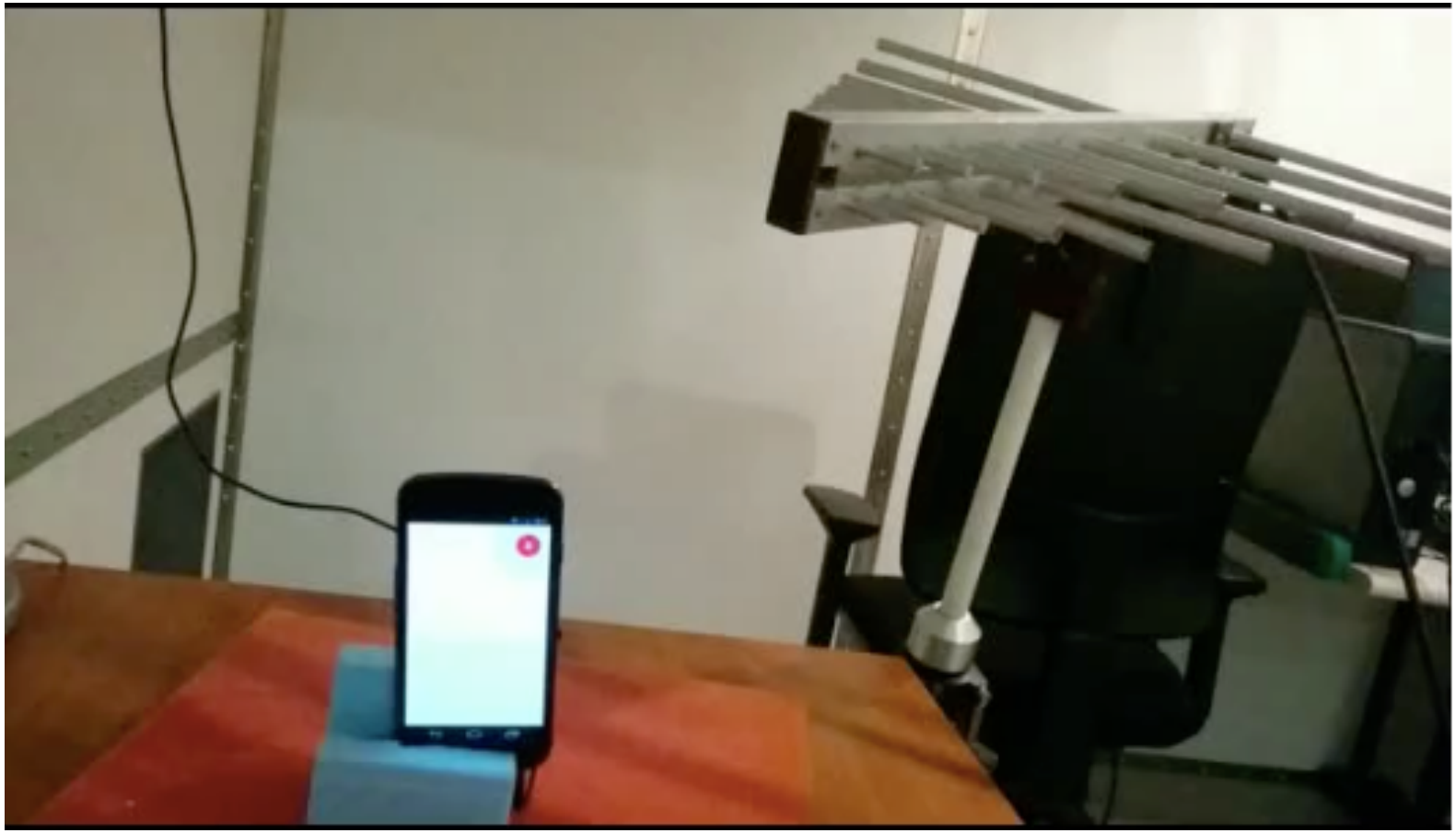
Signal onset

Ventricular sense

Results: Interference distances

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

GhostTalk on Mobile Phones



[http://www.wired.com/2015/10/this-radio-trick-silently-hacks-siri-from-16-feet-away/]

"Runs on a Chip"

How LED Lights Can Cause Problems With Your Garage Door Opener

NOVEMBER 4, 2013 BY TOMMY MELLO

If you've been experiencing problems with your garage door opener remote unit – sometimes it works, sometimes it doesn't – and can't track the problem down, you might look to the type of lights you're using in and around your garage for the culprit.

http://www.phoenixazgaragedoorrepair.com/garage-door-repair/1786/how-led-lights-can-cause-problems-with-your-garage-door-opener/garage-door-blog/

"Runs on a Chip"

Can LED lights interfere with your garage door opener?

By Deni Hawkins | Published: Apr 17, 2014 at 5:39 PM MDT | Last Updated: Apr 17, 2014 at 7:04 PM MDT

Recommend 0 G+1 0 Tweet 0 Print Email

NAMPA, Idaho (KBOI) - A local man makes strides to conserve energy, but believes it may have caused problems for him and his neighbors in the process.

http://www.phoenixazgaragedoorrepair.com/garage-door-repair/1786/how-led-lights-can-cause-problems-with-your-garage-door-opener/garage-door-blog/

No Worries As Long As No Antenna...

GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies

Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky[1], Yuval Elovici[1]

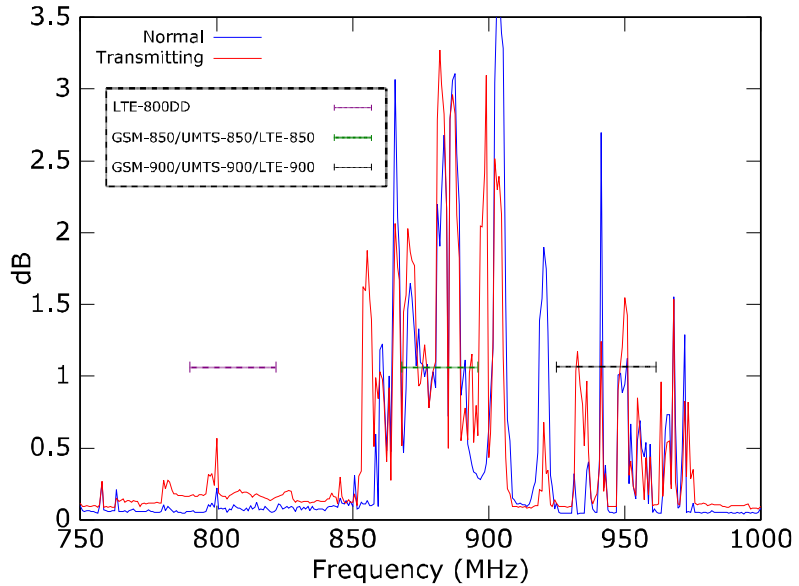


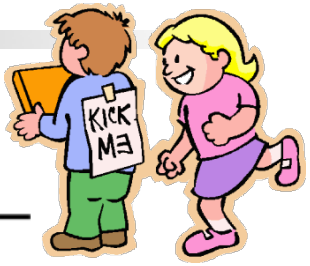
Figure 3: A plot of the amplitude of the radio waves emitted from a motherboard with an 800MHz I/O bus using DDR3-1600 RAM. Blue: casual use of the computer. Red: our transmission algorithm while using the dual channel data paths.

[USENIX Security 2015]

We propose that a computer's memory bus can be exploited to act as an antenna capable of transmitting information wirelessly to a remote location. When data is exchanged between the CPU and the RAM, radio waves are emitted from the bus's long parallel circuits. The emission frequency is loosely wraps around the frequency of the RAM's I/O bus clock with a marginal span of +/-200MHz. The casual use of a computer does not generate these radio waves at significant amplitude, since it requires a major buildup of voltage in the circuitry. Therefore, we have found that by generating a continuous stream of data over the multi-channel memory buses, it is possible to raise the amplitude of the emitted radio waves. Using this observation, we are able to modulate binary data over these carrier waves by deterministically starting and stopping multi-channel transfers using special CPU instructions.

Z-axis of MEMS gyroscopes

- 8 kHz acoustic tone hits resonant frequency of MEMS gyroscope
- Disturbs PID feedback control
- Drone falls from sky



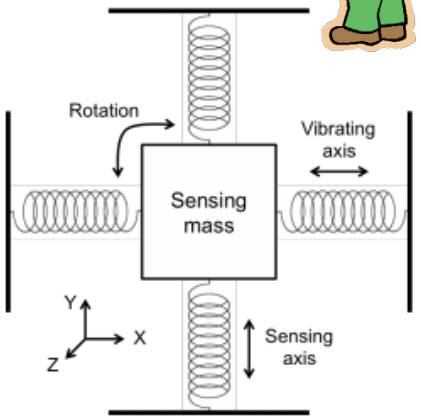


Figure 2: Concept of MEMS gyroscope structure for one axis

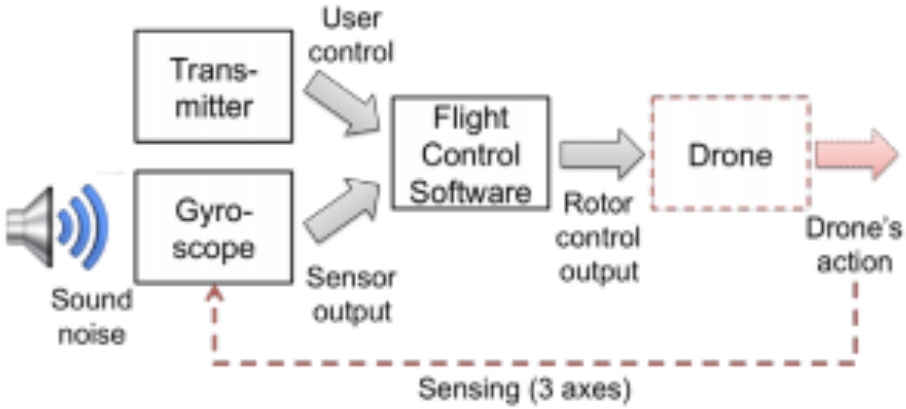


Figure 8: Propagation of the effect of sound noise

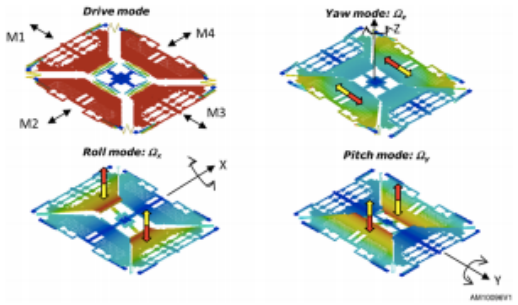
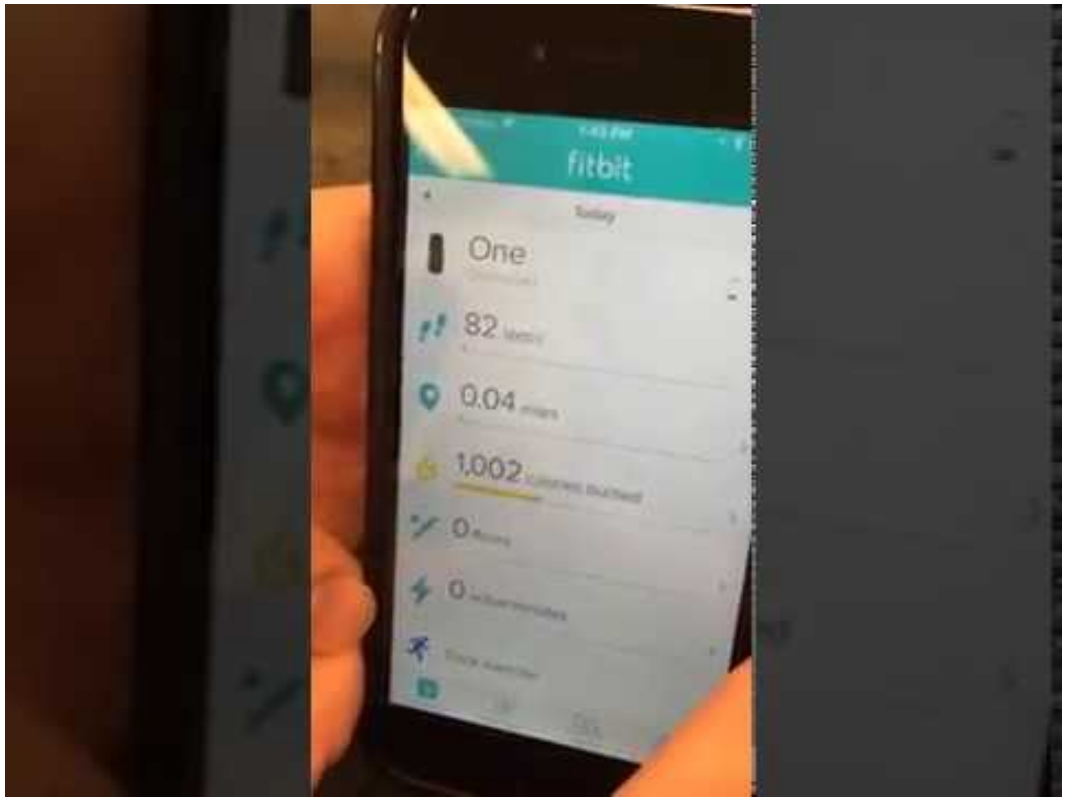


Figure 3: Operation of a three-axis MEMS gyroscope [10] (the X-, Y-, and Z-axes are defined as the pitch, roll, and yaw, respectively.)

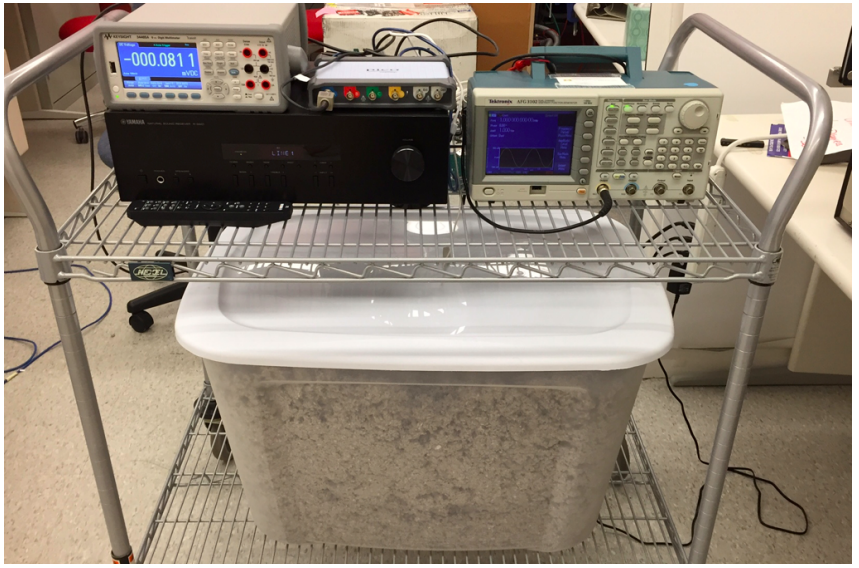
[Son et al., USENIX Security' 15]

Acoustic Attacks on MEMS Accelerometers

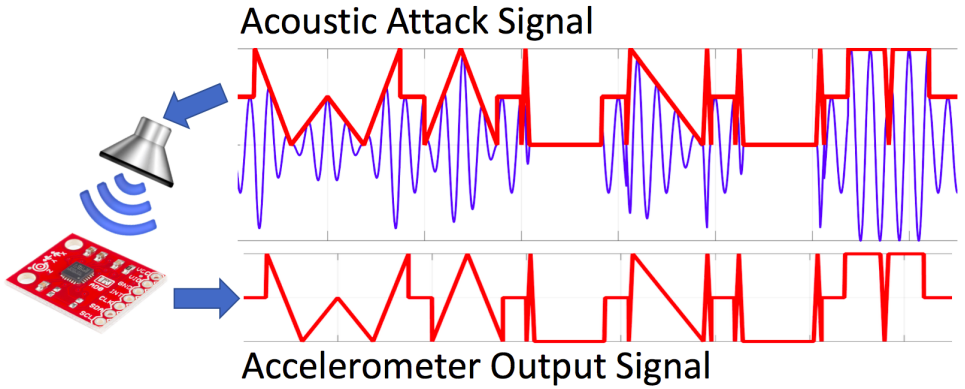
["WALNUT" by Trippel et al., IEEE Euro S&P 2017]



spqr.eecs.umich.edu/walnut



Unintentional Demodulation



vs.

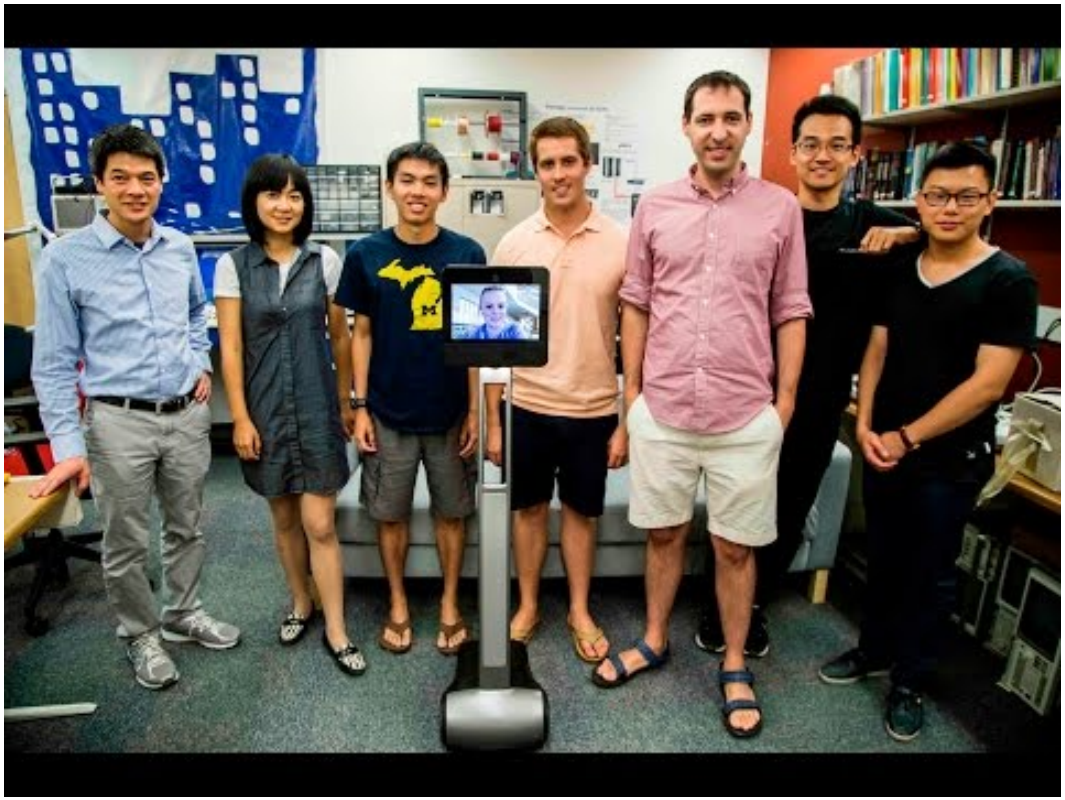
Both: Intentional signal modulation

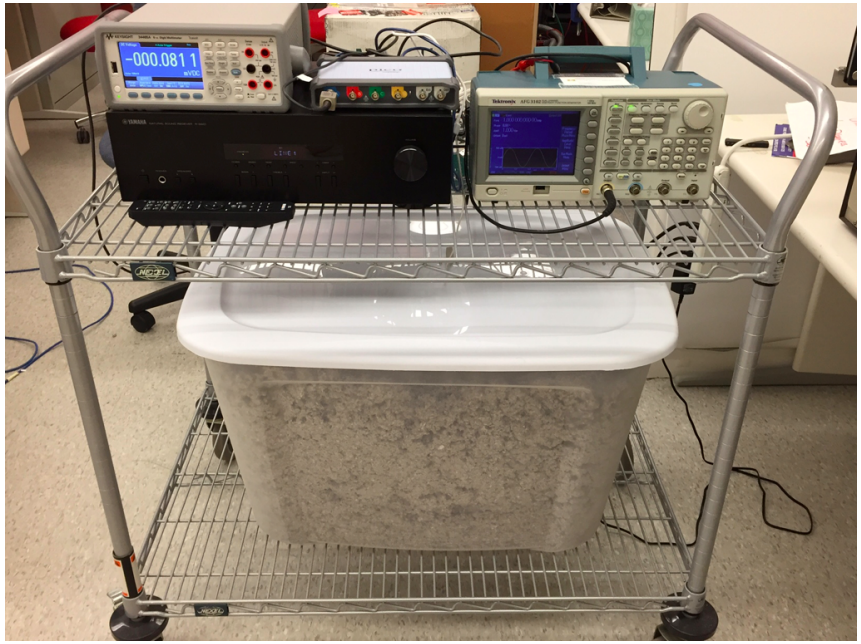
Intentional
signal demodulation

<u>Unintentional</u>
signal demodulation

Acoustic Rickroll

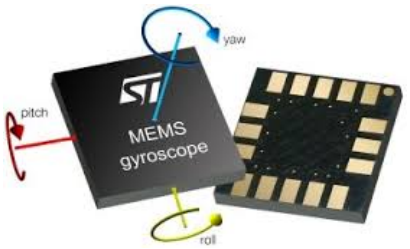
[spqr.eecs.umich.edu/walnut]

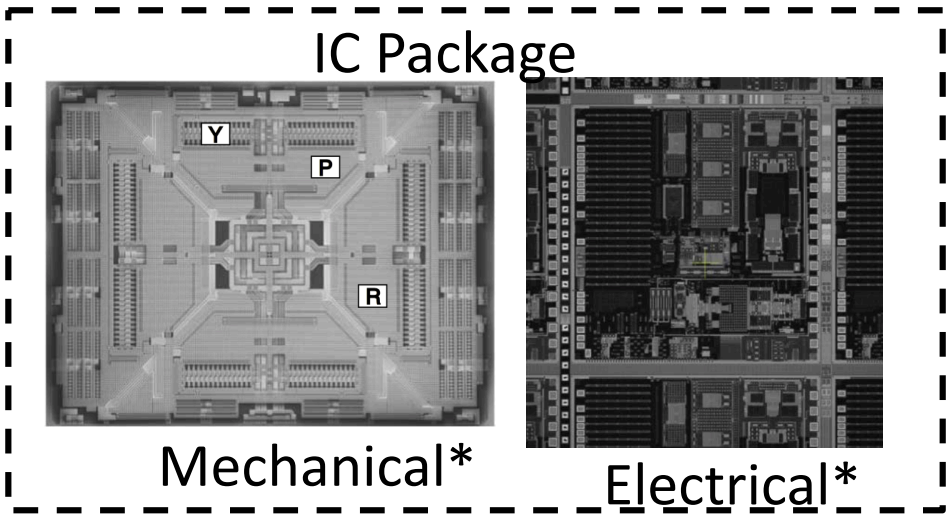




MEMS Sensors

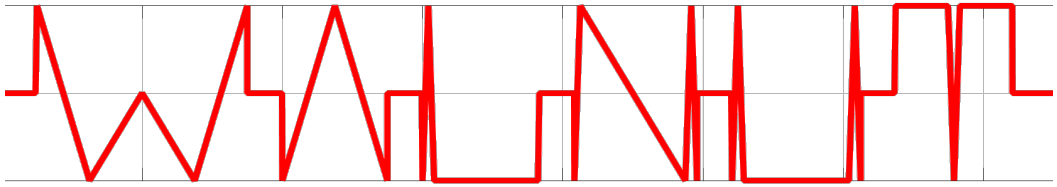
- **M**icro-**E**lectro-**M**echanical **S**ystems
  - Accelerometers
  - Gyroscopes
  - Clocks
- Advantages:
  - Low Cost – easy to manufacture
  - Low Power – some < 1 mA
  - Small Size – integrated circuit





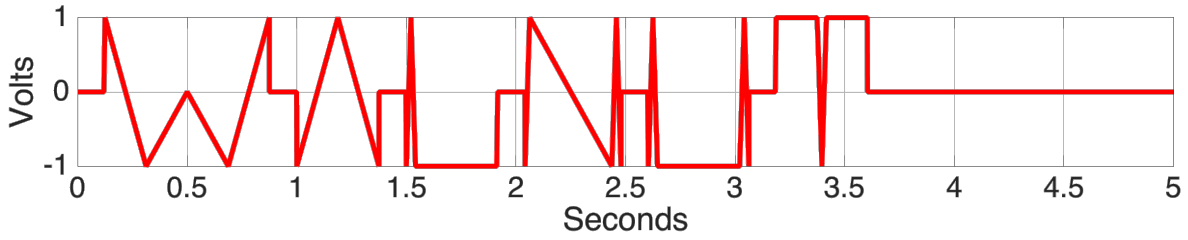
*Photos courtesy of "*Everything about STMicroelectronics' 3-axis digital MEMS gyroscopes – Technical Report*", by STMicroelectronics.

Controlling Output



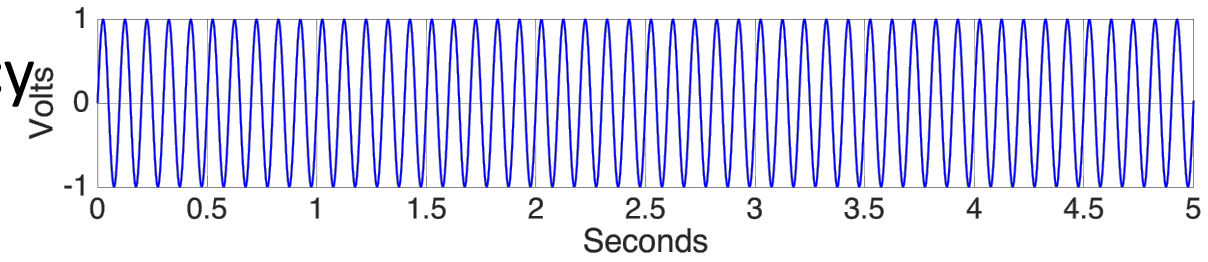
Output Control Modulation

Desired Accelerometer Output Signal



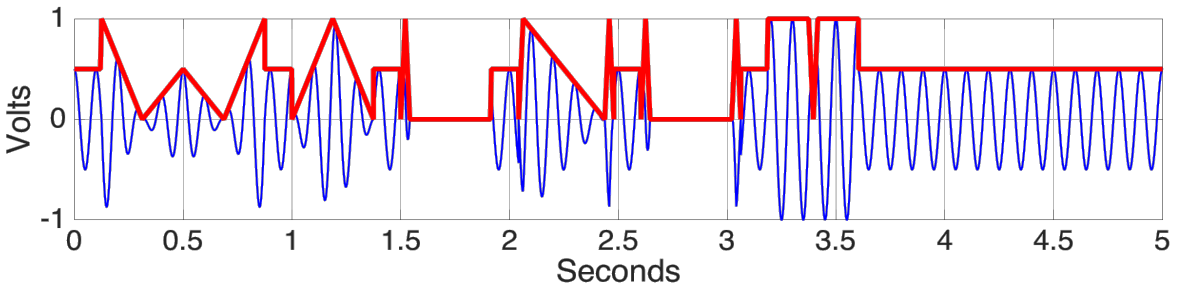
+

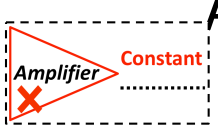
MEMS Resonant Frequency (Carrier Signal)

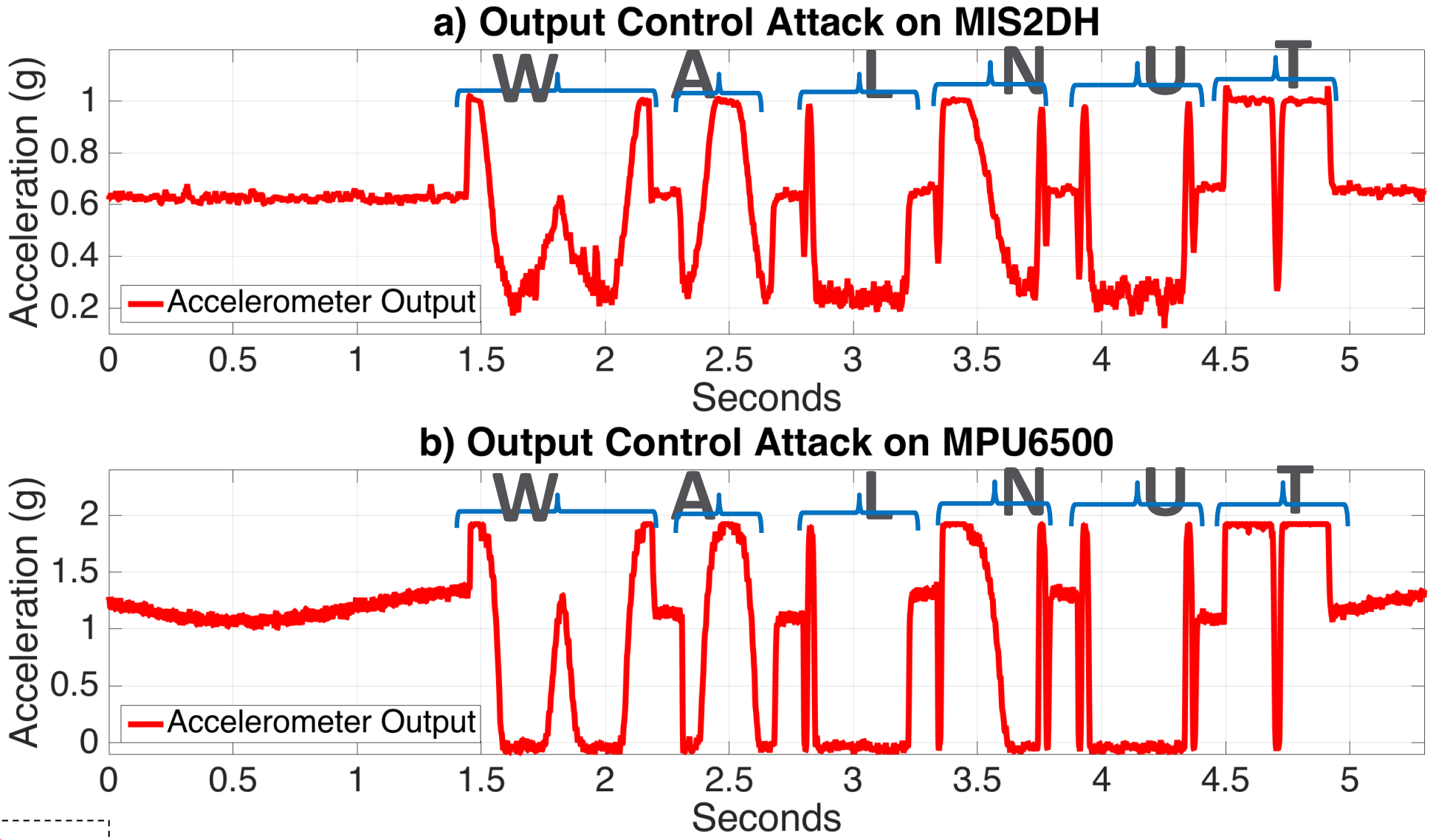


=

Modulated Acoustic Attack Signal






a) Output Control Attack on MIS2DH
W A L N U T
Acceleration (g)
1
0.8
0.6
0.4
0.2
Accelerometer Output
0 0.5 1 1.5 2 2.5 3 3.5 4 4.5 5
Seconds
b) Output Control Attack on MPU6500
W A L N U T
Acceleration (g)
2
1.5
1
0.5
0
Accelerometer Output
0 0.5 1 1.5 2 2.5 3 3.5 4 4.5 5
Seconds


Amplifier
Constant

Randomized Sampling

- Destroy predictability of sampling regime
- Randomize delay at each sampling interval