



Angry Cars

Hacking the car as a platform



OWASP

The Open Web Application Security Project





OWASP

The Open Web Application Security Project

Aaron Weaver

Principal Security Analyst, Pearson eCollege
OWASP Philadelphia Chapter Leader

PEARSON



OWASP

The Open Web Application Security Project

R-Link



A photograph of a bright green Renault car, possibly a Clio, parked on a street. The car is positioned in the lower half of the frame, angled slightly towards the viewer. In the background, there's a large, multi-story brick building with large windows. The overall lighting suggests it might be late afternoon or early evening.

The car is becoming a new platform,” said Mr. Hoffstetter. He said the seven-inch device can be controlled by voice recognition or by buttons on the steering wheel. “We need help now,” he said. “We need developers to work on apps.”

Patrick Hoffstetter, Renault’s Chief Digital Officer

”



OWASP
The Open Web Application Security Project

Application info

phone:

⚠ Your automobile
access handbrake, steering wheel

⚠ Network communication
full Internet access

⚠ Storage
modify/delete SD card contents

⚠ Phone calls
modify phone state, read phone state
and identity

⚠ System tools
write Access Point Name settings

Hide

- **Network communication**
view network state, view Wi-Fi state
- **System tools**
automatically start at boot



OWASP

The Open Web Application Security Project

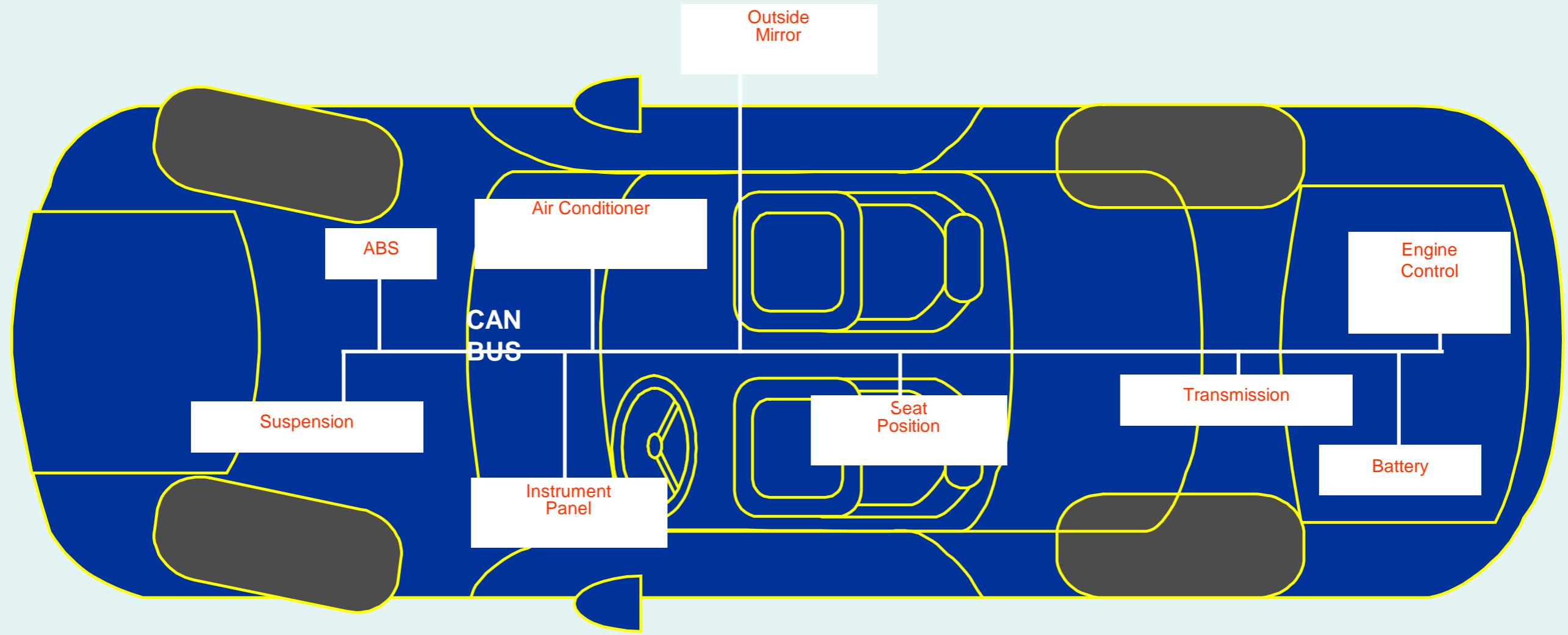
100 MB
of binary code spread
across
50–70
independent computers



Can Bus

Ethernet for Cars





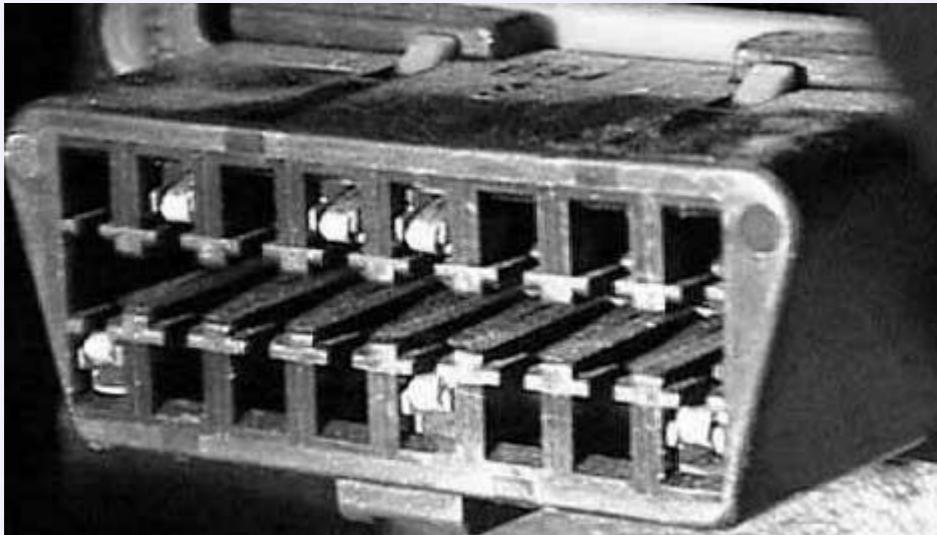


OWASP

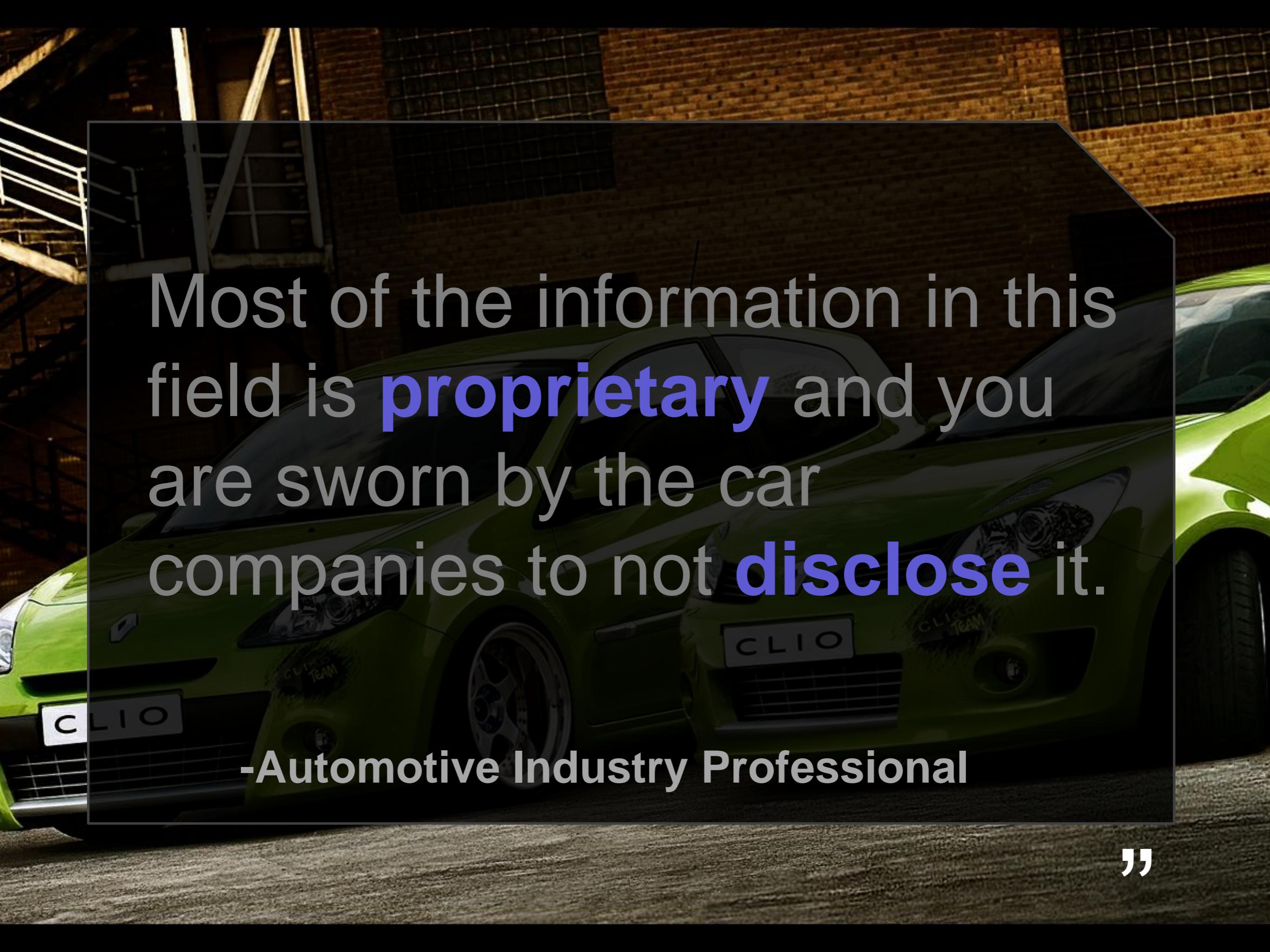
The Open Web Application Security Project

OBD-II

- On-Board Diagnostics





A green Renault Clio race car is shown from a front-three-quarter angle, positioned on a racing track at night. The background features a large, illuminated brick wall with a metal railing. The car's headlights are on, and its body has "CLIO TEAM" printed on it.

Most of the information in this field is **proprietary** and you are sworn by the car companies to not **disclose** it.

-Automotive Industry Professional

”



RIGHT To REPAIR COALITION 2012





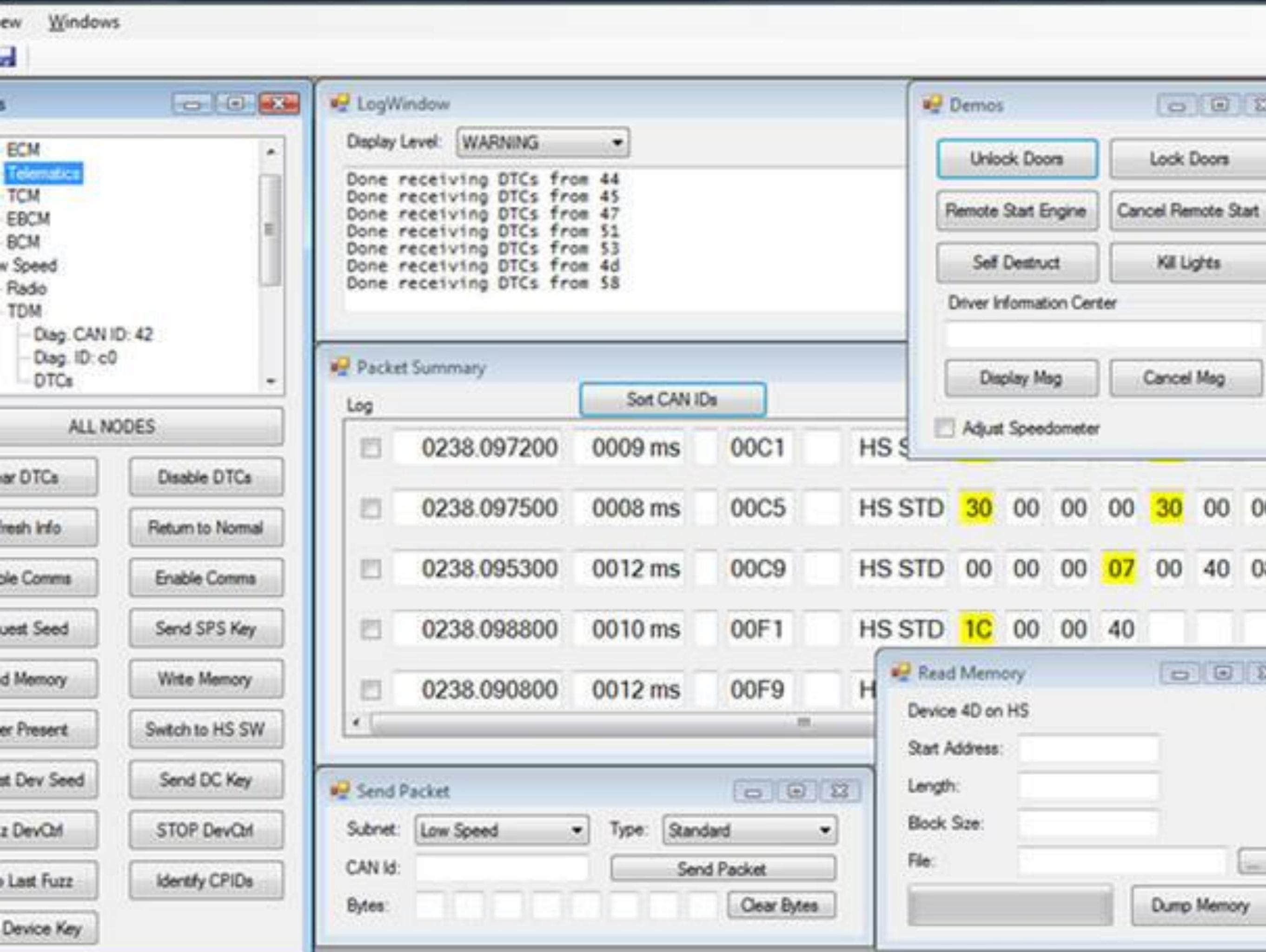
OWASP

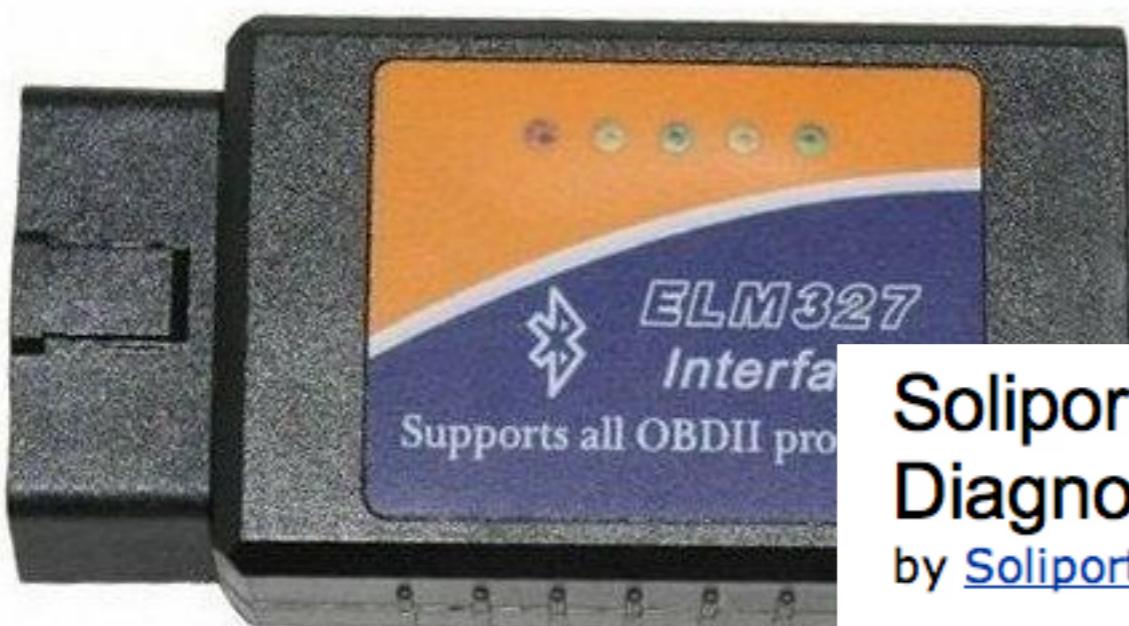
The Open Web Application Security Project

CAN Security Challenges

- Broadcast Nature
- Fragility to DoS
- No Authenticator Fields
- Weak Access Control







Soliport ELM 327 Bluetooth OBDII OBD2 Diagnostic Scanner

by [Soliport](#)

(173 customer reviews) | (15)

Price: **\$14.29**

In Stock.



OWASP

The Open Web Application Security Project

Android Torque

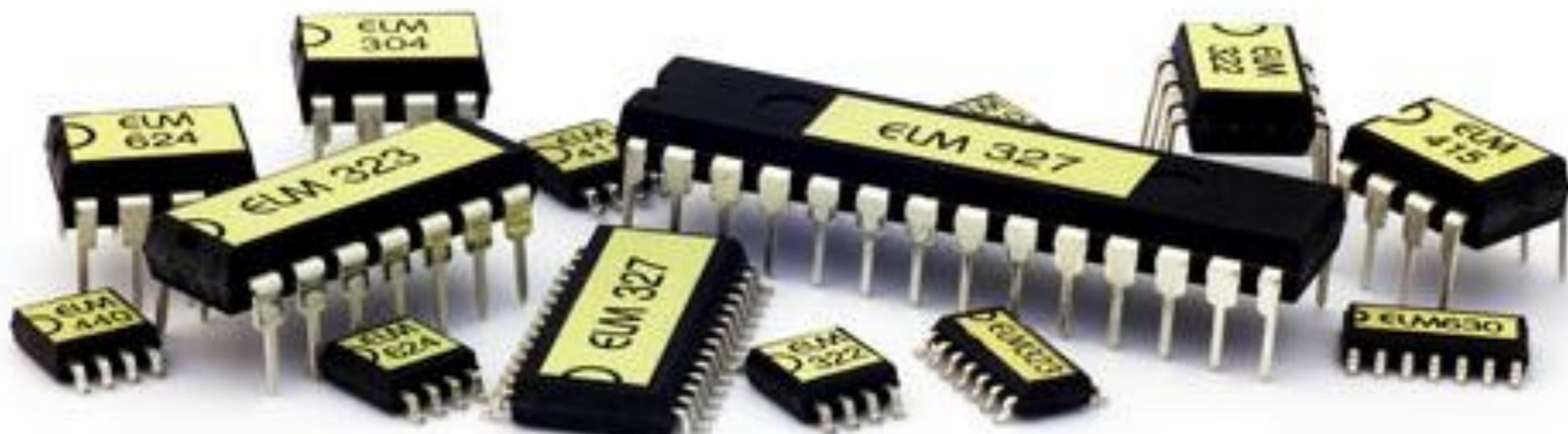


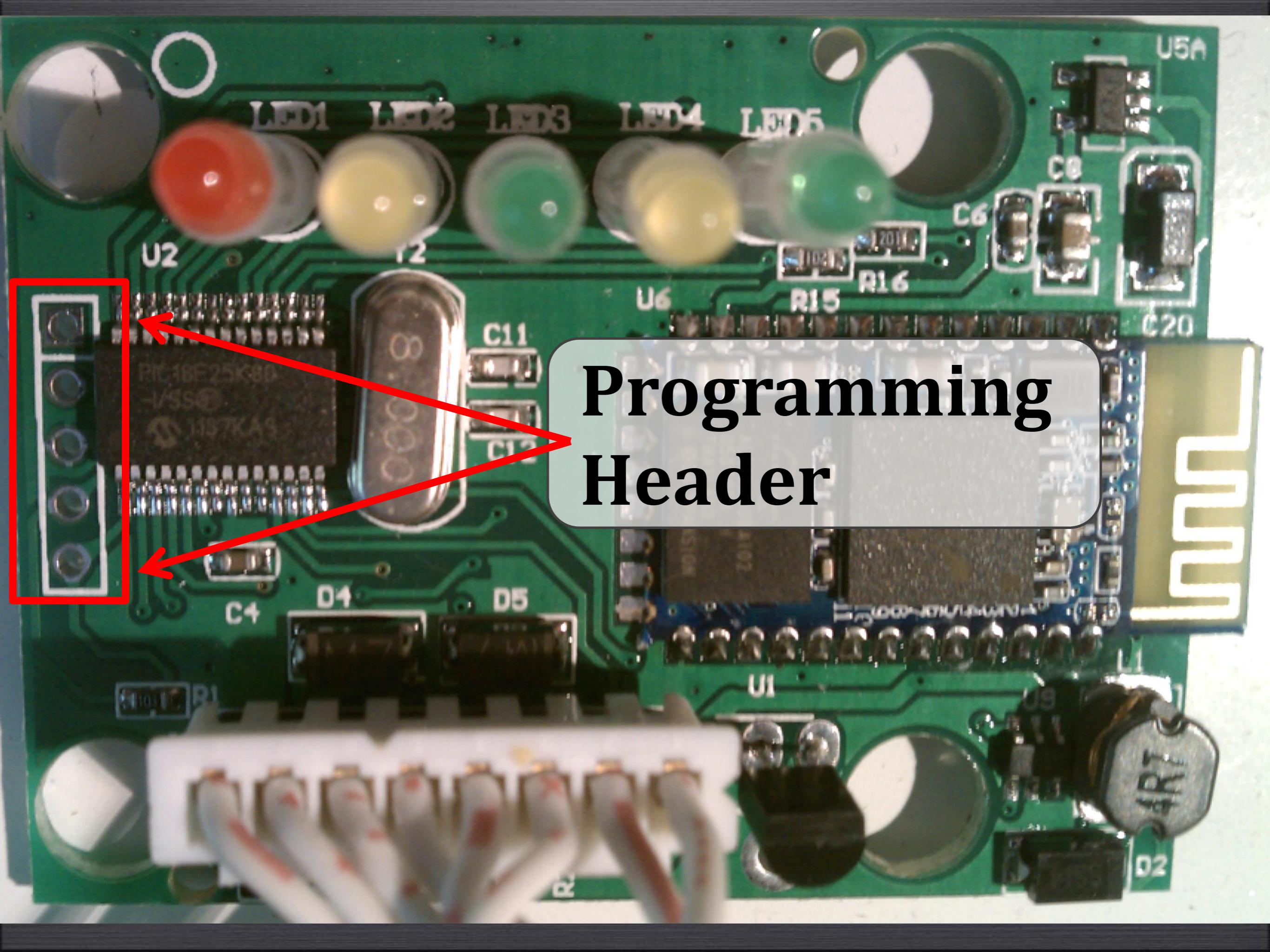


Small Solutions from...

ELM Electronics

Elm Electronics produces a number of integrated circuits or 'chips', such as those shown here:





**Programming
Header**



OWASP

The Open Web Application Security Project

Arduino + CanBus







Drive
Safe &
Save



1

Speak with your agent or [Enroll online](#). You receive an initial discount of up to 5% on your State Farm insurance premium just for participating.



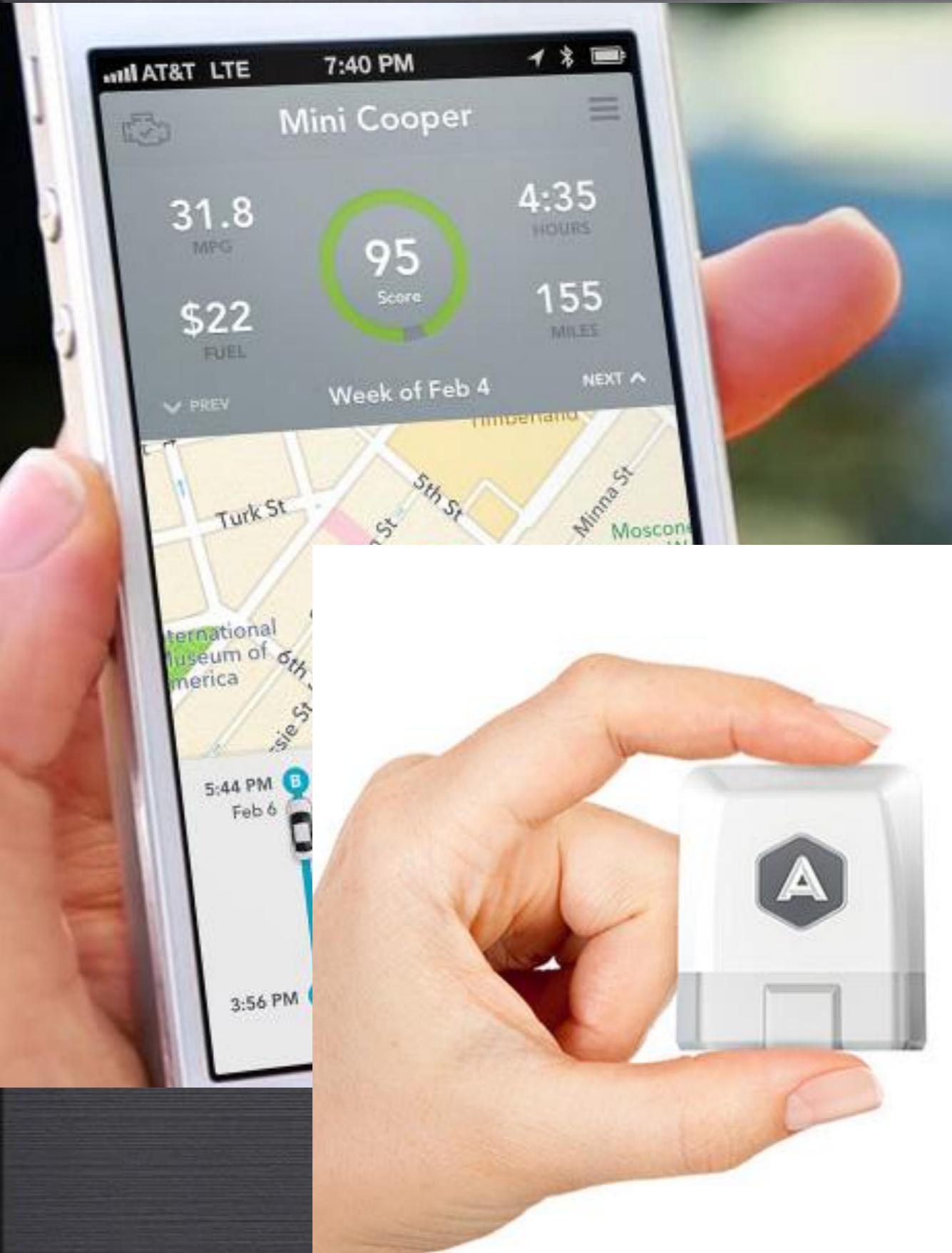
2

We ship you In-Drive, which includes a small device you plug into an easily accessible port under your dashboard.



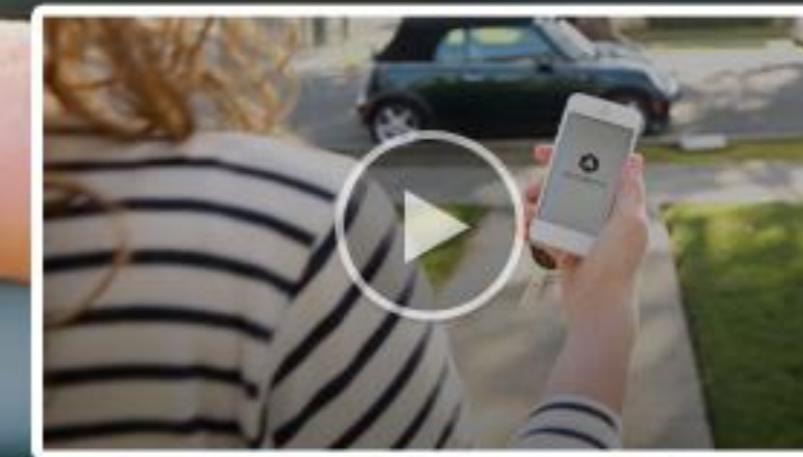
3

Enjoy the benefits of hands-free mobile talking, vehicle diagnostic reports and stolen vehicle recovery assistance for one year free. At each policy renewal you discover the extent of your insurance premium discounts. (With the opportunity for discounts up to 50%!)



Your Smart Driving Assistant

Every car since '96, connected.
\$69.95 - No subscription fees.





2001
Hyundai
Sonata
(EF)
GLS 2.5
AIRBAG



OWASP

The Open Web Application Security Project



WHAT'S POSSIBLE?



OV
The O





Packet					
07	AE	...	25	2B	
07	AE	...	20	88	
07	AE	...	86	07	
07	AE	...	FF	FF	

Result	Manual Override	At Speed	Need to Unlock [†]	Tested on Runway
Engages Front Left Brake	No	Yes	Yes	✓
Engages Front Right Brake/Unlocks Front Left	No	Yes	Yes	✓
Unevenly Engages Right Brakes	No	Yes	Yes	✓
Releases Brakes, Prevents Braking	No	Yes	Yes	✓



Firewall for my car?



OWASP

The Open Web Application Security Project





Vehicle to Vehicle Communication



Engine Control Unit

Transmission Control Unit

Body Controller
Locks/Lights/Etc

Radio

Antilock
Braking
System

Airbag Control Unit

TPMS

OBD-II

Anti-Theft

Keyless
Entry
HVAC

Internet/
PSTN



Telematics





OWASP

The Open Web Application Security Project

Tire Pressure Monitoring System [TPMS]

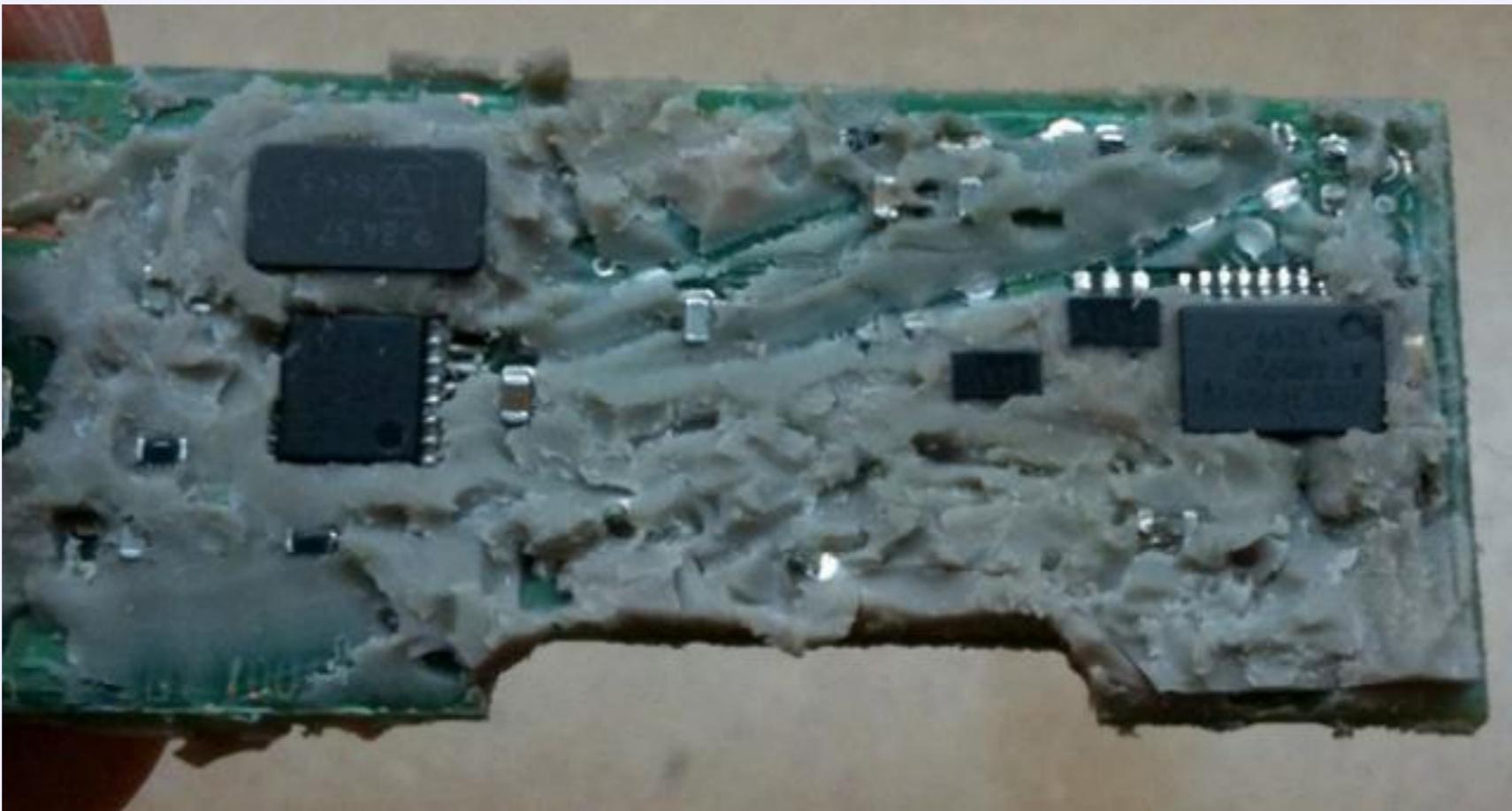




OWASP

The Open Web Application Security Project

What is it?





OWASP

The Open Web Application Security Project

OET Exhibits List

11 Matches found for FCC ID 'KR5S120092001'

<u>View Attachment</u>	<u>Exhibit Type</u>	<u>Date Submitted to FCC</u>	<u>Display Type</u>	<u>Date Available</u>
<u>Attestation</u>	Attestation Statements	05/28/2003	pdf	05/28/2003
<u>Block Diagram</u>	Block Diagram	05/28/2003	pdf	05/28/2003
<u>Cover Letter</u>	Cover Letter(s)	05/28/2003	pdf	05/28/2003
<u>Cover Letters</u>	Cover Letter(s)	05/28/2003	pdf	05/28/2003
<u>External Photos</u>	External Photos	05/28/2003	pdf	05/28/2003
<u>Label Locations</u>	ID Label/Location Info	05/28/2003	pdf	05/28/2003
<u>Internal Photos</u>	Internal Photos	05/28/2003	pdf	05/28/2003
<u>Description</u>	Operational Description	05/28/2003	pdf	05/28/2003
<u>Test Report</u>	Test Report	05/28/2003	pdf	05/28/2003
<u>Test Setup Photos</u>	Test Setup Photos	05/28/2003	pdf	05/28/2003
<u>Users Manual</u>	Users Manual	05/28/2003	pdf	05/28/2003

<http://transition.fcc.gov/oet/ea/fccid/>



Shell





50 Mercedes-Benz within 30 Miles of 18951

Change search location

30



miles

18951

Go

2011 Mercedes-Benz SL63 AMG

4,590 mi.

Silver, 2 door, 2WD, Convertible, Automatic, 8 Cylinders.

\$200 to Unlock Now!!!, \$300 to Schedule!!! (Bitcoins also accepted)

(Collegeville, PA ~ 19 mi. away)

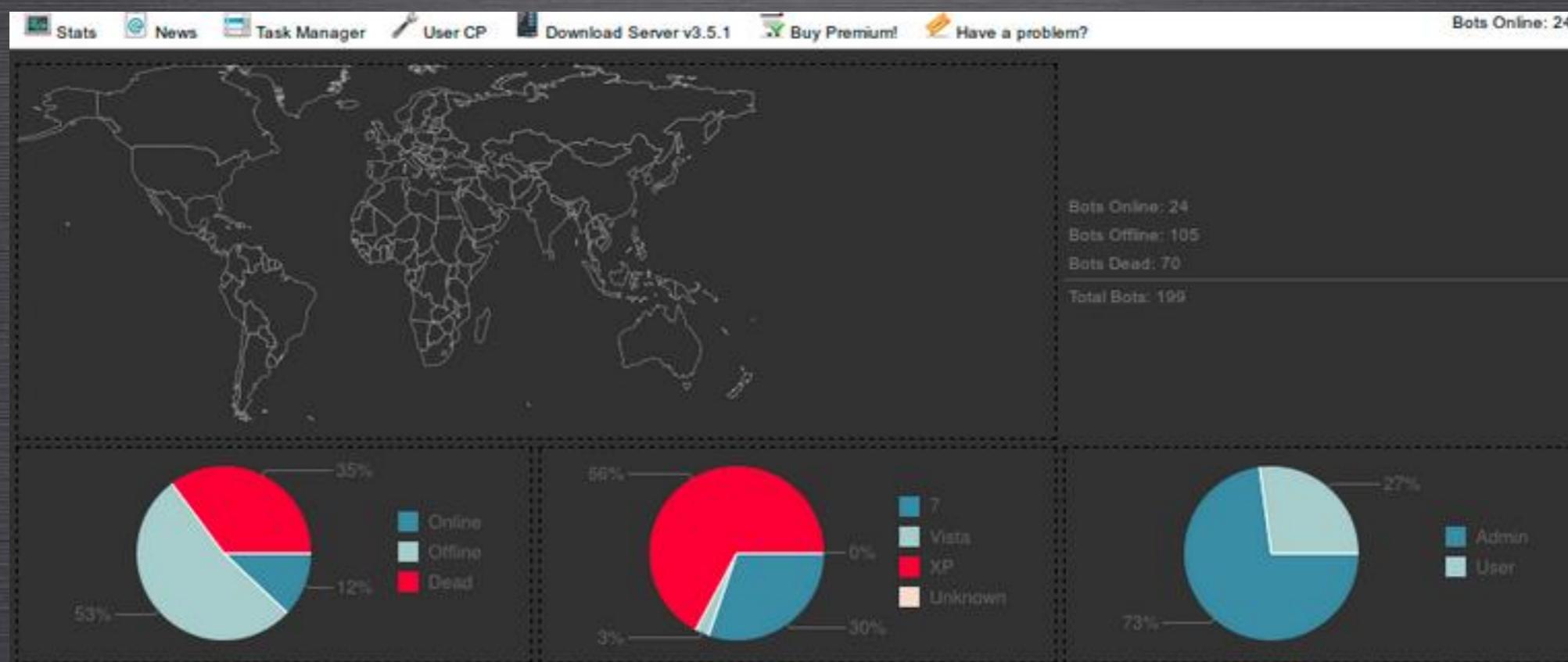
2011 Mercedes-Benz S550 4MATIC

15,576 mi.

Newly Listed

Black, 4 door, AWD, Sedan, 7-Speed Automatic, 5.5L V8 32V MPFI DOHC, Stock# BA378935.

\$150 to Unlock, \$250 to Schedule!!! (Bitcoins also accepted!) (Fort Washington, PA ~ 23 mi. away)





OWASP

The Open Web Application Security Project

APT

[Automotive Persistent Threat]

“

This progression mirrors the evolution of desktop computer compromises: from **individual attacks**, to mass exploitation via worms and viruses, to **third-party markets** selling compromised hosts as a service.

Source: Comprehensive Experimental Analyses of Automotive Attack Surfaces

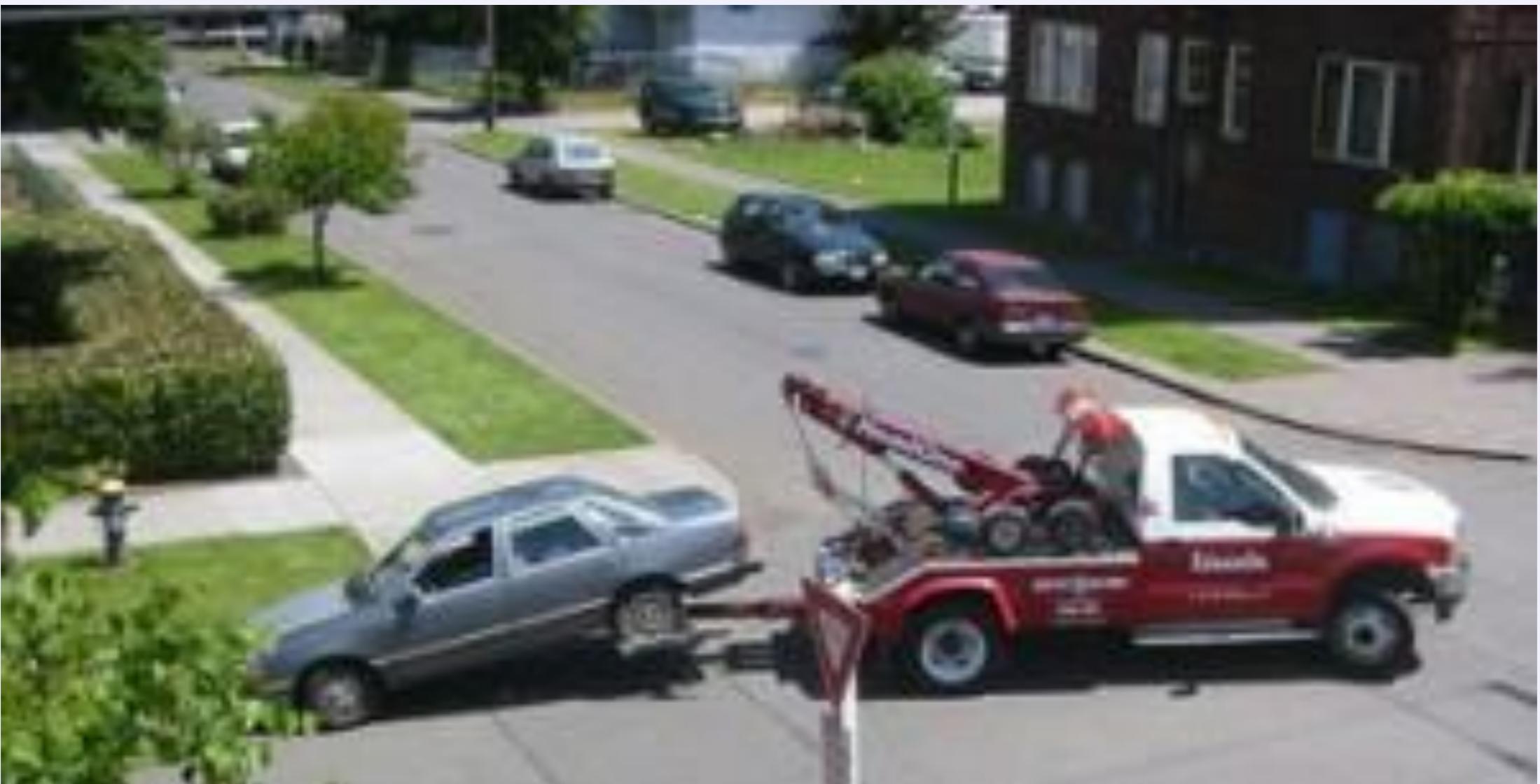
”

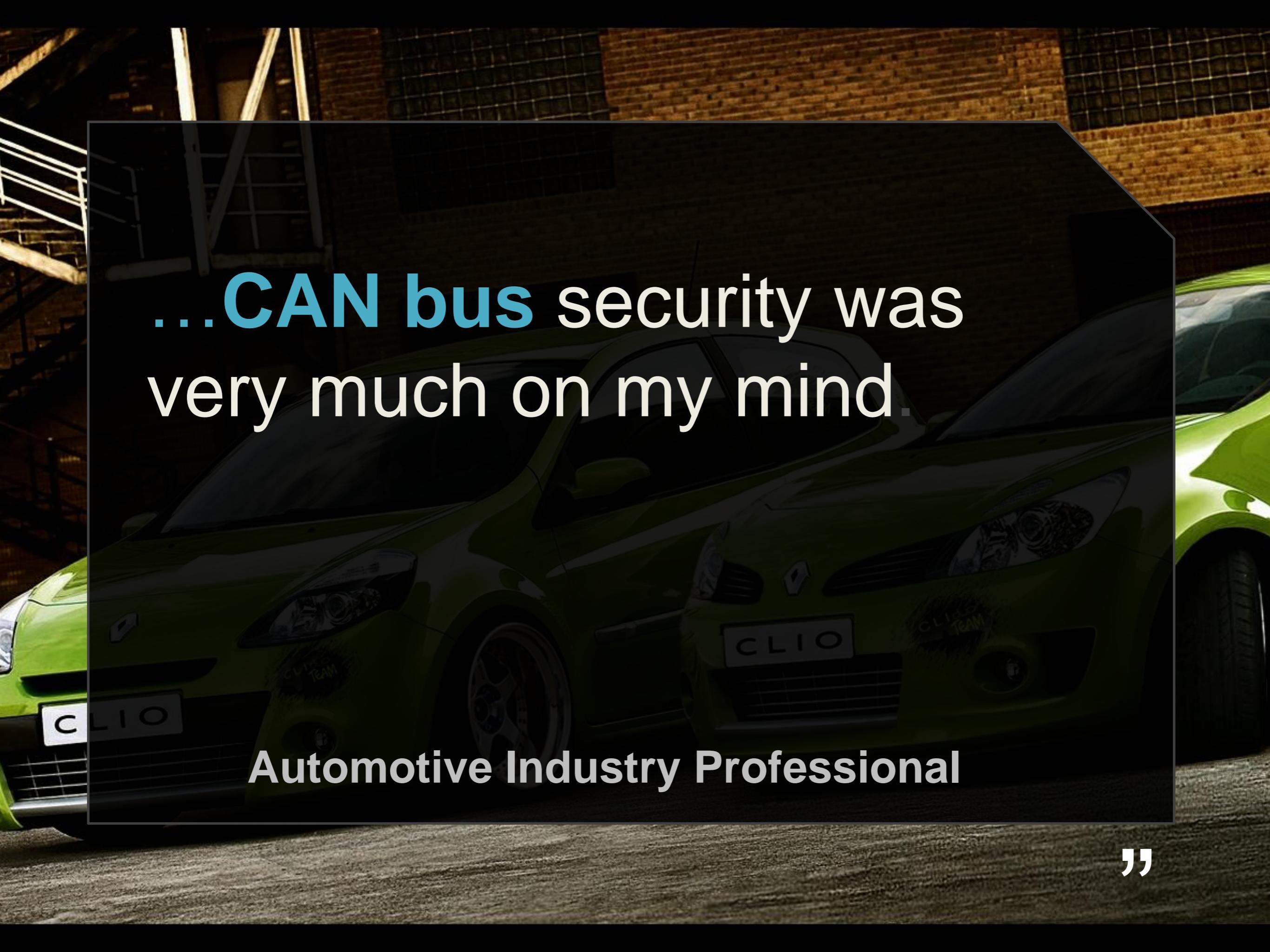


OWASP

The Open Web Application Security Project

Guy Disables More Than 100 Cars Remotely



A green Renault Clio car is parked in front of a brick wall at night. The car's headlights are on, and its license plate area displays the word "CLIO".

...CAN bus security was
very much on my mind.

Automotive Industry Professional

”

myford TOUCH





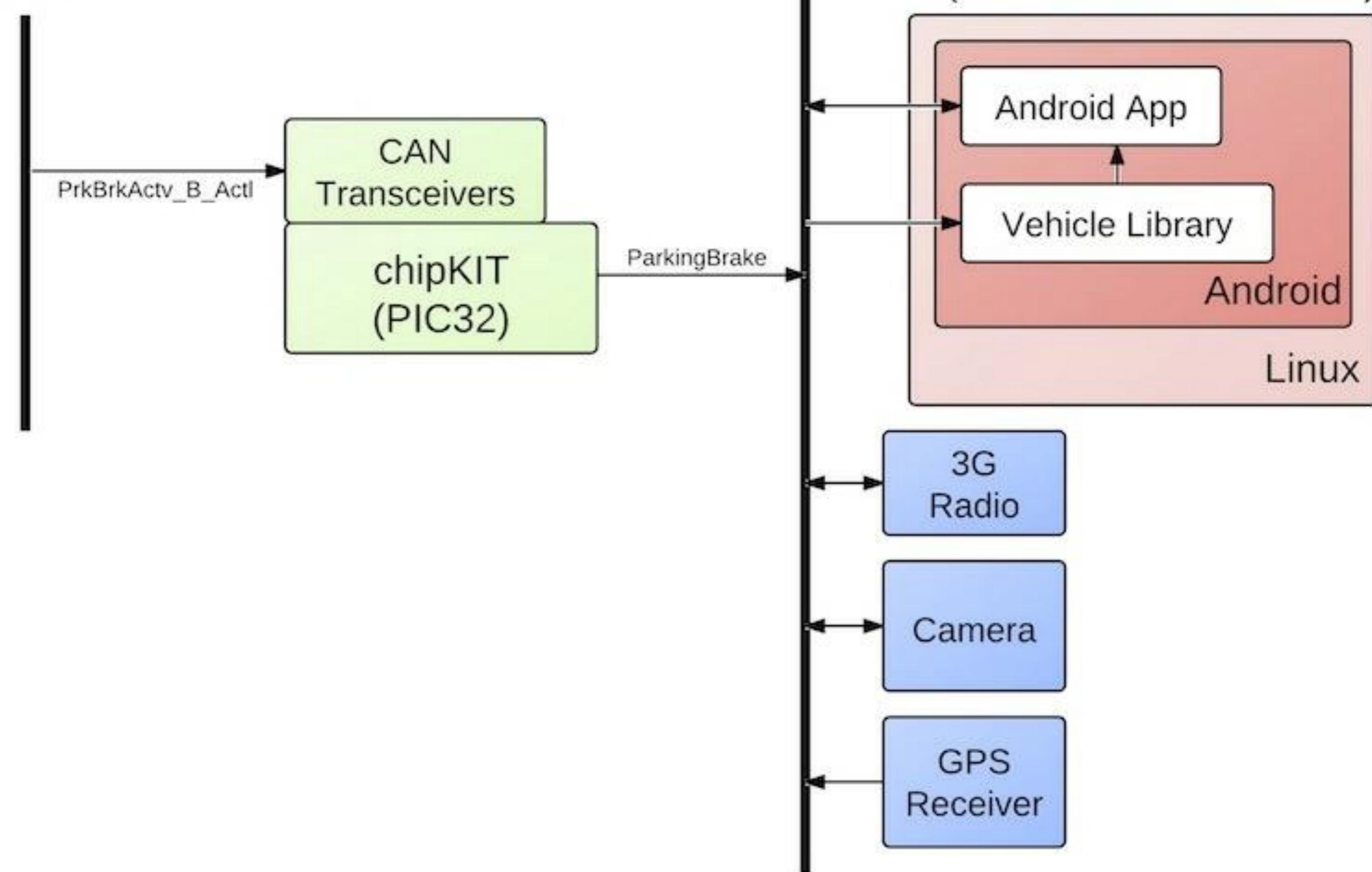
Ford and Bug Labs explore open innovation and crowd sourced, community-driven development

OpenXC Architecture

Reference Phase

CAN

USB / Internal Bus
Android Device
(API version 3.1 or later)





OWASP

The Open Web Application Security Project

Ford's Security

- A successful attack should require physical access to the internals of the module
- A successful attack of one device should not be transferrable to immediately hack all devices
- A general perimeter security architecture including hardware should be used to protect the most sensitive components
- External non-hardwired or user accessible interfaces should be hardened as much as possible with multiple levels of protection



OWASP

The Open Web Application Security Project

Ford's Security

- Protect the vehicle interface at all cost
- ...or to the same level as physical interfaces for serviceability currently mandated by law
- Anyone's failure gives everyone a problem







OWASP

The Open Web Application Security Project

BMW AppCenter





ConnectedDrive

Dienstestatus

Apps

BMW Apps

Facebook

 Twitter

Webradio

Plugins

The screen shows a feed of posts from a social media application:

- It's 66°F out and I'm driving a...
- I'm online in my BMW with B...
- On my way to SILVER AVENU...
- Arriving in SILVER AVENUE, ...
- It's 66°F here in EAST PALO A...

To the right, there is an "Entertainment d..." section showing active apps:

- BMW apps active:
- Web radio
- 'A' Net Station

At the bottom, it says "Web Radio The Way It Should Be".

Eingehende Tweets

13:34

 Tweet senden

Aktualisiert: 13:34



ThomasJons

Auf dem Weg nach B



JuliaSvena

10°C und ich fahr mei

TobyAmber

CUE
CUE





Phone A

Jeff Jones

123-456-7890

00:03:24



MPH



1564 mi

P RNDM





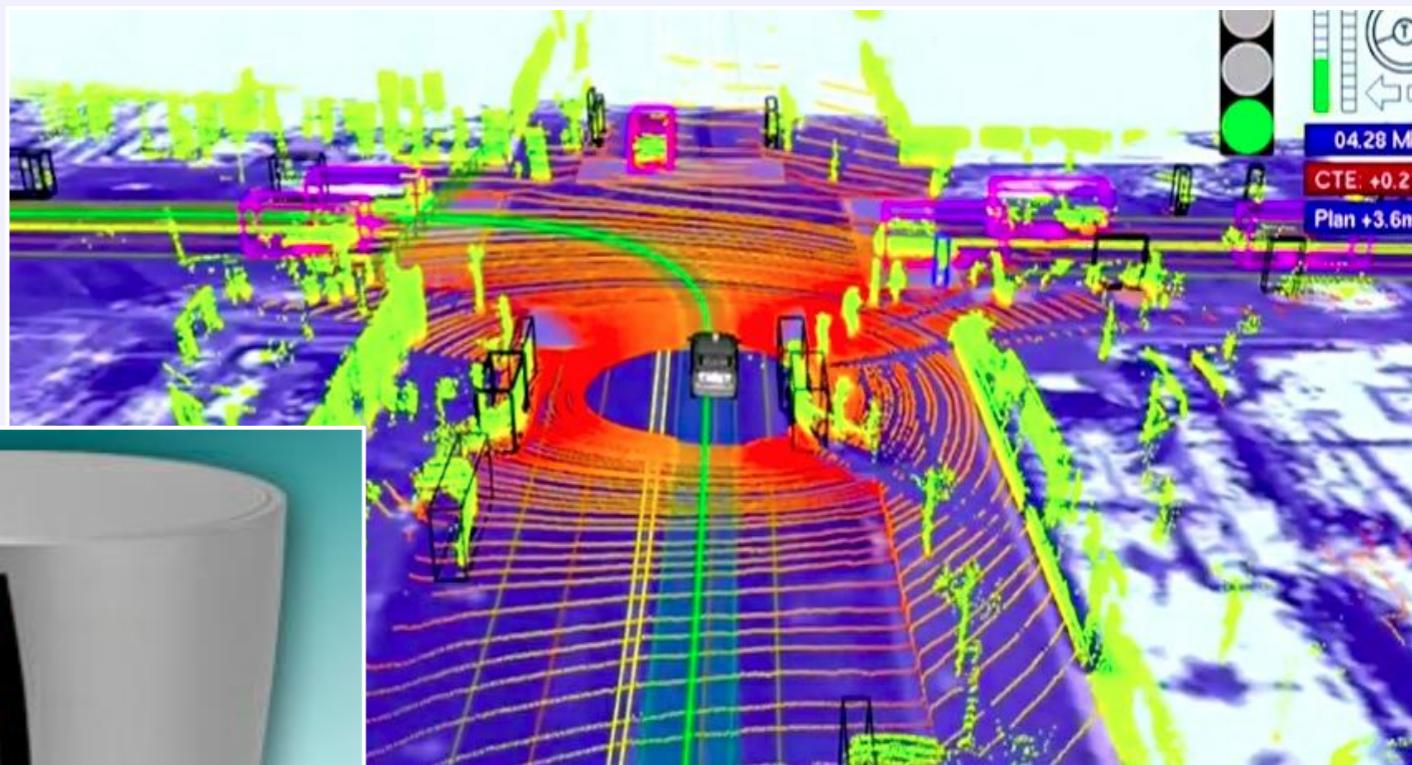




OWASP

The Open Web Application Security Project

Jam the laser?



the obsessive - compulsive detective



MONK

Skyline Hills Resort

Estimated Driving
Time: 32 Minutes

Aaron Weaver

* twitter: @weavera





OWASP

The Open Web Application Security Project

References

- <http://autosec.org>
- Experimental Security Analysis of a Modern Automobile
- Comprehensive Experimental Analyses of Automotive Attack Surfaces