USING HIP DEX FOR KEY MANAGEMENT AND ACCESS CONTROL IN SMART OBJECTS

Andrei Gurtov *(gurtov@ee.oulu.fi, University of Oulu, Finland)*

Ilya Nikolaevsky *(ilya.nikolaevskiy@hiit.fi, Aalto University, Finland)*

Andrey Lukyanenko *(andrey.lukyanenko@aalto.fi, Aalto University, Finland)*

Introduction

Designing proper security protocols for smart objects is a hard problem. Such devices have typically very restricted memory and CPU capabilities, and are battery powered. They cannot support floating point operations efficiently, even lack capability to implement a hash function. Their public-private keys might be pre-configured during production. Therefore, it's a challenge to implement a full scale of security capabilities provided in the Internet with full-scale protocols such as Host Identity Protocol (HIP) Base Exchange or IKEv2. A protocol designer often has at its disposal a small number of cryptography operations such as AES symmetric encryption with several operational modes. With that, a sufficiently strong protocol with authentication and encryption capabilities needs to be developed. Hence, certain advanced characteristics such as perfect forward security or complete privacy support have to be sacrificed.

HIP Diet Exchange DEX [6] was proposed as a modification of the base HIP specification that can operate without presence of a hash function, using only symmetric cryptography operations. It is envisaged for use for securing IEEE 802.15.4 networks, Smart Space environments [1], medical ICT [3], as well as future mobile telecommunication networks [4]. Currently newly formed IEEE Task Force 802.15.9 works on specifying KMPs for 802.15.4 and .7 networks [6].

Key management with HIP DEX

We have implemented HIP DEX in two independent versions, using Java for experimentation with SunSPOT sensors, as well as with C for beyond 4G tests [4]. The implementations proved the concept of HIP DEX design and enabled us to make initial performance measurements. We also measured performance of individual operations of HIP DEX and BEX on imote2 sensor platform [2], which is an example of rather powerful smart object.

One of the lessons we learnt during experiments is the dependence on libraries in code and its impact on the code size and its portability to other platforms. Another is that developing on sensor hardware such as TelosB is very hard and time consuming since combining several software components tends to exceed the maximum memory footprint.

Future open issues we would like to consider involve conversion between HIP DEX (in sensor network) and HIP BEX (in the Internet) in a gateway, especially if the gateway is not fully trusted. In that case, the gateway can add another layer of security around relatively weak HIP DEX without being able itself to decrypt the sensor data. We also working on 'emergency override' capability for sensor security which is often required e.g. for implanted medical devices that need urgent access from unauthorized personnel to save patient's life. The use of puzzles as a way to protect sensors against DoS attacks remain questionable and need more evaluation.

We have proposed a Medical Sensors Network (*MSN*) security framework with HIP DEX as a base. This framework provides energy efficient security and privacy for MSN. In our setup, each MSN has an external on-body device called *gateway* which has two wireless interfaces (one short-range wireless interface, e.g., 802.15.4 for maintaining connection with medical sensors, and one long-range wireless interface, e.g., UMTS or 802.11, for maintaining Internet connection). The sensors perform HIP handshake only once

during the initial pairing to produce asymmetric keys common to a particular sensor and a gateway. The security measures between the gateway and external parties are left out of scope here. In the absence of a gateway the sensors may switch to an emergency mode and use a different security protocol. Such an emergency operation is a crucial part of MSN functionality. However, the latter is a very challenging from security point of view.

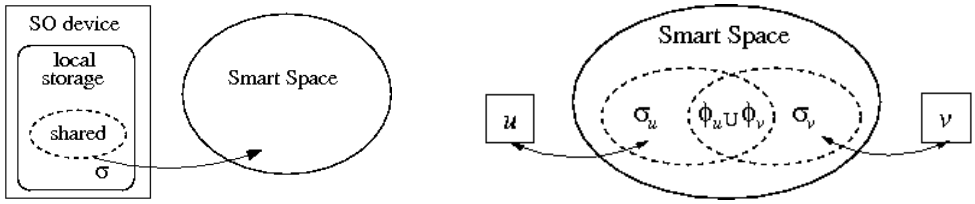
Access control for Smart Spaces

Based on [1, 7, 8] we can argue that the smart spaces approach suits well for development of intelligent applications with smart objects (SO). Any SO, being responsible for a narrow dedicated function, may keep locally only limited data storage. Most of data are shared by SOes and other participants in their smart space denoted $S = (n, I, \rho)$, where n is a space identifier, I is an information set of tuples (content) and ρ is a set of rules to deduce new knowledge from I. Semantic Web provides the RDF model for scalable and efficiently processable content representation, which further allows methods of ontology analysis and logic programming for rules of knowledge deduction.

An example of a smart environment is a patient with SO running on implanted devices and user mobile devices. Additional components such as home and hospital servers can also participate. The smart space is personal; it contains data sensed by the SOes, long-term information about the patient, and deduced knowledge. Knowledge deduction is typically delegated to capable and responsible participants like personal smartphone, private home or hospital server. A patient smart space can be dynamically composed with spaces of other environments, e.g., if the patient drives a car then the car smart space accounts current health status of the driver; in emergency cases, patient's smart space is supported with additional content and decision-making from doctor's smart space.

SO functionality is divided into the two basic classes. (A) SO is a sensor, which senses the environment and publishes the data into its smart spaces, e.g., heart rate. Other participants use the data for further smart decisions. (B) SO is an operational unit, which performs some actions in the environment, e.g., sending an urgent SMS to the doctor. In case (B), SO merely subscribes for the decision-related knowledge in the smart space; whenever responsible participants deduced the need of the action, the knowledge is published to notify all related SOes.

Techniques for efficient smart space-based programming for functionality (A) and (B) even for low-capacity devices exist [7]. Operations with smart spaces were elaborated in [8]. We conceptually define the following security layers in a smart spaces system with multiple SO. Let u and v be SO. The first security layer is based on a sharing function $\sigma_u(n) \subset I$ that defines what knowledge to publish in S identified with n, see Fig. 1 (a). The second security access function φ_u limits access of other participants to u's content; $\varphi_u(v) \subset I$ is the knowledge that u allows v to access. Hence u and v collaborate in the content $\varphi_u(v) \cup \varphi_v(u)$, see Fig. 1 (b). When u subscribes for knowledge k on decision-making then $k \in \varphi_v(u)$ for some v authorized for knowledge provision in such decisions.



(a) (b)

Fig. 1: SO security aspects. (a) sharing function; (b) access function.

Using HIP DEX, we can provide robust identities for smart objects that can be used for authentication and access control to different parts of personal smart space. In addition, encryption with HIP DEX provides confidentiality and message integrity.

Acknowledgment

This work is partly supported by project MAMMOTH from Finnish UBICOM program by Tekes. We also thank Dmitry Korzun, Boris Nechaev, and Dmitry Kuptsov for contributing to this position paper.

References

[1] D. Korzun, S. Balandin, V. Luukkala, P. Liuha, A. Gurtov, Overview of Smart-M3 Principles for Application Development, in Proc. of International Conference on Artificial Intelligence and Intelligent Systems (IS&IT), September 2011.

[2] D. Kuptsov, B. Nechaev, and A. Gurtov, Securing Medical Sensor Network with HIP, in Proc. of the 2nd International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth'11), October 2011.

[3] P. Nie, J. Vaha-Herttua, T. Aura and A. Gurtov, Performance Analysis of HIP Diet Exchange for WSN Security Establishment, in Proc. of 7th ACM Annual International Symposium on QoS and Security for Wireless and Mobile Networks, November 2011.

[4] J. Pellikka, Z. Faigl, A. Gurtov, Lightweight Host and User Authentication Protocol for All-IP Telecom Networks, submitted to WoWMoM'12

[5] R. Moskowitz, KMP Transport Proposal, https://mentor.ieee.org/802.15/dcn/12/15-12-0024-04-0009-kmp-transport-proposal.ppt

[6] R. Moskowitz, HIP Diet Exchange, http://tools.ietf.org/html/draft-moskowitz-hip-rg-dex-05

[7] D. Korzun, A. Lomov, P. Vanag, J. Honkola, S. Balandin. Generating Modest High-Level Ontology Libraries for Smart-M3. Proc. 4th Int'l Conf. Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM 2010), pp. 103-109, Oct. 2010.

[8] Oliver I., Boldyrev S. Operations on spaces of information. Proc. IEEE Int'l Conf. Semantic Computing (ICSC'09). IEEE Comp. Soc.; Sep 2009, pp. 267-274.