

Other Wireless

New ways to be Pwned

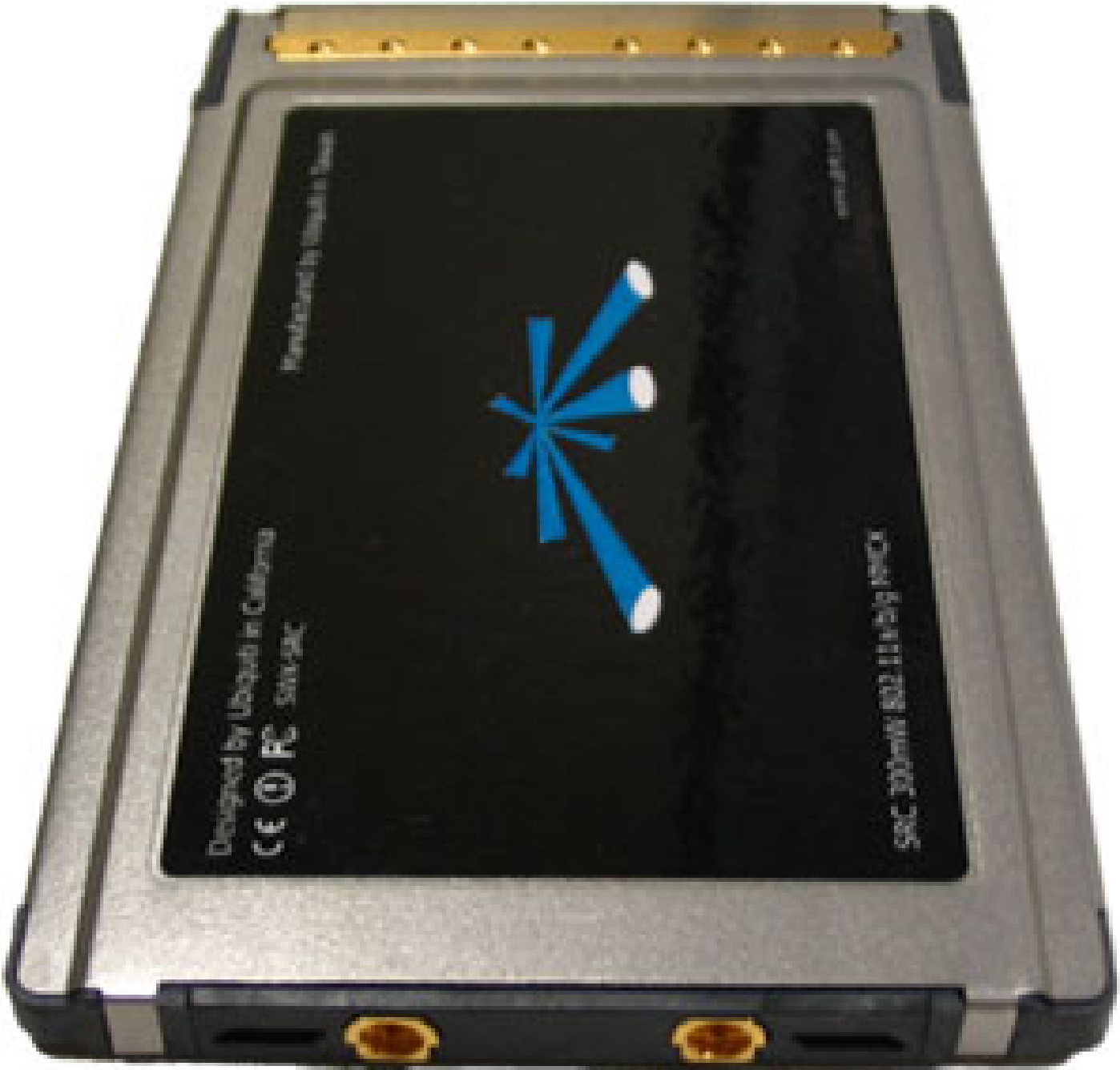
Luis Miras

<http://dwerd.blogspot.com>

luis@ringzero.net

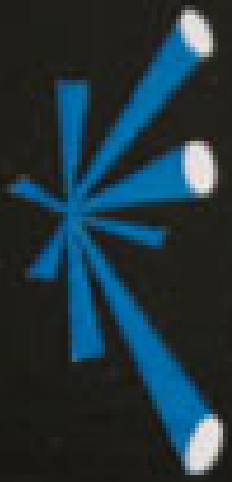
What I'm *Not* Covering





Designed by Ubiquiti in California
CE FCC

Manufactured by Ubiquiti in Taiwan



SPEC 300min 802.11n/b/g/n/AC

www.ubnt.com





What I *Will Be* Covering









Attack

- Passive (Sniffing)
 - authentication data
 - sensitive data
- Active (Injection)
 - Denial of Service
 - Execution of arbitrary commands

RF

- RF design is hard, not needed.
- Scanners are not needed.
- Devices come with TX and RX circuits.
(use them)
- Think of TX and RX circuits as a network socket.

Let's get HIDphy!!



HID – human interface device

- Keyboard
 - HID codes similar to ps/2 scan codes
- Mice
 - Relative movements and buttons
 - Positional movement and buttons



HID Device Info "Wireless Presentation Remote"



Vendor Name: Kensington
Product Name: Wireless Presentation Remote
Serial No:

VID: 047D
PID: 2010
Version: 0100

Languages

--

max Report Length
(including Report ID):

Input: 9
Output: 0
Feature: 0

Strings

2) Kensington
3) Wireless Presentation Remote
4) 0008001
5) Wireless USB Device

Collections

<input type="checkbox"/> Wireless Presentation Remote
└─ Generic Desktop: Keyboard (Application)

Device Research

Wireless Presentation Remote

Serial No. Model #: 33062

F0526077081

Kensington Technology Group

www.kensington.com

FCC ID:GV333062

800-535-4242 Rating: 3V 0.01A

Tested to comply with FCC Standards.

FOR HOME OR OFFICE USE.

900-0875-00



Made in China

OET List Exhibits Report - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://gullfoss2.fcc.gov/prod/oet/cf/eas/reports/\

FCC Home | Search | Updates | E-Filing | Initiatives | For Consumers | Find People

Federal Communications Commission

Office of Engineering and Technology










FCC > FCC E-filing > EAS > List Exhibits Page

OET Home Page

FCC Site Map

OET Exhibits List

9 Matches found for FCC ID 'GV333062'

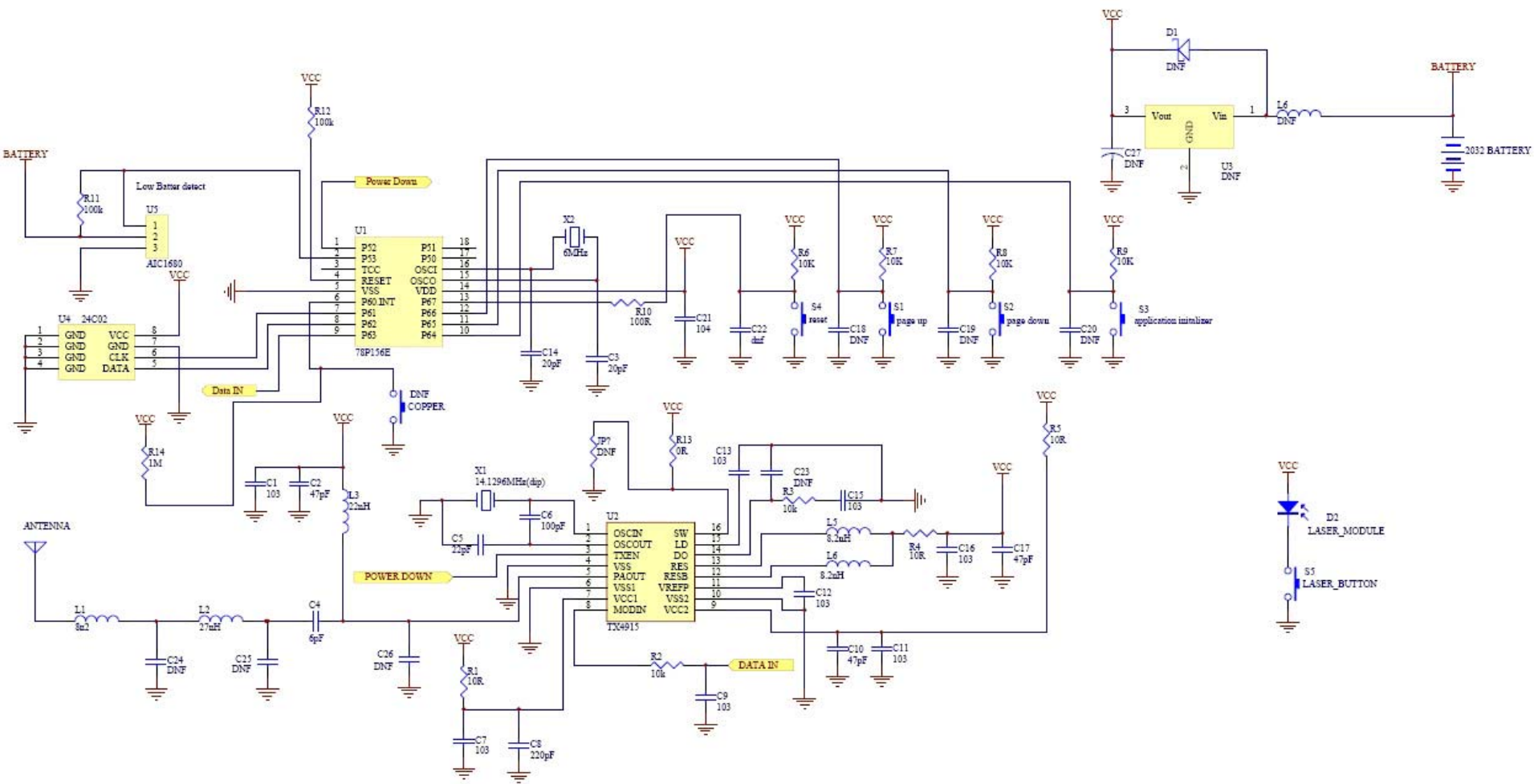
View Attachment	Exhibit Type	Description of Exhibit	Date Submitted to FCC	Display Type	Date Available
	Block Diagram	BLOCK DIAGRAM	10/02/2003	pdf	10/02/2003
	External Photos	EXTERNAL PHOTOS	10/02/2003	pdf	10/02/2003
	ID Label/Location Info	ID LABEL SAMPLE AND LOCATION	10/02/2003	pdf	10/02/2003
	Internal Photos	INTERNAL PHOTOS	10/02/2003	pdf	10/02/2003
	Operational Description	OPERATIONAL DESCRIPTION	10/02/2003	pdf	10/02/2003
	Schematics	CIRCUIT DIAGRAM	10/02/2003	pdf	10/02/2003
	Test Report	TEST REPORT	10/02/2003	pdf	10/02/2003
	Test Setup Photos	TEST SETUP PHOTOS	10/02/2003	pdf	10/02/2003
	Users Manual	MANUAL	10/02/2003	pdf	10/02/2003

Filing Options

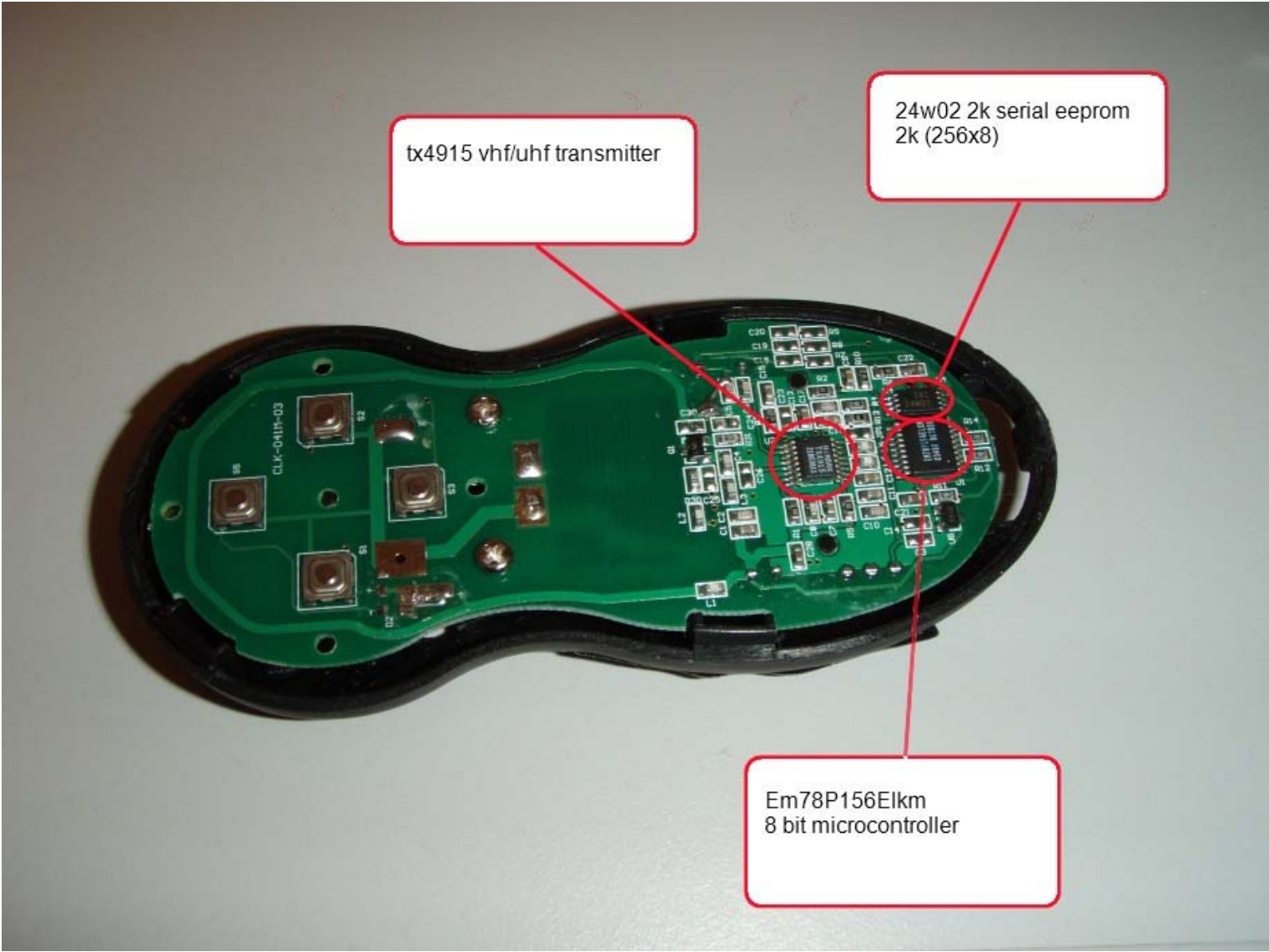
- [Grantee Registration](#)
- [Modify Grantee Information](#)
- [Form 731](#)
- [Complete Unfinished Form 731](#)
- [Add Attachments](#)
- [Submit Correspondence](#)
- [Register New Test Firm](#)
- [Renew Test Firm/Add Exhibits](#)
- [Test Firm Accrediting Body Login](#)
- [Return to 159 Form](#)

Reports

- [Pending Application Status](#)
- [Generic Search](#)
- [Grantee Search](#)



Device Internals



tx4915 vhf/uhf transmitter

24w02 2k serial eeprom
2k (256x8)

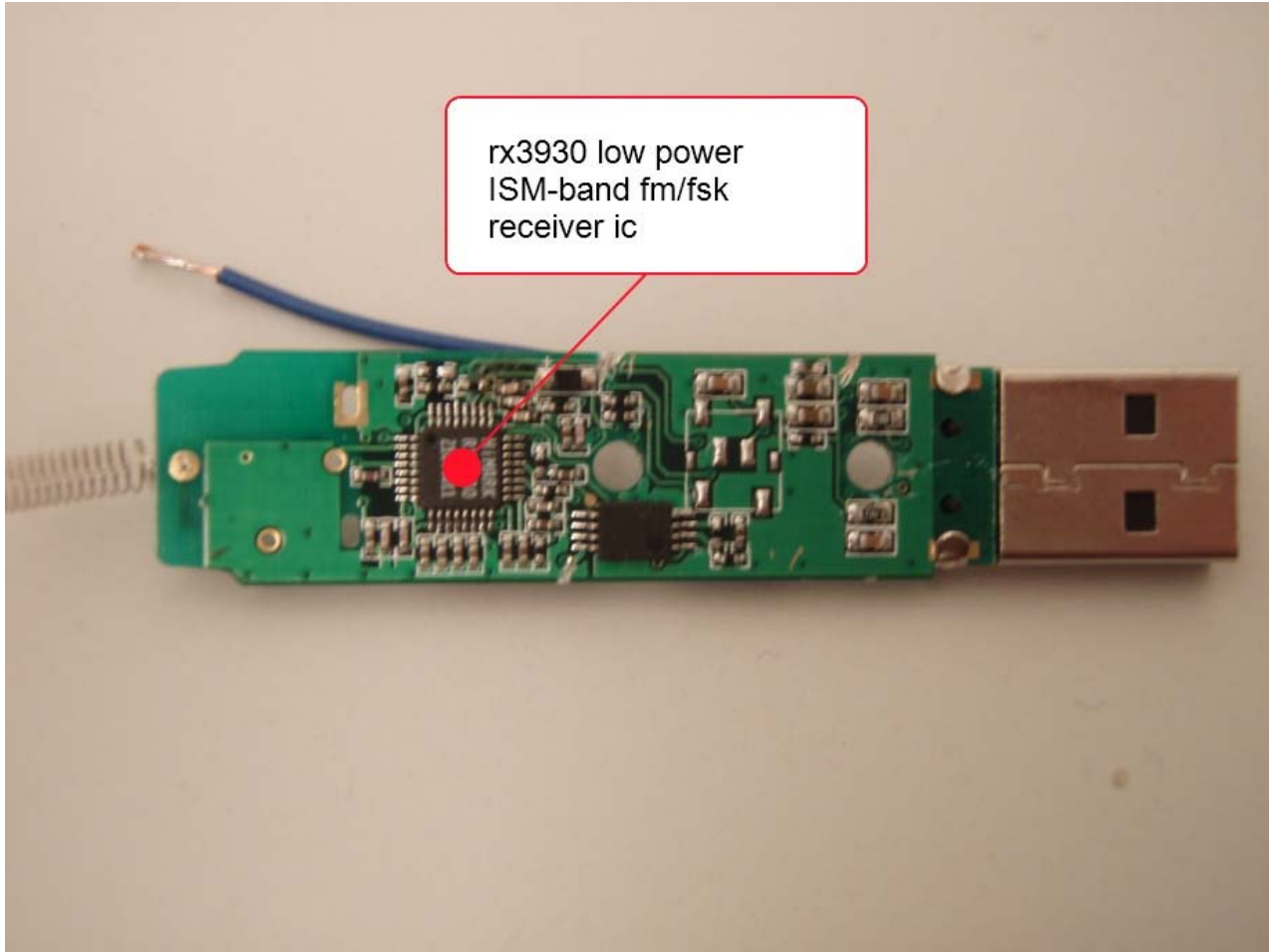
Em78P156Elkm
8 bit microcontroller

cy7c63723 usb/ps2
microcontroller

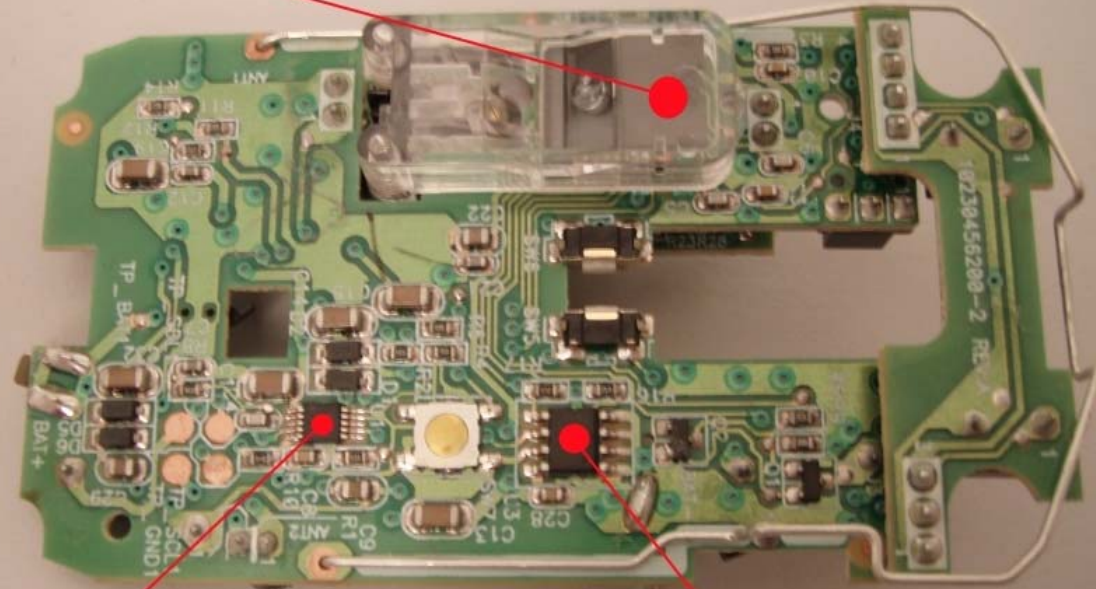
24w02 serial eeprom
2k (256x8)



rx3930 low power
ISM-band fm/fsk
receiver ic



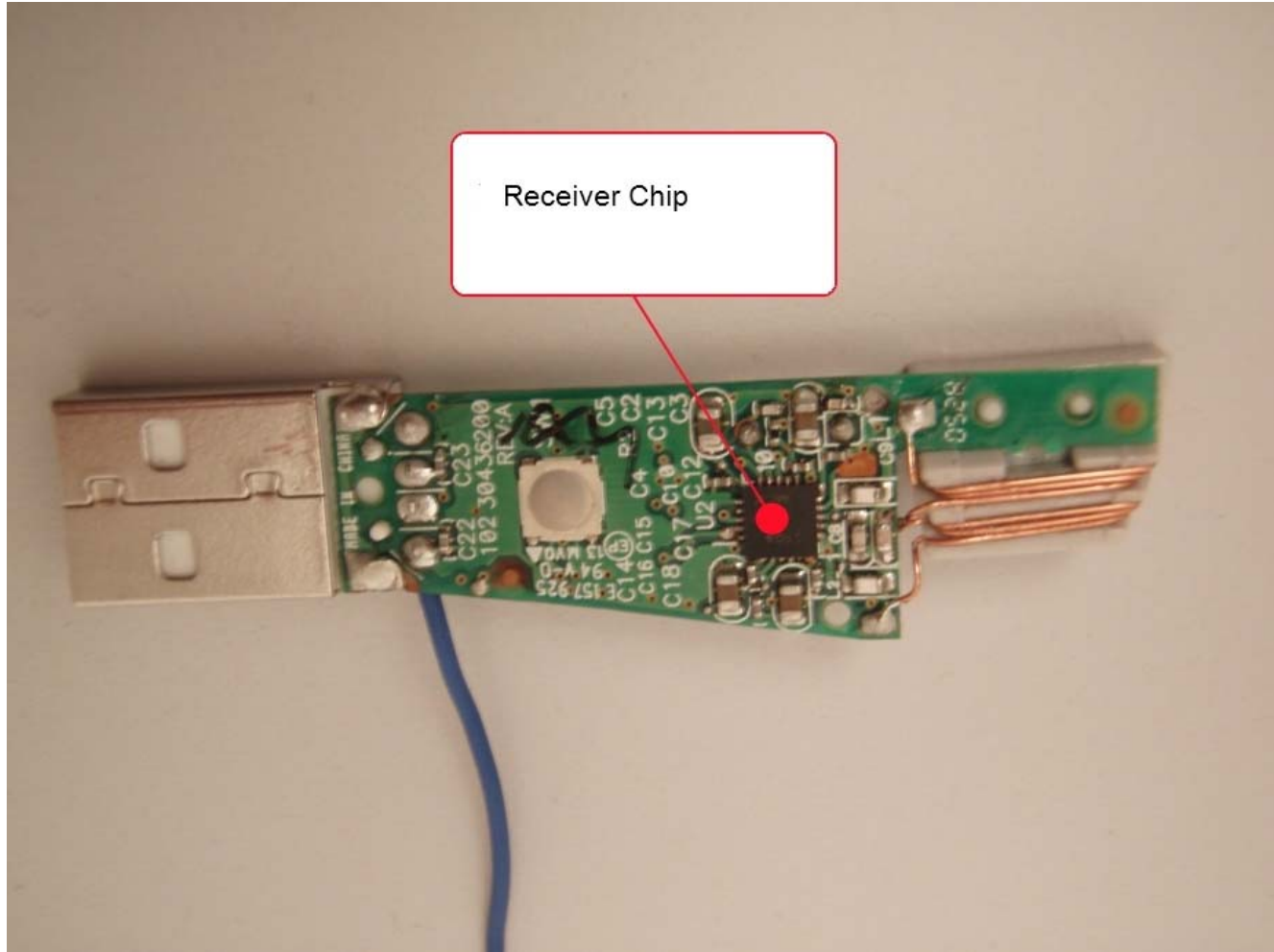
Microcontroller

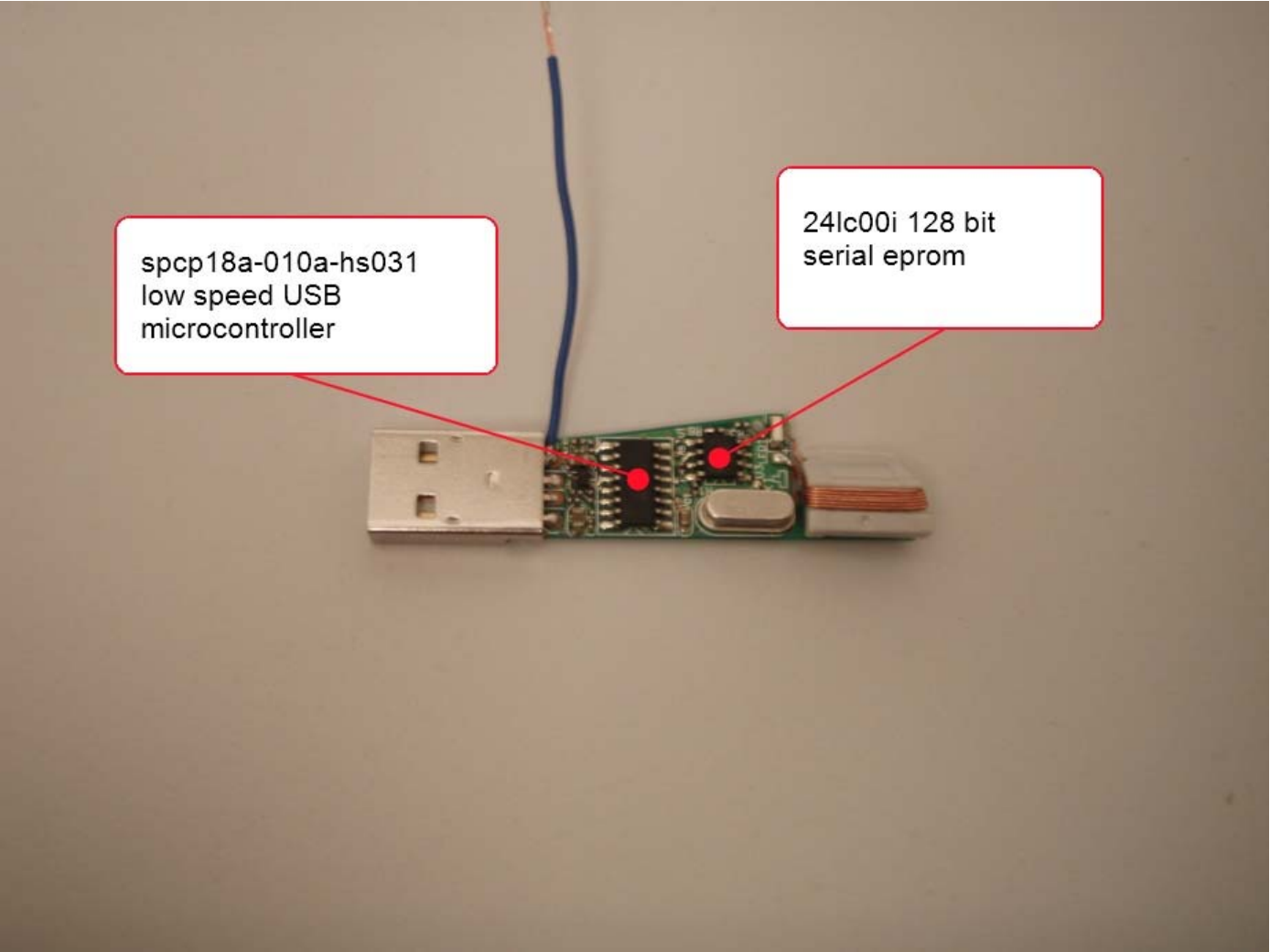


TX Chip

24aa16i 16kbit i2c
serial eeprom

Receiver Chip





A photograph of a custom USB device. The device consists of a green printed circuit board (PCB) with a silver USB-A connector on the left and a white cable on the right. A blue wire is connected to the top of the PCB. Two callout boxes with red borders and red lines pointing to specific components are overlaid on the image. The left callout box points to a black integrated circuit (IC) on the PCB, and the right callout box points to a smaller component on the PCB.

spcp18a-010a-hs031
low speed USB
microcontroller

24lc00i 128 bit
serial eeprom

Device Reversing

Communication

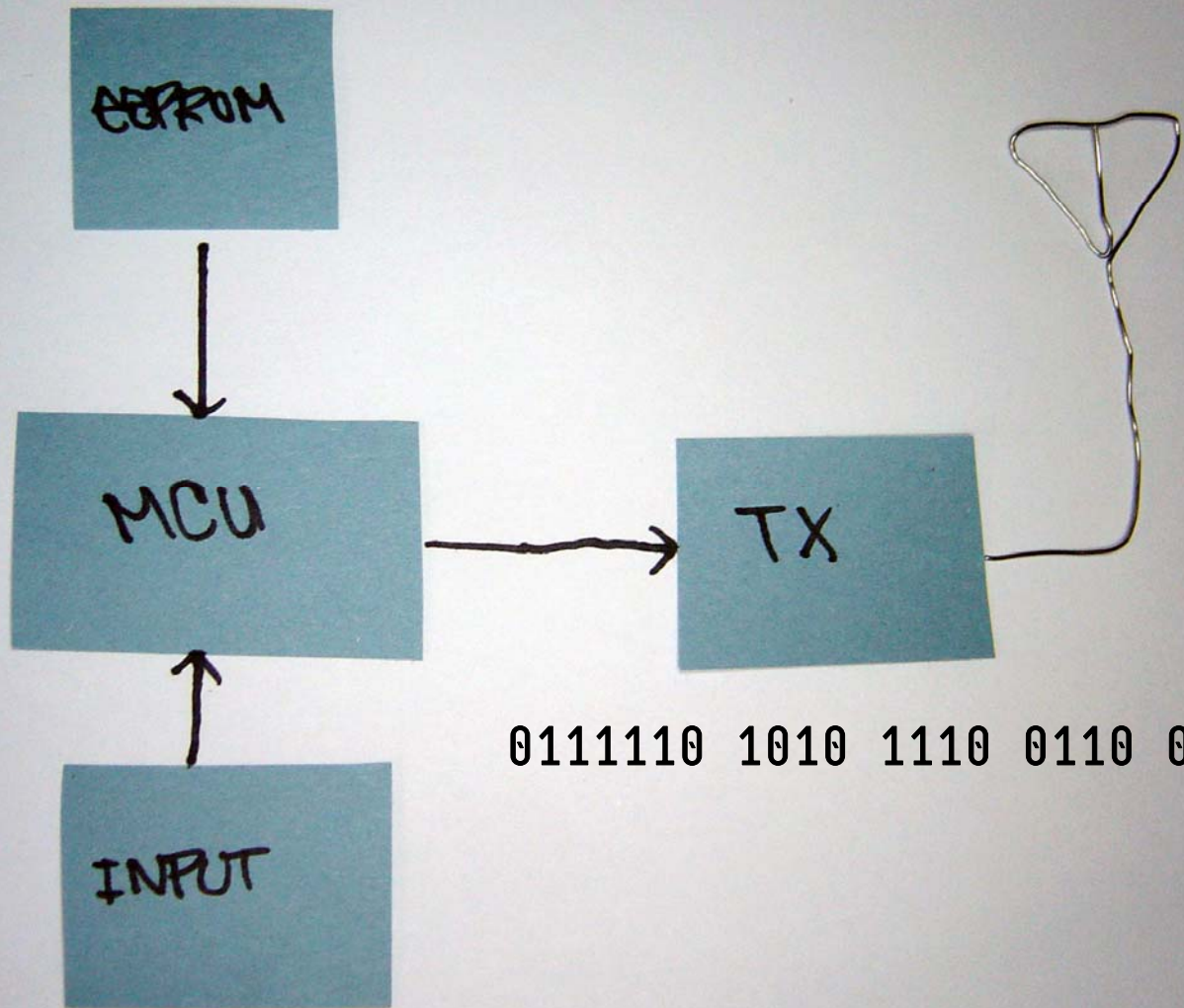
- One way traffic (replay attacks!)
 - except kb
- No standard data protocol
- Varied RF protocols and frequencies.
 - 27 Mhz
 - 900 Mhz
 - 2.4 Ghz



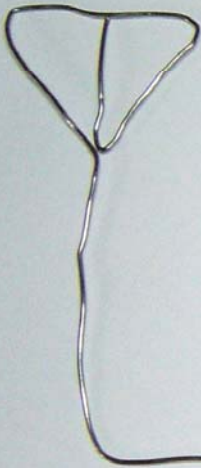
TX4915 Low Power ASK Transmitter IC

Applications

- ◆ Wireless mouse
- ◆ Car alarm and home security systems
- ◆ Remote control systems



0111110 1010 1110 0110 0100



RX



EEPROM



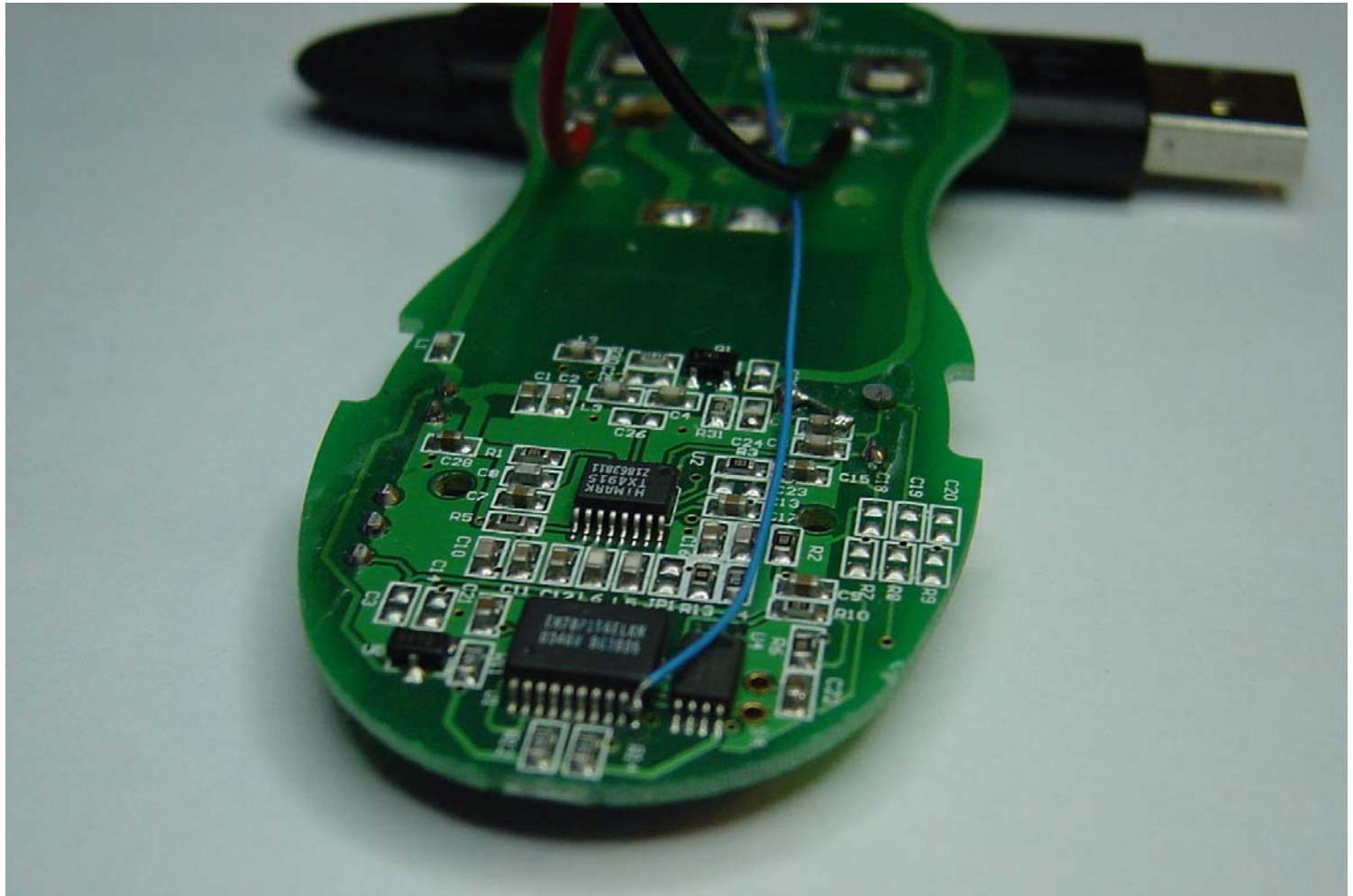
MCU
USB



0111110 1010 1110 0110 0100

Reversing the protocol

- One way messages must include
 - Authentication data (serial number)
 - Data
- Tap at the input to the TX Chip
 - No noise or errors
- Tap at the output of RX to verify and build the sniffer.





CH1

20Vpp Max

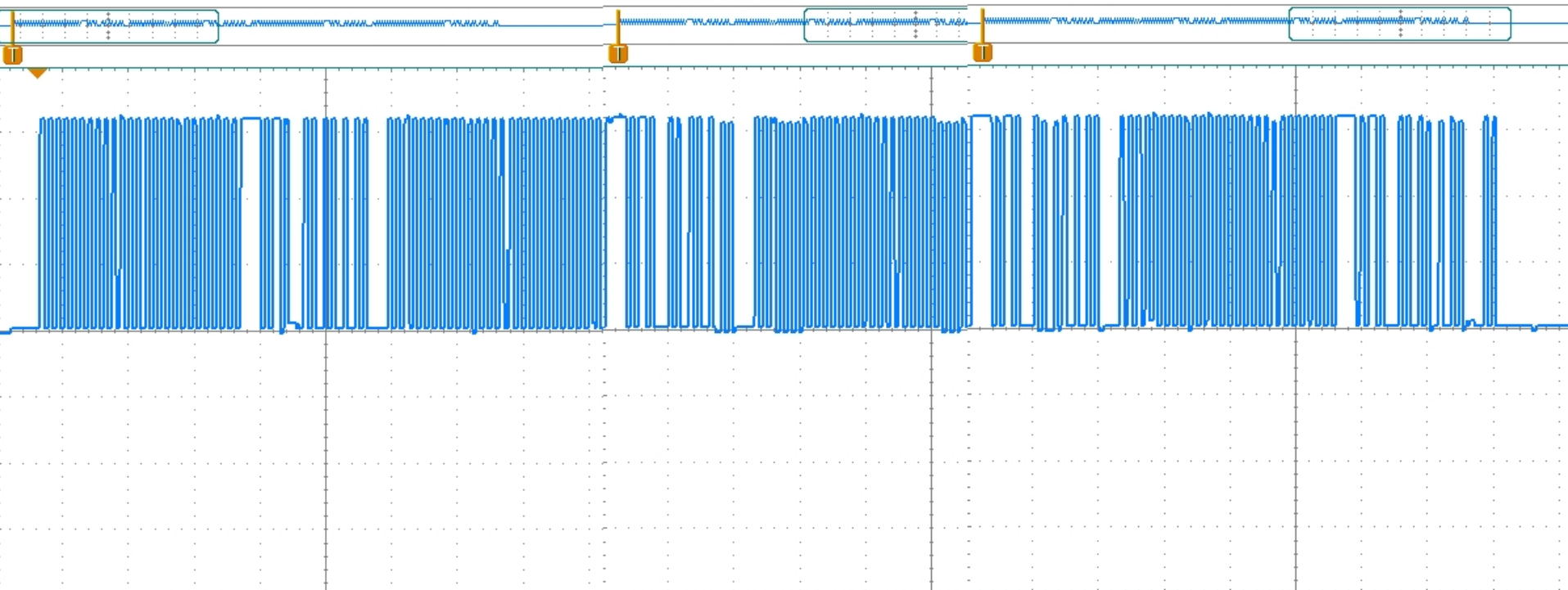
CH2

EXT Trigger TTL

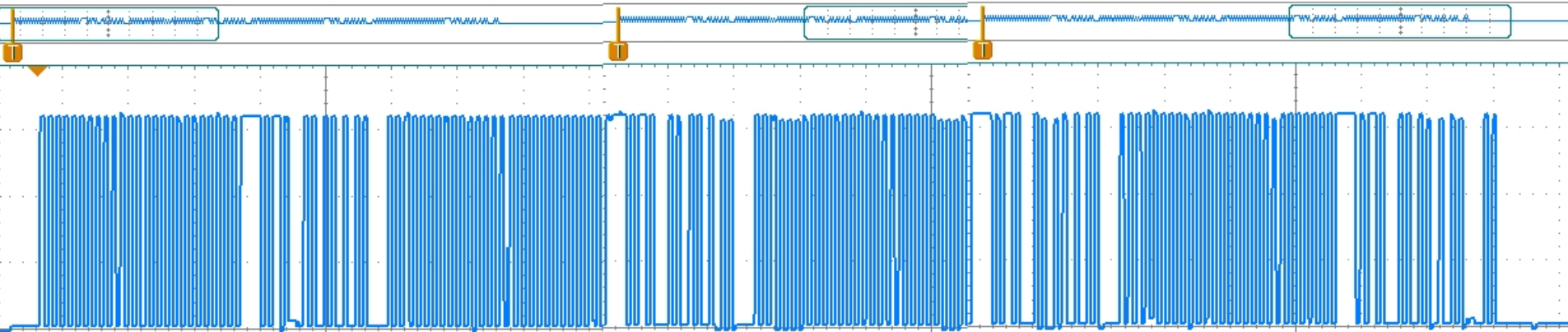
Parallax USB
Oscilloscope

PARALLAX
www.parallax.com





Vertical CH1 1V/DIV	Horizontal 2mS/DIV 25Ks/S	Trigger CH1 1.25V	Cursors TIME	Vertical CH1 1V/DIV	Horizontal 2mS/DIV 25Ks/S	Trigger CH1 1.25V	Vertical CH1 1V/DIV	Horizontal 2mS/DIV 25Ks/S	Trigger CH1 1.25V	Cursors TIME	Vertical CH1 1V/DIV	Horizontal 2mS/DIV 25Ks/S	Trigger CH1 1.25V
<input type="checkbox"/> 2.07	SETTINGS	BMP	OFF	<input type="checkbox"/> 2.07	SETTINGS	BMP	<input type="checkbox"/> 2.07	SETTINGS	BMP	OFF	<input type="checkbox"/> 2.07	SETTINGS	BMP



Data

Data

Data

Data

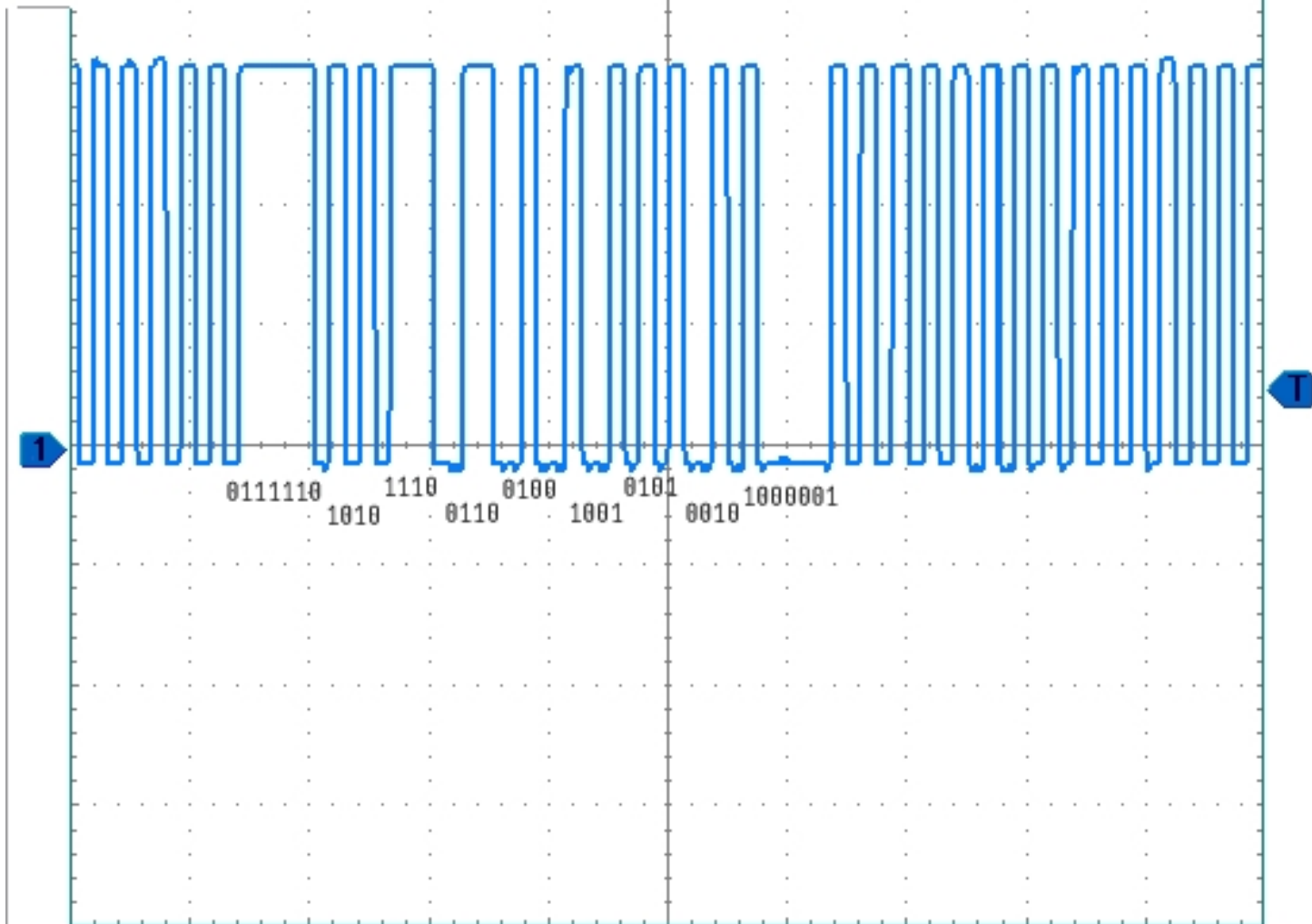
Vertical CH1 1V/DIV Horizontal 2mS/DIV 25Ks/S Trigger CH1 1.25 V Cursors TIME VOI

Vertical CH1 1V/DIV Horizontal 2mS/DIV 25Ks/S Trigger CH1 1.25 V Cursors TIME VOI

Vertical CH1 1V/DIV Horizontal 2mS/DIV 25Ks/S Trigger CH1 1.25 V Cursors TIME VOI

Vertical CH1 1V/DIV Horizontal 2mS/DIV 25Ks/S Trigger CH1 1.25 V Cursors TIME VOI

Save View as BMP



Vertical
CH1 200mV/DIV

Horizontal
1mS/DIV
50Ks/S

Trigger
CH1 0.62 V

Cursors
TIME VOLTS
OFF



2.07

SETTINGS

BMP

Reversing the Protocol

Page Down

01111110 1010 1110 0110 0100 1001 0101 0010 1000001

Page Up

01111110 1010 1110 0110 0100 1101 0101 0110 1000001

“Hide”

01111110 1010 1110 0110 0100 1011 0101 1010 1000001

Reversing the Protocol

Page Down

0111110 1010 1110 0110 0100 1001 0101 0010 **1000001**

Page Up

0111110 1010 1110 0110 0100 1101 0101 0110 **1000001**

“Hide”

0111110 1010 1110 0110 0100 1011 0101 1010 **1000001**

Reversing the Protocol

Page Down

1010 1110 0110 0100 1001 0101 0010

Page Up

1010 1110 0110 0100 1101 0101 0110

“Hide”

1010 1110 0110 0100 1011 0101 1010

Reversing the Protocol

Page Down

1010 1110 0110 0100 1001 **0101** 0010

Page Up

1010 1110 0110 0100 1101 **0101** 0110

“Hide”

1010 1110 0110 0100 1011 **0101** 1010

Reversing the Protocol

Page Down

1010 1110 0110 0100 **1001** 0101 **0010**

Page Up

1010 1110 0110 0100 **1101** 0101 **0110**

“Hide”

1010 1110 0110 0100 **1011** 0101 **1010**

Reversing the Protocol

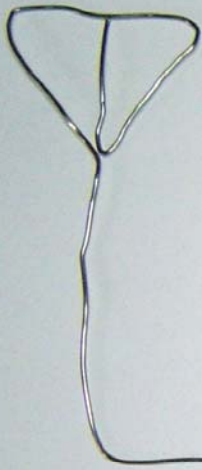
header	serial	data	serial	data	footer
0111110	XXXX XXXX XXXX XXXX	XXXX	XXXX	XXXX	01001

Attacks

BYOM (bring your own MCU)

- Ideally the original MCU would be reprogrammed
 - Most are OTP (One time programmable)
 - Can't read them, security fuse blown
- Our own MCUs are needed

Sniffing at the chiplevel



RX

EEPROM



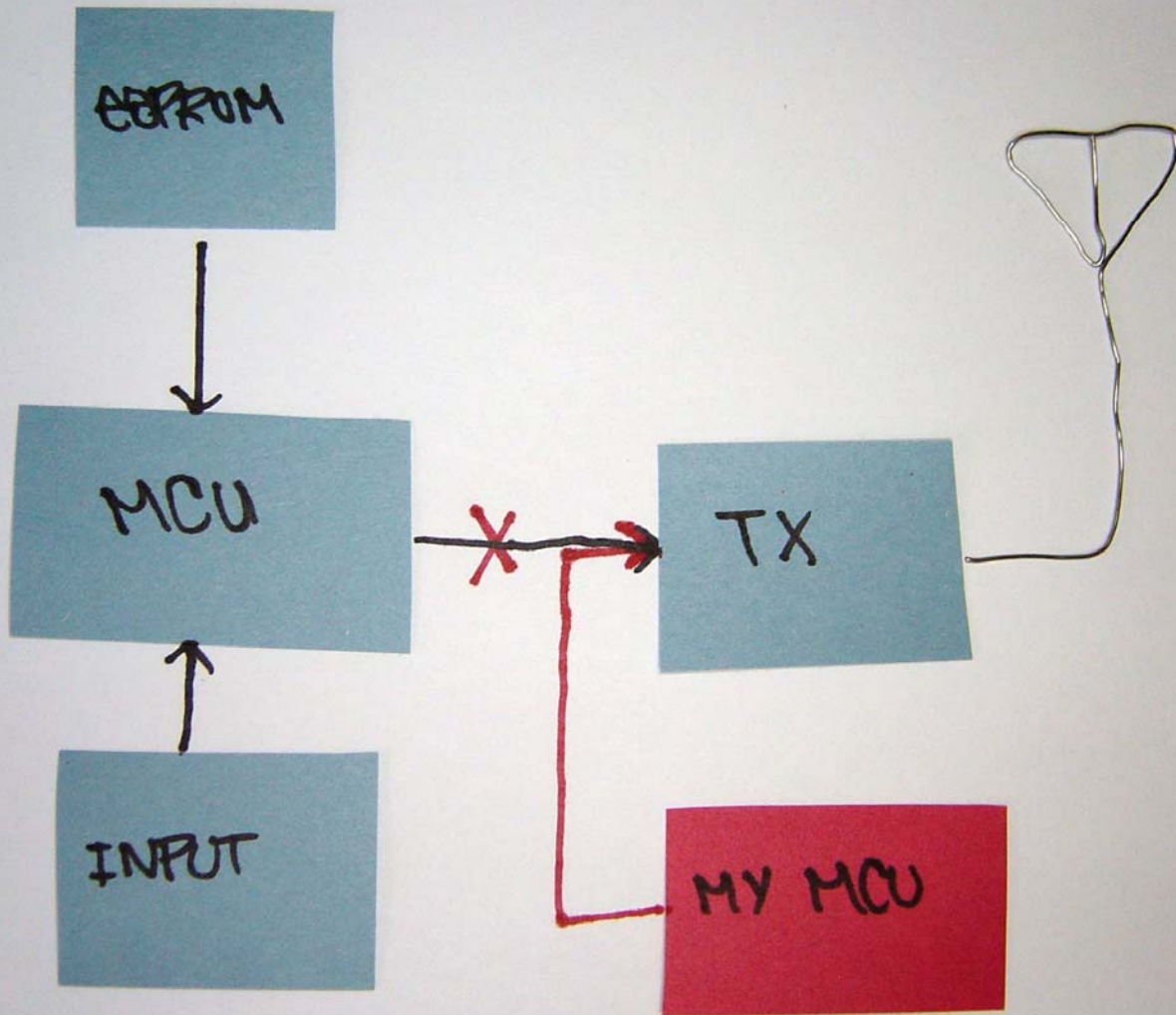
MCU
USB



MY MCU
USB



Injecting at the chip level



Passive attacks

- Needed to acquire authentication data
- Sensitive data from keyboards (passwords)
- Mouse data not very useful

Active attacks

- Attacks are HID type dependent
 - Keyboards (including presenters)
 - Mice

Active Keyboard Attacks



+ 'R' == (:

Run



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:

OK

Cancel

Browse...

Run



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:

iexplore http://www.attackersmachine.com|



OK

Cancel

Browse...

Run



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:

cmd|



OK

Cancel

Browse...

While at the cmd ...

Echo data to a bat file

Run the bat file

Active Mouse Attacks

What can be done by being able to inject mouse movement and clicks?

- Being able to see the screen.
(Attacking a live presentation)
- Blind

Accessibility for the Attacker



Blind Attacks

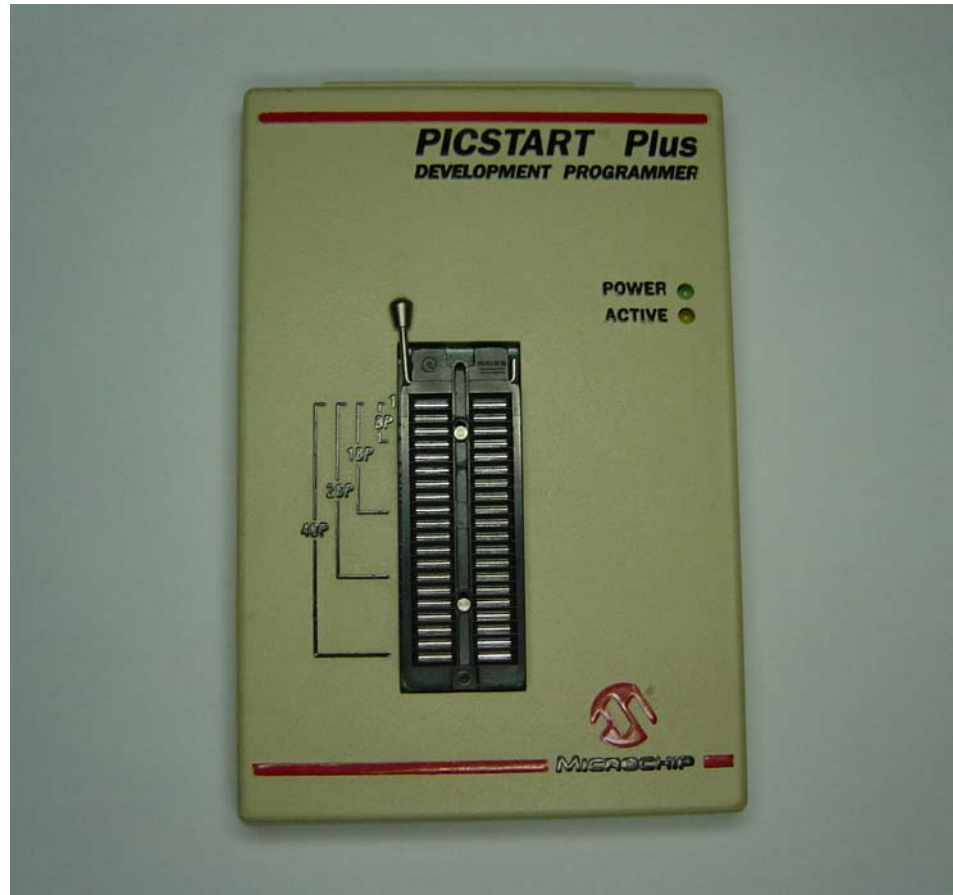
- No visual feedback.
- Educated guessing
- Mouse movement scripting

Getting Feedback

- Attempt to connect to controlled webserver
- Check logs
- Readjust and reattack

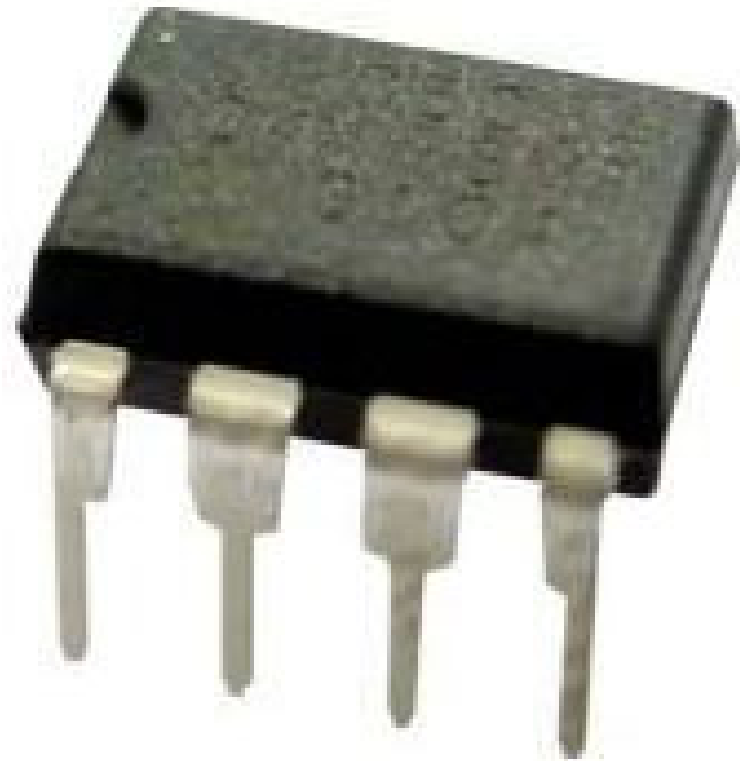
Microcontrollers

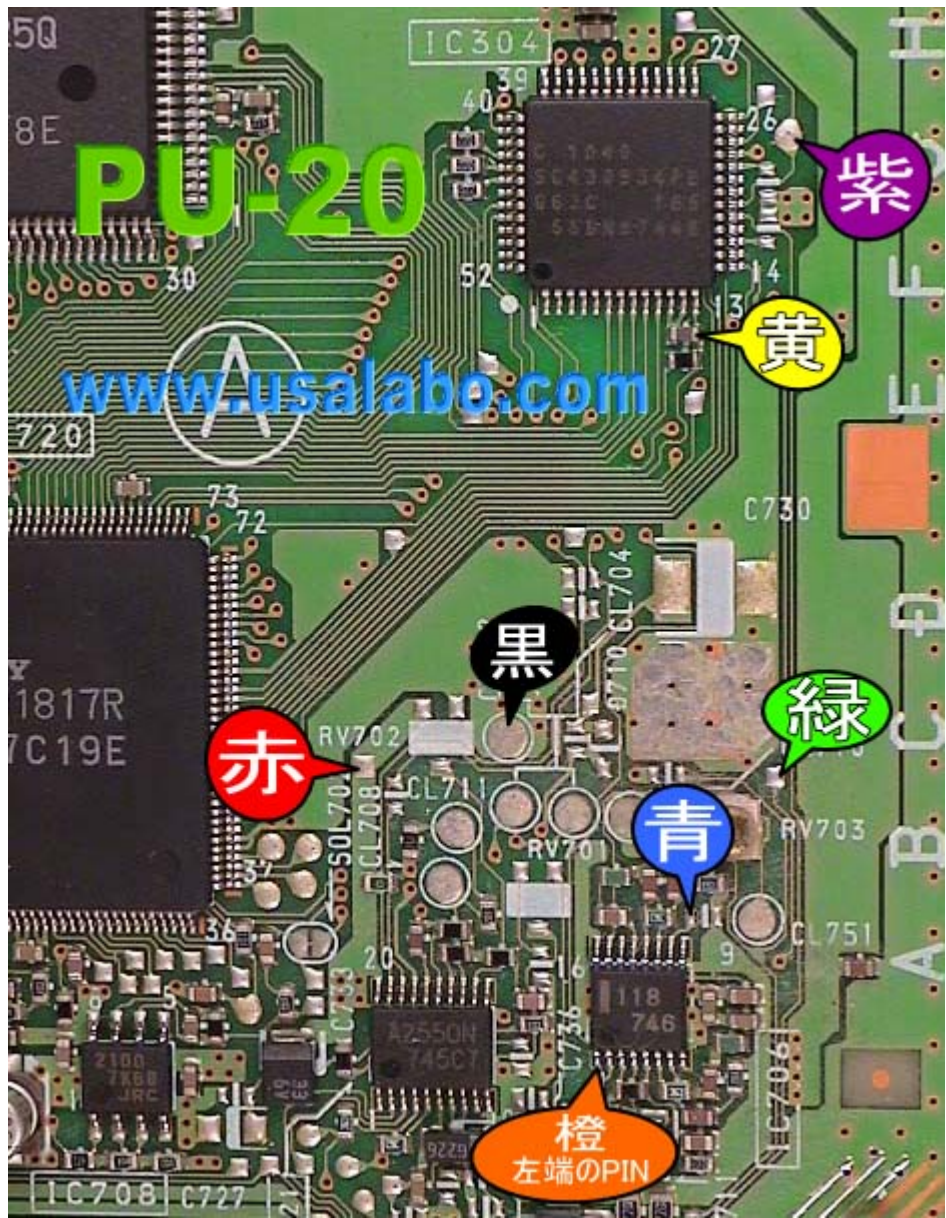
R.I.P

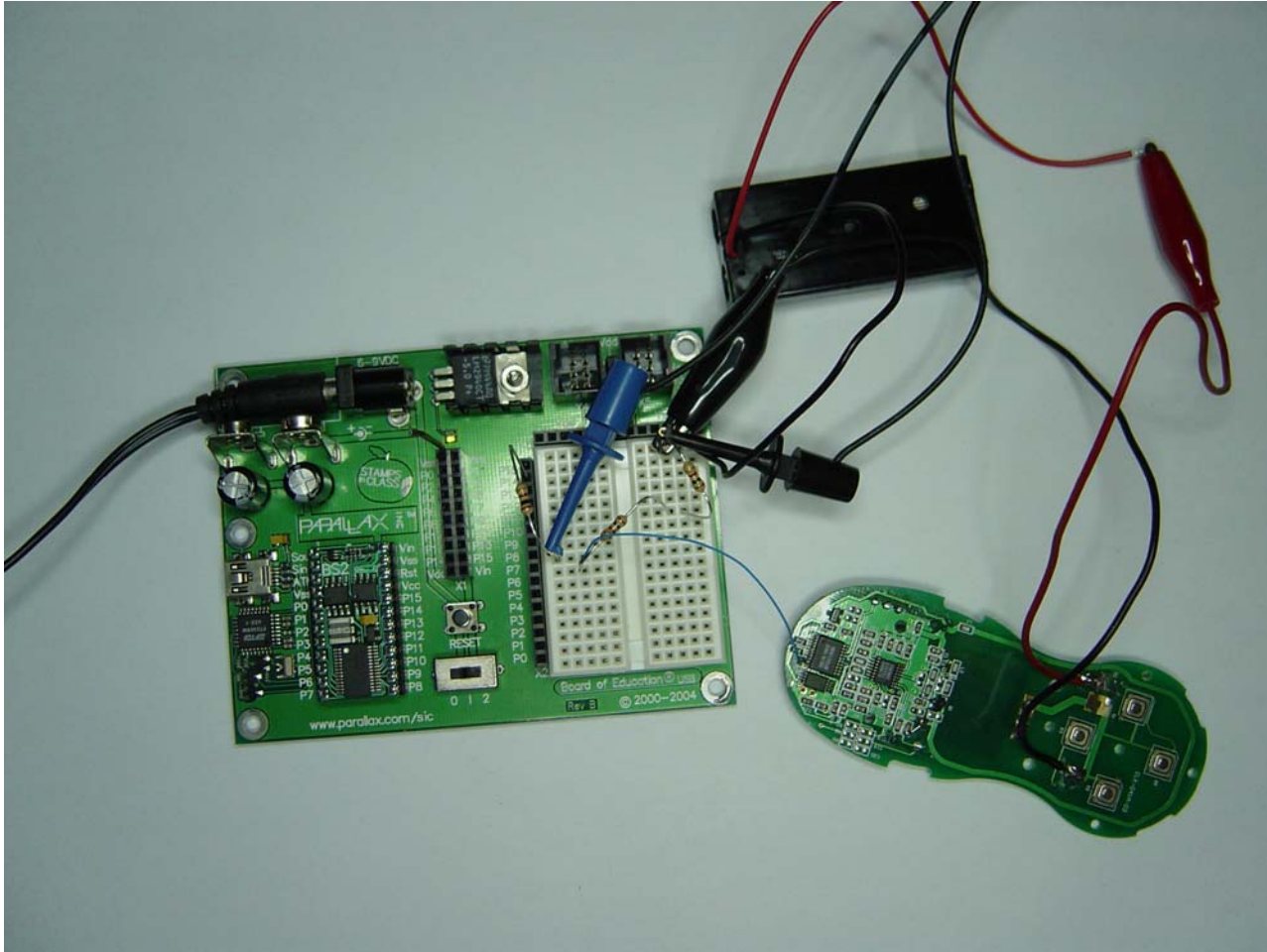


4.18.07

NEVA4GET







More MCU uses

- Custom bit stream sniffer/recorder/interface
- Custom bit generator driven by software

Future Work

- Keyboards
- Scripting interface
- Software controlled bit generation





Thank you for flying from San Francisco International, a world-class Airport dedicated to serving the "City by the Bay".

NOTIFICATION OF INSPECTION (NOI)

To protect you and your fellow passengers, Covenant Aviation Security (CAS) is required by law to inspect all checked baggage. CAS is a private company under contract with the Transportation Security Administration (TSA) to provide baggage and passenger screening at San Francisco International Airport.

As part of this process, your bag was identified for physical inspection. If your bag was locked using non-TSA recognized locks, CAS may have had to break the locks. If prohibited items, including Hazardous Materials, were discovered during an inspection, they were turned over to the appropriate authorities.

Furthermore, to ensure the highest quality of service, CAS employees are continuously monitored by either direct supervision or camera surveillance.

We appreciate your understanding and cooperation. For questions and packing tips that may assist you during your next trip, or to learn how to submit a claim, please visit us at www.covenantclaims.com or call us toll free at 1-800-764-8050.

Screener ID: 126365

Flight: UA 474

Summary

- Find FCC ID info
- Tap into data path.
- Reverse the protocol
- Inject/Sniff data using customized MCUs
- Client enforced security is still client enforced security

Questions?

<http://dwerd.blogspot.com>

luis@ringzero.net