Truck Hacking:

An Experimental Analysis of the SAE J1939 Standard

10th USENIX Workshop On Offensive Technologies (WOOT'16)

Liza Burakova, Bill Hass,
Leif Millar & Andre Weimerskirch

UMTRI TRANSPORTATION RESEARCH INSTITUTE UNIVERSITY OF MICHIGAN

8/9/2016

Are trucks more secure than cars?

Outline

I. Motivation
II. Prior Work
III. Technical Background
IV. Targets
V. Attacks
    A. Instrument Cluster
    B. Powertrain
VI. Tools & Test Environment
VII. Future Work
VIII. Defenses

Why Heavy Vehicles?

- Disconnect between consumer automotive and heavy vehicle industries

- Higher impact than consumer vehicles
  - Heavy vehicles physically massive
  - Expensive & hazardous cargo
  - More susceptible to bad driving conditions
  - Backbone of economy
  - And...

… there are a couple potentially affected industries…

Heavy Trucks

Buses


SCHOOL BUS
AmTran
STOP
405
NORTH SYRACUSE
CENTRAL SCHOOLS
405


Hybrid
octranspo.com
5105
9 CENTRE RIDEAU
3 RIDEAU CENTRE
CENTRE RIDEAU
OC Transpo
The Telfer MBA
The power to outperform
5105
OC Transpo

Recreational Vehicles (RVs)

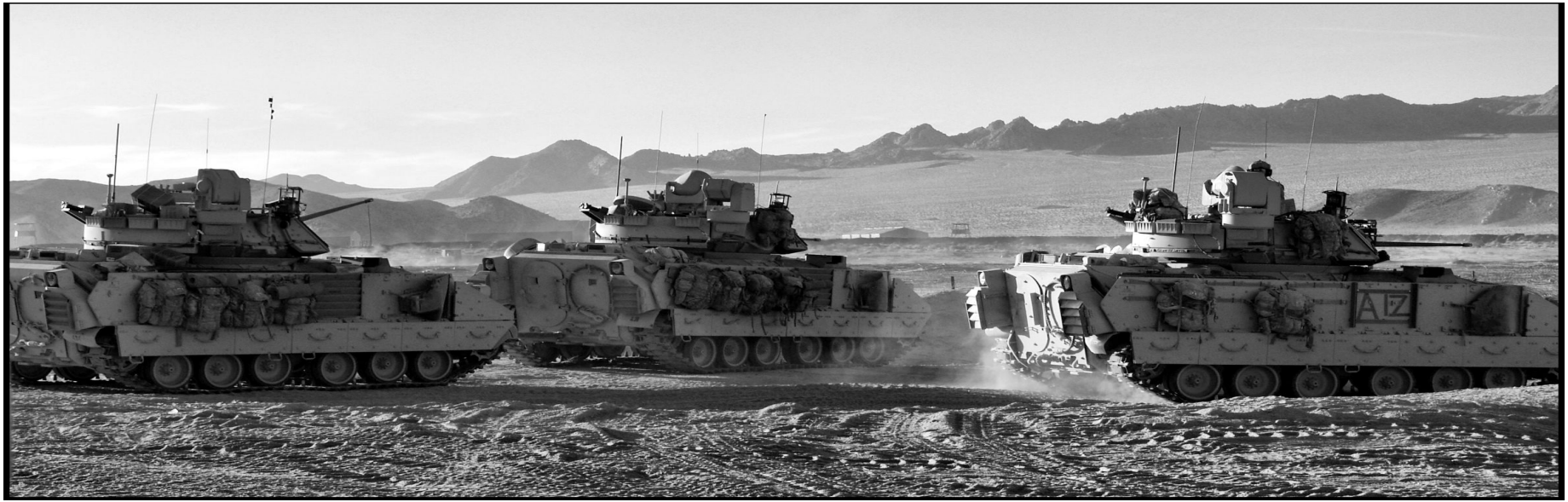
Agriculture Machinery

Forestry Machinery

Construction Vehicles

Heavy Haul & Passenger Locomotives

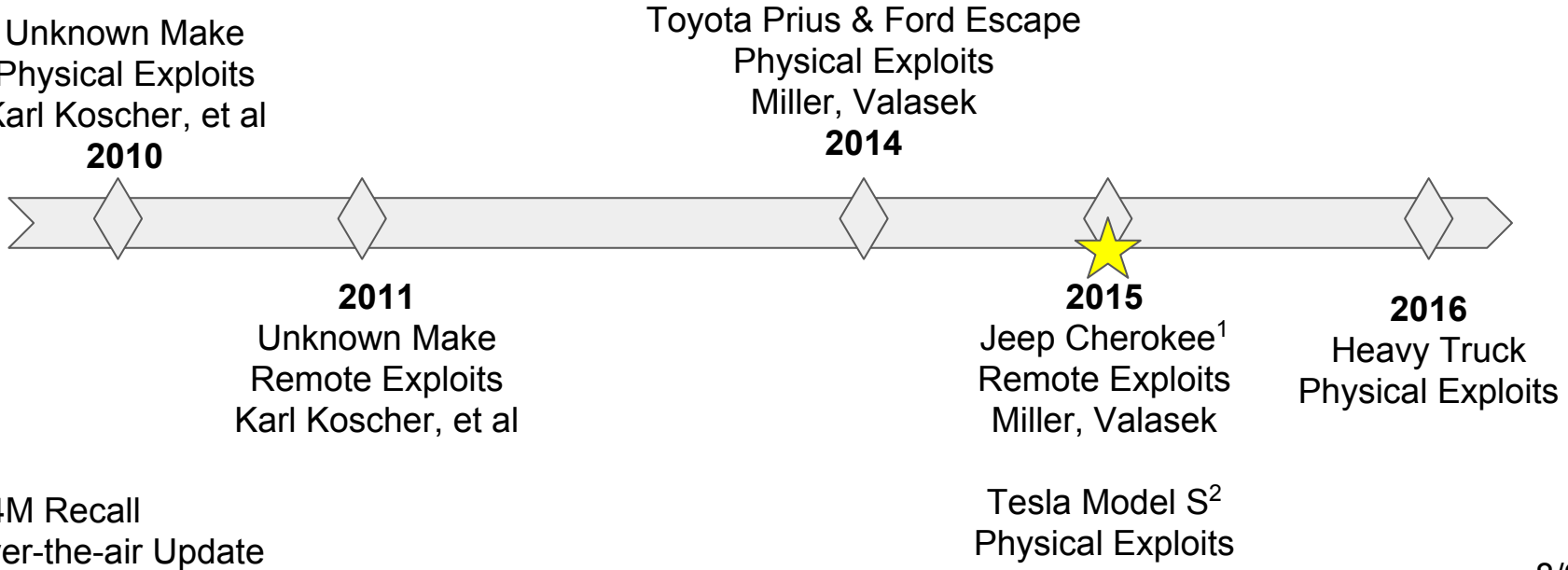
Military Vehicles (MiLCAN)



Marine Navigation Systems (NMEA2000)

Prior Work - CAN Exploits

- Consumer automobile segment scrutinized after public hacks in 2015
- Pattern of physical exploit ---> remote exploit

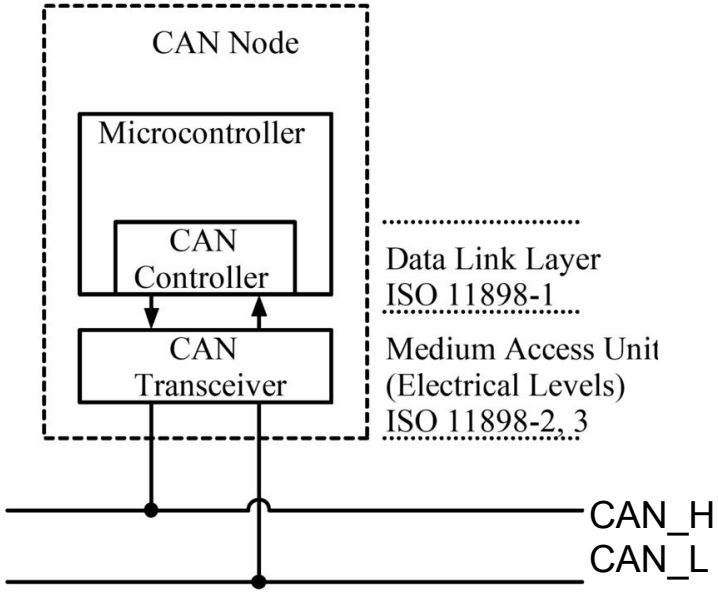


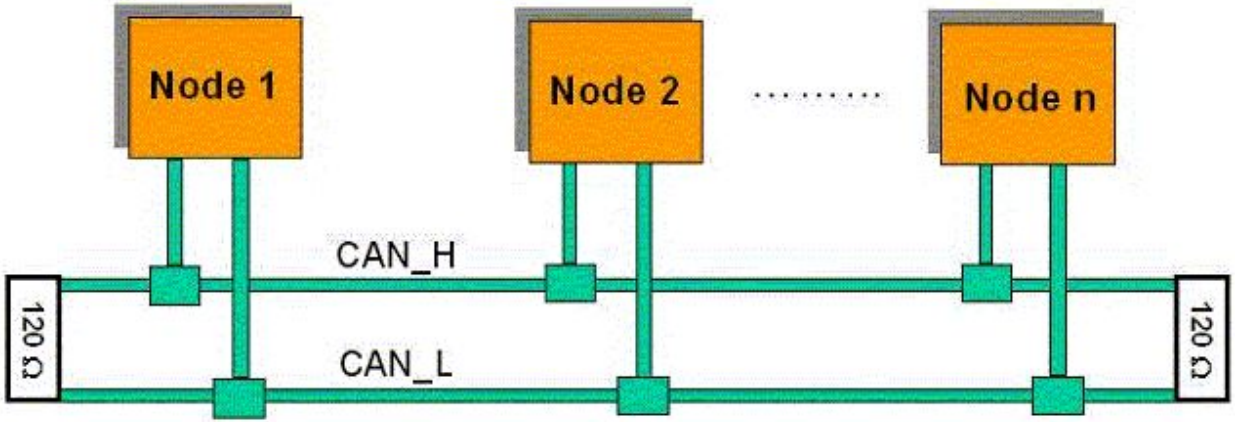
[1]1.4M Recall
[2]Over-the-air Update

So what is CAN?

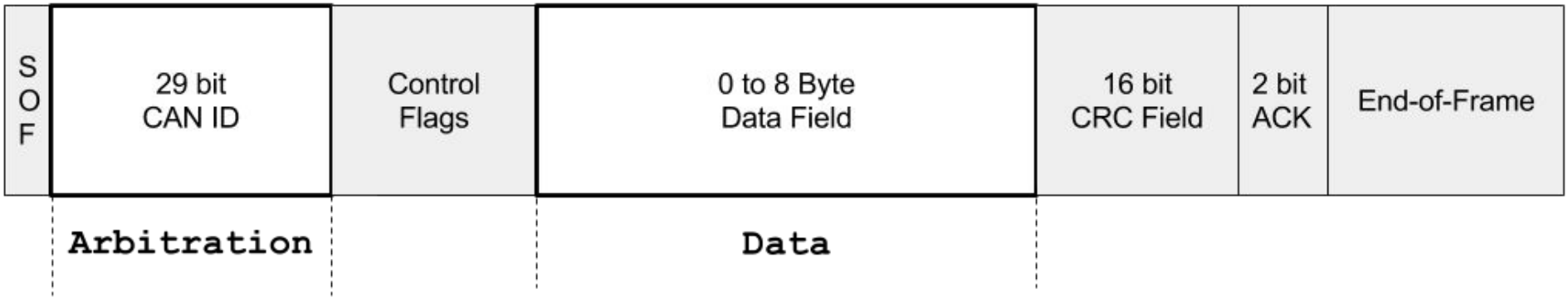
CAN Overview

- Broadcast transceiver
- Allows microcontrollers to communicate with each other
- Nodes see everything on the network





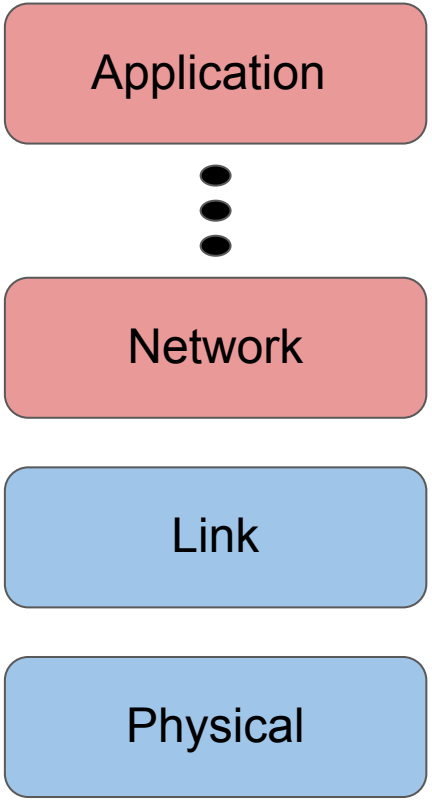
Extended CAN Frames



But what is J1939

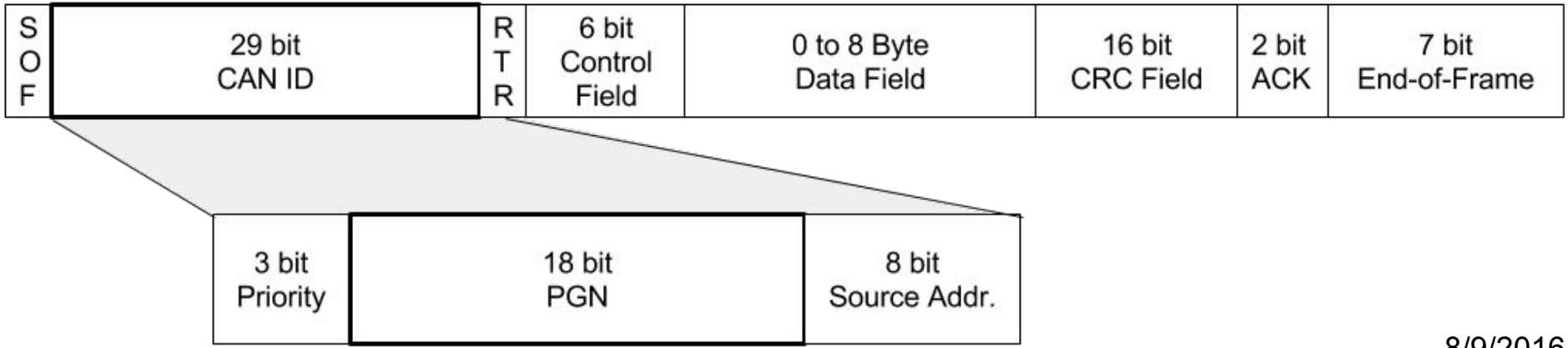
What is J1939?

- Not CAN
  - Built on top of it
  - Physical & link layer == CAN
- Defines network -> application layers
- Detailed documentation publicly available through Society of Automotive Engineers (SAE)

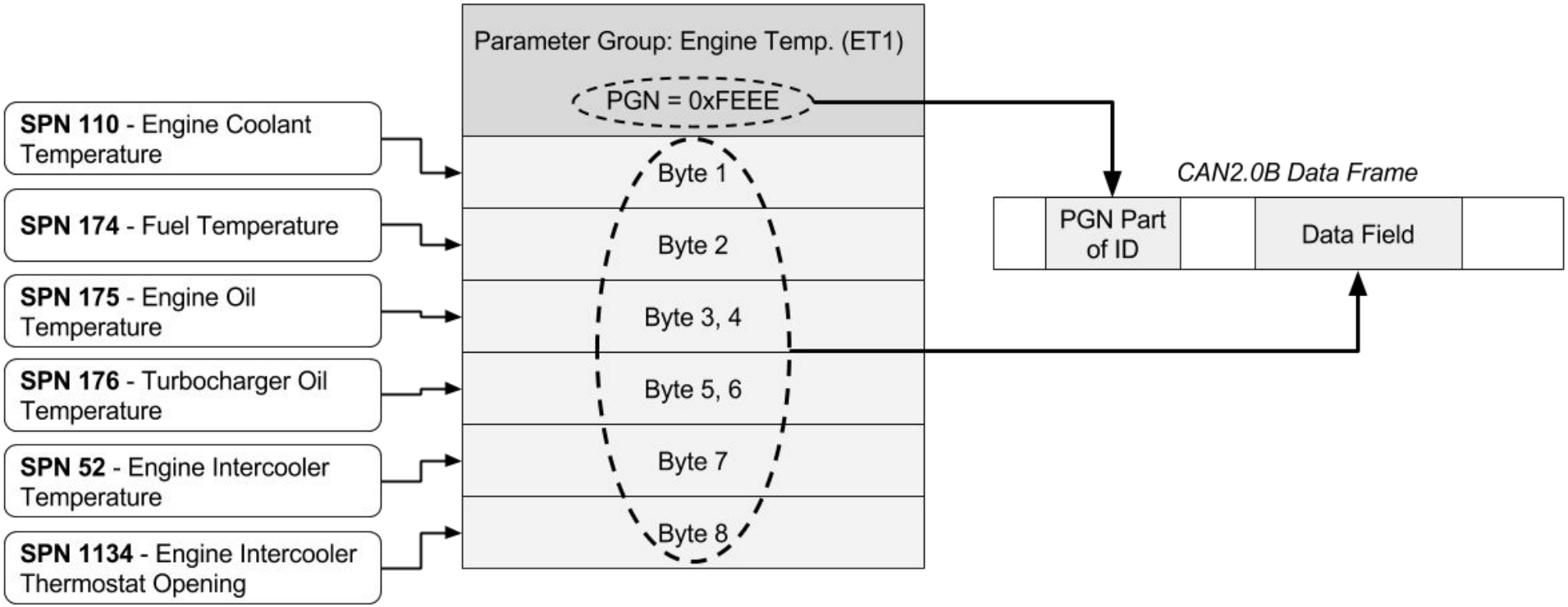


SAE J1939 Overview

- Successor to SAE J1708/J1587
  - J1708 == physical & link
  - J1587 == transport & application
- Inside the CAN ID:
  - PGN
  - SRC & DST



J1939 Overview Continued



Is security built on top?

IP/TCP + HTTP (no security) → IP/TCP + HTTPS (yay security!)

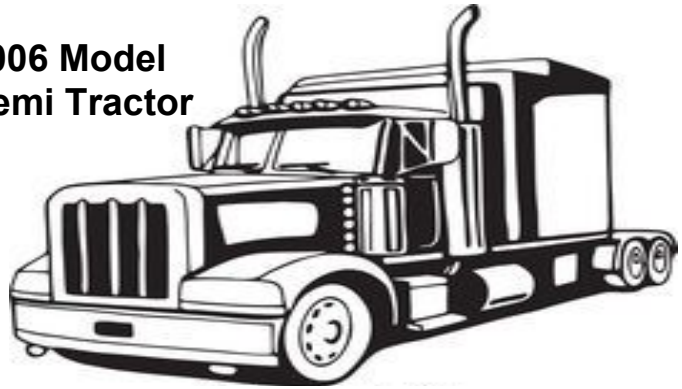
:D

CAN + Car app. layer (no security) → CAN + J1939 (security???)

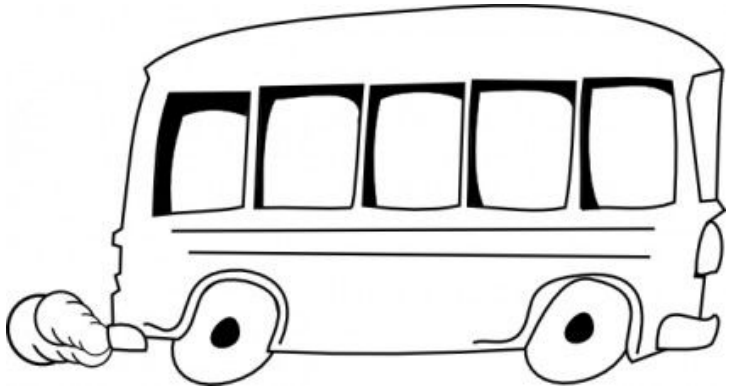
¯_(ツ)_/¯

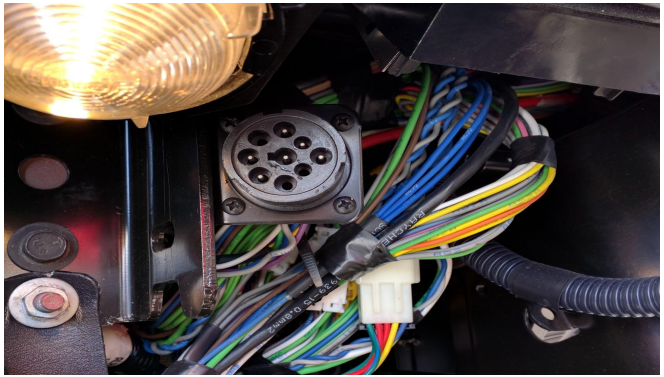
Our Targets

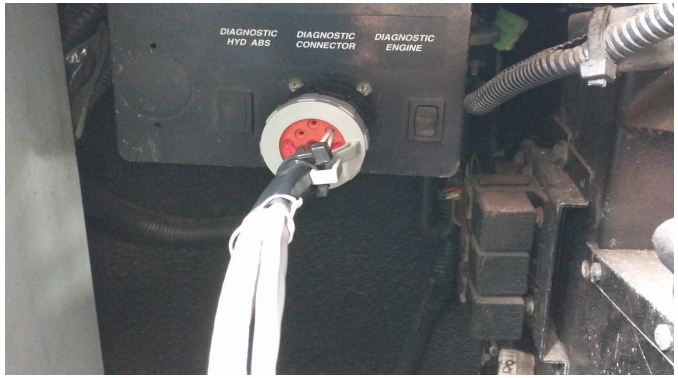
2006 Model
Semi Tractor



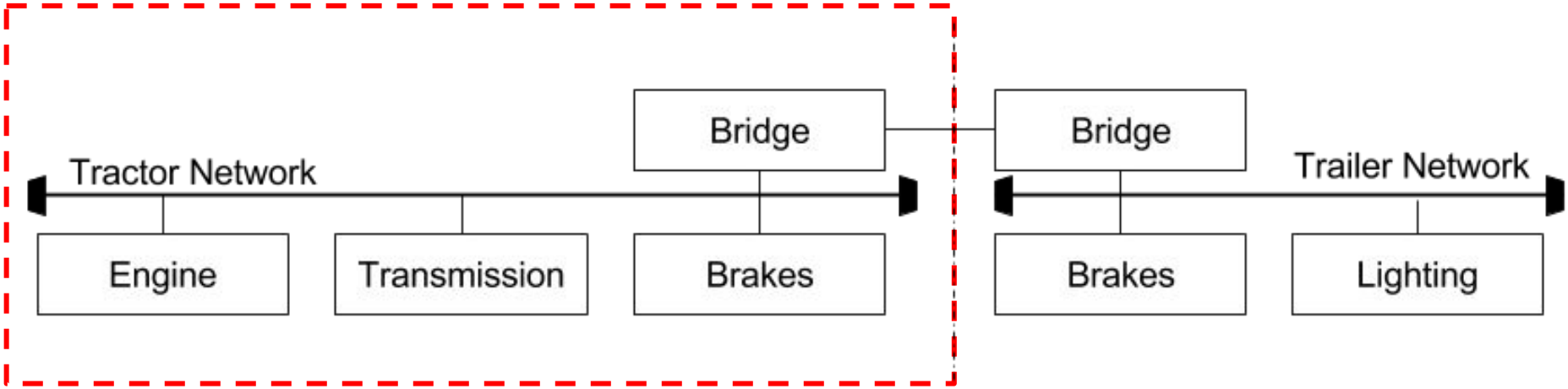
2001 Model School Bus







Typical Heavy Truck Network



Instrument Cluster Attack

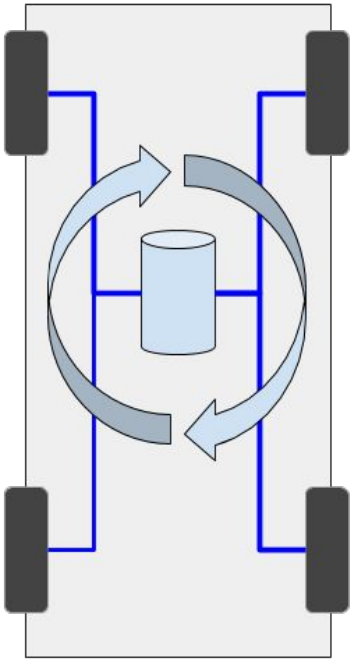
Experiment Progression:

Packet snooping & packet injection

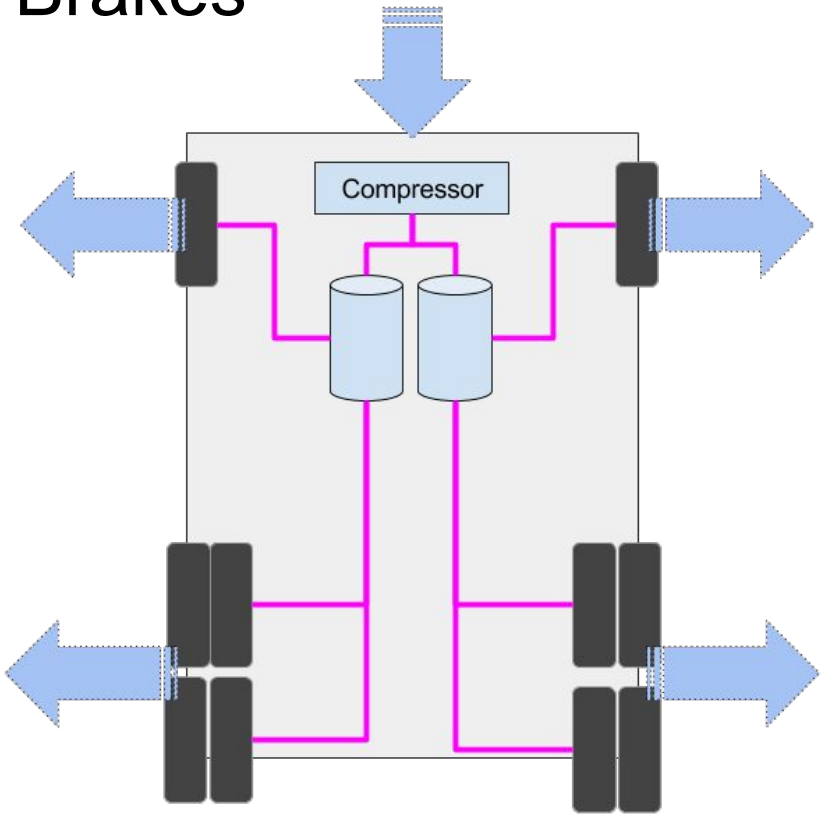
Heavily relied on by vehicle operators


10
15
20
25
30
35
40
0 RPM
5
25
35
45
55
65
75
85
0

Hydraulic & Pneumatic Brakes



Hydraulic Fluid-based Brakes



Pneumatic Brakes


0 RPM
X 100
MPH
KM/H
17
FAULTS

Powertrain Attack

Experiment progression:

Packet recording, replay attack, packet injection script

Powertrain Attack

Part 2: Electric Boogaloo

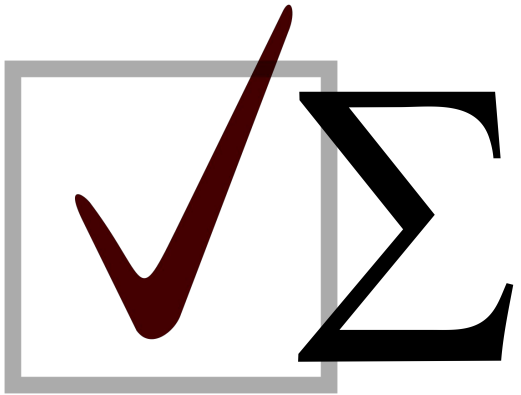
Unmodified attack from 2006 model year truck on 2001 model year school bus

8/9/2016

A very powerful message

- Single PGN for all these attacks
  - Remove driver's ability to input via accel. pedal
  - Disable engine brake
  - Command high and low RPM values

- Largest hurdle: implementing checksum
  - No RE required... checksum is public as well!



Making It Happen

Tools

- PEAK USB-PCAN
  - Data Collection
  - Packet Injection
  - Python APIs
    - Fuzzing Script
- Vector CANoe
  - Data Collection
  - Packet Injection
  - CAPL Scripting language
- Diagnostic Tool
  - ABS valve modulation
  - Engine cylinder cutoff

Test Environment

1. Idle Truck
    - Initial data gathering
    - Attack development
2. Public Roads
    - Data gathering in motion
3. MCity
    - Attacks while in motion

Looking towards the future...

Remote Compromises?

- Telematic Gateway Unit (TGU)
  - Cellular, Bluetooth, CAN (J1939) interfaces
  - C4MAX - Telnet port open by default

Spain	864
Chile	187
Morocco	138
United States	118
Germany	56

C4MAX units on public IP space

- Fleet Management Systems
  - Ubiquitous in several industries
  - GPS data, CAN bus access

Further Areas of Interest

- Diagnostics tool emulation
- More safety critical attacks
- Malicious trailers

So Many Activities...

- Autonomous Semi Trucks
- Connected Vehicles
  - V2V / V2I
- Cargo Ships
- Aircraft

Vulnerability Mitigation Techniques

- Securing the Vehicle Bus:
  - Network Segregation & Isolation
  - Intrusion Detection Systems
  - Message Ownership Verification
  - Message Authentication
  - Strict Message Timing Detection
- Best Practices from ‘traditional’ security domain:
  - Passwords on externally facing devices
  - Vendor Review

Travel to this workshop and future research is sponsored by National Motor Freight Traffic Association, Inc. (NMFTA). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect those of NMFTA.

Truck Hacking:

An Experimental Analysis of the SAE J1939 Standard

10th USENIX Workshop On Offensive Technologies (WOOT'16)

ybura, billhass, ltmillar
@umich.edu

UMTRI TRANSPORTATION RESEARCH INSTITUTE UNIVERSITY OF MICHIGAN

8/9/2016