# NSA Playset: Bridging the Airgap without Radios

# Speaker Bio

@r00tkillah Michael Leibowitz

- Day job in product security
- Froots around with electronics

- The views expressed.. NOT MY EMPLOYERS!

# ANT Catalog

TOP SECRET//COMINT//REL TO USA, FVEY

## LOUDAUTO

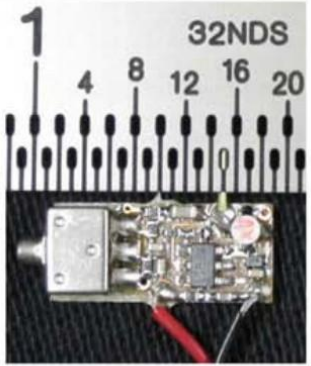
ANT Product Data

07 Apr 2009

(TS//SI//REL TO USA,FVEY) Audio-based RF retro-reflector. Provides room audio from targeted space using radar and basic post-processing.

**(U) Capabilities**

(TS//SI//REL TO USA,FVEY) LOUDAUTO's current design maximizes the gain of the microphone. This makes it extremely useful for picking up room audio. It can pick up speech at a standard, office volume from over 20' away. (NOTE: Concealments may reduce this distance.) It uses very little power (~15 uA at 3.0 VDC), so little, in fact, that battery self-discharge is more of an issue for serviceable lifetime than the power draw from this unit. The simplicity of the design allows the form factor to be tailored for specific operational requirements. All components at COTS and so are non-attributable to NSA.



# ANT Catalog

TS//SI//REL TO USA,FVEY) Room audio is picked up by the microphone and converted into an analog electrical signal. This signal is used to pulse position modulate (PPM) a square wave signal running at a pre-set frequency. This square wave is used to turn a FET (field effect transistor) on and off. When the unit is illuminated with a CW signal from a nearby radar unit, the illuminating signal is amplitude-modulated with the PPM square wave. This signal is re-radiated, where it is picked up by the radar, then processed to recover the room audio. Processing is currently performed by COTS equipment with FM demodulation capability (Rohde & Schwarz FSH-series portable spectrum analyzers, etc.) LOUDAUTO is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

**Unit Cost: $30**

**Status:** End processing still in development

**POC:** [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

# NSA Playset

**Site Information**
- Contributions
- Project Requirements
- Open Problems

**Passive Radio Interception**
- TWILIGHTVEGETABLE (GSM)
- LEVITICUS
- DRIZZLECHAIR
- PORCUPINEMASQUERADE (WiFi)

**Physical Domination**
- SLOTSCREAMER (PCI)
- ADAPTERNOODLE (USB)

**Hardware Implants**
- BROKENGLASS
- CHUCKWAGON
- TURNIPSCHOOL

- CACTUSTUTU
- TINYALAMO (BT)

**RETROREFLECTORS**
- CONGAFLOCK

**Welcome to the home of the NSA Playset.**

In the coming months and beyond, we will release a series of dead simple, easy to use tools to enable the next generation of security researchers. We, the security community have learned a lot in the past couple decades, yet the general public is still ill equipped to deal with real threats that face them every day, and ill informed as to what is possible.

Inspired by the NSA ANT catalog, we hope the NSA Playset will make cutting edge security tools more accessible, easier to understand, and harder to forget. Now you can play along with the NSA!

https://en.wikipedia.org/wiki/NSA_ANT_catalog

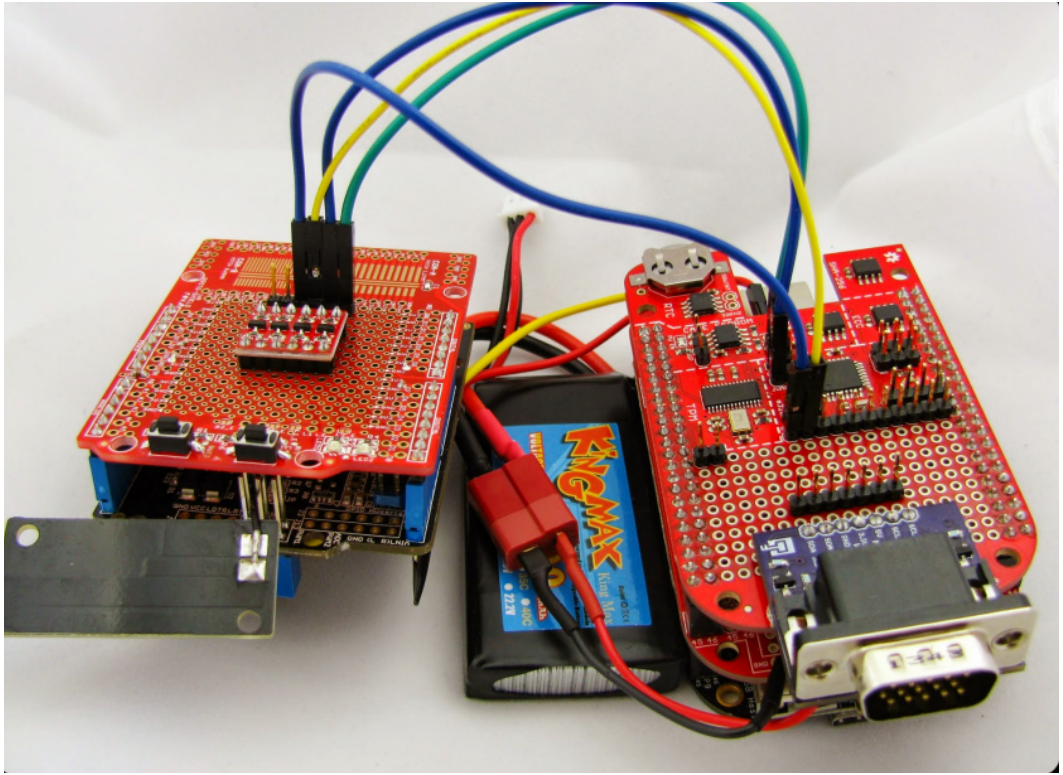
If you feel like you can contribute, please join the discussion here:

https://groups.google.com/forum/#!forum/nsaplayset

Check out Mike's HITB2014 talk here:

http://www.nsaplayset.org/ossmann_hitb2014.pdf

# NSA Playset: CHUCKWAGON



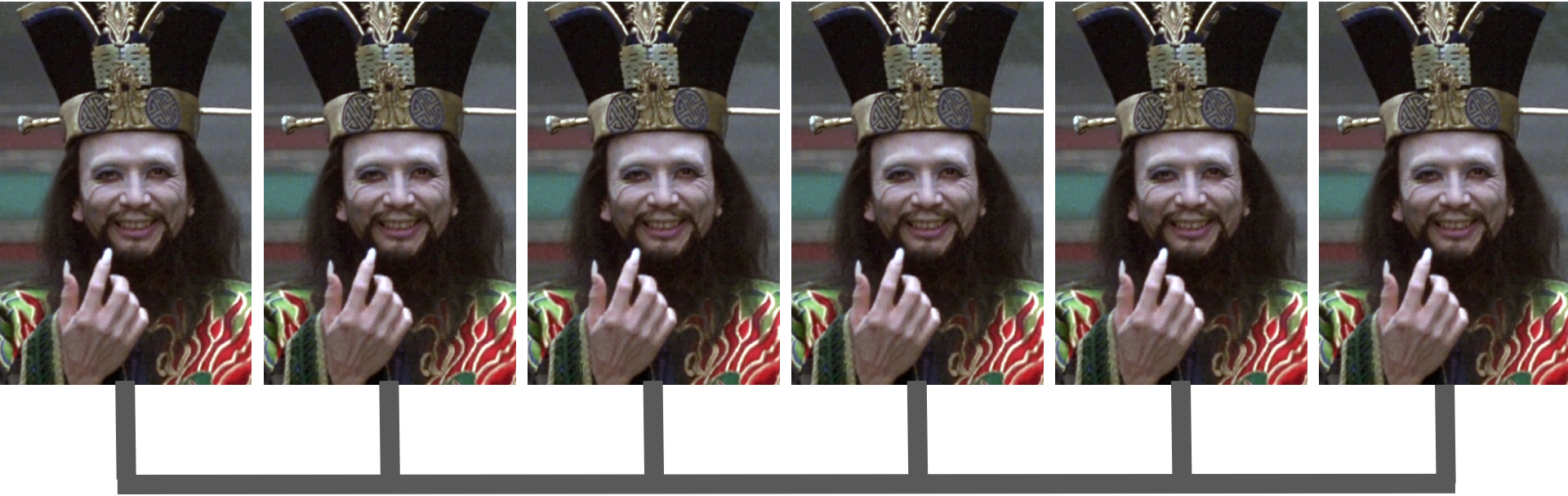
# Meet LoPan

# But what about 6LowPan?






# Traditional topologies don’t work



# LoPan devices communicate in short bursts to preserve their energy

# With limited range and spread

# How can they express themselves?

# How can they express themselves?






# With 6 Lo Pans, you need to bridge different mediums to spread

Jack Burton?!

# With 6 Lo Pans, you need to bridge different mediums to spread

# With 6 Lo Pans, you need to bridge different mediums to spread

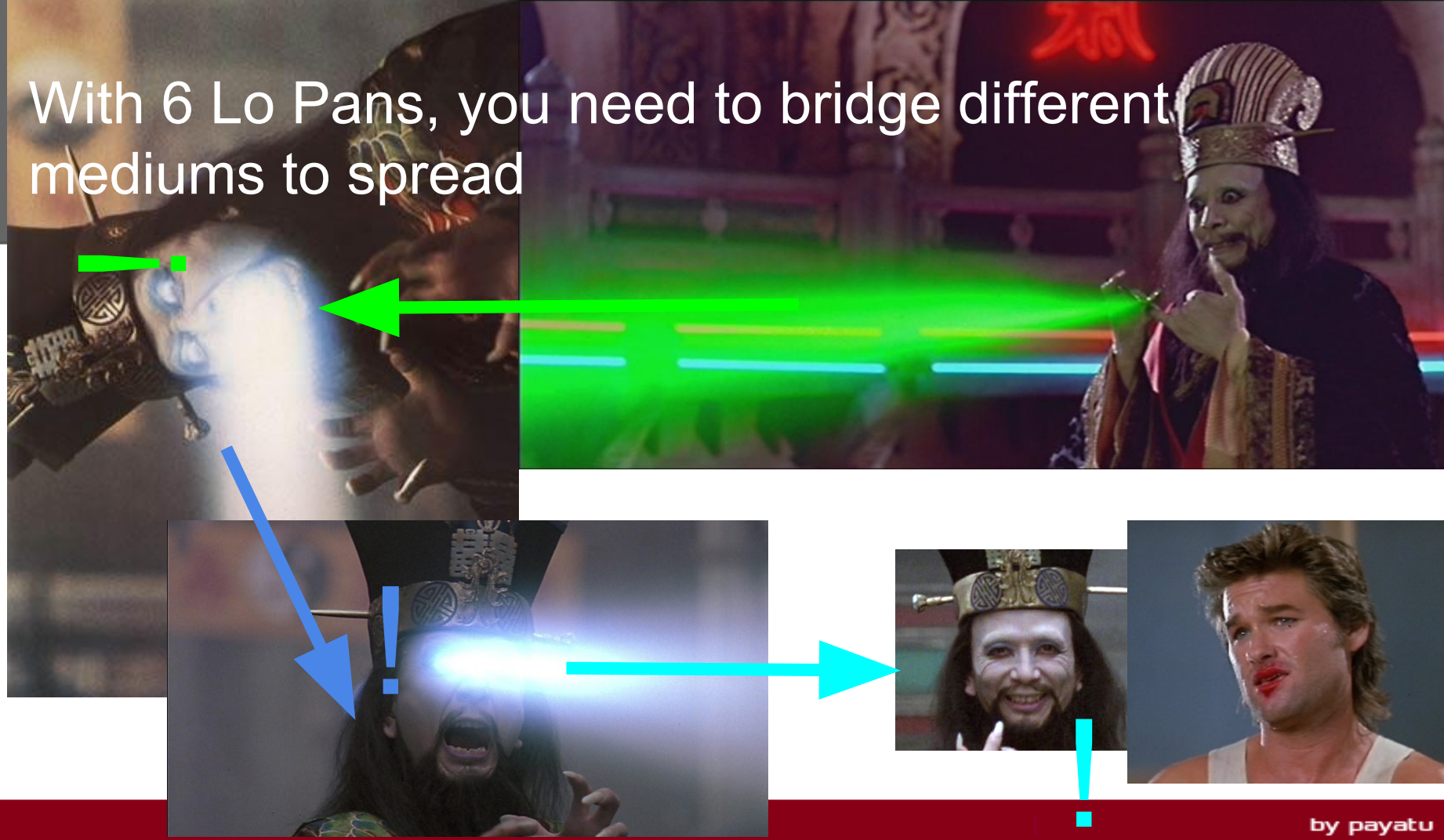



# With 6 Lo Pans, you need to bridge different mediums to spread

# With 6 Lo Pans, you need to bridge different mediums to spread

# With 6 Lo Pans, you need to bridge different mediums to spread

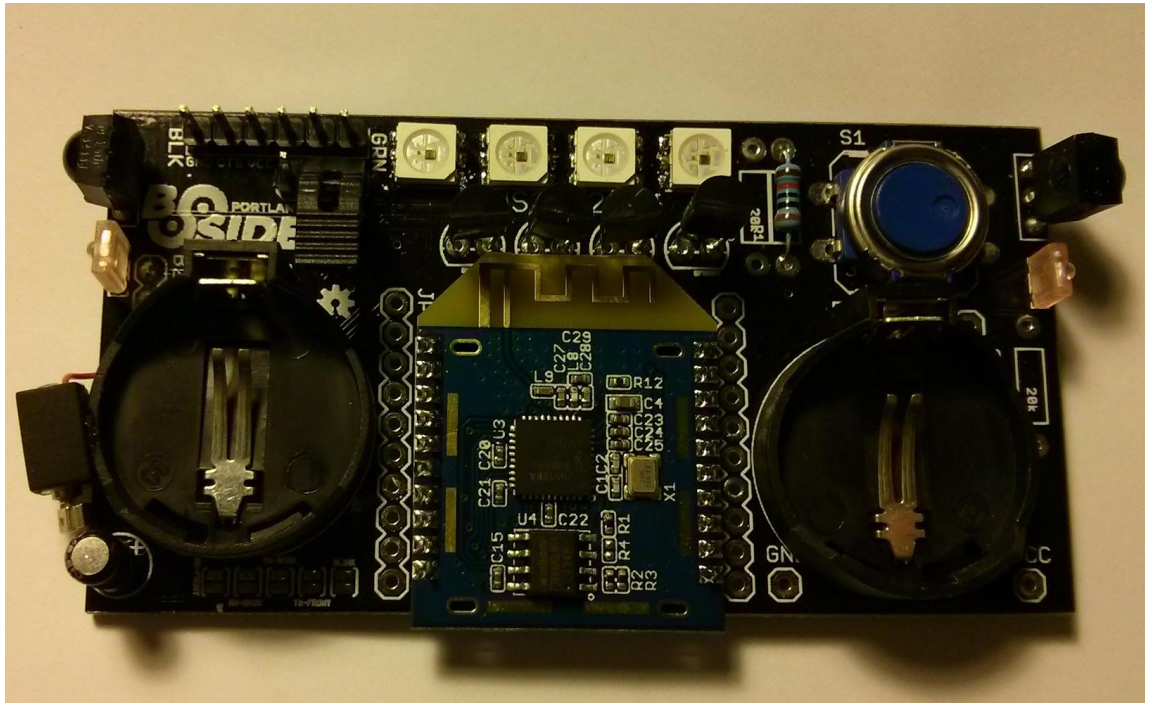
# With 6 Lo Pans, you need to bridge different mediums to spread



# And then one Lo Pan can bridge the message to Jack

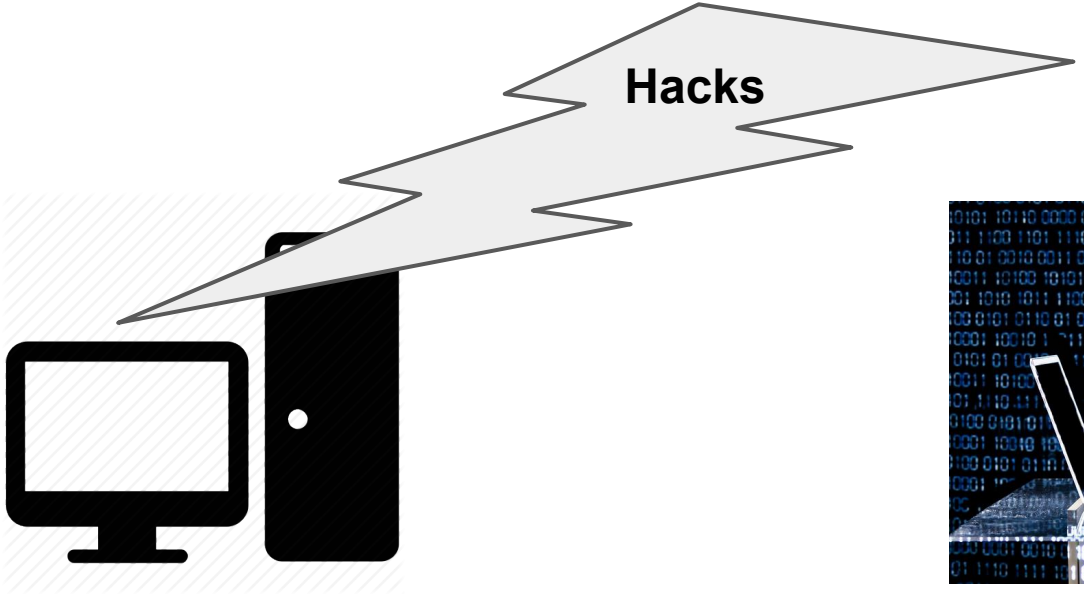
# IoT: Smart Shirts

# Thinking Cap/Internet of Hats



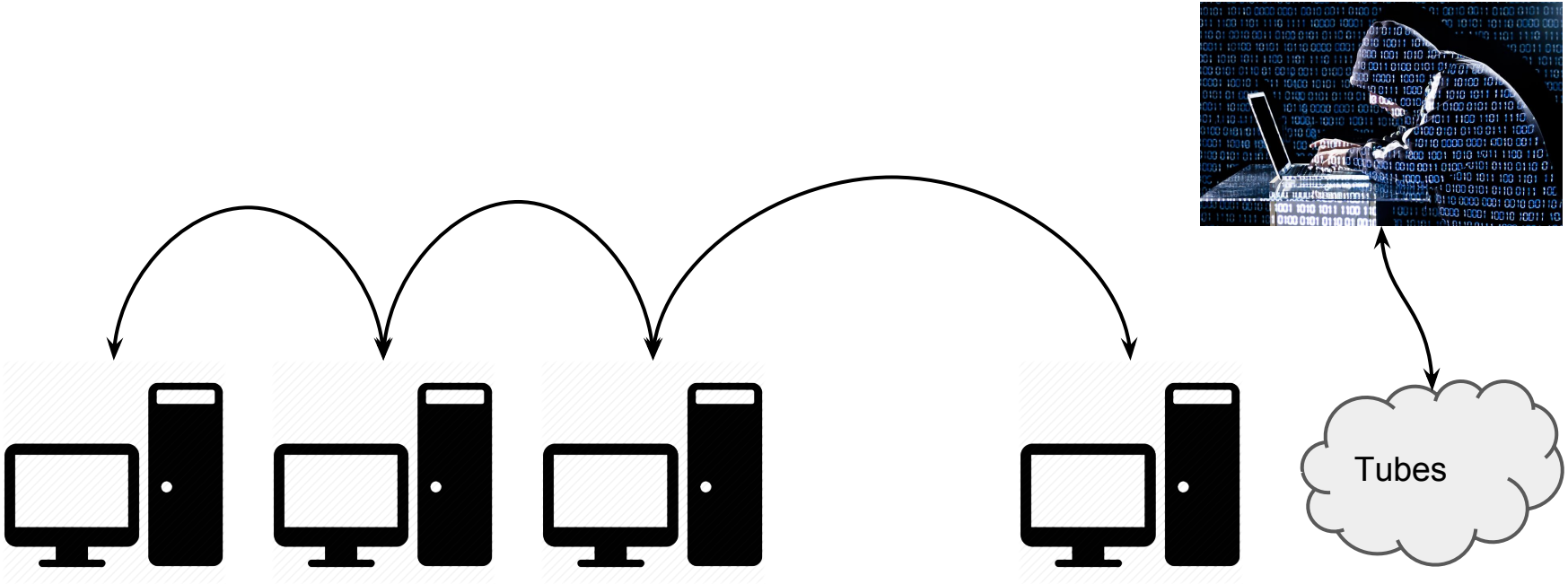
# Radio Hostile Environments

# Basic Theory of Operation

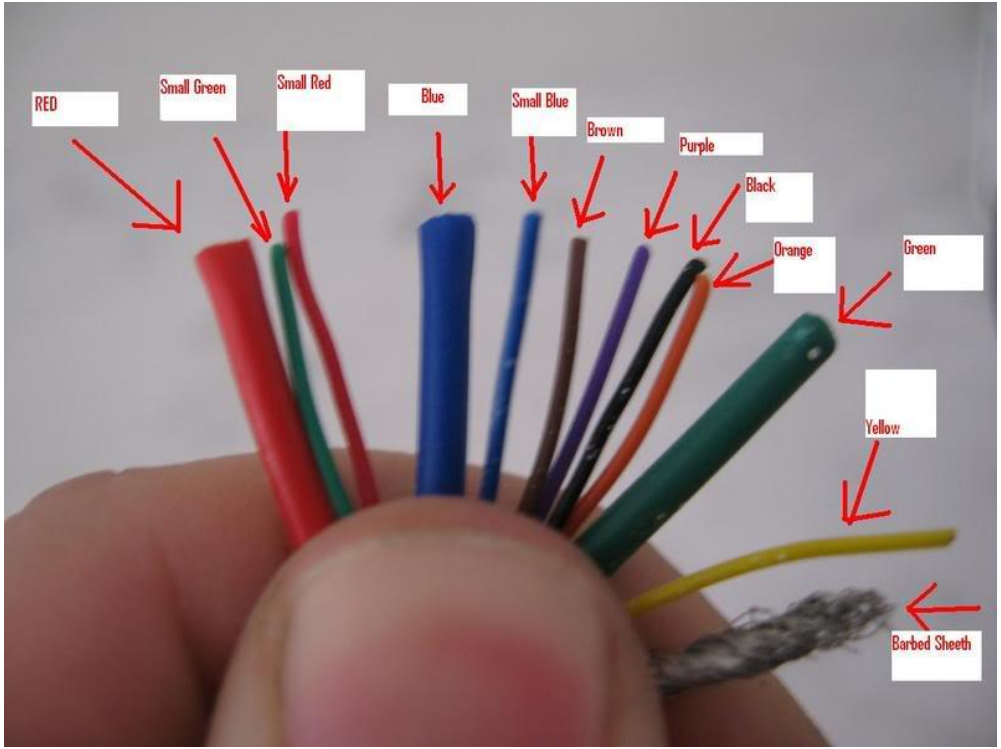


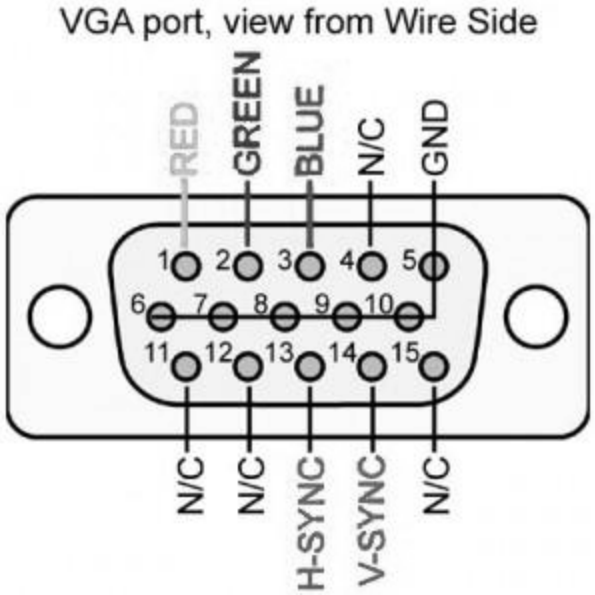

Victim

# Advanced Usage

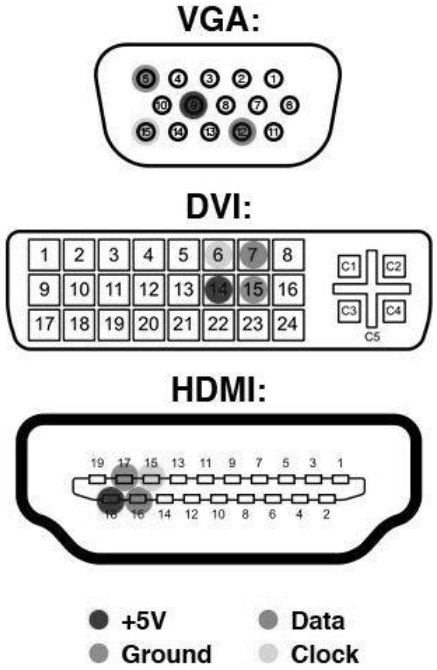


# VGA Pinout

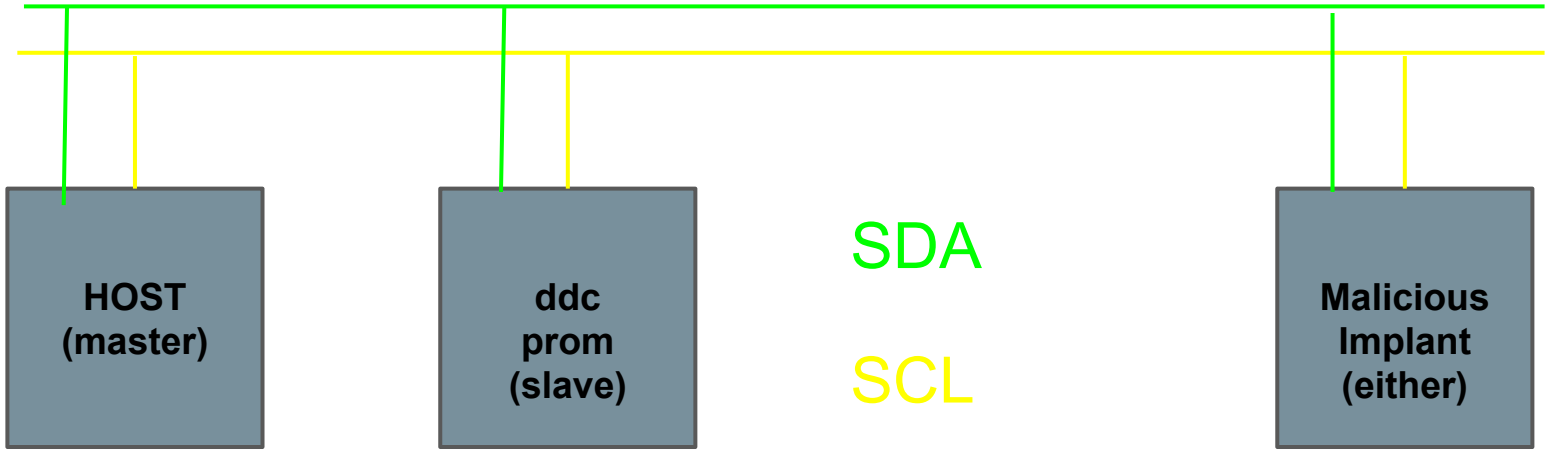

RED
Small Green
Small Red
Blue
Small Blue
Brown
Purple
Black
Orange
Green
Yellow
Barbed Sheeth


VGA port, view from Wire Side
RED
GREEN
BLUE
N/C
GND
1 2 3 4 5
6 7 8 9 10
11 12 13 14 15
N/C
N/C
H-SYNC
V-SYNC
N/C

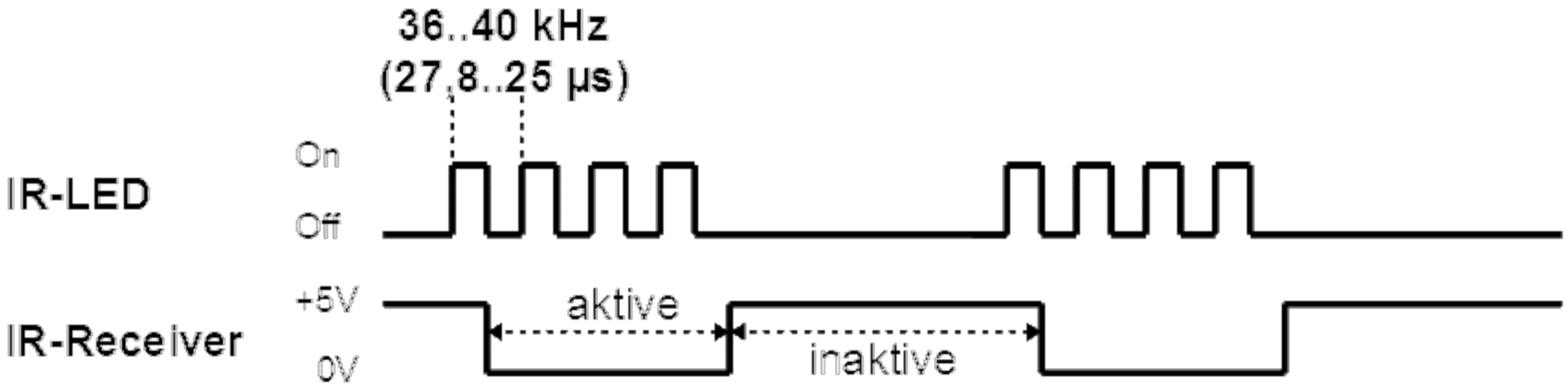
# What Your Mother Didn't Tell You About VGA

# I2C

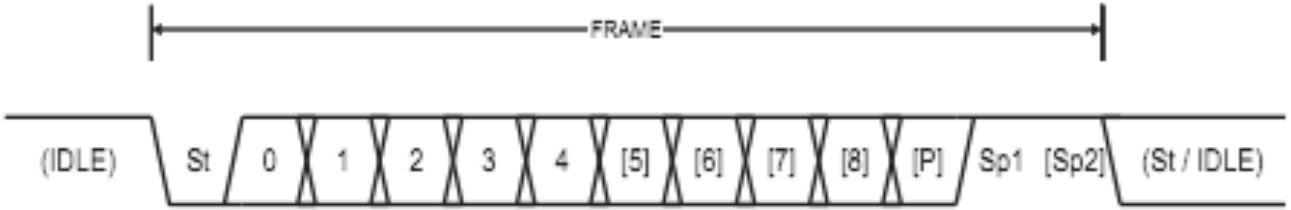

HOST
(master)
ddc
prom
(slave)
SDA
SCL
Malicious
Implant
(either)

# Basics of CIR



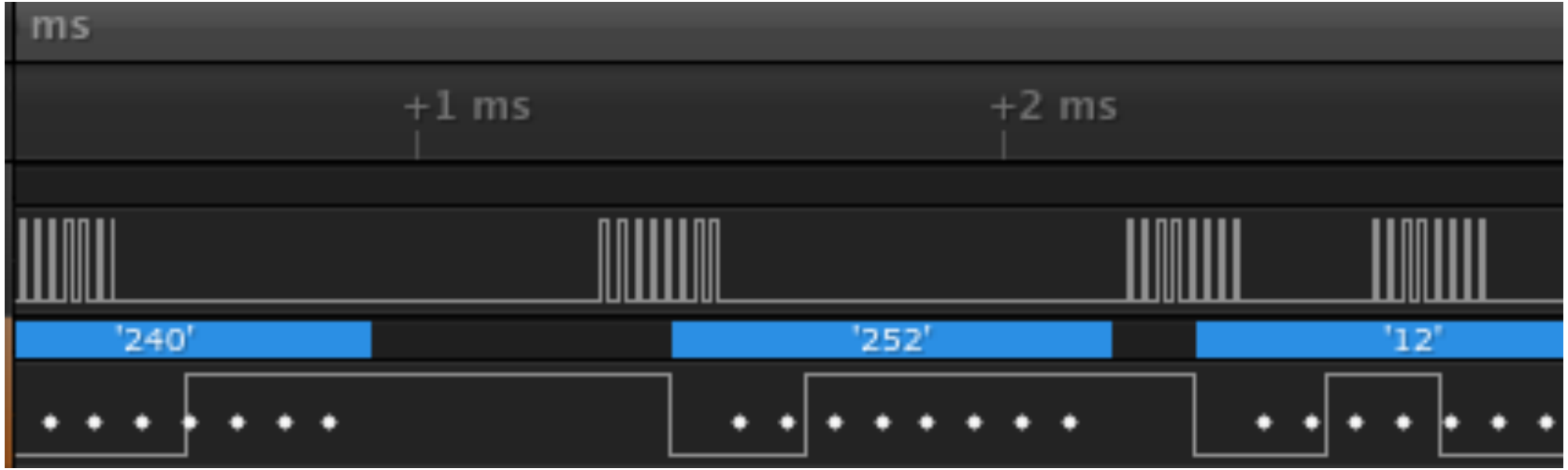
# UART

**Figure 19-4.** Frame Formats

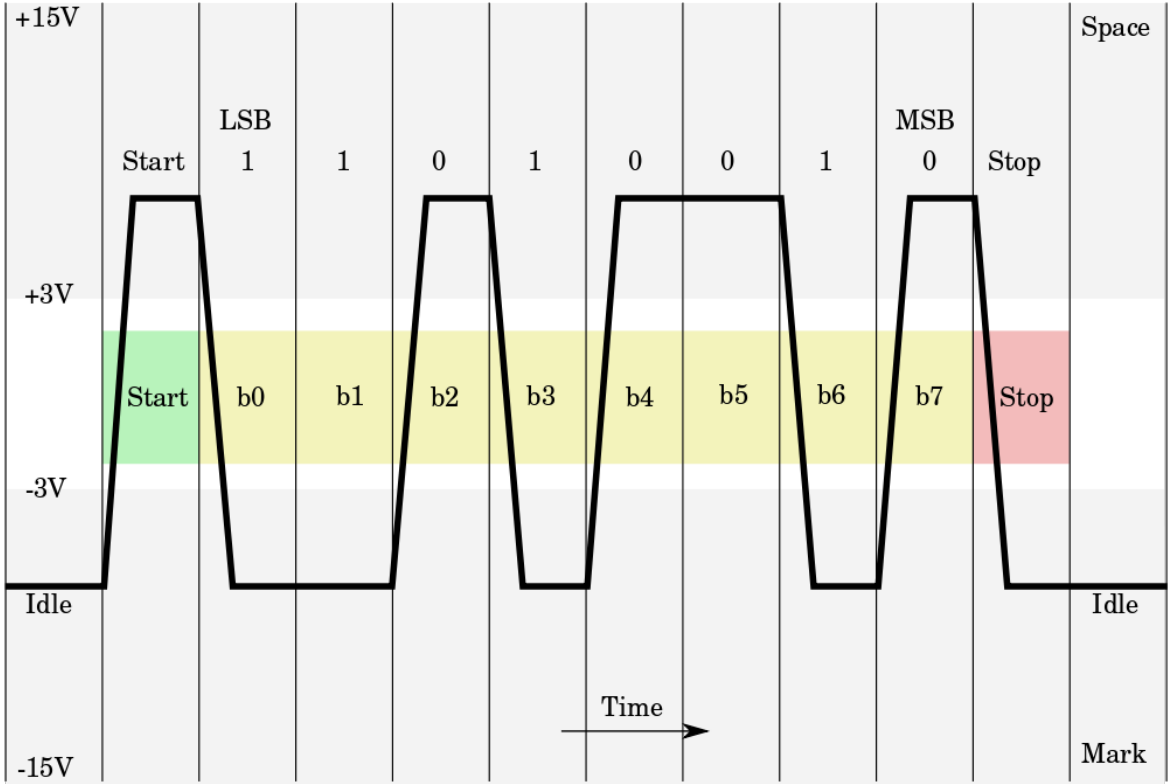



| | |
|---|---|
| **St** | Start bit, always low. |
| **(n)** | Data bits (0 to 8). |
| **P** | Parity bit. Can be odd or even. |
| **Sp** | Stop bit, always high. |
| **IDLE** | No transfers on the communication line (RxDn or TxDn). An IDLE line must be high. |

# CIR & UART



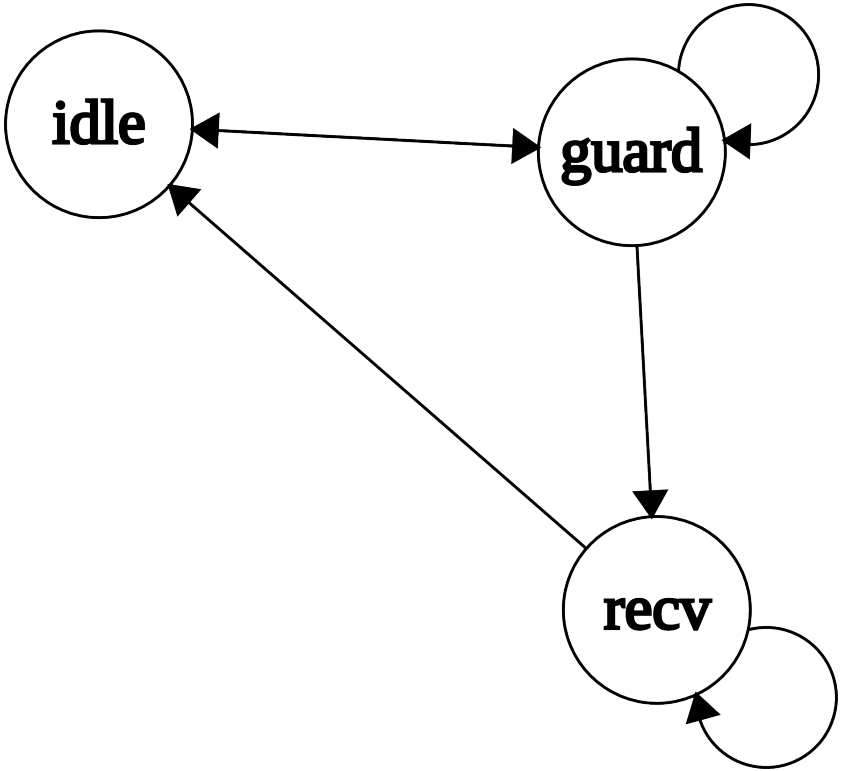
# The Zero Hour



# Packet Format

```
struct __attribute__ ((__packed__)) IRFrame
{
    uint16_t source;
    uint16_t destination;
    int  type: 4;
    int  hops: 4;
    uint8_t  payload[BLOB_SIZE];
    uint16_t crc;
}
```

# Eating Garbage



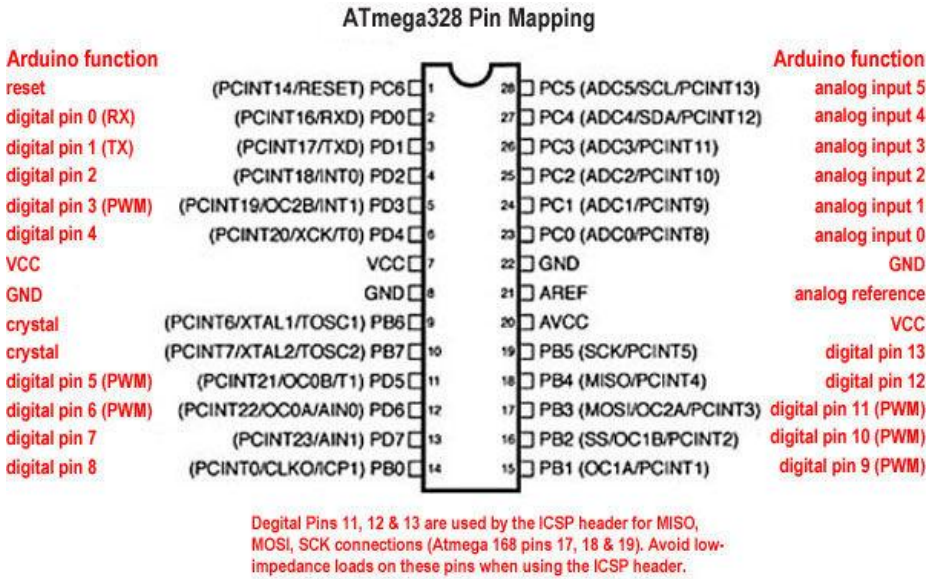
# Meshing

```
int  hops: 4;


if (!forme() && hops < 15) {
  hops++;
  send();
}
```

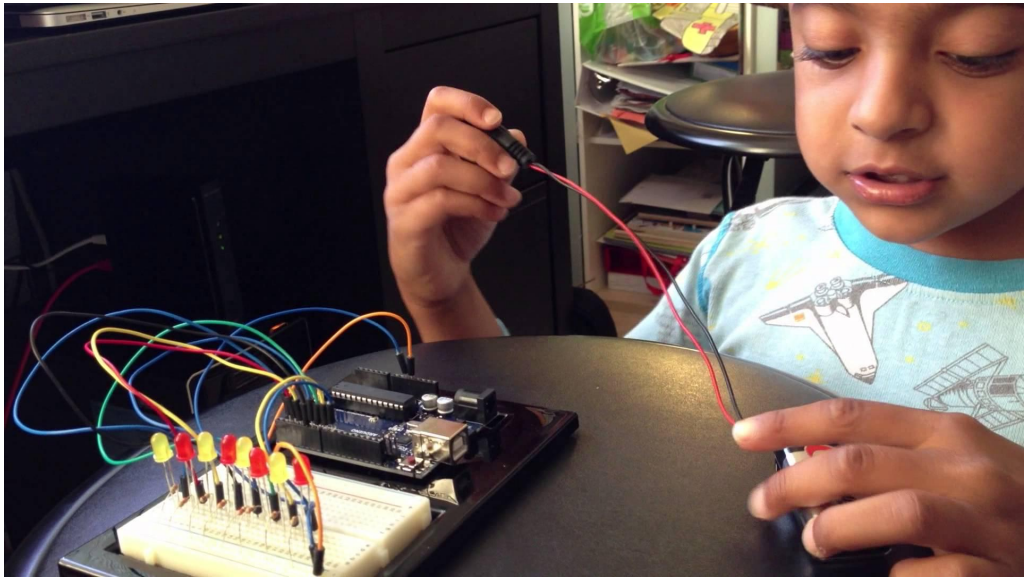
# Playsetable HW Platform

Requirements:

- small
- cheap
- easy
- fun



# Playsettable SW Platform



ARDUINO™

# Arduino?!

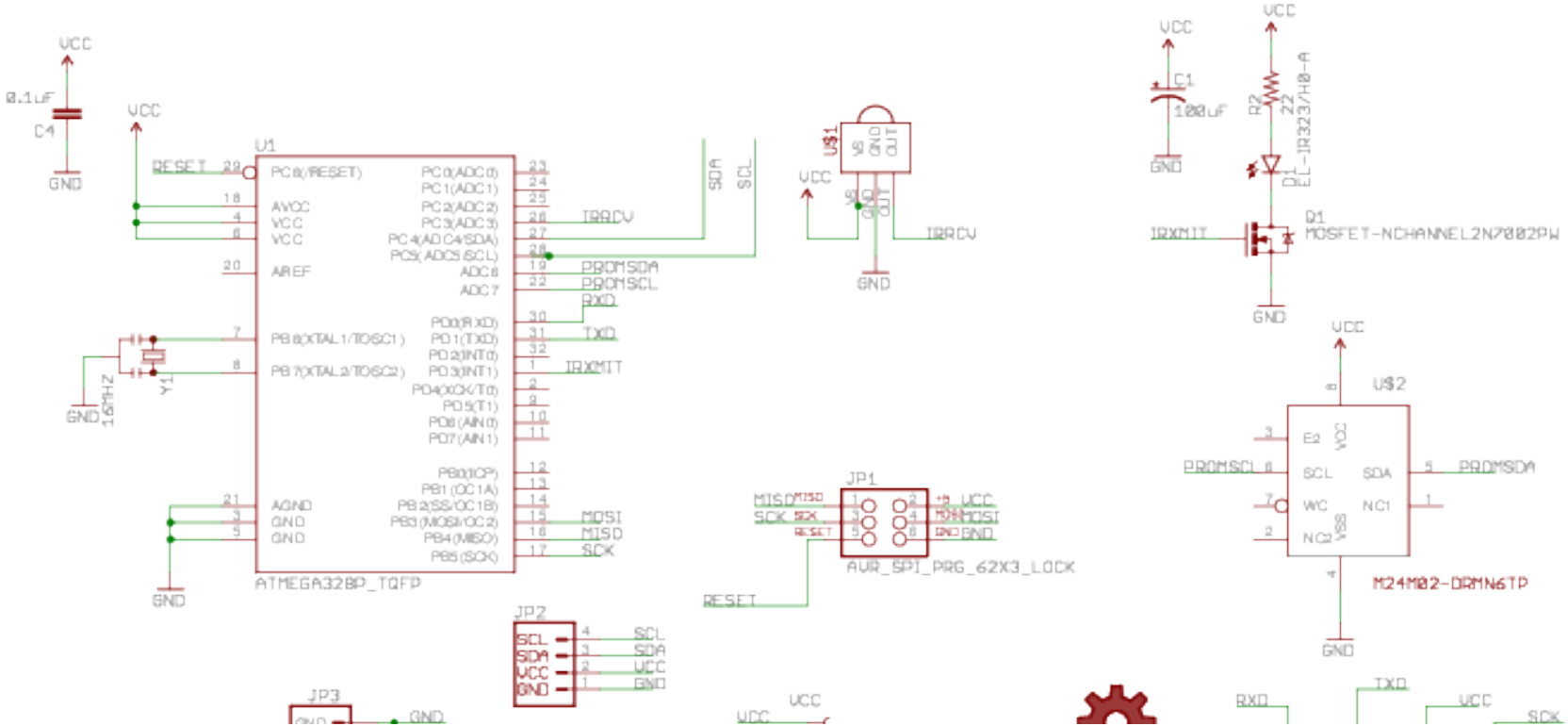
Blink | Arduino 1.0

Blink

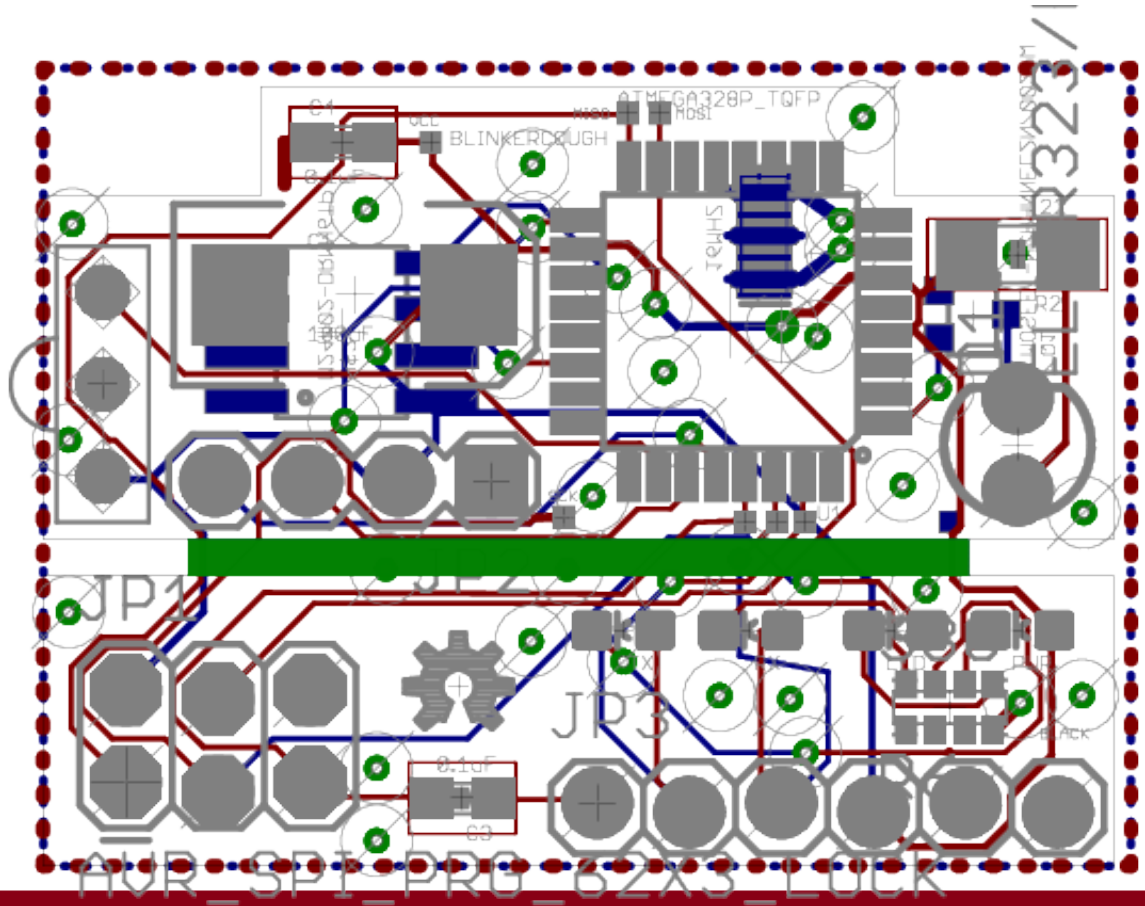
```
/*
  Blink
  Turns on an LED on for one second, then off for one second, repeatedly.

  This example code is in the public domain.
 */

void setup() {
  // initialize the digital pin as an output.
  // Pin 13 has an LED connected on most Arduino boards:
  pinMode(13, OUTPUT);
}

void loop() {
  digitalWrite(13, HIGH);   // set the LED on
  delay(1000);              // wait for a second
  digitalWrite(13, LOW);    // set the LED off
  delay(1000);              // wait for a second
}
```

1 Arduino Uno on /dev/tty.usbmodemfd131

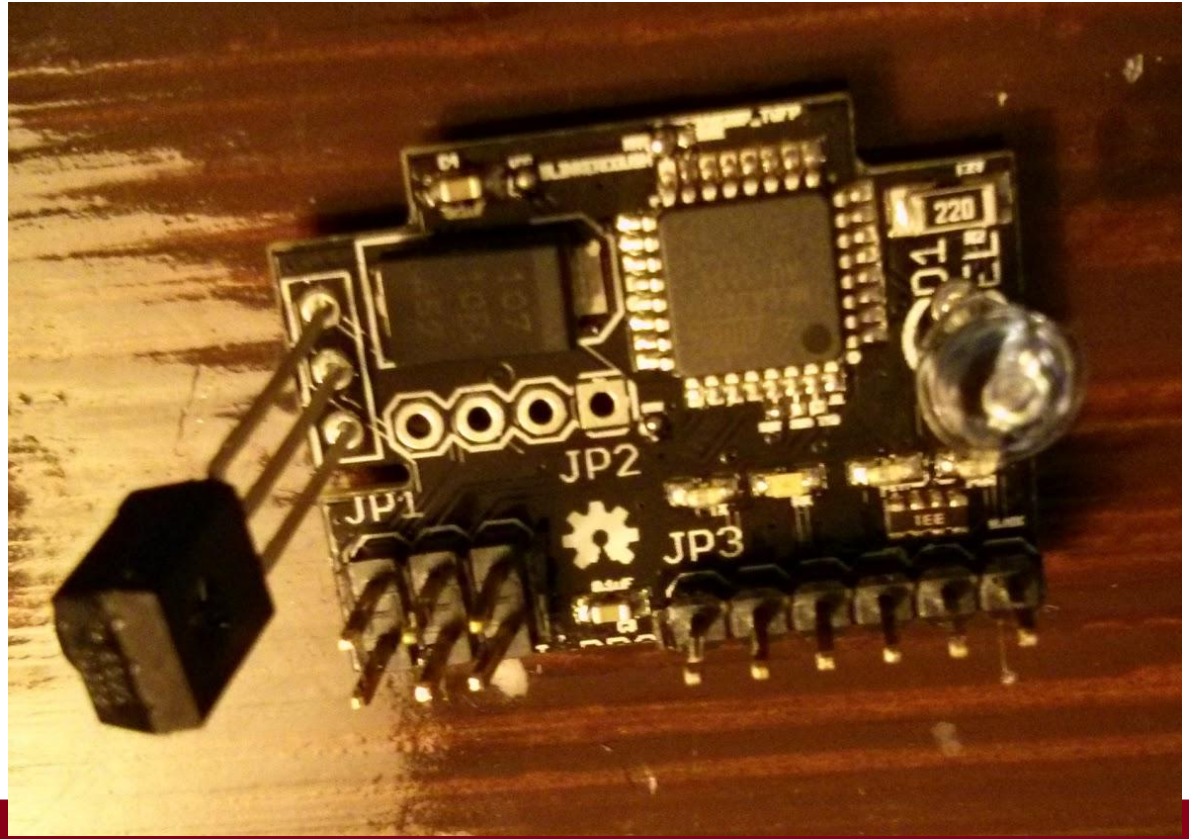
# HW details


VCC
0.1uF
C4
GND
U1
RESET
PC6(/RESET)
AVCC
VCC
AREF
PB6(XTAL1/TOSC1)
PB7(XTAL2/TOSC2)
AGND
GND
PC0(ADC0)
PC1(ADC1)
PC2(ADC2)
PC3(ADC3)
PC4(ADC4/SDA)
PC5(ADC5/SCL)
ADC6
ADC7
PD0(RXD)
PD1(TXD)
PD2(INT0)
PD3(INT1)
PD4(XCK/T0)
PD5(T1)
PD6(AIN0)
PD7(AIN1)
PB0(ICP)
PB1(OC1A)
PB2(SS/OC1B)
PB3(MOSI/OC2)
PB4(MISO)
PB5(SCK)
ATMEGA32BP_TQFP
IRRCV
PROMSDA
PROMSCL
RXD
TXD
IRXMIT
MOSI
MISO
SCK
SDA
SCL
16MHZ
Y1
U$1
VS GND OUT
JP1
MISO SCK RESET
VCC MOSI GND
AVR_SPI_PRG_62X3_LOCK
JP2
SCL SDA VCC GND
JP3
C1
100uF
R2
22
D1
EL-1R323/H8-A
Q1
MOSFET-NCHANNEL2N7002PW
U$2
E2 SCL WC NC2
VCC SDA NC1 VSS
M24M02-DRMN6TP

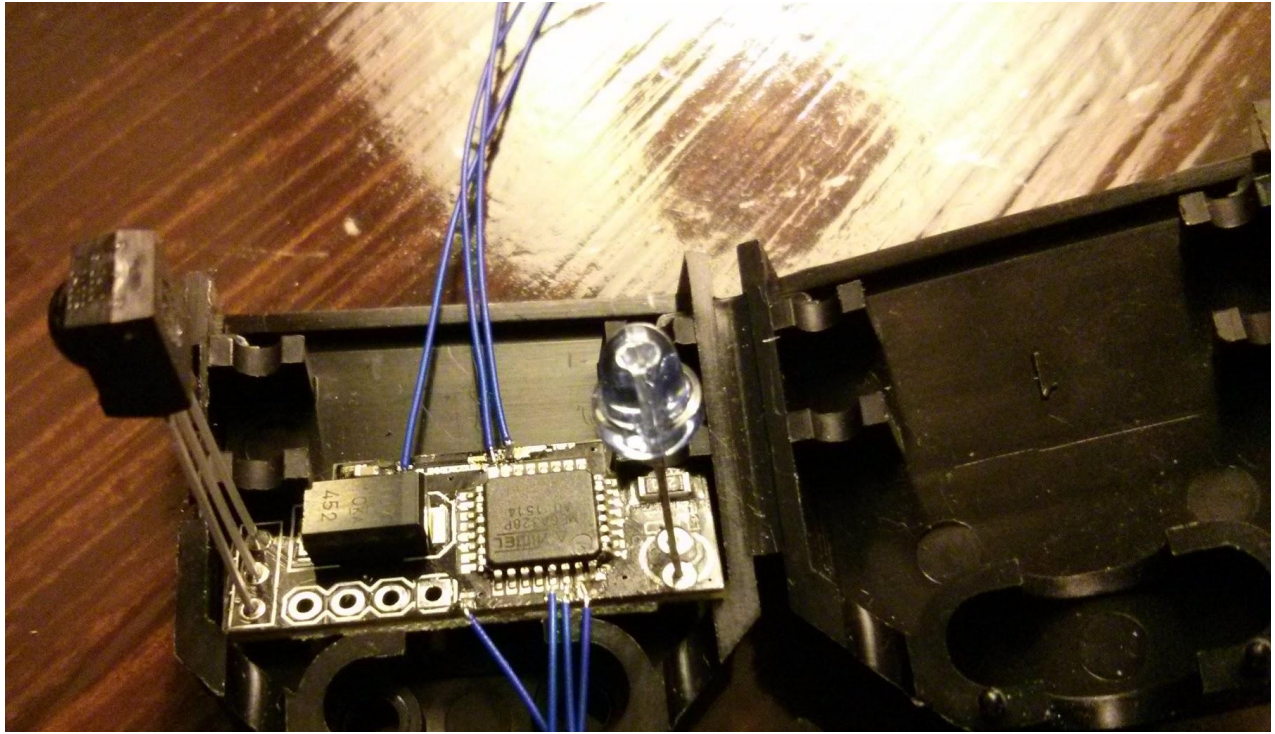
# More HW



# Easy to Play With



# Ready for Implantation



# faraday cage

# Long Distance

# Demo

# Thanks!

@joefitz, @laplinker, all teh playset peeps