FISHY, IOT SECURITY FOR THE AUTOMOTIVE SUPPLY CHAIN

Software is alive and, as it grows, so do its security issues. In this context, IoT is no exception. Fishy, a European project belonging to the H2020 program in which we participate, is an example of an effort that will bring cybersecurity to the IoT supply chain and, more specifically, to the automotive sector.

The world of IoT has long time since become part of our lives. It arrived loaded with new challenges and evolutions that have allowed us to improve our daily lives in simple things such as improving our eating or sports habits, obtaining information and managing remote devices in real time, managing our refrigerator, expanding the capabilities of the TV or improving the cleanliness of our homes through smart vacuum cleaners.

IoT has also **made it possible to reduce expenses, costs and losses**, facilitating the creation of technological ecosystems that have improved other areas such as industry, transportation or healthcare.

But one challenge will always remain: **security**. Software is alive and as it grows, so do its vulnerabilities. It is not uncommon for large companies that devote a great deal of effort to protecting their systems to announce that one of them has been compromised.

The IoT is no exception and great efforts are being made to preserve the security and integrity of the systems and the data they contain. **Fishy, a European project under the H2020 program**, is an example of an initiative that will bring cybersecurity to the IoT supply chain. Capgemini Engineering participates by demonstrating the capabilities of the ENSCONCE platform, integrating FISHY and REMOTIS, an autonomous vehicle.

One of the main problems in the automotive sector is that manufacturers have become system integrators. Manufacturers receive numerous components from different IoT system suppliers and integrate them into their vehicles. The problem grows when **the same vehicle model can be sold with components from different suppliers**, making the issue a real challenge.

This issue of IoT component supply chain management and security is a major concern for the industry. Every IoT device is susceptible to being flawed or attacked through the use of a security breach in its software, either because they contain bugs that are detected after being incorporated into vehicles or because they have been tampered with as part of an attack.

Fishy will provide a security layer to **manage the software status of vehicle components and sensors**, ensuring that nothing is tampered with and that all embedded software is free of known bugs.

Capgemini Engineering concerns about safety, anticipating security issues that may arise in the Smart City and bringing FISHY to its autonomous vehicle.