Design and Implementation of a Digital Access Control Protocol

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Gerhard Hassenstein, Prof. Dr. Annett Laube
Expert: Andreas Fischer (VBS Bern)

Peer-to-peer sharing business models are on the advance, especially car-sharing. Technologies like Bluetooth make it possible that customers can use their own smartphones to open rental cars. While this is very convenient for the users, such systems demand special requirements on access control systems.

Scope

Access control systems for physical objects like cars come with two main concerns.
First, equipping each car with an internet connection involves high costs. For many use cases, it is smarter not to assume an ever-present internet connection and use a protocol that allows offline access instead.
Second, due to the low-bandwidth of technologies like Bluetooth Low Energy and Near-field communication, the size of the exchanged messages between the smartphone and the car need to be small, because larger messages result in longer transmission times, which directly affects the usability.

Approach

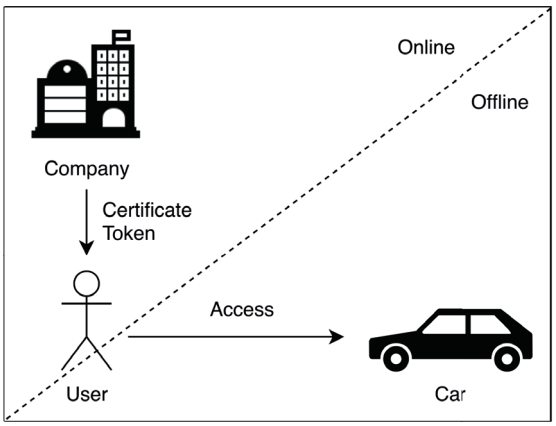
In this thesis, we designed and implemented a generic access control protocol. Our protocol tackles both concerns and provides useful features for scalable applications with a high level of security.
Our solution combines authentication with public key certificates and authorization with digitally signed authorization tokens. Although this approach is well-proven, the traditional X.509 or GPG certificates have a large overhead in size. This makes them impractical for transmission over low-bandwidth channels.
Instead of using one of the extensive certificate standards, we designed space efficient custom public key certificates and authorization tokens.

Results

To test the usability of the developed protocol, we implemented a prototype that comprises the following three parts. A multi-platform mobile application, a web-service and a coffee-machine as a target instead of a car controlled by a small computer. When the user wants to brew a coffee, the app sends a single message over Bluetooth Low Energy to the coffee maker.
We made performance tests with the prototype, which showed that the average time for authentication and authorization is 495 ms. Therefore it can be concluded that the developed protocol could fulfill requirements in practice.

Gian-Luca Frei

Fedor Gamper



Offline Access