TNO-ESI Symposium
Managing Complexity, October 3rd 2017

A holistic and layered security approach is necessary

In the present connected world, cyber security is a major issue. As hightech systems have become more and more part of composed services and Systems of Systems, software engineers urgently need to address the security challenge. Speakers during the second parallel session during TNO-ESIs Symposium on Managing Complexity explained about the present state of affairs and told software engineers how to go about this.

“What does it take to come to security by design?” Jimmy Troost, lead for the Dutch HTSM Security Roadmap and director of Thales Research and Technologies in Delft, directly confronted his audience with a key question. “A cyber security framework must fit, in which the sequence of identification of threats, protection against them, detection, response and recovery are all in place.”
One of the connected hightech domains in which cyber security is a top priority is automotive. Timo van Roermund from the world's leading automotive semiconductor supplier NXP: “In 1980, the first Electronic Control Units were introduced in cars, followed by CAN Bus in 1995, a network of five to ten ECUs. From 2000 onward, cars with up to 150 ECUs and 200 million lines of code have moved into the highest complexity domain of System of Systems; via Bluetooth and Wi-Fi they have become a totally connected part of an intelligent environment.”

High complexity, high vulnerability

Trends like connectivity, driver replacement, powertrain management, body & comfort and driver experience have all become software controlled. “Apart from physical safety issues, cars worldwide contain data with a total worth of 750 billion dollars. This has caused an increased need for security, not in the least underlined by a 2015 hack which gave total control of vehicles and led to a 1.4 million cars recall costing a billion dollars. High complexity comes hand in hand with high vulnerability”, says Van Roermund.
Security and privacy by design cannot be based on a single counter measure, urges Van Roermund: “You need multiple protection layers, at different levels in the systems. People often only think of prevention. That alone will not do, you should think beyond that: a secure external interface, secure domain isolation, secure internal communication, secure software execution over all 200 million lines to prevent, detect and reduce the impact and exclude vulnerabilities.”
You can realize that in practice by creating four protection layers, says Van Roermund: “A secure telematica control unit, a secure gateway, a secure network and secure processing. Also, encryption alone is not enough. On top of that, physical and logical isolation and access control are needed.”
Most vulnerabilities stem from design weaknesses in hardware, service and integration. “Therefore, a holistic approach is necessary”, Van Roermund concludes.

In-depth defense

Thomas Quillinan of Thales Research in Delft sees the same with respect to the supply chain. Thales, just like other hightech system OEMS, produces very complex systems without full control over its suppliers. “When all parties keep the info in their own 'stove pipe' there can be no proper interconnection. Nobody owns all the info, so how do you organize information sharing of sensor data necessary for interfaces? When access rights and multi-organization data sharing comes in sight, politics, privacy and legislation issues pop up.”
Creating walls between stove pipes is not the way to go. “You have to have in-depth defense. And you can create that by breaking the information into different components, label it, protect & encrypt it and see to it that integrity and availability is safeguarded. At this point, management of the keys to the information is the issue: provide access on a need to know basis. Information sharing and data security are both equally vital.”

Balanced approach

Quillinan remarks that the mindset towards security has to change. “When someone asks me: 'can we turn off security in the case of an emergency' he has totally missed the point. You need security exactly for emergencies.” No security system can ever be perfect, he says. “If you wish a perfect system, you need to kill all humans. But a sound risk assessment beforehand, together with a properly balanced approach to security effort and yield should bring you a long way.”