Securing Interactions of Smart Objects in Smart-M3 Spaces

Ilya Nikolaevskiy*, Andrei Gurtov*†, Dmitry Korzun*‡
*Helsinki Institute for Information Technology (HIIT), Finland
†University of Oulu, Finland
‡Petrozavodsk State University (PetrSU), Russia
{ilya.nikolaevskiy, dkorzun}@hiit.fi, gurtov@ee.oulu.fi

Abstract

We propose an initial implementation of integration of Host Identity Protocol (HIP) to Smart-M3 platform. Our solution employs a lightweight variant of the HIP exchange—Diet EXchange (DEX). It allows establishing authenticated connections of smart objects to shared Smart-M3 spaces and securing transfer of private data.

Index Terms: Host identity protocol, Smart-M3, Security, Smart spaces.

A smart space is an ecosystem of interacting computational objects (smart objects). They share resources and services running on devices of the current environment [1], [2]. The M3 concept—Multidevice, Multidomain, and Multivendor [3]—aims at interoperable information smart spaces for various domains, spanning from embedded domains to the Web. The fusion of physical and information worlds is not bound to any device type, device vendor, or application domain. Smart-M3 [3] is an open-source platform that implements M3-based smart spaces.

Smart-M3 enables even low-capacity devices to possess limited embedded intelligence locally. The opportunity is crucial in emergency scenarios for implantable devices carriers [4] Advanced processing of patients data from multiple medical sensors is possible with automatic reasoning and decision making on a portable user device without access to the Internet. In one possible scenario portable user device may infer malfunction of Implantable Medical Device (IMD) and report it to patient and doctor by analyzing readings from IMD. While such behavior is possible with other approaches, smart spaces approach makes programming much easier and thus reduces errors in software.

In this extended abstract we focus on the problem of secure communication in Smart-M3 spaces, where many devices are of low capacity (restricted memory, CPU capabilities, battery, etc.). In this case, it is a challenge to implement a full scale of security capabilities provided in the Internet, e.g., with such a protocol as Host Identity Protocol (HIP) Base Exchange or IKEv2 [5]. We propose a HIP-based extension for secure transfer of private data in Smart-M3 spaces. This extension is of uttermost importance in medical applications, where the data privacy must be guaranteed even in Mobile Health (mHealth) settings, when a patient and her/his devices are mobile.

Our proposal design employs HIP Diet Exchange (DEX) [6] to establish secure associations between a Smart-M3 Knowledge Processor (KP) and Semantic Information Broker (SIB). HIP DEX is a lightweight modification of the HIP Base Exchange protocol (BEX). HIP DEX requires rather limited computation capabilities from the devices [7]. It uses Elliptic Curve Cryptography to distribute shared secret between Initiator and Responder, see Fig. 1. In mHealth context the medical sensors will run KP and be initiators of the HIP DEX. Portable user device or on-body gateway will run SIB and be HIP responder. Although HIP

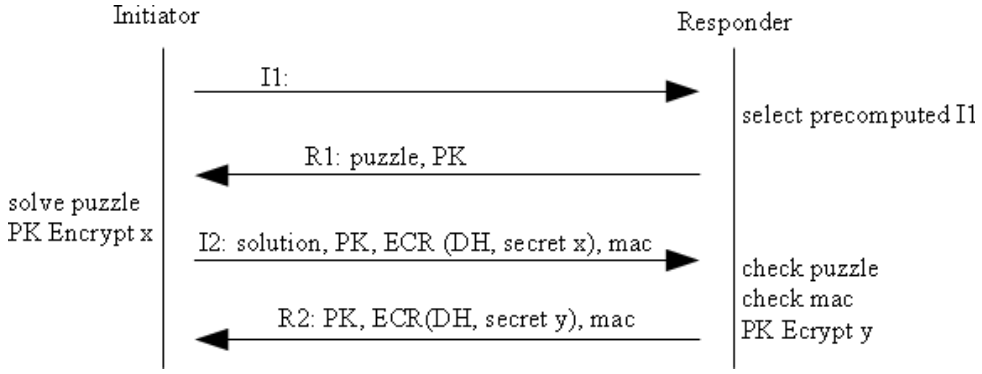

Fig. 1. HIP DEX scheme. Only four packets of total size about 530 bytes are used.

DEX is designed to work in the restricted environments it still provides possibility to control performance level by adjusting cryptographic puzzle difficulty.

Since Smart-M3 has modular architecture it may be preferable to add HIP DEX as a new module into SIB and KP. Instead we propose to embed HIP DEX as a library only in modules responsible for network interaction. Such approach produces less overhead and allows tight integration of HIP and Smart-M3.

The HIP exchange also authenticates both devices, providing robust identities for smart objects. The authentication is crucible in the mHealth area to prevent adversaries to control IMD. The tight integration of HIP and the SIB access module allows using HIP cryptographic identities for access control within the Smart-M3 space. In particular, SIB may restrict access to information that the KPs publish in the shared space.

We started the implementation of our proposal. The implementation is based on low-level ANSI C KP interface provided within SmartSlog SDK [8] and Redland SIB (http://sourceforge.net/projects/smart-m3/files/Smart-M3_B_v0.3.1-alpha/). We use HDX++ library (http://sourceforge.net/projects/hdx/) for HIP DEX protocol. We implemented a secure sib-tcp module of SIB and ansi-c-kpi module for KPI side. This research was supported by Academy of Finland project SEMOHealth.

REFERENCES

[1] D. J. Cook and S. K. Das, "How smart are our environments an updated look at the state of the art," *Pervasive and Mobile Computing*, vol. 3, no. 2, pp. 53–73, 2007.

[2] D. G. Korzun, S. I. Balandin, V. Luukkala, P. Liuha, and A. V. Gurtov, "Overview of Smart-M3 principles for application development," in *Proc. Congress on Information Systems and Technologies (IS&IT'11), Conf. Artificial Intelligence and Systems (AIS'11)*, vol. 4. Moscow: Physmathlit, Sep. 2011, pp. 64–71.

[3] J. Honkola, H. Laine, R. Brown, and O. Tyrkkö, "Smart-M3 information sharing platform," in *Proc. IEEE Symp. Computers and Communications*, ser. ISCC '10. IEEE Computer Society, Jun. 2010, pp. 1041–1046.

[4] A. Gurtov, I. Nikolaevskiy, and A. Lukyanenko, "Using HIP DEX for key management and access control in smart objects," in *Proc. of Workshop on Smart Object Security*, Mar. 2012.

[5] A. Gurtov, M. Komu, and R. Moskowitz, "Host Identity Protocol (HIP): Identifier/locator split for host mobility and multihoming," *Internet Protocol Journal*, vol. 12, no. 1, pp. 27–32, Mar. 2009.

[6] R. Moskowitz, "HIP Diet EXchange (DEX): draft-moskowitz-hip-rg-dex-06," May 2012, work in progress. Expires in November 2012.

[7] P. Nie, J. Vähä-Herttua, T. Aura, and A. Gurtov, "Performance analysis of HIP diet exchange for WSN security establishment," in *Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks*, ser. Q2SWinet '11. New York, NY, USA: ACM, 2011, pp. 51–56. [Online]. Available: http://doi.acm.org/10.1145/2069105.2069114

[8] D. G. Korzun, A. A. Lomov, P. I. Vanag, J. Honkola, and S. I. Balandin, "Multilingual ontology library generator for Smart-M3 information sharing platform," *International Journal on Advances in Intelligent Systems*, vol. 4, no. 3&4, pp. 68–81, 2011.