What is Octane?

- OCTANE is an automotive security testbed that facilitates the analysis, understanding, and testing of automotive cyber-physical systems
- Reduces the barrier of entry into security research
- Easier training of automotive networks
- Provide security focused features
  - Ability to replay
  - Fuzz testing
- Open Source Tool
  - Help shaping the research
  - Provide security analysis functions
Why is Automotive Security Testing Challenging?

<table>
<thead>
<tr>
<th>Facts</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automotive networks (e.g., CAN) are</td>
<td>Limited documentation about propriety implementations of</td>
</tr>
<tr>
<td>standardized</td>
<td>automotive networks</td>
</tr>
<tr>
<td>Automotive network software is readily</td>
<td>• Designed for testing</td>
</tr>
<tr>
<td>available off the shelf</td>
<td>• Does not cover security features</td>
</tr>
<tr>
<td></td>
<td>• Expensive</td>
</tr>
<tr>
<td>More students are studying information</td>
<td>Students do not learn automotive networks in school.</td>
</tr>
<tr>
<td>security in school</td>
<td></td>
</tr>
</tbody>
</table>
Solution: OCTANE

<table>
<thead>
<tr>
<th>Issues</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited documentation about propriety implementations of automotive networks</td>
<td>Enables reverse engineering &amp; storing of the discovered information in XML files</td>
</tr>
<tr>
<td>• Designed for testing</td>
<td>Software package is specifically designed for security testing &amp; is released open source</td>
</tr>
<tr>
<td>• Does not cover security features</td>
<td></td>
</tr>
<tr>
<td>• Expensive</td>
<td></td>
</tr>
<tr>
<td>Students do not learn automotive networks in school.</td>
<td>Help students learn automotive networks.</td>
</tr>
</tbody>
</table>
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 has been 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.
Exemplary Automobile Network

- Front Stability Control
- Rear Stability Control
- Tire Pressure Control
- Telematics Control Unit
- Side Mirror Controller
- Body Control Unit
- Door Locks
- Multimedia Display
- Stability Control Unit
- Multimedia Head Unit
- Engine Control Unit
- Junction Box
- OBD Port

Networks:
- CAN Network
- FlexRay Network
- LIN Network
- MOST Network
OCTANE

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

• Software Package
  • **Goal:**
    • Facilitate reverse engineering and security testing architecture
    • Easily share knowledge
    • Packet monitoring and identifying
    • Inject packets

• Hardware Framework
  • **Goal:**
    • Enable use of low cost adaptors with the advanced software.
OCTANE Architecture

- **GUI Layer**
  - Bus Control
  - Bus Monitor
  - XML Edit Interface

- **Processing Layer**
  - Data Converter
  - XML Access

- **Thread Layer**
  - Receive Thread
  - Transmit Thread

- **Hardware Middle Layer**
  - CAN Interface
  - FlexRay Interface

- **Hardware Layer**
  - Kvaser API
  - CAN-AVR Interface

- **XML File**

**Provides expansion opportunities**
- Easily use different hardware
- Industry may have their own xml files that they don’t want to release
- Rapid prototype
XML Automation

- Enables storage and sharing of packets
- Provides a user the ability to quickly and accurately reproduce and identify network traffic

- Improvements from previous version
  - Packet Sequences
  - Calculated Packet Responses
  - Filtering
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.: 621
DLC: 8
Data: 11 80 03 00 00 00 00 00
Compact Bus Monitor

- Enables a better means to follow the changes in the message values.
- Can be used to easily recognize dynamic packets and the bits that are changing.
XML Filter

- Enables instant recognition of known packets using the previously identified packets.
Filter and Highlight

- Enables researchers to focus their studies by using highlighting or filtering features.
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

![Custom Transmit interface](image)
Edit XML of Packets

- Enables easy editing of XML files without the need of accessing the actual XML files.
- Provides a user the ability to build and modify the database without having any knowledge about databases or XML schema.
Log To File

- Enables easy logging of the packets in a text file that can be easily accessed by a wide variety of third party applications.
- Provides tabular structure to enable accessing the tabular version of the logs in the excel program.
Let the fun begin
Research Opportunities

• Research Opportunities
  • Firewall
  • Intrusion Detection System
  • Packet Encryption
  • ECU Authentication
  • ECU Security
  • Rapid prototyping
Wrap-Up & Discussion

• OCTANE Advantages
  • A number of features that facilitates security research, reverse engineering and sharing knowledge between groups

• Potential extension of OCTANE
  • Vulnerability Analysis
  • Intrusion Detection
  • Firewalls
  • Implementing and evaluating security defense mechanism
http://octane.gmu.edu/