OCTANE
(Open Car Testbed and Network Experiments): Bringing Cyber-Physical Security Research to Researchers and Students

6th Workshop on Cyber Security Experimentation and Test (CSET `13)
August 12, 2013
Washington, D.C.

Christopher E. Everett        Damon McCoy
George Mason University
How OCTANE can help with security research!

- Advantages:
  - Sharing of portable XML files
  - Easy to use GUI for software package
  - Quick addition of network hardware
  - Straight-forward guidelines to setup/select hardware framework for testing
  - Software package to be released open source

- These advantages mean:
  - Your lab can be up and running faster and at a lower cost!
  - Your team does not have to worry about the network setup and configuration but can focus on your expertise – Security!
  - Your team can extend the software package to fit your needs instead of being limited by a commercial software package designed for network development.
Why is Automotive Security Testing Challenging?

<table>
<thead>
<tr>
<th>Positives</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automotive networks (e.g., CAN) are standardized</td>
<td>Limited documentation about propriety automotive network implementations of networks</td>
</tr>
<tr>
<td>Automotive network hardware is readily available off the shelf</td>
<td>Hardware is designed for testing and building the systems</td>
</tr>
<tr>
<td>Automotive network software is readily available off the shelf</td>
<td>Software is designed for testing and building the systems &amp; is expensive</td>
</tr>
<tr>
<td>Automotive networks are readily available (most folks have a car)</td>
<td>Researchers do not want to use their own vehicles for invasive testing &amp; purchasing new cars is expensive</td>
</tr>
<tr>
<td>Automotive parts are readily available (numerous stores selling parts)</td>
<td>Automotive parts infrastructure designed for replacement/repair</td>
</tr>
</tbody>
</table>
## Solution: OCTANE

<table>
<thead>
<tr>
<th>Issues</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited documentation about propriety automotive network implementations of networks</td>
<td>Enables reverse engineering &amp; storing of the discovered information in XML files</td>
</tr>
<tr>
<td>Hardware is designed for testing and building the systems</td>
<td>Hardware framework is selected based on research/teaching needs</td>
</tr>
<tr>
<td>Software is designed for testing and building the systems &amp; is expensive</td>
<td>Software package is specifically designed for security testing &amp; will be released open source</td>
</tr>
<tr>
<td>Researchers do not want to use their own vehicles for invasive testing &amp; purchasing new cars is expensive</td>
<td>Hardware framework enables selection of low cost network setup</td>
</tr>
<tr>
<td>Automotive parts infrastructure designed for replacement/repair</td>
<td>Hardware framework provides a guide to selection of parts</td>
</tr>
</tbody>
</table>
OCTANE

• Software package and hardware framework for reverse engineering and testing of automotive networks

• Software Package
  • **Goal:** Facilitate reverse engineering and security testing
  • Architecture
  • XML automation
  • Packet monitor
  • Custom transmit

• Hardware Framework
  • **Goal:** Enable researchers/students to quickly setup an automobile network
  • Lab network setup
  • Real-world test setup
OCTANE Architecture

- Provides expansion opportunities
  - New hardware can quickly be added through the hardware layer without re-coding the GUI or processing layers
  - XML access provides access to a portable, human-readable file for storing and sharing information
XML Automation

• Enables storage and sharing of packets, messages, and ECU IDs for future use
• Provides a user the ability to quickly and accurately reproduce and identify network traffic

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&lt;Packet&gt;</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>&lt;Name&gt;</strong></td>
<td>Stop Network Communications</td>
<td><strong>&lt;\Name&gt;</strong></td>
</tr>
<tr>
<td><strong>&lt;ID&gt;</strong></td>
<td>210</td>
<td><strong>&lt;\ID&gt;</strong></td>
</tr>
<tr>
<td><strong>&lt;DLC&gt;</strong></td>
<td>2</td>
<td><strong>&lt;\DLC&gt;</strong></td>
</tr>
<tr>
<td><strong>&lt;Message&gt;</strong></td>
<td>104A</td>
<td><strong>&lt;\Message&gt;</strong></td>
</tr>
<tr>
<td><strong>&lt;\Packet&gt;</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• Future Improvements
  • Wildcards
  • Packet Sequences
  • Packet Responses
  • Packet Subroutines
  • Calculated Packet Responses
Bus Monitor

- Enables viewing of received network packets and transmission of selected packets back to the network.
- Provides a user the ability to test interactions with the network and test security features of the network.

CAN Packet Identity No.: 210
DLC: 2
Data: 10 4A
Custom Transmit

- Enables transmission of pre-configured packets to the network
- Provides a user the ability to test interactions with the network and test security features of the network
Hardware

- **Lab Network Setup**
  - Process to select parts to meet research types, automotive network types, automobile types, adapters, and budget

- **Real-World Test Setup**
  - Process to select automobiles that meet automotive network types, automobile types, adapters, and access

From: Wikimedia Commons

- 2013 Chevrolet Cruze
- 2011 Chevrolet HHR
- 2010 Toyota Matrix
Research and Teaching Opportunities

- **Research Opportunities**
  - Firewall
  - Intrusion Detection System
  - Packet Encryption
  - ECU Authentication
  - ECU Security

- **Teaching Opportunities**
  - Undergraduate Lab Security Exercise
  - Undergraduate Lab Embedded Programming Exercise
  - Graduate Security Testing Exercise
OCTANE Advantages

- Portable XML files
- GUI for fast and accurate packet receipt and transmission
- GUI for creation of XML files
- Wide variety of network hardware
- Hardware framework provides many options for researchers
- Open source software package enables sharing and extensions

Results in:
- Faster setup and configuration!
- Cheaper setup and configuration!
- More time spent on security setup and testing!
Wrap-Up & Discussion

- Future Work / Thoughts
  - XML Automation Extensions
    - Sharing of XML files useful?
    - How would security testing be changed?
  - Remote Access
    - Open the door for researchers to test solutions on other automotive networks?
    - Would researchers/students use remote access?
  - Firewalls
    - Too complicated for CAN networks?
    - Who would manage rules?
  - ECU Security
    - Is ECU built-in security too complicated for automotive manufacturing environment?
    - Who would manage keys/security authorization?