CONTROLLER AREA NETWORK (CAN) DEEP PACKET INSPECTION

Görkem Batmaz, Systems Engineer
Ildikó Pete, Systems Engineer
28th March, 2018
Car Hacking

“Immediately my accelerator stopped working. As I frantically pressed the pedal and watched the RPMs climb, the Jeep lost half its speed, then slowed to a crawl.” (Andy Greenberg, Wired)

2014 Jeep Cherokee (remote attack)
Engage brakes, Take control of steering
Agenda

AUTOMOTIVE SECURITY
- Connectivity in Modern Vehicles
- Controller Area Network (CAN) Vulnerabilities

CAN ATTACKS
- Attack Types
- Detection & Prevention

CAN ANOMALY DETECTOR
- Data
- Approach

RESULTS & CONCLUSIONS
- Discussion of Results
Automotive Security

1. Increasing Complexity & functionality
2. Interconnectedness

Vehicle to Vehicle Communication

Engine Control Unit

Transmission Control Unit

Infotainment

TPMS

OBD-II

Internet

Telematics

Figure 1. Some connections of a modern car
Controller Area Network (CAN) Security
CAN Characteristics

Message types: Information, Diagnostic

Message exchange: Broadcast

Message-based protocol, no addressing

Arbitration method to resolve priorities

Figure 2. The CAN network
CAN Vulnerabilities

Confidentiality | Every message sent on CAN is broadcast to every node → Eavesdropping

Authenticity | Lack of sender authentication → Masquerading

Availability | Arbitration rules (high priority messages) → Denial of Service

Non Repudiation | No mechanisms to prove an ECU sent or received a message
Most Critical Attack Types on CAN

- **REPLAY**: Replace message contents with some pre-recorded values
- **INJECTION**: Inject false messages appearing to be legitimate
- **DOS**: Flood the network

**CAN Attacks**

**CAN Anomaly Detector**

**Results & Conclusions**
Detection & Prevention

Device identification

CRYPTOGRAPHIC SERVICES

ANOMALY DETECTION

Over-the-air updates
ECU software integrity

ANTI-MALWARE
Tamper detection

Secure boot
Anomaly Detection

Finding unusual patterns in data that do not conform to expected behavior

E.g. fraud detection
Types of Anomalies

- **Point Anomaly**
  - E.g. vehicle speed is **500 miles/hour**

- **Collective Anomaly**
  - E.g. vehicle speed is **80 miles/hour** & steering wheel angle is **90 degrees**

- **Contextual (Conditional) Anomaly**
  - E.g. vehicle speed changes from **50 miles/hour** to **80 miles/hour** in less than **X seconds**
Controller Area Network (CAN) Anomaly Detector
<table>
<thead>
<tr>
<th>Automotive Security</th>
<th>CAN Attacks</th>
<th>CAN Anomaly Detector</th>
<th>Results &amp; Conclusions</th>
</tr>
</thead>
</table>

Detect security-related CAN network anomalies resulting from malicious activities.

**Attacks:** Injection, Replay

**Anomalies:** Contextual
CAN Frame

- **Start of Frame**: 1 bit
- **CAN ID**: 11 or 29 bits
- **RTR**: 1 bit
- **Control**: 6 bits
- **Data**: 0-64 bits
- **CRC**: 16 bits
- **ACK**: 2 bits
- **End of Frame**: 7 bits

**CAN Message**
# The Dataset: BB8 CAN flow

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>MessageID</th>
<th>Length</th>
<th>PAYLOAD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>BYTE</strong> 0</td>
</tr>
<tr>
<td>574165791302335</td>
<td>101</td>
<td>8</td>
<td>143</td>
</tr>
<tr>
<td>574165791302421</td>
<td>102</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>574165791302432</td>
<td>103</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>574165791302441</td>
<td>104</td>
<td>6</td>
<td>223</td>
</tr>
</tbody>
</table>
Constraints

- Multiple ECUs on the CAN BUS
- Unstructured Data
- Power/Performance

Solutions

- Message ID Selection
- Content Extraction
- Recurrent Neural Networks (RNNs)
Automotive Security

CAN Attacks

CAN Anomaly Detector

Results & Conclusions

Security Solution

CAN BUS

CAN Firewall

Policy Handler

CAN Anomaly Detector

Message ID selector & Content Extractor

1st NNs

2nd NN

Output: Probability of an attack

Contextual Anomaly Detection

Stage 2 Detection

Errors
Recurrent Neural Network (RNN)
Recurrent Neural Network (RNN)
Long Short Term Memory Cell (LSTM)

CAN BUS Input $(t)$

Hidden $(t-1)$

Input
Forget
Cell
Output

Memory $(t-1)$

CAN BUS Input $(t+1)$

Hidden $(t)$

Next Step

Memory $(t)$
Dense Layer

LSTM CELL

DENSE LAYER

OUTPUT

DENSE LAYER

OUTPUT

Dense Layer
Contextual Anomaly Detection Work Flow

- **Binary Pre-Processing**
- **Training (Titan X)**
  - Hyperparameters
  - Model HDF
- **Inference**
- **Errors**
  - Custom error metric
  - Input for Second Stage
Contextual Anomaly Detection Work Flow - 2nd Stage

Errors from 1st NNs → Training (Titan X) → Inference → Probability of an Attack

Hyperparameters
Model HDF
Training Architecture
Production Architecture

DATA SOURCE
CAN FLOW

FRAMEWORK
TensorRT

Probability of an Attack
NVIDIA DRIVE GPU

Model
Model Evaluation

Using Sensitivity & Specificity

True Positives (Anomalies) caught

True Negatives allowed
X axis: Deviation

Y axis: Frequency of errors

Median of Positives: 7.82

Median of Negatives: 0.04

Figure 3. Histogram - Error values output by the 2nd NN
Automotive Security  CAN Attacks  CAN Anomaly Detector  Results & Conclusions

Figure 4. Histogram - Error values output by the 2nd NN

X axis: Deviation

Y axis: Frequency of errors

- Sensitivity: 0.87
- Specificity: 0.94
Results Per Attack Type

Injection attacks
- Total: 37
- Detected: 32

Replay attacks
- Total: 42
- Detected: 37
Conclusion

A wall between Autonomous-Driving Software and the unsecured CAN-BUS

- Low inference computational cost
- Fast response
- Offline training

Future Work
THANK YOU

QUESTIONS?
References

[1] Ivan Studnia, Vincent Nicomette, Eric Alata, Yves Deswarte, Mohamed Kaâniche, Youssef Laarouchi
Survey on security threats and protection mechanisms in embedded automotive networks
Retrieved: https://hal.archives-ouvertes.fr/hal-01176042/document


A Car Hacking Experiment: When Connectivity meets Vulnerability

[4] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage
Comprehensive Experimental Analyses of Automotive Attack Surfaces


Anomaly Detection: A Survey

[8] Dhruba K. Bhattacharyya, Jugal Kumar Kalita
Network Anomaly Detection - A machine learning perspective
Images

Figure 1. Connections of a modern car
Figure 2. CAN network
Figure 3. Histogram - Error values output by the 2nd NN
Figure 4. Histogram - Error values output by the 2nd NN
Equations in a LSTM Cell – without the dense layer.

\[ f_t = \sigma_g(W_f x_t + U_fh_{t-1} + b_f) \]
\[ i_t = \sigma_g(W_i x_t + U_i h_{t-1} + b_i) \]
\[ o_t = \sigma_g(W_o x_t + U_o h_{t-1} + b_o) \]
\[ c_t = f_t \circ c_{t-1} + i_t \circ \sigma_c(W_c x_t + U_c h_{t-1} + b_c) \]
\[ h_t = o_t \circ \sigma_h(c_t) \]