Program Automotive Security and Privacy

FFI Board Funded Program

2015-10-02

Abstract

This document describes the FFI board funded program "**Automotive Security and Privacy**". This document is prepared by the working group that consists of representatives from Swedish automotive industry (Volvo AB, Volvo Cars, Scania) and academia as well as research institutes (SP, Viktoria Swedish ICT, Chalmers).

Automotive industry is experiencing new safety and security risks because of a paradigm shift towards connected and autonomous vehicles coupled with increasing reliance on electrical and/or electronic (E/E) systems. In this regard, this program envisages establishing that security and privacy are assumed-to-be quality features of vehicles. The mission is not only to improve product quality and safety but also to contribute to sustainable transport systems and society by adopting "security-by-design" and "privacy-by-design" approaches.

The program spans from traditionally "isolated" vehicles to increasingly connected and autonomous vehicles. This program supports research activities that aim at developing concepts, methods, tools, and processes by adopting a holistic approach to improve security. This program strongly encourages collaboration across OEMs, industrial partners, academia, research institutes and other relevant stakeholders. Research projects with strong industrial involvement and high potential of developing technologies with higher Technology Readiness Level (TRL) can potentially address needs of the Swedish automotive industry, making Swedish products more attractive on future competitive markets.

The program duration is four years (2016 – 2019) with a total budget of 80 MSEK, including public funding of 40 MSEK and industrial contributions of 40 MSEK. Calls, evaluation of applications and following up of the results of this program will be taken care of by FFI normal procedures.

Background

The automotive industry is experiencing a paradigm shift towards autonomous and connected vehicles. Consequently, vehicles are becoming increasingly personalized and part of the Internet of Things (IoT). Simultaneously, the usage of electronics and the importance of electrical and/or electronic (E/E) systems (see Figure 1) are expected to continue to increase in the coming years, resulting in new risks.

Management of safety risks caused by malfunctioning behavior of E/E systems is standardized and relatively well-established in the automotive industry. On the other hand, security risks caused by unauthorized and malicious manipulations of the E/E systems have only recently gained attention in the automotive industry. This aligns poorly with the strong focus on safety. It has been shown that it was possible to mount attacks that can jeopardize safety of drivers, passengers and other road users[1,2] and demonstration of vulnerabilities has triggered the recalls of vehicles[3].

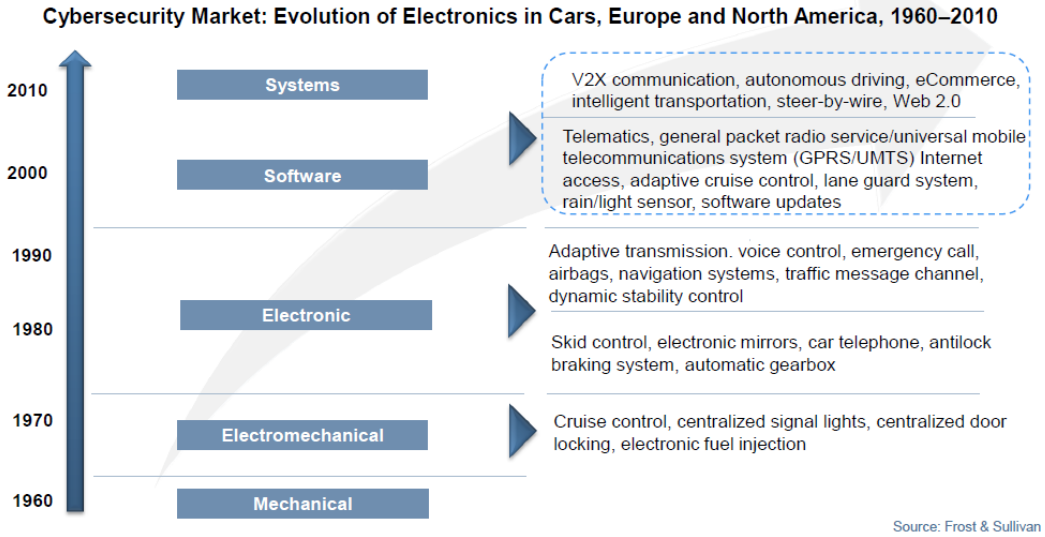

Figure 1: Evolution of electronics in cars[4].

Moreover, market research predicts that 85% of all cars will be connected to the Internet by 2020 and cyber-crimes will be a real threat to the industry[4]. This clearly indicates that research activities need to be performed in order to systematically and effectively deal with security and privacy risks to improve the overall quality and safety of vehicles.

Program objectives

Vision: Establish that security and privacy are assumed-to-be quality features of vehicles.

Mission: The mission is to improve product quality and safety as well as to contribute to sustainable transport systems and society by adopting “security-by-design” and “privacy-by-design” approaches. Thus this program contributes significantly to the FFI goals of reducing the environmental impact of transport, reducing the number killed and injured in traffic, and strengthening international competitiveness.

[1] K. Koscher et al, “Experimental security analysis of a modern automobile.”, IEEE Symposium on Security and Privacy (SP), pages 447–462, 2010.

[2] Charlie Miller and Chris Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle”, August 10, 2015.

[3] Online, http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/, Last accessed: August 12, 2015.

[4] N. Tare. NE30-01: Cybersecurity in the automotive industry. Frost & Sullivan, October 2014.

Goals: Goals of the program are defined as follows:

- Understand security challenges and associated safety, privacy, financial, and operational risks.
- Develop common best practices, guidelines and policies for the Swedish vehicle industry.
- Investigate existing security-relevant technologies from other industrial domains, and if possible adapt them in the context of the automotive industry. If required, investigate and develop new automotive-specific security technologies.
- Investigate, develop, and integrate processes to ensure security.

Program description

This program takes a holistic approach to address security and privacy challenges in the context of the automotive industry. In line with traditional methodologies and processes, security and privacy should not be treated as an isolated technology and an afterthought in the original system development process. Rather, security and privacy need to be built-in to the process from the beginning when designing a system. Vehicle features, applications, security technologies and communication services need to be developed and fine-tuned together to offer the required functionality to deliver the expected service in time to be useful. This program supports research activities that aim at developing concepts, methods, tools, and mechanisms to adopt a holistic approach to ensure end-to-end security.

However, adding security to legacy systems as well as incorporating security features to new designs requires work on many different levels; from concept phase, product development phase to operational and decommissioning phases. Also, the system must be able to deal with not only today's threats but also with new threats emerging in the coming 10 to 20 years. There is a need to detect and deal with security problems in a timely manner. It is essential to have requirements, policies and guidelines for development and security testing, validation and verification (V&V). Possibly, standards need to be developed to deal with both internal devices and third-party products including integration of consumer devices.

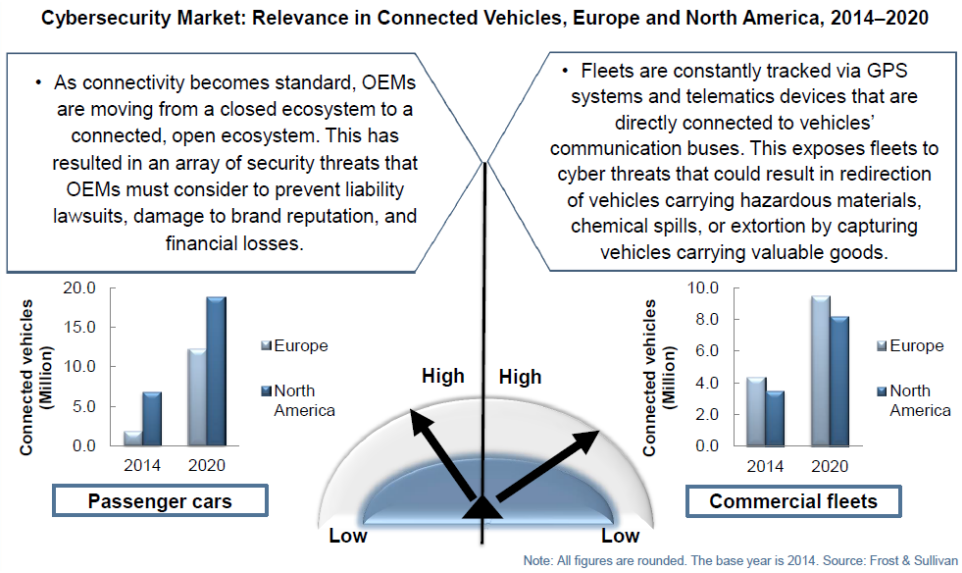

Figure 2: Security in the context of connected vehicles[4].

Integration and synthesis of existing, established methods and security mechanisms from other industries (IT, avionics, software engineering and industrial control systems) are strongly encouraged where such possibilities exist. Automotive security is rapidly converging with traditional information technology (IT)

security[5]. Alongside new challenges, this phenomenon opens up new opportunities for the automotive industry to tackle security concerns by taking advantage of well-established IT security technologies. Furthermore, it is very important to consider alignment with and leveraging on existing technologies and processes from functional safety domain within the automotive industry.

The automotive industry is quite familiar with various safety standards and relevant requirements, methods, tools and processes. Competence and expert-level knowledge have already been built in this area. This can be utilized to develop a critical mass of competence and knowledge in the security area if the existing methodologies and processes can be adapted alongside new approaches to handle security concerns. As a result, a cross-disciplinary approach of handling security and safety risks by using a common framework needs to be investigated, developed and adopted.

Standards and collaborative efforts are emerging globally. This program focuses on helping the Swedish industry to excel in efficient and effective adoption, adaption, and implementation of available technologies and solutions to minimize security risks. At the same time, the Swedish automotive industry needs to leverage international initiatives by exploiting existing research results as well as body of knowledge, participating in on-going initiatives and attending external events. This program aims to support such activities.

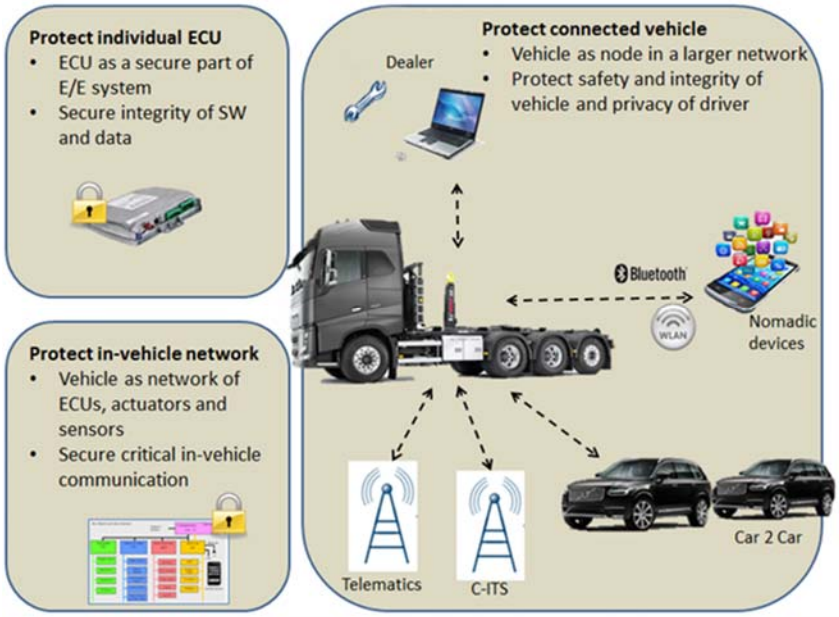

Figure 3: Different abstraction levels and scope of automotive security[6].

Program scope

The program spans from traditionally "isolated" vehicles to increasingly connected and autonomous vehicles (see Figure 3). The overall program is divided into four different sub-areas:

I. Security Engineering,
II. Automation, Connected and Autonomous Vehicles,
III. Process and Technology Management, and

[5] N. Tare. NE30-01: Cybersecurity in the automotive industry. Frost & Sullivan, October 2014.
[6] Inspired by a presentation by Dr. Klaus Dietrich (Robert Bosch GmbH) at ESCAR 2012 in Germany.

IV. Exploitation, Dissemination and Standardization.

A suggested list of research topics within each subarea is presented in Figure 4. A project may cover research activities encompassing one or more of the proposed sub-areas.

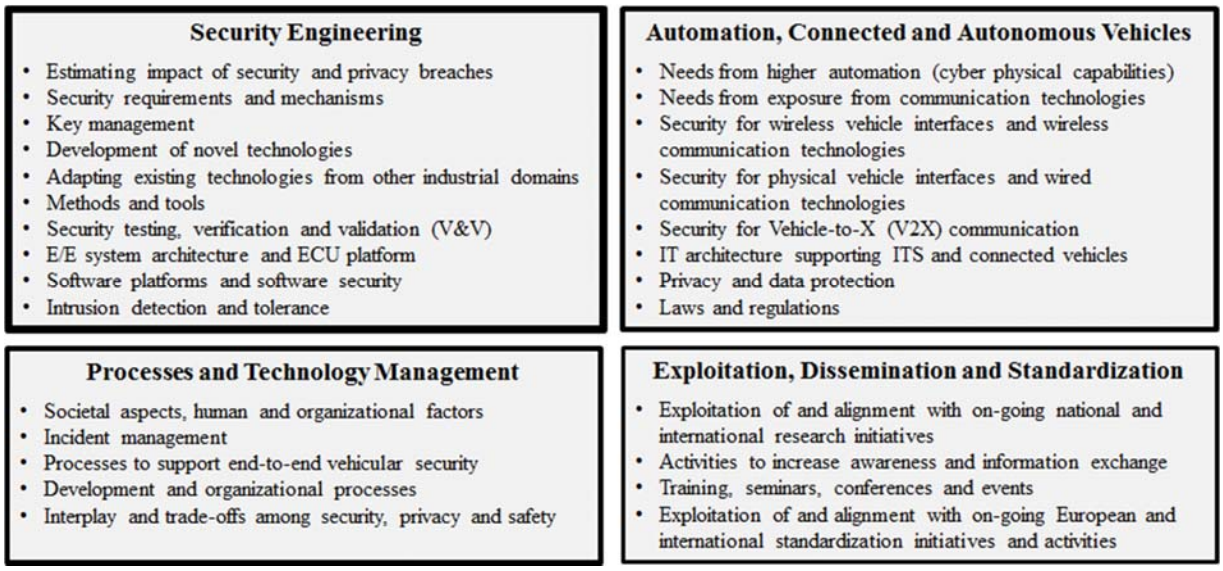

Figure 4: Suggested scope and list of topics to be covered within each sub-area.

This program strongly encourages collaboration across OEMs, industrial partners, academia, research institutes and other relevant stakeholders. The program supports both foundational and applied research, from Technology Readiness Level 1, TRL 1, (Basic Technology Research) to TRL 7 (System prototype demonstration in an operational environment). However, this program emphasizes research activities that can potentially lead to technologies with higher TRL not only to contribute to the advancement of state-of-the-art and state-of-the-practice but also to achieve the program goals.

Expected results

Collaboration across OEMs, industrial partners, academia and research institutes along with other relevant stakeholders is expected to be established as a result of this program. This along with dissemination and exploitation of research results would allow for development of a critical mass of awareness, knowledge and competence in Sweden and minimization of vehicle related security risks.

Research projects with strong industrial involvement and high potential of developing technologies with higher technology readiness level (TRL) can assist in addressing potential future needs of the Swedish automotive industry. Furthermore, the developed technologies will have the potential of assuring that social and environmental sustainability is maintained, making Swedish products more attractive on future competitive markets.

Program budget and application process

The program duration is four years (2016 – 2019) with a total budget of 80 MSEK, including public funding of 40 MSEK and industrial contributions of 40 MSEK.

Calls, evaluation of applications and following up of the results of this program will be taken care of by FFI normal procedures. Exploitation, dissemination and standardization initiatives and activities is planned to be coordinated across the projects within the program.