Title of thesis work

Evaluating security concerns of software structure on high performance in-vehicle computational nodes

Background of thesis work

There is a paradigm shift in automotive industry towards autonomous and connected vehicles. Vehicles are getting increasingly connected and becoming an integrated part of ecosystem around Internet of Things. Until most recent years, cyber security issues were mainly of concern for other industries, for example, defence, finance, mobile telecom, IT and other internet based industries. A quick check on any search site reveals the increasing incidents around cyber-crimes with vehicles. Security is going to be a major threat for automotive industry.

Security is often treated as isolated technology or an afterthought in the system. It needs to be addressed very early in the concept, design & development phase. The traditional approach is automotive industry when developing in-vehicle software & electronic architecture is to provide increasing functionalities for end customers while balancing constraints like cost, scalability, maintainability, manufacturability and so on while not compromising safety and quality. However, security is an often neglected area until recently when its impact on safety, quality and uptime is getting obvious due to different hacking incidents around the world.

The state-of-the-art vehicle architecture consists of number of electronic control units (ECU) interconnected by different bus communication system typically CAN. With major vendors now offering more powerful processor chips combined with goal to reduce cost, weight and maintenance, the trend is now towards centralization of functionality by reduction in number of ECUs. Due to this there has been increased interest to integrate functionalities into few powerful ECUs called computational nodes. But the physical connection to most of the sensors and actuators will continue to exist and therefore the need for I/O nodes.

The focus for this thesis is to evaluate security concerns and propose mechanisms for software architecture allocated to high performance computational nodes. OEMs that have considered security from the beginning will be able to guarantee the safety of the vehicle when new advanced functionalities are being rolled out. We are therefore looking for students who have an interest in security and who want to be a part of the team investigating software architecture alternatives when moving towards homogenous centralized architecture.

When moving towards the homogenous centralized architecture, a few powerful computational nodes will integrate many applications with different levels of security. The first step is to systematically identify security flaws when using this approach of integrating many applications on a single node. Based on the identified flaws, security mechanisms to mitigate some of the prioritized flaws need to be investigated in detail. It is crucial to ensure that a security flaw in one application does not influence others. For example, sensitive information from one application may propagate to another or influence access to common resources by a denial of service attack. One could apply access control mechanisms based on rules similar to the Unix file system in Unix with possibility to read/write/execute based on owner/groups. A virtualization technique like sandboxing is another mechanism for separating executing applications and their access to shared resources. Then there is the containers technique like Docker which enables packaging and deployment of software which runs independently by having an additional layer of abstraction over Linux OS.
*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 methods for systematic evaluation of secure vehicle application software architecture and evaluating the results in the context of an industrial use case provided by Volvo truck based on ongoing work with more centralized architecture to improve data security of the automotive E/E systems.

**Background of students**

Candidates should be in the final year of their Master’s studies. Suitable masters’ programmes include Software Engineering, Electrical Engineering, Computer Science, Computer Engineering, IT, Mechatronics. Candidates with equivalent background from other programmes will also be considered.

This work focuses on concept and design phases of the system development lifecycle. Several subject areas such as computer and network/IT security, programming in C, 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 favourably. As the work environment is highly international, good skills in English, both oral and written, are required.

**Description of thesis work**

The objective of this thesis is to identify security flaws and propose mechanisms to mitigate those flaws when moving multiple truck applications from the existing heterogeneous distributed architecture towards homogenous centralized architecture. The security mechanisms to be addressed can be defined as thesis starts. Consequently, the research contribution will be around recommendation for software architecture on these centralized powerful computational nodes. The results will be used as an input to people developing next generation commercial vehicle architecture.

The work in this thesis will be carried out as collaboration between Volvo Trucks and department of computer science and engineering at Chalmers. The work will be roughly organized according to the following phases:

1. Survey the literature on secure vehicle application software architecture. This work will focus on studying the literature related to understanding the security flaws when integrating application with different levels of security on a single computing platform.
2. A simple prototype demonstrator based on UDP/IP/Ethernet running on Linux OS is available. The students are expected to explore security flaws in it.
3. Define mechanisms to tackle selected security concerns from the previous step
4. Evaluate the identified mechanisms in the demonstrator. Basic skills of programming in C++ and basic knowledge of Linux OS should be sufficient.

After a successful thesis project, students will gain experience in the field of automotive E/E application development and security design in particular. Students will gain experience from
state-of-the-art hardware and software platforms as well as tools. Students will also have an opportunity to gain insights into how research is conducted in the automotive industry.

**Thesis level:** Masters

**Language:** English

**Starting date:** January 2017

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

**Academic Tutor:** Tomas Olovsson, Associate professor, Computer Science and Engineering, Chalmers.

**Industrial Tutor:** From Advanced Technology & Research at Volvo Group Trucks Technology:

  Christian Sandberg, christian.sandberg@volvo.com, Telephone: +46 31 322 6094
  Atul Yadav, atul.yadav@volvo.com, Telephone: +46 31 322 8868