Model-based Cybersecurity Engineering for Connected and Automated Vehicles

The FLOURISH Project

David Robles-Ramirez, Theo Tryfonas, Ponciano J. Escamilla-Ambrosio, Tesleem Fagade, Kalliopi Anastasopoulou, Andrea Tassi, Robert Piechocki
Connected and Automated Vehicles?
• FLOURISH is a multi-sector collaboration aiming to contribute to the delivery of advanced technologies for Connected Autonomous Vehicles (CAVs) in the UK. The Flourish project addresses two different but critical issues for CAVs:
  • Ensuring that wireless connectivity and cybersecurity of CAVs are considered by design; and
  • Optimising individuals’ experience when using the technology, with a particular focus on the needs of an ageing population.
Open Challenges

- Geographical addressing
- Risk analysis and management
- Data-centric Trust and Verification
- Anonymity, Privacy and Liability
- Secure localization
- Forwarding algorithms
- Delay and Reliability constraints
- Prioritization of data packets and congestion control
Attack Surfaces

Third party connected services

Brought-in connectivity

GPS

DSRC

4G

OEM connected services
Solutions for Security, Privacy and Trust (SPT)

- **Proactive security**: digitally signed messages with certificates (PKI), proprietary system design (protocols and HW), tamper resistant HW
- **Reactive security**: signature-based and anomaly-based intrusion detection
- **Anonymity and privacy**: linkability between *pseudonyms*
- **Secure localization**: tamper-proof GPS, etc
Public Key Infrastructure for C-ITS: an example

Generic C-ITS deployment model for generation and distribution of cryptographic material (EU C-ITS WG5-Annex 1)

- To support different jurisdictions or set of applications
- To increase efficiency
- To distribute certificates to C-ITS device
- To ensure the registration of the telematics device
- To grant the permission to operate
- To revocate certificates associated with specific telematics devices
Building blocks

Cooperative Service Module

Secure Credential Management System (PPKI-based)

Ultra-Secure Services (e.g., Human State Monitoring Service)

Human-Machine Interface

Event Data Recorder

bristol.ac.uk
Model-Based Systems Engineering

• Define CAV development lifecycle and IV&V strategy
  • Considering alignment with ISO/IEC 15288 “Systems Engineering Life Cycle Processes” and/or IEEE 1220 “Application and Management of the Systems Engineering Process”

• Develop generic CAV system architecture
  • Using MODAF/SysML embedded systems modelling
  • In line with MoD Standard 23-09 (GVA)
Model-Based Systems Engineering (cont’d)

• Assess CAV GVA against C-ITS platform 2016 report key requirements
  • Consider tailoring IV&V processes towards generic certification

• Develop an SoS view of CAV operation
  • System-of-systems (or network-of-networks) model
  • Suitable simulation (e.g. system dynamics, cybernetics/viable system, game theory etc. - tbc) to identify emergent behaviours, unintended consequences and potential risks
LIDAR scenario diagram
<table>
<thead>
<tr>
<th>Use case name: &lt;&lt;N&gt;&gt; authenticates</th>
<th>Use case name: &lt;&lt;N&gt;&gt; RSU Authenticates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Participating actor:</strong> CAV</td>
<td><strong>Participating actor:</strong> RSU</td>
</tr>
<tr>
<td><strong>Entry condition:</strong> An entry package is sent from RSU</td>
<td><strong>Entry condition:</strong> Receive data from the LIDAR</td>
</tr>
<tr>
<td>Events flow: The package is received. The CAVs actor runs the authentication element. The &lt;&lt;N&gt;&gt; element obtains the RSU credentials from the package. The &lt;&lt;N&gt;&gt; stereotype instance creates complementary information from de credentials. The &lt;&lt;N&gt;&gt; stereotype instance runs the authentication function. The &lt;&lt;N&gt;&gt; creates the assertion {True, False}. This use case extends the Receives RSU instructions use case and Receives data from RSU use case</td>
<td>Events flow: The package is received. The RSU actor runs the authentication element. The &lt;&lt;N&gt;&gt; element obtains the LIDAR credentials from the package. The &lt;&lt;N&gt;&gt; stereotype instance create complementary information from de credentials The &lt;&lt;N&gt;&gt; stereotype instance runs the authentication function. The &lt;&lt;N&gt;&gt; creates the assertion {True, False}. This use case extends the Read BBR data instructions use case.</td>
</tr>
<tr>
<td><strong>Exit condition:</strong> The CAVs authenticate the package received</td>
<td><strong>Exit condition:</strong> The RSU authenticates the package received.</td>
</tr>
</tbody>
</table>
Re-engineered architecture using IoTSecM
Model-based security

- Systematic documentation of security requirements
- Controls not just baselined, but selected based on need
  - which became clear to all
- Ability to simulate the logic of external security analysis techniques
  - here fault trees, could be others (or combination)
- Compatible with use cases implemented at other WPs
- Potentially standardizing the UK GVA for CAVs
• Thank you