Angry Cars
Hacking the car as a platform

OWASP
The Open Web Application Security Project
Aaron Weaver
Principal Security Analyst, Pearson eCollege
OWASP Philadelphia Chapter Leader
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*
⚠️ 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
100 MB of binary code spread across 50–70 independent computers
Ethernet for Cars
• On-Board Diagnostics
Most of the information in this field is proprietary and you are sworn by the car companies to not disclose it.

-Automotive Industry Professional
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) | 👍 Like (15)

Price: $14.29

In Stock.
Elm Electronics produces a number of integrated circuits or 'chips', such as those shown here:
Programming Header
Arduino + CanBus
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.

1

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

2

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.
WHAT’S POSSIBLE?
<table>
<thead>
<tr>
<th>Packet</th>
<th>07 AE ... 25 2B</th>
</tr>
</thead>
<tbody>
<tr>
<td>07 AE ... 20 88</td>
<td></td>
</tr>
<tr>
<td>07 AE ... 86 07</td>
<td></td>
</tr>
<tr>
<td>07 AE ... FF FF</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Result</th>
<th>Manual Override</th>
<th>At Speed</th>
<th>Need to Unlock†</th>
<th>Tested on Runway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engages Front Left Brake</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>✓</td>
</tr>
<tr>
<td>Engages Front Right Brake/Unlocks Front Left</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>✓</td>
</tr>
<tr>
<td>Unevenly Engages Right Brakes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>✓</td>
</tr>
<tr>
<td>Releases Brakes, Prevents Braking</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>✓</td>
</tr>
</tbody>
</table>
Firewall for my car?
Tire Pressure Monitoring System [TPMS]
What is it?
# OET Exhibits List

11 Matches found for FCC ID 'KR5S120092001'

<table>
<thead>
<tr>
<th>View Attachment</th>
<th>Exhibit Type</th>
<th>Date Submitted to FCC</th>
<th>Display Type</th>
<th>Date Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation</td>
<td>Attestation Statements</td>
<td>05/28/2003</td>
<td>pdf</td>
<td>05/28/2003</td>
</tr>
<tr>
<td>Block Diagram</td>
<td>Block Diagram</td>
<td>05/28/2003</td>
<td>pdf</td>
<td>05/28/2003</td>
</tr>
<tr>
<td>Cover Letter</td>
<td>Cover Letter(s)</td>
<td>05/28/2003</td>
<td>pdf</td>
<td>05/28/2003</td>
</tr>
<tr>
<td>Cover Letters</td>
<td>Cover Letter(s)</td>
<td>05/28/2003</td>
<td>pdf</td>
<td>05/28/2003</td>
</tr>
<tr>
<td>External Photos</td>
<td>External Photos</td>
<td>05/28/2003</td>
<td>pdf</td>
<td>05/28/2003</td>
</tr>
<tr>
<td>Label Locations</td>
<td>ID Label/Location Info</td>
<td>05/28/2003</td>
<td>pdf</td>
<td>05/28/2003</td>
</tr>
<tr>
<td>Internal Photos</td>
<td>Internal Photos</td>
<td>05/28/2003</td>
<td>pdf</td>
<td>05/28/2003</td>
</tr>
<tr>
<td>Description</td>
<td>Operational Description</td>
<td>05/28/2003</td>
<td>pdf</td>
<td>05/28/2003</td>
</tr>
<tr>
<td>Test Setup Photos</td>
<td>Test Setup Photos</td>
<td>05/28/2003</td>
<td>pdf</td>
<td>05/28/2003</td>
</tr>
</tbody>
</table>

http://transition.fcc.gov/oet/ea/fccid/
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)
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
Guy Disables More Than 100 Cars Remotely
...**CAN bus** security was very much on my mind.
Ford and Bug Labs explore open innovation and crowd sourced, community-driven development.
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

Source: Michael Westra, Sync Lead Ford
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 black eye

Source: Michael Westra, Sync Lead Ford
Jam the laser?
the obsessive - compulsive detective

MONK
Skyline Hills Resort

Estimated Driving Time: 32 Minutes
References

- [http://autosec.org](http://autosec.org)
- Experimental Security Analysis of a Modern Automobile
- Comprehensive Experimental Analyses of Automotive Attack Surfaces