Security Risk Analysis for Automotive Systems

GENIVI All Member Meeting
Munich 16.5.2019
Dirk Leopold
Agenda

Overview itemis AG

Terms and Concepts
  - Risk and Risk Management
  - Privacy, Safety and Security

Methodology for Security Risk Analysis
Risk Analysis in the Automotive Domain
itemis AG
Short Facts

- founded 2003
- privately held – organic growth
- offices in Germany, France, Switzerland, Tunisia
- 225 employees + freelancers
- 22 Mio. Euros revenue
- 30% Automotive – 70% other
  (Insurance, Telecom, Logistics, Railway, Retail, …)
itemis AG
Methods and Tools

- Model Based Software Development
- Domain Specific Languages & Language Engineering
- Requirements Engineering & Traceability
- Productline Engineering & Variant Management
- Security & Safety

- GENIVI Associate Member
- Franca Project Lead
Security Analyst is a software tool supporting modular risk assessment of automotive systems

- based on various norms and best practice approaches (ISO 31000, ISO 27005, Common Criteria, STRIDE, TARA, ISO 21434...)
- result of cooperation between Fraunhofer AISEC (methods) itemis AG (tooling) and one German OEM since Q1 2016

Main functions supported within automotive security engineering

- system analysis and identification of security risks
- system design and definition of appropriate protective measures
R&D Project „SecForCARs“
Security For Connected, Automated Cars

- „Bundesministerium für Bildung und Forschung“ R&D project
- duration: 1st April 2018 – 31st March 2021
- allocated funding of 7.2 million Euros
- kick-off: 12th-13th April in Munich
- partners include industry, SME, research and academia
  - Infineon, Robert Bosch GmbH, ESCRYPRT
  - Itemis, Mixed Mode, Schutzwerk
  - Fraunhofer AISEC, Fraunhofer IEM
  - Universität Ulm, TU Braunschweig, TU München, Hochschule Karlsruhe

https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/sicherheit-fuer-vernetzte-autonome-fahrzeuge
Terms and Concepts
Risk Management

- Likelihood
- Negative Consequences
- Risk
- Risk not acceptable
- Risk reducing measures
- Acceptable Risk

Risk Management
ISO 26262
Hazard Analysis and Risk Assessment

Risk = (expected loss in case of accident) \times (probability of accident occurring)

or

Risk = \text{Severity} \times (\text{Exposure} \times \text{Controllability})

Automotive Safety Integrity Levels (ASIL)

- define the degree of rigor applied in the assurance of the safety requirements
- levels A – D
- QM level (quality management without specific safety aspect)
Terms and Concepts
Privacy, Security and Safety

Privacy

Safety

Security

?
Terms and Concepts
Privacy, Security and Safety

Privacy

Safety

Security

...
“Security by Design“
Security Risk Analysis in the Development Life Cycle

- Initiation
- Requirements
- Design
- Specification
- Implementation
- Approval
- System Testing
- Component Testing
- Operation...
Modular Risk Assessment (MoRA) Methodology

- Model the Target of Evaluation
- Determine Protection Needs
- Analyze Threats
- Analyze Risks

Security Risk Analysis

Domain Experts...

- Model the Target of Evaluation
- Determine Protection Needs
- Analyze Threats
- Analyze Risks
Security Risk Analysis

… and Security Experts have to work together!

Model the Target of Evaluation

Determine Protection Needs

Analyze Threats

Analyze Risks
Modular Risk Assessment (MoRA) Core Activities

- Model the Target of Evaluation
- Determine Protection Needs
- Analyze Threats
- Analyze Risks

- Damage Level
- Estimated likelihood level
- Risk level
Modular Risk Assessment (MoRA) Results

Model the Target of Evaluation
- Functions
- Data
- Components
- Connections
- Assumptions

Determine Protection Needs
- Assets
- Security Attributes
- Security Goals

Analyze Threats
- Threats
- Controls

Analyze Risks
- Estimated likelihood level
- Damage Level
- Risk level

Results
Modular Risk Assessment (MoRA)

Example Configuration

- Model the Target of Evaluation
  - Functions
  - Data
  - Components
  - Assumptions

- Determine Protection Needs
  - Assets
  - Security Attributes
  - Security Goals
  - Damage Criteria

- Analyze Threats
  - Threats
  - Threat Catalog

- Controls
  - Control Catalog

- Analyze Risks
  - Estimated likelihood level
  - Damage Level
  - Risk level
Negative Consequences
Damage Potential (DP)

- the damage potential (DP) describes the potential damage resulting from the loss of a defined security goal
- severity levels of damages have to be defined and documented for each damage class (e.g. very high, high, moderate, low, very low)
- qualitative and quantitative damage properties have associated with severity levels (e.g. financial loss exceeding 1 million Euros -> very high)
- the rules for the aggregation of damage potentials across damage classes have to be defined and documented (e.g. mathematical weighted model)

\[
\text{aggregation formulas default} = \text{MAX}
\]

\[
\begin{align*}
\text{MAX} & : \text{max(} \text{Monetary}_\text{max}, \text{Potential harm}_\text{max}, \text{Privacy}_\text{max}, \text{Functionality}_\text{max} \text{)} \\
\text{ACC} & : \text{let } [\text{if } v \rightarrow \text{very high then } v \text{ else } v + 1] \\
& \quad \text{with } v = \text{MAX} \\
\text{DIS} & : \text{let } [\text{if } v \rightarrow \text{very low then } v \text{ else } v - 1] \\
& \quad \text{with } v = \text{MAX}
\end{align*}
\]
Likelihood Determination

Attack Potential

- no statistical data (e.g. MTBF) applicable in the realm of security!!
- risk factors required for the calculation of RAP
  - expertise (e.g. layman, proficient, expert, multiple experts)
  - knowledge about SUD (e.g. public, restricted, sensitive, critical)
  - equipment (e.g. standard, specialized, bespoke, multiple bespoke)
  - required time (e.g. minutes, hours, days, years)
- likelihood determined by the required capabilities of the attacker to perform a successful attack = required attack potential (RAP)
Risk Analysis
Determining the Security Risk

- combining damage potentials (severity) & attack potentials (likelihood)

<table>
<thead>
<tr>
<th>Damage potentials</th>
<th>Risks Table</th>
<th>Required attack potentials</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Beyond high</td>
<td>High</td>
</tr>
<tr>
<td>Very low</td>
<td>Low risk</td>
<td>Low risk</td>
</tr>
<tr>
<td>Low</td>
<td>Low risk</td>
<td>Moderate risk</td>
</tr>
<tr>
<td>Moderate</td>
<td>Low risk</td>
<td>Moderate risk</td>
</tr>
<tr>
<td>High</td>
<td>Moderate risk</td>
<td>High risk</td>
</tr>
<tr>
<td>Very high</td>
<td>Moderate risk</td>
<td>Very high risk</td>
</tr>
</tbody>
</table>

- calculation of resulting risk for each Security Goal / asset in matrix

- creation of risk analysis reports
Risk Analysis in the Automotive Domain

Special Challenges

– Highly distributed system development (OEM, Tier 1, Tier 2, ...)
– Impact of (semi-)autonomous vehicles
– Influence of changes during the life cycle
  – Periodical reevaluation of risk levels
  – Continuous update and tracking of system dependencies
  – Influence of system updates on security and safety
    – Remote software updates?
    – Status of certifications?
    – Selective deactivation of functions?
– Automotive Responsible Disclosure (ARD)
– ...

Remote software updates?
Status of certifications?
Selective deactivation of functions?
THANK YOU FOR YOUR ATTENTION!

Contact:
Dirk Leopold
leopold@itemis.de