Thesis Proposal: Vulnerability Analysis of Automotive Embedded Systems

Extent
Two Master’s Thesis Students

Earliest start date
January 2016

Supervision
Provided by researchers and engineers at Embedded and Electrical Systems, Advanced Technology and Research, Volvo Group Trucks Technology, Volvo AB

Suitable for
Software Engineering, Computer Science, Computer Engineering, IT, Mechatronics or equivalent.

Prerequisites
Basic background in computer science, computer engineering and/or software engineering. Knowledge in one or more of the following areas is beneficial: programming embedded systems, network/IT/computer security, verification and testing of software, real-time systems, software engineering and distributed systems. Requirement to have taken at least one university level course within the security area.
1. BACKGROUND

Safety has traditionally been regarded as one of the most important attributes in the automotive industry. On the contrary, security has hardly been addressed in the context of automotive systems. Nevertheless, security and safety are often interconnected. Security threats against vehicle(s) could potentially affect the safety of the human being involved. Consequently, security has recently become a major concern for the automotive electrical and/or electronic (E/E) systems. Security puts new requirements on architecture design and the introduction of security mechanisms into the system.

We are now looking for students who are ready to accept challenging tasks within this exciting area. Do you want to be a part of the team that is developing data security solutions for the embedded systems of the next-generation commercial vehicles?

1.1. Data Security of Automotive E/E Systems

An increasing degree of computerized control in the automotive industry brings with it a corresponding array of potential threats. To make the situation worse, the attack surface of the modern road vehicles is growing swiftly as more safety mechanisms, sophisticated services and communication features are incorporated into vehicles, and are primarily implemented in software. Ironically, at the same time, one fact has emerged from the security field: Software will always have security problems. In recent years, researchers have shown numerous attacks on vehicles, some of which have been widely covered in mainstream media, such as the Jeep hack by Miller and Valasek, with a subsequent recall by Chrysler of 1.4 million vehicles as a result in 2015; and the vulnerability affecting BMW Connected Drive that could let attackers unlock vehicles, leading to 2.2 million cars needing software updates.

Adding security to legacy systems as well as incorporating security mechanisms to new designs constitute manifold challenges, such as, what kind of mechanism may be used, where to put them, how they affect the system to name a few.

1.2. Embedded system data security research at Volvo

The Electrical and Embedded Systems department at Advanced Technology and Research is at the centre of automotive embedded security research within Volvo. We are continuously pushing the frontiers within the field, such as the currently running, publically funded HEAVENS project (FFI/Vinnova), which has reached international recognition as being in the frontlines of areas such as threat analysis and risk management.

This thesis project will contribute to security projects within the department by identifying and evaluating mechanisms and suggest architectural changes that would improve data security of the automotive E/E systems.

2. SCOPE

This project is suitable for two full-time Master’s student(s). Experienced engineers and researchers at Advanced Technology and Research, Volvo Group Trucks Technology will supervise the thesis workers. The work will take place in Gothenburg, Sweden. Apart from the thesis report, students are expected to give a presentation at Volvo AB at the end of the project.

2.1. Thesis Project Goals

This thesis work is expected to advance the activities carried out in security – related projects at the Electrical & Embedded Systems department by investigating ways to improve data security of the automotive embedded systems. The exact goals of the project are to be defined as the thesis starts, but a preliminary list of goals includes:

- Survey and identify root causes for past attacks on vehicles
- Investigate suitable mechanisms or architectural changes that would mitigate and prevent attacks
- Developing, implementing and evaluating security mechanisms to improve data security of the automotive embedded systems.

2.2. Prerequisites

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.

Several subject areas such as computer and network/IT security, programming in C, modelling languages, software engineering, software verification and testing, 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, however a requirement is for the applicants to have taken at least one security course a university level. As the work environment is highly international, good skills in English, both oral and written, are required.

2.3. Benefits

After a successful thesis project, students will gain experience in the field of automotive E/E system development and using security mechanisms in embedded real-time automotive systems. Students will gain experience from state-of-the-art hardware and software platforms as well as tools used within the automotive industry. Students will also have an opportunity to gain insights into how research is conducted in the automotive industry.

2.4. Contact information

Please contact Christian Sandberg (christian.sandberg@volvo.com) for more information.