Promiscuity, the nRF24L01+'s Duty

Travis Goodspeed
<travis at radiantmachines.com>

20 May, 2011
Hack in the Box
Amsterdam, Netherlands

nH HOTELES

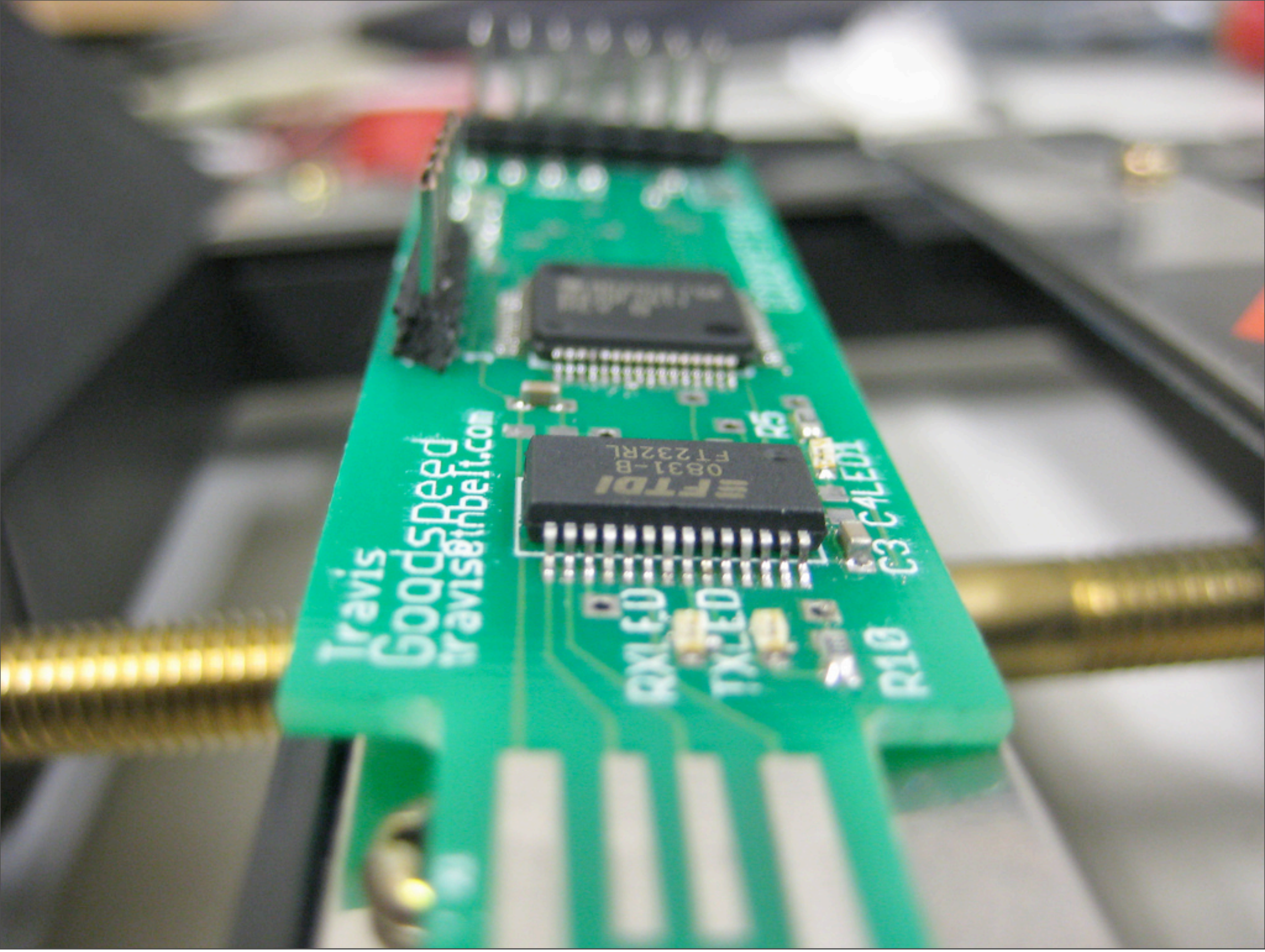
Welcome

GOODSPEED, TRAVIS
It is a pleasure to welcome you to NH Grand Hotel Krasnapolsky

OK to continue

www.nh-hotels.com

Friday, May 20, 2011


Travis
Goodspeed
travis@thebeef.com
FTDI
0831-B
FT232RL
RXLED
TXLED
R10
C3
C4
LED

Thank you kindly.

- Michael Ossmann
- Thorsten Schröder and Max Moser
- Sergey Bratus

Microsoft 2.4 GHz Keyboard

- 2.4GHz Nordic, XOR crypto
- SYNC varies by unit.
  - There's no promiscuous mode.
- Initial Exploit in Keykeriki 2.0
  - Max Moser and Thorsten Schröder
  - Amiccom A7125, nRF24L01+

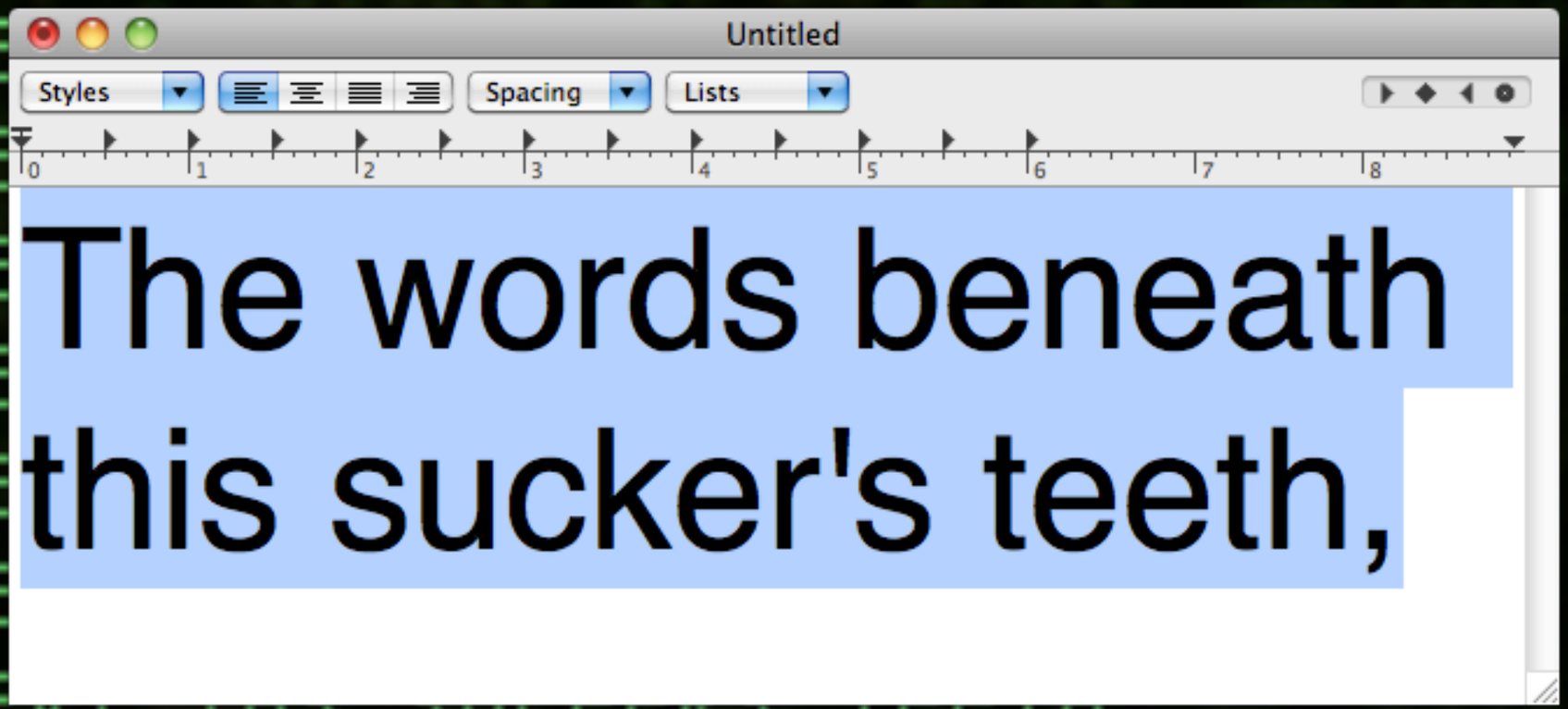
Introduction

- What is the hack?
- Why is it hard?
- How does it work?

Layer 1 Attacks

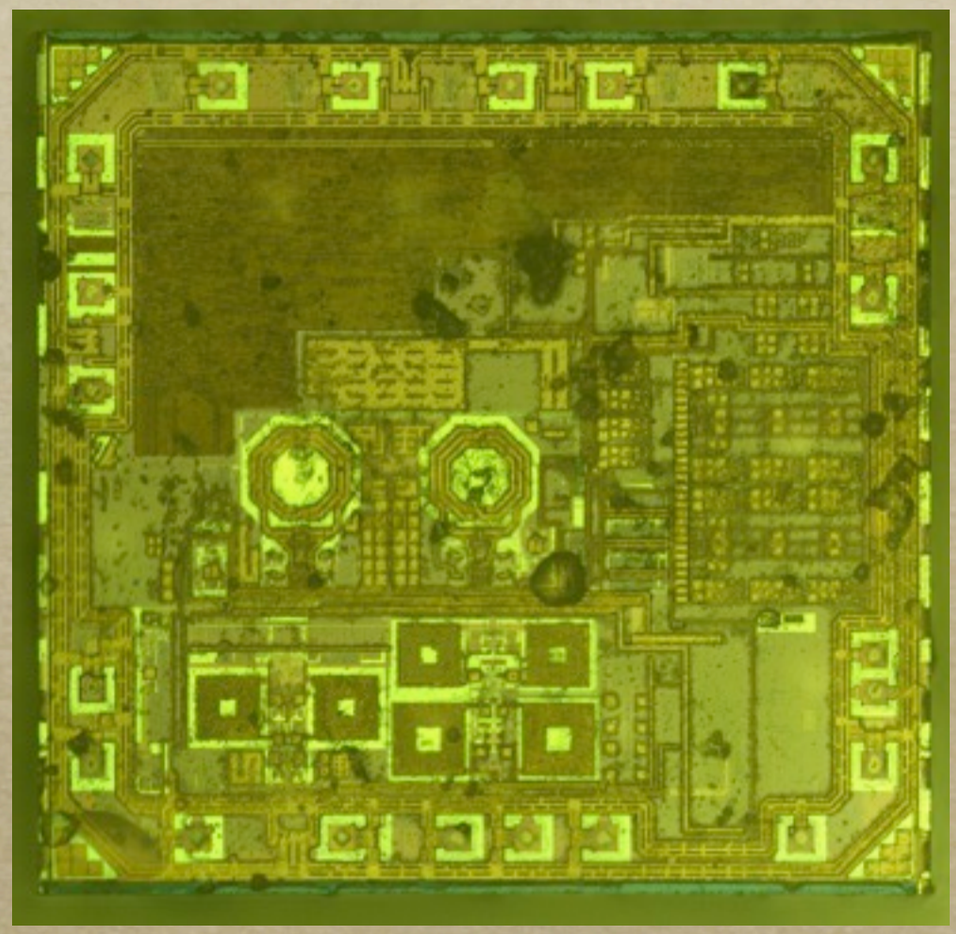
Friday, May 20, 2011

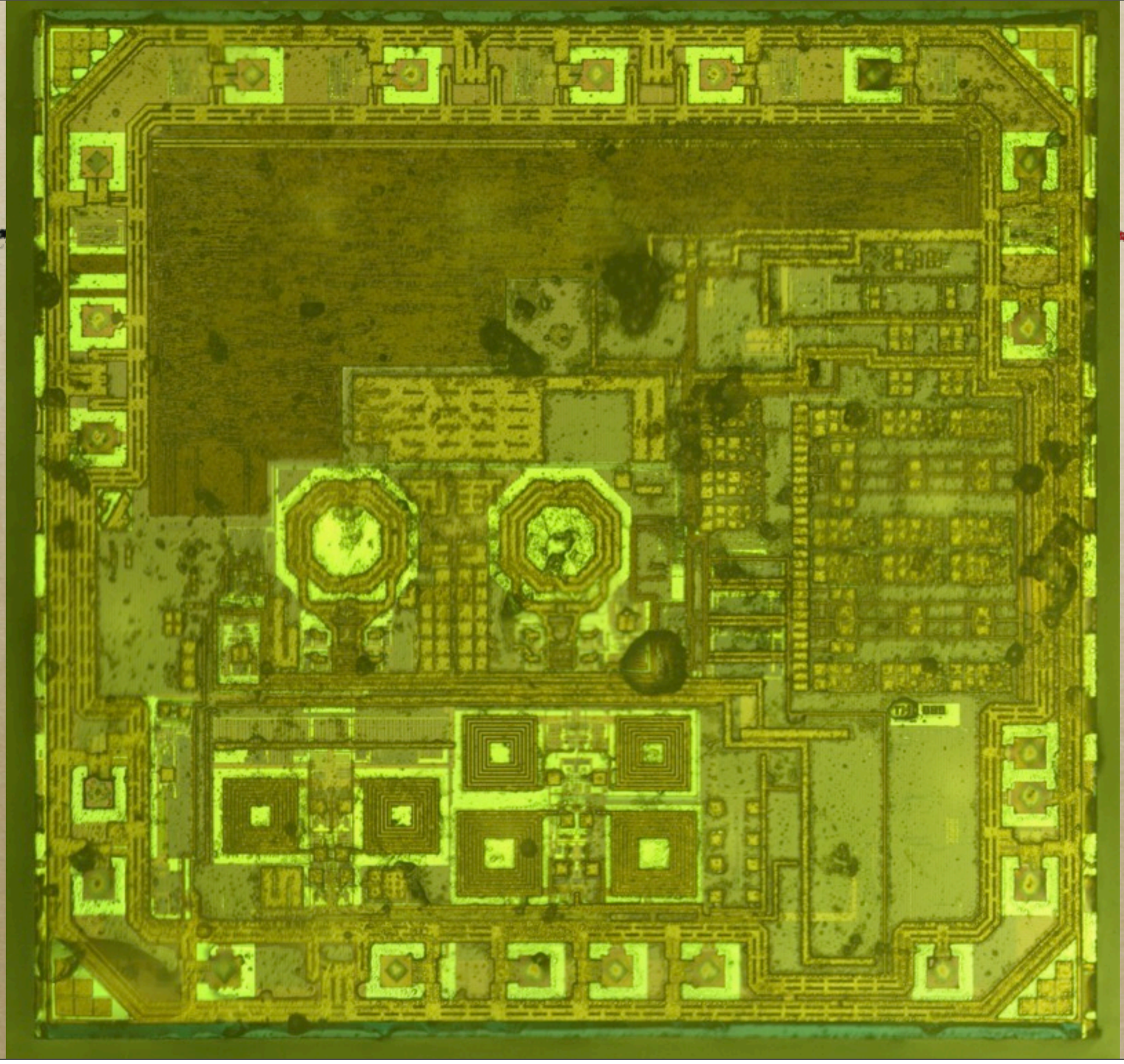
```
#  TE_ORDS_BENEEAT_THS_SU
#  TE_ORDS_BENEEAT_THS_SUC
#  TE_ORDS_BENEEAT_THS_SUCE
#  TE_ORDS_BENEEAT_THS_SUCEE
#  TE_ORDS_BENEEAT_THS_SUCEER
Unknown character 0x34.
#  TE_ORDS_BENEE
#  TE_ORDS_BENEE
#  TE_ORDS_BENEE
#  TE_ORDS_BENEE
#  TE_ORDS_BENEE
#  TE_ORDS_BENEE
Unknown character 0x36.
#  TE_ORDS_BENEEAT_THS_SUCEERS_TEETH_
```



nRF24L01+

- 2.4GHz 2FSK Transceiver
- Auto-ACK, Auto-Retry
- No promiscuous mode.





Building a Promiscuous Mode

- Wifi, Ethernet
  - Missing the Address.
  - Turn off matching.
- Bluetooth, Microsoft Keyboards
  - Missing the Sync.
  - Can’t turn off matching!

Building a Promiscuous Mode

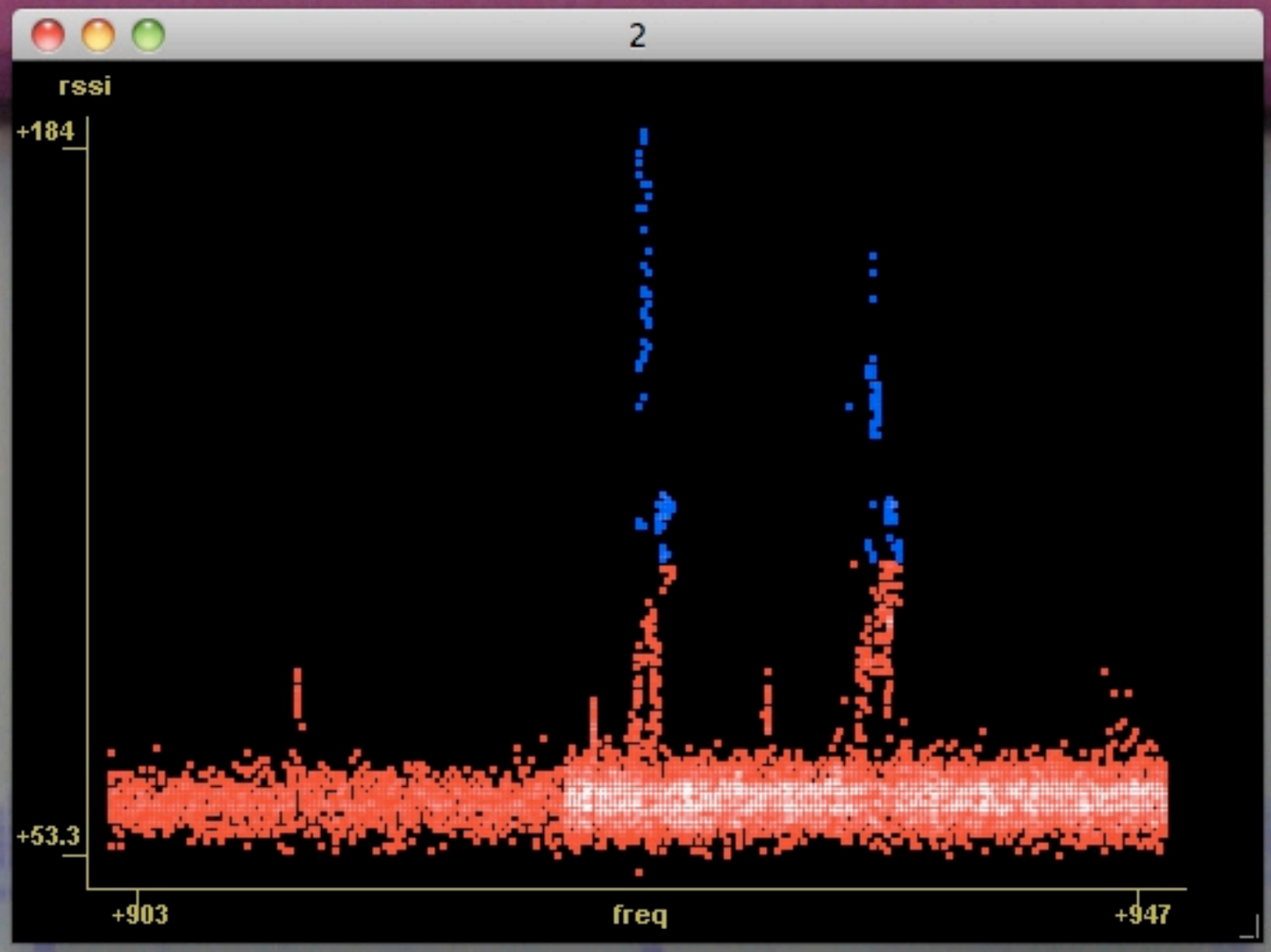
- Software Defined Radio
  - Expensive ($$), Finicky
- Bit Banging
  - Expensive ($), Custom
- Hardware Tricks
  - Cheap (¢), Commodity

Why mess with toy radios?

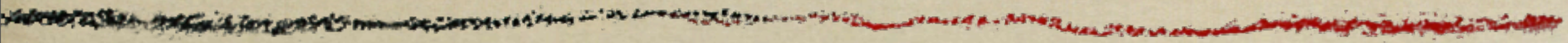
Real Men Carry Pink Pagers

Travis Goodspeed

Michael Ossmann



Friday, May 20, 2011



Friday, May 20, 2011

Down to Layer 1

- What does Ethernet *look* like?
- What does digital radio *look* like?
- There's plenty of room at the bottom.

Ethernet

- Preamble
  - AA AA AA AA AA AA AA AA
- Sync
  - AB
- Body
  - dest, src, etc

Preamble is a repeating pattern.

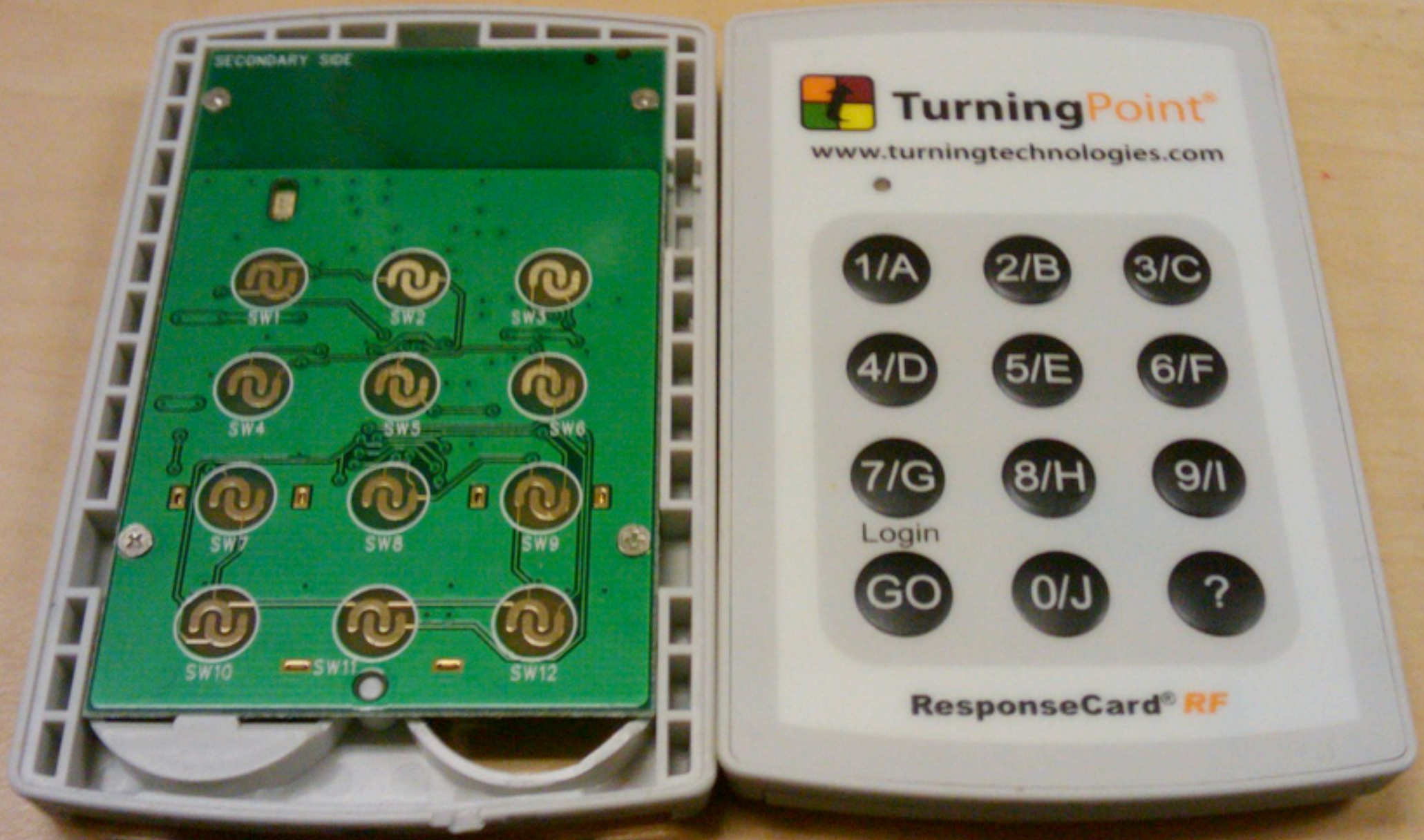
Sync breaks that pattern.

Layer 1 Ethernet Frame

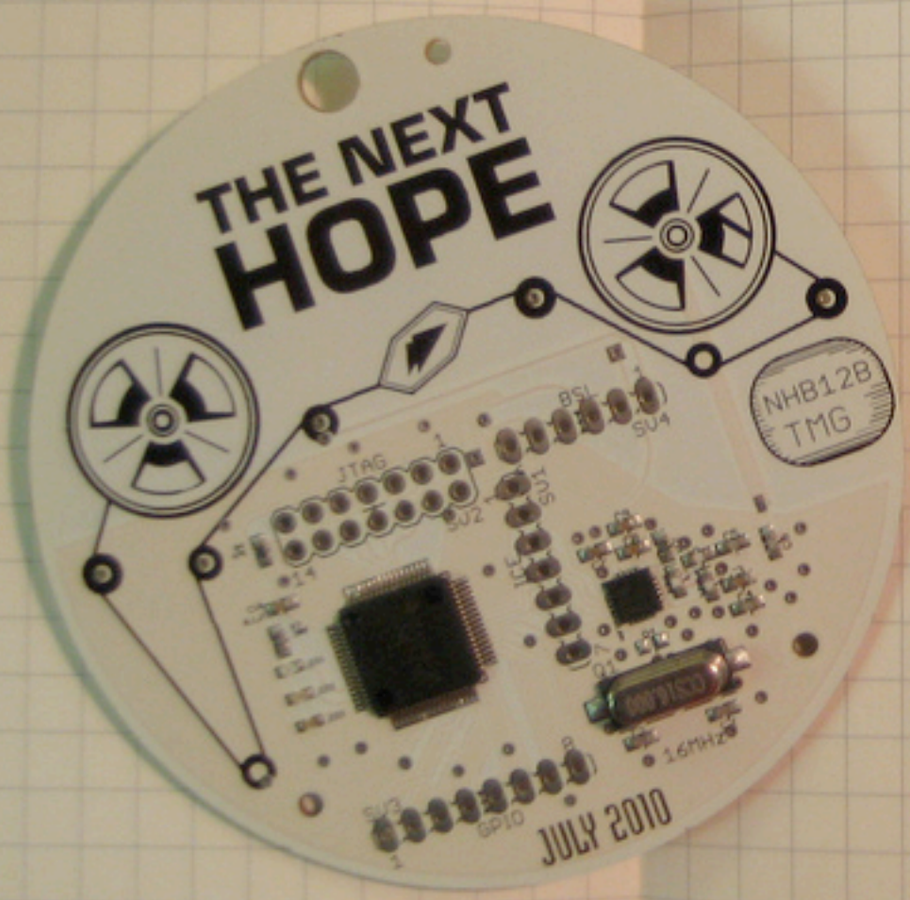
- AA AA AA AA AA AA AA AB
- 00 DE AD BE EF 00 CA FE BA BE ...

Radio

- Shorter Preamble, to conserve power.
- Longer Sync, to combat noise.
- Varied Sync
  - Unique to protocol or *to the device*.



Friday, May 20, 2011


THE NEXT
HOPE
NHB12B
TMG
JTAG
BSL
SU4
SU2
SU1
SU3
SP10
16MHz
JULY 2010


Error
The currently attached accessory is not supported by this iPod.
MENU

Preamble -- Sync

- Ethernet
  - AA AA AA AA AA AA AA -- AB
- Radio
  - 55 -- 12 34 56
  - 55 -- 01 02 03 02 01
  - 00 00 00 -- 00 A7

Varied Syncs

- Sync per Protocol
  - 123456, Turning Point Clicker
  - 0102030201, OpenBeacon
  - C2BD, Nike Shoe Pod
- Sync per Device
  - Microsoft 2.4GHz Keyboards
  - Bluetooth

The Old Fashioned Way

- Dump firmware into IDA.
- Reverse engineer it.
  - Looking for radio register settings.

CC1101 - Device Control Panel (offline)

File Settings View Evaluation Board Help

Easy Mode | Expert Mode | Register View | RF Parameters | Register reset

Select configuration:

```
SimpliciTI Ping packet, High data rate (250 kbaud), Base frequency 902 MHz
SimpliciTI Ping packet, High data rate (250 kbaud), Base frequency 868 MHz
SimpliciTI Ping packet, High data rate (250 kbaud), Base frequency 434 MHz
SimpliciTI Ping packet, Low data rate (2.4 kbaud), Base frequency 902 MHz
SimpliciTI Ping packet, Low data rate (2.4 kbaud), Base frequency 868 MHz
SimpliciTI Ping packet, Low data rate (2.4 kbaud), Base frequency 434 MHz
```

The selected configuration will set both the register values and t

Packet TX | Packet RX

Ping

Preamble	Sync	Length	Dest. Address	Source Address	Port	Device Info	Transactio ID	Payload	FCS
4	4	1	4	4	1	1	1	2	2
		0xD	0x0000AAAA	0x0000BBBB	0x01	0x34	0x00	1234	

Packet count: 100 Infinite

Sent packets: 0

Frequency: 905.998993 MHz

Output power: 0 dBm

TX RX

Start Stop

Not connected | Off-line mode | Radio state: N.A.

Friday, May 20, 2011

CC1101 - Device Control Panel (offline)

File Settings View Evaluation Board Help

Easy Mode | Expert Mode | Register View | RF Parameters | Register reset

Typical settings

```
Data rate: 1.2 kBaud,  Dev.: 5.2 kHz,  Mod.: GFSK, RX BW: 58 kHz,  Optimized for sensitivity
Data rate: 1.2 kBaud,  Dev.: 5.2 kHz,  Mod.: GFSK, RX BW: 58 kHz,  Optimized for current consumption
Data rate: 1.2 kBaud,  Dev.: 5.2 kHz,  Mod.: ASK,  RX BW: 58 kHz,  Optimized for sensitivity
Data rate: 2.4 kBaud,  Dev.: 5.2 kHz,  Mod.: GFSK, RX BW: 58 kHz,  Optimized for sensitivity
```

RF Parameters

Base frequency: 867.999939 MHz	Channel number: 0	Channel spacing: 199.951172 kHz	Carrier frequency: 867.999939 MHz
Xtal frequency: 26.000000 MHz	Data rate: 1.19948 kBaud	RX filter BW: 58.035714 kHz	Manchester enable
Modulation format: GFSK	Deviation: 5.157471 kHz	TX power: 0 dBm	PA ramping

Range Extender: None | High Gain Mode(RX)

Continuous TX | Continuous RX | Packet TX | Packet RX | RF Device Commands | PER Test Configuration

Packet payload size: 30 Add seq. number

Packet count: 100 Infinite

Random: 47 de b3 12 4d c8 43 bb 8b a6 1f 03 5a 7d 09 38 25 1f 5d d4 cb fc 96 f5 45 3b 13 0d 89 0a

Text

Hex

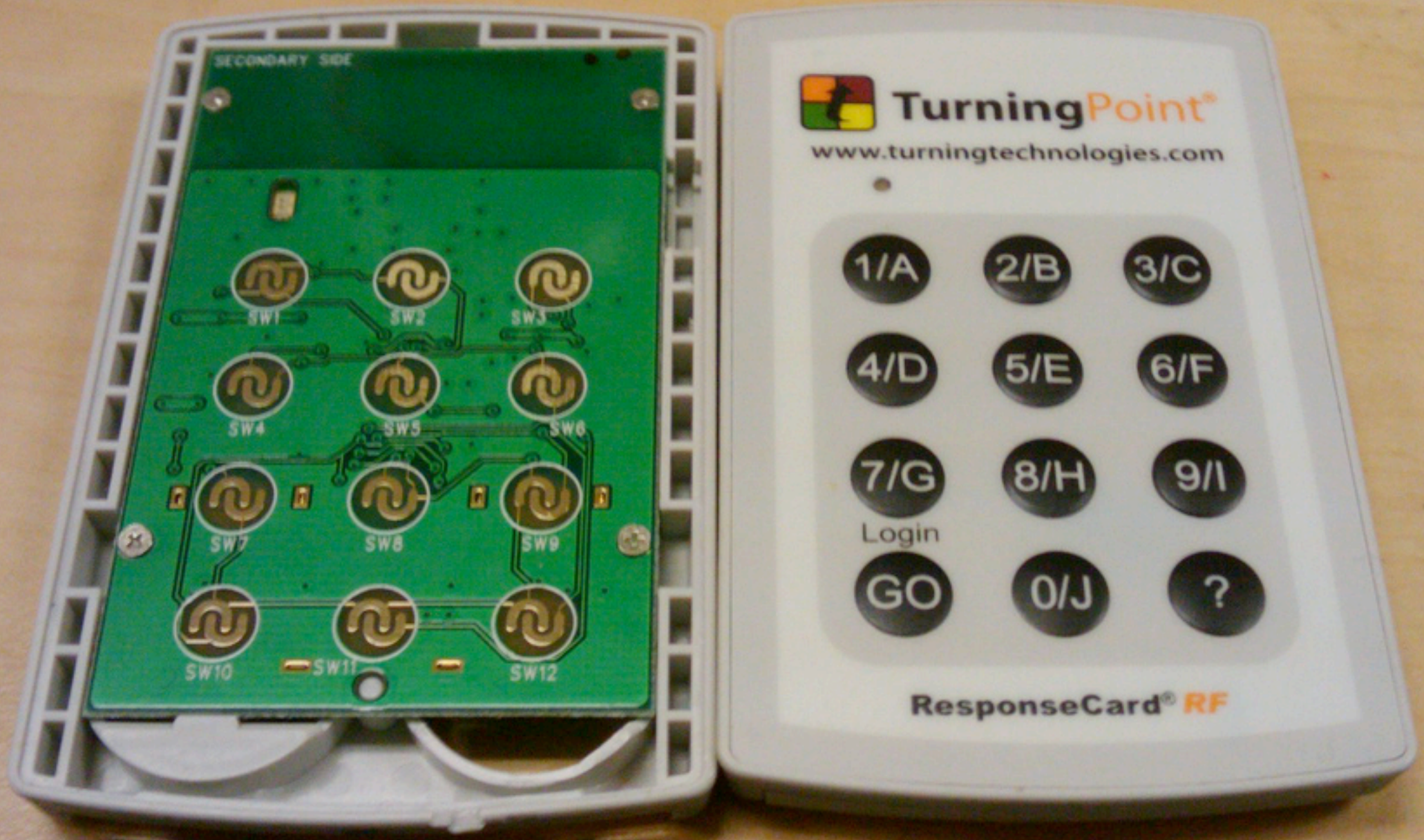
TX RX

Not connected | Off-line mode | Radio state: N.A.

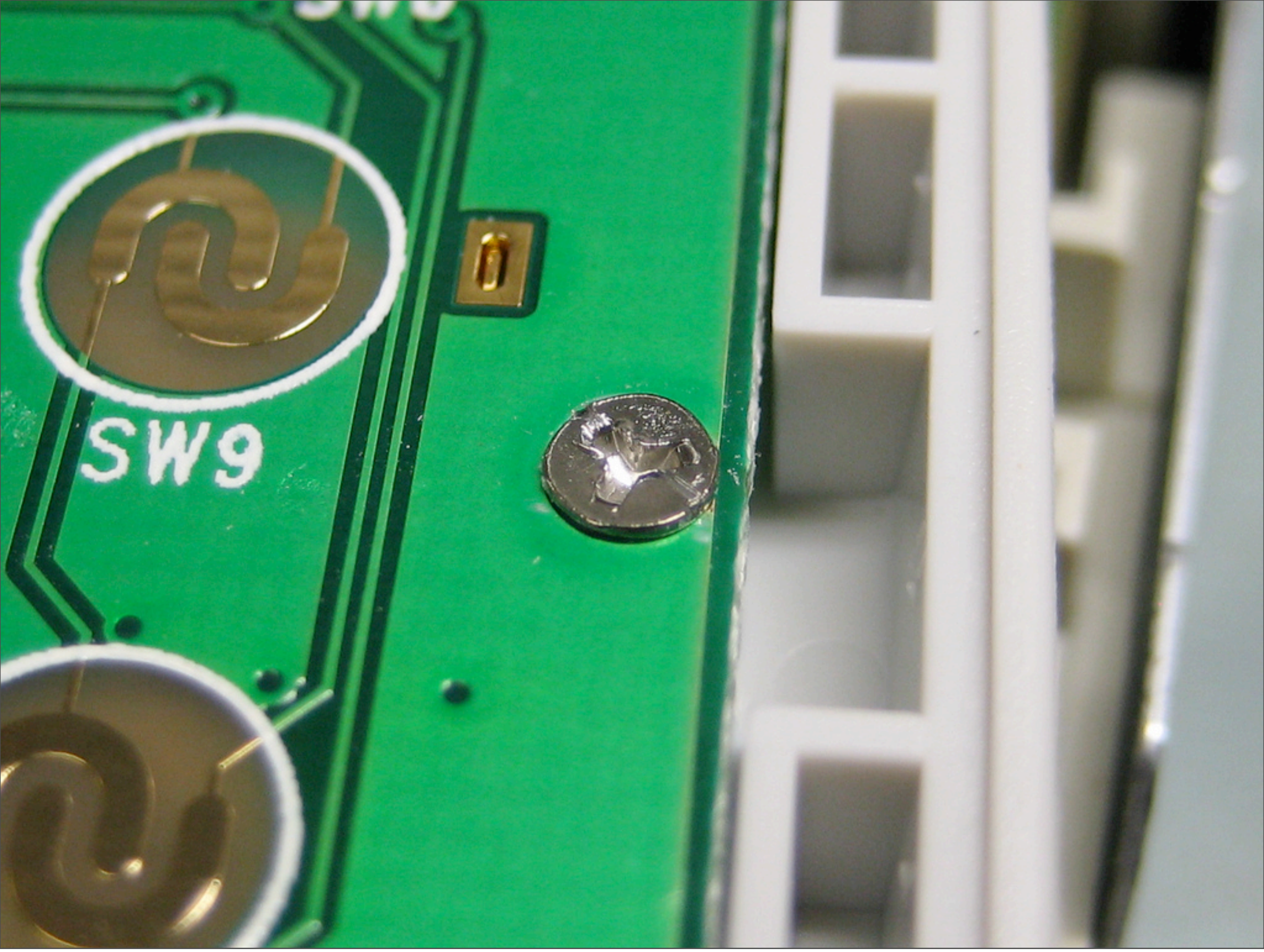
Radio Registers

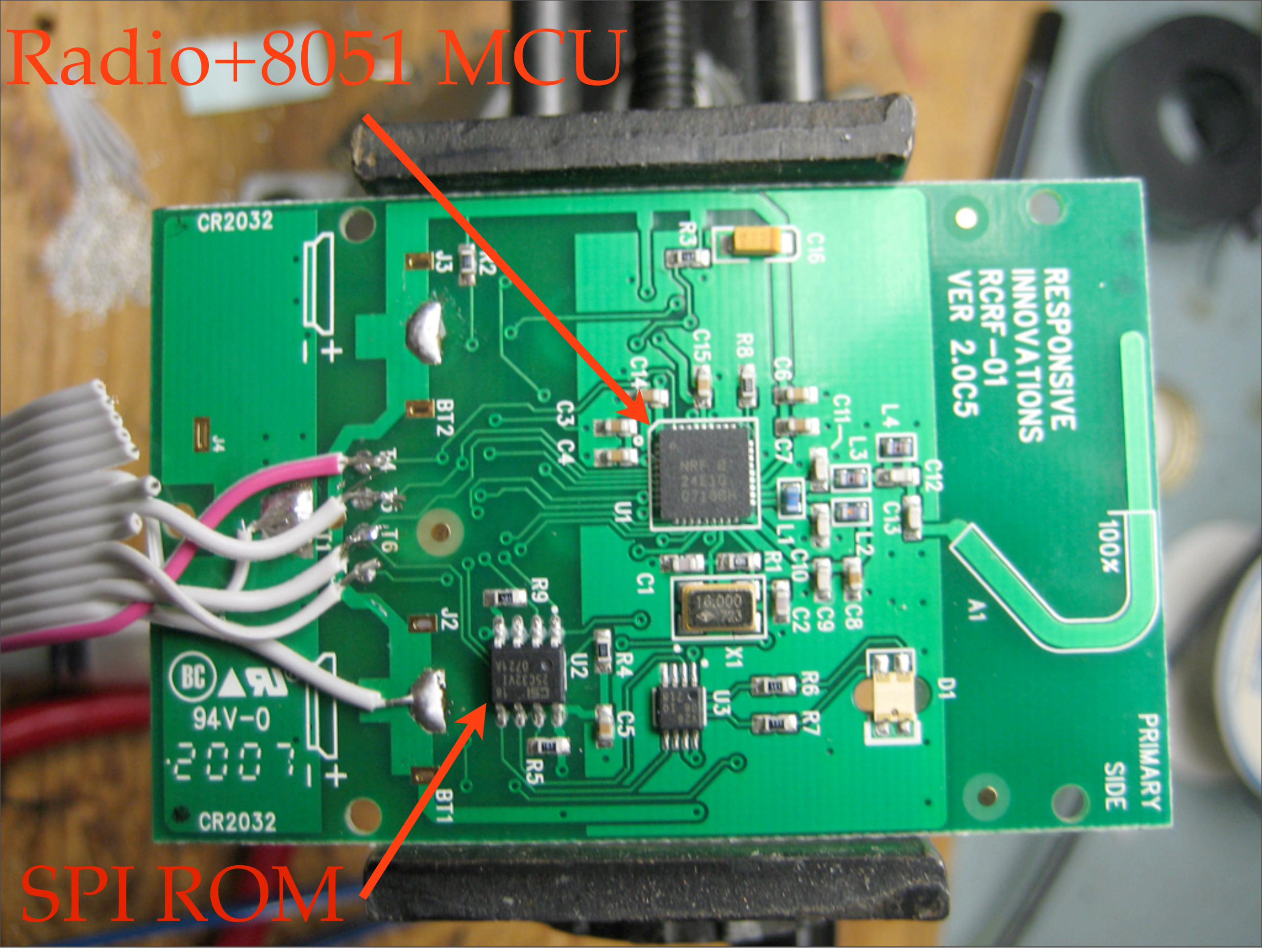
Name	Address	Description
FSCTRL1	0x000B	Frequency Synthesizer Control
IOCFG0	0x0002	GDO0 Output Pin Configuration
FSCTRL0	0x000C	Frequency Synthesizer Control
FREQ2	0x000D	Frequency Control Word, High Byte
FREQ1	0x000E	Frequency Control Word, Middle Byte
FREQ0	0x000F	Frequency Control Word, Low Byte
MDMCFG4	0x0010	Modem Configuration
MDMCFG3	0x0011	Modem Configuration
MDMCFG2	0x0012	Modem Configuration
MDMCFG1	0x0013	Modem Configuration
MDMCFG0	0x0014	Modem Configuration
CHANNR	0x000A	Channel Number
DEVIATN	0x0015	Modem Deviation Setting

Friday, May 20, 2011



Friday, May 20, 2011

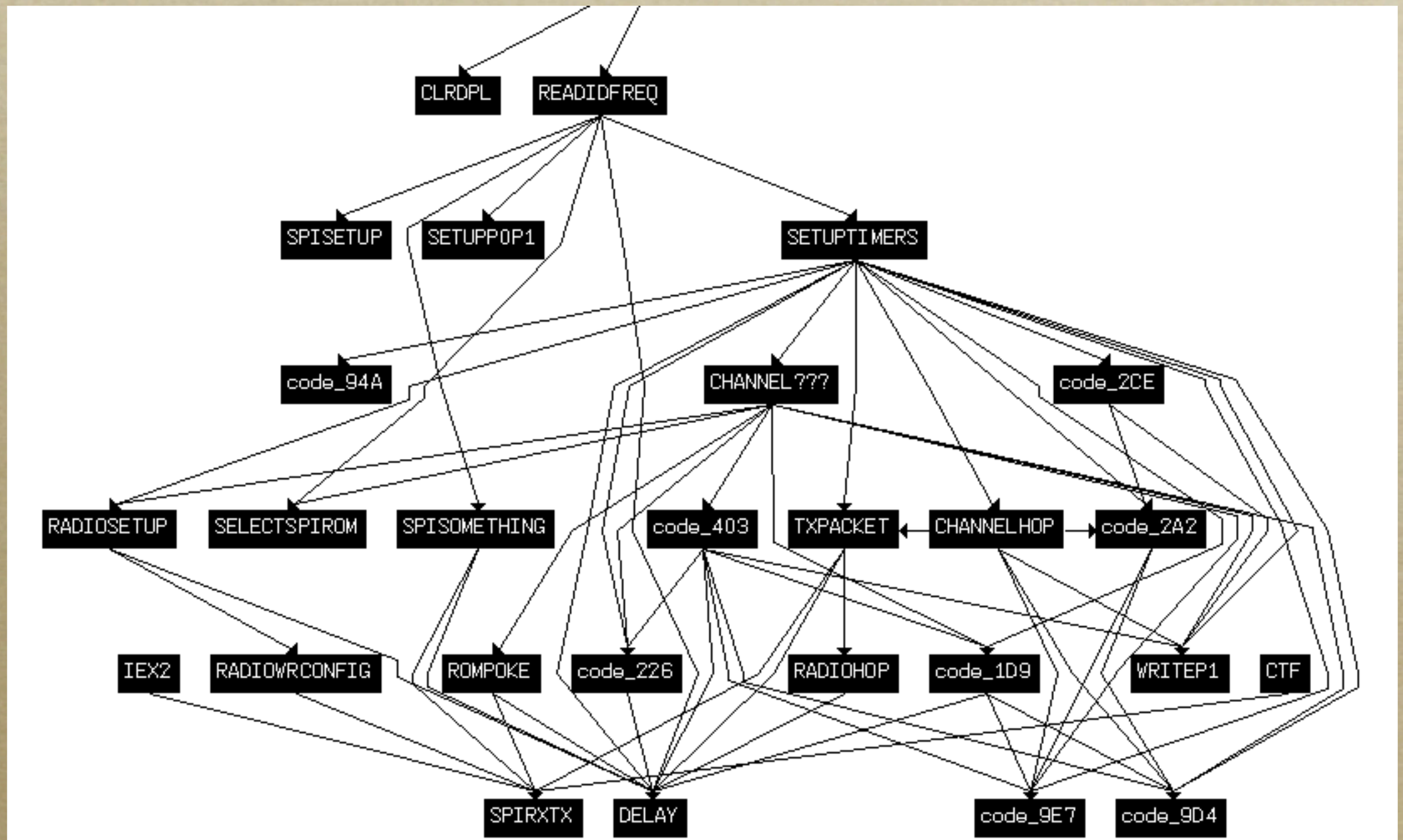

SW9


Radio+8051 MCU
SPI ROM
CR2032
RESPONSIVE
INNOVATIONS
RCRF-01
VER 2.0C5
PRIMARY
SIDE
94V-0
CR2032

Clicker Firmware Extraction

- SPI Flash is External
  - No code protection. Just read it!
- First 7 octets are metadata.
- Eighth octet loads into CODE:0x0000.

Just 3kB of Code



Transmit Function

- Sends these bytes:
  - (1E) (1F) (20) //Sync
  - (1B) (1C) (1D) //Dest Address
  - (input) //Button (ASCII)

Sync Code

- MOV 0x1E, #0x12
- MOV 0x1F, #0x34
- MOV 0x20, #0x56

- Sync is 0x123456.

Sniffing Constant Sync

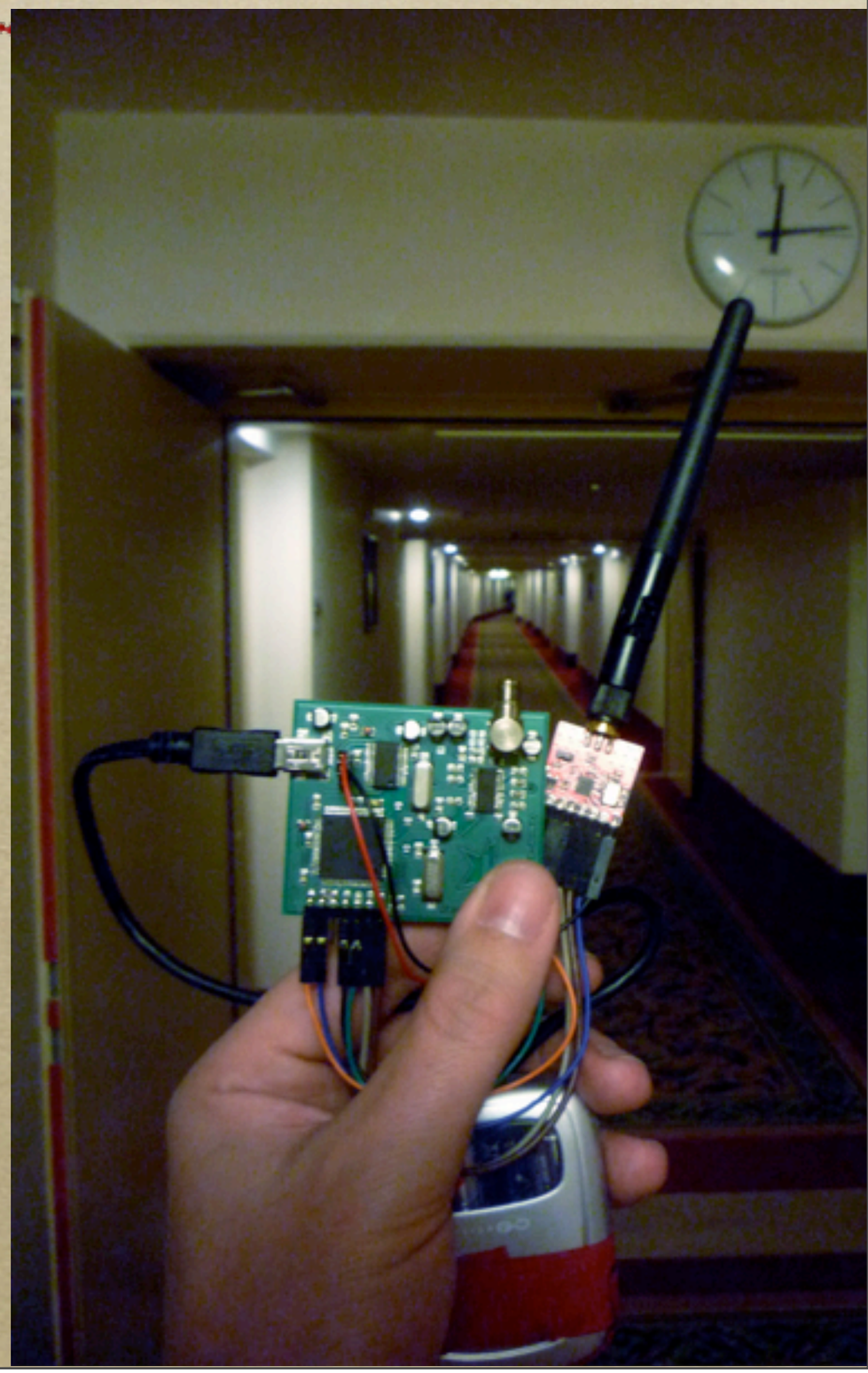
```
client.RF_setfreq((2400+0x29) * 10**6);
client.poke(0x06,0x00); #1Mbps
client.poke(0x07,0x78); #Reset status register

client.RF_setmaclen(3); # SETUP_AW for 3-byte addr
client.RF_setsmac(0x123456);
client.RF_setpacketlen(4);

#Power radio, prime for RX, two-byte checksum.
client.poke(0x00,0x70|0x03|0x04|0x08);
```

```
air-2% goodfet.nrf sniffftp | head
Listening as 0000123456 on 2441 MHz
  1f 87 60 35
  1f 87 60 35
  1f 87 60 35
  1f 87 60 35
  1f 87 60 35
  1f 87 60 35
  1f 87 60 35
  1f 87 60 35
  1f 87 60 35
```

This method sucks:
1) Repeat for every device.
2) Helpless if devices have unique Syncs.

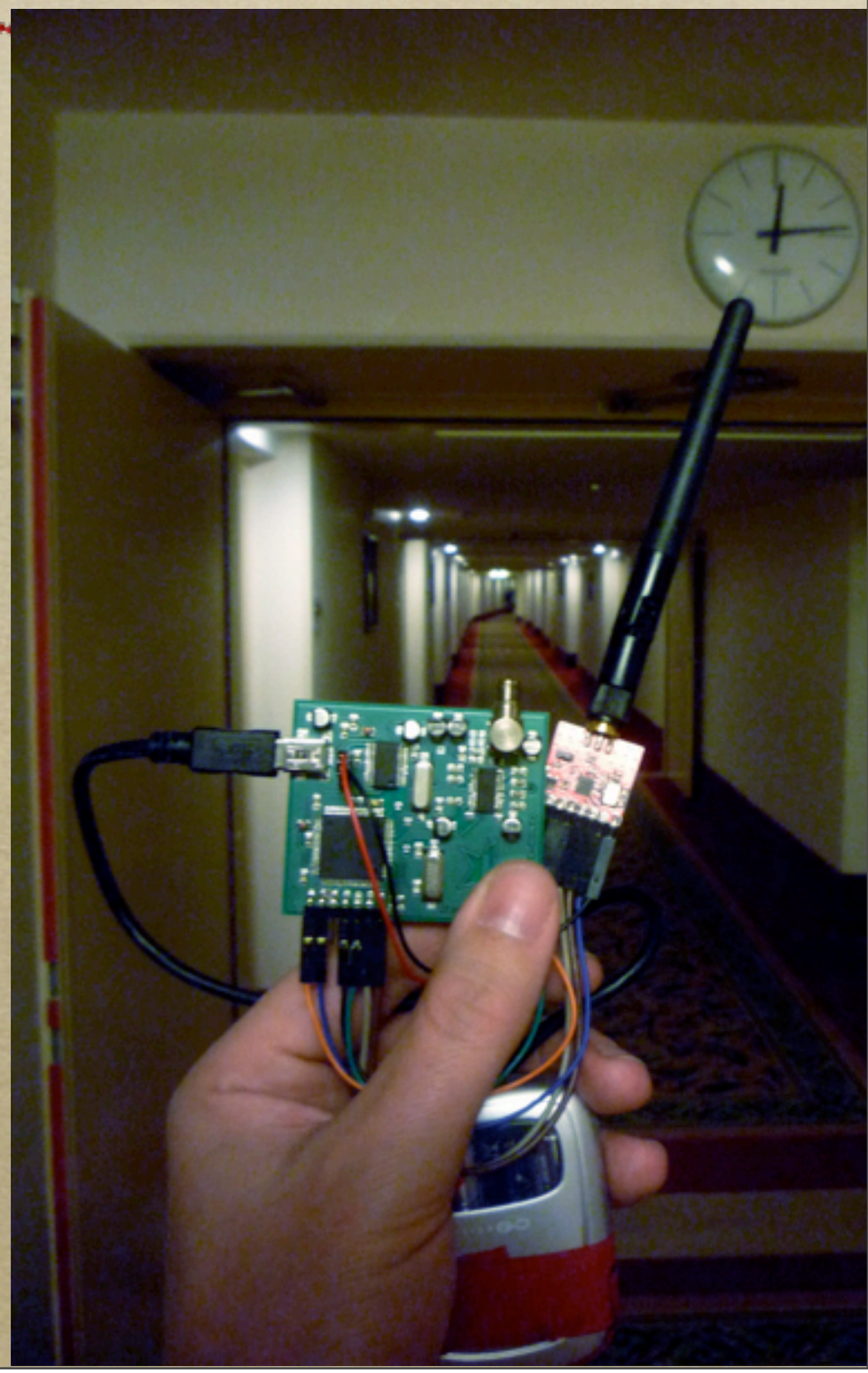
Keykeriki and Ubertooth

- Fast MCU
- Raw Radio
- Software Filtering
  - (Not SDR)



Keykeriki

- Moser and Schröder
- Amiccom A7125
  - Raw 2FSK Radio
  - Bits on a wire.
- ARM Processor
  - 2 Megabaud in Software



Ubertooth

- Michael Ossmann
- Sniffs Bluetooth Channels
- Software matching on Preamble/Sync

Autotuning

```
air-2% goodfet.nrf autotune
Autotuning as 0000000055 on 2499 MHz
sync,mac,r5,r6
Tuned to 2480 MHz
Tuned to 2481 MHz
'55,0102030201,51,09' looks valid          1          0.00820
'55,0102030201,51,09' looks valid          2          0.01600
'55,0102030201,51,09' looks valid          3          0.02326
'55,0102030201,51,09' looks valid          4          0.02837
Tuned to 2482 MHz
Tuned to 2483 MHz
```

Autotune Trick

- Reduce match length to minimum.
- Hardware match on the *Preamble*,
  - as if it were a Sync,
  - preceded by noise,
  - tossing out false positives.
- Match on Sync once it’s found.

Match Preamble as a Sync

- Preamble is often predictable.
  - 0xAA* or 0x55* for 2FSK.
  - 0x00* for DSSS.
- Match on it!

Minimum Sync Length

- Radio preambles are short.
  - Reduces power consumption.
- Radio Syncs are long.
  - Reduces false positives.

Minimum Sync Length

03	SETUP_AW			
	Reserved	7:2	000000	R/W
	AW	1:0	11	R/W

RX/TX Address field width

'00' - Illegal

'01' - 3 bytes

'10' - 4 bytes

'11' – 5 bytes

LSByte is used if address width is below 5 bytes

2 bytes!

Noise Characterization

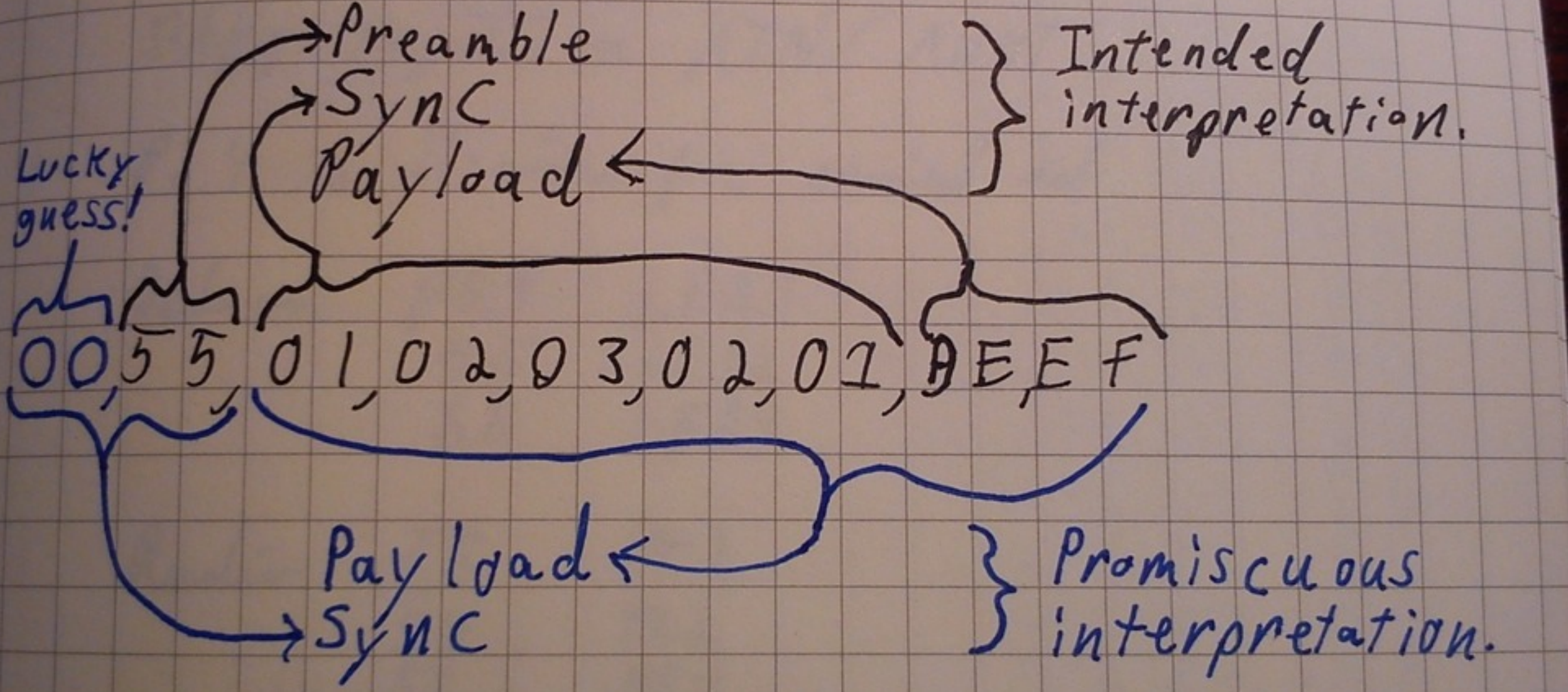
- 00*, Noise is beneath center.
- FF*, Noise is above center.
- 55* || AA*, Clock feedback.

Precede Sync by Noise

- Noise is most often 00*, FF*, 55*, or AA*.
- Preamble is 55 or AA.

- 0055 and 00AA are good choices.
- 5555 and AAAA are idiotic choices.

nRF24L01+ Sniffer Diagrams



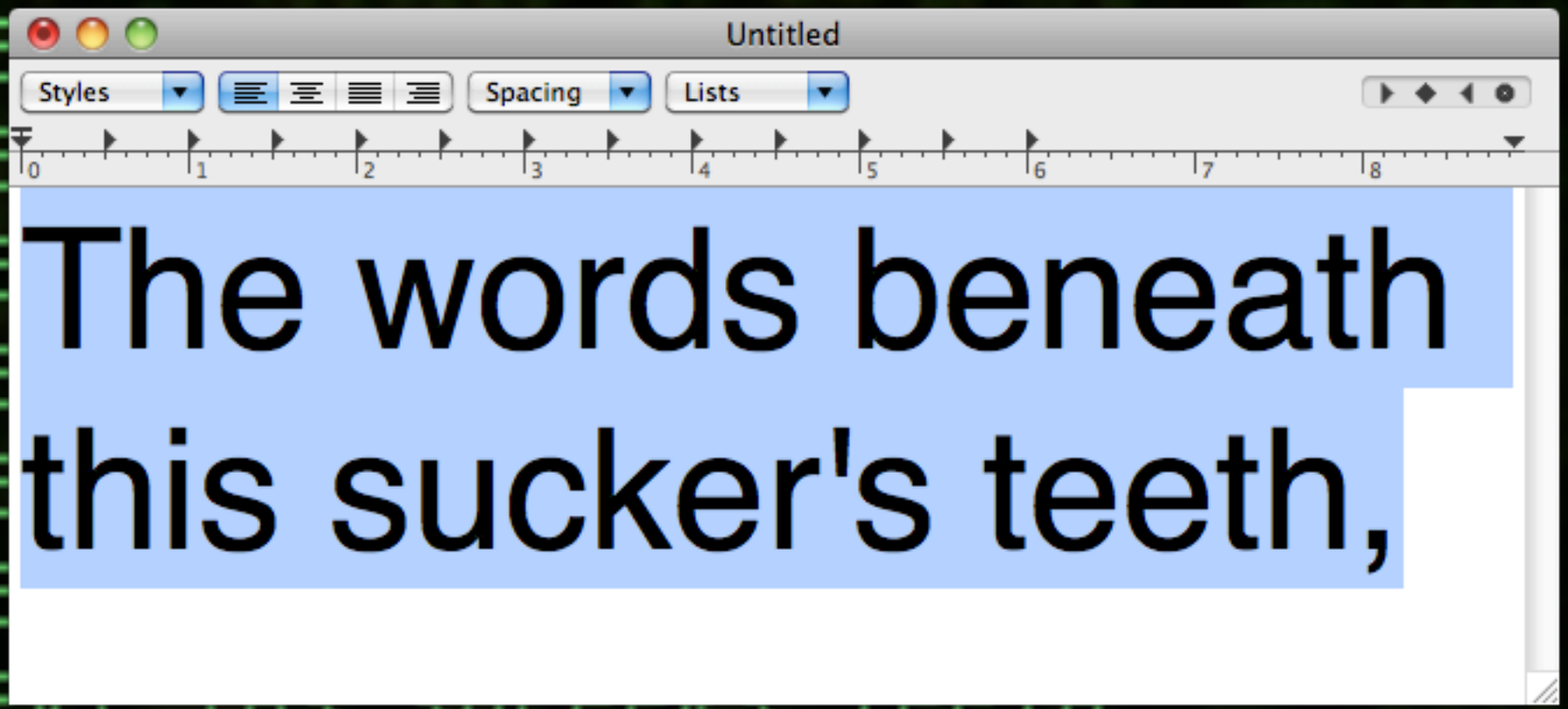
False Positives

- False positives are predictable,
  - Look like background noise.
  - Common values can be filtered.

False Positives

- 55 FF FF FF FF FF
- FF FF FF E0 00 00
- AA AA AB 55 55 55
- 01 02 03 02 01
- AA AA AA AA AA

```
#  TE_ORDS_BENEEAT_THS_SU
#  TE_ORDS_BENEEAT_THS_SUC
#  TE_ORDS_BENEEAT_THS_SUCE
#  TE_ORDS_BENEEAT_THS_SUCEE
#  TE_ORDS_BENEEAT_THS_SUCEER
Unknown character 0x34.
#  TE_ORDS_BENEE
#  TE_ORDS_BENEE
#  TE_ORDS_BENEE
#  TE_ORDS_BENEE
#  TE_ORDS_BENEE
#  TE_ORDS_BENEE
Unknown character 0x36.
#  TE_ORDS_BENEEAT_THS_SUCEERS_TEETH_
```



Friday, May 20, 2011

Reversing by Autotune

- Less need for firmware.
- Breaks in minutes, not days.

```
air-2% goodfet.nrf autotune
Autotuning as 0000000055 on 2499 MHz
sync,mac,r5,r6
Tuned to 2480 MHz
Tuned to 2481 MHz
'55,0102030201,51,09' looks valid          1          0.00820
'55,0102030201,51,09' looks valid          2          0.01600
'55,0102030201,51,09' looks valid          3          0.02326
'55,0102030201,51,09' looks valid          4          0.02837
Tuned to 2482 MHz
Tuned to 2483 MHz
```

Reversing by Autotune

- Before Autotuning,
  - Dump firmware.
  - Reverse with IDA.
  - Load registers and sniff.
- Autotune is faster.
  - But it doesn’t always work.

Another Way

- Some radios have no Preamble!
- How else can we find the Sync?

Software Matching

- Sniff with a short, noisy Sync.
- Search for known plaintext.

Software Matching

```
pro% goodfet.nrf sniffprom 0xAA | grep --color "19 92 44"
 df ed ff aa aa ff aa af fd 7f 12 34 56 19 92 44 35 0e bb 5f
 aa d5 bf aa aa ff ff bf fd 7f 12 34 56 19 92 44 35 0e bb 5f
 b6 ff ff aa aa ff aa b5 fd 7f 12 34 56 19 92 44 35 0e bb 7f
 a9 ad 5f aa aa ff eb 56 fd 5f 12 34 56 19 92 44 35 0e bb 5f
 ae aa ff aa aa ff aa ad fd 7f 12 34 56 19 92 44 35 0e bb 5f
 ff ed 57 fd 7f 12 34 56 19 92 44 35 0e bb 6f e4 75 94 ba 51
 aa aa ef aa aa ff aa ab f9 55 12 34 56 19 92 44 35 0e bb 7f
 ea ef ff ea aa ff fd ff fd 7f 12 34 56 19 92 44 35 0e bb 57
 aa af 5f aa aa ff ff ff fd 7f 12 34 56 19 92 44 35 0e bb 7b
 ab 6b 57 aa aa ff ff ff fd 55 12 34 56 19 92 44 35 0e bb 5f
 b6 aa bf aa ab ff ff ff fd 7f 12 34 56 19 92 44 35 0e bb 7d
 a6 d7 5f aa aa fe b5 ad fd 55 12 34 56 19 92 44 35 0e bb 56
 a5 45 a2 99 69 55 50 55 52 40 2a aa ef 7f ea af ff ff ff fd
 ff ff ff fd 7f 12 34 56 19 92 44 35 0e bb 5f ff 7f ff f6 ff
```

12 34 56

```
ff aa af fd 7f 12 34 56 19 92 44
ff ff bf fd 7f 12 34 56 19 92 44
ff aa b5 fd 7f 12 34 56 19 92 44
ff eb 56 fd 5f 12 34 56 19 92 44
ff aa ad fd 7f 12 34 56 19 92 44
12 34 56 19 92 44 35 0e bb 6f e4
```

Conclusions

- Layer 1 is unexplored.
  - New vulnerabilities waiting.
  - New techniques needed.

Spoilers

- This lecture:
  - Packets outside of packets.
  - Sniffing beneath Layer 2.
- Coming soon:
  - Packets *inside* of packets.