Security Analysis of Automotive Architectures using Probabilistic Model Checking

Philipp Mundhenk, Sebastian Steinhorst, Martin Lukasiewycz, Suhaib A. Fahmy, Samarjit Chakraborty
philipp.mundhenk@tum-create.edu.sg
Examples for Automotive Security
Examples for Automotive Security


Examples for Automotive Security


Motivation

• **What** influence do component vulnerabilities have on the security of a specific function?

• Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

• **How much** effort should be invested in the consideration of security during implementation of specific components?
Motivating Example
Motivating Example
Motivating Example
Motivating Example
Motivating Example

\[ s = (s_{3G}, s_{CAN_1}, s_{m_{conf}}) \]
Motivating Example

\[ s = (s_{3G}, s_{\text{CAN}_1}, s_{m_{\text{conf}}}) \]

- **secure**
- **3G exploitable**
- **3G & m exploitable**
Motivating Example

\[ s = (s_{3G}, s_{CAN_1}, s_{m_{conf}}) \]

- **secure**
- **3G exploitable**
- **3G & m exploitable**

<table>
<thead>
<tr>
<th>Module</th>
<th>Interface</th>
<th>CVSS v2 Vector</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Park Assistant (PA)</td>
<td>CAN1/CAN2</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>12 (C)</td>
</tr>
<tr>
<td>Power Steering (PS)</td>
<td>CAN3</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Gateway (GW)</td>
<td>CAN1/CAN2</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Telematics (3G) 3G</td>
<td>CAN1/FR 3G</td>
<td>3.8 (AV:A/AC:H/Au:S)</td>
<td>52 (A)</td>
</tr>
<tr>
<td></td>
<td>3G</td>
<td>1.9 (AV:A/AC:H/Au:M)</td>
<td>52 (A)</td>
</tr>
<tr>
<td>FlexRay Bus Guardian (BG)</td>
<td>local</td>
<td>0.2 (AV:L/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
</tbody>
</table>

Message (m)
- **integrity**
  - unencrypted CMAC128: 1.2 (AV:A/AC:H/Au:S)
  - AES128: 1.2 (AV:A/AC:H/Au:S)

Message (m)
- **confidentiality**
  - unencrypted CMAC128: (instant)
  - AES128: (instant)
Motivating Example

\[ s = (s_{3G}, s_{CAN_1}, s_{m_{conf}}) \]

- **secure**
- **3G exploitable**
- **3G & m exploitable**

<table>
<thead>
<tr>
<th>Module</th>
<th>Interface</th>
<th>CVSS v2 Vector</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Park Assistant (PA)</td>
<td>CAN1/CAN2/FR</td>
<td>1.2 (AV:A;AC:H;Au:S)</td>
<td>12 (C)</td>
</tr>
<tr>
<td>Power Steering (PS)</td>
<td>CAN3</td>
<td>1.2 (AV:A;AC:H;Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Gateway (GW)</td>
<td>CAN1/CAN2/FR</td>
<td>1.2 (AV:A;AC:H;Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Telematics (3G)</td>
<td>CAN1/FR 3G</td>
<td>3.8 (AV:A;AC:L;Au:S)</td>
<td>52 (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.9 (AV:N;AC:H;Au:M)</td>
<td>52 (A)</td>
</tr>
<tr>
<td>FlexRay Bus Guardian (BG)</td>
<td>local</td>
<td>0.2 (AV:L;AC:H;Au:S)</td>
<td>4 (D)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message (m) integrity</th>
<th>unencrypted</th>
<th>$\infty$ (instant)</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CMAC128</td>
<td>1.2 (AV:A;AC:H;Au:S)</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>AES128</td>
<td>1.2 (AV:A;AC:H;Au:S)</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message (m) confidentiality</th>
<th>unencrypted</th>
<th>$\infty$ (instant)</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CMAC128</td>
<td>$\infty$ (instant)</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>AES128</td>
<td>1.2 (AV:A;AC:H;Au:S)</td>
<td>-</td>
</tr>
</tbody>
</table>
Motivating Example

\[ s = (s_{3G}, s_{CAN_1}, s_{m_{conf}}) \]

<table>
<thead>
<tr>
<th>Module</th>
<th>Interface</th>
<th>( \eta ) (CVSS v2 Vector)</th>
<th>( \varphi ) (ASIL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Park Assistant (PA)</td>
<td>CAN_1/CAN_2</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>12 (C)</td>
</tr>
<tr>
<td>Power Steering (PS)</td>
<td>CAN_1</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Gateway (GW)</td>
<td>CAN_1/CAN_2</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Telematics (3G)</td>
<td>CAN_1/FR</td>
<td>3.8 (AV:A/AC:L/Au:S)</td>
<td>52 (A)</td>
</tr>
<tr>
<td></td>
<td>CAN_1/3G</td>
<td>1.9 (AV:A/AC:H/Au:M)</td>
<td>52 (A)</td>
</tr>
<tr>
<td>FlexRay Bus Guardian (BG)</td>
<td>local</td>
<td>0.2 (AV:L/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Message (m) integrity</td>
<td></td>
<td>( \infty ) (instant)</td>
<td></td>
</tr>
<tr>
<td>unencrypted</td>
<td>CMAC128</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES128</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td></td>
</tr>
<tr>
<td>Message (m) confidentiality</td>
<td></td>
<td>( \infty ) (instant)</td>
<td></td>
</tr>
<tr>
<td>unencrypted</td>
<td>CMAC128</td>
<td>( \infty ) (instant)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES128</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td></td>
</tr>
</tbody>
</table>

secure

3G exploitable

3G & m exploitable
Motivating Example

\[ s = (s_{3G}, s_{CAN_1}, s_{m_{conf}}) \]

\[ s_0 = (0, 0, 0) \]

\[ s_1 = (1, 1, 0) \]

\[ s_2 = (1, 1, 1) \]

<table>
<thead>
<tr>
<th>Module</th>
<th>Interface</th>
<th>( \eta ) (CVSS v2 Vector)</th>
<th>( \varphi ) (ASIL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Park Assistant (PA)</td>
<td>CAN_1/CAN_2 /FR</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>12 (C)</td>
</tr>
<tr>
<td>Power Steering (PS)</td>
<td>CAN_2</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Gateway (GW)</td>
<td>CAN_1/CAN_2 /FR</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Telematics (3G)</td>
<td>CAN_1/FR</td>
<td>3.8 (AV:A/AC:L/Au:S)</td>
<td>52 (A)</td>
</tr>
<tr>
<td></td>
<td>CAN_1/3G</td>
<td>1.9 (AV:N/AC:H/Au:M)</td>
<td>52 (A)</td>
</tr>
<tr>
<td>FlexRay Bus Guardian (BG)</td>
<td>local</td>
<td>0.2 (AV:L/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Message (m)</td>
<td>unencrypted</td>
<td>( \infty ) (instant)</td>
<td>-</td>
</tr>
<tr>
<td>Message (m)</td>
<td>CMAC128</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>AES128</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>-</td>
</tr>
<tr>
<td>Message (m)</td>
<td>unencrypted</td>
<td>( \infty ) (instant)</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>CMAC128</td>
<td>( \infty ) (instant)</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>AES128</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>-</td>
</tr>
</tbody>
</table>
Motivating Example

\[ s = (s_{3G}, s_{CAN_1}, s_{m_{conf}}) \]

\[ s_0 = (0, 0, 0) \]

\[ s_1 = (1, 1, 0) \]

\[ s_2 = (1, 1, 1) \]

<table>
<thead>
<tr>
<th>Module</th>
<th>Interface</th>
<th>( \eta ) (CVSS v2 Vector)</th>
<th>( \varphi ) (ASIL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Park Assistant (PA)</td>
<td>CAN1/CAN2/FR</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>12 (C)</td>
</tr>
<tr>
<td>Power Steering (PS)</td>
<td>CAN3</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Gateway (GW)</td>
<td>CAN1/CAN2/FR</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Telematics (3G)</td>
<td>CAN1/FR</td>
<td>3.8 (AV:A/AC:L/Au:S)</td>
<td>52 (A)</td>
</tr>
<tr>
<td></td>
<td>3G</td>
<td>1.9 (AV:N/AC:H/Au:M)</td>
<td>52 (A)</td>
</tr>
<tr>
<td>FlexRay Bus Guardian (BG)</td>
<td>local</td>
<td>0.2 (AV:L/AC:H/Au:S)</td>
<td>4 (D)</td>
</tr>
<tr>
<td>Message (m) integrity</td>
<td>unencrypted</td>
<td>( \infty ) (instant)</td>
<td>-</td>
</tr>
<tr>
<td>validation</td>
<td>CMAC128</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>-</td>
</tr>
<tr>
<td>AES128</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Message (m) confidentiality</td>
<td>unencrypted</td>
<td>( \infty ) (instant)</td>
<td>-</td>
</tr>
<tr>
<td>validation</td>
<td>CMAC128</td>
<td>( \infty ) (instant)</td>
<td>-</td>
</tr>
<tr>
<td>AES128</td>
<td>1.2 (AV:A/AC:H/Au:S)</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Process

Architecture

Assessment

component security scores
Process

Architecture

Markov Model

Assessment

component security scores
Process

Architecture

Markov Model

Assessment

component security scores

Properties

\[ P =? \ [F \leq 1 \ x] \]
Process

Architecture

Markov Model

Assessment

component security scores

Properties

\( P =? [F \leq 1 \ x] \)

Probabilistic Model Checking

Results
Architecture Security Analysis

![Diagram showing different architectures with various components like CAN, GW, 3G, PA, and PS.](image)

- **a) Confidentiality (read)**
- **b) Integrity (create/modify)**
- **c) Availability (interrupt)**

![Bar charts for each architecture showing exploitability in one year](image)
Architecture Security Analysis

a) Confidentiality (read)
b) Integrity (create/modify)
c) Availability (interrupt)

Exploitability in one year (rate)

0 0.01 0.1

0 0.01 0.1

0 0.01 0.1

Architecture

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3

1 2 3
Summary

- Component influence can be quantified
- Comparison of architectures is enabled
- Effect of changes and security can be demonstrated
Summary

• **What** influence do component vulnerabilities have on the security of a specific function?
Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

  ➔ Component influence on system can be quantified
Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

  ➔ Component influence on system can be quantified

- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?
Summary

- **What** influence do component vulnerabilities have on the security of a specific function?
  - Component influence on system can be quantified
- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?
  - Comparison of architectures is enabled
Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

  ➔ Component influence on system can be quantified

- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

  ➔ Comparison of architectures is enabled

- **How much** effort should be invested in the consideration of security during implementation of specific components?
Summary

- **What** influence do component vulnerabilities have on the security of a specific function?

  ➔ Component influence on system can be quantified

- Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

  ➔ Comparison of architectures is enabled

- **How much** effort should be invested in the consideration of security during implementation of specific components?

  ➔ A quantifiable measure for security impact is given
Summary

• **What** influence do component vulnerabilities have on the security of a specific function?

  ➔ Component influence on system can be quantified

• Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

  ➔ Comparison of architectures is enabled

• **How much** effort should be invested in the consideration of security during implementation of specific components?

  ➔ A quantifiable measure for security impact is given

Future work:

• increase scalability to full vehicle network
Summary

• **What** influence do component vulnerabilities have on the security of a specific function?

  ➔ **Component influence on system can be quantified**

• Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? **Which**?

  ➔ **Comparison of architectures is enabled**

• **How much** effort should be invested in the consideration of security during implementation of specific components?

  ➔ **A quantifiable measure for security impact is given**

Future work:

• increase scalability to full vehicle network
• optimize security of architectures
Summary

• What influence do component vulnerabilities have on the security of a specific function?

  ➔ Component influence on system can be quantified

• Is a certain architecture design decision beneficial in comparison to an alternative in terms of security? Which?

  ➔ Comparison of architectures is enabled

• How much effort should be invested in the consideration of security during implementation of specific components?

  ➔ A quantifiable measure for security impact is given

Future work:

• increase scalability to full vehicle network
• optimize security of architectures
• synthesize new secure architectures
For more Information:

www.mundhenk.org