SecFutur: Security Engineering Process for Networked Embedded Devices (Extended Abstract)

Simin Nadjm-Tehrani
Dept. of Computer and Information Science,
Linköping University,
S-581 83 Linköping,
Sweden.
e-mail: simin.nadjm-tehrani@liu.se

Ask an engineer in the embedded systems sector about the challenges in product development and the chances are that the keywords size, performance, and cost will be included in the answer. Indeed the driving force in the embedded market has been miniaturisation, faster time to market, and higher performance in the past decade. This equation is subject to a rapid change in the years to come. With more and more embedded devices perpetually connected via a network we see the emergence of security properties among the basic requirements in product development. This is a radical departure from the earlier state of the "things" where the devices were naturally protected from security threats by operating in closed and controlled environments. On the one hand the very effect of miniaturisation and cost efficiency is the embedding of digital components in new applications and sectors. On the other hand, the drive for cheaper systems that are adapted in a flexible manner has eliminated the properiety interfaces and isolated systems. Today's systems are increasingly adopting open standards; and when it comes to networked devices we see the emergence of IP networks in as diverse domains as the energy sector, banking and telecommunications.

This dramatic change together with the increased hostility in the operational environment of networked applications makes security requirements a basic tenet that needs to realised by additional building blocks (e.g. access control, authentication, intrusion monitoring and forensics). It is also increasingly evident that these requirements can not be met through an add-on feature developed at late development stages. Efficient development of secure embedded systems requires an engineering process that brings together existing solutions in hardware and software and can be demonstrated to achieve design goals such as resource efficiency as well meeting legal and international requirements. Examples of such

requirements are non-repudiation of state, time and data in controlling sensor networks, legal requirements for calibration of gauging devices and integrity in payment systems crossing enterprise and national borders.

In this talk I briefly describe the objectives of a three year European FP7 project addressing security in future networked environments (SecFutur). The project has started in May 2010, aiming to flexibly integrate security solutions into a framework for development of networked embedded systems. The challenge that the project addresses is to combine given building blocks such as authentication and identification mechanisms within an existing platform-based design process with as few changes as possible, and in as many domains as possible. To support this process, the project will need to create abstractions that can be used to demonstrate freedom from misuse, credibility, and operational integrity of data and services at an early design stage, and to support the satisfaction of high level security properties by integration of known security building blocks.

This will be done by adaptation of development environments with support for verification of security aspects aiming to demonstrate the intended interaction of security building blocks with functional requirements in systems. In addition, the project will create validation and test environments that can be used to illustrate the enforcement of the required levels of security when using the building blocks within the proposed engineering process. The overall SecFutur process will thereby include support at design time, after reconfiguration, evolution and updates, as well as run-time security monitoring of embedded and networked devices.

Three application areas are provided by the industrial stakeholders in the project consortium: remote metering devices for future smart grids, flexible wireless communication systems in emergency management environments, and automatic update of customer service gateways installed by a telecom operator to block anomalous network traffic while preserving customer privacy.

The project partners, that are gratefully acknowledged in formulating the objectives of the project, are: Fraunhofer-SIT Institute (Germany) acting as the coordinators, Ascom (Switzerland) Ltd., Infineon Technologies AG (Germany and Austria), Institution of the Russion Academy of Sciences - St. Petersburg Institute for Informatics and Automation (Russia), Linköping University (Sweden), Mixed Mode GmbH (Germany) SEARCH-LAB security Evaluation Analysis and Research Laboratory Ltd. (Hungary), Telefonica (Spain), Universidad de Malaga (Spain). Associated partners are Defence R &D Canada and Queensland University of Technology (Australia).