



Enabling Efficient Common Criteria Security Evaluation for Connected Vehicles

Angelos Stamou¹, **Panagiotis Pantazopoulos¹**,
Sammy Haddad² and Angelos Amditis¹

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

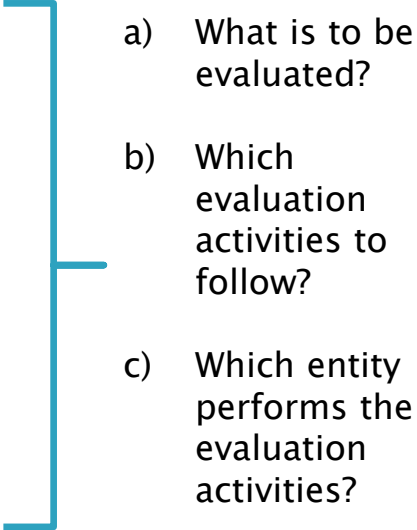
2 Oppida, Montigny-le-Bretonneux, France,
Email Sammy.haddad@oppida.gr

Presentation breakdown

- ▶ 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



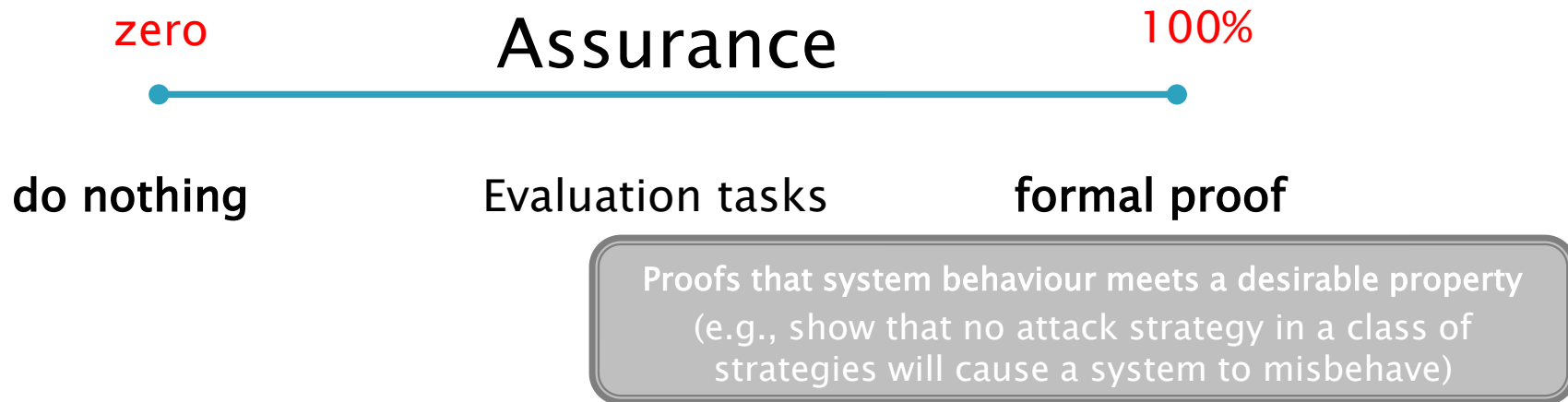
The challenge of security assurance (evaluation)

- ▶ 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
- 
- a) What is to be evaluated?
 - b) Which evaluation activities to follow?
 - c) Which entity performs the evaluation activities?

parallel lines with software testing

The challenge of security assurance (evaluation)

▶ Spectrum of the solutions efficiency



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



a trade-off between efficiency and cost

Approaches to security assurance (evaluation)

▶ **Vulnerability tests**

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

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

▶ **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

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

[1] S. Haddad, A. Boulanger, P. Cincilla, and B. Lonc, CARSEM: A Cooperative Autonomous Road-vehicles Security Evaluation Methodology. In 25th ITS World Congress, September 2018, Denmark.

[2] P. Pantazopoulos, S. Haddad, C. Lambrinouidakis, C. Kalloniatis, K. Maliatsos, A. Kanatas, A. Váradi, M. Gay, A. Amditis, "Towards a Security Assurance Framework for Connected Vehicles", The 5th IEEE WoWMoM Workshop on Smart Vehicles, Chania, Greece, June 12, 2018.

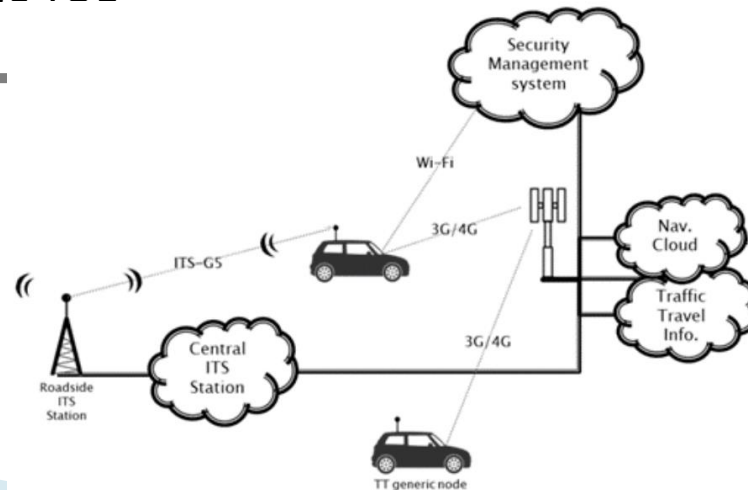
Common Criteria (ISO/IEC 1540) for connected vehicles

- ▶ 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



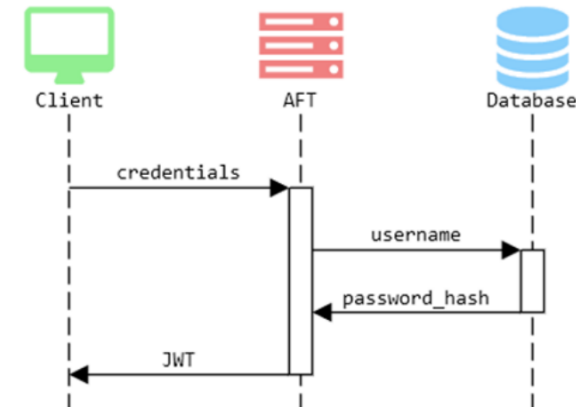
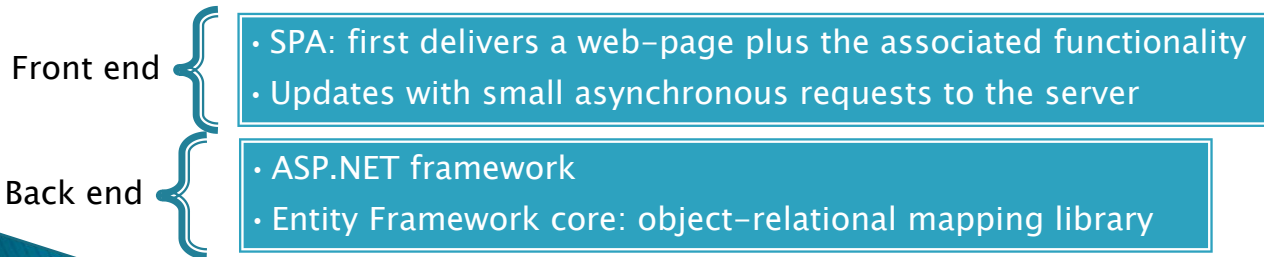
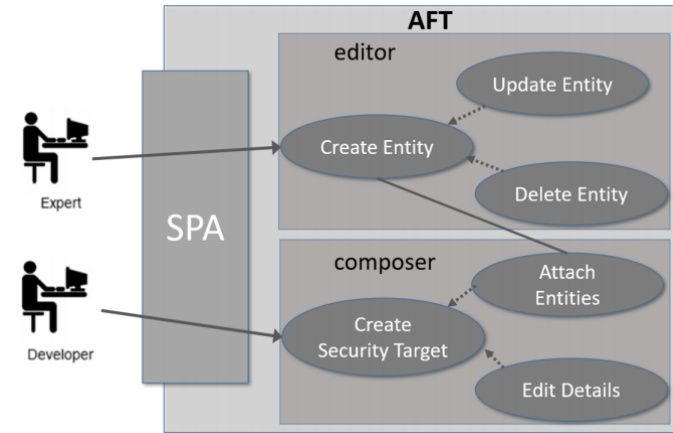
Highest assurance is needed as safety is involved

Costs need to be reduced

Relevant SW tools are scarce!

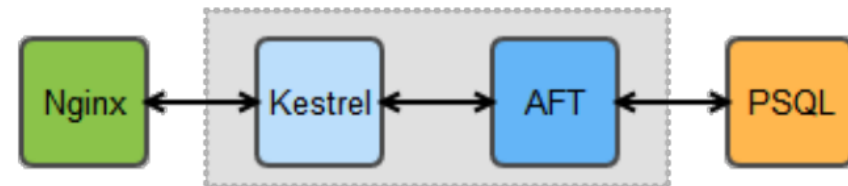
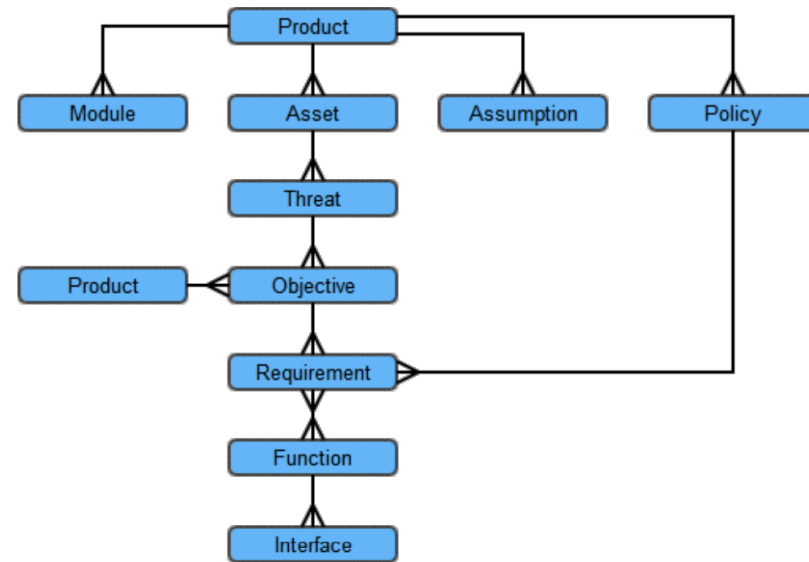
AFT toolkit to lower costs for CC-based approaches

- ▶ 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



AFT toolkit to lower costs for CC-based approaches

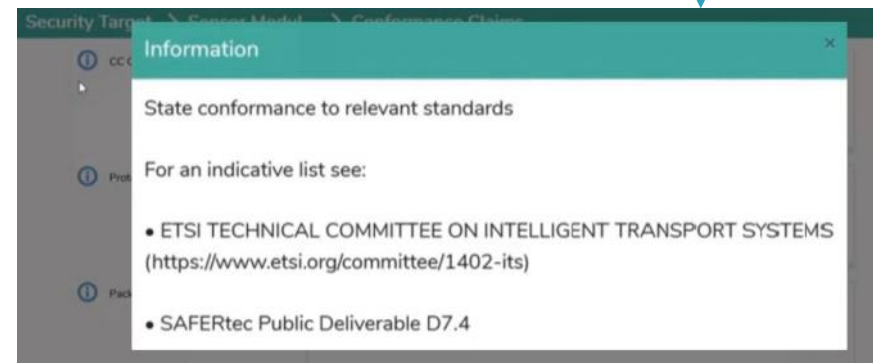
- ▶ Implementation choices
 - Server component is the more logic-heavy part
 - Written in C# and run on the .Net Core framework
- ▶ Basic functionality
 - Building blocks to support the Security Target compilation
 - Graphical tool to support the evaluation of the product design and its interfaces specifications
- ▶ 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**¹ 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 experimentation²
 - 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

[1] K. Maliatsos et al., “Standardizing Security Evaluation Criteria for Connected Vehicles: A Modular Protection Profile”, IEEE Conference on Standards for Communications and Networking, Granada, Spain, October 2019
[2] A. Marchetto, et al., “CVS: Design, Implementation, Validation and Implications of a Real-world V2I Prototype Testbed”, 91st IEEE Vehicular Technology Conference (VTC2020), Belgium, May 2020.



Empirical evaluation of the AFT effectiveness

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

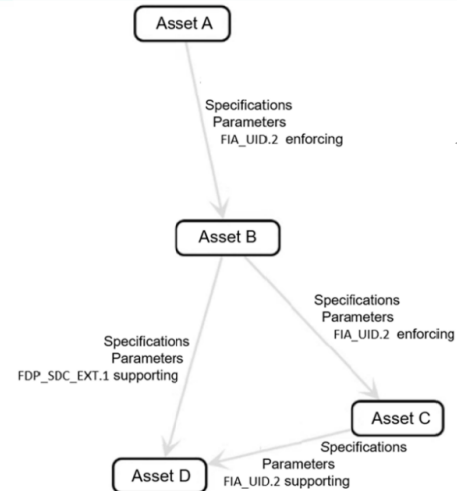
Assurance component	Task Input	Regular (<i>i.e.</i> , unassisted) CC efforts	Using the AFT
ADV (ADV_FSP)	<p>Documents describing the ToE interfaces and association with SFRs</p> <p>Error summaries for each ToE interface</p>	<p>Initial documentation: 7 days</p> <p>Extra evaluation efforts: 2 days</p> <p>Extra efforts per evaluation task cycle: 0,5 days</p> <p>Documents evaluation</p> <p>Iteration 1: 2 days</p> <p>Iteration 2: 2 days</p> <p>Higher iterations: 0.5 days</p> <p>Cost estimation: 3 working days</p>	<p>Estimated time needed for extra evaluation to be <i>reduced up to 50%</i> as AFT provides graphical tools & templates</p> <p>Better quality of inputs (more structured and harmonized) to <i>reduce evaluation time up to 30%</i></p>

ADV (ADV_FSP)

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)

The screenshot shows the SAFERtec AFT interface. The top bar is green with the text 'SAFERtec AFT > ADV'. Below it, there are two main sections: 'Assets' and 'Security Function Interface'. The 'Assets' section has three rows, each with a dropdown menu for 'Select Asset to edit/delete' and a corresponding action button (+, edit, or -). The 'Security Function Interface' section has a 'Source for new Interface' dropdown, a 'Target for new Interface' dropdown, a text input for 'New Interface name', and two more dropdowns for 'Select TSFI to edit/delete'.



'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

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/>

Thank you!

Looking forward to your questions

Panagiotis Pantazopoulos

Institute of Communications and Computer Systems

Athens, Greece

ppantaz@iccs.gr



"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"