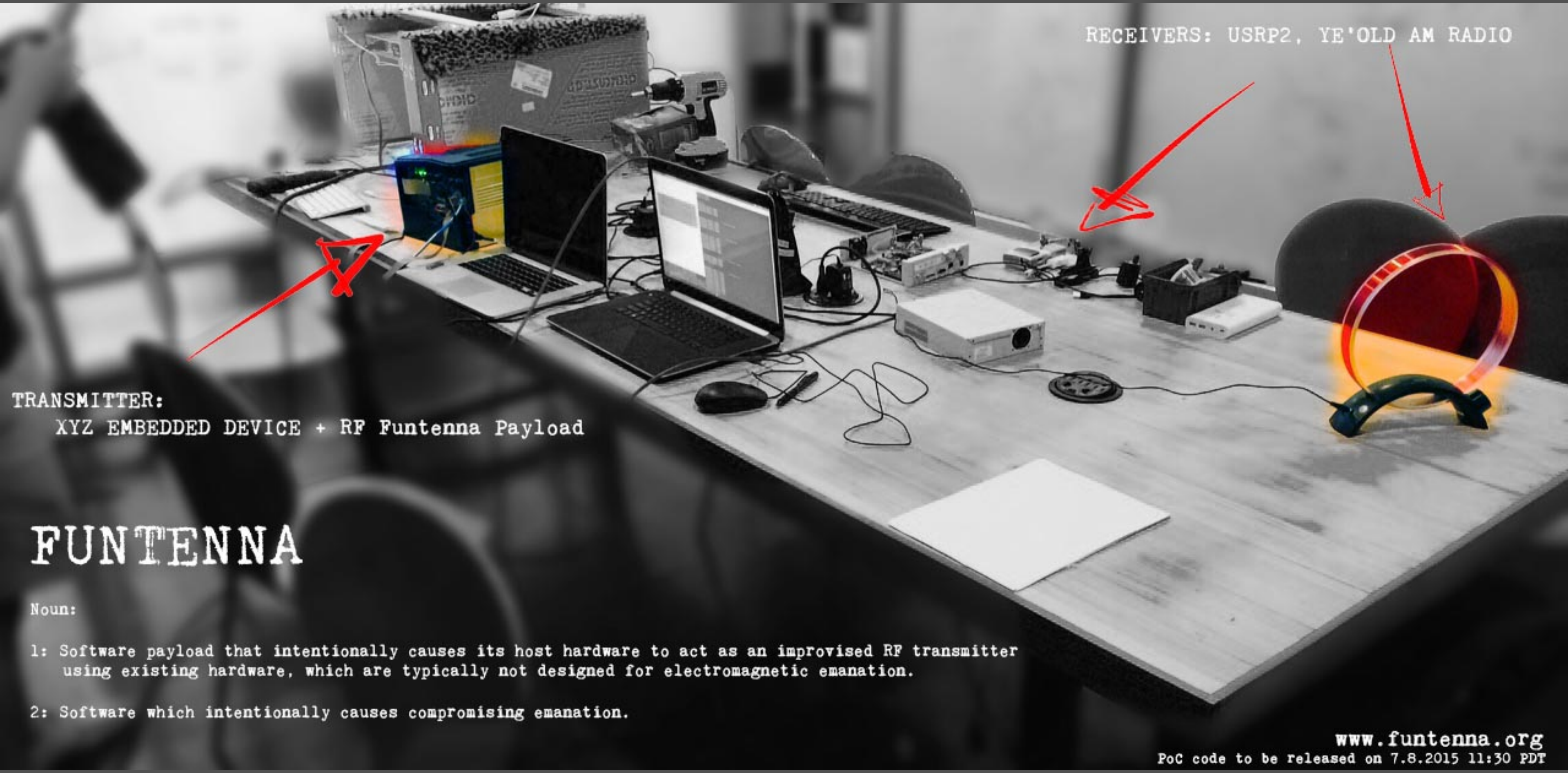
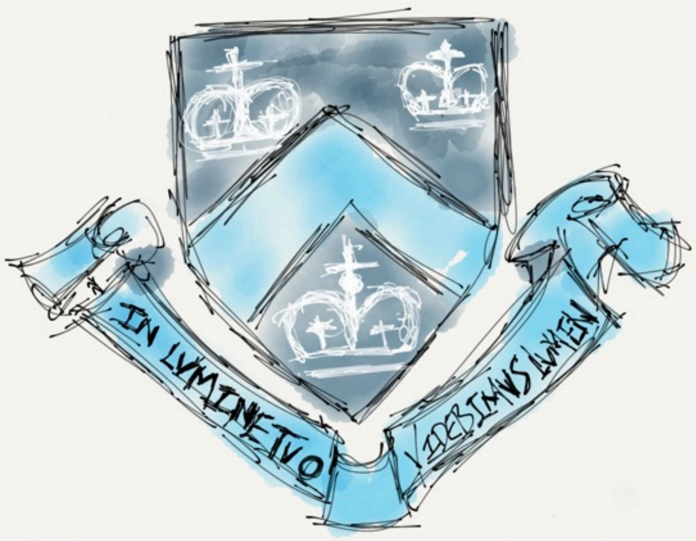


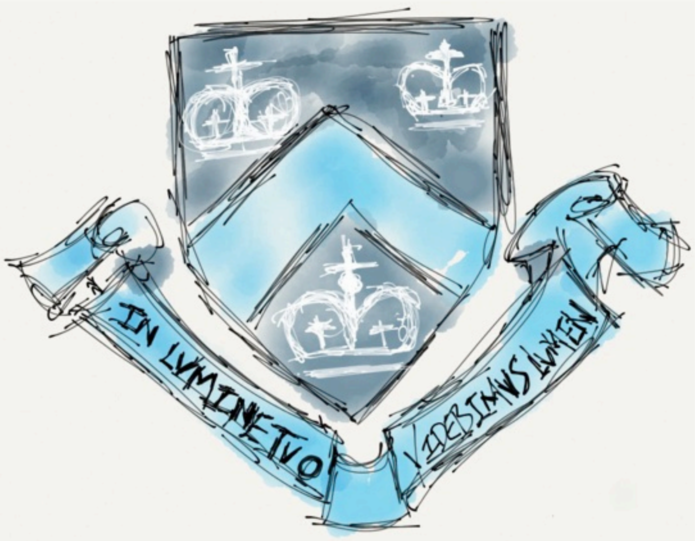
Ang Cui, PhD
a@redballoonsecurity.com

About me,

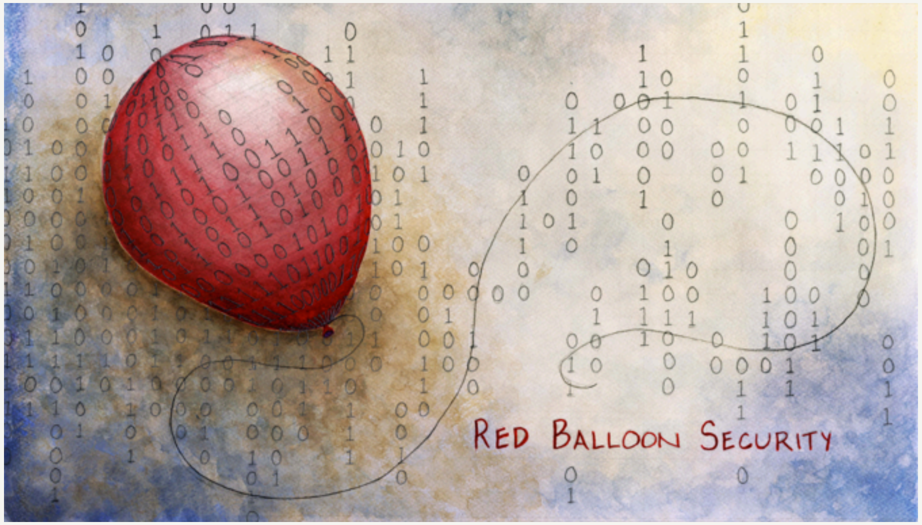


Columbia University

About me,



Columbia University



Red Balloon Security

Disclaimer

1. Research presented in this talk not funded by any government sources or Columbia University.

Disclaimer

1. Research presented in this talk not funded by any government sources or Columbia University.
2. Research presented not related to Red Balloon Security.

Disclaimer

1. Research presented in this talk not funded by any government sources or Columbia University.
2. Research presented not related to Red Balloon Security.
3. I only pretend to know how electricity works.

Boss Hardware :)

You are doing **real science** when you are using…

Boss Hardware !!

You are doing **real science** when you are using…

You purchased this item on July 16, 2013.
View this order

Roll over image to zoom in

Geo-Phone Paranormal Research Tool

by Gen-El

11 customer reviews

List Price: ~~$59.95~~
Price: $49.49 + $5.50 shipping
You Save: $10.46 (17%)

Note: Not eligible for Amazon Prime.

In Stock.

Ships from and sold by General Electromagnetics.

Estimated Delivery Date: Aug. 6 - 11 when you choose Standard at checkout.

- Ultrasensitive vibration detector

Boss Hardware !!

You are doing real science when you are using…

Customer Questions & Answers

Have a question? Ask the owners here | Ask

Don't see what you're looking for? Submit your question to our community by clicking the 'Ask' button above.

0 votes

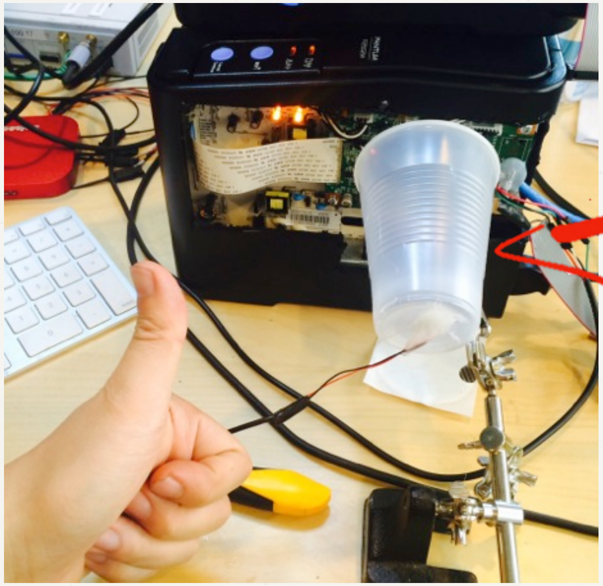
Geo pone converts noise into voices? have I got that right, and these voices are they Alive humans like your neighbors that you hear?

A: It hears through vibrations, you have to set it down on something and then hook either a recorder or headphones to it to hear anything. I thought it was something else when I bought it. I didn't want to have to hook something up to it to hear sounds. as for voices, I only tried it once and I think it picked up everything.

Sandra Labella answered on April 17, 2014

Boss Hardware !!

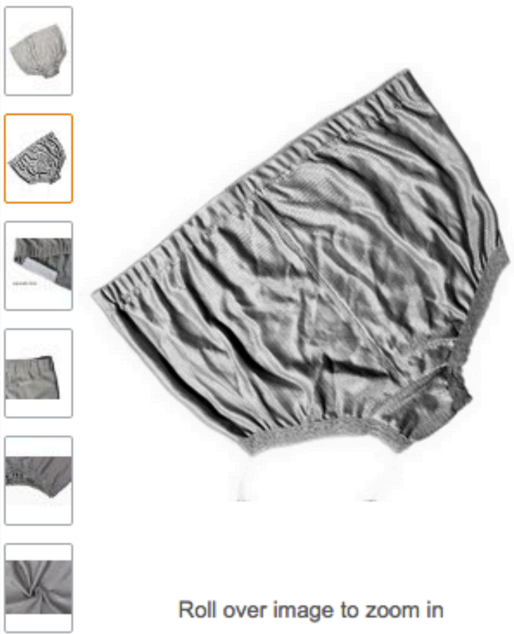
You are doing real science when you are using…



Homemade dog whistle detector
(in a cup)

Boss Hardware

You are doing **real science** when you are using…



Roll over image to zoom in

Anti-Radiation Shield Women Maternity Briefs Panties Protection Medium 8900651M

Be the first to review this item

List Price: ~~$99.98~~
Price: $75.98 ✓Prime & Free Returns. Details
You Save: $24.00 (24%)

Only 1 left in stock.

Sold by OurSure and Fulfilled by Amazon. Gift-wrap available.

Want it Tuesday, Aug. 4? Order within **28 hrs 58 mins** and choose **One-Day Shipping** at checkout. Details

- 100% Silver-Nylon Blend
- 100% silver blend fabric provides super RF radiation shield effeciveess up to 60 dBin the frequency range from 10 MHz to 3 GHz and beyond,let you take advantage to prevent your baby from RF radiation
- Silky feel, light stretch, comfort woman briefs offer full front and back coverage following the natural leg curve
- Breathable and comfortable

Funtenna!

Noun:

Funtenna!

Noun:

1: Malware that intentionally causes compromising emanation.

Funtenna!

Noun:

1: Malware that intentionally causes compromising emanation.

2: Software payload that intentionally causes its host hardware to act as an improvised RF transmitter using existing hardware, which are typically not designed for electromagnetic emanation.

xyz
Thing

xyz

Thing

Laptop

xyz ← Thing

Laptop, Server,

xyz
Thing

Laptop, Server, phone,

xyz
Thing

Laptop, Server, phone,
router

xyz
Thing

Laptop, Server, phone,
router, printer,

xyz Thing

Laptop, Server, phone, router, printer, TV, car, building etc

xyz Thing

\+ Funtenna payload

xyz Thing

+

Funtenna payload

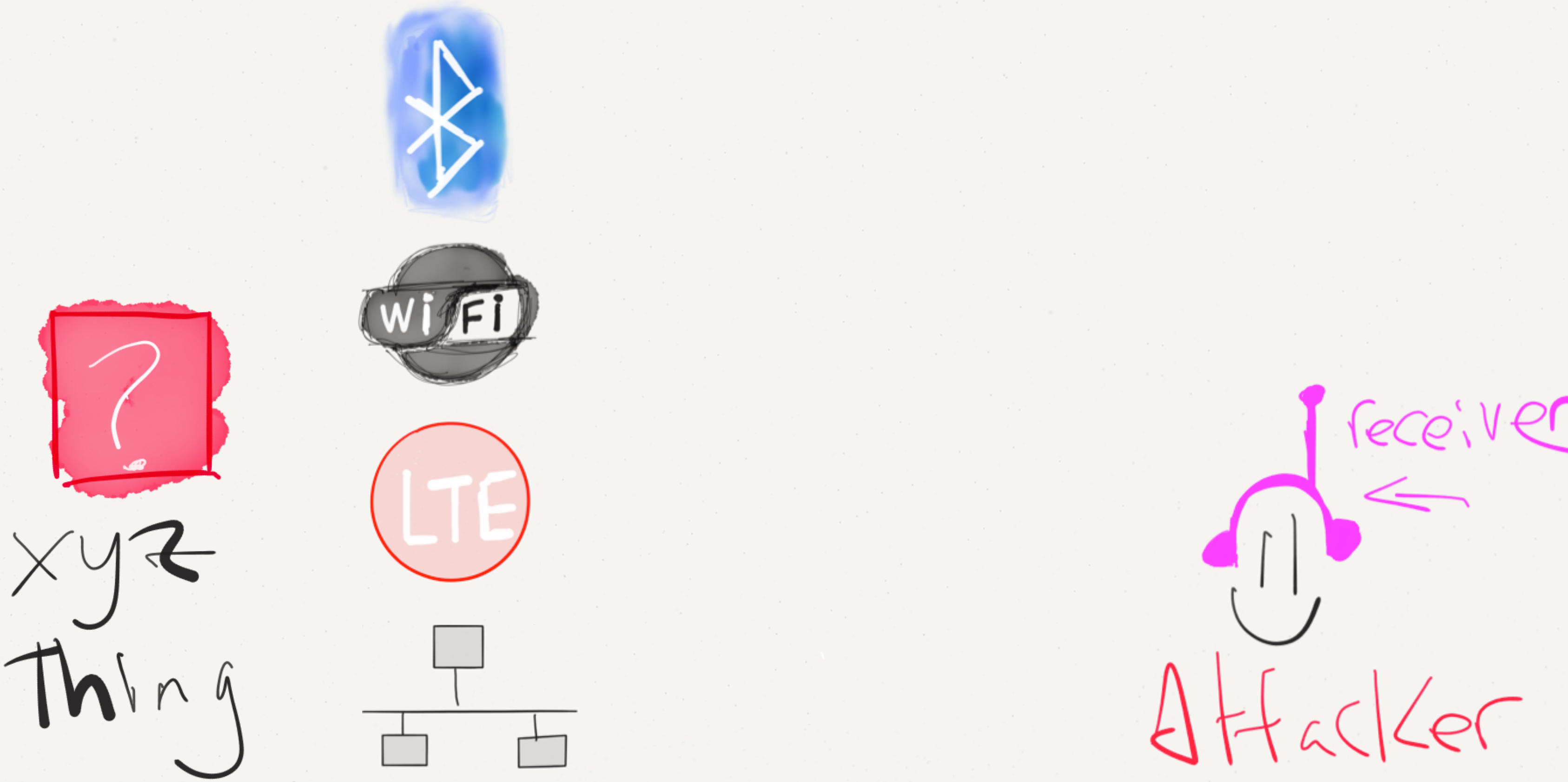
(tiny malware)

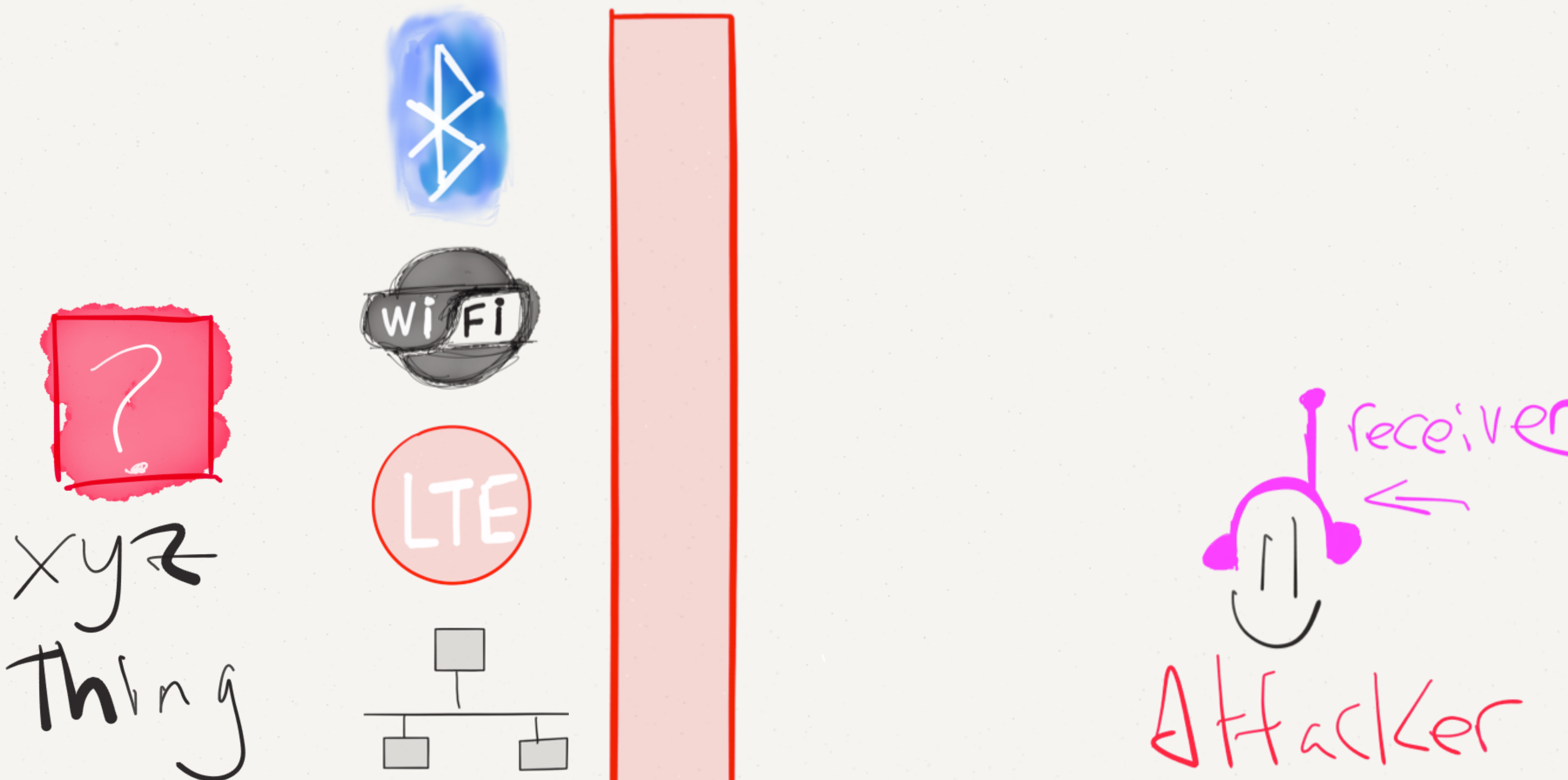

?
xyz
Thing


xyz
Thing
Attacker

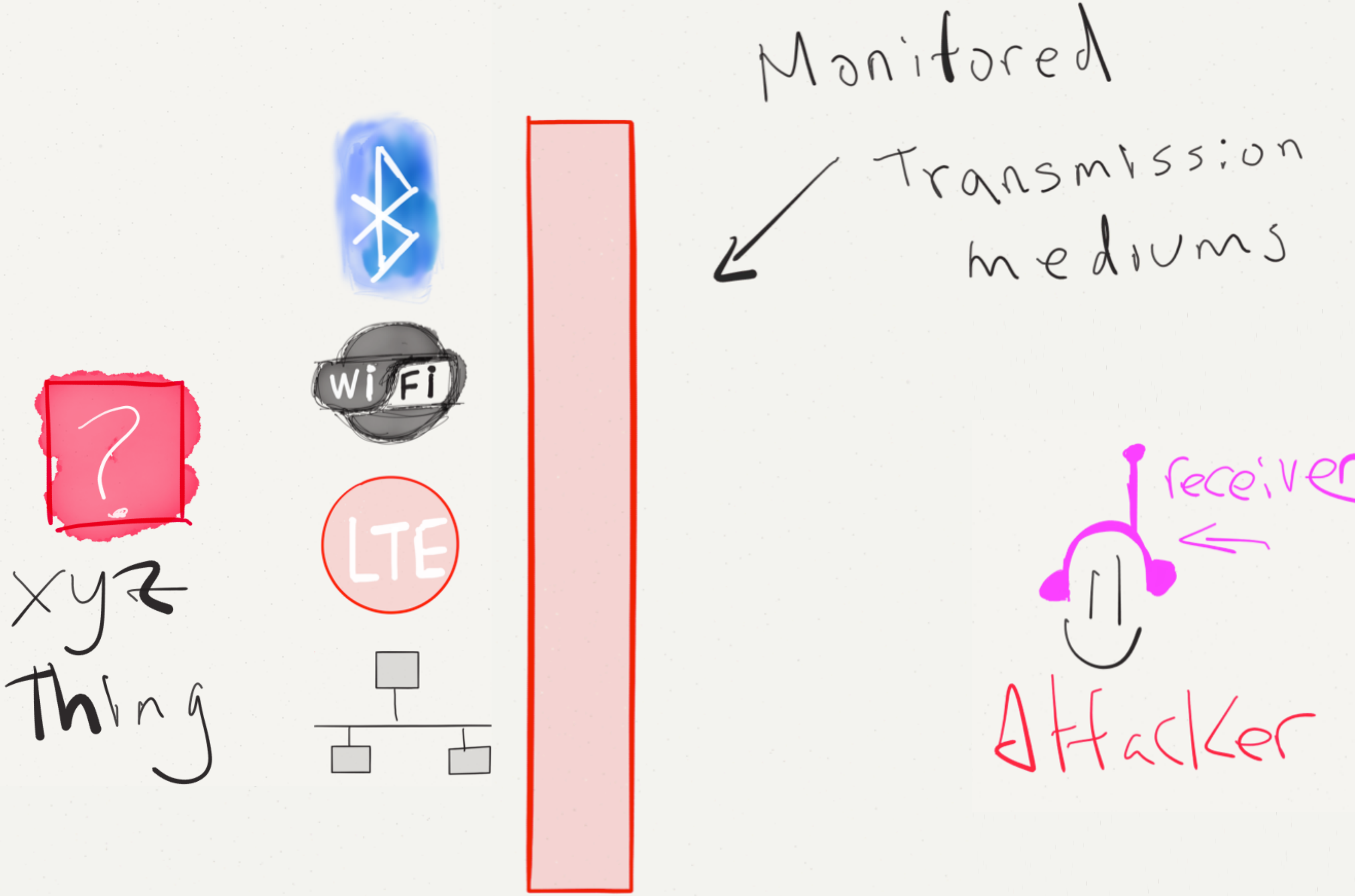

?
xyz
Thing
all your
secret info
Attacker

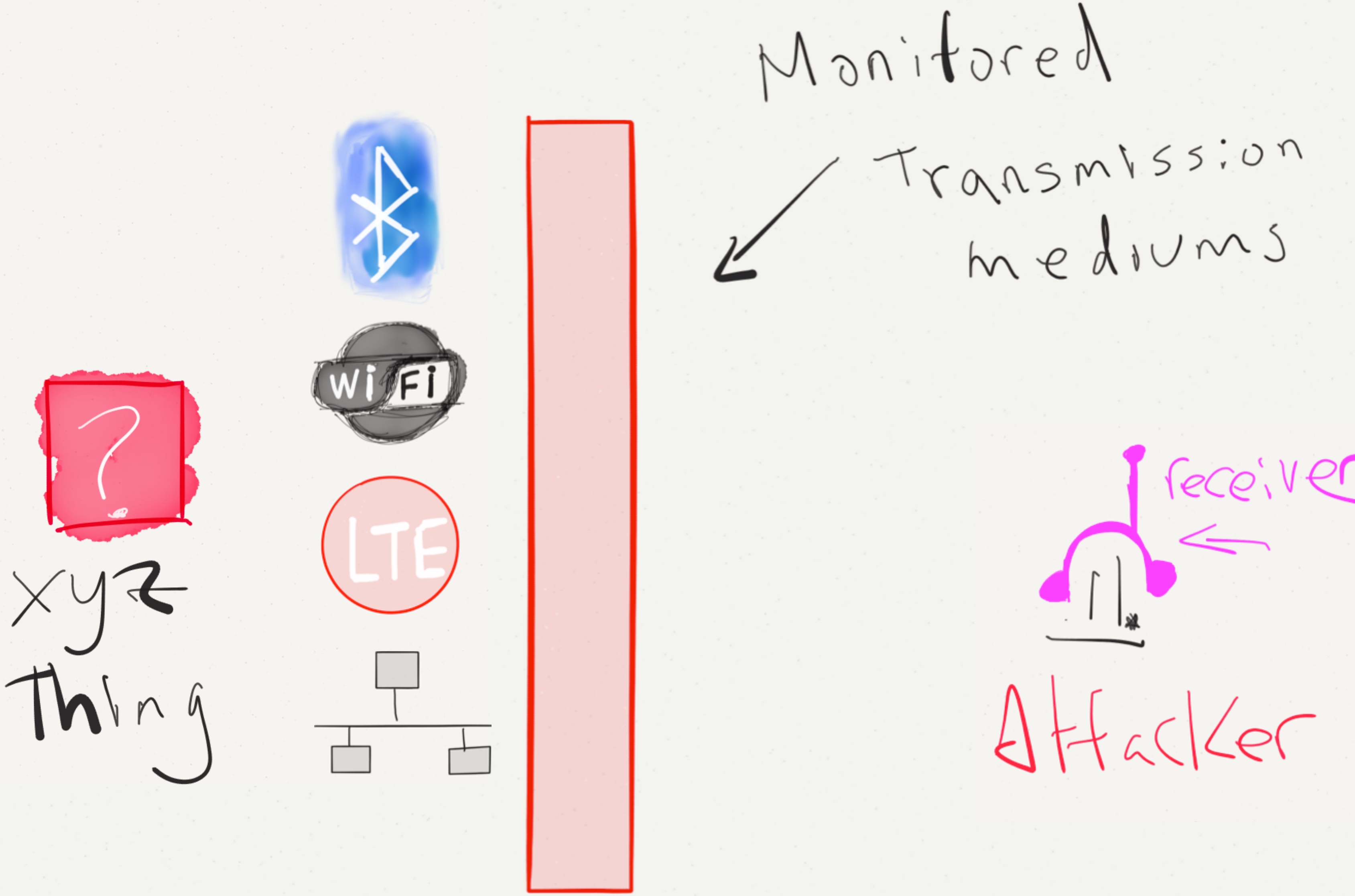

xyz
Thing
receiver
Attacker


xyz
Thing
Wi Fi
LTE
receiver
Attacker



xyz
Thing
Wi Fi
LTE
receiver
Attacker


Monitored
Transmission mediums
Wi Fi
LTE
xyz Thing
receiver
Attacker



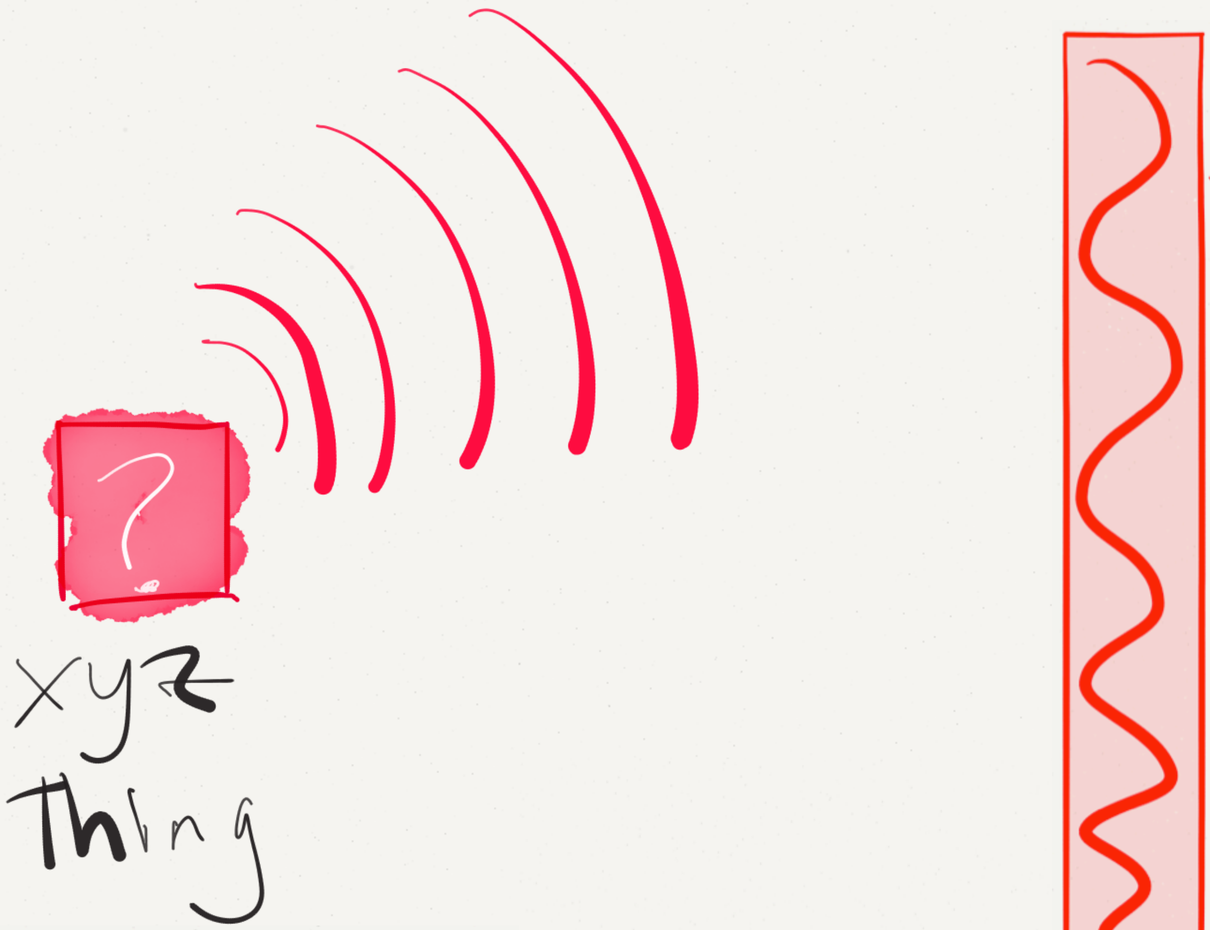
Monitored
Transmission mediums
xyz Thing
WiFi
LTE
receiver
Attacker

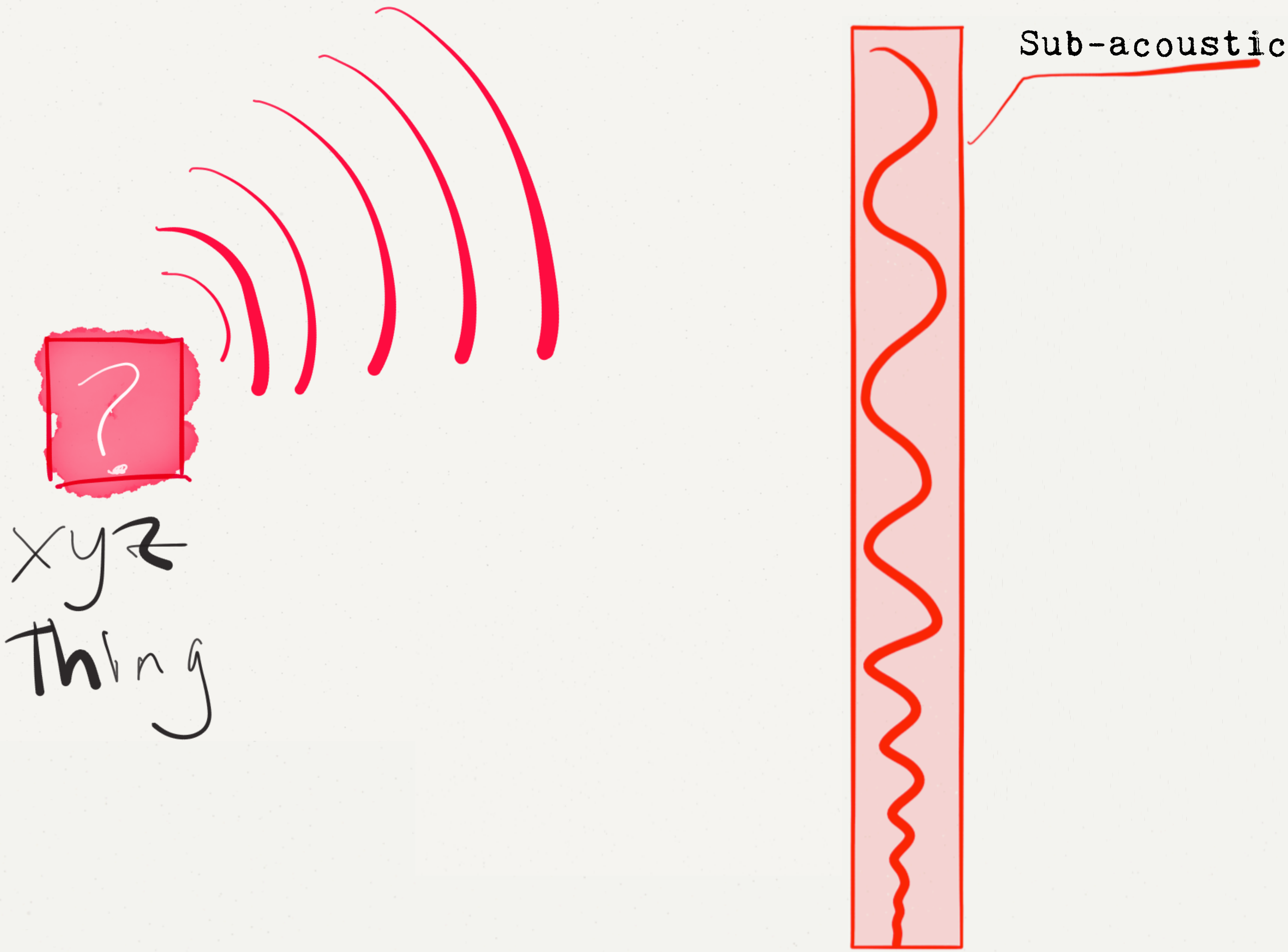

xyz
Thing
Wi Fi
receiver
Attacker

Transmission medium of the attacker's choosing

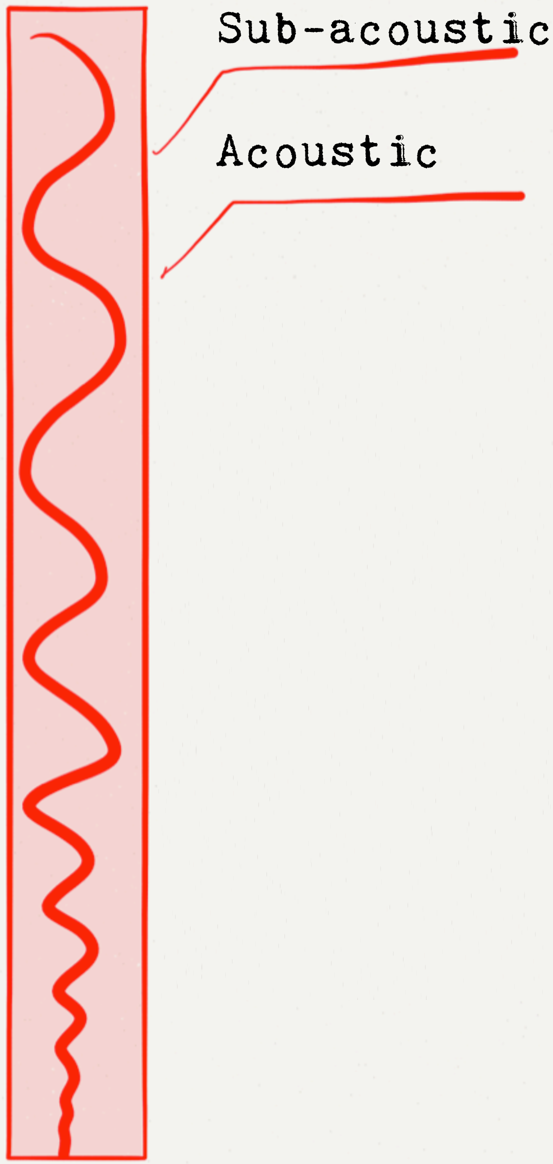
Transmission medium of the attacker's choosing

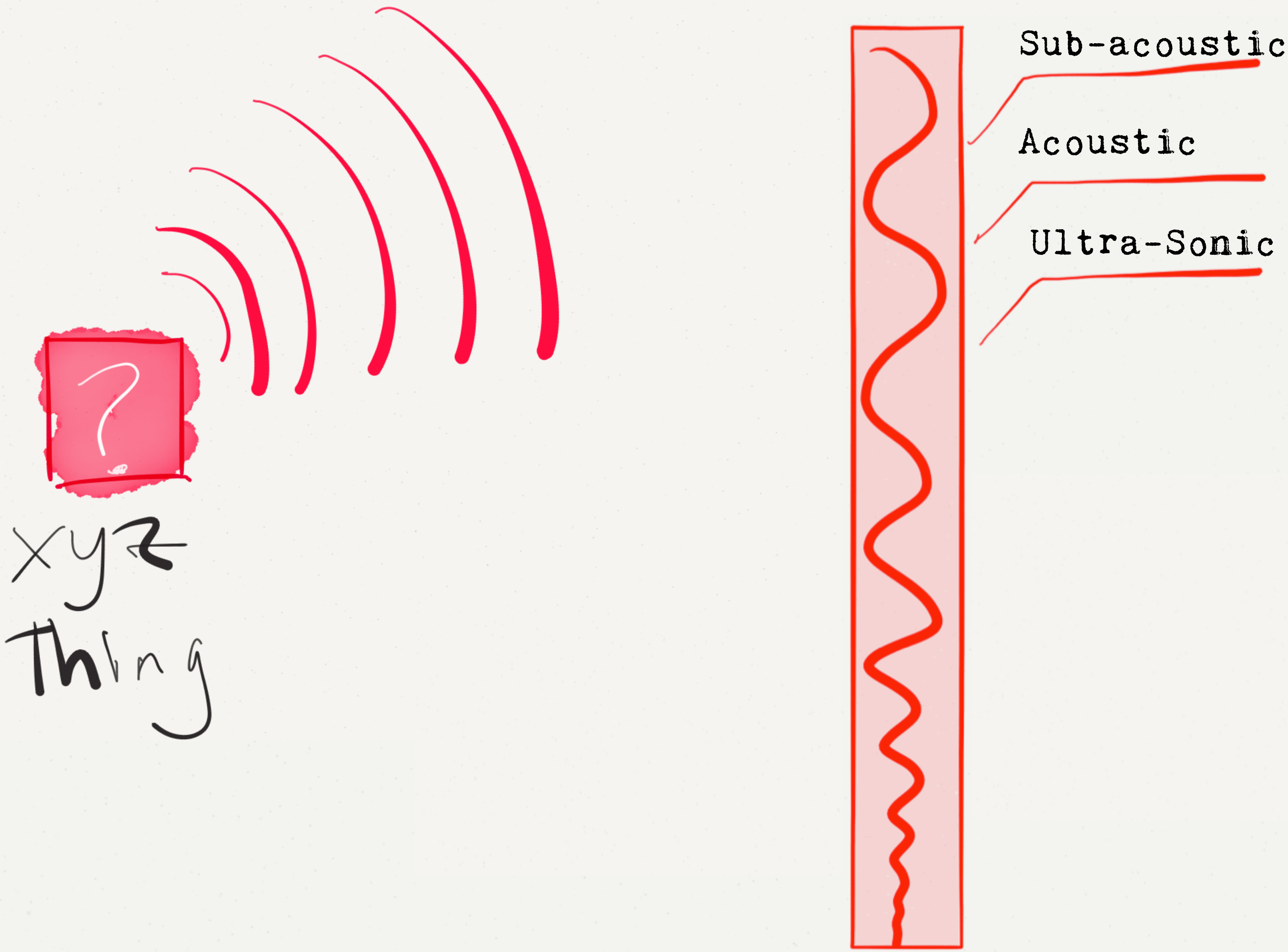
Where you don't monitor

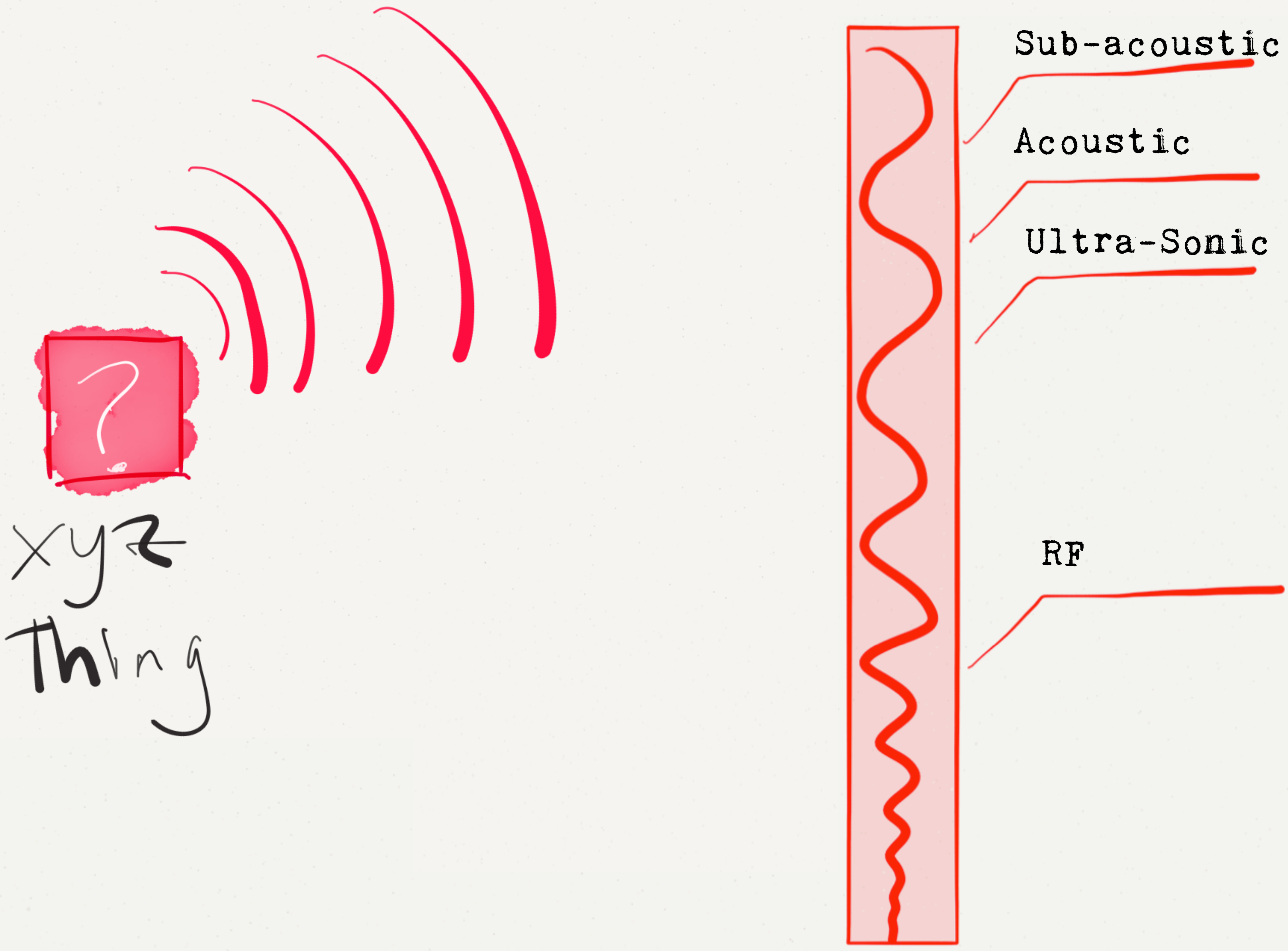

?
xyz
Thing

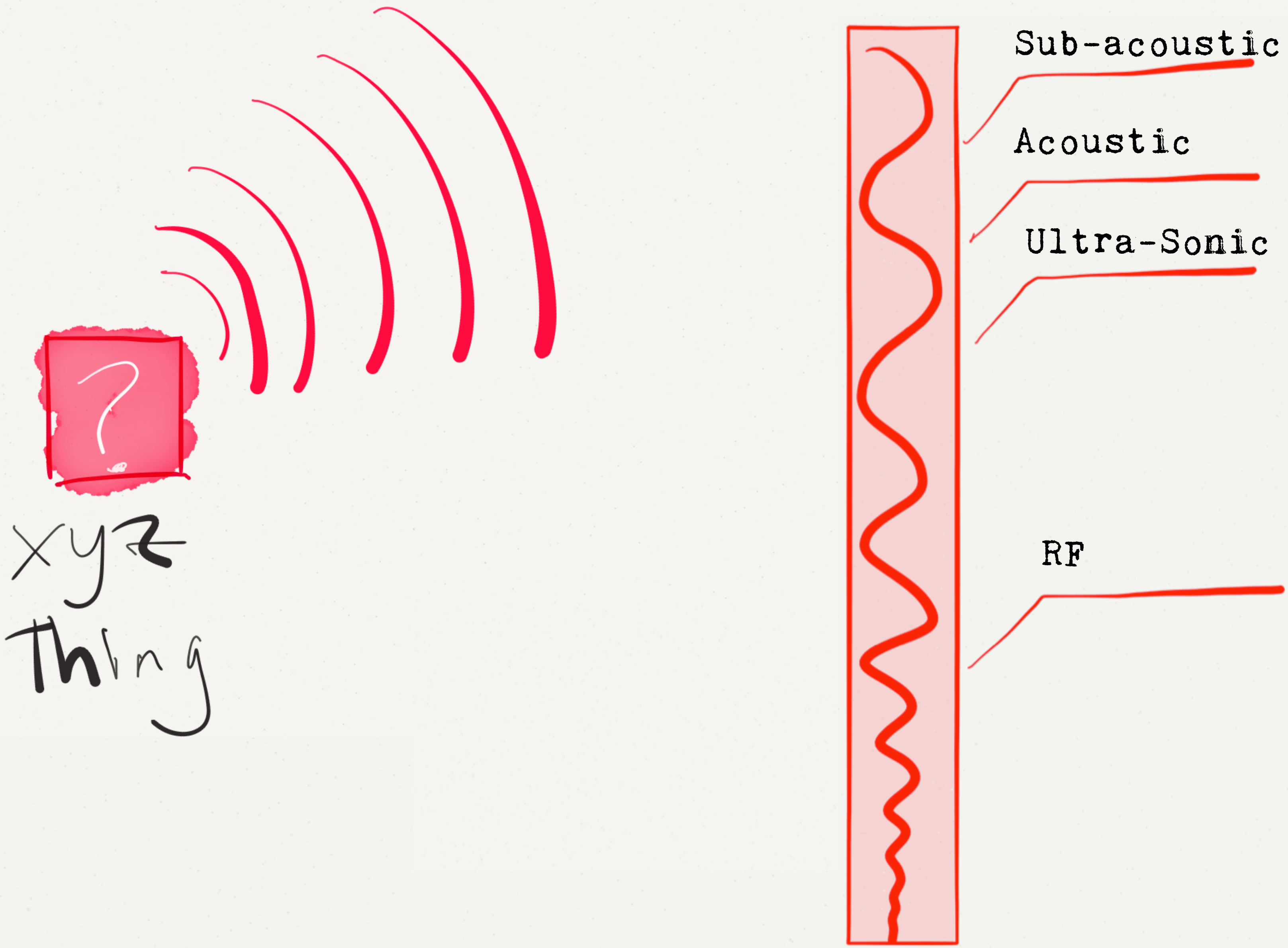

?
xyz
Thing
Sub-acoustic


xyz
Thing


Sub-acoustic
Acoustic

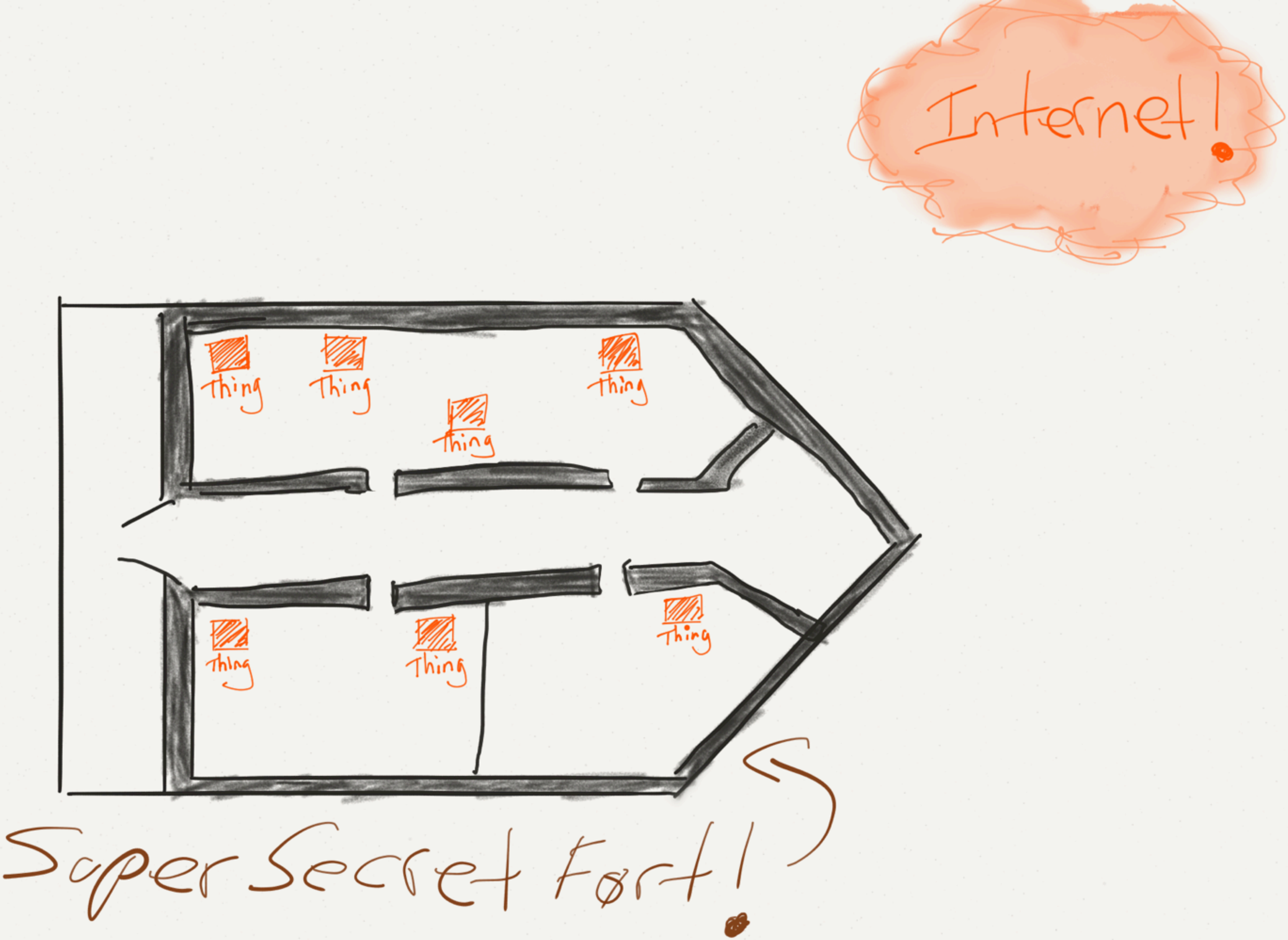

xyz
Thing
Sub-acoustic
Acoustic
Ultra-Sonic


xyz
Thing
Sub-acoustic
Acoustic
Ultra-Sonic
RF

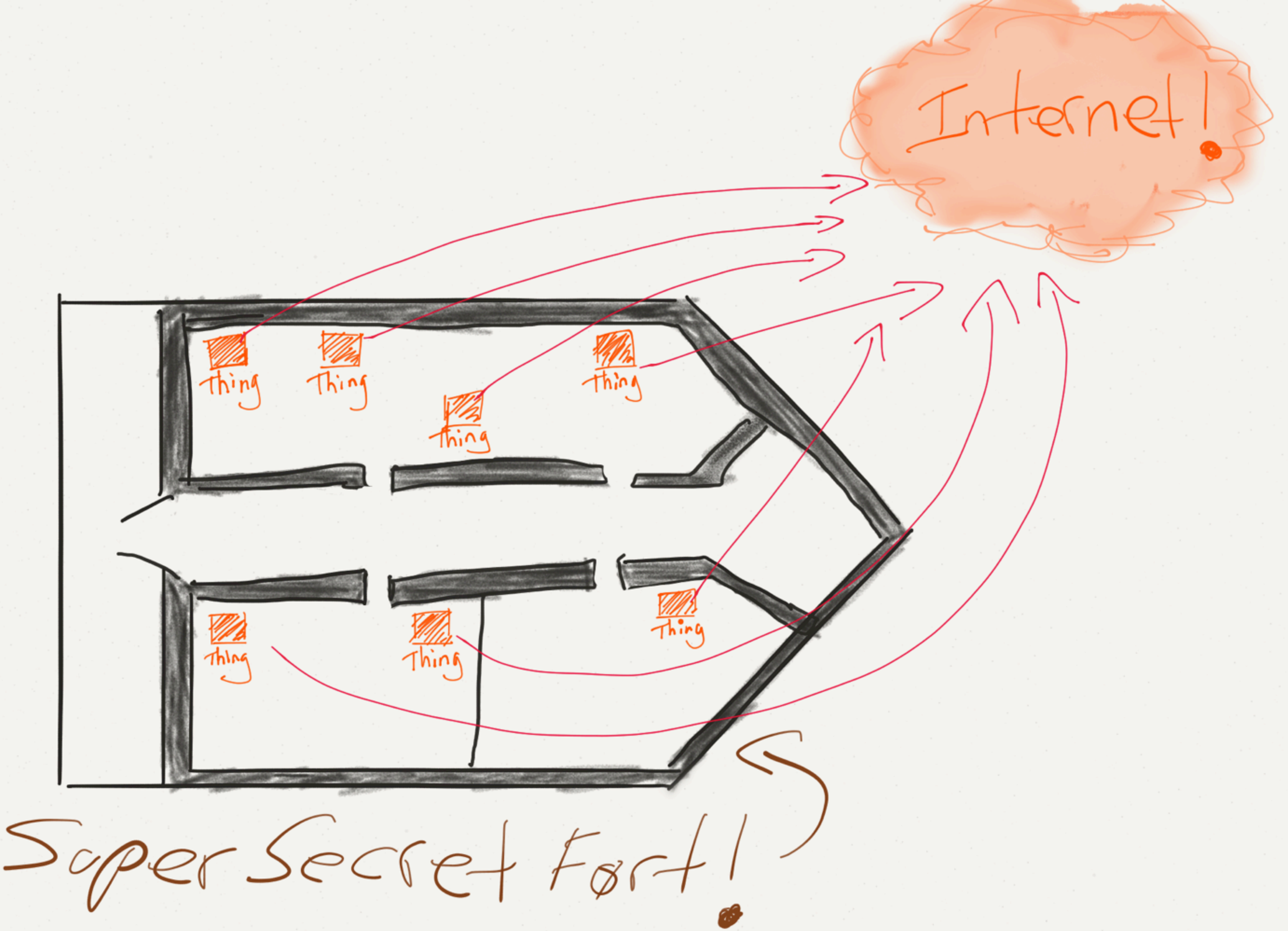

xyz
Thing
Sub-acoustic
Acoustic
Ultra-Sonic
RF

why?

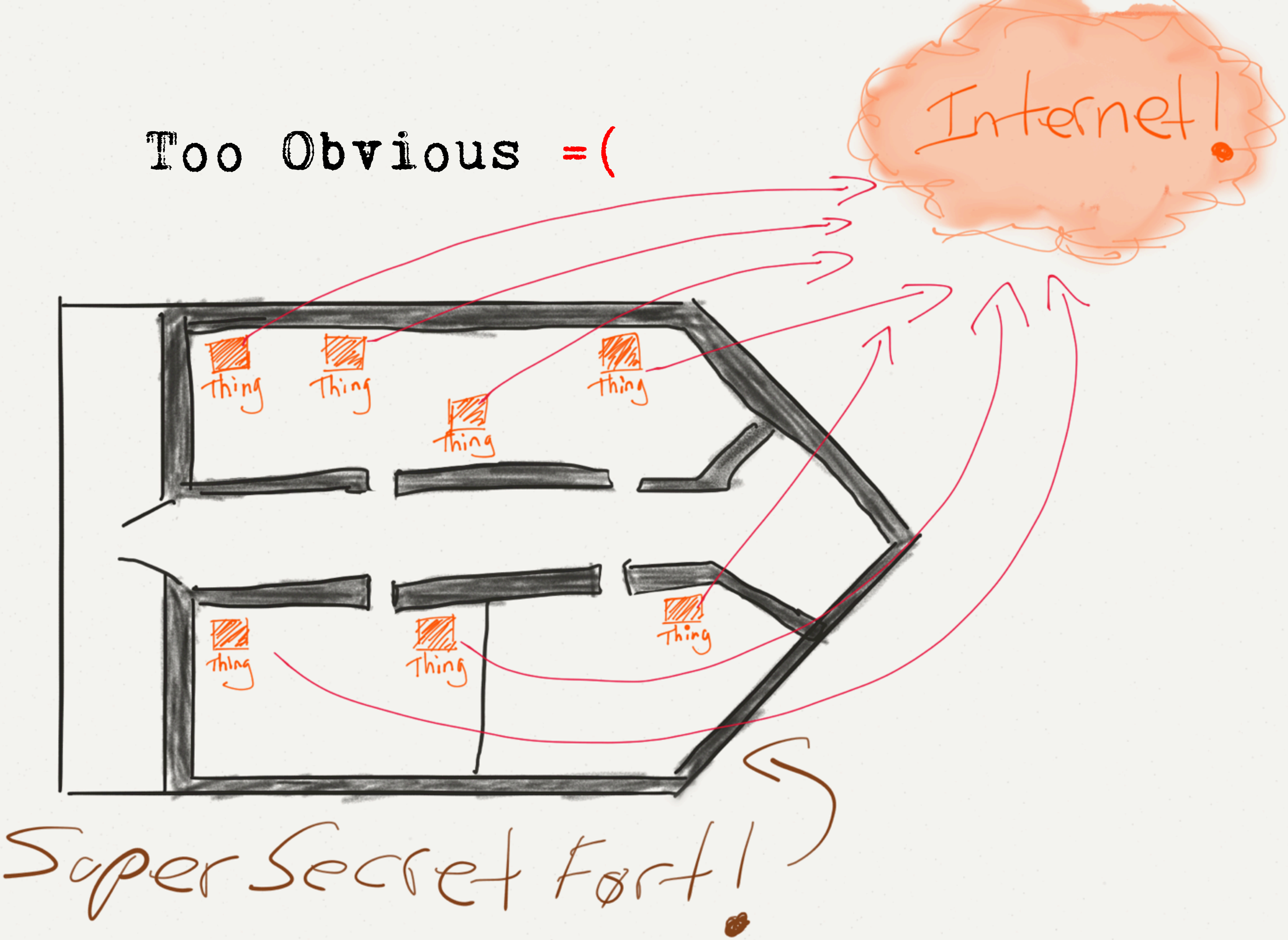

Super Secret Fort!

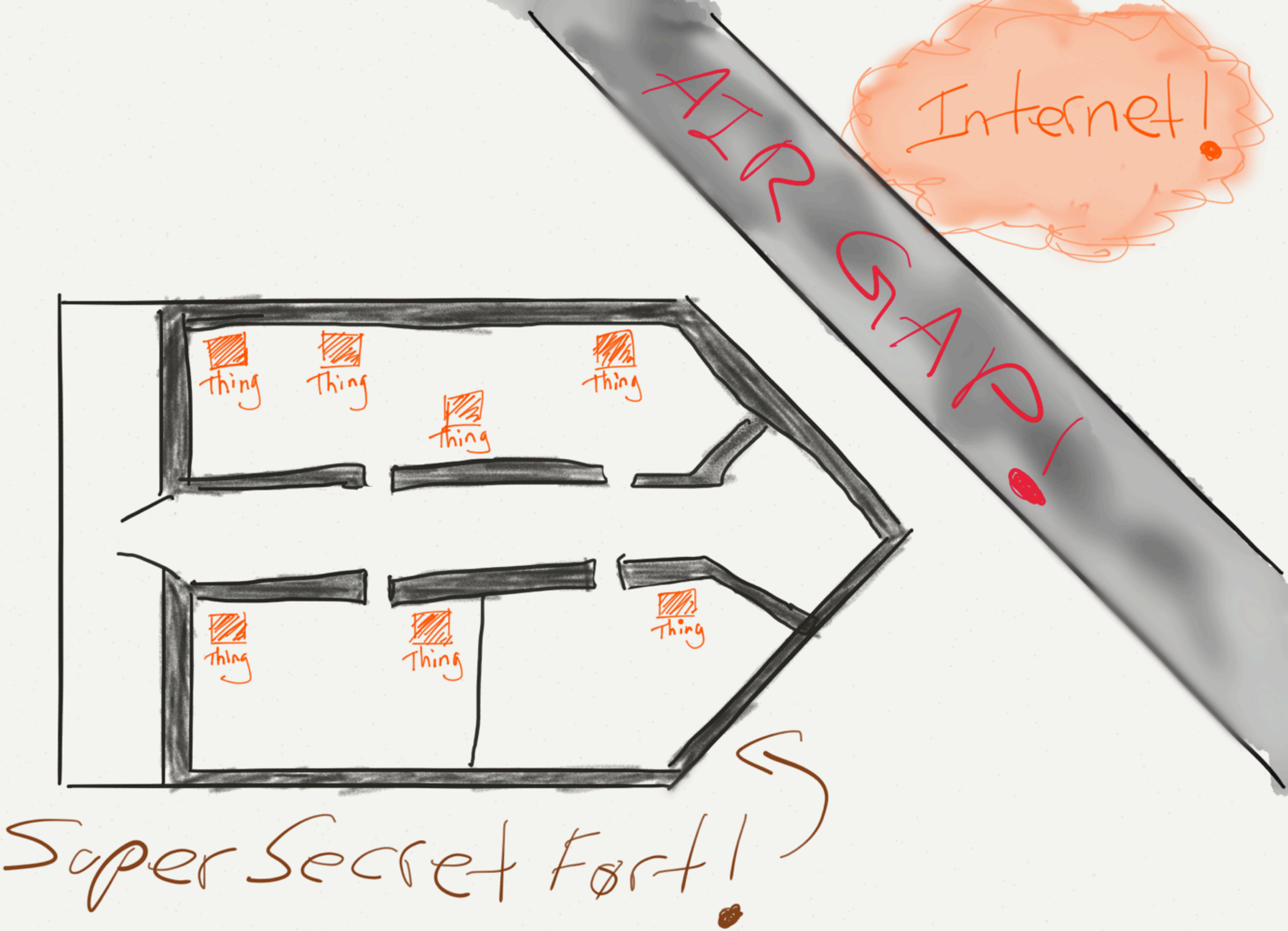


Internet!
Thing
Thing
Thing
Thing
Thing
Thing
Thing
Super Secret Fort!


Internet!
Thing
Thing
Thing
Thing
Thing
Thing
Thing
Super Secret Fort!

Too Obvious =(


Internet!
Thing
Thing
Thing
Thing
Thing
Thing
Thing
Super Secret Fort!


Internet!
AIR GAP!
Thing
Thing
Thing
Thing
Thing
Thing
Thing
Super Secret Fort!

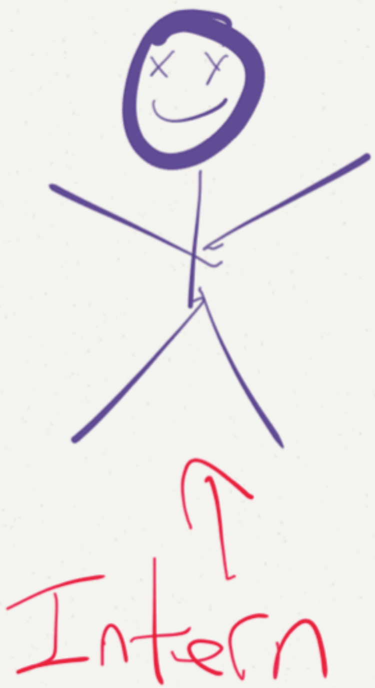
Anti Super Secret Fort Technology

Anti Super Secret Fort Technology

Amazing Ninja Tech

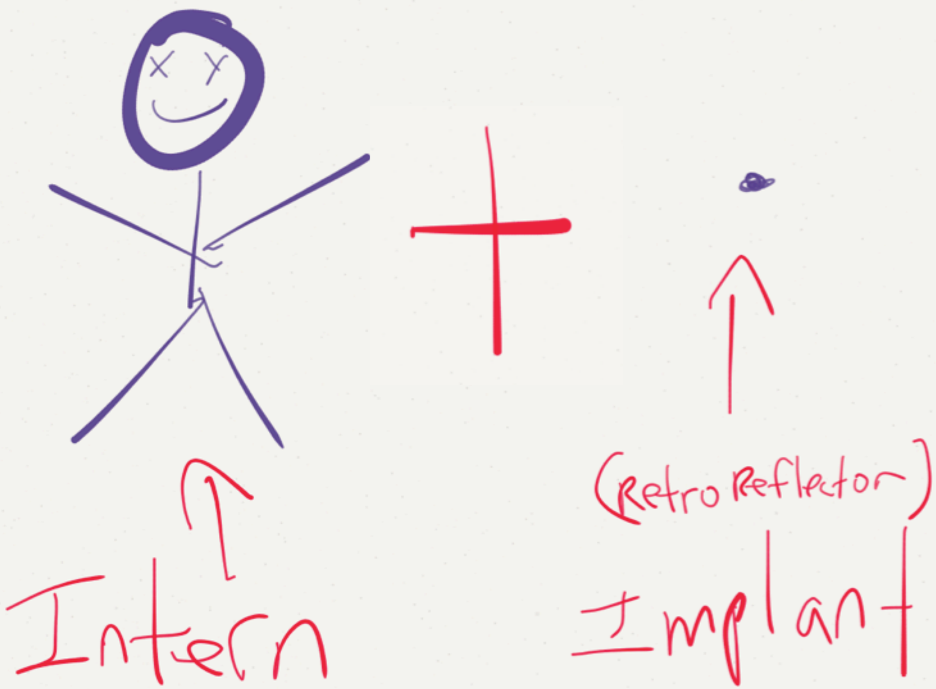
Anti Super Secret Fort Technology

Amazing Ninja Tech



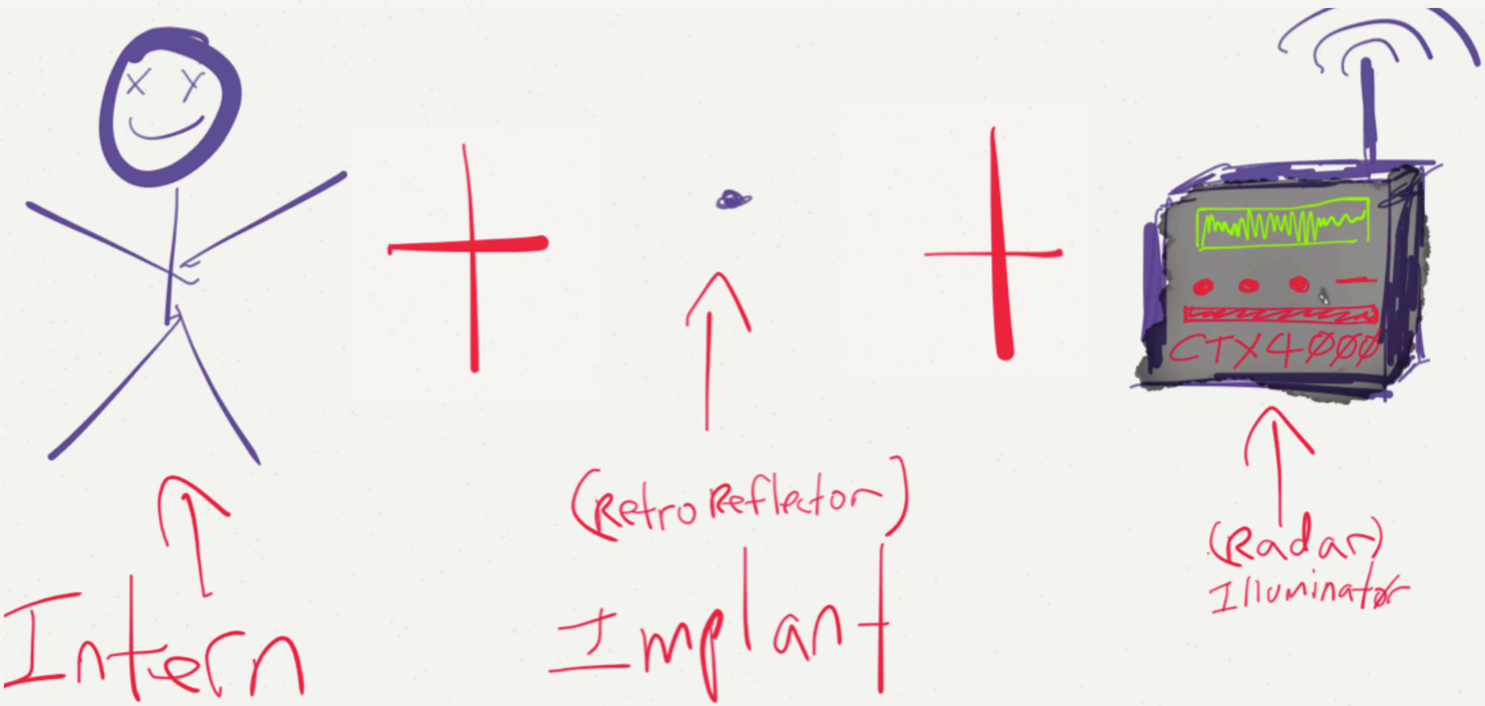
Anti Super Secret Fort Technology

Amazing Ninja Tech

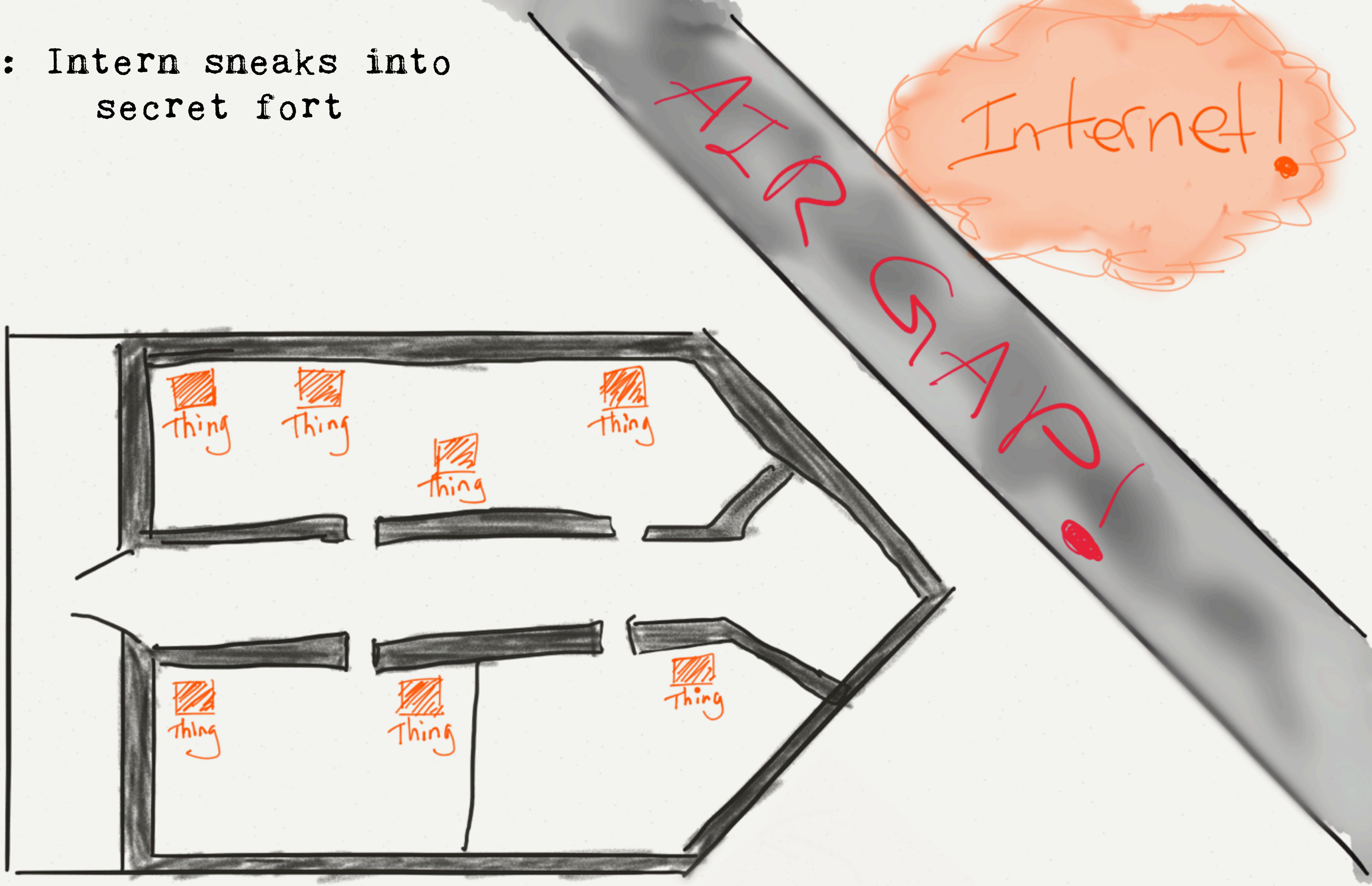


Anti Super Secret Fort Technology

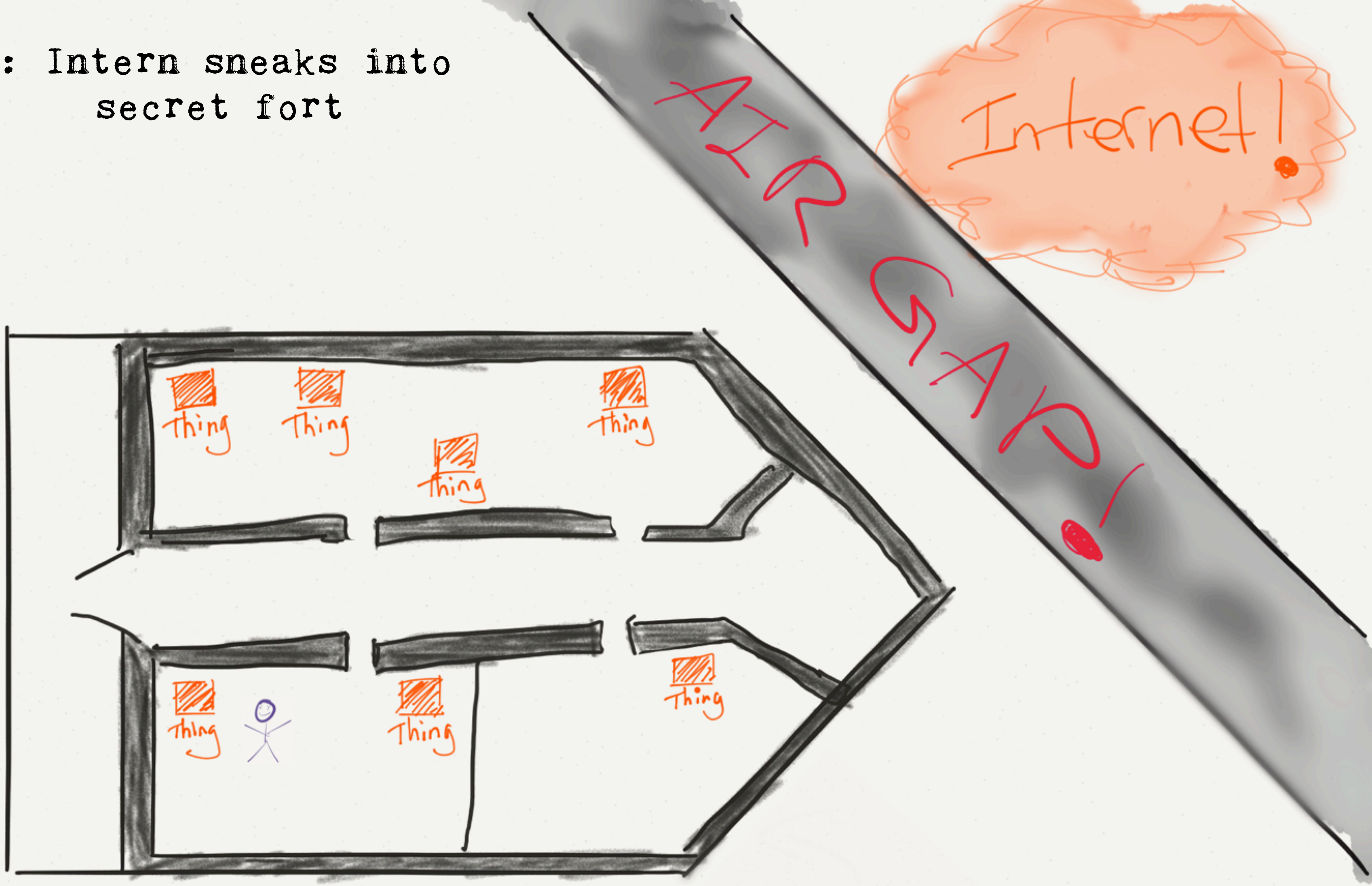
Amazing Ninja Tech



Step 1: Intern sneaks into secret fort

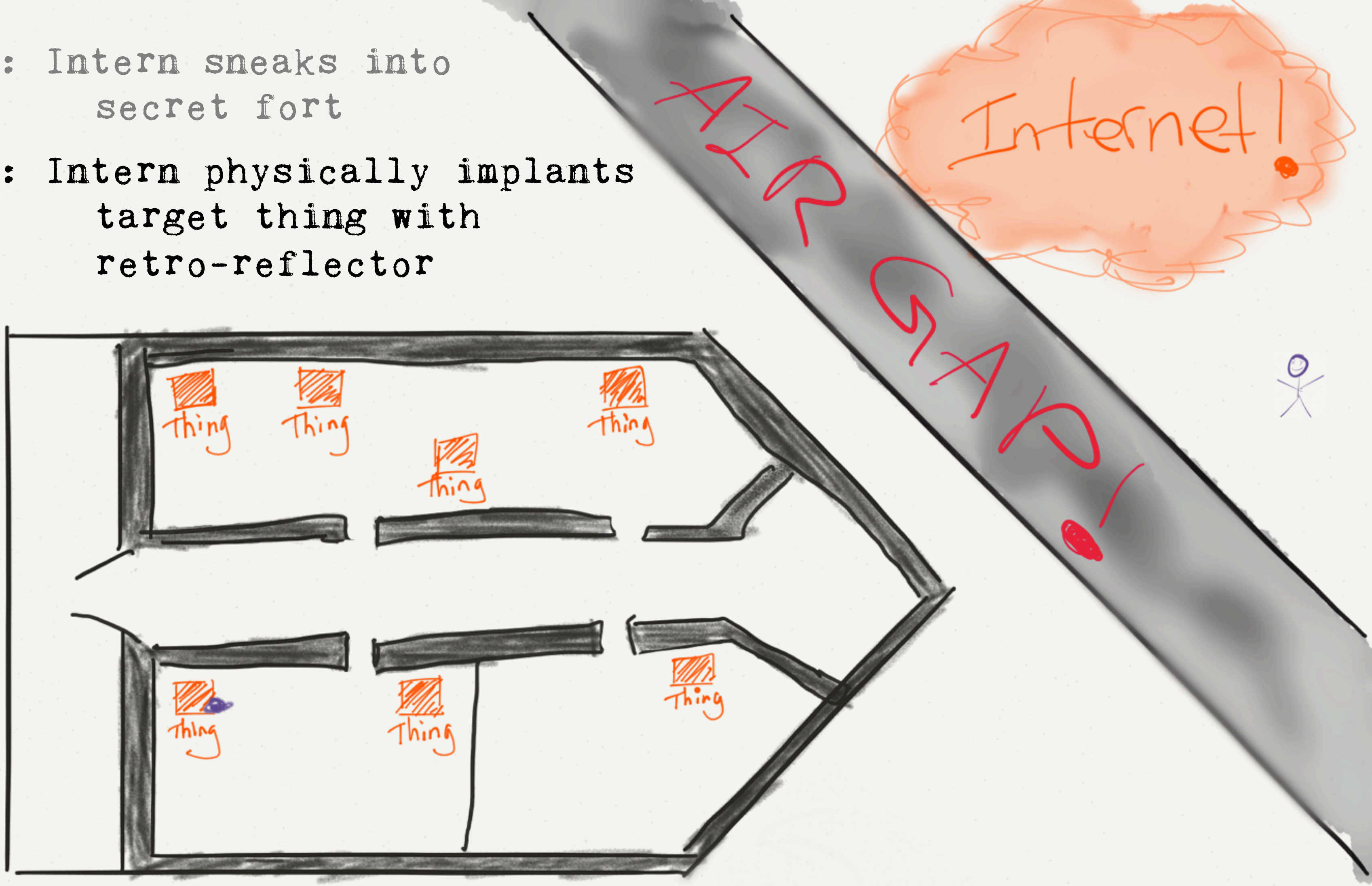


Step 1: Intern sneaks into secret fort



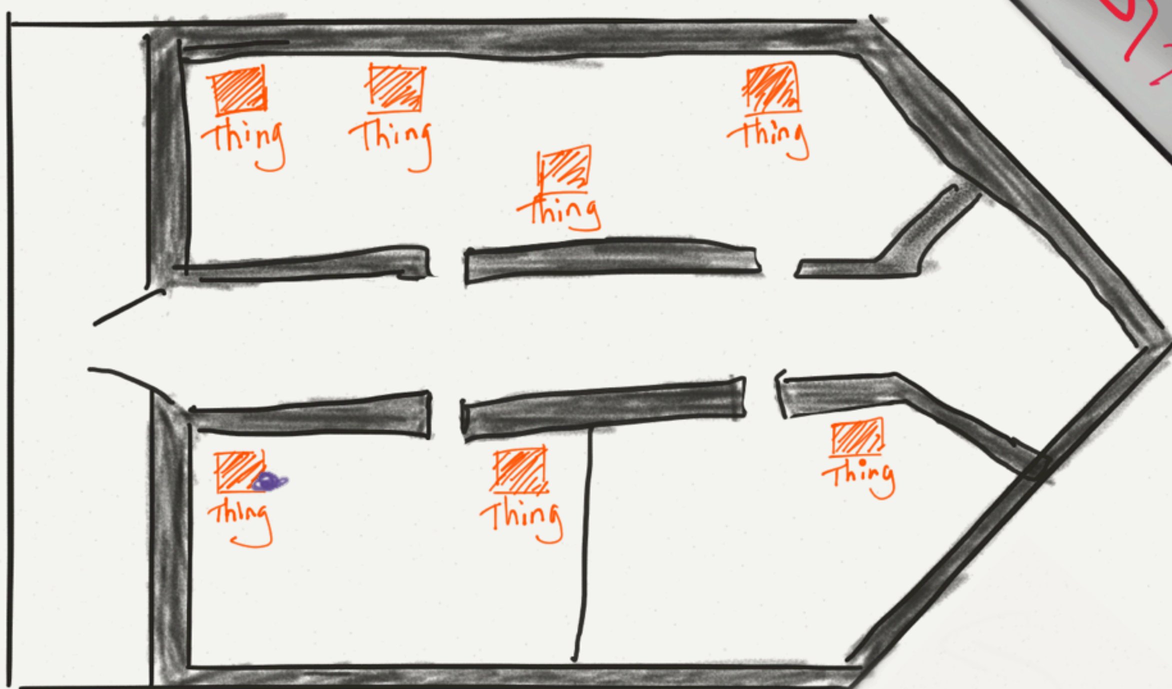
Step 1: Intern sneaks into secret fort

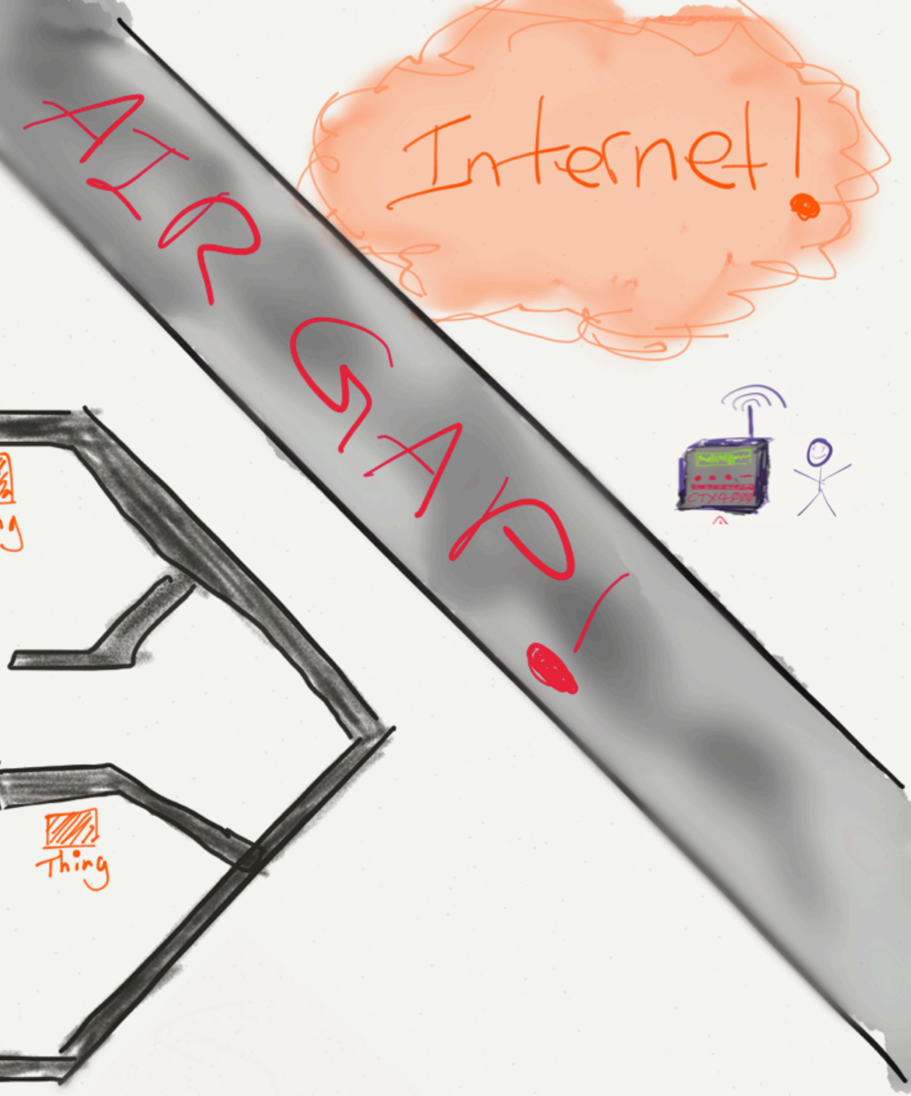
Step 2: Intern physically implants target thing with retro-reflector



Step 1: Intern sneaks into
secret fort

Step 2: Intern physically implants
target thing with
retro-reflector

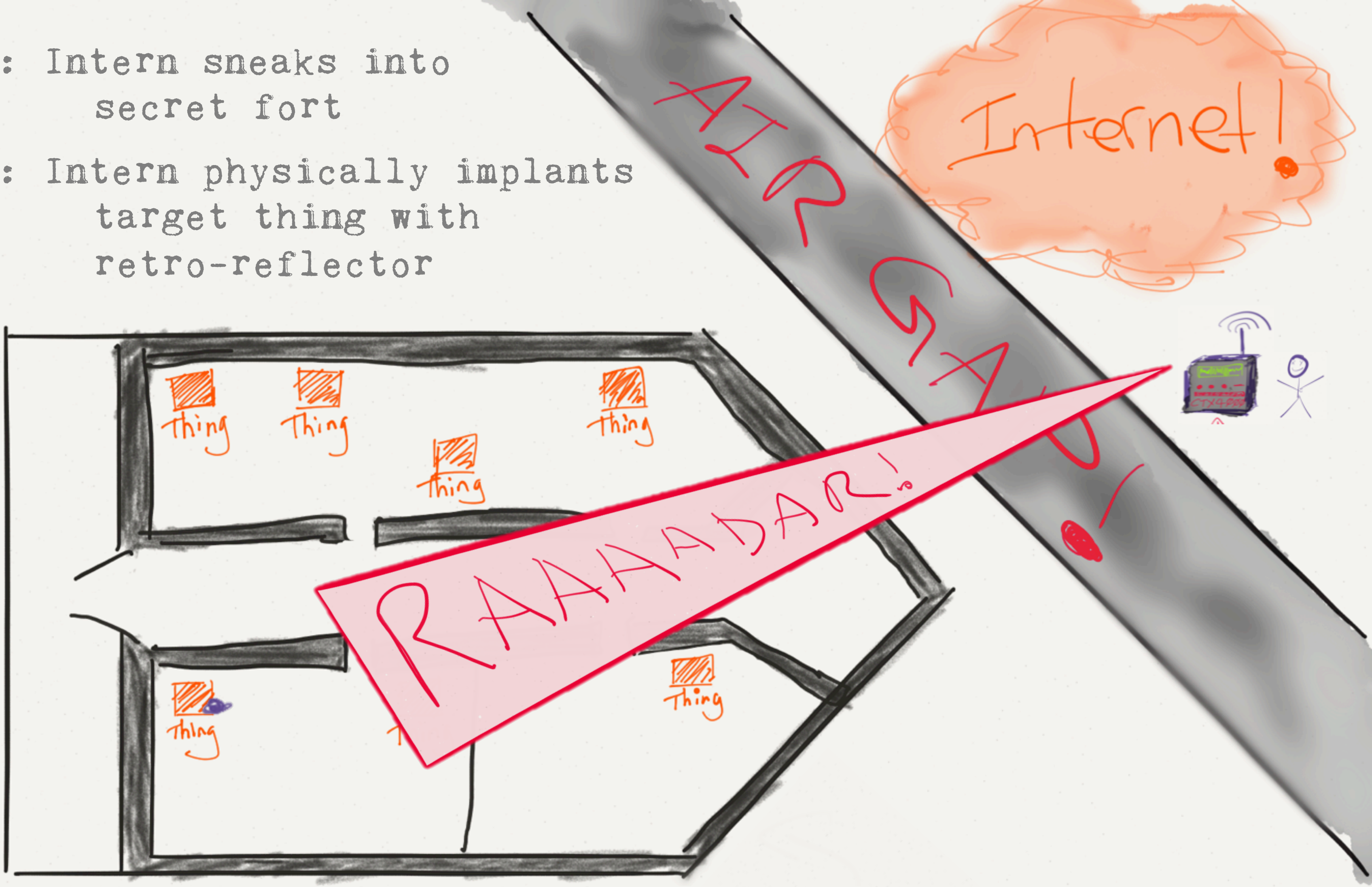




Step 3: Continuous RF Illumination (CTX4k, etc)
into secret fort

Step 1: Intern sneaks into secret fort

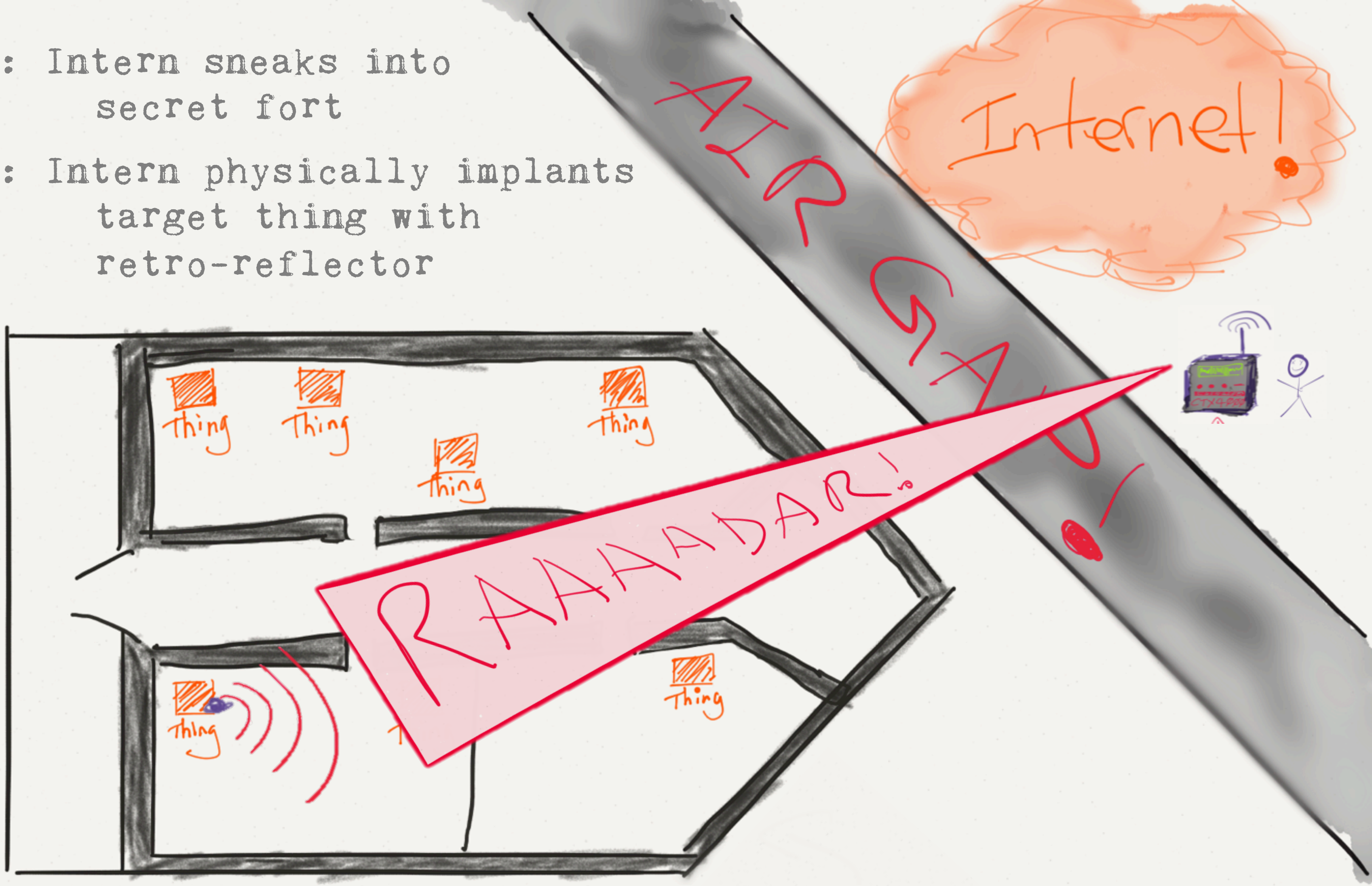
Step 2: Intern physically implants target thing with retro-reflector



Step 3: Continuous RF Illumination (CTX4k, etc) into secret fort, secret data comes out

Step 1: Intern sneaks into secret fort

Step 2: Intern physically implants target thing with retro-reflector



Step 3: Continuous RF Illumination (CTX4k, etc) into secret fort, secret data comes out

Good idea if…

Good idea if…

1: Infinite Interns

Good idea if…

1: Infinite Interns

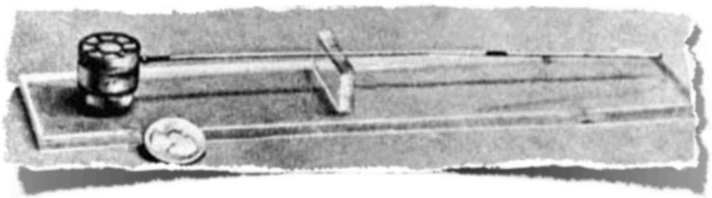
2: Not worried about leaving evidence behind (see #1)

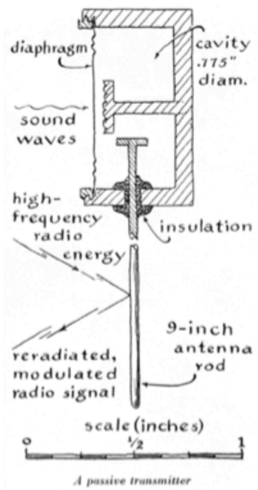
Retroreflector Technology

Retroreflector Technology

In Historical Context…

"The Thing"





(from Scientific American, 1968)

sites.apam.columbia.edu/courses/apph4903x/Great_Seal_Bug.pdf

Retroreflector
In Historical Context…

Way back when…

Retroreflector
In Historical Context…

Designed for this

Retroreflector
In Historical Context…

Phone

Phone

Deployed in the age of this

Retroreflector
In Historical Context…

office

Designed for this

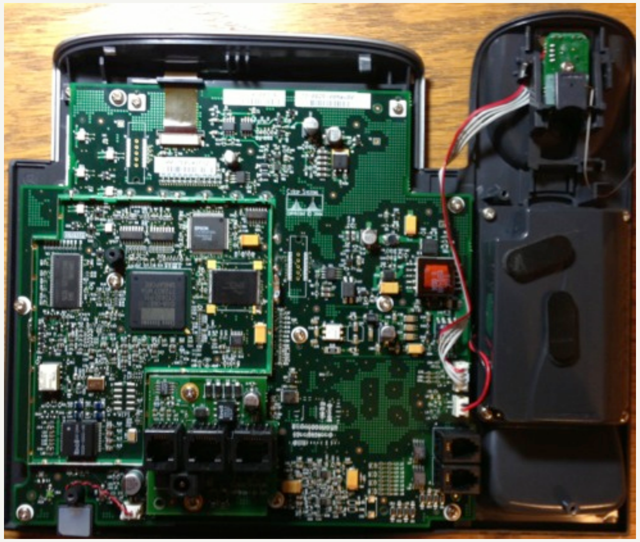
Retroreflector
In Historical Context…

office

office

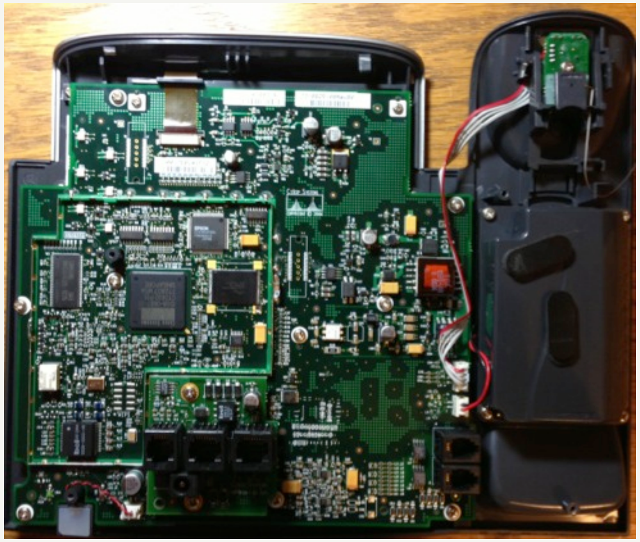
Deployed in the age of this

The Difference?



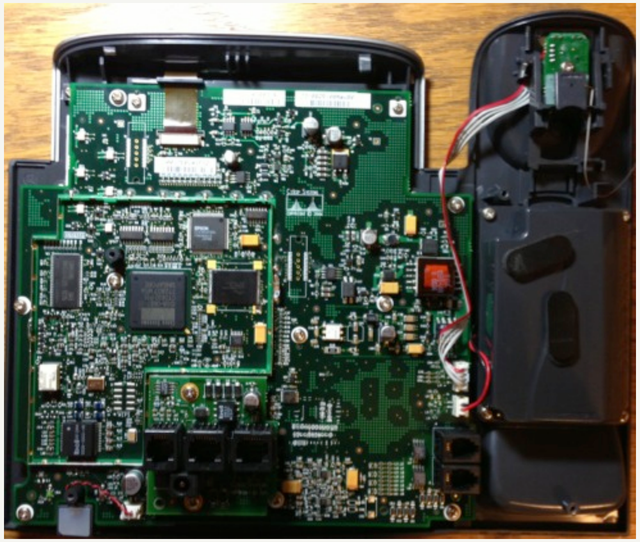
The Difference?

~ 50 Million Transistors



The Difference?

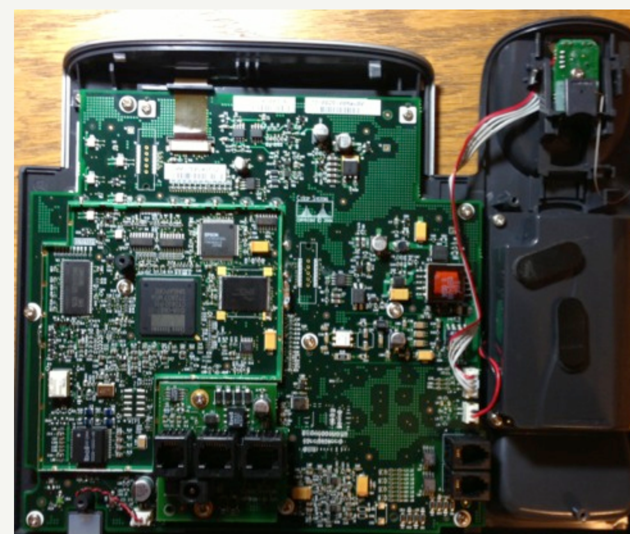
~ 50 Million Transistors
~ 1 Million Lines of Code



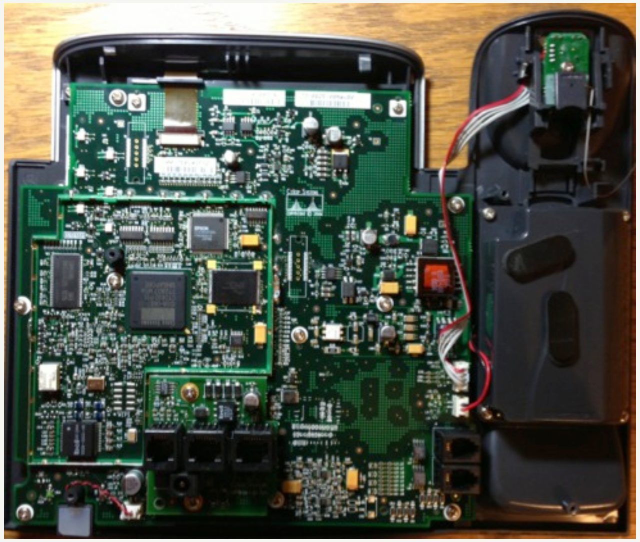
The Difference?

~ 50 Million Transistors
~ 1 Million Lines of Code

All-purpose computing hardware
Inside special-purpose packaging



Leverage This Difference



~ 50 Million Transistors
~ 1 Million Lines of Code

All-purpose computing hardware
Inside special-purpose packaging

And…

"Emanate like a"

~~Scrub~~

BOSS!

Leverage This Difference

And…

1. Exfiltrate using only software

Leverage This Difference

And…

1. Exfiltrate using only software
2. Exfiltrate using all the things

Leverage This Difference

And…

1. Exfiltrate using only software
2. Exfiltrate using all the things
3. Exfiltrate using arbitrary frequency range

Leverage This Difference

And…

1. Exfiltrate using only software
2. Exfiltrate using all the things
3. Exfiltrate using arbitrary frequency range

4. Evaporate when done

Part I

Compromising Emanations!

Part I

Compromising Emanations!

Part II

Firmware Shenanigans

Prior Art

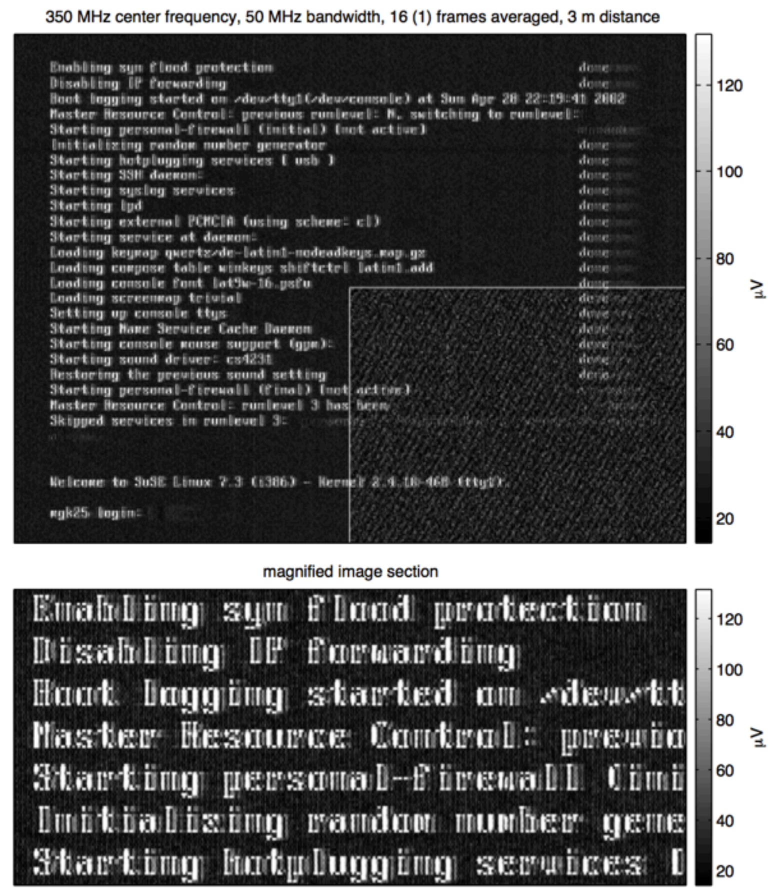
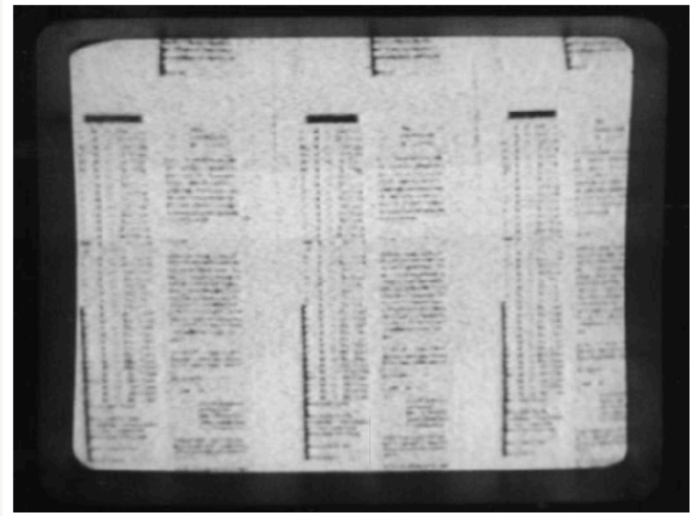


Fig. 1. Eavesdropped Linux boot screen visible on the LCD of a Toshiba 440CDX laptop (log-periodic antenna, vertical polarization).



Electromagnetic Eavesdropping Risks of Flat-Panel Displays

Markus G. Kuhn

University of Cambridge, Computer Laboratory,
15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom
`http://www.cl.cam.ac.uk/~mgk25/`

PRIOR ART

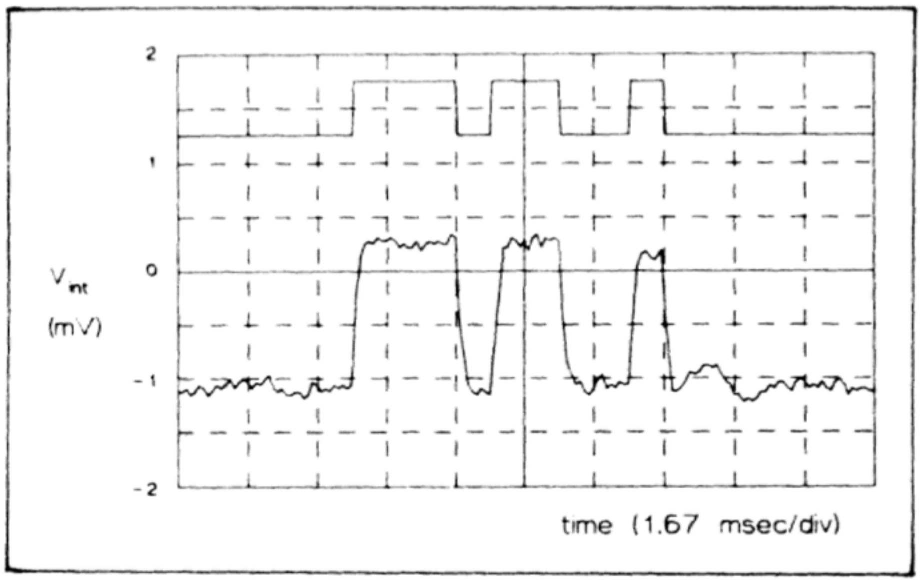


Fig. 4. Original and intercepted data signal at 7 m and 98 MHz (FM band).

The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables

Peter Smulders

Example: Acoustic Crypto-Analysis
Genkin, Shamir, Tromer

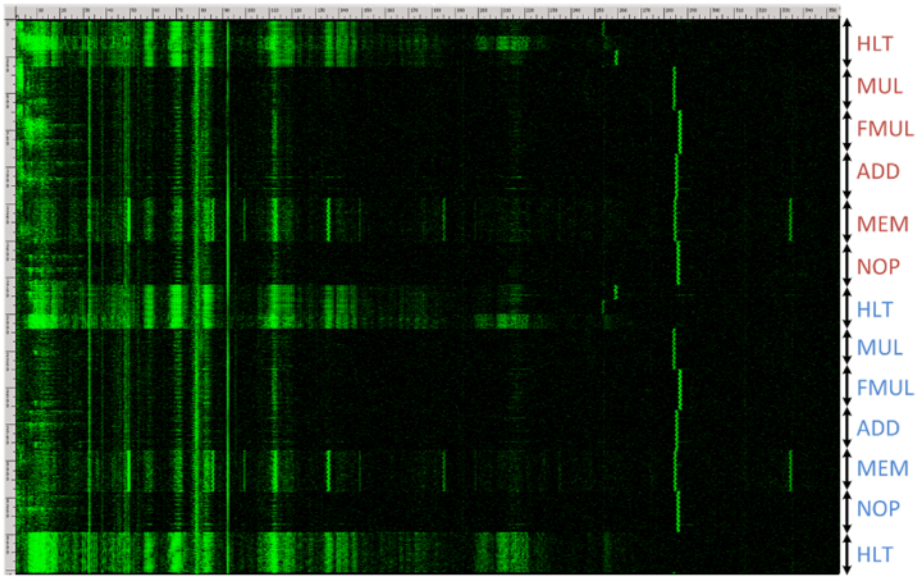


Figure 7: Acoustic measurement frequency spectrogram of a recording of different CPU operations using the Brüel&Kjær 4939 microphone capsule. The horizontal axis is frequency (0–310 kHz), the vertical axis is time (3.7 sec), and intensity is proportional to the instantaneous energy in that frequency band.

RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis*

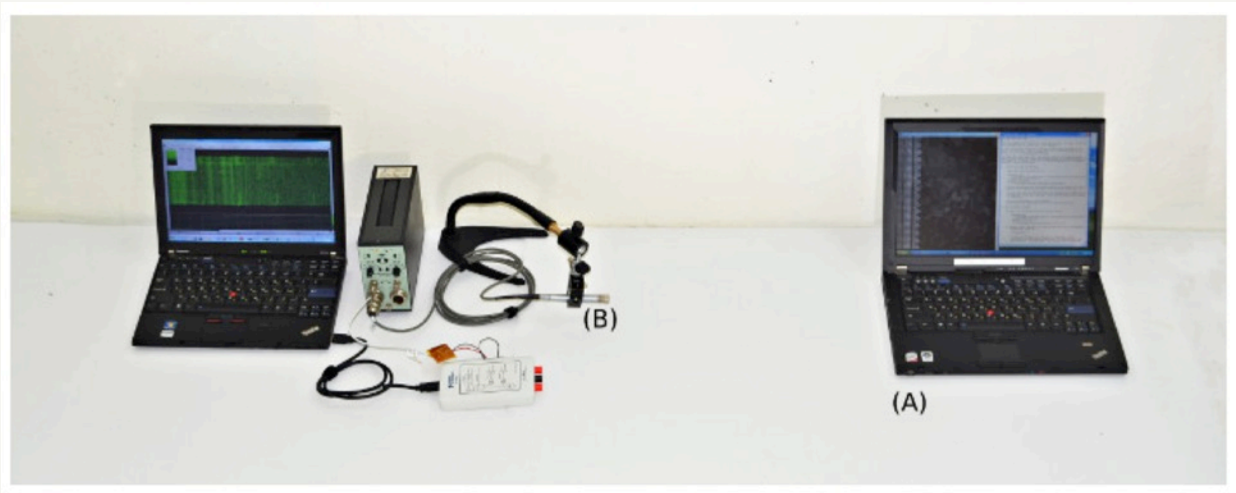
Daniel Genkin
Technion and Tel Aviv University
danielg3@cs.technion.ac.il

Adi Shamir
Weizmann Institute of Science
adi.shamir@weizmann.ac.il

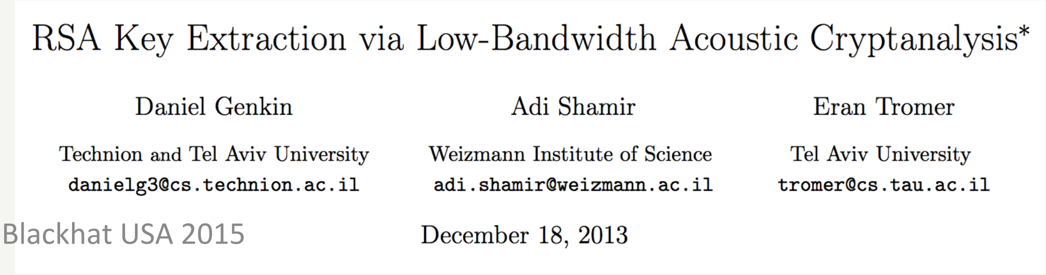
Eran Tromer
Tel Aviv University
tromer@cs.tau.ac.il

December 18, 2013

Example: Acoustic Crypto-Analysis
Genkin, Shamir, Tromer



4 Meters!


RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis*

Daniel Genkin
Technion and Tel Aviv University
danielg3@cs.technion.ac.il

Adi Shamir
Weizmann Institute of Science
adi.shamir@weizmann.ac.il

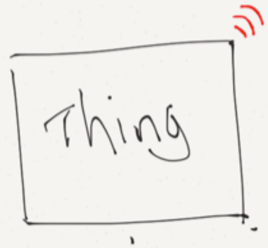
Eran Tromer
Tel Aviv University
tromer@cs.tau.ac.il

December 18, 2013

Majority of
Compromising Emanations Research

Majority of
Compromising Emanations Research

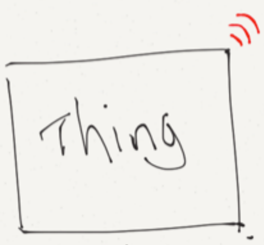
Faint, accidentally
Leaked signal



Majority of
Compromising Emanations Research

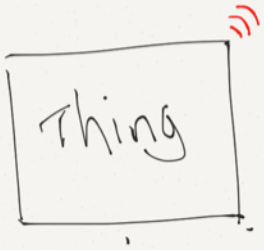
Big powerful receiver

Faint, accidentally
Leaked signal

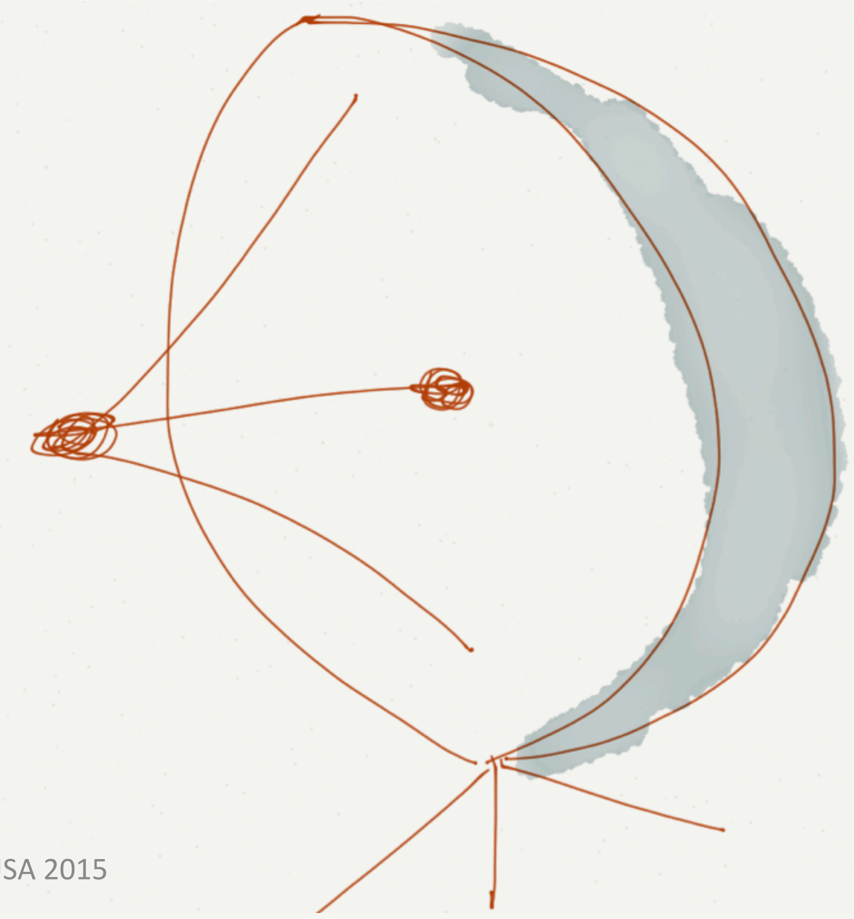


What if…

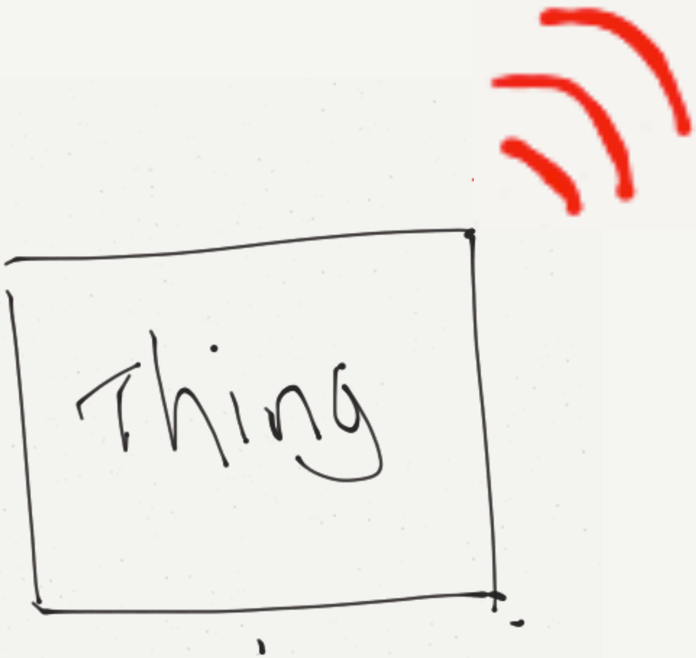
Faint, accidentally
Leaked signal



Big powerful receiver

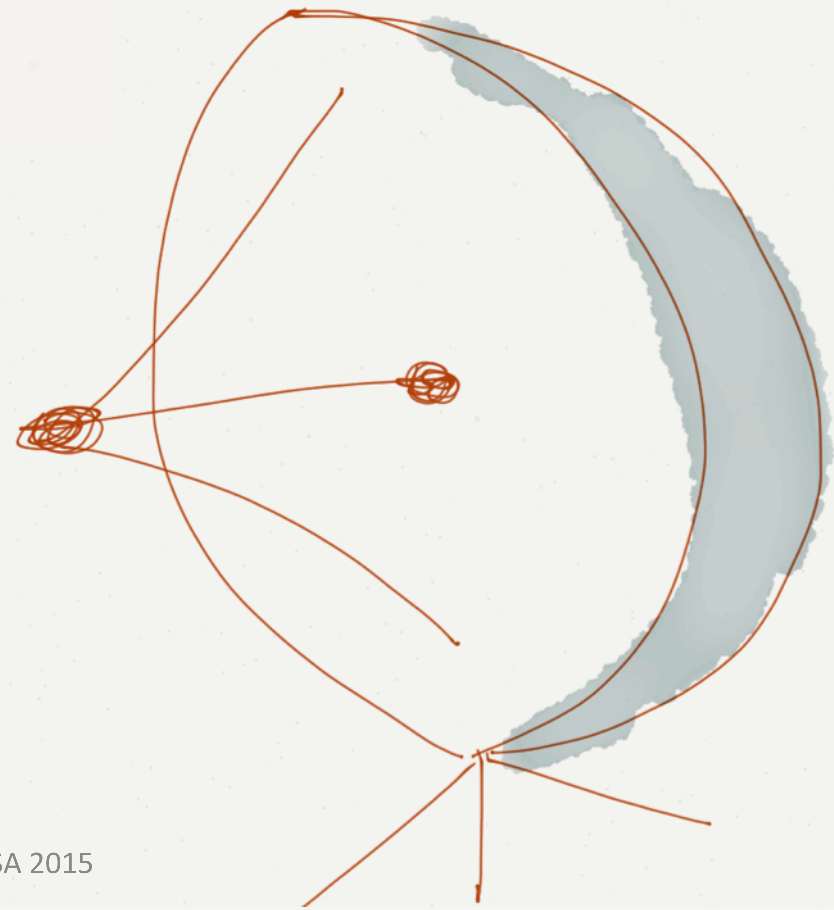


What if…

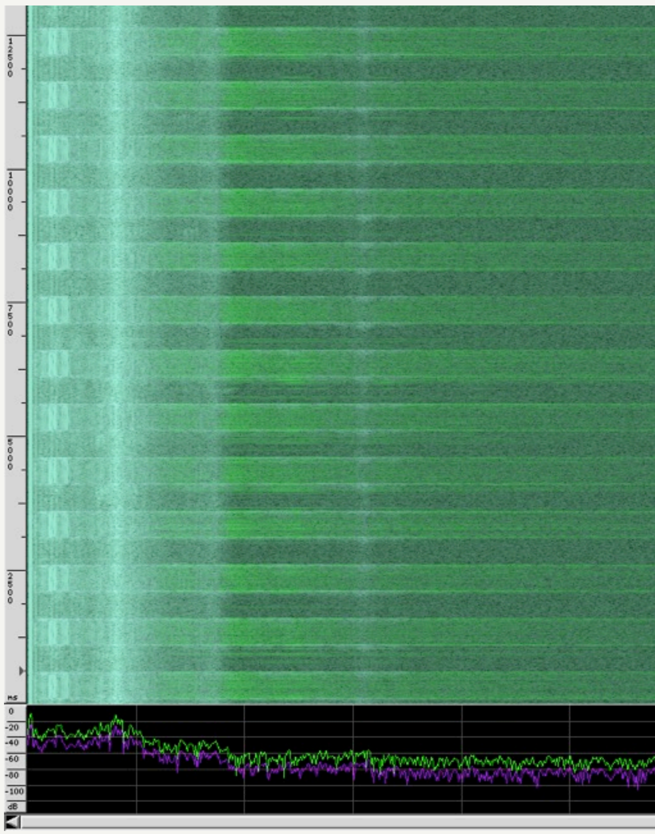


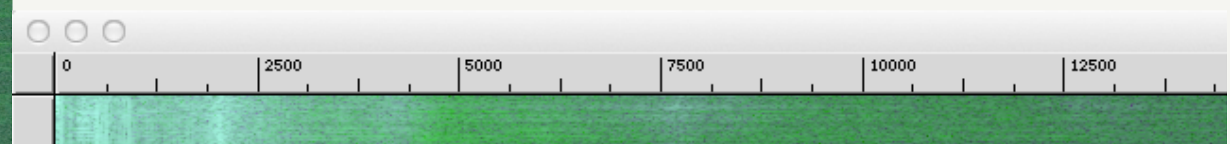
Loud, intentionally generated compromising emanation

Big powerful receiver

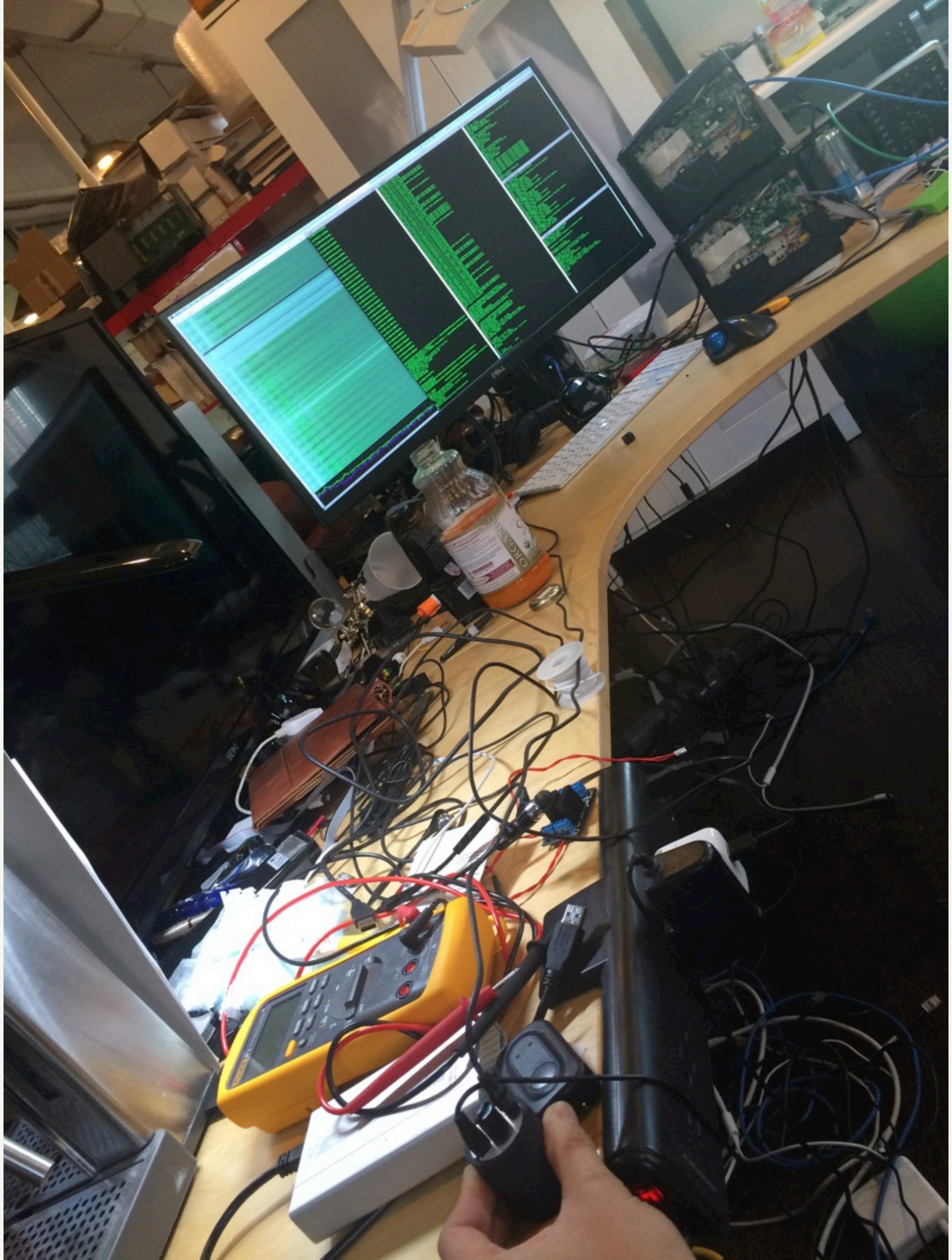


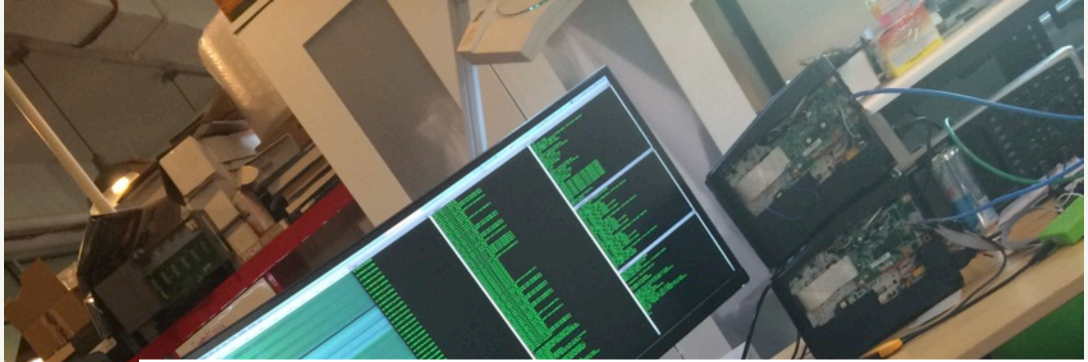
DEMO 1: Acoustic Funtenna Emanation





Sub 1khz emanation





Customer Questions & Answers

Have a question? Ask the owners here | Ask

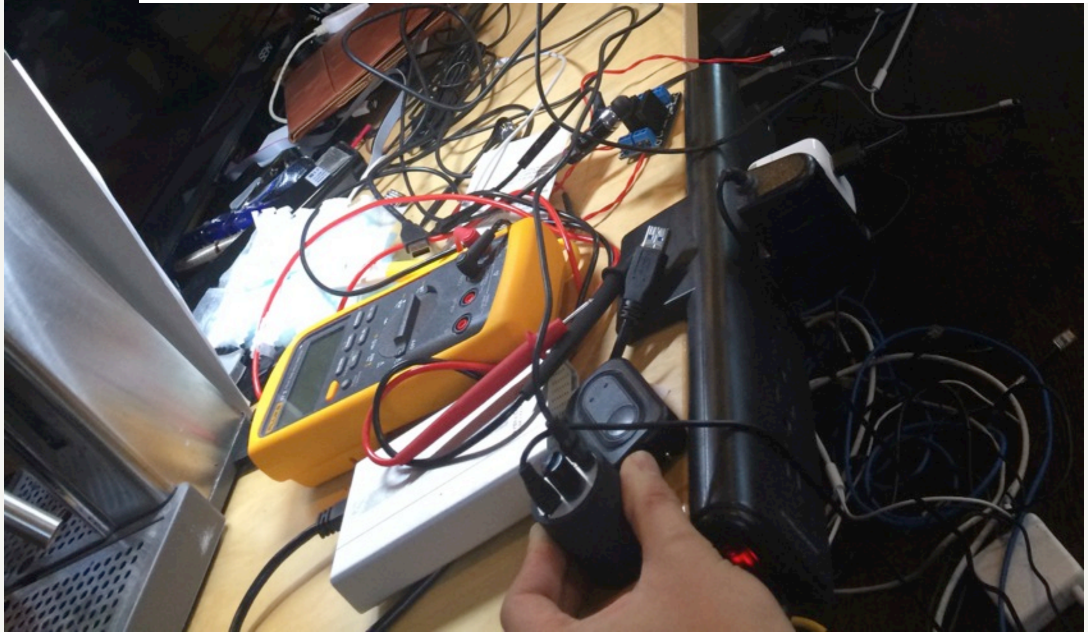
Don't see what you're looking for? Submit your question to our community by clicking the 'Ask' button above.

0 votes

Geo pone converts noise into voices? have I got that right, and these voices are they Alive humans like your neighbors that you hear?

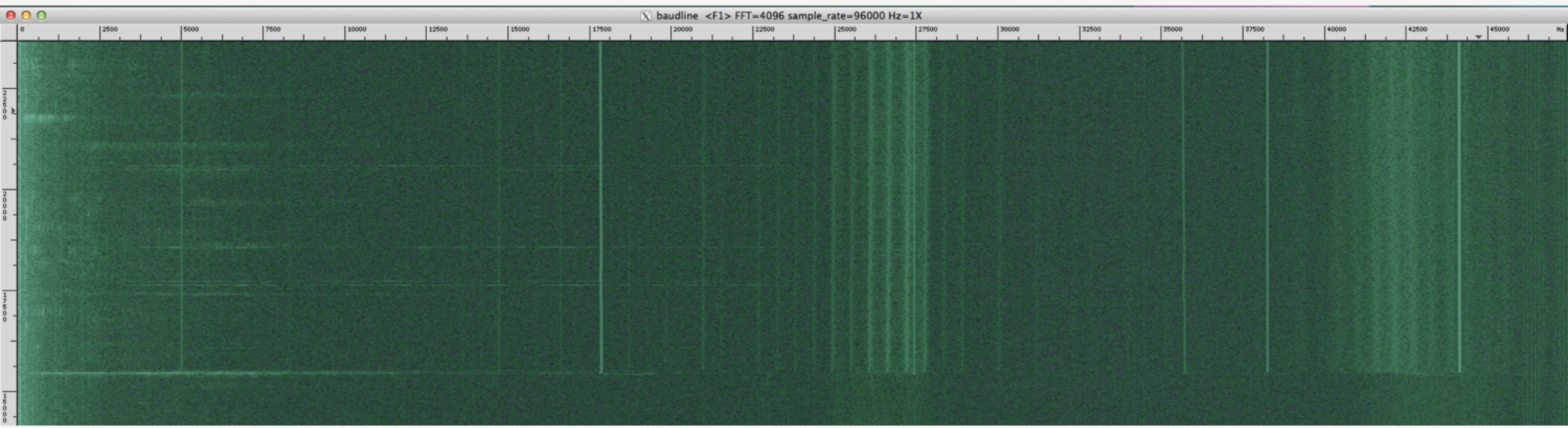
A: It hears through vibrations, you have to set it down on something and then hook either a recorder or headphones to it to hear anything. I thought it was something else when I bought it. I didn't want to have to hook something up to it to hear sounds. as for voices, I only tried it once and I think it picked up everything.

Sandra Labella answered on April 17, 2014

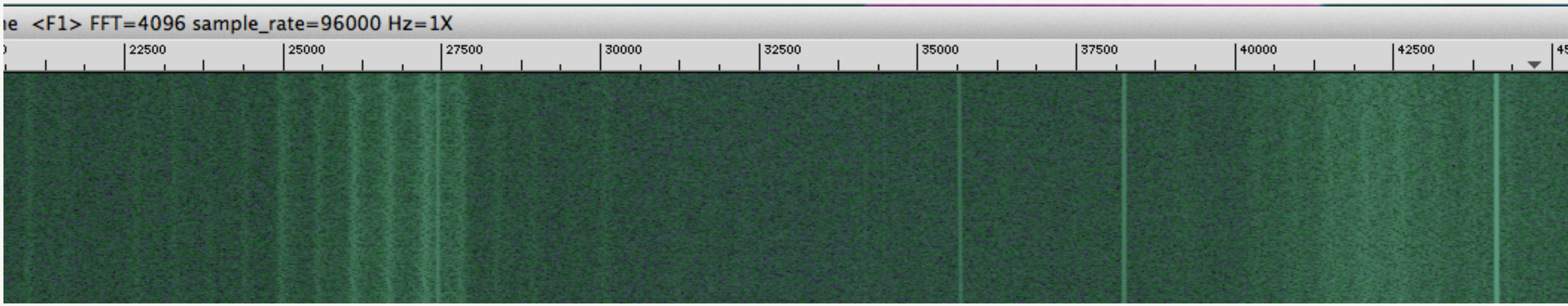


No, not like Alive humans

DEMO 1.5: Ultrasonic Funtenna Emanation



DEMO 1.5: Ultrasonic Funtenna Emanation



~27 Khz

~42 Khz

Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations

Markus G. Kuhn* and Ross J. Anderson

University of Cambridge, Computer Laboratory, New Museums Site, Pembroke Street, Cambridge CB2 3QG, United Kingdom
{mgk25,rja14}@cl.cam.ac.uk

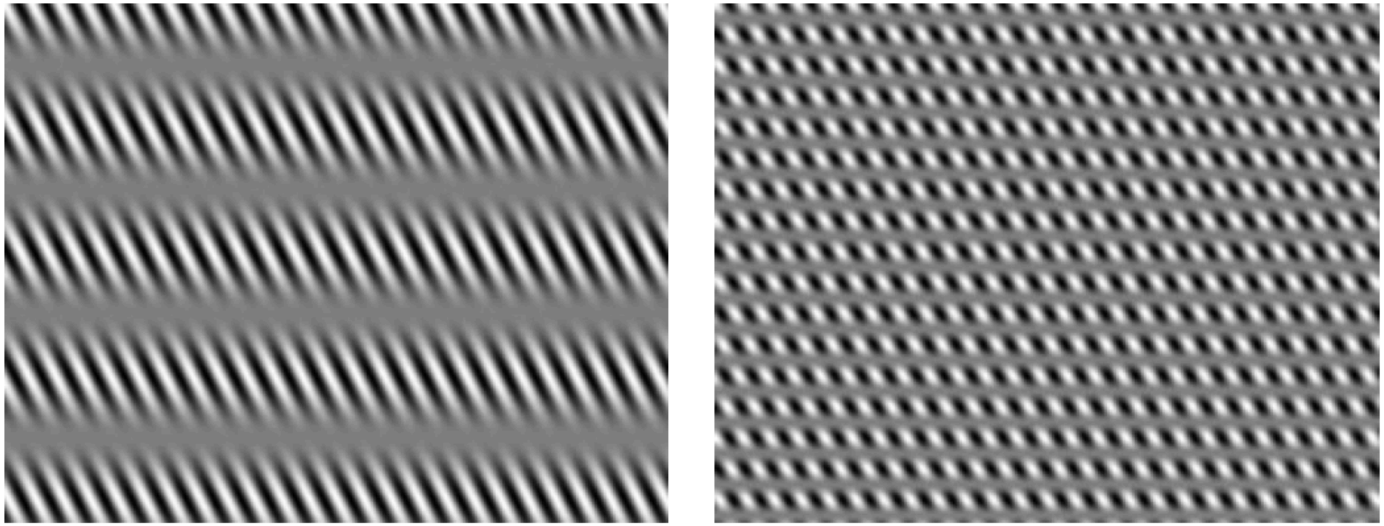


Fig. 1. Example screen contents that cause the authors' computer monitor to broadcast an $f_t = 300$ Hz (left) and 1200 Hz tone (right) on an $f_c = 2.0$ MHz carrier in amplitude modulation.

```
ModeLine "1152x900"  95  1152 1152 1192 1472  900 900 931 939
```

Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations

Markus G. Kuhn and Ross J. Anderson

Computer Laboratory

UNIVERSITY OF CAMBRIDGE

http://www.cl.cam.ac.uk/~mgk25/ih98-tempest-slides.pdf

Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations

Markus G. Kuhn and Ross J. Anderson
Computer Laboratory
UNIVERSITY OF CAMBRIDGE

http://www.cl.cam.ac.uk/~mgk25/ih98-tempest-slides.pdf

Conclusions

→ Interesting field of study, mostly unexplored in the open literature

Probably not a new idea

But not discussed "in the open"

A decade later…

BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations

Guri, Monitz, Mirski, Elovici

Distance: 40cm
Data Rate: 1-8 bits per hour

On Covert Acoustical Mesh Networks In Air

Hanspach & Goetz

Distance: 19.7 M
Data Rate: 20 bits per second

AirHopper: Bridging the Air-Gap Between Isolated Networks and Mobile Phones Using Radio Frequencies

Guri, Kedma, Kachlon, Elovici

Distance: 7 M
Data Rate: 60 bits per second

The next steps

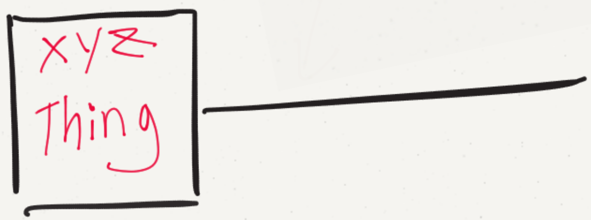
The next steps

1. Generalize and Unify Methodology

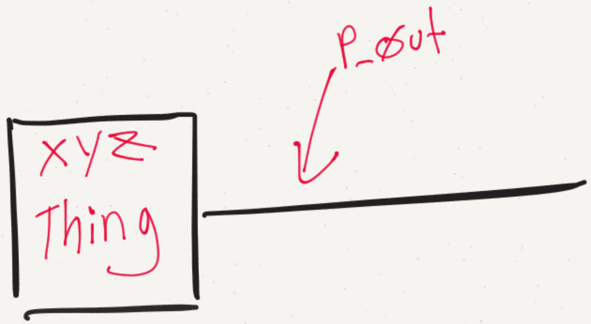
The next steps

1. Generalize and Unify Methodology
2. Minimize hardware dependencies

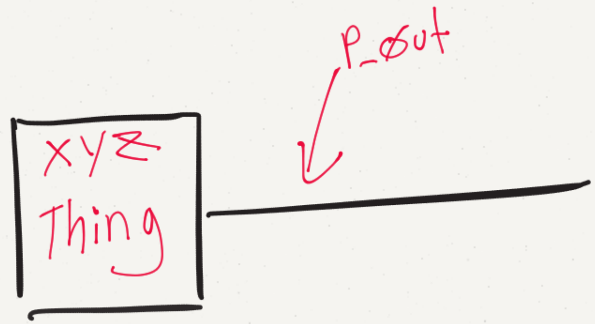
Funtenna 1Ø1



Funtenna 1Ø1

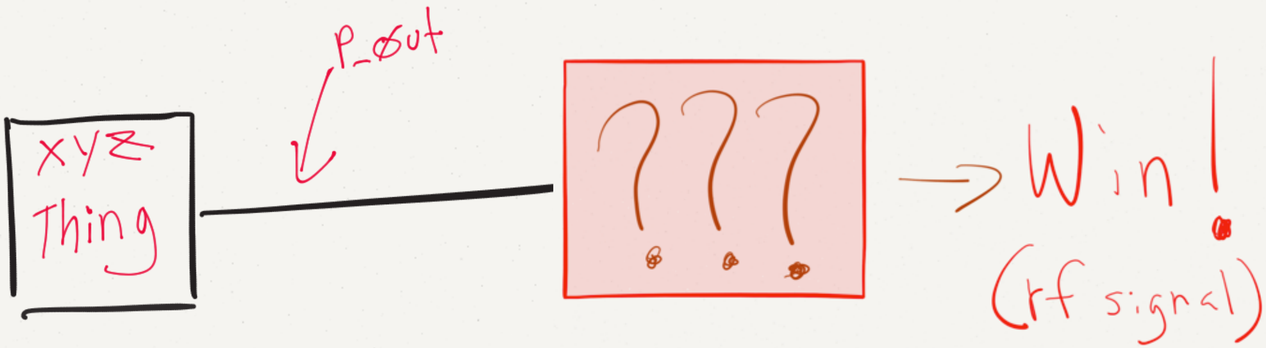


Funtenna 1Ø1



P_out: 0 1 0 1 0 1 0 1 0 1

Funtenna 1∅1



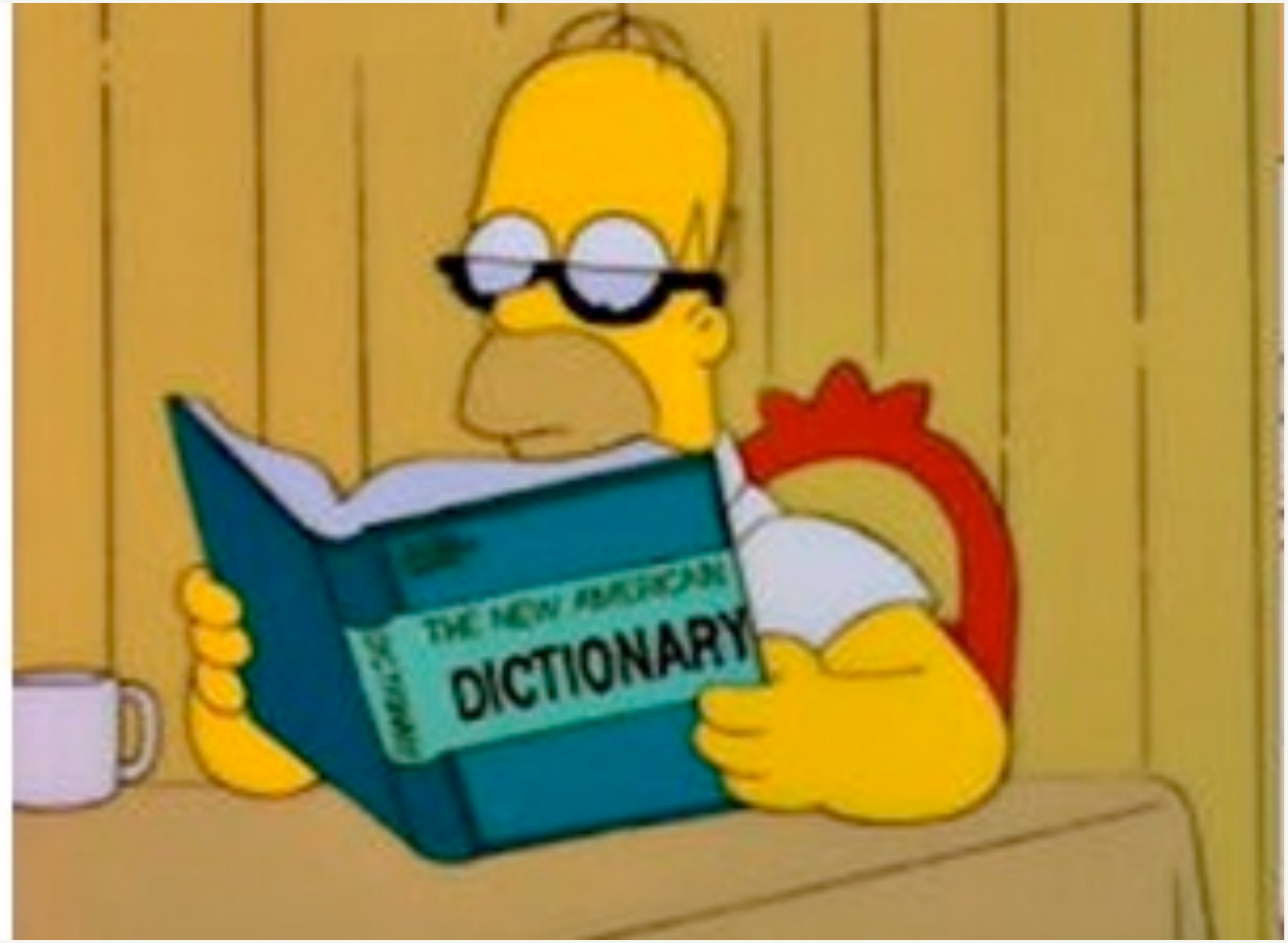
P_out: 0 1 0 1 0 1 0 1 0 1

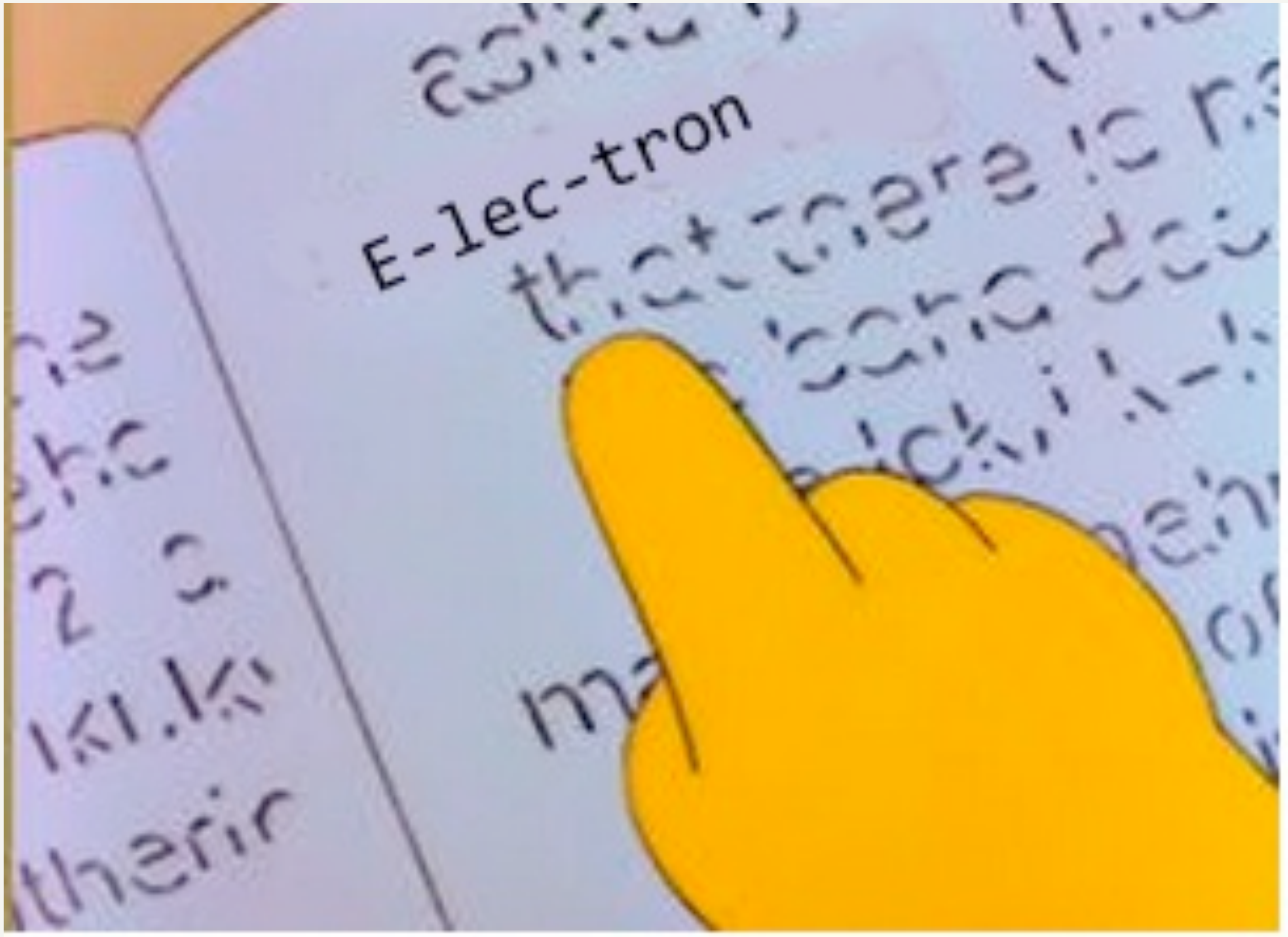

Advanc
SDR


Advanced
SDR


Beginnin
RADIO


Beginning
RADIO
VIA 9GAG.COM


THE NEW AMERICAN
DICTIONARY


E-lec-tron

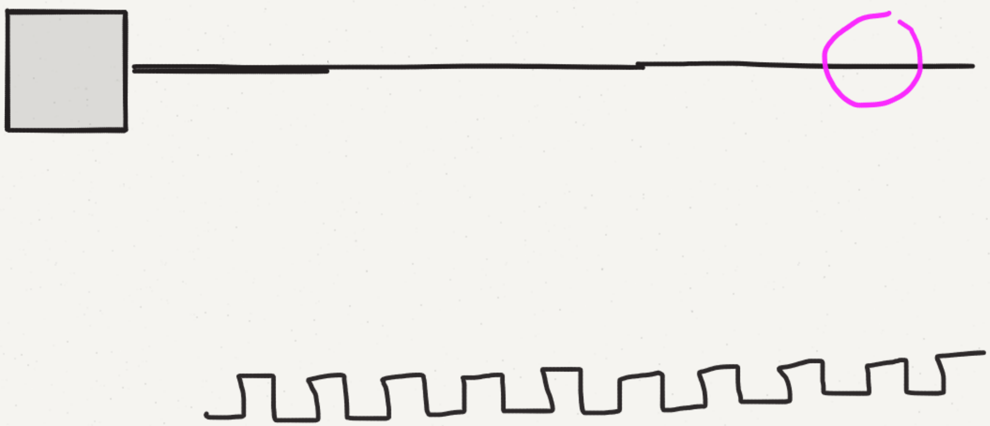
$$\nabla \times E = \frac{\partial B}{\partial t}$$

$$\nabla \times H = \frac{\partial D}{\partial t}$$

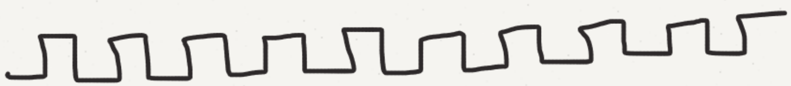
$$\nabla \cdot D = 0$$

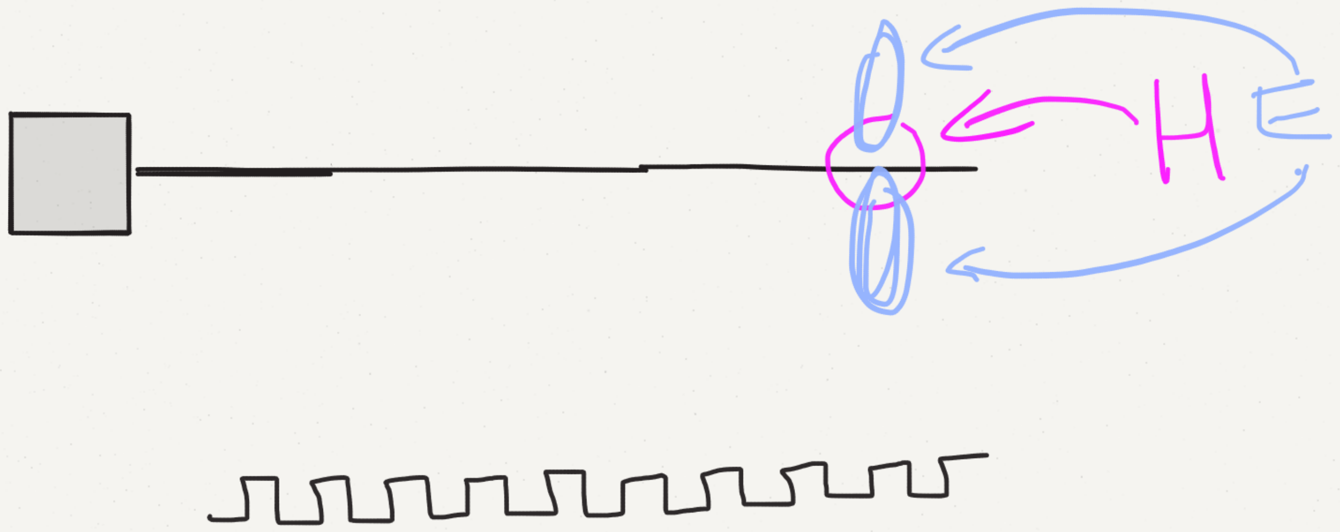
$$\nabla \cdot B = 0$$

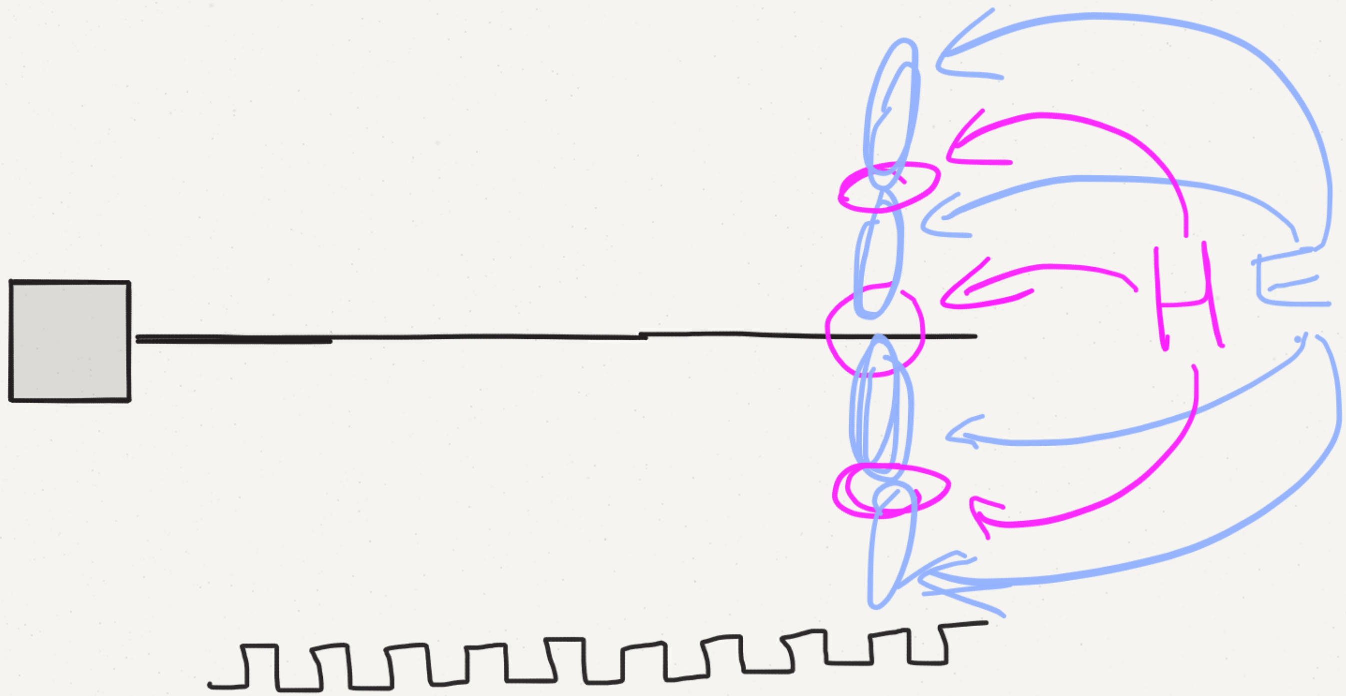
Maxwell's equations



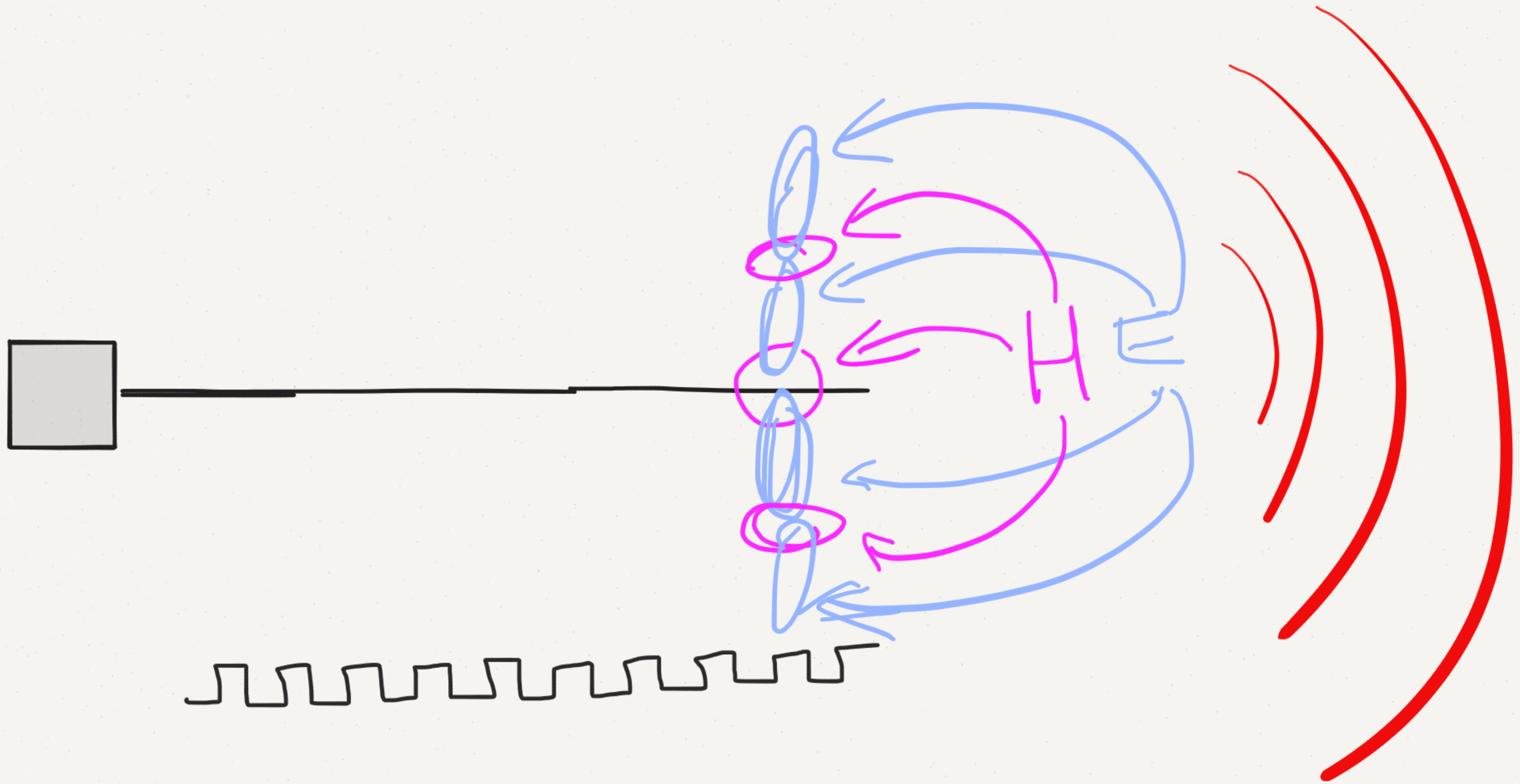

H

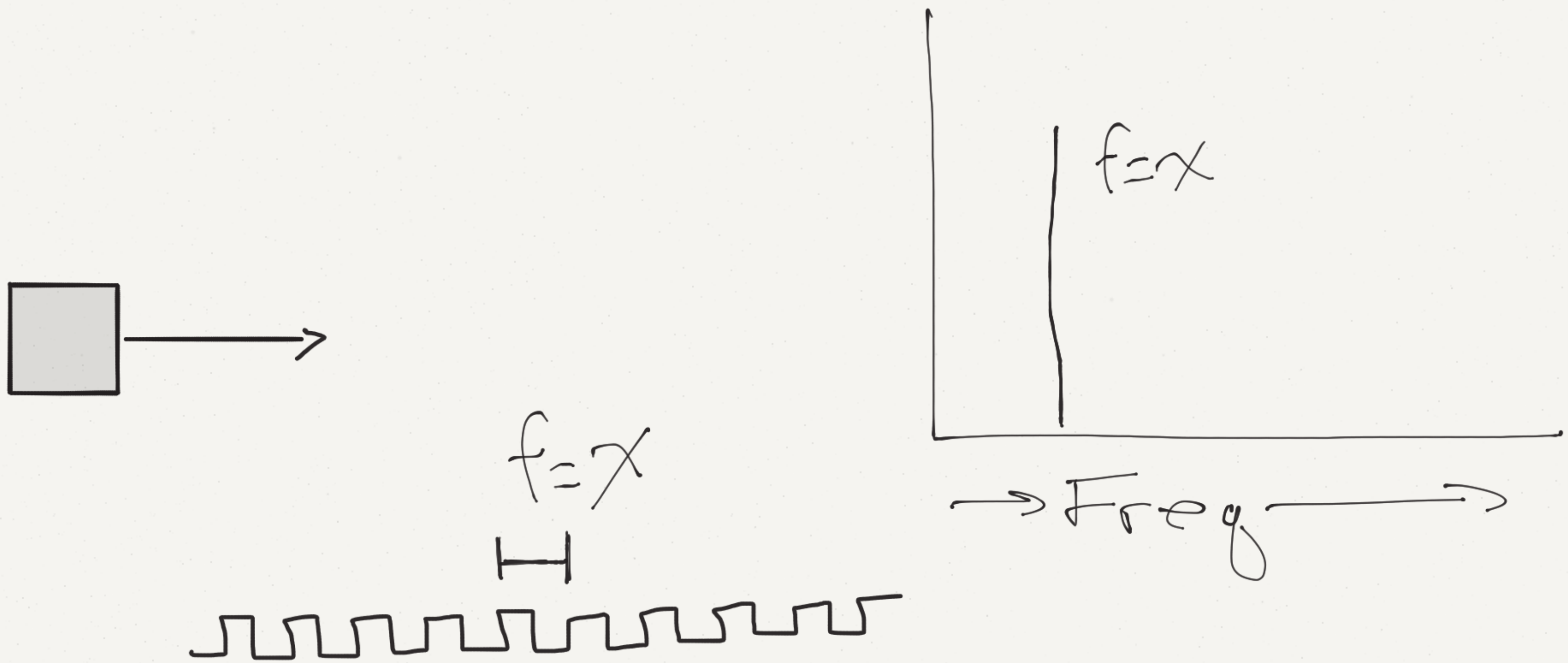


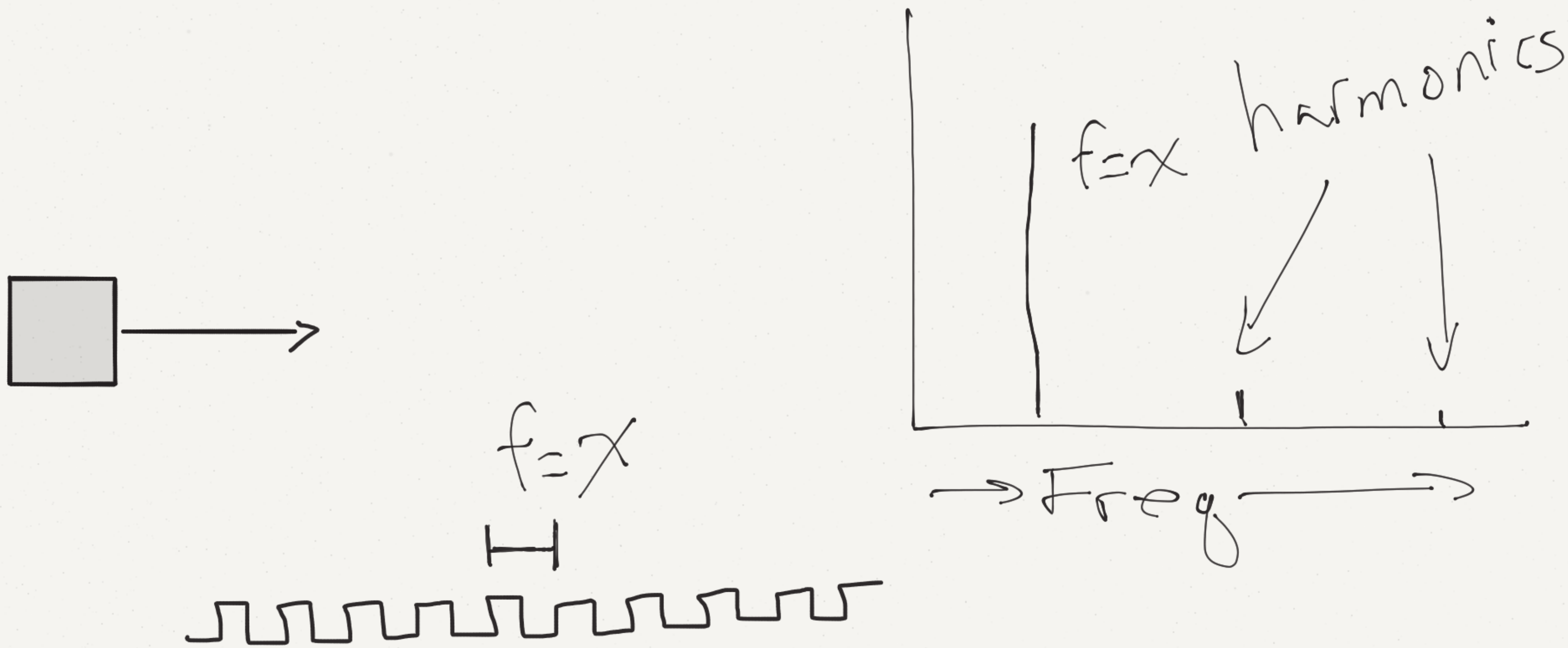

H
E



H


H


f=x
f=x
Freq


f=x
f=x
harmonics
Freq

Common Output Pins

- PWM (Pulse Width Modulation)
- GPIO (General Purpose Input Output)
- UART (Universal Asynchronous Receive Transmit)

Funtenna 1Ø2

Science!

Funtenna 1Ø2

Science!

For each

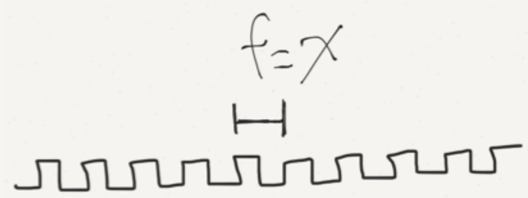
- PWM
- GPIO
- UART

Funtenna 1Ø2

Science!

For each

- PWM
- GPIO
- UART



Funtenna 1Ø2

Science!

For each

- PWM
- GPIO
- UART

1. Possible values for f
2. Optimal values for f

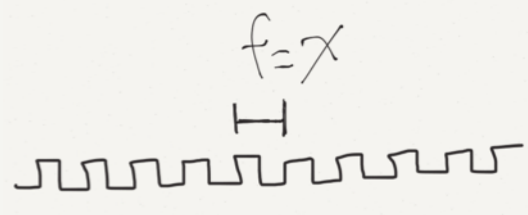
Funtenna 1Ø2

Science!

For each

- PWM
- GPIO
- UART

1. Possible values for f
2. Optimal values for f



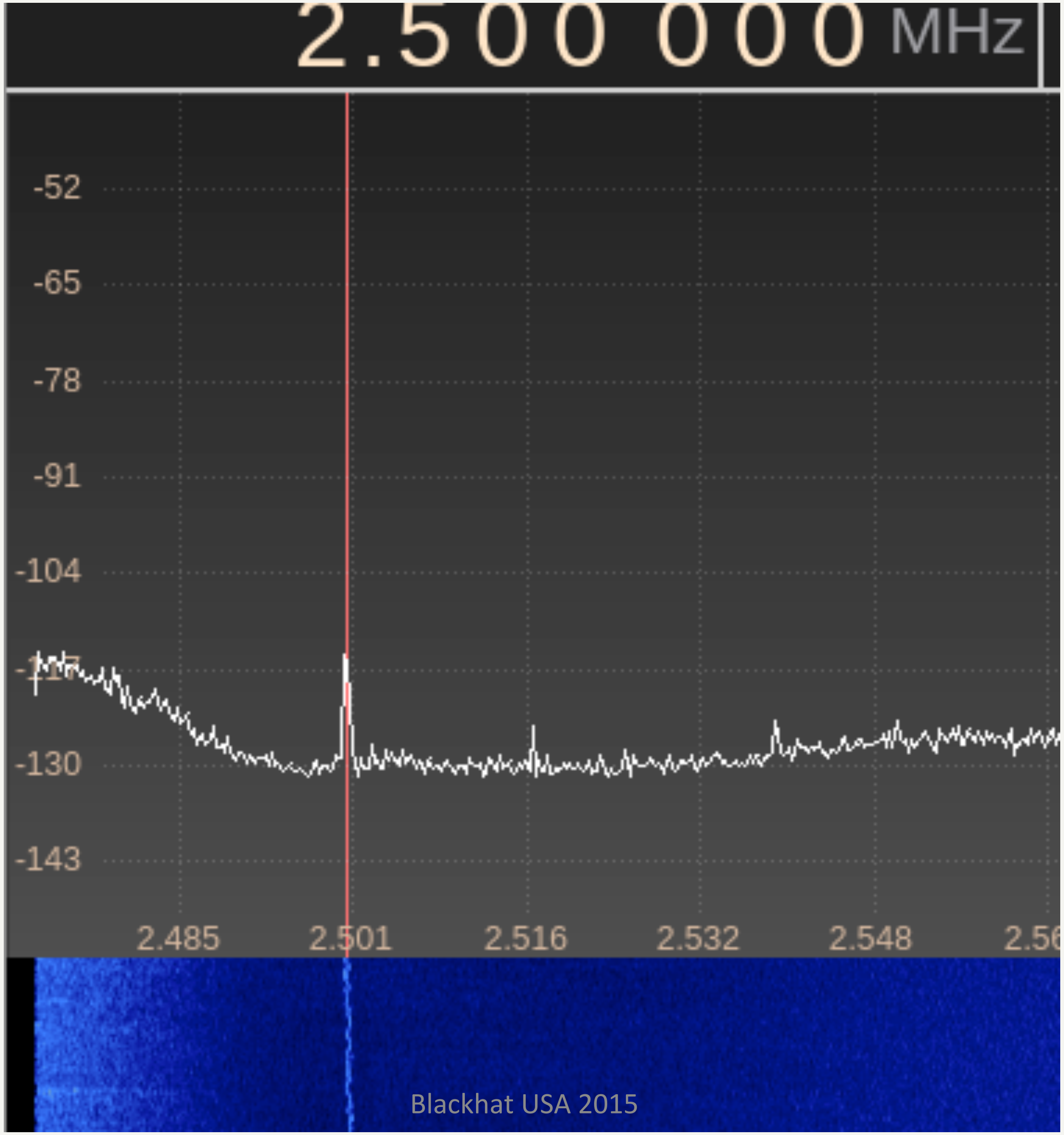
For each radiator length

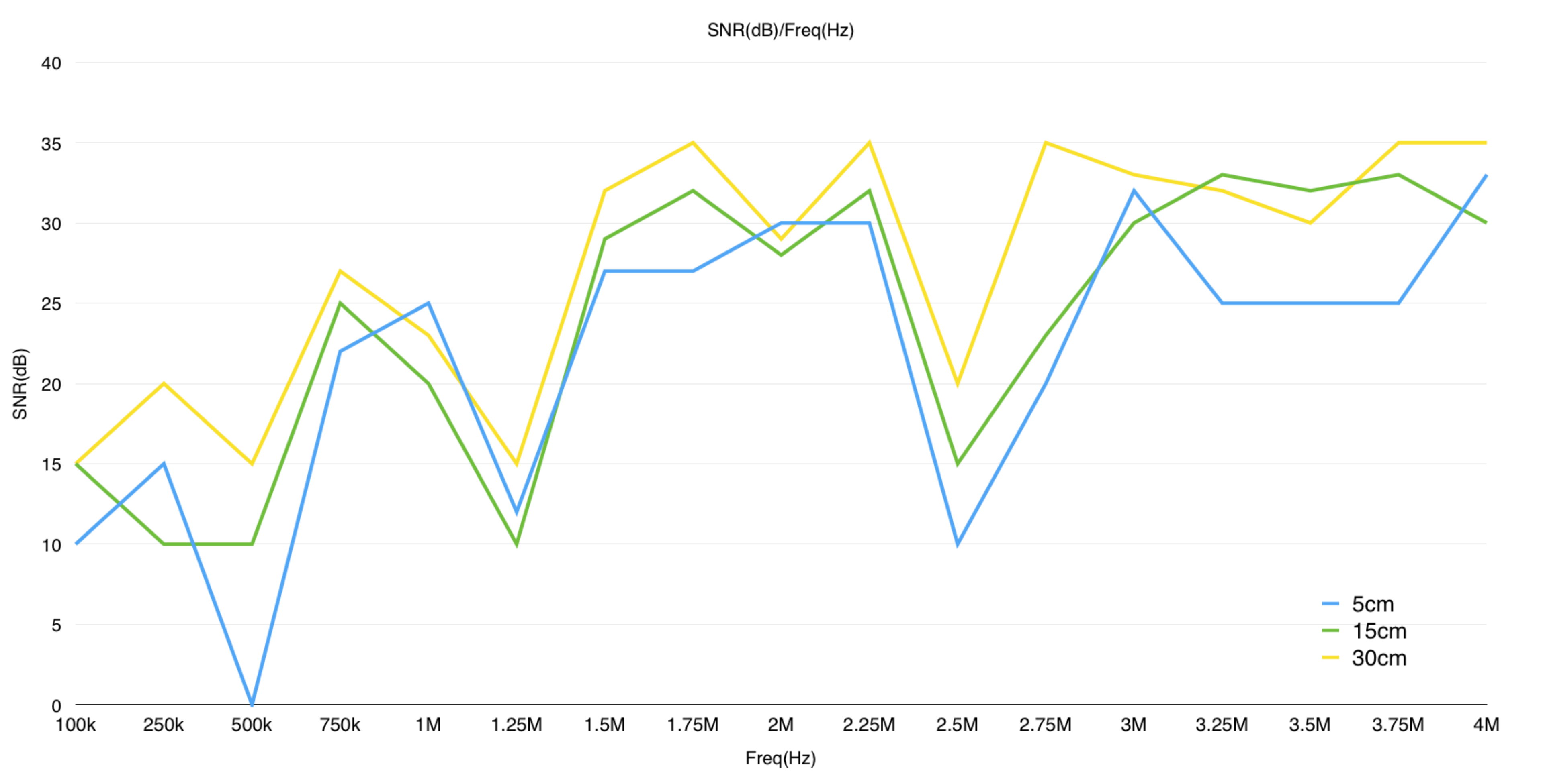
- 0cm
- 15cm
- 30cm

Experimental Setup

- "Faraday" Cage
- Buspirate (transmitter)
- USRP2 & BasicRX Board (receiver)

For example,
30cm radiator, f=500khz, harmonic signal @ 2.5mhz





Full raw dataset available at www.funtenna.org

Funtenna 1Ø2

Data Analysis…

Possible values for f

Optimal values for f

Optimal length of radiator

Funtenna 1ø2

Data Analysis…

Optimal length of radiator

Anything > 0, longer better…

Funtenna 1Ø2

Data Analysis…

Possible values for f

PWM: 10khz - 4mhz
GPIO: 10khz - 5mhz
UART: 10khz - 4mhz

Funtenna 1Ø2

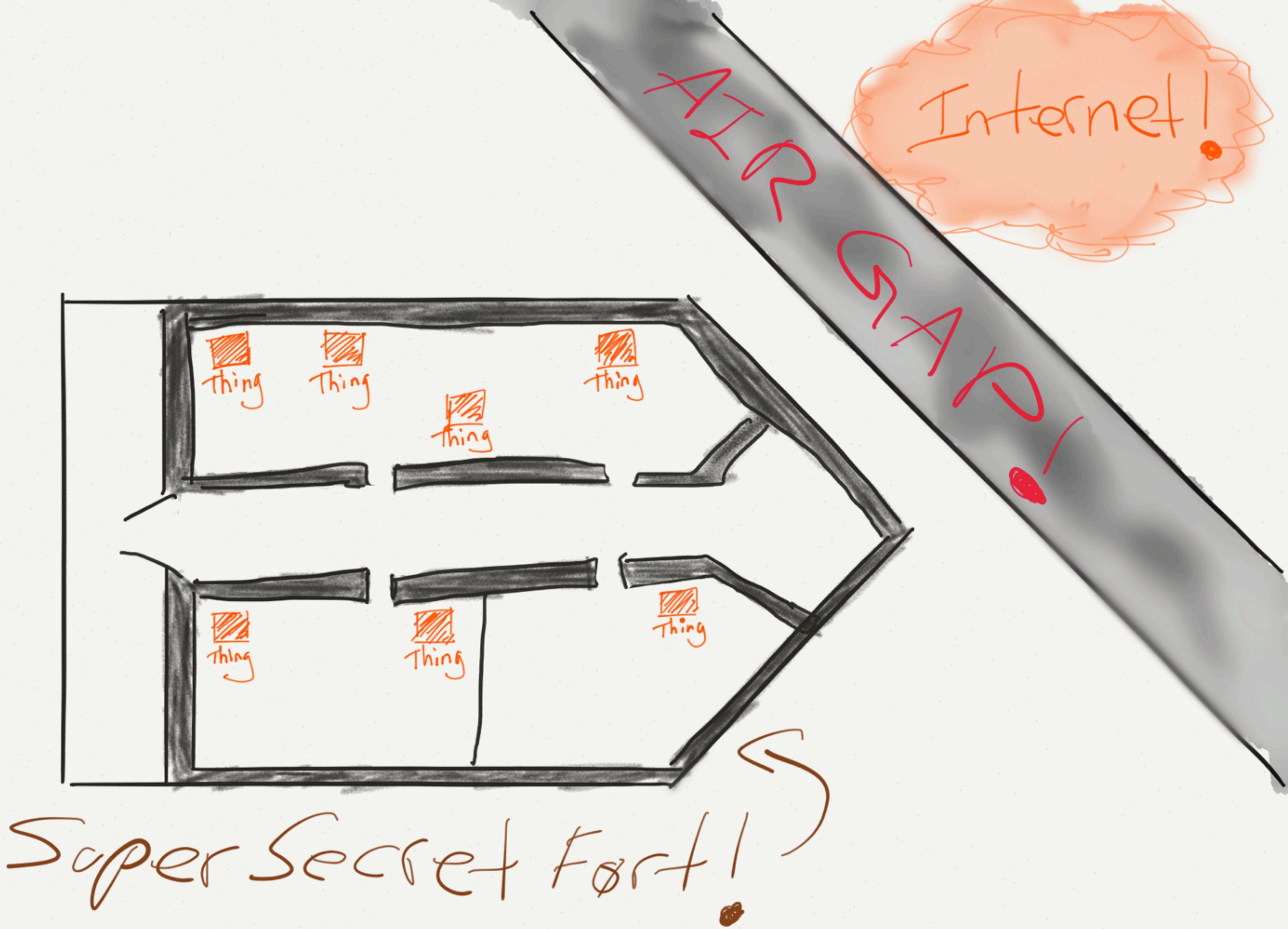
Data Analysis…

Possible values for f

PWM: 10khz - 4mhz
GPIO: 10khz - 5mhz
UART: 10khz - 4mhz

Optimal values for f

120Mhz - 205Mhz


Internet!
AIR GAP!
Thing
Thing
Thing
Thing
Thing
Thing
Thing
Super Secret Fort!

Internet!

AIR GAP!

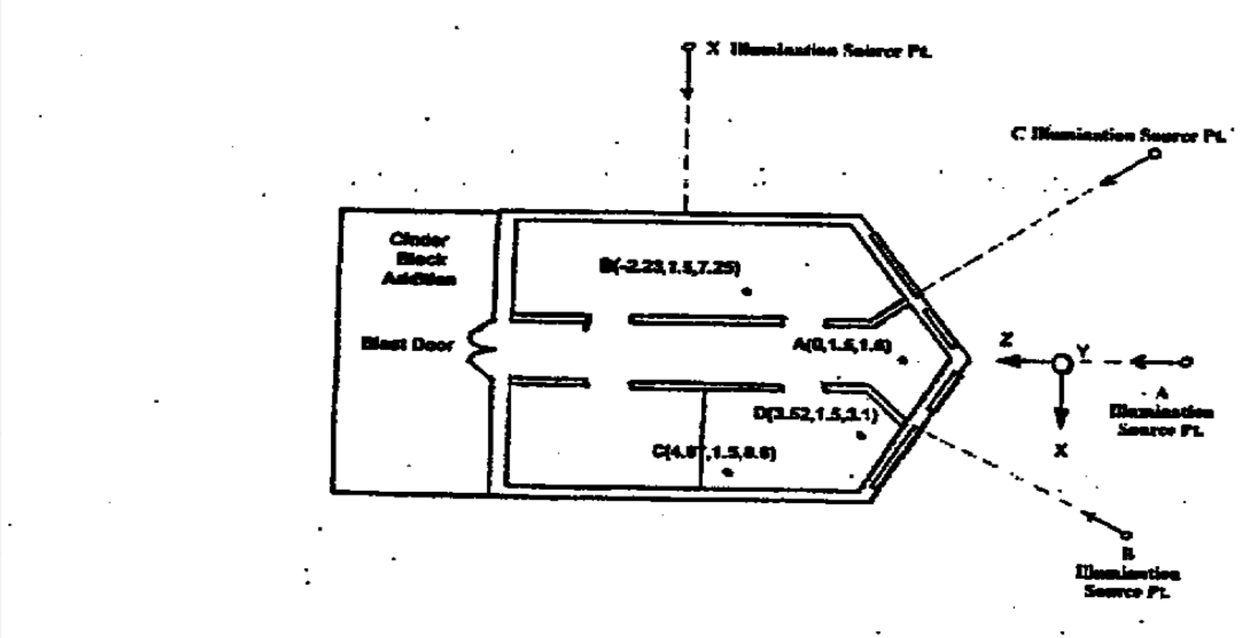


Figure 2. Diagram of Building 12500 at the A-15A Site on Elgin Air Force Base,

Super Secret Fort!

Measurement of RF Propagation into Concrete Structures over the Frequency Range 100 MHZ to 3 GHz

by

Clayborne D. Taylor
Samuel J. Gutierrez
Steven L. Langdon
Kenneth L. Murphy
William A. Walton, III

Phillips Laboratory/WSM
3550 Aberdeen Ave. SE
Kirtland AFB, NM 87117-5776

ISBN 9781461378617

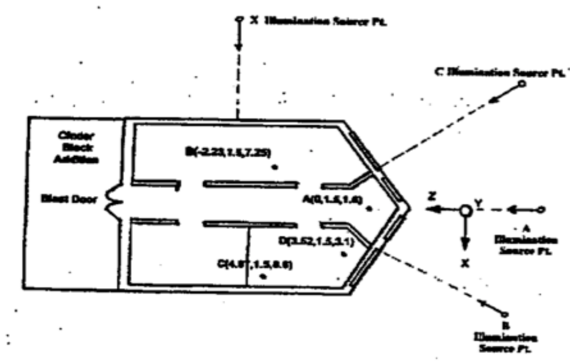


Figure 2. Diagram of Building 12500 at the A-15A Site on Elgin Air Force Base,

Say you wanted to Funtenna out of a
2-ft reinforced concrete structure

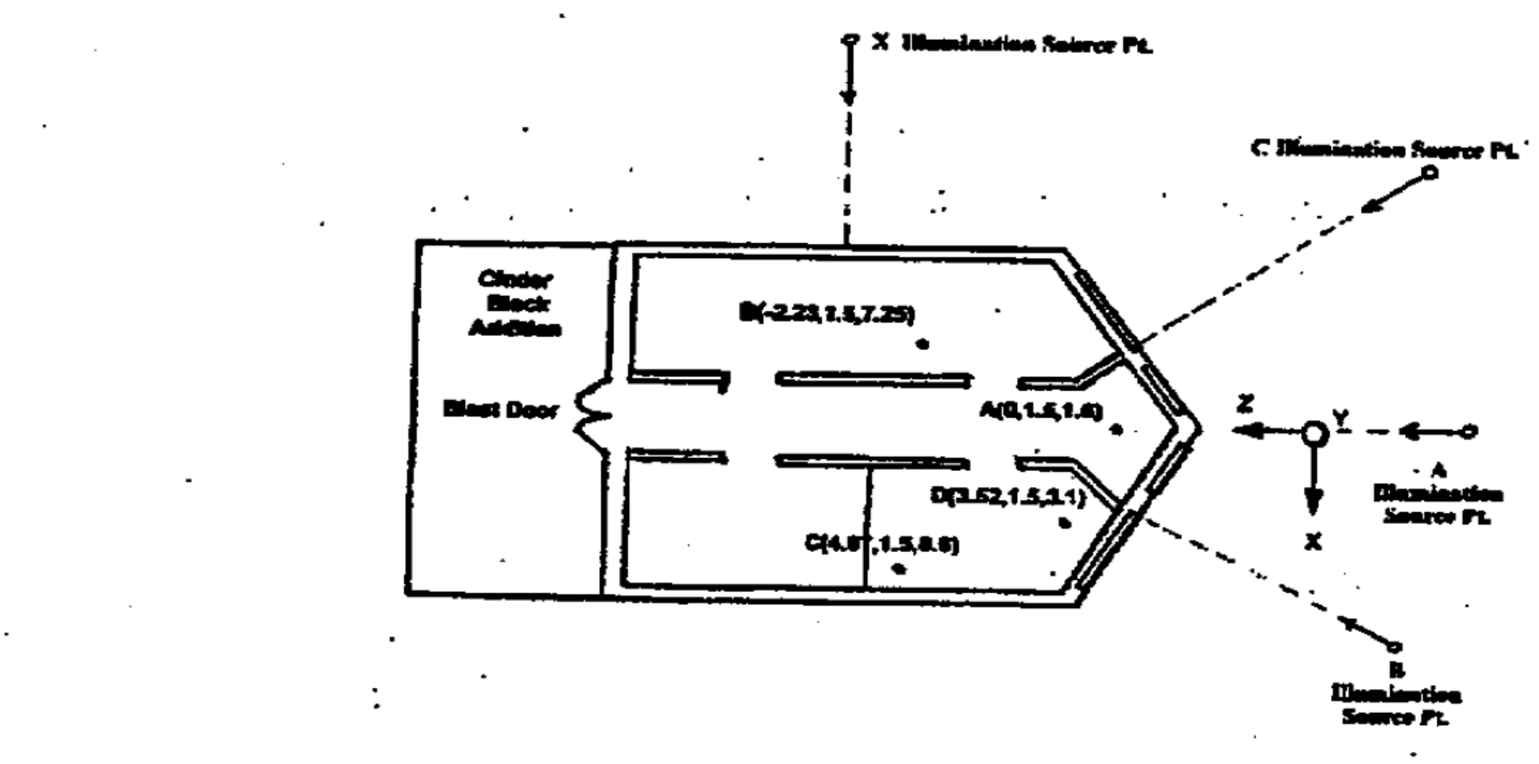


Figure 2. Diagram of Building 12500 at the A-15A Site on Elgin Air Force Base,

ISBN 9781461378617

Say you wanted to Funtenna out of a
2-ft reinforced concrete structure

ISBN 9781461378617

structures. For two-feet thick concrete walls, the measured attenuation above 200 MHz appears to increase with an increase in frequency. And for frequencies near and below 100 MHz, rebar attenuation becomes significant and seems to affect the magnetic field more than the electric field penetration. In the frequency range between 120 and 205 MHz the attenuation is often less than 20 dB. For four-inch and eight-inch thick walls the attenuation is much less (see Table 3).

F <= 100Mhz, bad for magnetic field penetration

F >= 200Mhz, bad for electric field penetration

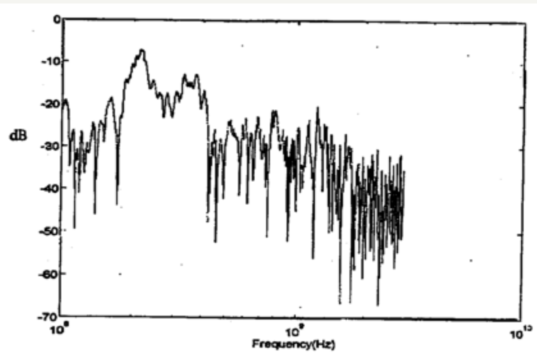


Figure 5. The internal electric field (E_y) at measurement point B relative to the incident electric field for illuminating source point X.

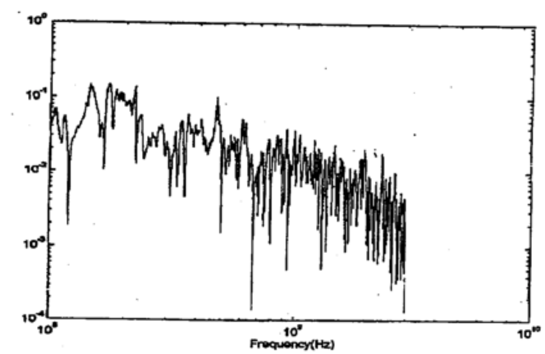
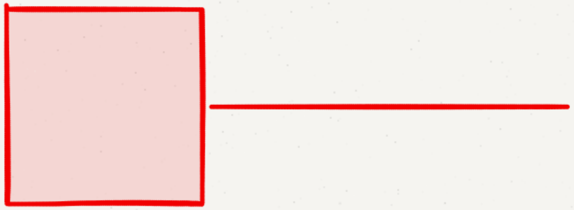
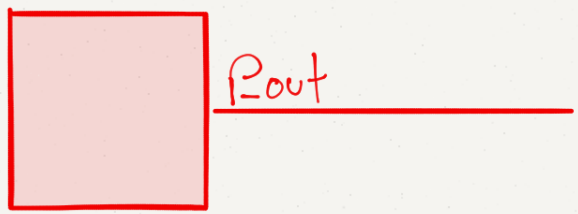


Figure 4. The internal magnetic field (H_z) at measurement point B relative to the incident magnetic field for illumination source point X.

Generalized Funtenna Algorithm



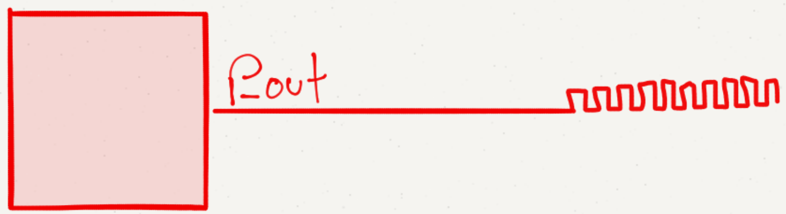
Generalized Funtenna Algorithm



P_out → 1
Delay(x)
P_out → 0
Delay(x)

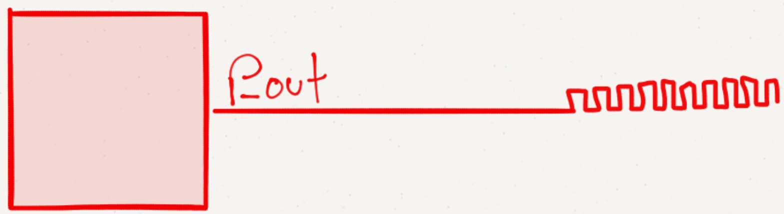
Generalized Funtenna Algorithm

P_out → 1
Delay(x_1)
P_out → 0
Delay(x_1)



Generalized Funtenna Algorithm

$$\left.\begin{array}{l} P\_out \to 1 \\ Delay(d_1) \\ P\_out \to 0 \\ Delay(d_1) \end{array}\right] f = X$$



Generalized Funtenna Algorithm

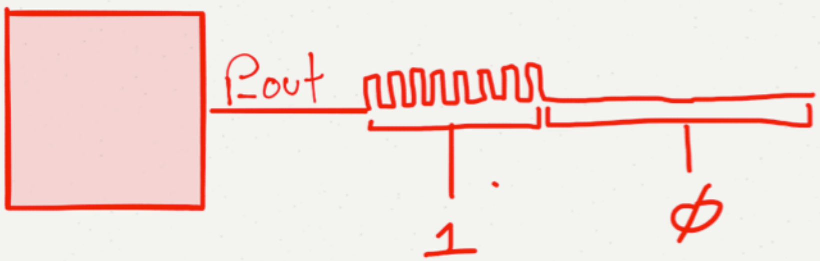
Do "Symbol Duration" Times

$$\left.\begin{array}{l} P\_out \rightarrow 1 \\ Delay(d_1) \\ P\_out \rightarrow \emptyset \\ Delay(d_1) \end{array}\right] f = X$$

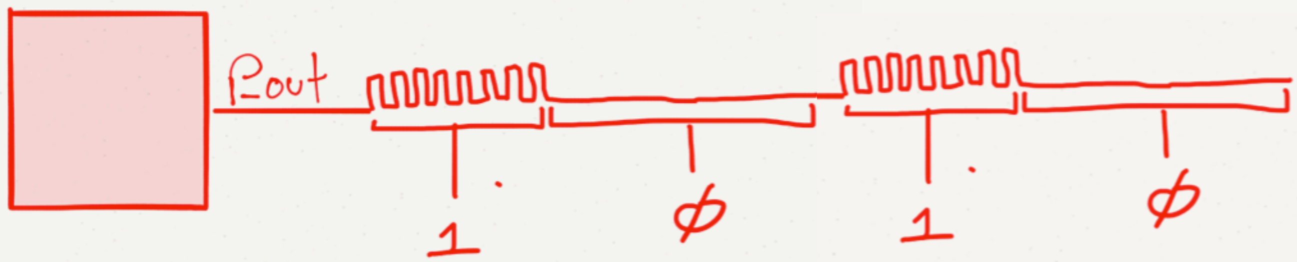
Generalized Funtenna Algorithm

- ASK (Amplitude Shift Keying)
- FSK (Frequency Shift Keying)
- OOK (On-Off Keying)

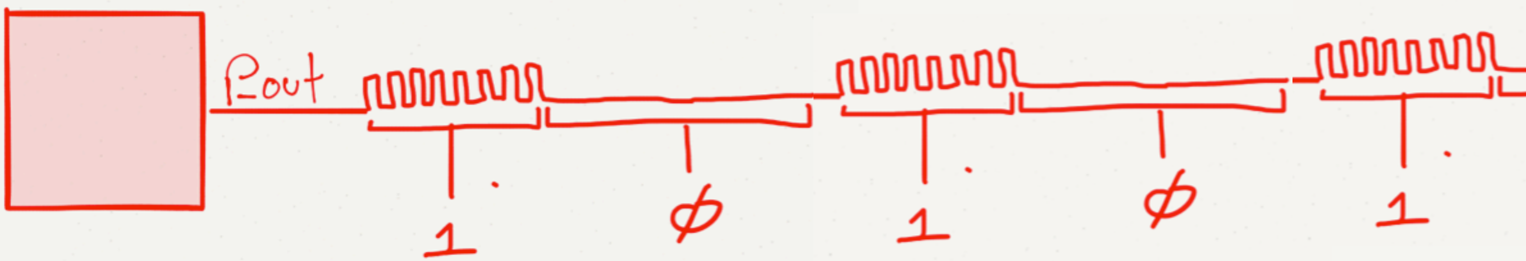
Generalized Funtenna Algorithm
Amplitude-Shift Keying



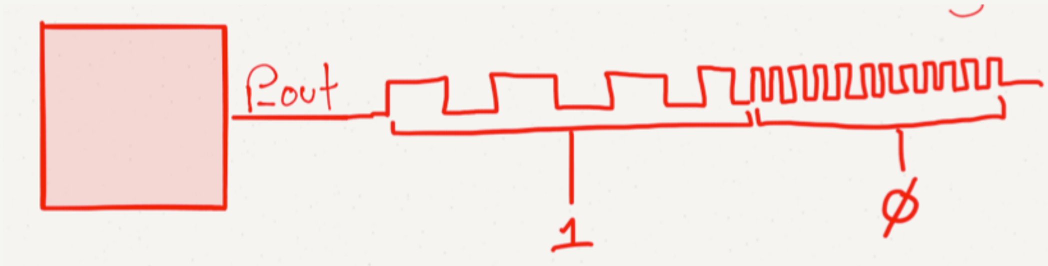
Generalized Funtenna Algorithm
Amplitude-Shift Keying



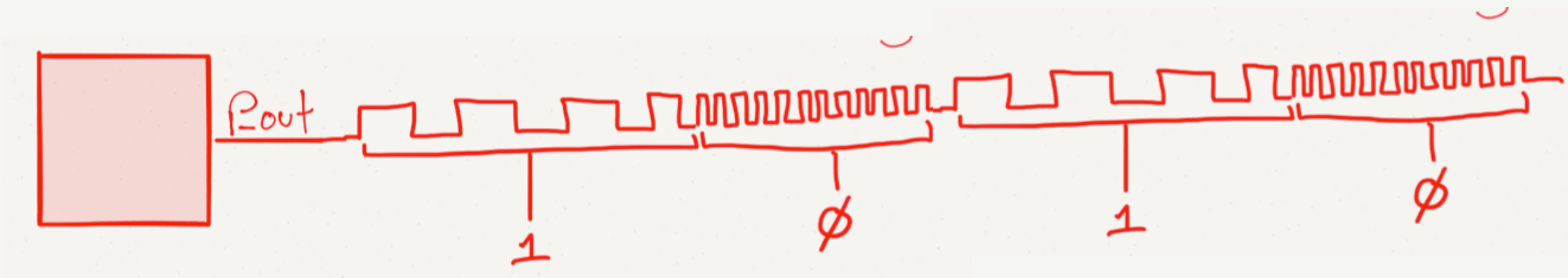
Generalized Funtenna Algorithm
Amplitude-Shift Keying



Generalized Funtenna Algorithm
Frequency-Shift Keying (sort of)

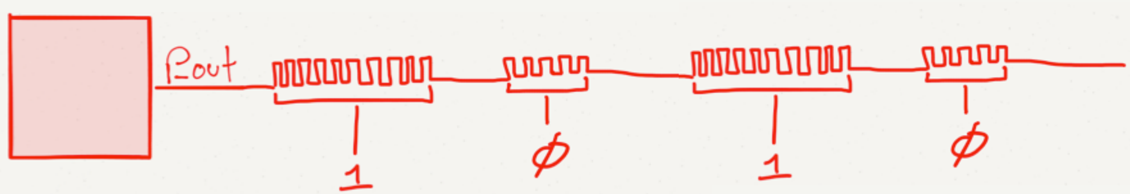


Generalized Funtenna Algorithm
Frequency-Shift Keying (sort of)

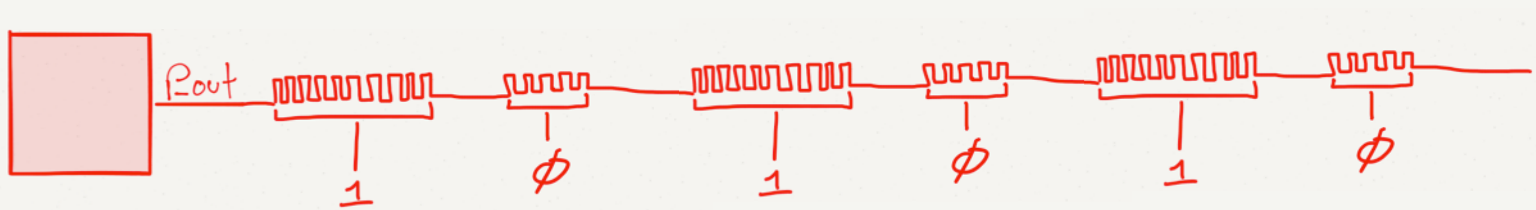


Generalized Funtenna Algorithm
On-Off Keying

Generalized Funtenna Algorithm
On-Off Keying



Generalized Funtenna Algorithm
On-Off Keying



Funtenna In Practice

Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

113 reviews

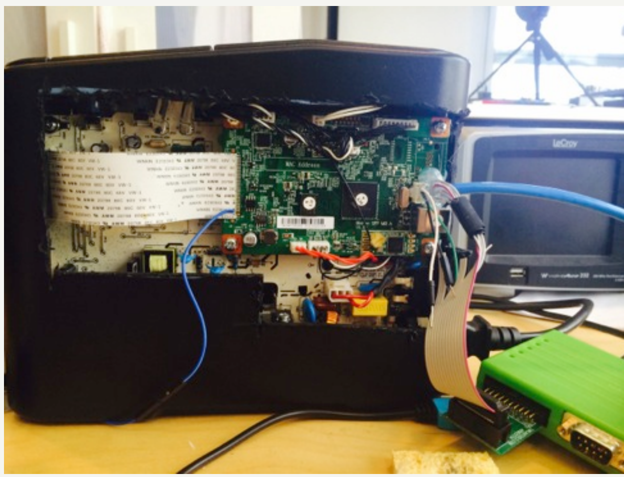
Stores

Newegg.com	Free shipping, no tax - **$39.99**
eBay	Free shipping, no tax - **$53.00**

View all stores and prices »

Funtenna In Practice

Pantum P2502W Wireless Monochrome
Laser Printer

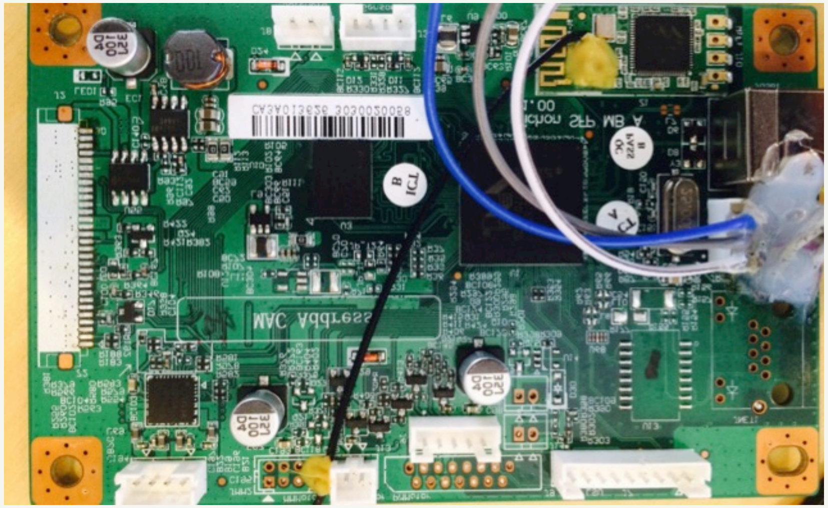


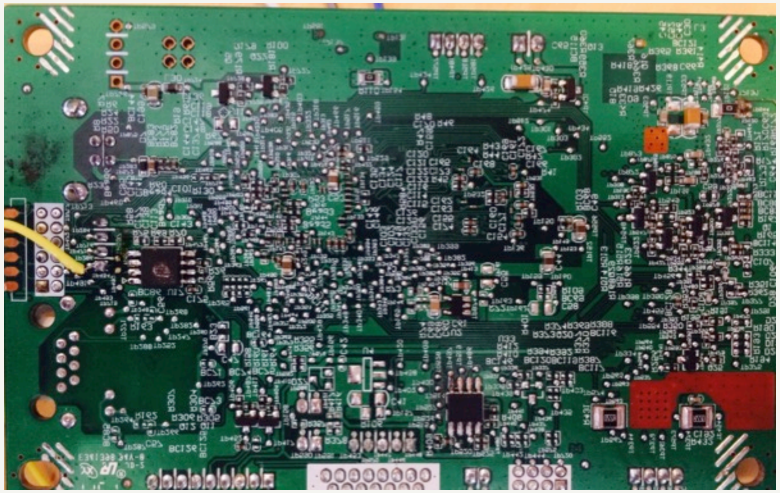
1. Cheap
2. Typical ARM SoC
3. GPIO (lots)
4. PWM
5. UART
6. JTAG

Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

The Controller Board



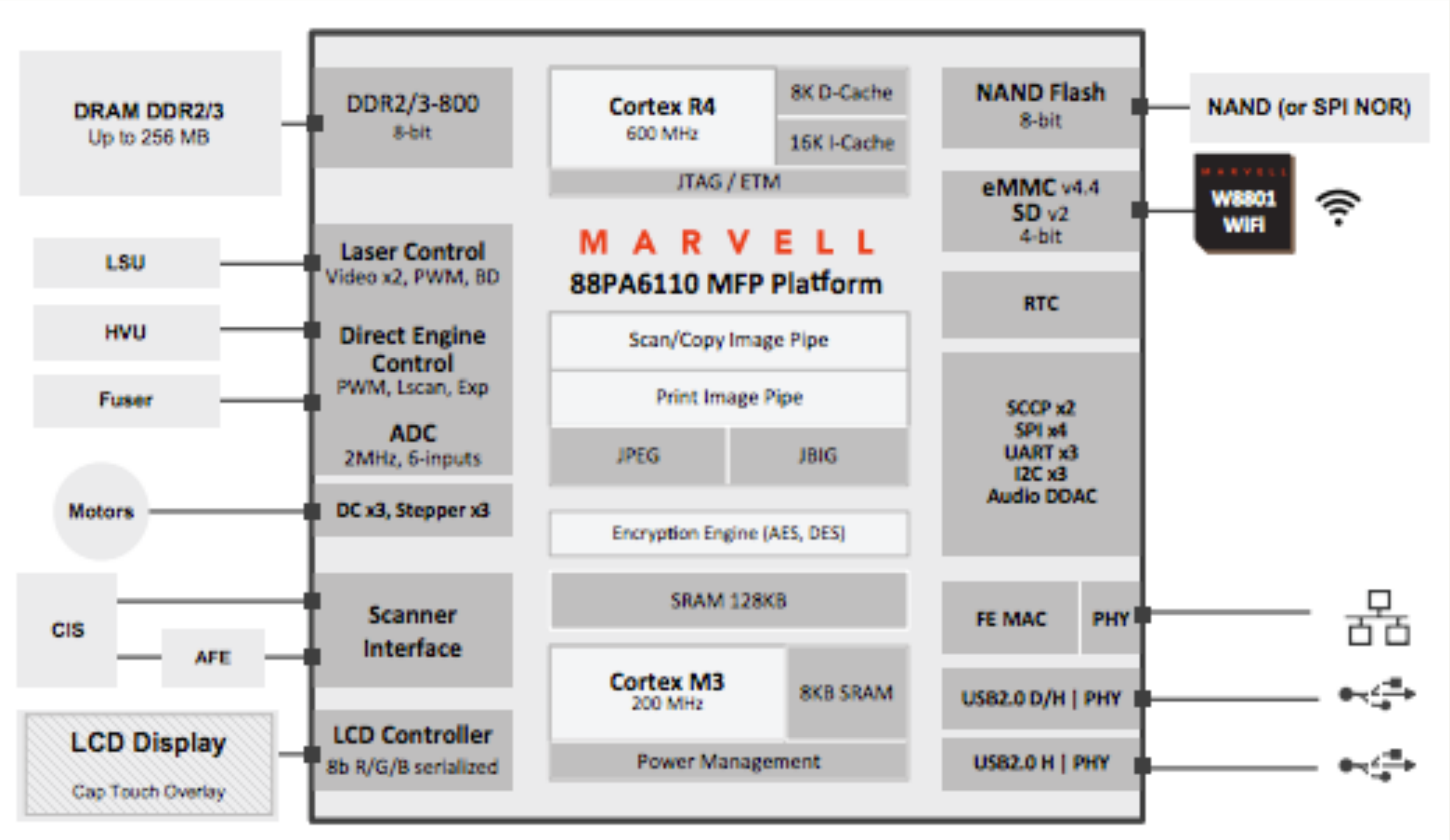


Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

The SoC

Marvell 88PA6110



The product brief
http://www.marvell.com/printers/assets/Printer_88PA6110-01_pb_FINAL.pdf

Funtenna In Practice

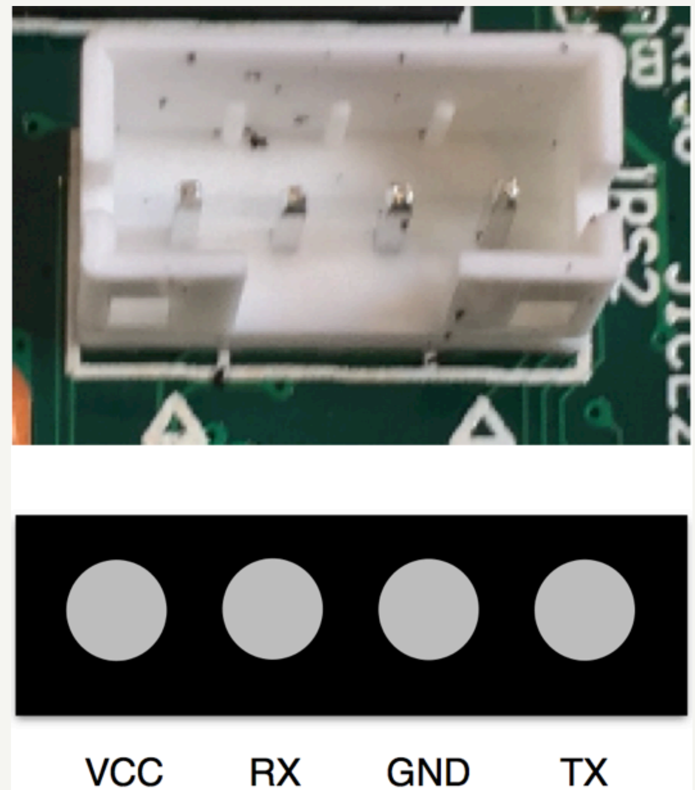
Pantum P2502W Wireless Monochrome Laser Printer

Hardware Triage

Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

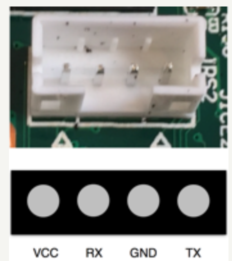
Hardware Triage

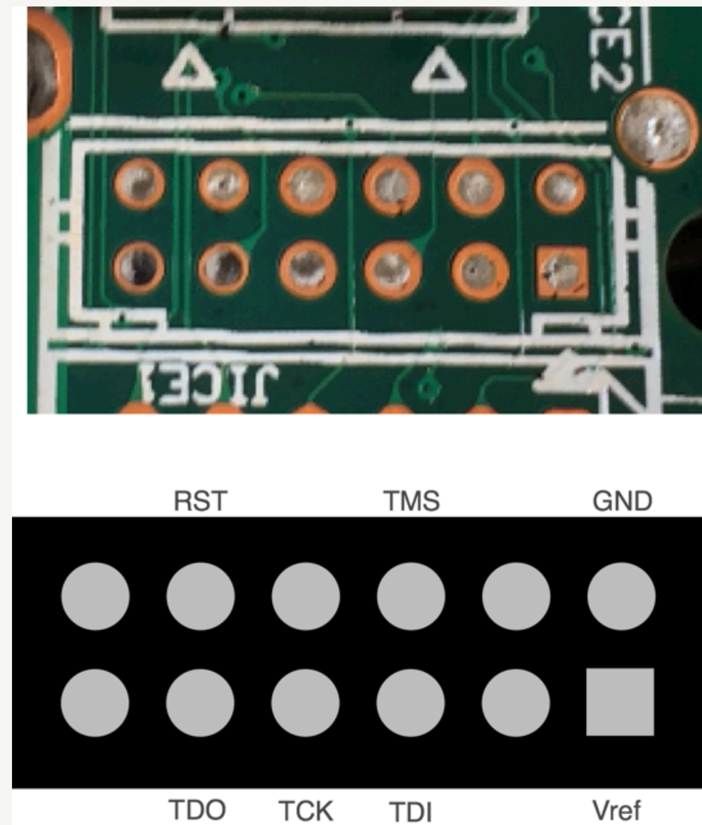


Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

Hardware Triage





Funtenna In Practice (PWM)

Pantum P2502W Wireless Monochrome Laser Printer

13Khz PWM

Funtenna In Practice (PWM)

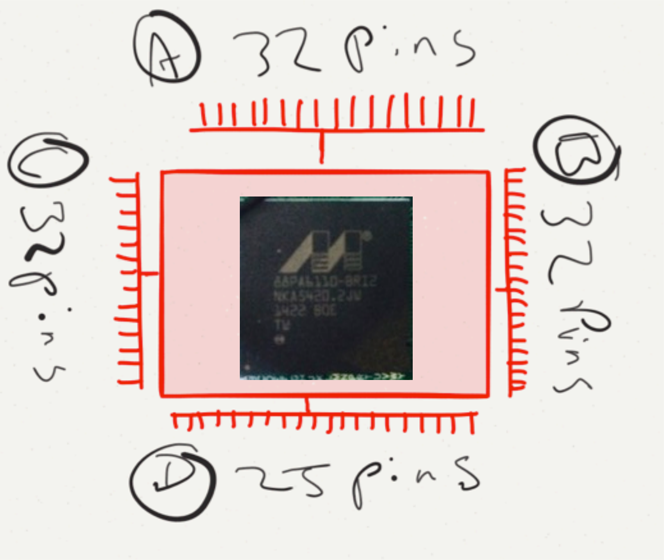
Pantum P2502W Wireless Monochrome Laser Printer

13Khz PWM

No love -(

Funtenna In Practice (GPIO)

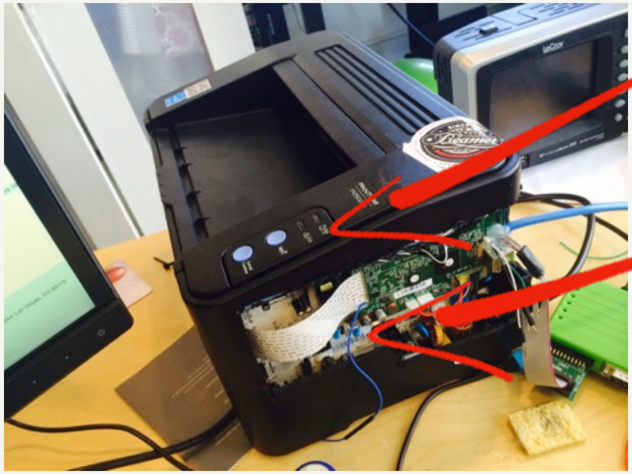
4 GPIO Banks, 121 pins in all



Funtenna In Practice (GPIO)

Input pins: Buttons, few sensors, switches

Funtenna In Practice (GPIO)



Output pins: LEDs, Engine Control, Power Control, Fuser Control, Toner Control and lots more!

Funtenna In Practice (GPIO)

Which pin to flip?

"Emanate like a"

~~Scrub~~

BØSS!

Funtenna In Practice (GPIO)

Which pin to flip? Every pin, at the same time!

Funtenna In Practice (GPIO)

OFF

On

Which pin to flip? Every pin, at the same time!

```
FD040000  8021D3FB 80[illegible]05058 80407C08 8021D3FB  ..!.XP...|@...!.
FD040010  00000300 00000000 FFFE3C07 00000000  ..........<.....
FD040020  00000000 00000000 00000000 00000000  ................
FD040030  00000000 00000000 00000000 00000000  ................
FD040040  00000000 00000000 00000000 00000000  ................
FD040050  00000000 00000000 00000000 00000000  ................
FD040060  00000000 00000000 00000000 00000000  ................
FD040070  00000000 00000000 00000000 00000000  ................
```

GPIO Bank A – Memory Mapped Control Registers

0x20 - Pin OFF

0x24 - Pin On

Funtenna In Practice (GPIO)

```
.equ all_p1mp, 0xffffffff
.equ gpio_bank_a_off_addr, 0xFD040020
.equ gpio_bank_b_off_addr, 0xF8040020
.equ gpio_bank_c_off_addr, 0xF8041020
.equ gpio_bank_d_off_addr, 0xF8042020
_loopy:
    LDR     R5, =all_p1mp
    LDR     R1, =gpio_bank_a_off_addr
    LDR     R2, =gpio_bank_b_off_addr
    LDR     R3, =gpio_bank_c_off_addr
    LDR     R4, =gpio_bank_d_off_addr
```

Funtenna In Practice (GPIO)

```
.equ all_p1mp, 0xffffffff
.equ gpio_bank_a_off_addr, 0xFD040020
.equ gpio_bank_b_off_addr, 0xF8040020
.equ gpio_bank_c_off_addr, 0xF8041020
.equ gpio_bank_d_off_addr, 0xF8042020
_loopy:
    LDR     R5, =all_p1mp
    LDR     R1, =gpio_bank_a_off_addr
    LDR     R2, =gpio_bank_b_off_addr
    LDR     R3, =gpio_bank_c_off_addr
    LDR     R4, =gpio_bank_d_off_addr
```

```
    STR     R5, [R1, #0x4]
    STR     R5, [R2, #0x4]
    STR     R5, [R3, #0x4]
    STR     R5, [R4, #0x4]
```

All Pins on

Funtenna In Practice (GPIO)

```
.equ all_p1mp, 0xffffffff
.equ gpio_bank_a_off_addr, 0xFD040020
.equ gpio_bank_b_off_addr, 0xF8040020
.equ gpio_bank_c_off_addr, 0xF8041020
.equ gpio_bank_d_off_addr, 0xF8042020
_loopy:
    LDR     R5, =all_p1mp
    LDR     R1, =gpio_bank_a_off_addr
    LDR     R2, =gpio_bank_b_off_addr
    LDR     R3, =gpio_bank_c_off_addr
    LDR     R4, =gpio_bank_d_off_addr
```

```
    STR     R5, [R1, #0x4]
    STR     R5, [R2, #0x4]
    STR     R5, [R3, #0x4]
    STR     R5, [R4, #0x4]
```

```
    STR     R5, [R1]
    STR     R5, [R2]
    STR     R5, [R3]
    STR     R5, [R4]
```

All Pins off

Funtenna In Practice (GPIO)

```
.equ all_p1mp, 0xffffffff
.equ gpio_bank_a_off_addr, 0xFD040020
.equ gpio_bank_b_off_addr, 0xF8040020
.equ gpio_bank_c_off_addr, 0xF8041020
.equ gpio_bank_d_off_addr, 0xF8042020
_loopy:
    LDR     R5, =all_p1mp
    LDR     R1, =gpio_bank_a_off_addr
    LDR     R2, =gpio_bank_b_off_addr
    LDR     R3, =gpio_bank_c_off_addr
    LDR     R4, =gpio_bank_d_off_addr
```

```
    STR     R5, [R1, #0x4]
    STR     R5, [R2, #0x4]
    STR     R5, [R3, #0x4]
    STR     R5, [R4, #0x4]
```

All Pins on

```
    STR     R5, [R1]
    STR     R5, [R2]
    STR     R5, [R3]
    STR     R5, [R4]
```

Funtenna In Practice (GPIO)

```
.equ all_p1mp, 0xffffffff
.equ gpio_bank_a_off_addr, 0xFD040020
.equ gpio_bank_b_off_addr, 0xF8040020
.equ gpio_bank_c_off_addr, 0xF8041020
.equ gpio_bank_d_off_addr, 0xF8042020
_loopy:
    LDR     R5, =all_p1mp
    LDR     R1, =gpio_bank_a_off_addr
    LDR     R2, =gpio_bank_b_off_addr
    LDR     R3, =gpio_bank_c_off_addr
    LDR     R4, =gpio_bank_d_off_addr
```

```
    STR     R5, [R1, #0x4]
    STR     R5, [R2, #0x4]
    STR     R5, [R3, #0x4]
    STR     R5, [R4, #0x4]
```

All Pins on

F = Approx 5mhz

```
    STR     R5, [R1]
    STR     R5, [R2]
    STR     R5, [R3]
    STR     R5, [R4]
```

Funtenna In Practice (GPIO)

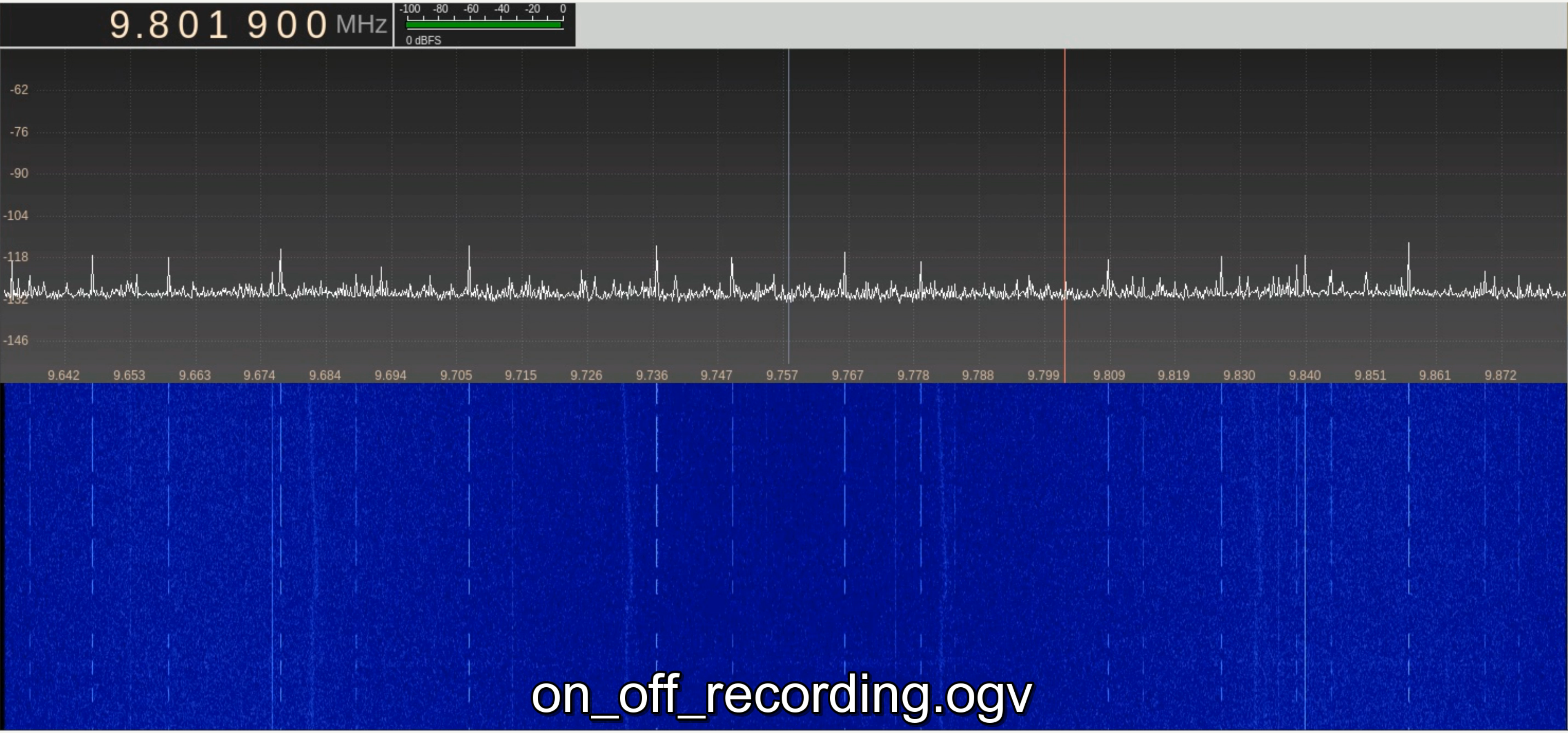
F = Approx 5mhz

And things get really interesting

Funtenna In Practice

Funtenna Demo 2: ALL GPIO Funtenna - On Off Keying

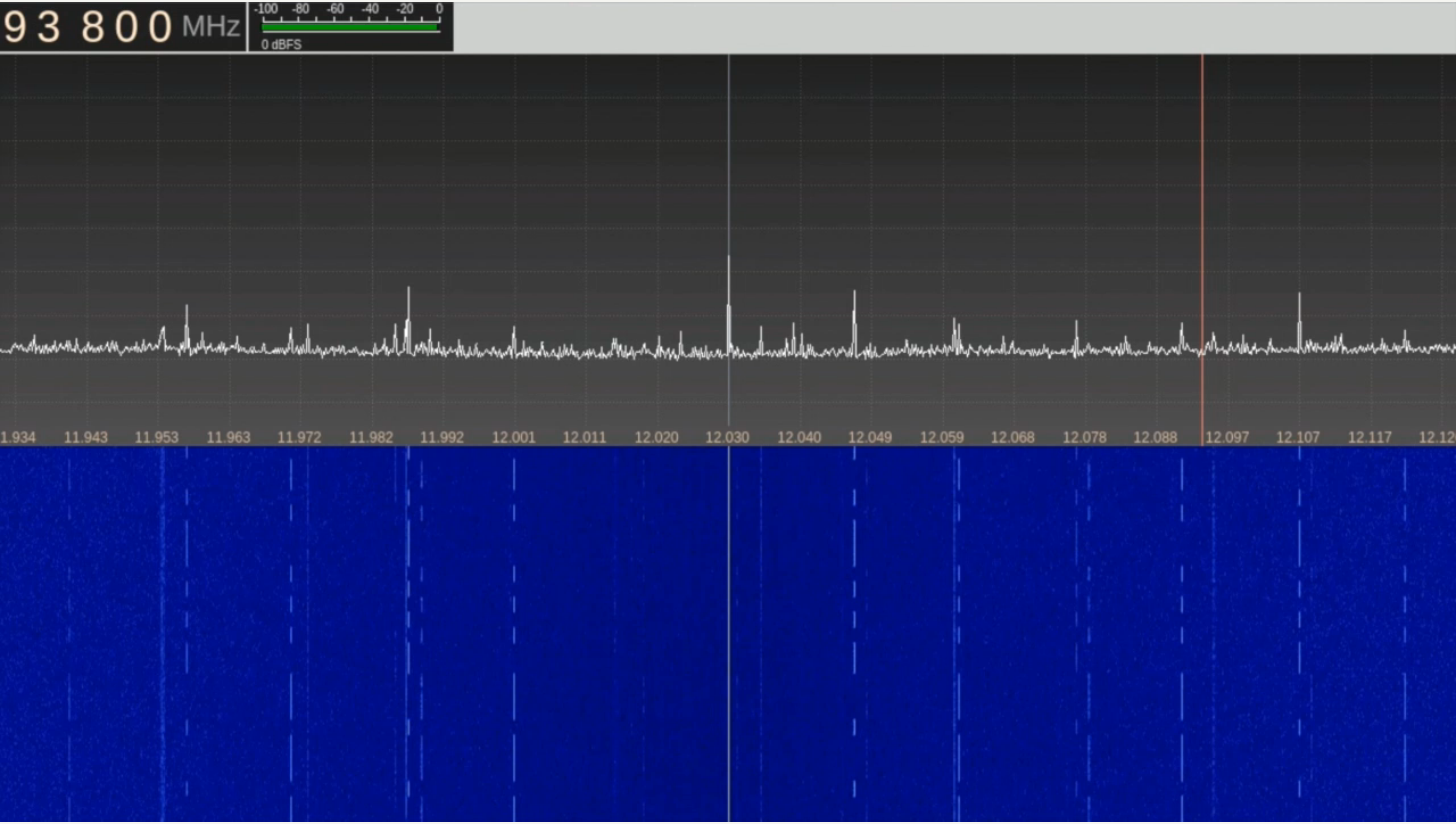
Funtenna Demo 2: ALL GPIO Funtenna - On Off Keying



Funtenna In Practice

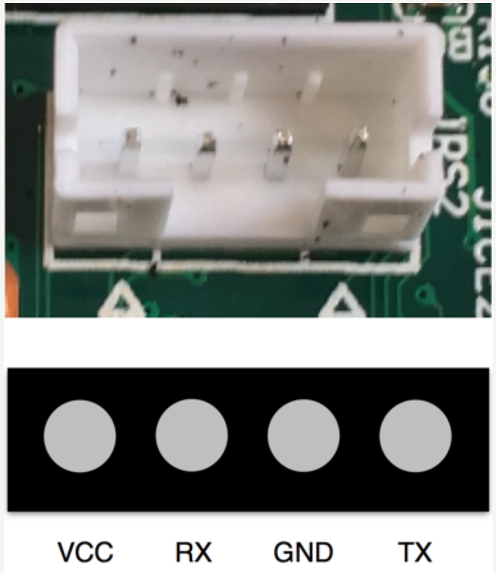
Funtenna Demo 2: ALL GPIO Funtenna - Freq Shift Keying (sort of)

Funtenna Demo 2: ALL GPIO Funtenna - Freq Shift Keying (sort of)



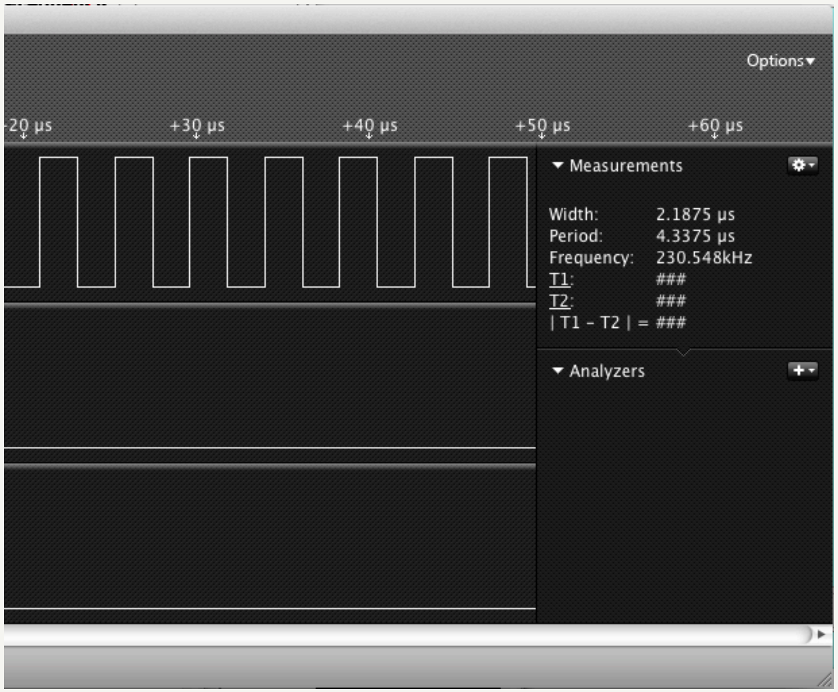
Funtenna In Practice

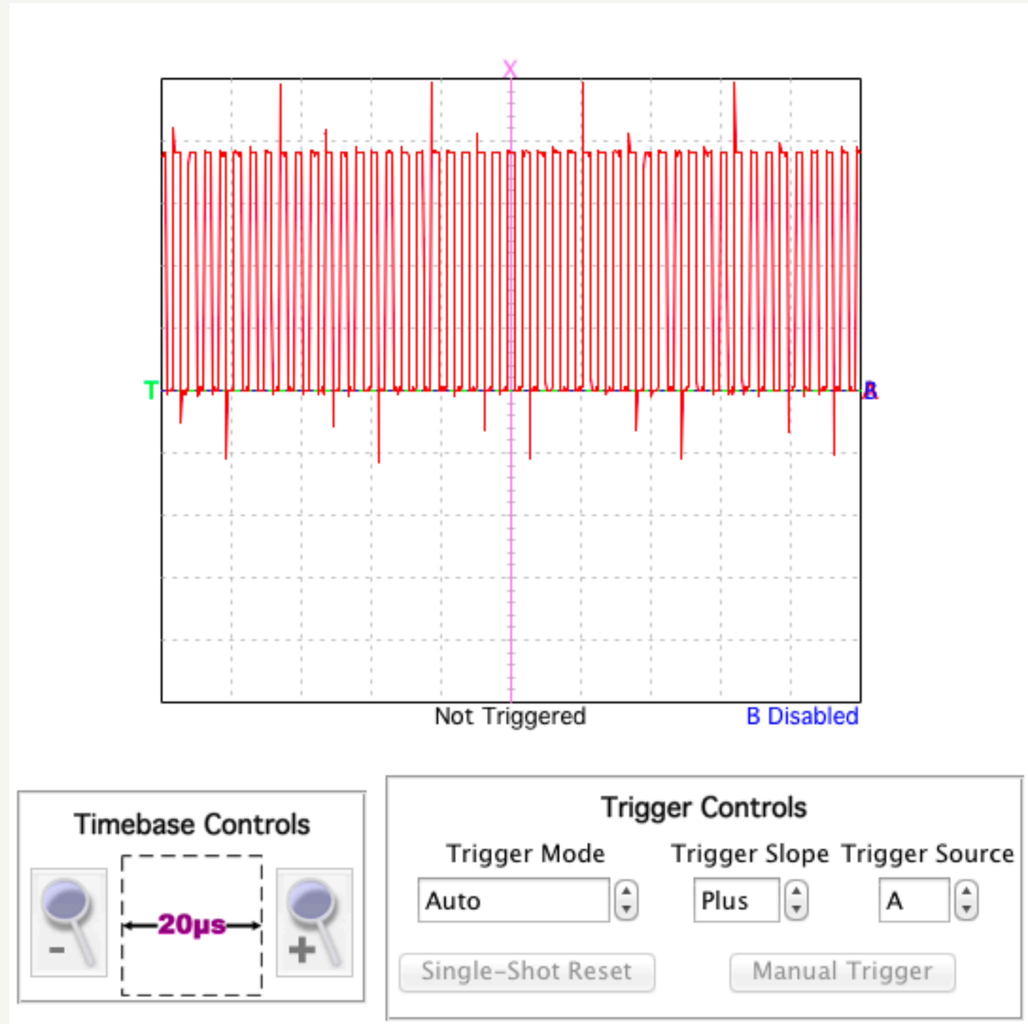
Pantum P2502W Wireless Monochrome Laser Printer



UART Funtenna

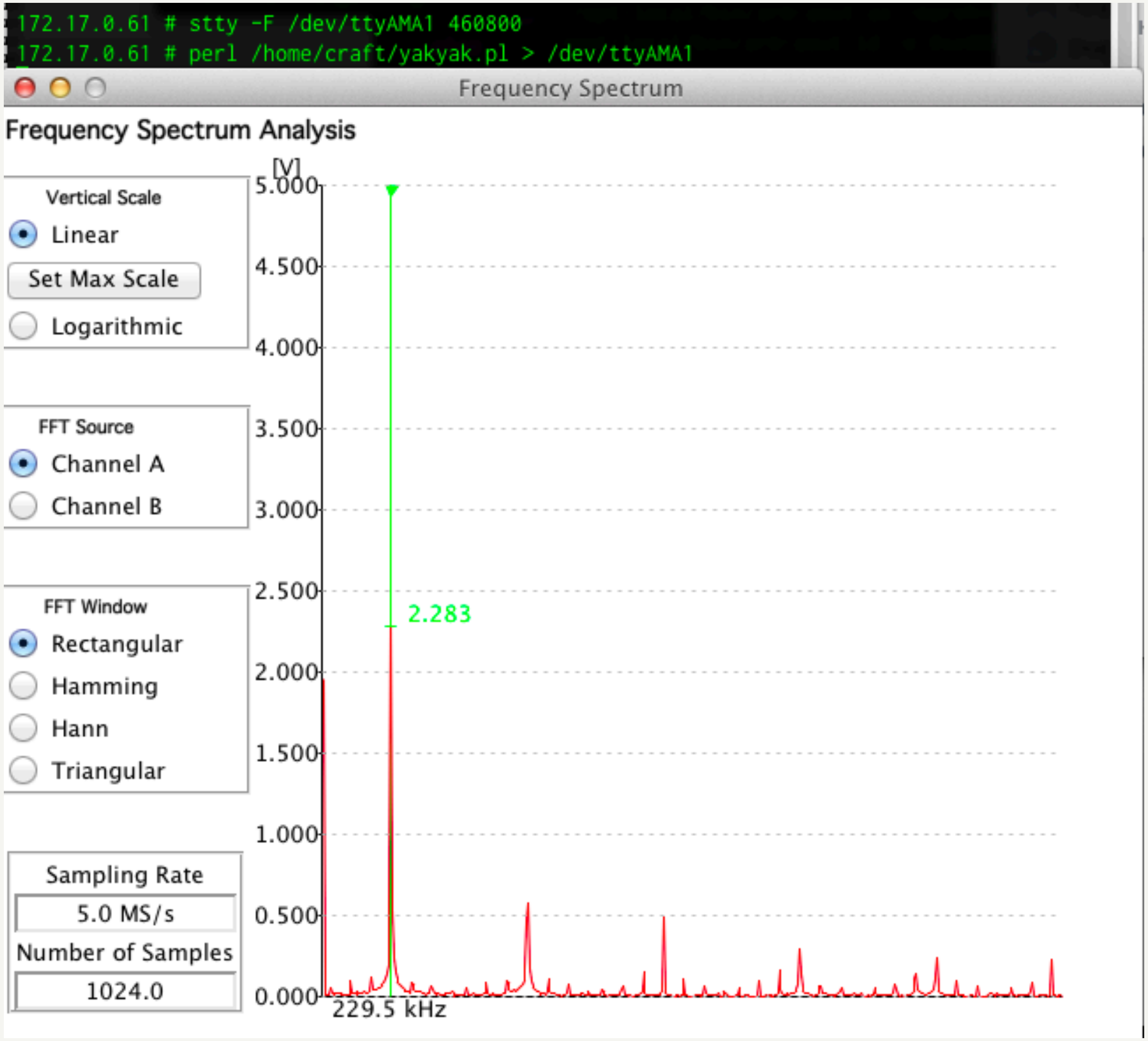
UART Funtenna 460800 baud



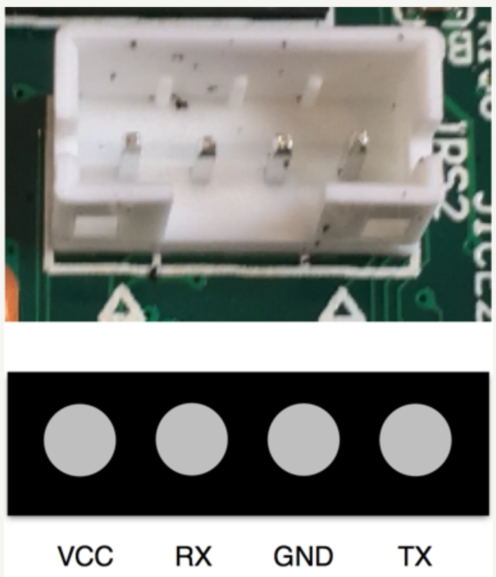


"UUUUUUUUUUUUU"

UART Funtenna 460800 baud



Funtenna In Practice

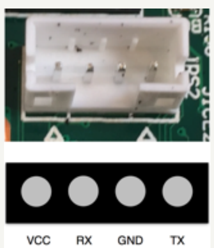


Let's be more sneaky…

Funtenna In Practice

```
LDR          R3, =asc_1121944 ; "/home/lihaixiong/source/common/devices/"...
BL           sub_49F668
MOV          R3, R0
MOV          R2, R3
LDR          R3, =dword_EC6
STR          R2, [R3]

asc_1121944      DCB "/home/lihaixiong/source/common/dev"
                 DCB "ices/uart/dwapb/src/dw_apb_uart.c",0
```



dw_apb_uart.c

Funtenna In Practice

SYNOPSYS®

DesignWare DW_apb_uart Databook

DesignWare Synthesizable Components for AMBA 2
DW_apb_uart

dw_apb_uart.c

Funtenna In Practice

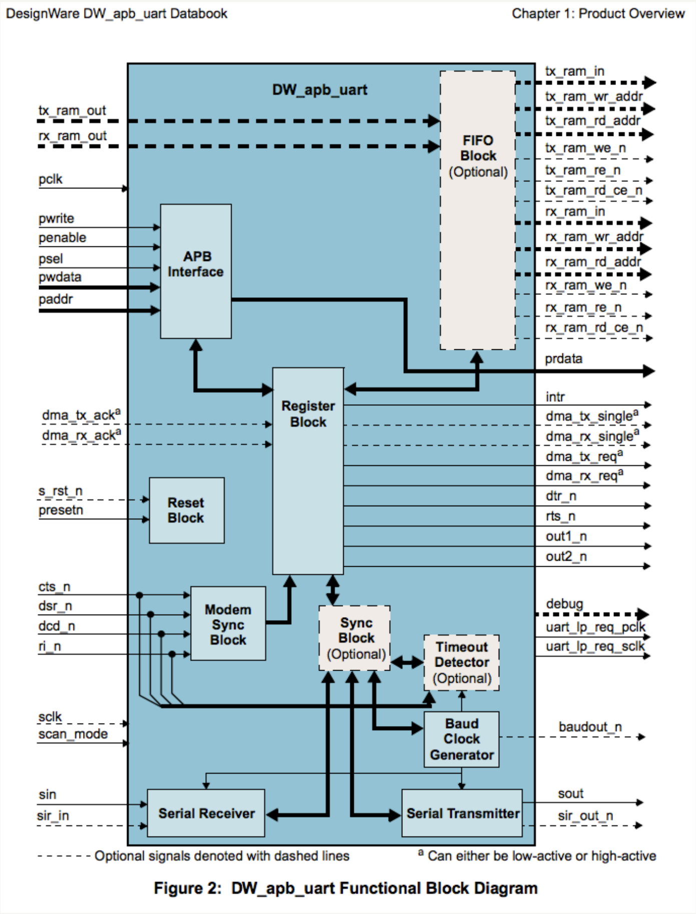
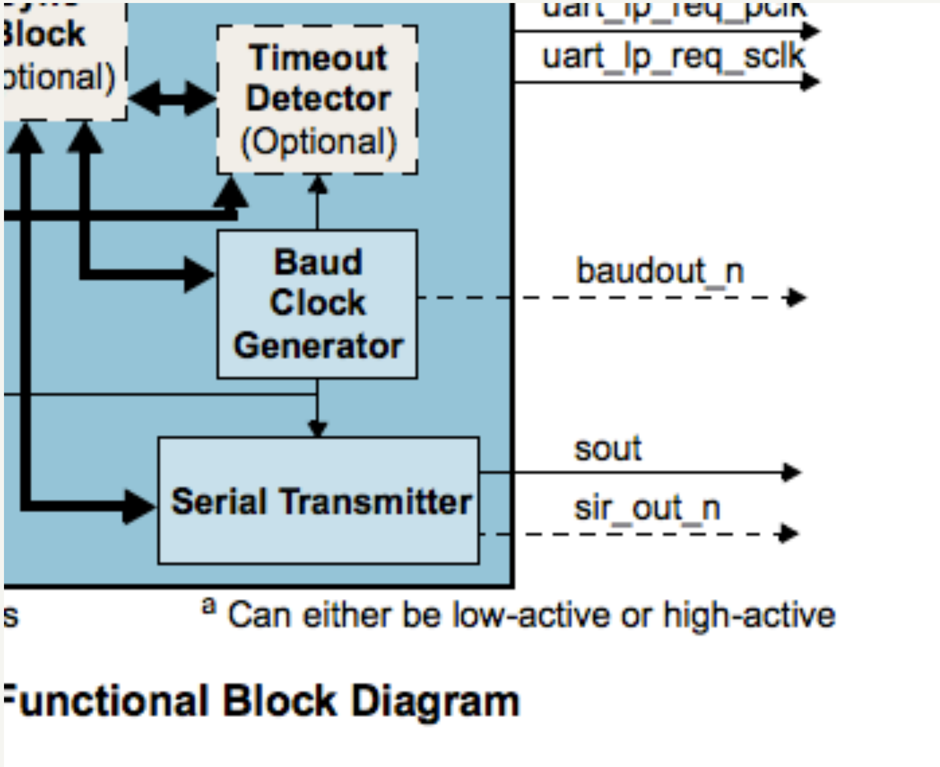


Figure 2: DW_apb_uart Functional Block Diagram

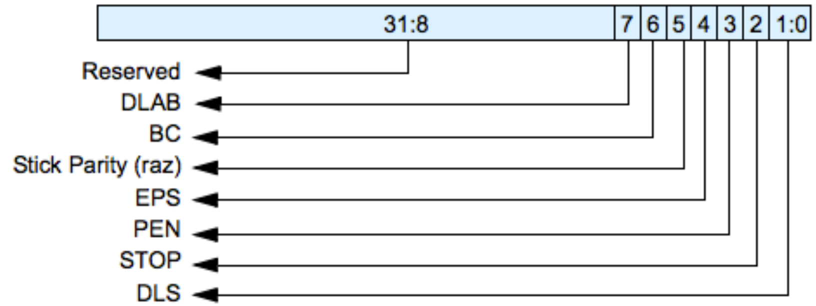


FLIP sout pin

Step 1: UART Break-Ctrl Bit -> 1

LCR

- **Name:** Line Control Register
- **Size:** 32 bits
- **Address Offset:** 0x0C
- **Read/write access:** read/write



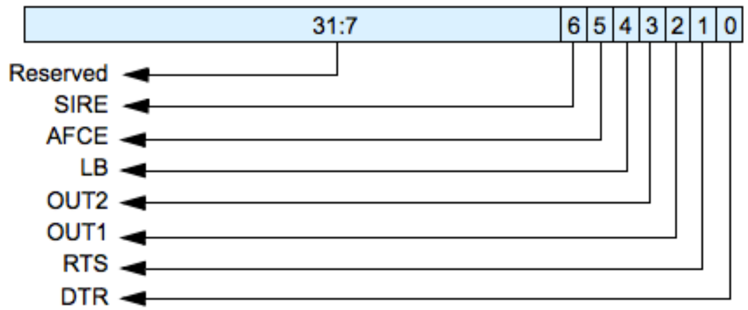
6	Break (or BC)	R/W	Break Control Bit. This is used to cause a break condition to be transmitted to the receiving device. If set to one the serial output is forced to the spacing (logic 0) state. When not in Loopback Mode, as determined by MCR[4], the sout line is forced low until the Break bit is cleared. If SIR_MODE == Enabled and active (MCR[6] set to one) the sir_out_n line is continuously pulsed. When in Loopback Mode, the break condition is internally looped back to the receiver and the sir_out_n line is forced low. **Reset Value:** 0x0

FLIP sout pin

Step 2: UART Loopback bit -> 1

MCR

- **Name:** Modem Control Register
- **Size:** 32 bits
- **Address Offset:** 0x10
- **Read/write access:** read/write



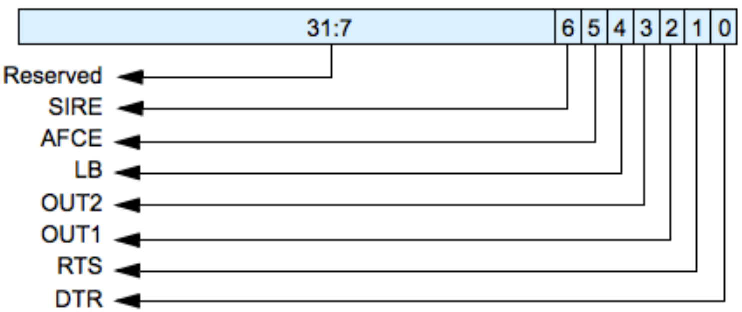
4	LoopBack (or LB)	R/W	LoopBack Bit. This is used to put the UART into a diagnostic mode for test purposes. If operating in UART mode (SIR_MODE != Enabled or not active, MCR[6] set to zero), data on the sout line is held high, while serial data output is looped back to the sin line, internally. In this mode all the interrupts are fully functional. Also, in loopback mode, the modem control inputs (dsr_n, cts_n, ri_n, dcd_n) are disconnected and the modem control outputs (dtr_n, rts_n, out1_n, out2_n) are looped back to the inputs, internally. If operating in infrared mode (SIR_MODE == Enabled AND active, MCR[6] set to one), data on the sir_out_n line is held low, while serial data output is inverted and looped back to the sir_in line. **Reset Value:** 0x0

FLIP sout pin

Step 3: UART Loopback bit -> 0

MCR

- **Name:** Modem Control Register
- **Size:** 32 bits
- **Address Offset:** 0x10
- **Read/write access:** read/write



4	LoopBack (or LB)	R/W	LoopBack Bit. This is used to put the UART into a diagnostic mode for test purposes. If operating in UART mode (SIR_MODE != Enabled or not active, MCR[6] set to zero), data on the sout line is held high, while serial data output is looped back to the sin line, internally. In this mode all the interrupts are fully functional. Also, in loopback mode, the modem control inputs (dsr_n, cts_n, ri_n, dcd_n) are disconnected and the modem control outputs (dtr_n, rts_n, out1_n, out2_n) are looped back to the inputs, internally. If operating in infrared mode (SIR_MODE == Enabled AND active, MCR[6] set to one), data on the sir_out_n line is held low, while serial data output is inverted and looped back to the sir_in line. **Reset Value:** 0x0

FLIP sout pin

Funtenna In Practice (UART)

```
.equ uart_conf_reg, 0xFD060000

   @ set BREAK bit to force SOUT to low
   MOV     R1, #0x43
   LDR     R2, =uart_conf_reg
   STR     R1, [R2, #0xc]
   MOV     R1, #0x23
   MOV     R3, #0x33
```

```
STR     R1, [R2, #0x10]
```

Uart_sout -> 1

Funtenna In Practice (UART)

```
.equu uart_conf_reg, 0xFD060000

    @ set BREAK bit to force SOUT to low
    MOV     R1, #0x43
    LDR     R2, =uart_conf_reg
    STR     R1, [R2, #0xc]
    MOV     R1, #0x23
    MOV     R3, #0x33
```

```
STR     R1, [R2, #0x10]
```

Uart_sout -> 1

```
STR     R3, [R2, #0x10]
```

Uart_sout ->0

Funtenna In Practice (UART)

```
.equ uart_conf_reg, 0xFD060000

   @ set BREAK bit to force SOUT to low
   MOV     R1, #0x43
   LDR     R2, =uart_conf_reg
   STR     R1, [R2, #0xc]
   MOV     R1, #0x23
   MOV     R3, #0x33
```

```
STR     R1, [R2, #0x10]
```

Uart_sout -> 1

```
STR     R3, [R2, #0x10]
```

Uart_sout ->0

Funtenna In Practice (UART)

```
.equ uart_conf_reg, 0xFD060000

   @ set BREAK bit to force SOUT to low
   MOV     R1, #0x43
   LDR     R2, =uart_conf_reg
   STR     R1, [R2, #0xc]
   MOV     R1, #0x23
   MOV     R3, #0x33
```

```
STR     R1, [R2, #0x10]
```

Uart_sout -> 1

```
STR     R3, [R2, #0x10]
```

Uart_sout ->0

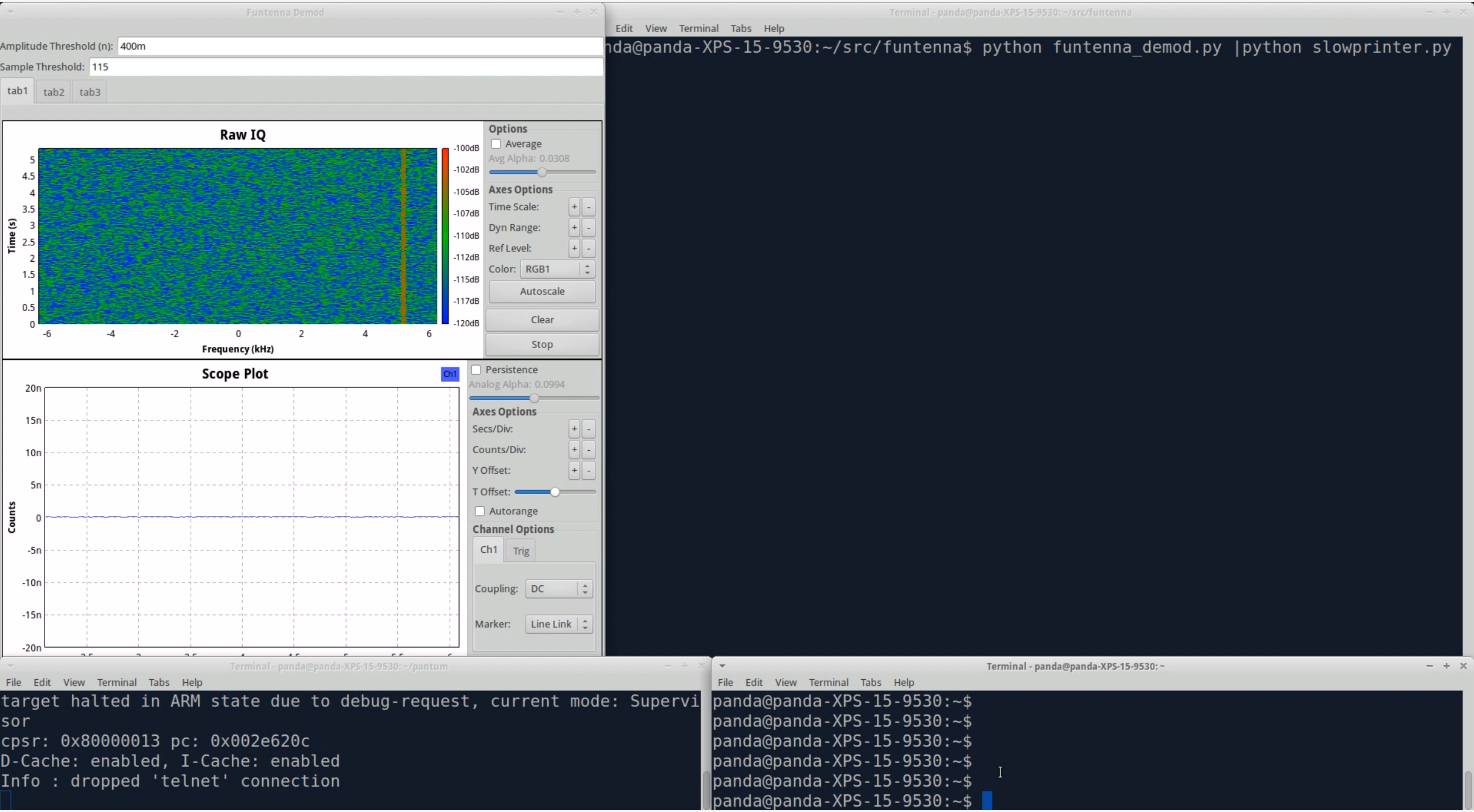
F = Approx 500khz

Funtenna In Practice

Funtenna Demo 2: UART, On Off Keying

UART Pin, 10 feet of console cable

Funtenna Demo 2: UART FUNTENNA DEMOD



Take Away

- Funtenna works
- Network IDS is no substitute for host-based defense
- Host-based embedded defense important!

Big Thanks!

Chris Evans

Big Thanks!

Joseph Pantoga

Big Thanks!

Kang-Wei Chang

www.funtenna.org

Ang Cui, PhD
a@redballoonsecurity.com

Backup slides

Funtenna In Practice (GPIO)

Which pin to flip? Every pin, at the same time!

Memory Mapped Registers

0x1600D58 <- Contains GPIO Bank & Register List

GPIO bank A - 0x1600DA8 MEMREG 0xFD040000
GPIO bank B - 0x16011B8 MEMREG 0xF8040000
GPIO bank C - 0x16015C8 MEMREG 0xF8041000
GPIO bank D - 0x16019D8 MEMREG 0xF8042000

Funtenna In Practice (GPIO)

Which pin to flip? Every pin, at the same time!

Memory Mapped Registers

0x1600D58 <- Contains GPIO Bank & Register List

01600D58	00B315AC	01600DA8	FD040000	00B315C4
01600D68	016011B8	F8040000	00B315DC	016015C8
01600D78	F8041000	00B315F4	016019D8	F8042000

GPIO bank A - 0x1600DA8 MEMREG 0xFD040000
GPIO bank B - 0x16011B8 MEMREG 0xF8040000
GPIO bank C - 0x16015C8 MEMREG 0xF8041000
GPIO bank D - 0x16019D8 MEMREG 0xF8042000

Funtenna In Practice (GPIO)

Which pin to flip? Every pin, at the same time!

Memory Mapped Registers

0x1600D58 <- Contains GPIO Bank & Register List

GPIO bank A - 0x1600DA8 MEMREG 0xFD040000
GPIO bank B - 0x16011B8 MEMREG 0xF8040000
GPIO bank C - 0x16015C8 MEMREG 0xF8041000
GPIO bank D - 0x16019D8 MEMREG 0xF8042000

01600D58	00B315AC	01600DA8	FD040000	00B315C4
01600D68	016011B8	F8040000	00B315DC	016015C8
01600D78	F8041000	00B315F4	016019D8	F8042000

01600DA8	4750494F	01600D58	CDCDCD00	FD040080	OIPGX.`
01600DB8	CDCDCD00	00000000	00000000	CDCDCDCD	....
01600DC8	4750494F	01600D58	CDCDCD00	FD040084	OIPGX.`
01600DD8	CDCDCD00	00000001	00000000	CDCDCDCD	....
01600DE8	4750494F	01600D58	CDCDCD00	FD040088	OIPGX.`
01600DF8	CDCDCD00	00000002	00000000	CDCDCDCD	....
01600E08	4750494F	01600D58	CDCDCD01	FD04008C	OIPGX.`
01600E18	CDCDCD00	00000003	00000000	CDCDCDCD	....
01600E28	4750494F	01600D58	CDCDCD01	FD040090	OIPGX.`
01600E38	CDCDCD00	00000004	00000000	CDCDCDCD	....
01600E48	4750494F	01600D58	CDCDCD00	FD040094	OIPGX.`
01600E58	CDCDCD00	00000005	00000000	CDCDCDCD	....
01600E68	4750494F	01600D58	CDCDCD01	FD040098	OIPGX.`
01600E78	CDCDCD00	00000006	00000001	00000000	....
01600E88	4750494F	01600D58	CDCDCD00	FD04009C	OIPGX.`

GPIO Bank A