Security modeling in automotive industry.

Background
The in-vehicle network of a modern car is consisted of approximately more than 100 Electronic Control Units (ECU) that control different parts of a car such as engine, doors, airbags and infotainment system. These ECUs connect to each other over multiple sub-networks and gateways using different communication technologies such as CAN, LIN, MOST, and FlexRay. The in-vehicle networks are prone to network attacks mainly due to the lack of procedures for verifying the authenticity and the integrity of the communications.

Development of electronics for vehicles is a highly distributed effort, involving individuals from many different organizations using different methods. To introduce security and privacy as an integral part of the design work, there is a need for a consistent way to model these attributes. Increased precision and traceability between analysis, requirements, tests and field data would decrease risks and could decrease lead times. Broad deployment of modeling techniques in the research and design organization involves significant obstacles like education, time available for extra work and possible licenses. Before such deployment is possible, mature modeling techniques need to be developed taking in account for the constraints from the state of the practice in the design work today.

HoliSec (Holistic Approach to Improve Data Security) is a 3-year Swedish research project started in April 2016. The objective of the project is to holistically address security concerns in the complete automotive chain from concept, design, development, integration, testing, verification & validation and operational phases. Results of the project are expected to improve the overall safety, uptime and quality of road vehicles. This thesis project will contribute to the overall objectives of the HoliSec project by investigating the constraints and requirements of modelling by working with design models provided by Volvo Cars.

Requirements
- The candidate’s MSc. programme should preferably be Software Engineering, Computer Science, Computer Engineering, IT and Electrical Engineering. Candidates with equivalent background from other programmes will also be considered.
- The candidates should be in their final year of MSc. Studies.
- Several subject areas such as computer and network/IT security, modelling languages, software engineering, software verification and testing, embedded and real-time systems are relevant in the context of this thesis work. Knowledge in one or several of these areas will be considered favorably.
- Good skills in English as the work environment is international.

Description of thesis work
The goal of this thesis is to propose appropriate modeling techniques and tools that can help improving security design work at Volvo cars. The scientific contribution includes evaluating state of
the art security modeling to state of the practice in automotive industry and increase knowledge in how to increase traceability between security attributes to security analysis.

The work consists of the following steps:

1. Survey state of the art in security modeling
2. Survey state of the practice of modeling at Volvo cars
3. Selection of candidate modeling techniques
4. Apply the candidate techniques to enrich existing models
5. Compare and analyze the results

The work consists in adding security attributes to a few existing models to get a practical connection to the design work at Volvo cars. The work includes tracing the model to a threat model and adding countermeasures.

The students will be compensated according to Volvo Cars policy upon successful completion of the thesis work.

Questions

1. What type of models are suitable (formal (math), semi formal (UML), informal (text)) taking into account the models currently available from design teams?
2. What is the maturity level (tools available, competence required, competence available) of different security modelling techniques and what is the gap to application at Volvo cars?

**Thesis level:** Masters

**Language:** English

**Starting date:** January 2017 (or earlier upon agreement)

**Number of students:** The thesis is suitable for two students working in collaboration

**Academic Tutor:** Dr. Riccardo Scandariato, Associate professor in the Software Engineering division, Computer Science and Engineering, Chalmers.

**Industrial Tutor:** Henrik Broberg, Henrik.broberg@volvocars.com, +46 31 59 66 07