Access Tokens for the IoT

Jens-Matthias Bohli
NEC Laboratories Europe
bohli@neclab.eu

Introduction

The vision of the Internet of Things has been discussed for several years now, and has already attracted attention beyond the research community. Besides the widespread use of RFID chips, the Internet of Things is also characterized by smart real-world objects that report status of themselves or the environment detected by sensors. Some objects also offer to change their status or the environment through actuators. Communication and management platforms for smart objects are currently developed. Privacy, security and trust are an essential component in such a platform due to the sensitivity of personal data and the impact that decisions and actuations have on the real world.

This paper discusses access protection for smart objects. The focus is on access tokens that support payment, and access tokens for wireless sensor networks with unprotected sensor nodes. The goal is to present specific requirements and point to initial solutions.

Access restrictions on the smart object are needed to prevent unauthorized access to the object, to protect the data or actuation offered by the smart object, or to prevent malicious access patterns that aim at exhausting limited resources in a DoS attack. The SENSEI project [1] considered two kinds of access restricted objects. 1) Objects that can only be accessed by a small restricted group and 2) Objects that are in principle publicly available but require payment for access. The assumed use case is a network of sensor equipped parking lots that allow the user to find a parking space remotely or reserve the parking space (actuation). Being able to offer payment for access to objects or wireless sensor network can also be an incentive to accelerate wide deployments of this technology [2].

Setting

The involved parties are the owner of the object, a framework provider, where the object is registered, and the users wishing to access the object. Initially, the object has a shared key with the framework provider. Users have to receive an access token from the framework provider in order to access the object. The communication between the user and the object can be via an Internet-based gateway, or locally. In the case of a local connection the token might be obtained online during the access, or in advance. The considered tokens only base on symmetric cryptographic primitives so that they are also suitable for objects with limited computational resources.

Payment Tokens

Tokens that support payment in an IoT-market have certain specific requirements. From the point of view of the framework provider, who also has to deal with the payment, both, the object and user are untrusted in terms of the payment. Therefore the accountability requirements are strong: the object owner should be able to claim an access only and only if a paying user had access to the object.

Depending on the payment model, relaying of credentials between different users needs to be prevented. The proposed protocols assume for this reason smartcards as trusted hardware on the user side. In case of a flat payment scheme as suggested in [2], also collusions between user and objects are harmful. A solution can be found when giving up privacy requirements such that malicious users can be identified.

Untrusted Nodes

An important security requirement for all protocols to be used in a wireless sensor network where a request is propagated through the network is resilience against node compromise. It should not be possible to circumvent the AC by placing malicious nodes or physically attacking a small share of the deployed nodes. For a malicious or compromised node, we assume that the node is fully controlled by the adversary who learns then all data stored by the node and has access to all services offered by the node. This is the scenario considered in [3].

Clearly any solution fails, where the access control is done solely by compromised nodes, or, where the information stored in the compromised nodes enables the adversary to obtain access to the whole wireless sensor network. Thus, in principle every node has to check the authenticity of the access request. This requires features similar to public-key-signatures, where public information suffices to verify the authenticity of a message. A possible solution is a broadcast authentication scheme, that provides flexible trade-offs between security level and efficiency [4]

Conclusions

The paper identified some requirements for access tokens for smart objects and presented initial ideas for possible solutions. An access control suite for smart object will have to be flexible enough to provide access tokens for multiple purposes and support a wide class of the objects from unprotected, computationally restricted to protected and unrestricted objects.

[1] FP7 IP SENSEI, http://www.sensei-project.eu/, see in particular deliverable D3.5
[2] Jens-Matthias Bohli, Christoph Sorge, and Dirk Westhoff
"Initial observations on economics, pricing, and penetration of the internet of things market."
In Computer Communication Review (Editorial Note), vol. 39, no. 2, pp. 50-55, 2009

[3] Jens-Matthias Bohli, Alban Hessler, Osman Ugus, and Dirk Westhoff "A Secure and Resilient WSN Roadside Architecture for Intelligent Transport Systems" In ACM Conference on Wireless Network Security, WiSec'08, pp. 161-171, ACM, 2008
[4] R. Canetti, J. A. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas. Multicast security: A taxonomy and some efficient constructions. In INFOCOM '99 , pages 708--716. IEEE, 1999.