PROJECT RESULTS

CAT209 | Robust and user-centric technology platform for secure wearable objects aimed at Internet of Things and Smart City applications

[H2O - Human to Objects]

H2O creates a technology platform for the development and customisable integration of secure wearable objects. It delivers solutions which are cost-effective, ensures privacy and security, as well as enables easy and user-friendly interactions. The project also validates the platform's capabilities with the help of representative use cases.

Businesses, military forces and medical professionals have been using wearable technology for decades, but the private consumer market has only recently started to feature items, such as smart glasses, smart watches, hearables, fitness and health trackers, smart jewellery or smart clothing. The most successful wearable devices on the market right now are smart watches and health and fitness trackers.

However, with the market growth for wearables also grew calls to simplify the user-interface and to make customisation much easier. Furthermore, lack of proper security and privacy protection were a constant cause for alarm. Hence, the underlying rationale for the H2O project was to give wearable computing and the target business areas – Internet of Things (IoT) and Smart-City applications (notably e-Mobility, e-Health and e-Commerce) – a real boost by providing the missing key elements required to further drive these businesses, while continuing to improve the digital lifestyle of the user.

Towards a secure and user-friendly wearables platform

The H2O project defined, designed, developed and validated a technology that establishes secure, bidirectional wireless interaction between objects or individuals, based on capacitive conductivity of human skin. In addition, the project investigated human-to-object interaction in different application areas, and also manufactured H2O-specific devices and integrated them in the use-case-specific architecture deployed in six demonstrators.

The project's main objectives were to:

— Provide a robust, open, technology platform (hardware, embedded software and management tools) for the development and customisable integration of a large variety of secure wearable objects aimed at providing user interaction which is trusted, privacy-preserving and easy to establish in future IoT and Smart City environments;

— Address the double challenge of high security in an open and a non-secure environment supporting multi-tenants business models;

— Provide cost-effective and fast operational solutions;

— Validate the capabilities of the platform in representative IoT or Smart-City use cases, such as eHealth, e-Mobility or e-Commerce. The validation process included several facets, such as user panelization, fast-track prototyping, living labs and pre-deployment schemes in real working conditions.

The main project deliverables were:

— A high-performance, reliable, ultra-low-power body communication coupling (BCC) technology;

— A representative set of non-intrusive, secure, low-cost, wearable devices, suitable for several application domains pertaining to IoT or Smart-City. Robust and easy-to-use form factors (such as watch, bracelet and clips) suitable for target applications were also implemented;

— A fully trusted and privacy-protecting transaction environment, enabling objects which users wear or touch to seamlessly initiate applications or communicate with other objects;

— An open software-development kit (SDK) and application-certification tool-chains which facilitate third-party development of wearable computing apps, and ensure such apps can be automatically verified before being remotely loaded onto user-owned wearable devices;

— A complete reference and trusted-security architecture enabling seamless, secure synchronisation of wearable devices. This synchronisation includes loading credentials onto a blank wearable device;

— A pilot implementation of wearable-computing scenarios in IoT or Smart-City application domains, together with initial quality-of-service (QoS) or quality-of-experience (QoE) feedback.

Spreading the good news

H2O continued the standardisation effort (started in a previous project) to promote the replacement of the secure element (SE) legacy framework set up in the early 1990's, which allows for the separation of hardware and software elements and also deals with other key issues such as privacy. This new standardisation framework will ease the deployment and implementation of security functions in the core of the chips integrated in the upcoming devices.

H2O's creative work resulted in eight patent applications and more than seven articles, reports and papers, which were presented at conferences or submitted for publication (and some even won awards). Project members participated in some 50 events, such as workshops, conferences and exhibitions, all of which supported the dissemination of the knowledge and experience gained from the project, while promoting and marketing its achievements and products.

Targeting premium secure-wearables markets

According to Gartner, a research company, worldwide wearable device sales will grow 26% in 2019 and worldwide shipments will reach 225m in the same year (an increase of 25.8% from 2018), growing to 453m units by 2020. Notably, the total addressable market for H20, when considering only the selected use cases analysed in the project, is between five and 10 million devices (a small share of the wearable market), with a large part coming from access control and payment. However, the market for pure payment or omnichannel (the seamless multichannel approach to selling regardless of shopping method) access control will be more difficult to target, due to increased competition from mainstream wearable stakeholders integrating payment schemes, and a price war in the consumer market.

Indeed, if the overall volume is expected to be small, the overall value could be significant, at up to €3 billion of the total available European market. H20 will position its products in the premium secure-wearable markets, thanks to its notably differentiating features (over those in traditional wearables), namely its focus on advanced seamless security/privacy, something most end-consumers are not ready to pay for, and not nearly enough aware of. As a consequence, the 'sweet spots' are logically in business-to-business (B2B) markets, which can not only value these features, but also adopt the relevant processes needed to implement them. The top market is therefore access control for various vertical sectors: corporate, industry, banks and the like. Here, H20 products can differentiate themselves from others, thanks to such additional features as: ultra-wideband (UWB) for indoor localisation/tracking; tight security based on eSE and BCC; medical sensors for healthcare; near-field communication (NFC) for payments; in addition to data storage and logical security. A prime target for H20 products could therefore be high-end markets for access control and healthcare.