Enabling Efficient Common Criteria Security Evaluation for Connected Vehicles

Angelos Stamou\textsuperscript{1}, Panagiotis Pantazopoulos\textsuperscript{1}, Sammy Haddad\textsuperscript{2} and Angelos Amditis\textsuperscript{1}

\textsuperscript{1} Institute of Communication and Computer Systems, Athens, Greece, 
Email angelos.stamou@iccs.gr ppantaz@iccs.gr, a.amditis@iccs.gr

\textsuperscript{2} Oppida, Montigny-le-Bretonneux, France, 
Email Sammy.haddad@oppida.gr
The problem of security assurance

Background and approaches to security assurance evaluation
  ◦ Under-explored challenges

Introducing the Assurance Framework Toolkit (AFT)
  ◦ Software design
  ◦ AFT implementation choices

Empirical evaluation of SAT

Take-home results
The challenge of security assurance (evaluation)

- A “post-design/implementation” question
- establish trust that a system satisfies its intended cyber-security behavior or
- the degree of confidence that the security requirements of an IT system are satisfied

parallel lines with software testing

a) What is to be evaluated?
b) Which evaluation activities to follow?
c) Which entity performs the evaluation activities?
The challenge of security assurance (evaluation)

- Spectrum of the solutions efficiency

<table>
<thead>
<tr>
<th>Assurance</th>
<th>do nothing</th>
<th>Evaluation tasks</th>
<th>formal proof</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>zero</td>
<td></td>
<td>100%</td>
</tr>
</tbody>
</table>

- formal proofs are increasingly-difficult if not infeasible, as complexity increases
- the question is what happens (practically) in-between the extreme values

Proofs that system behaviour meets a desirable property (e.g., show that no attack strategy in a class of strategies will cause a system to misbehave)

a trade-off between efficiency and cost
Approaches to security assurance (evaluation)

- **Vulnerability tests**
  - a quick perimeter definition
  - experts run tests of their choice during a predefined time-period
  - depends on the expertise of the tester
  - comparison between tests is tricky

- **Conformity checks**
  - validates a system’s compliance to a specific reference
  - fastest and cheapest evaluation scheme
  - a reference conformity list has to be kept up to date (occasionally cumbersome)
  - anything not conformant to a subset of this list cannot be validated

low to medium assurance level (in the product’s security)

medium levels of assurance
Approaches to security assurance (evaluation)

- Get someone else to do the job and leave me alone!

- **Assurance framework(s)**
  - most complete and exhaustive one
  - requires a precise description of the evaluation objectives and requirements to prescribe dedicated and extensive evaluation activities
  - comes at the expense of considerable cost and time-to-complete
  - requires rare and expensive accredited evaluators

- Common Criteria
- ISO/SAE 21434
- FIPS 140–2
- Carsem¹
- SAFERtec²

(up to) the highest level of assurance


Common Criteria (ISO/IEC 1540) for connected vehicles

- **Target of Evaluation (ToE):** the system to be evaluated
- **Protection Profile (PP):** Generic yet systematic definition of evaluation tasks for a generic type of product
- **Security Target (ST):** the document specifying TOE and the evaluation tasks
- **The Security Functional Requirements (SFR):** the specification of the security functions that the TOE must implement
- **Assurance Levels:** EAL 1 to EAL7, each of them increasing the level of requirements and evaluation tasks to be undertaken on the TOE

The first version of the CC dates back to 1994

Inspired by previous assurance evaluation initiatives: TCSEC (US DoD), ITSEC (EU standard), the Canadian CTCPEC4

Last version standardized in 2009, 5 revisions ever since

Highest assurance is needed as safety is involved

Costs need to be reduced

Relevant SW tools are scarce!
AFT toolkit to lower costs for CC-based approaches

- **Software design**
  - Cross-platform Single Page application
    - 2 user roles defined
    - Realizes data structures as entities and their relations

- **Requirements met**
  - Adaptability
  - Modularity
  - Extensibility
  - Interoperability

**Front end**
- SPA: first delivers a web-page plus the associated functionality
- Updates with small asynchronous requests to the server

**Back end**
- ASP.NET framework
- Entity Framework core: object-relational mapping library

July 26 – 28 2021  IEEE Cyber Security and Resilience Conference
AFT toolkit to lower costs for CC-based approaches

- **Implementation choices**
  - Server component is the more logic-heavy part
  - Written in C# and run on the .Net Core framework

- **Basic functionality**
  - Building blocks to support the Security Target compilation
  - Graphical tool to support the evaluation of the product design and its interfaces specifications

- **Deployment chain**
  - The Kestrel Web server and the AFT application are the main executables
  - The Server communicates with a PostgreSQL database
AFT relevance to the connected vehicles

- Populated with vehicular data (i.e., threats, objectives etc.)
  - Provided by a dedicated modular Protection Profile and the reference ETSI TVRA (TR 102 893) report
  - User selects the appropriate data or adds new

- AFT data shaped by our real-world V2I testbed experimentation
  - AFT V2I functional requirements have been earlier tested

- Special functionality added to guide the automotive product developer in the compilation of CC evaluation inputs
  - Pointers to external technical documents, relevant standards


Empirical evaluation of the AFT effectiveness

- Actual experimental AFT evaluation would call for numerous applications on real-world products taking significant time and funds

<table>
<thead>
<tr>
<th>Assurance component</th>
<th>Task Input</th>
<th>Regular (i.e., unassisted) CC efforts</th>
<th>Using the AFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADV (ADV_FSP)</td>
<td>Documents describing the ToE interfaces and association with SFRs</td>
<td><strong>Initial documentation</strong>: 7 days</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Extra evaluation efforts</strong>: 2 days</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Extra efforts per evaluation task cycle</strong>: 0.5 days</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Error summaries for each ToE interface</td>
<td><strong>Documents evaluation</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Iteration 1: 2 days</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Iteration 2: 2 days</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Higher iterations: 0.5 days</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Cost estimation</strong>: 3 working days</td>
<td></td>
</tr>
</tbody>
</table>

Evaluates the functional description of a product at the interface-level

AFT helps the developer to
- automatically identify the mandatory evaluation inputs
- provide the justifications needed (e.g., SFRs related to each interface)
‘Take-home’ remarks

- The connected vehicles paradigm poses increasingly high security assurance requirements

- Only approaches that rely on the most credible security assurance framework (Common Criteria standard) can meet the requirements

- The address the cost limitation of the (CC-based) assurance frameworks and account-for automotive attributes, AFT online toolkit has been introduced to assist the process and reduce costs

Provides support for efficient execution of evaluation classes

Incorporates automotive data, requirements and experimentation results

- ASE (Security Target evaluation)
- ADV (Architectural design evaluation)
- ATE (Functional and independent test evaluation)

- Modular Protection Profile
- Results from real-world testing of requirements
Thank you!
Looking forward to your questions

Panagiotis Pantazopoulos
Institute of Communications and Computer Systems
Athens, Greece
ppantaz@iccs.gr

Code can be found at:
https://isense-gitlab.iccs.gr/safertec/aft

A 3.48’ mins video demonstrator in deliverable D6.3 at:
https://www.safertec-project.eu/publications/public-deliverables/

“This work was part of the SAFERtec project which was funded by the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319”