Fuzz Testing for Automotive cyber-security

Practical Experimentation

Daniel S. Fowler

June 25th, 2018

Daniel S. Fowler

PhD. Research Student, Automotive Cyber-security

Fuzz Testing for Automotive Cyber-Security

The HORIBA MIRA Collaboration With Coventry University

Systems Security Research Group, Institute of Future Transport and Cities

Coventry University & HORIBA MIRA Collaboration

Coventry University

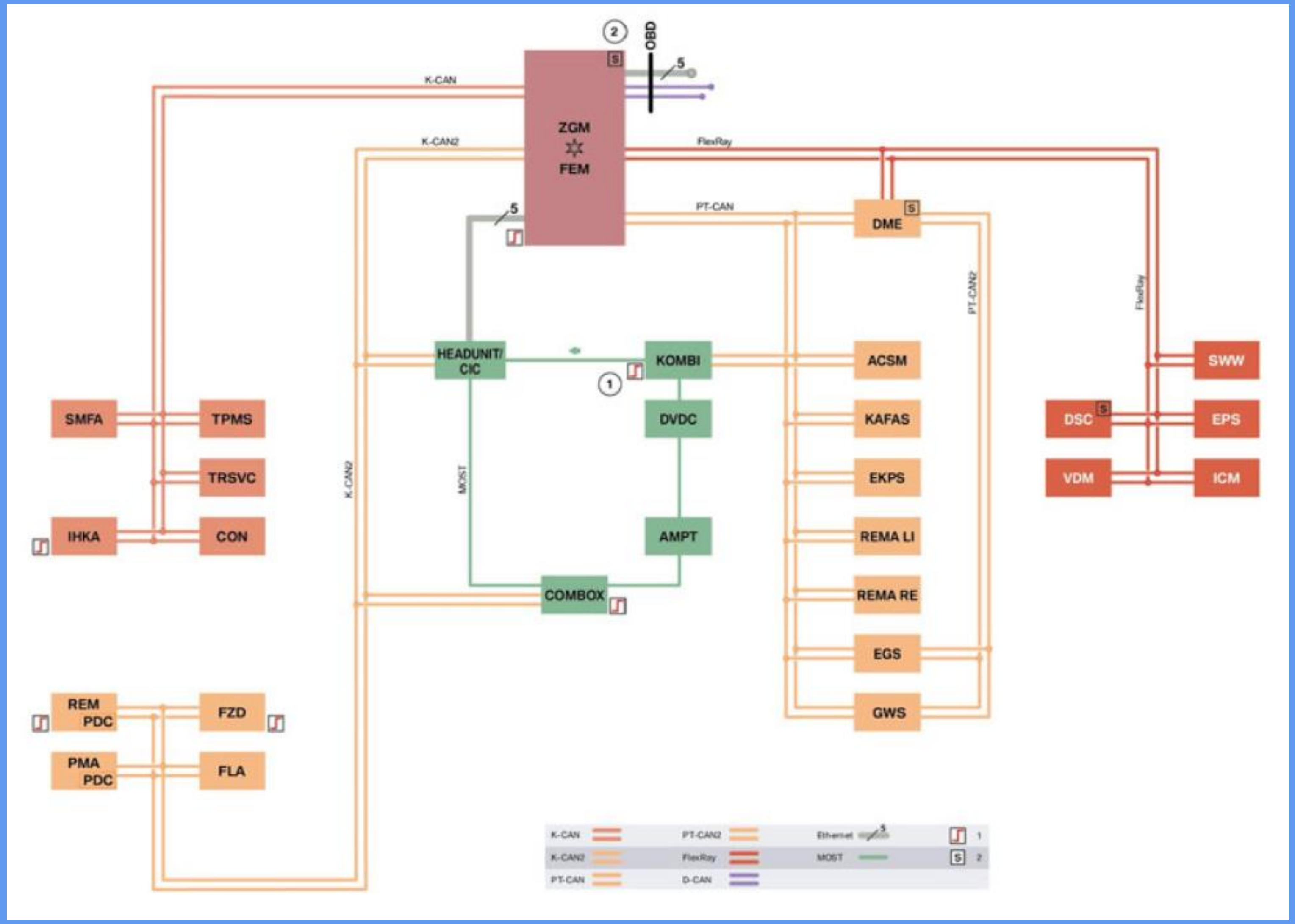
- Multidisciplinary teaching and research
- Centre of England
- Global vision
- Strong ties to automotive industries

Ayr
United Kingdom
Bangor
Middlesbrough
Isle of Man
Blackpool
Leeds
Hull
Liverpool
Sheffield
Stoke-on-Trent
Nottingham
Norwich
England
Wales
Ipswich
Headington
Swansea
Bristol
London
Leigh-on-Sea
Cardiff
Reading
Barnstaple
Southampton
Exeter
Portsmouth
Bournemouth

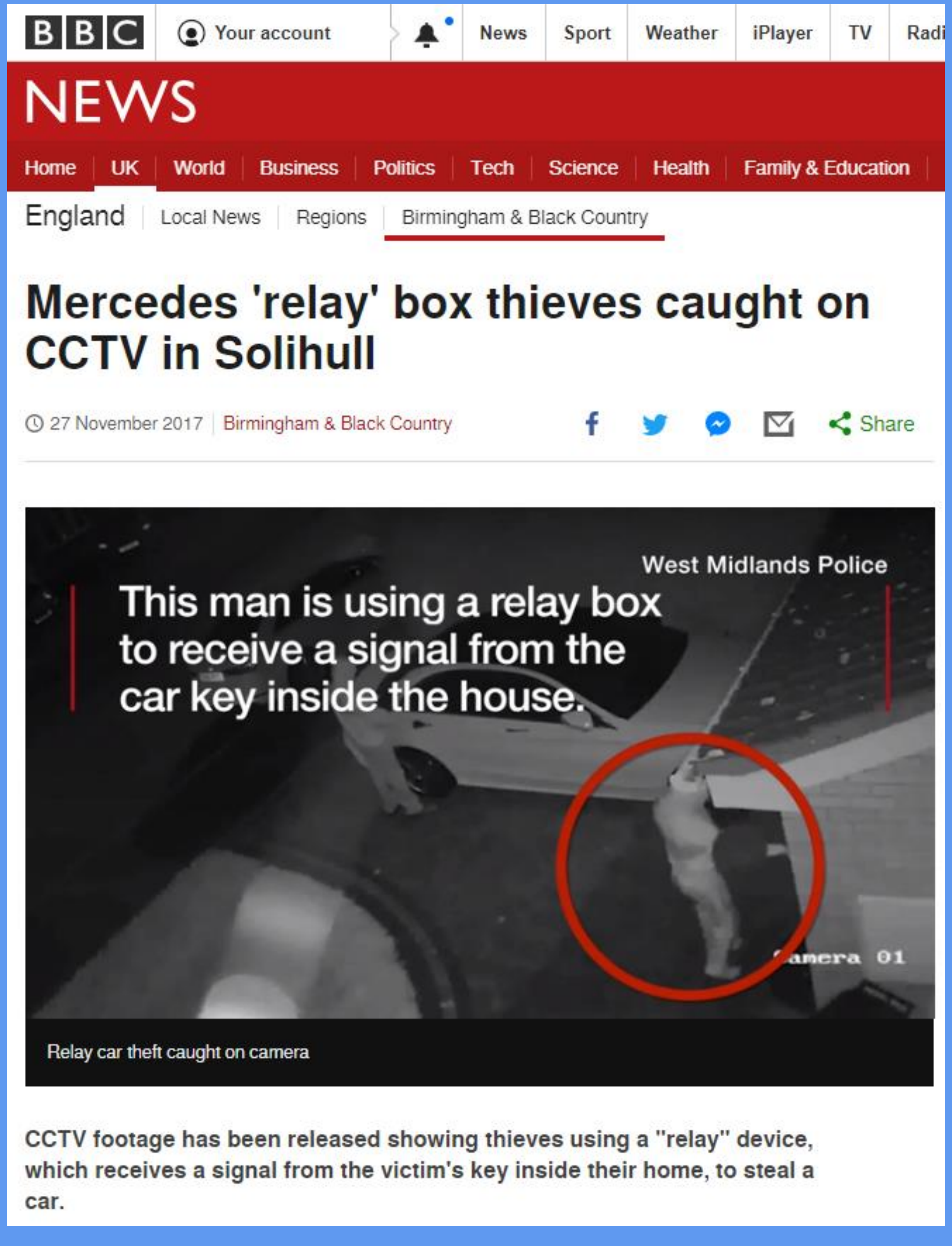
HORIBA MIRA

- Also in central England at an ex-WWII airfield
- Engineering, research and test services
- Automotive, defence, aerospace and rail
- Motor Industry Research Association (MIRA)
- Owned by Japanese company HORIBA

A Vehicle is a Hackable Cyber-Physical System



How can vehicle manufacturers test for cyber-security?



BBC | Your account | News | Sport | Weather | iPlayer | TV | Radi

NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Family & Education

England | Local News | Regions | Birmingham & Black Country

Mercedes 'relay' box thieves caught on CCTV in Solihull

27 November 2017 | Birmingham & Black Country

Share

West Midlands Police

This man is using a relay box to receive a signal from the car key inside the house.

Camera 01

Relay car theft caught on camera

CCTV footage has been released showing thieves using a "relay" device, which receives a signal from the victim's key inside their home, to steal a car.

http://www.bbc.co.uk/news/uk-england-birmingham-42132689

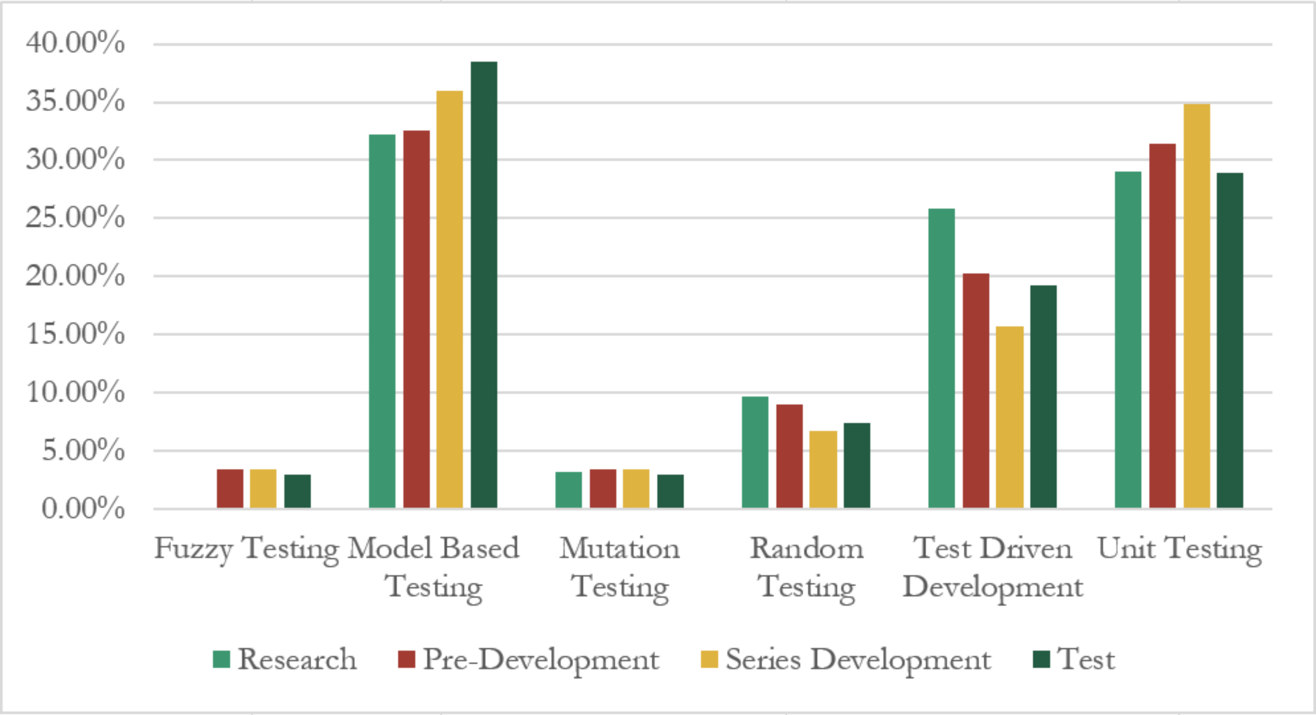
What would be worst than Dieselgate in the future?

Worst case scenario, a vehicle virus!

"One of the biggest risks for autonomous vehicles is somebody achieving a fleet wide hack.“ – Elon Musk

Source: NGA 2017 Summer Meeting - https://youtu.be/2C-A797y8dA

What testing methods can be used for non-functional (security) testing?

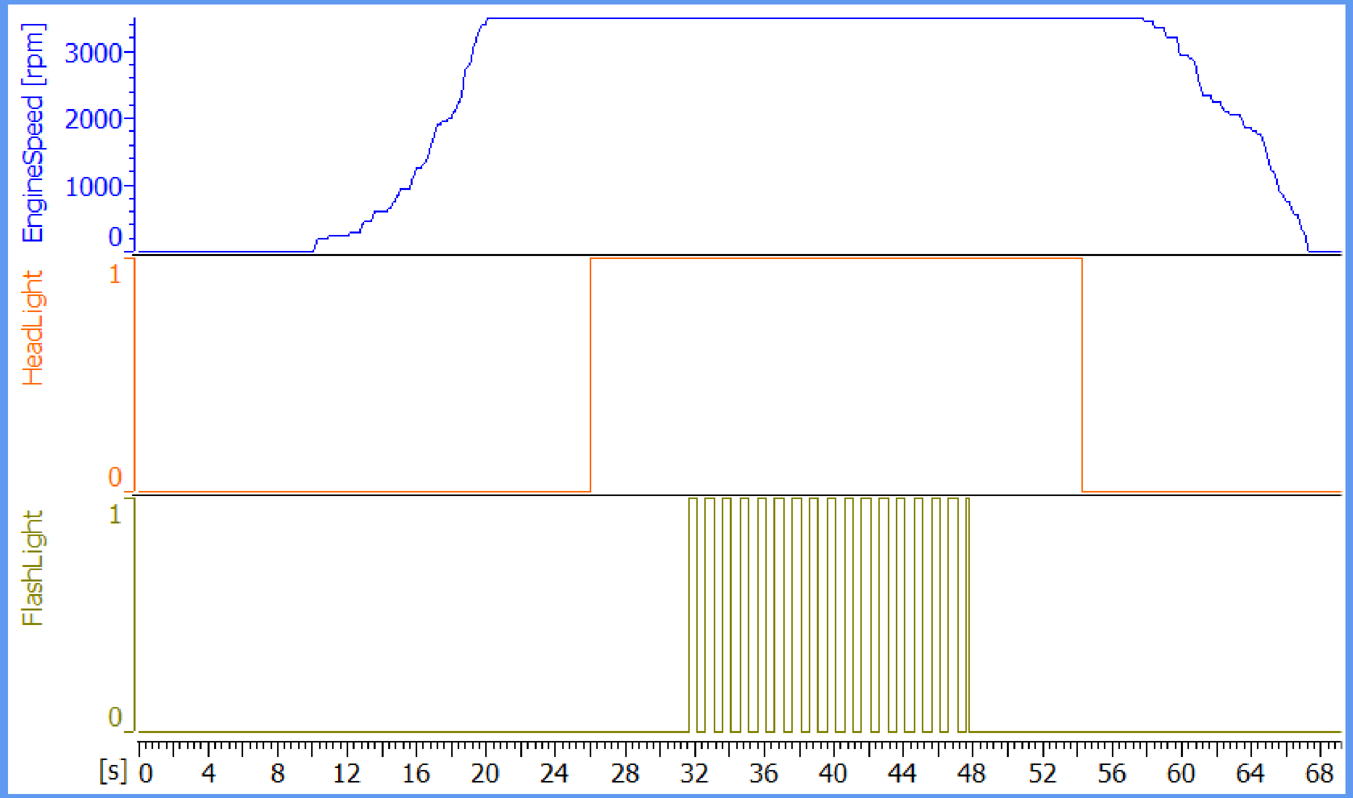


H. Altinger, F. Wotawa, and M. Schurius, “Testing methods used in the automotive industry: results from a survey,” in Proceedings of the 2014 Workshop on Joining AcadeMiA and Industry Contributions to Test Automation and Model-Based Testing - JAMAICA 2014. San Jose, California: ACM, 2014, pp. 1–6

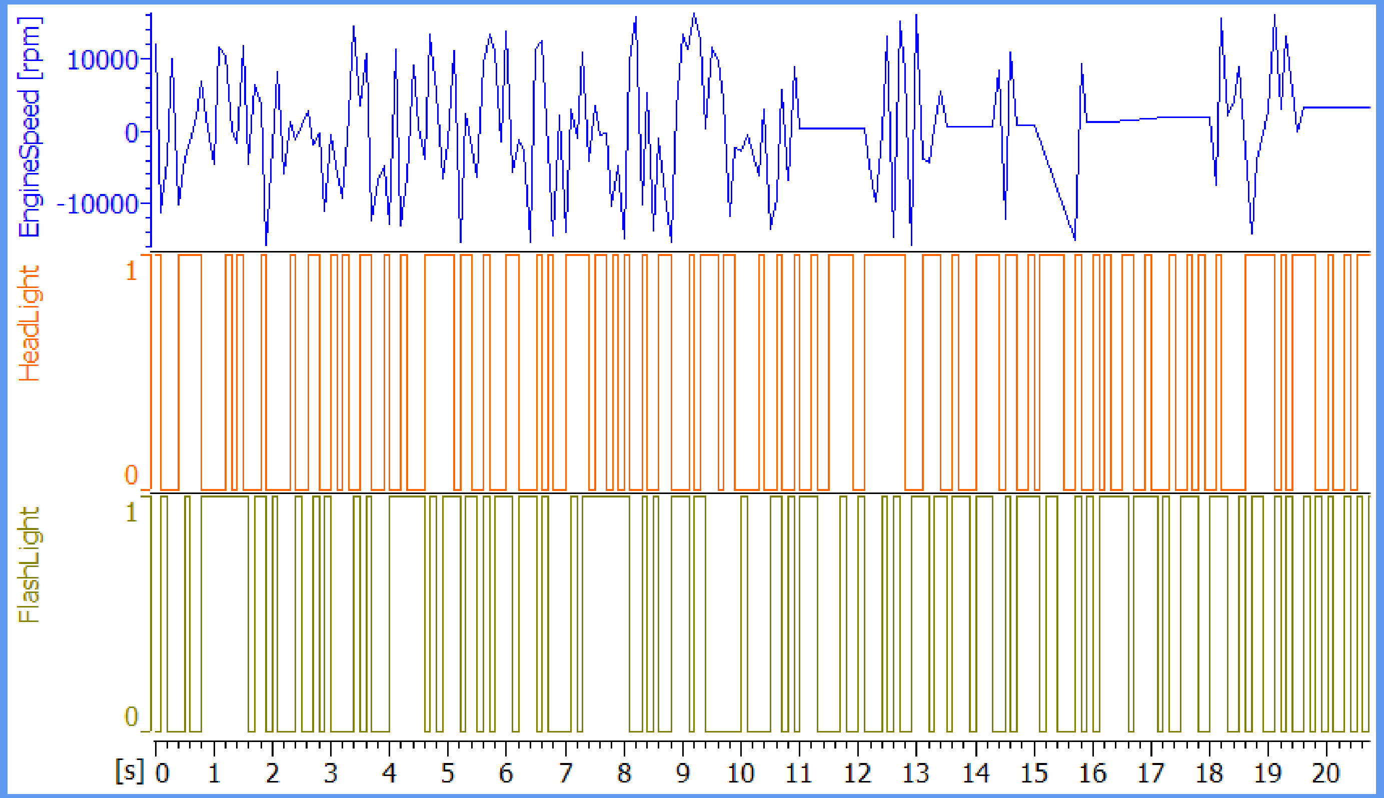
Should we use more tests that use random and mutated inputs, and huge data volumes?

If so, how do we make such tests useful?

What is a fuzz test?



Normal signals

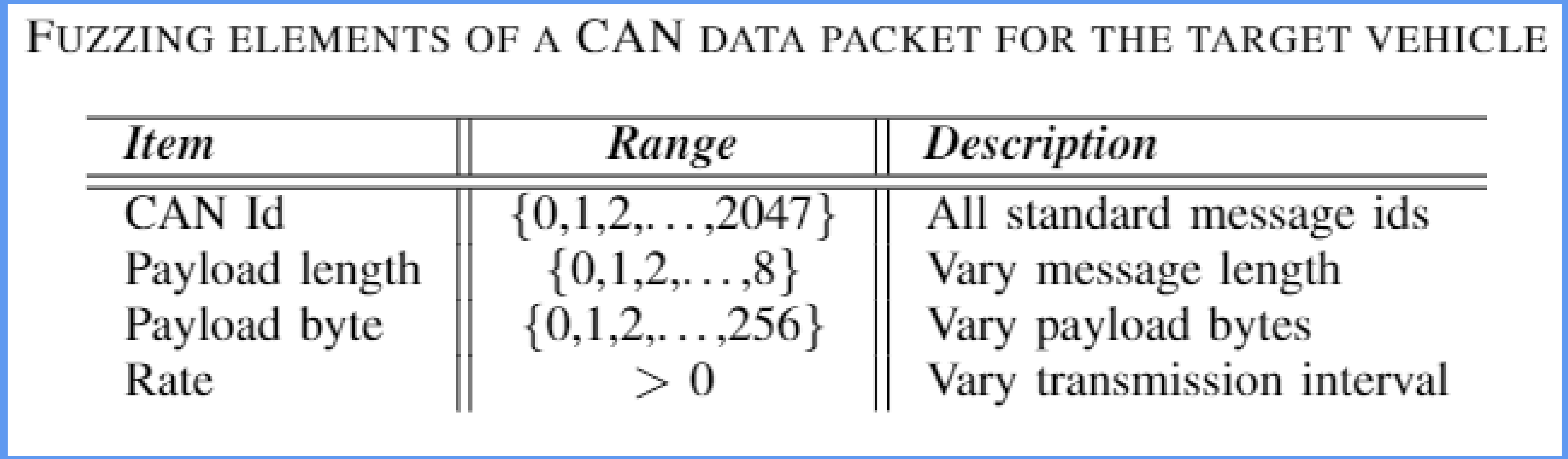


Random data injection

- A dynamic analysis test method.
- Well established in traditional IT systems testing.
- Monitor the system response to lots of random inputs.

Target for Fuzzing

Controller Area Network (CAN)
- commonality for vehicle network and components (ECUs)



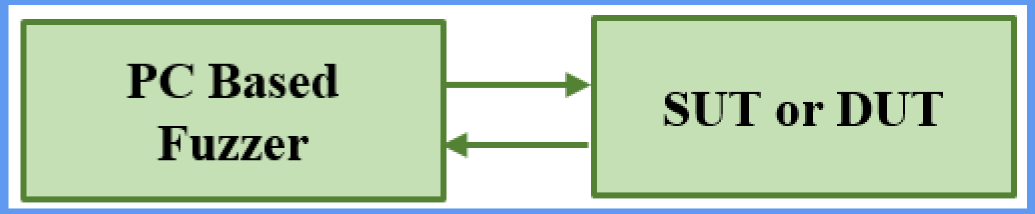
FUZZING ELEMENTS OF A CAN DATA PACKET FOR THE TARGET VEHICLE

Item	*Range*	*Description*
CAN Id	$\{0,1,2,\ldots,2047\}$	All standard message ids
Payload length	$\{0,1,2,\ldots,8\}$	Vary message length
Payload byte	$\{0,1,2,\ldots,256\}$	Vary payload bytes
Rate	> 0	Vary transmission interval

Straightforward and robust vehicle communications standard

However, designed pre-Internet, pre-Connectivity – designed without security

A Windows PC Based CAN Fuzzer



- Simple install
- Easy configuration
- Easy to use GUI
- USB to CAN connection

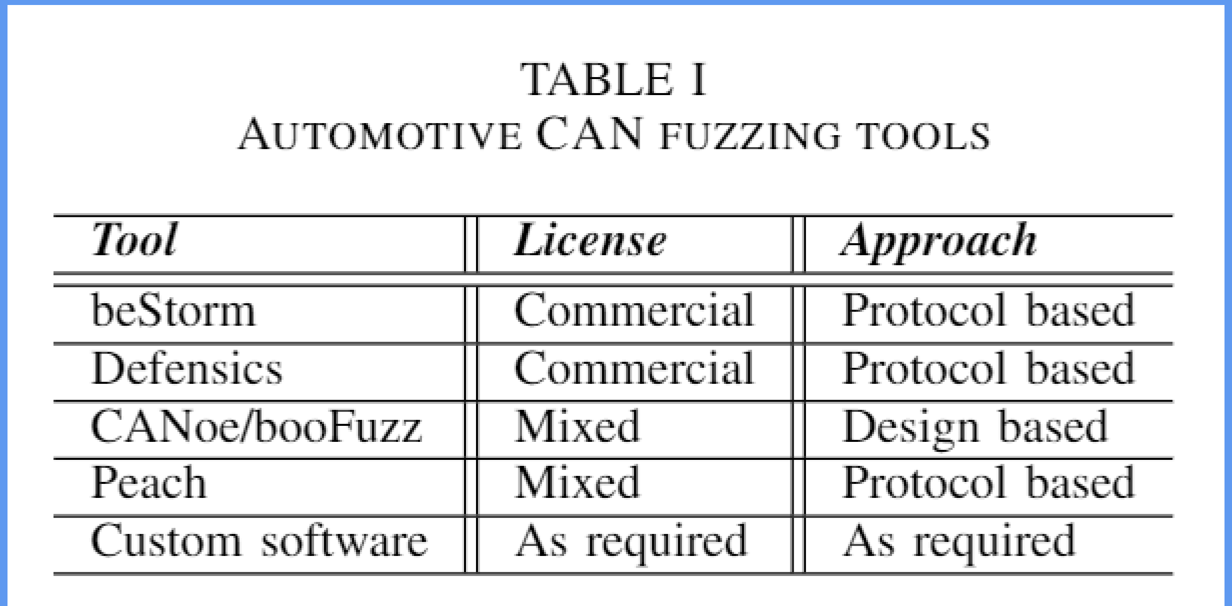
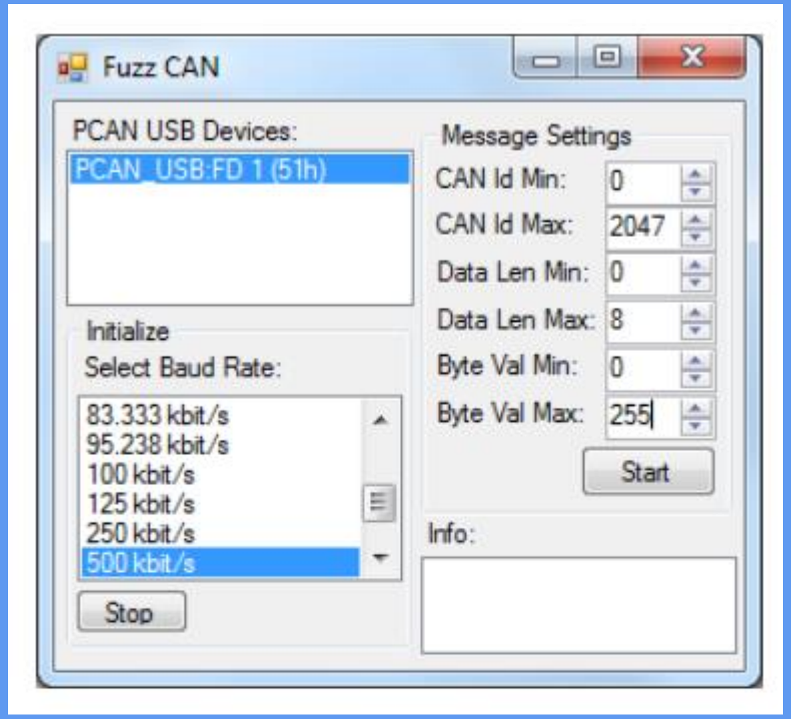


TABLE I
AUTOMOTIVE CAN FUZZING TOOLS

Tool	*License*	*Approach*
beStorm	Commercial	Protocol based
Defensics	Commercial	Protocol based
CANoe/booFuzz	Mixed	Design based
Peach	Mixed	Protocol based
Custom software	As required	As required

- Existing fuzzers have a learning curve
- They are not designed specifically for CAN

CAN Fuzzer



Fuzz CAN

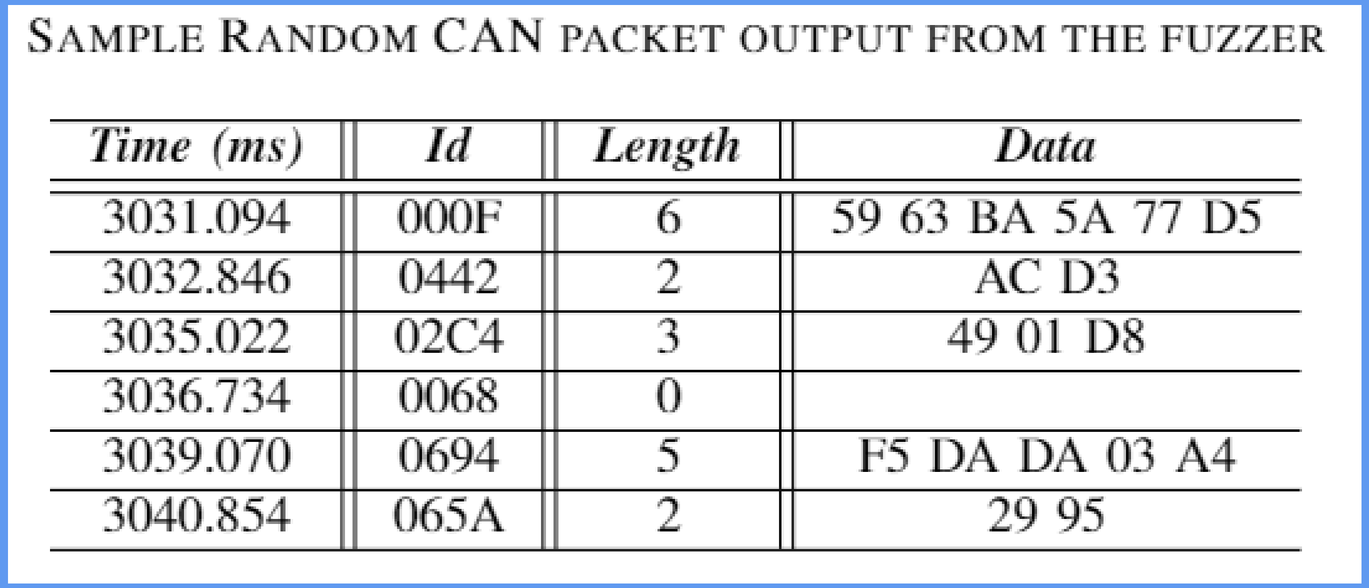
PCAN USB Devices:
PCAN_USB:FD 1 (51h)

Initialize
Select Baud Rate:
83.333 kbit/s
95.238 kbit/s
100 kbit/s
125 kbit/s
250 kbit/s
500 kbit/s

Message Settings
CAN Id Min: 0
CAN Id Max: 2047
Data Len Min: 0
Data Len Max: 8
Byte Val Min: 0
Byte Val Max: 255

Info:

One of the configuration screens



Sample Random CAN packet output from the fuzzer

Time (ms)	*Id*	*Length*	*Data*
3031.094	000F	6	59 63 BA 5A 77 D5
3032.846	0442	2	AC D3
3035.022	02C4	3	49 01 D8
3036.734	0068	0	
3039.070	0694	5	F5 DA DA 03 A4
3040.854	065A	2	29 95

Example output

Sent to CAN

Checking fuzzer output

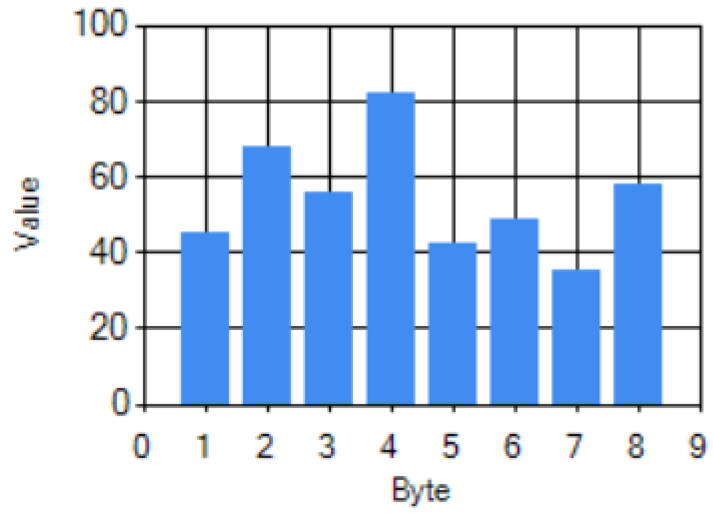


Fig. 4. Mean values for each data byte position from 100000 captured vehicle CAN messages

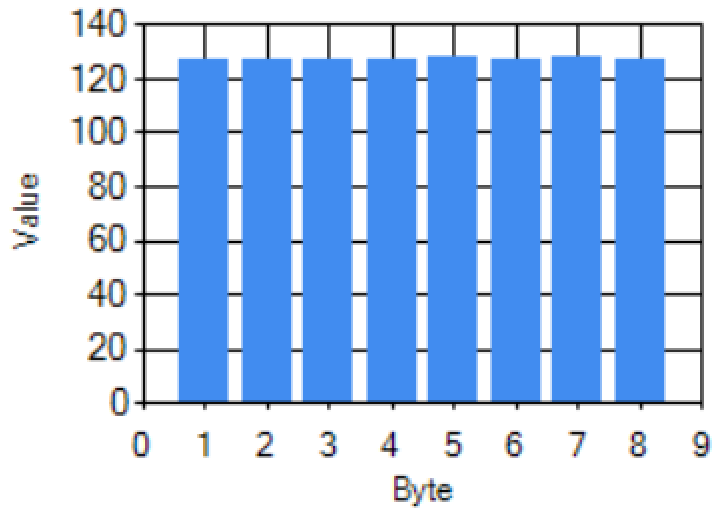


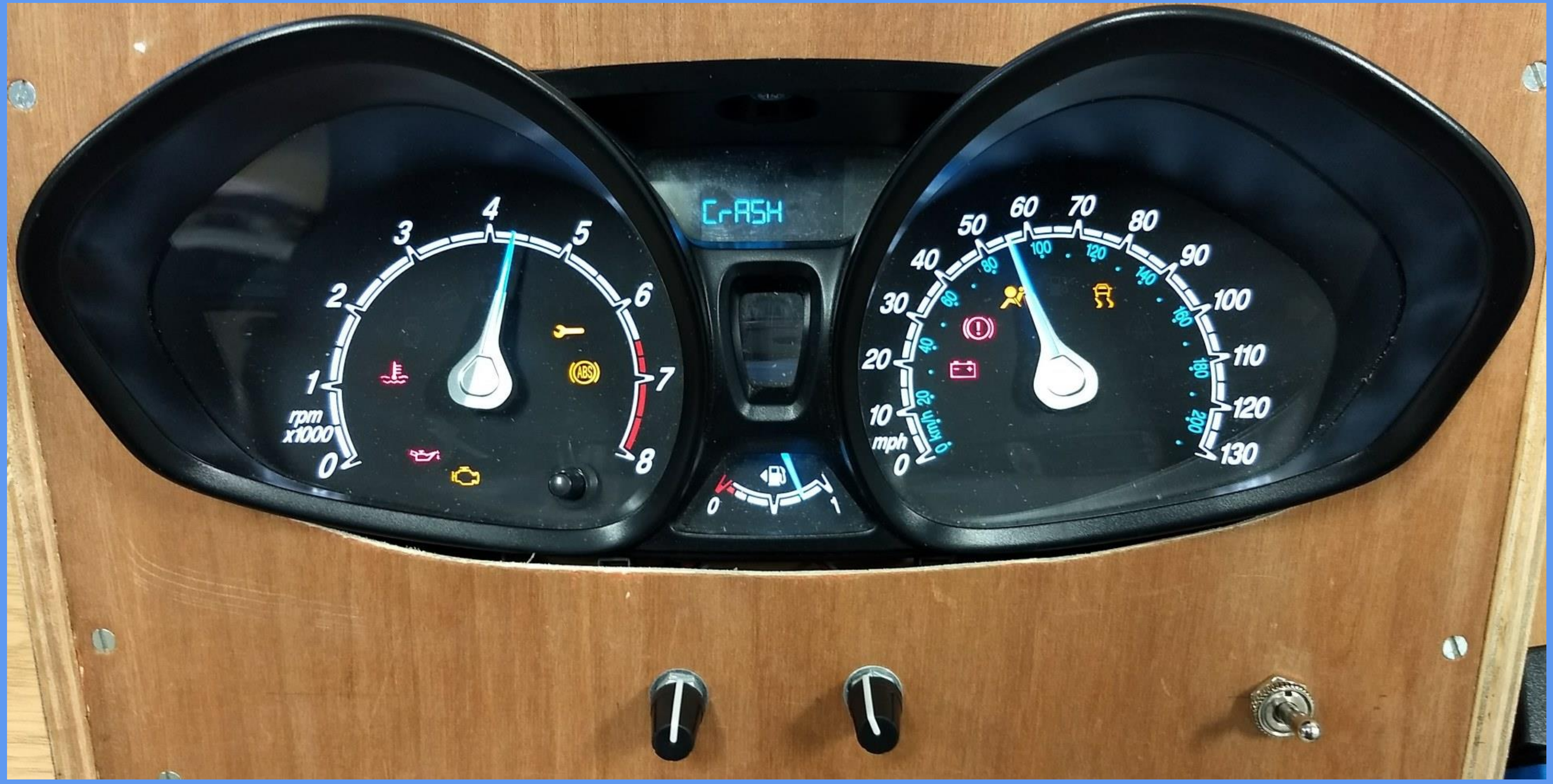
Fig. 5. Mean values for each data byte position from 66144 randomly generated CAN messages

Mean byte values from vehicle CAN data

Mean byte values from fuzzer generated CAN data

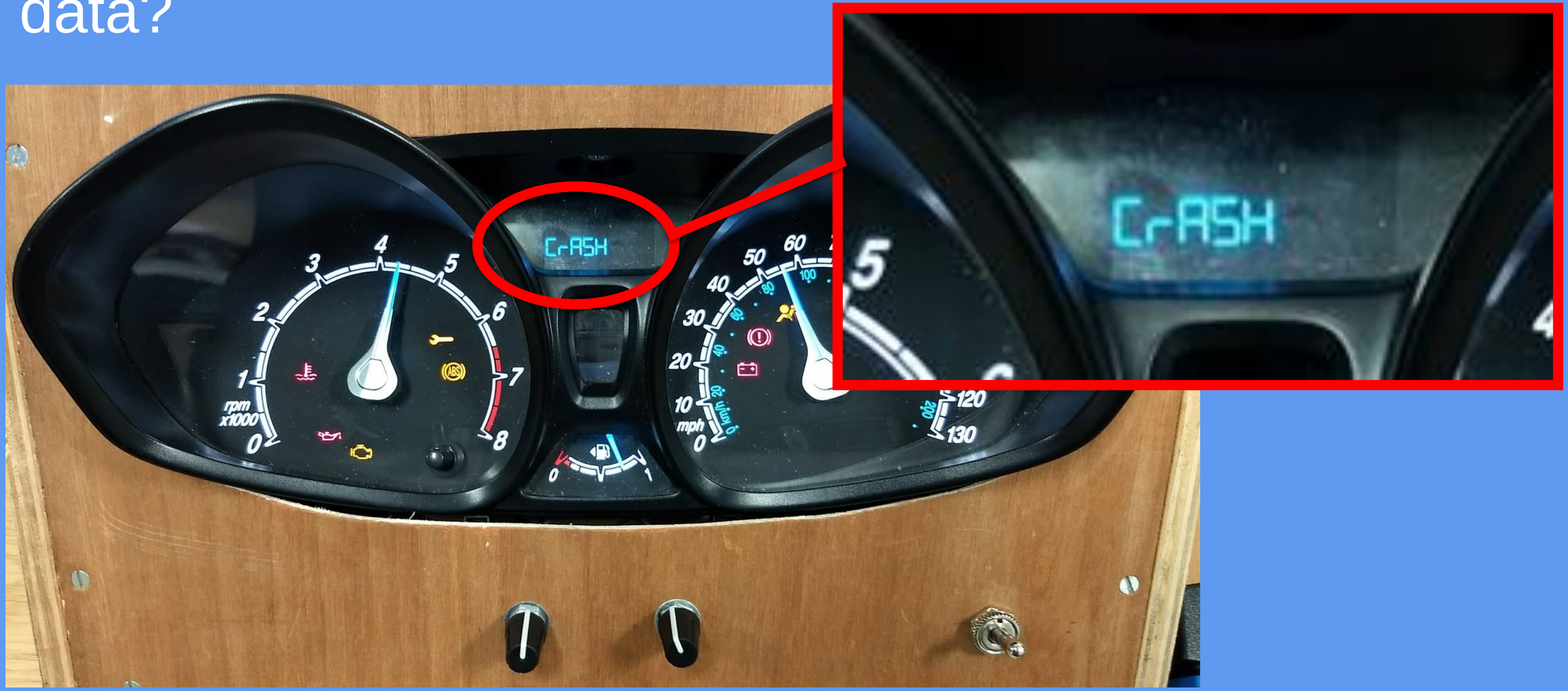
Running The Fuzzer

What happens if vehicle systems are not designed to reject fuzzed data?



Running The Fuzzer

What happens if vehicle systems are not designed to reject fuzzed data?



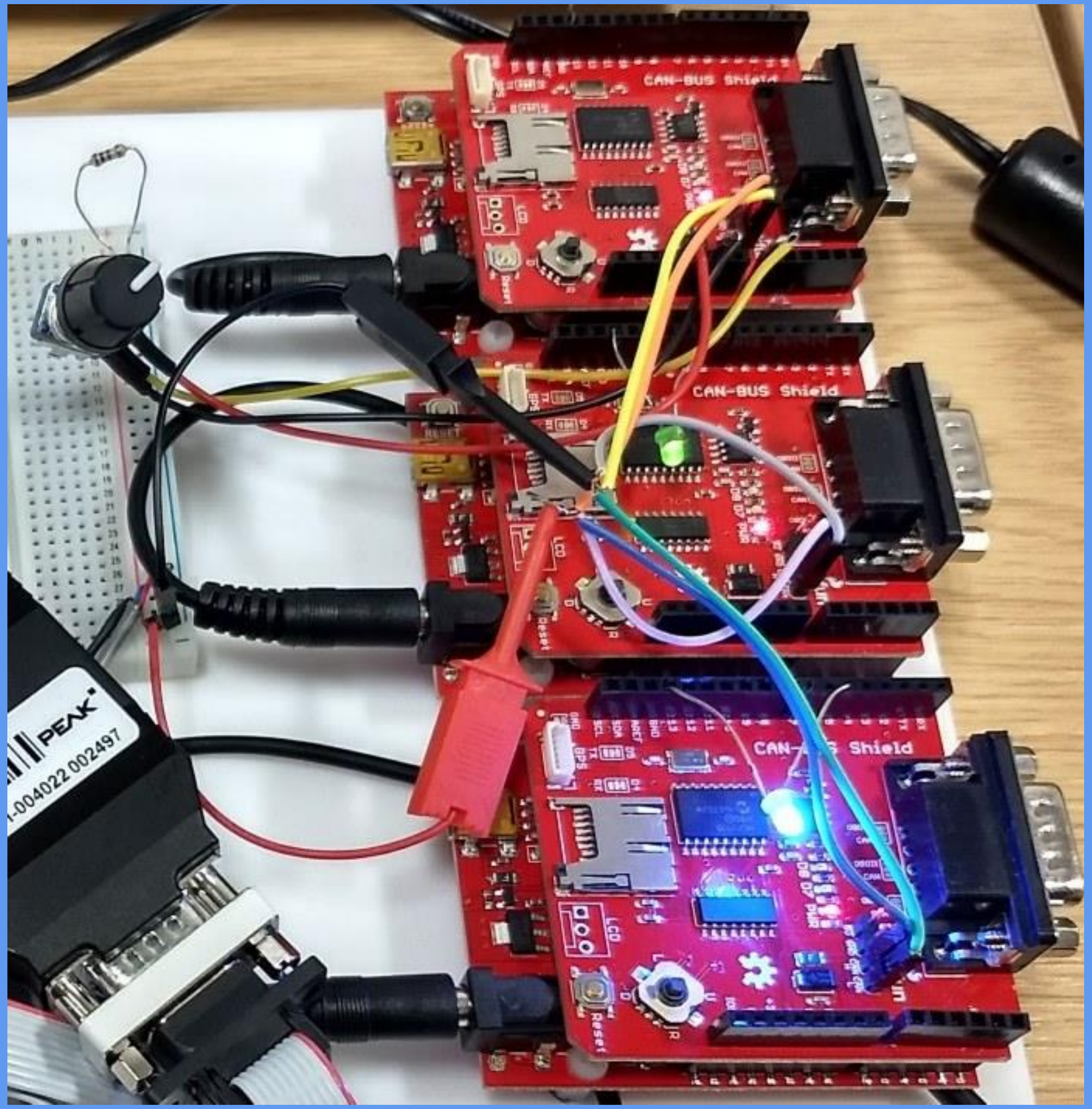
They are not safe!

From - “Experimental Security Analysis of a Modern Automobile”

“In fact, because the range of valid CAN packets is rather small, significant damage can be done by simple fuzzing of packets (i.e., iterative testing of random or partially random packets). Indeed, for attackers seeking indiscriminate disruption, **fuzzing is an effective attack by itself**.”

K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in Security and Privacy (SP), 2010 IEEE Symposium on, 2010, pp. 447–462

Test Bench Target

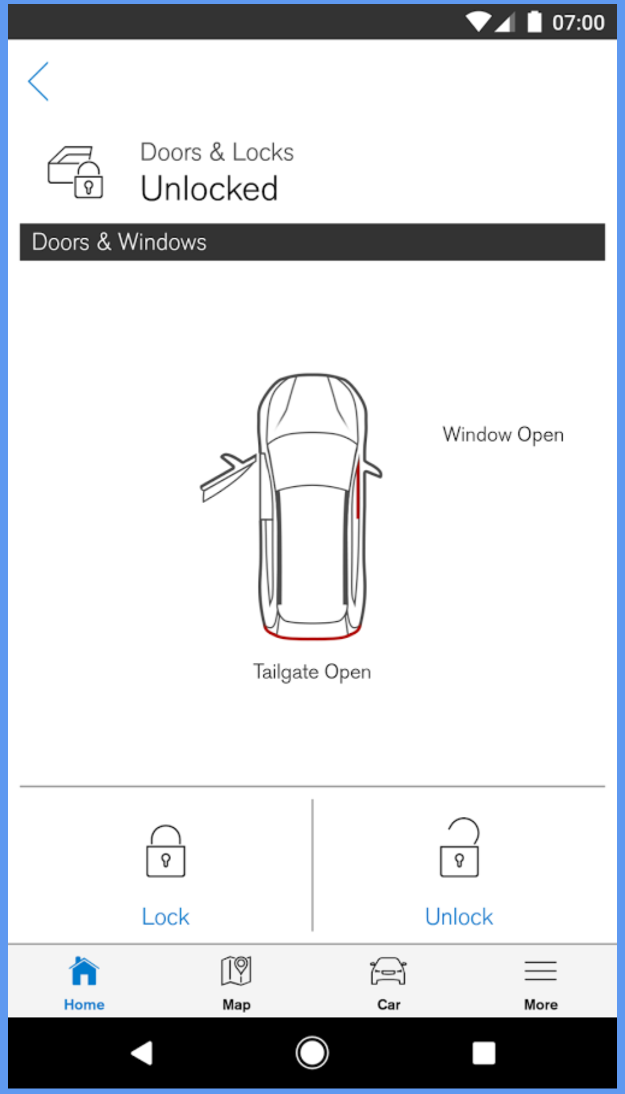


Three Arduino “ECUS”

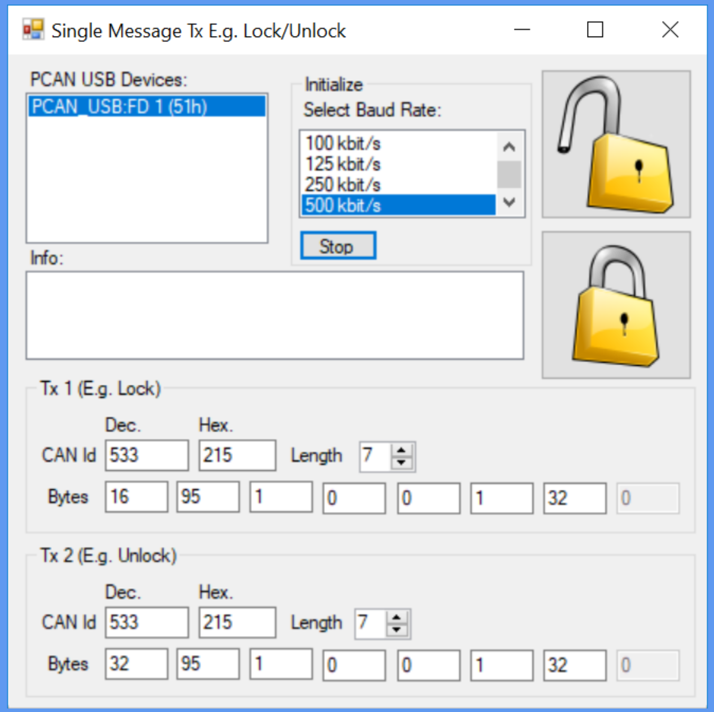
CAN bus

CAN to USB for PC Interface

Scenario



Unlocking via an app


Single Message Tx E.g. Lock/Unlock

PCAN USB Devices:
PCAN_USB FD 1 (51h)

Initialize
Select Baud Rate:
100 kbit/s
125 kbit/s
250 kbit/s
500 kbit/s

Info:

Tx 1 (E.g. Lock)

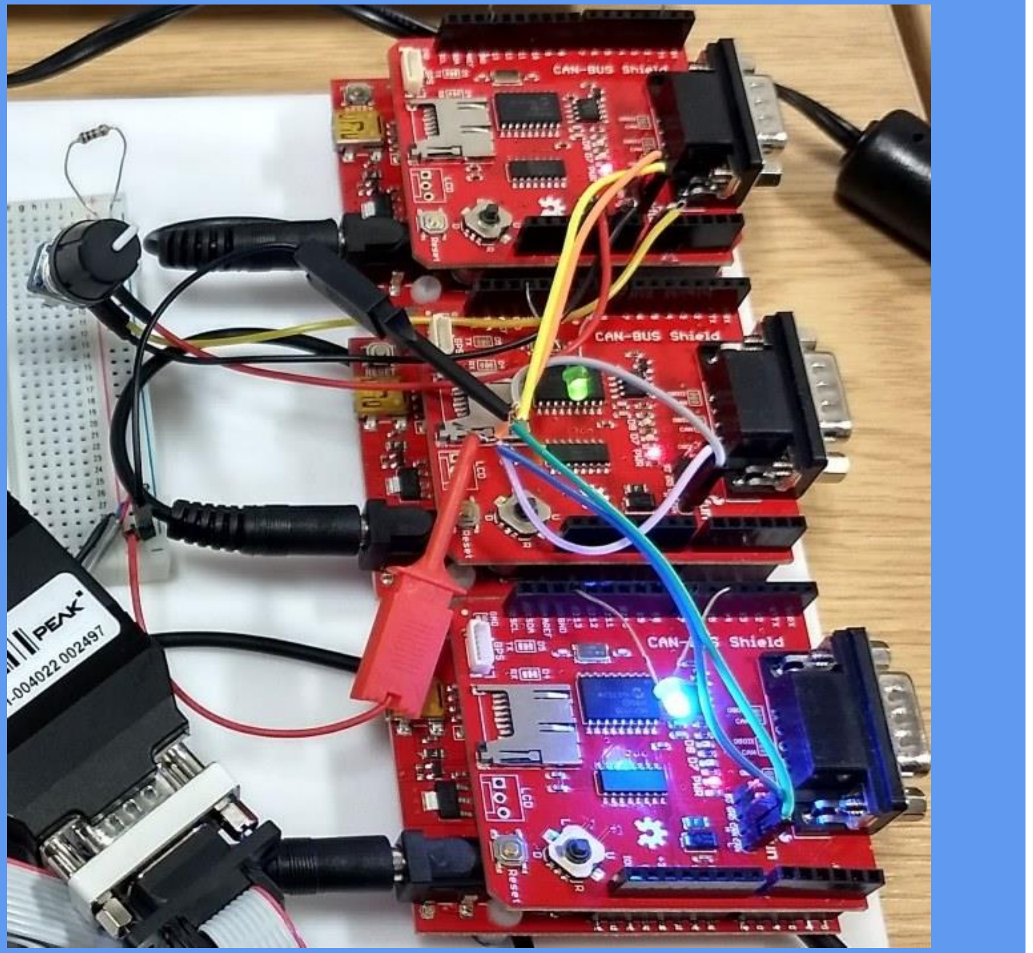
	Dec.	Hex.					
CAN Id	533	215	Length	7			
Bytes	16	95	1	0	0	1	32	0

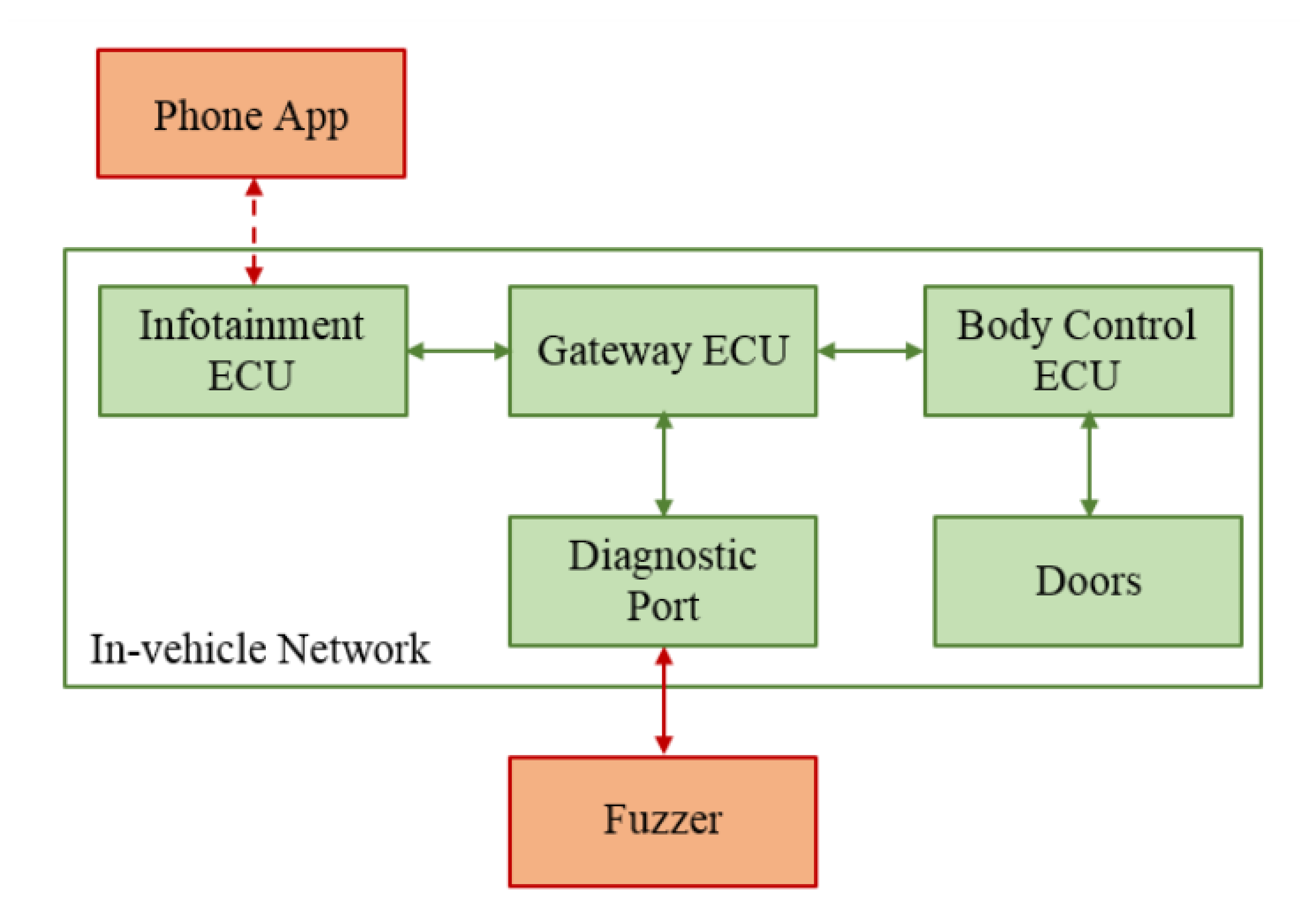
Tx 2 (E.g. Unlock)

	Dec.	Hex.					
CAN Id	533	215	Length	7			
Bytes	32	95	1	0	0	1	32	0

PC Implementation

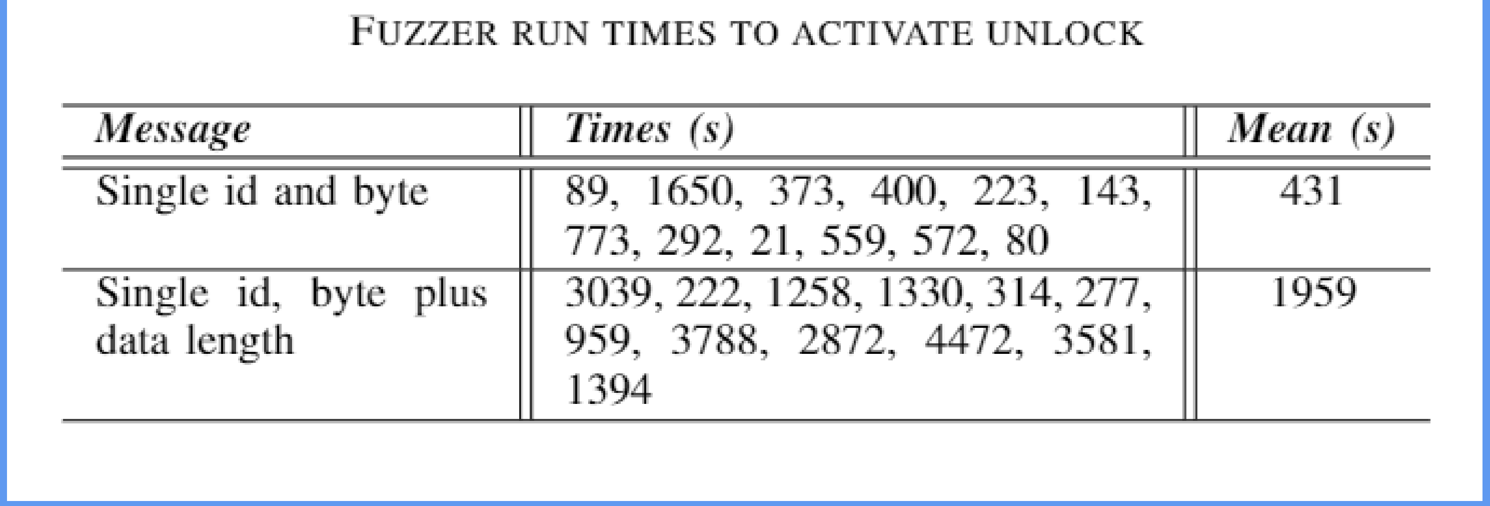
Target of Evaluation





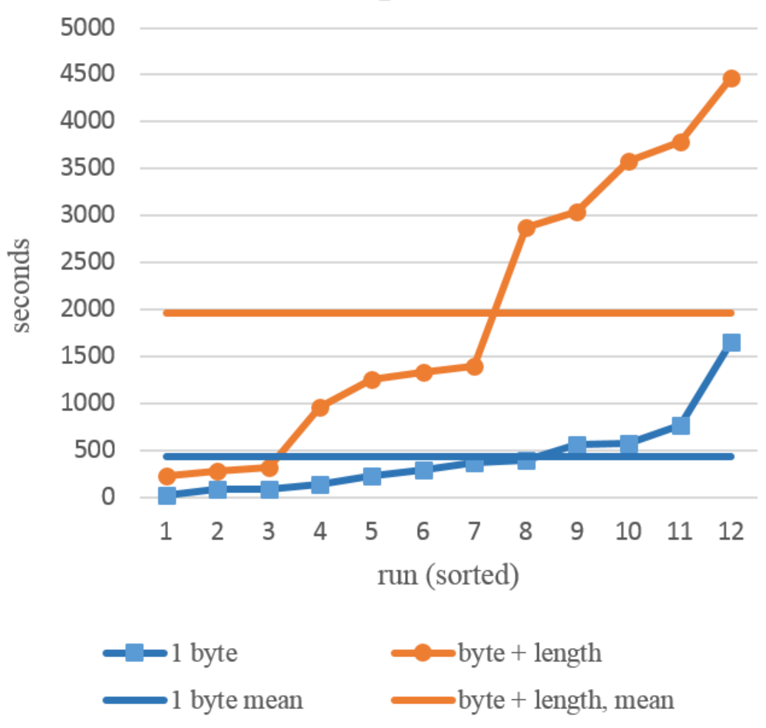
LED on, door unlocked

Fuzzing for Reverse Engineering



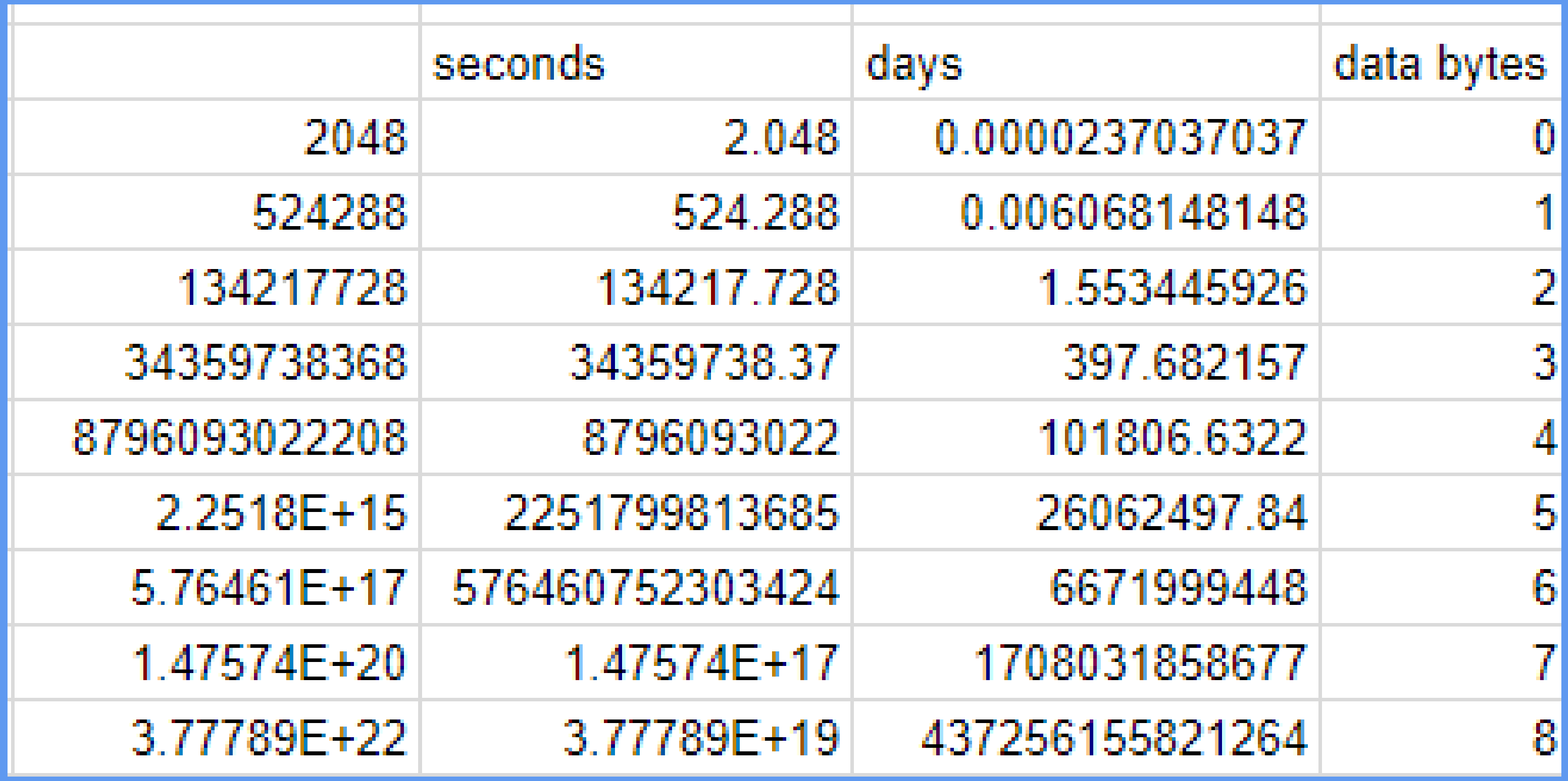
FUZZER RUN TIMES TO ACTIVATE UNLOCK

Message	*Times (s)*	*Mean (s)*
Single id and byte	89, 1650, 373, 400, 223, 143, 773, 292, 21, 559, 572, 80	431
Single id, byte plus data length	3039, 222, 1258, 1330, 314, 277, 959, 3788, 2872, 4472, 3581, 1394	1959



- Fuzzer finds unlock command
- Changing message increases find time

Pure Random CAN fuzzing not practical



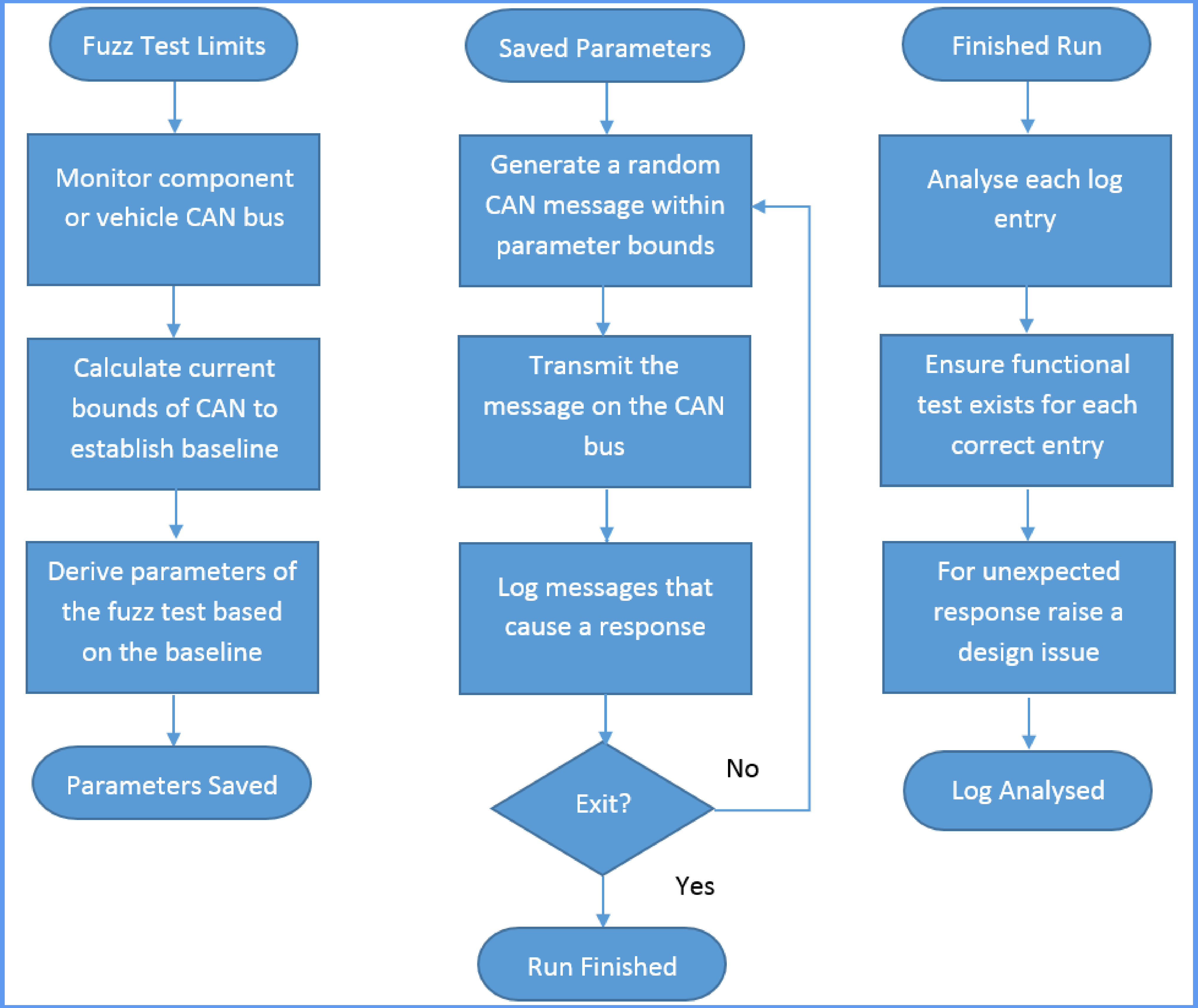
	seconds	days	data bytes
2048	2.048	0.0000237037037	0
524288	524.288	0.006068148148	1
134217728	134217.728	1.553445926	2
34359738368	34359738.37	397.682157	3
8796093022208	8796093022	101806.6322	4
2.2518E+15	2251799813685	26062497.84	5
5.76461E+17	576460752303424	6671999448	6
1.47574E+20	1.47574E+17	1708031858677	7
3.77789E+22	3.77789E+19	437256155821264	8

@1000hz

Not possible to test
every CAN message

What Next?

Developing a Fuzz Test Methodology



Fuzz Test Limits
Monitor component or vehicle CAN bus
Calculate current bounds of CAN to establish baseline
Derive parameters of the fuzz test based on the baseline
Parameters Saved
Saved Parameters
Generate a random CAN message within parameter bounds
Transmit the message on the CAN bus
Log messages that cause a response
Exit?
No
Yes
Run Finished
Finished Run
Analyse each log entry
Ensure functional test exists for each correct entry
For unexpected response raise a design issue
Log Analysed

Uses for Fuzz Test Methods

- *Detection* – Finding known ECU, component, or vehicle functionalities. (Reverse engineering.)

- *Discovery* – Finding unknown ECU, component, or vehicle functionalities. (Undocumented functions.)

- *Intrusion* – Overcome security mechanisms. (Confidentiality, Integrity, Availability)

- *Assurance* - Ensure confidence in ECU, component, or vehicle specifications. (Maintain a safe state under cyber attack.)

Observations

- Literature
  - Few sources on fuzz testing automotive systems
  - Few how-to and reproducible methods
- A fuzz test is potentially destructive, need manufacturer support
- Fuzzing can break security properties (the CIA triad)
  - Confidentiality, Integrity, Availability
- Pure fuzz testing not practical, and it must be automated
- Cyber-Physical Systems monitoring must be considered
- A fuzz test is one part of the security assurance solution
- What about sensors, HMI, wireless, V2X?
  - Scope for further contributions

?