Encryption-Based Access Control for Building Management

Laurent Gomez[*], Annett Laube[*], Vincent Ribiere[†], Alessandro Sorniotti[*],
Christophe Trefois[*], Marco Valente[†], Patrick Wetterwald[†]
[*]SAP Research, SAP Labs France, Sophia Antipolis
[†]Cisco Systems France

I. Introduction

The vision of ubiquitous computing is a network of small, inexpensive, robust processing devices, distributed throughout everyday life. Wireless Sensor Networks (WSNs) are an essential part to realize this dream. Sensor Networks can be seen as sources of input, delivering data from the real world into the digital world.

Wireless sensors have the advantage of lower installation costs and ease of deployment compared with wired sensors. Low cost often arises as a requirement to justify the adoption of WSN technology for particular business scenarios: this results in sensors often being simple devices, with limited computing and transmitting power as well as limited battery capacity.

In addition to technical challenges (e.g. data routing from the sensor nodes to the business applications, data processing, filtering), the integration of WSNs with business applications raises security issues. Although each business application has its own specific security requirements, a controlled access to sensor data, from its production at sensor nodes to its use at business applications is a general requirement.

II. Motivation

In many WSN scenarios, nodes are required to sense a vast range of different data types: in a building management scenario where ambient sensors are installed in or around the building, appliances and furniture information like temperature, humidity, light, motion and sound are collected.

The sensed data can be highly sensitive. Moreover, the sensed data often have very different levels of sensitivity: temperature and humidity in the different parts of a building are less sensitive than information related to presence in rooms, like motion and sound.

Several consumers of wireless sensor data, belonging to an heterogeneous population, have intrinsically different data access rights: normal users can get access to simple building information like temperature and humidity. The access to information related to presense in the rooms, is restricted to managers and responsibles for the building and resources, like electricity, heating and air conditioning.

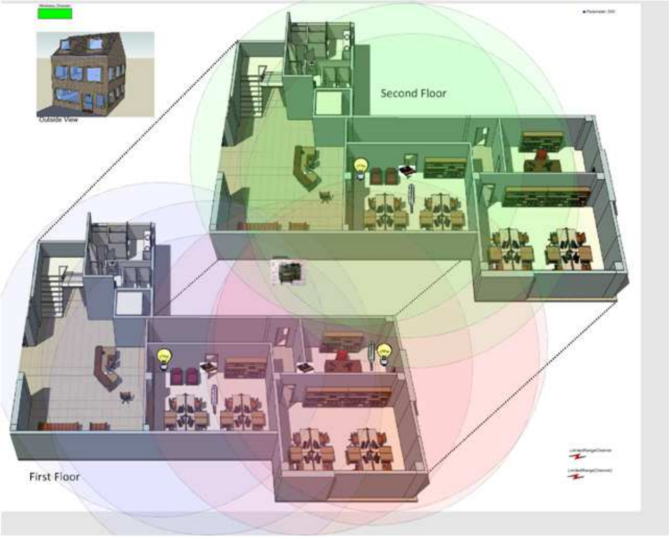

Fig. 1. WSN in a building

Data consumers can be therefore conveniently organized in hierarchies. Low levels in the hierarchy can just access data with low level of sensitivity whilst higher levels can also access more sensitive data. The problem of hierarchical access control therefore clearly arises. A solution to such a problem is additionally complicated by the resource limitation of some WSN installations. We present the implementation of a hierarchical access control scheme for wireless sensor data. Access control is enforced using light-weight cryptography: sensors encrypt data prior to transmission, thus embedding access control right at the source. Thanks to the key generation mechanism, multiple consumers, with different access rights, converge on the same decryption key if their privileges are sufficient. The protocol achieves two very desirable goals for WSNs: it does not use complex operations and it does not require any interaction between the different nodes and the different data consumers.

III. Solution

A. Scenario

Our demonstration shows a scenario in the area of building management. A WSN is deployed within a building to monitor

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.4019
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.4019

light, temperature, room presence, etc., as shown in Figure 1. The WSN is connected to a monitoring application for the building. The WSN delivers large amounts of information that can be used to monitor the energy consumption in different parts of the building and to detect energy losses (e.g. electricity, heat).

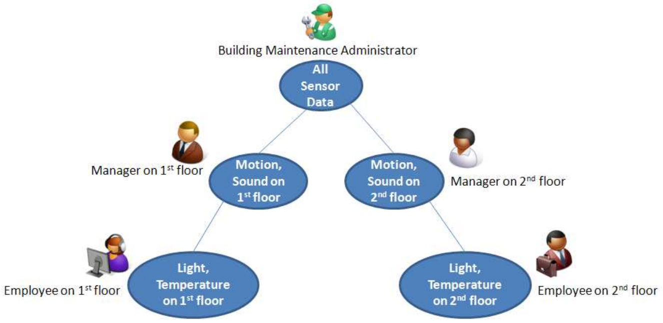
Building Maintenance Administrator
All Sensor Data
Manager on 1st floor
Motion, Sound on 1st floor
Motion, Sound on 2nd floor
Manager on 2nd floor
Employee on 1st floor
Light, Temperature on 1st floor
Light, Temperature on 2nd floor
Employee on 2nd floor

Fig. 2. Authorization hierarchy

In our scenario, we assume an office building consisting of several floors. Each floor is rented by a different company. As the WSN is deployed in the entire building, we have to ensure that sensitive information belonging to a company is not disclosed to another company. Therefore, we implemented the encryption-based access control for the data delivered by the sensor network.

The previously mentioned classification of sensor data in unclassified information (temperature, light) and sensitive information (motion, sound) can be extended taking different locations in the building into account. The employees of a company should get only access to information belonging to public parts of the building and parts rented by their company. Access to sensor information from other rooms in the building is not permitted. The resulting authorization hierarchy is shown in Figure 2.

B. Access Control Scheme

In [1], the authors propose a novel approach for access control for wireless sensor data, based on an end-to-end symmetric encryption from sensor nodes to business applications.

The hybrid approach, relying on active contributions of the nodes (distributed approach) maintains most of the intelligence of the system in a centralized entity. The key intuition is to use light-weight cryptography to achieve access control: if sensor data are encrypted, only the owner of the decryption key can access the data. The scheme allows the generation of hierarchical, time-bounded cryptographic keys. Sensor nodes just have to perform simple encryption operations to enforce data access control, regardless of who the listeners are and what their capabilities are. A central authority is charged of delivering keys to applications based on system's policies.

First of all, a classification of sensor data is established, based on their level of sensitivity, or **authorization level**. Data whose disclosure does not raise high privacy issues are mapped to low authorization levels. Similarly, highly sensitive data are mapped to high authorization levels. The resulting mapping expresses the security preferences of an **Access Control Module (ACM)** and defines the access control policy.

Each authorization class is then mapped to cryptographic material. Sensor data associated to the same class is encrypted with the same cryptographic material. In addition, following the hierarchical organisation of the sensor data classification, this material allows to encrypt any lower class of sensor data.

The ACM assesses the authorization level of business applications and provides them with time-bounded **grants** which allow them to derive the keys to decrypt sensor data from the cleared authorization class, and lower.

C. Hardware Infrastructure

Our prototype consists of two main building blocks: the business application and WSN with the connecting WLAN infrastructure.

The building management application is running on SAP Netweaver that is connected to an Access Controller managing a sensor gateway with IP connectivity. As sensor gateway we use a Xbow NB100 Stargate Netbridge running XServe software. The Stargate Netbridge has an ethernet interface (connected to the Access Controller) and a USB port. A Micaz mote running XMeshBase is connected to the Stargate via that USB port (through a MIB520 interface board) and acts as a base station interfacing the Stargate to the sensor network. XServe represents Crossbows server interface to the base station.

Our WSN is made of Xbow Micaz 802.15.4 motes running an extended version of the Xmesh software. Each sensor mote is equipped with a Crossbow MTS310 sensor board providing the following data: dual-axis accelerometer (ADXL202), dual-axis magnetometer, light, temperature and acoustic.

The Access Controller, a dedicated application, manages the Xbow sensor gateway and motes. This server also implements the ACM described in the previous section.

IV. Conclusion

Our demonstration shows a building management scenario implementing end-to-end confidentiality for sensor data. The encryption-based access control is part of the security services of the Enterprise Integration Component [2], a high-level middleware to support seamless integration of WSNs into business applications, developed in the scope of the WASP project.

Acknowledgment

This work is partially financed by the European Commission under the Framework 6 IST Project "Wirelessly Accessible Sensor Populations (WASP)"[3].

References

[1] A. Sorniotti, R. Molva, and L. Gomez, "Efficient access control for wireless sensor data," *to appear in the 19th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2008.

[2] L. Gomez, A. Laube, and A. Sorniotti, "Design guidelines for integration of wireless sensor networks within enterprise systems," in *in the proceedings of the International Conference on on MOBILe Wireless MiddleWARE, Operating Systems, and Applications*, ACM Digital Library, Ed., 2008.

[3] WASP, "WASP (Wirelessly Accessible Sensor Populations), IST 034963," 2006. [Online]. Available: www.wasp-project.org

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.4019
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.4019