InSecTT - Wireless Security Testing Environment for smart IOT

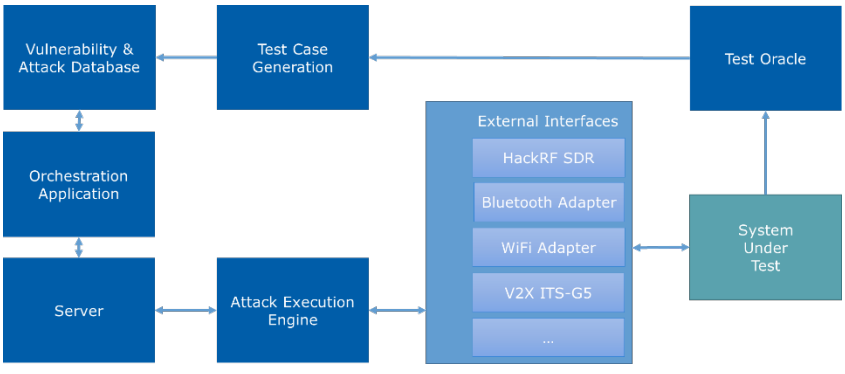
The effect of smart, connected electronic systems on many aspects of modern life is increasing. Such devices join, adapt, collaborate, and interact, and can now also be found in modern cars, trucks, trains or planes. Often, human safety directly depends on such systems.

A modern car is composed of 100+ electronic control units, many of which now use wireless communication, for example via Bluetooth, Wifi, NFC, and other technologies. For example, Intelligent Transportation Systems (ITS) depend on IEEE 802.11p radios (or alternatively cellular communication) for vehicle-to-vehicle (V2V) or vehicle -to-Infrastructure (V2I) technologies for information exchange, generalized as vehicle-to-anything (V2x). Vehicles may also receive software updates "over the air" (OTA) using IEEE 802.11 (WLAN) home access points. Other examples include vehicle entertainment systems connecting via Bluetooth to a passenger's mobile devices. This has tremendously improved our comfort, safety, and driving efficiency. But on the other hand, it provides more than enough opportunities (also called "attack surface") for malign actors ("hackers").

Cyber resiliency is therefore a major goal in design and verification/validation. In the project InSecTT, AVL together with leading cybersecurity experts from academia and industry developed a novel **system-level cyber-security test bed**, to verify cyber-resilience of connected vehicles.

One challenge was to test vehicles under real-life conditions, while still being in the controlled environment of an automotive test bed. For such realistic context, all relevant aspects need to be simulated in high fidelity: environment, traffic, movements, radio channels, interactions, etc. The diversity of wireless systems requires the support of a wide range of technologies. Cybersecurity testing tries to find (hidden) vulnerabilities in systems before the "malign attackers" find them. Thus, AVL's focus was on algorithms (both classical and AI-based) to automate the discovery of relevant test cases (attacks), in order to raise efficiency and speed up the process.

A set of building blocks was developed and integrated to build flexible test systems for different vehicles and scenarios.



As a result, a highly automated cybersecurity test system was developed, which allows developers to greatly extend the number of tests within the same (or even less) time and budget. As a result, OEMs and operators are able to find hidden vulnerabilities before market release, and can continue to safeguard vehicles throughout their lifetime, therefore raising quality and cyber-resilience significantly.