CANtact
Open Tools for Automotive

Eric Evenchick
Who?
Who?
Cars are Computers
Cars are Computers

- Safety
- Advanced Features
- Emissions
Cars are Networks

- Modern vehicle: ~100 Electronic Control Units (ECUs)
- Internal network is trusted
Cars are Networks

• Now with Internet!
  • 1996: GM launches OnStar
  • Today: many cars have vehicle apps
  • April 2018: all cars sold in EU must have eCall
Vulnerable Systems

- Millions of lines of code in a vehicle
- Internal network is trusted
- Potential for abuse is high
“With 50 times more code than a Raptor Fighter jet!”
“250 times more code than the […] Space Shuttle!”
Automotive Security

- Security by Obscurity
- Access to CAN is “hard”
- Researchers don’t know CAN
- Once we connect to IP…
A Brief History of Car Hacking

- 1991 - CARB introduces OBD, required for CA
- 1996 - OBD-II required for all US vehicles
- 2008 - All US vehicles must use CAN bus
- 2010 - CAESS publishes first paper
- 2015 - Miller & Valasek demonstrate remote exploit
- 2015 - Megamos Crypto attack released (key attacks)
Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Hackers can easily drain the battery on the world's most popular electric car

The popular Nissan Leaf electric car can be drained of its battery life using little more than its vehicle identification number (VIN).

The major security hole was found by researcher Troy Hunt, who figured out that the Leaf's smartphone app interface (API) uses only the VIN to control car features remotely without passwords. These features include seeing the car's current battery life, times and distances the car has traveled, and...
What is CAN?

• Controller Area Network

• Low cost, integrated controllers

• Types:
  • High speed (differential)
  • Low speed (single ended)
  • Fault Tolerant

• CAN FD
How CAN Works

- **Bus**: collection of collected controllers
- **Frame**: a single CAN ‘packet’ consisting of:
  - **Identifier** - What is this message?
  - **Data Length Code** - How long is the data?
  - **Data** - What does it say?
How CAN Works

Signal Database

<table>
<thead>
<tr>
<th>ID</th>
<th>Byte 0</th>
<th>Byte 1</th>
<th>Byte 2</th>
<th>Byte 3</th>
<th>Byte 4</th>
<th>Byte 5</th>
<th>Byte 6</th>
<th>Byte 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x123</td>
<td>0x05</td>
<td>0xDC</td>
<td>0xDE</td>
<td>0xAD</td>
<td>0xBE</td>
<td>0xEF</td>
<td>0xDE</td>
<td>0xAD</td>
</tr>
</tbody>
</table>

Engine Control Module

Instrument Cluster
How CAN Works

Signal Database

<table>
<thead>
<tr>
<th>ID</th>
<th>Byte 0</th>
<th>Byte 1</th>
<th>Byte 2</th>
<th>Byte 3</th>
<th>Byte 4</th>
<th>Byte 5</th>
<th>Byte 6</th>
<th>Byte 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x123</td>
<td>0x05</td>
<td>0xDC</td>
<td>0xDE</td>
<td>0xAD</td>
<td>0xBE</td>
<td>0xEF</td>
<td>0xDE</td>
<td>0xAD</td>
</tr>
</tbody>
</table>

Engine Control Module

Engine RPM

0x5DC = 1500 RPM

Instrument Cluster
How CAN Works

Diagnostics

Client (Scan Tool) -> UDS Request -> Server (Automotive Controller) -> UDS Response -> Client (Scan Tool)
OBD-II

- Diagnostic standard
- Originally for smog testing
- Provides easy network access
  - As of 2008: CAN
- Cheap useful tools!
Should You Hack Your Car?
Yes!
Hack Your Car

• Low Cost OBD-II Tools
• Bluetooth or USB
• Totally Insecure!
Hack Your Car

- Perform Diagnostics
- Learn how cars work
- Most tools are expensive :(
- CANtact: Open Source Hardware & Software for CAN Bus
CANtact Hardware

- Single Channel USB High-Speed CAN device
- Uses “virtual serial port” and LAWICEL protocol
- Based on single MCU: STM32F0
- Jumper selectable pinout & termination
- Open source hardware
CANtact Software
Current Software Limitations

Commercial

• Expensive
• Windows only
• Not extensible

Open Source

• Linux only
• Hard to use
• Limited graphical tools
Design Goals

• Cross-platform (Windows, OS X, Linux)
• GUI, easy to use
• Raw CAN + Diagnostics
• Easy to extend
• Hardware Agnostic
• Focus on Reverse Engineering
Design Choices

• Java 8 + Netbeans Platform
• Direct device access
• Open source
I had a problem so I thought to use Java

Now I have a ProblemFactory
<table>
<thead>
<tr>
<th>Timestamp</th>
<th>ID</th>
<th>DLC</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.817</td>
<td>192</td>
<td>0</td>
<td>5E  BF  EB  37  ED</td>
</tr>
<tr>
<td>24.813</td>
<td>1431</td>
<td>161</td>
<td>80  4A  80  68  D3  5E  6A 14</td>
</tr>
<tr>
<td>24.810</td>
<td>1196</td>
<td>0</td>
<td>8D  A3  E8  37  18  D4  2A 1E</td>
</tr>
<tr>
<td>24.808</td>
<td>1516</td>
<td>0</td>
<td>8E  43  9E  48  FB  81  9B 11</td>
</tr>
<tr>
<td>24.804</td>
<td>2156</td>
<td>0</td>
<td>5D  2D  22  51  95  42  09  SF</td>
</tr>
<tr>
<td>24.802</td>
<td>3166</td>
<td>0</td>
<td>57  E2  DB  6E  DB  12  54  57</td>
</tr>
<tr>
<td>24.789</td>
<td>516</td>
<td>0</td>
<td>57  43  C6  0A  44</td>
</tr>
<tr>
<td>24.789</td>
<td>1900</td>
<td>0</td>
<td>8A  20  88  28  8E  D2  85 52</td>
</tr>
<tr>
<td>24.789</td>
<td>1039</td>
<td>0</td>
<td>2E  C6</td>
</tr>
<tr>
<td>24.775</td>
<td>125</td>
<td>0</td>
<td>13A</td>
</tr>
<tr>
<td>24.771</td>
<td>1042</td>
<td>0</td>
<td>8C  DF  00  6D  F5  83  4E</td>
</tr>
<tr>
<td>24.777</td>
<td>1413</td>
<td>0</td>
<td>83  33  A3  3F  58  3D  F6 01</td>
</tr>
<tr>
<td>24.773</td>
<td>1244</td>
<td>0</td>
<td>3C  83  C1  6A  81  1A  CE 79</td>
</tr>
<tr>
<td>24.763</td>
<td>1125</td>
<td>0</td>
<td>8D  C9  C7  51  E6  50  40  38</td>
</tr>
<tr>
<td>24.763</td>
<td>1178</td>
<td>0</td>
<td>6A  DF  B5  17  39  AA</td>
</tr>
<tr>
<td>24.762</td>
<td>720</td>
<td>0</td>
<td>87  52  A0  12  9F  17  15 56</td>
</tr>
<tr>
<td>24.762</td>
<td>1655</td>
<td>0</td>
<td>32  F6  92</td>
</tr>
<tr>
<td>24.749</td>
<td>1276</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24.749</td>
<td>1479</td>
<td>0</td>
<td>82  1A  7D  B2  83  D5  45</td>
</tr>
<tr>
<td>24.735</td>
<td>1375</td>
<td>0</td>
<td>52  52  0C  68  0E</td>
</tr>
<tr>
<td>24.735</td>
<td>1152</td>
<td>0</td>
<td>8C  B9  4D  24  91  DF  64 32</td>
</tr>
<tr>
<td>24.735</td>
<td>829</td>
<td>0</td>
<td>85  EC  A5  24  9B  1F  95 73</td>
</tr>
<tr>
<td>24.735</td>
<td>1236</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24.716</td>
<td>784</td>
<td>0</td>
<td>8D  D3  6F  2D  72  68  3F 48</td>
</tr>
<tr>
<td>24.716</td>
<td>1118</td>
<td>0</td>
<td>7B  DD  44  2A  31  54  88</td>
</tr>
<tr>
<td>24.716</td>
<td>1718</td>
<td>0</td>
<td>8F  E0  70  53  76  B0  ED 01</td>
</tr>
<tr>
<td>24.716</td>
<td>1980</td>
<td>0</td>
<td>75  87  2E  5C  13  63  27</td>
</tr>
<tr>
<td>24.716</td>
<td>784</td>
<td>0</td>
<td>49  69  88  4C</td>
</tr>
<tr>
<td>24.716</td>
<td>1118</td>
<td>0</td>
<td>1D  7</td>
</tr>
<tr>
<td>24.716</td>
<td>899</td>
<td>0</td>
<td>80  3A  8A  0F  BA  24  07 63</td>
</tr>
<tr>
<td>24.716</td>
<td>448</td>
<td>0</td>
<td>12A</td>
</tr>
<tr>
<td>24.698</td>
<td>855</td>
<td>0</td>
<td>69  DB  90  10  A5  7F</td>
</tr>
<tr>
<td>24.694</td>
<td>1920</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24.694</td>
<td>1298</td>
<td>0</td>
<td>87  50  A0  4A  EB  7D  49 71</td>
</tr>
<tr>
<td>24.694</td>
<td>398</td>
<td>0</td>
<td>8E  EB  7A  55  C7  24  87 26</td>
</tr>
<tr>
<td>24.686</td>
<td>398</td>
<td>0</td>
<td>8E  DA  0A  57  01  28  D0 2D 1B</td>
</tr>
</tbody>
</table>
Live
Live
ISOTP
Diagnostics
Scripting

• Built in support for scripting in Javascript
• onCanReceived and onIsotpReceived callbacks
• Transmit, log, etc…
• Example: Security Key Extraction
Risk?

- Who’s hacking cars?
  - Owners: increase performance
  - Thieves: financial gain
  - Stunts: personal gain, brand damage
  - Cybercrime: Ransomware?
  - etc…
Analyzing Risk
Usage Models

• Traditionally, vehicle occupants are trusted

• Today:
The Connected Car

100% Of cars will be connected by 2025

75% Of cars on the road will be autonomous by 2035

Source: 1GSMA 2013, 2Navigant Research 2013
Emerging Tech

• Crypto CAN (MACs, proprietary)

• CAN FD

• Automotive Ethernet
  • IEEE 100BASE-T1 (BroadR-Reach)
Questions?

https://github.com/linklayer

http://cantact.io

@ericevenchick

eric@evenchick.com