SMART E-MOBILITY CHALLENGE

THE WEEVE PLATFORM: TRUST IS SUPREME

FOR THIS E-V CHALLENGE, WE UNPACKED THE CORE TECHNOLOGIES UNDERNEATH THE WEEVE PLATFORM

PROBLEM BEING SOLVED

The Weeve IoT-Blockchain platform provides cryptographic key addresses to all machines used in the ecosystem. This public-private key pair, for instance, can be coupled for the ethereum chain or many others thus providing an easily interoperable solution within different chains. Trust is supreme. With the Weeve patented technology -testimony, which is a cryptographic proof over the execution of some program. In contrast to code attestation techniques being static by nature, a testimony is dynamic and linked to a particular process (program at runtime) including inputs from and to other peripherals or processes.

As data produced from the car is vulnerable to attacks, the utmost care must be taken to secure the process of harvesting the data and turning it into a tradable asset. By secure we understand the authenticand confidential processing of data. It encompasses the linkage of device identities with harvested data and measures safeguarding data privacy. The first is a prerequisite to link the data with the device owner or an account necessary for the monetization of the data.
The latter is the central ingredient for a fair trade within a marketplace. There is a strong connection between data privacy and exclusivity. Suppose, for the nonce, that data would not be kept in a private way. It thus can easily be replicated, as it is a simple sequence of bitstrings. Consequently, one can increase the supply, which leads to a reduction in price. It is clear that a price decrease due to information leakage is an undesired property in an Economy of Things.

SOLUTION BEING PROVIDED

The core of our technological pillar in our architecture is a tamper proof mechanism to store and access the sensitive data. Several of our core technologies rely on cryptographic credentials. Being, for example, able to handle transactions in an autonomous way, brings a lot of risks if the private key to sign transactions is exposed. Secure storage makes sure that all the sensitive credentials are confidential and of integrity. In this case, we rely heavily on utilizing the Trusted Execution Environment. Secure storage is a mechanism anchored in the secure OS. The only way to read, write and erase objects is through the mediation of a trusted authority. To be a bit more precise, when the TA is calling the write function provided by Trusted Storage API to write data to a persistent object, a corresponding syscall implemented in TEE Trusted Storage Service will be called, which in turn will invoke a series of TEE file operations to store the data. TEE file system will then encrypt the data and

send rich operating system file operation commands and the encrypted data to TEE supplicant by a series of RPC messages. TEE supplicant will receive the messages and store the encrypted data accordingly to the Linux file system. Reading files is handled in a similar manner.
Only properly authorized normal OS programs are able to read, write or delete those files, since every single one of these operations can only be executed through the secure worlds API (namely a \secure storage call").

TECHNOLOGY COMPONENTS

The Weeve Data Firewall technology filters out low-quality data sets to make sure that only reliable data is processable. The testimony, a patent-pending cryptographic technique, enables data authentication at the IoT device, adding a standardised quality control to data assessment. The unique method significantly reduces data forgery and device contamination, while increasing data integrity.
One core ingredient of our stack is a lightweight secure communication protocol, called TEE-MQTTS. The goal of the cryptographic protocol is to establish an authentic and confidential connection between an IoT device and a broker (e.g. cloud backend).
With the protocol we transport digital assets - for example charge received in the car and the payment from the cars wallet via virtual tokens from the IoT device to the backend, such that digital assets are kept private (confidentiality) and are protected against manipulation, origin impersonation (authenticity) and replay in transit. Our protocol is inspired by the famous MQTT protocol.

BUSINESS VALUE

Vehicles of the future such as our Jaguar heavily rely on data as the source to self-sovereign, intelligent and autonomous decisions. Already today vehicles generate up to 25 GB of data per hour and this is expected to double considering there will be 200 sensors installed in connected cars by 2020.

Once autonomous vehicles become mainstream, forecasts estimate that the amount of generated data will equate to 300 TB of data annually. To expose the full business potential of V2V/V2X, challenges related to autonomous payment, fuelling/charging, intelligent driving and transportation, or fleet control need to be solved in order to complement the customer experience.

All of this requires enterprises to think of innovative solutions beyond their perimeters. For example, the car manufacturer has to synergize with the fuel/energy charging station operator. For the prolonged adoption of automation in these domains, sensors and the way the data is sourced bears a sensitive role. The manipulation of connected vehicles and the environment they interact with is a severe threat that hampers a wide-range commercialisation of V2X applications and services resulting in huge commercial and personal losses.

Weeve provides with its platform solution the common technology layer for the V2V/V2X domain to break out of monolithic businesses and explore the benefits arising from the cross-collaboration with novel ecosystem partners.

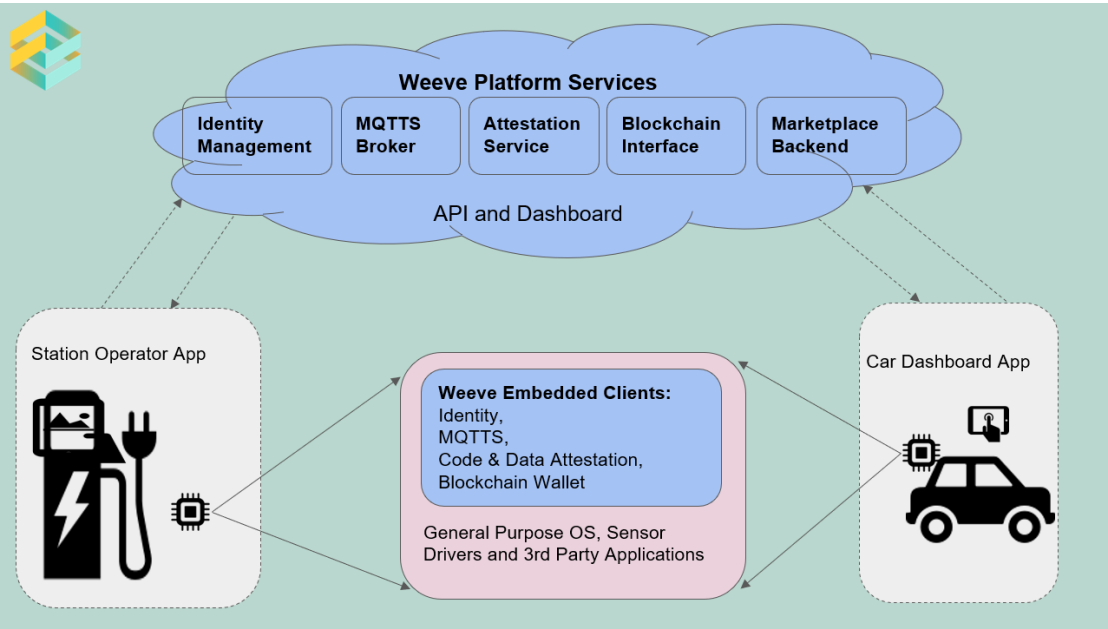
The platform allows the secure interconnection of vehicles and environmental devices operated by potentially competing players, and implement data-driven applications

and services beyond the present technological borders.

The platform safeguards the validity of the data and enables vehicle payments, attestation of data, and commercialization of the data through marketplaces. For instance, concepts built around preventing fuel fraud which cause huge commercial damages to fleet providers and transportation companies or safeguarding odometer readings; which enable a true car sharing marketplace to come into effect will only be made possible via a secure and scalable multifunctional IoT Platform.

TIOTA MACHINE Security USE CASE

Our protocol is inspired by the famous MQTT protocol, the de-facto standard communication protocol for IoT, extended with cryptographic features normally obtained from the computationally expensive SSL/TLS protocol.



THESE PARTNERS CONTRIBUTED TO OUR SUCCESSFUL POC