Embedded Security Testing in Virtual Vehicles

Extensive hacking simulations with the help of a XiL testing environment

Modern software-controlled vehicle systems no longer only need to be functionally secure; they also require protection against attacks by cyber criminals. To test whether hacked ECUs remain secure in the context of the entire vehicle, ETAS and ESCRYPT rely on virtualization. This enables the advantages of XiL* technology to also be used in security testing.

AUTHORS

Jürgen Crepin is Senior Expert Marketing Communication at **ETAS GmbH**.

Dr. Tobias Kreuzinger is Senior Manager for Test and Validation at **ETAS Inc.** in Ann Arbor, Michigan, USA.

A nightmare: hackers gain access to the vehicle system, intercept sensor signals, and instead input corrupt data into ECU interfaces. Out of the blue, the driver is unable to react, trapped inside an externally controlled vehicle. To ensure such scenarios remain fiction, we need reliable security solutions.

But can hacker attacks be tested? Or more precisely: can it be proven that security measures are capable of reliably protecting vehicle systems? In the area of functional safety, Hardware-in-the-Loop (HiL) systems have been established to verify that functions react as planned, both during normal operation and interruptions. Developers test the software and the interaction of distributed sensor systems and vehicle domains in simulations of complete vehicles, including all ECUs and data networks. Real-time HiL systems such as ETAS LABCAR, the co-simulation solution ETAS COSYM, or virtual ECUs generated by ETAS ISOLAR-EVE provide the technological basis.

New option: Security-in-the-Loop

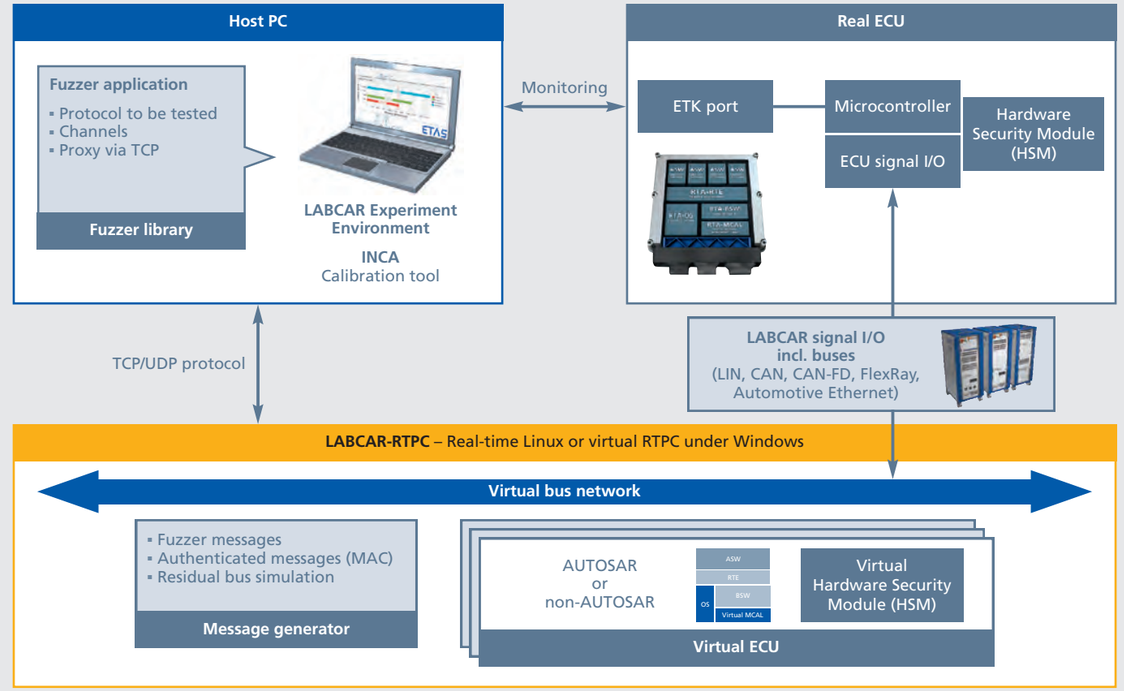
For security testing, the true-positive method, i.e., testing for anticipated behavior, is less effective because at the time of the development the attack scenarios are generally unknown, or known security gaps are directly closed. Instead, the focus is on searching systematically for vulnerabilities. Software-in-the-Loop (SiL) or HiL testing environments are also suitable here.

The challenge lies in combining competencies from different domains. Security experts have to familiarize themselves with the XiL testing method while XiL test engineers must become familiarized with methods from the traditional IT environment. Together, they can then identify potential vulnerabilities in the embedded system. Since the primary focus here is on security-relevant vehicle functions, such security tests have to be consistently planned and efficiently executed from the outset.

ETAS and ESCRYPT recognized this challenge early on and consolidated their know-how in the fields of safety, XiL methods, and automotive security. The result is a solution that brings together the best of both worlds (see figure). A virtual test area based on the LABCAR hardware, the Linux-based simulation target LABCAR-RTPC (Real-Time PC), and the virtual ECU solution ISOLAR-EVE makes it possible to simulate attacks on individual ECU interfaces and attempts to manipulate ECU functions in the context of the entire vehicle.

LABCAR for security tests

While ETAS is responsible for the test system, ESCRYPT contributes its security expertise when it comes to choosing meaningful testing methods – for example:



Basic structure of a security test system.

▪ **Penetration (PEN) testing:** testers attempt to manipulate the behavior of ECUs externally (for example, through human intervention), read out data without authorization, or corrupt the embedded system. To ensure ideal test coverage, the partially automated PEN Testing-in-the-Loop from ETAS and ESCRYPT utilizes an "attack library," which is continually being extended with experience gained from ESCRYPT consulting projects.

▪ **Fuzzing:** testing software – "the fuzzer" – automatically generates random input or deliberately manipulated commands that are used to flood ECU ports. When simulating attempted intrusions or manipulation by hackers, knowledge about the protocol, the software system, and the crypto security of tested ECUs is usually integrated into the signal generation to enhance testing efficiency.

▪ **Message authentication (MAC) testing** checks whether the systems are accessible by input from authorized sources. For this, the test system offers the possibility to generate cryptographic encryption keys and counters, as well as mechanisms for interpreting them during decoding.

Based on the responses of individual or several interconnected ECUs, the tests make it possible to systematically detect vulnerabilities in the vehicle IT system. Theoretically, there exist an almost infinite number of test vectors. Thus, it is necessary to practically limit test cases. ETAS and ESCRYPT therefore not only simply provide simulation and testing tools – they also offer competent support with the preparation of test plans and configuration of the LABCAR test environment.

XiL technology and tools for ECU access (e.g. ETK) from ETAS are the prerequisite for comprehensive security tests: testers have full, time-synchronous access to the memory and internal data handling of tested ECUs, and can precisely track their functions and processes during the PEN, fuzz, and MAC tests. It is these real-time mechanisms and extended monitoring functions that permit the required depth and scope of analysis.

Summary

ETAS and ESCRYPT have built up expertise in the fields of automotive security and XiL-based testing over many years. They are now merging these competencies to ensure comprehensive protection of ECU networks. Combined with the use of meaningful testing procedures, XiL systems are ideally suited for verifying security mechanisms and detecting security vulnerabilities, thus representing another key step towards the securely connected vehicle of the future.

On the next page you will find out what possibilities the ESCRYPT Testing Laboratory offers.

* XiL = Model-, Software-, and Hardware-in-the-Loop (MiL, SiL, HiL)