A Proposed Security Layer for the Internet of Things Communication Reference Model

VŠB - Technical University of Ostrava, Czech Republic

Eng. Hamoud M. Aldosari: mub0002@vsb.cz

Abstract

Based on the IoT Communication Reference Model, the poster proposes a substantial amendment to its layers through adding an extra layer called “Security Layer”. This layer will collect all security mechanisms provided at the different layers in the current communication reference model into one layer. This proposed layer can be considered as a step forward to a centralized management of all security mechanisms into a single and powerful layer. The Security Layer aims to confirm the identity of the sender/receiver, and to help to block connections to potentially vulnerable services. Furthermore, this centralization would allow other IoT’s Communication Reference Model Layers to perform their specified functions without paying attention to any security problems, thus supporting the creation of future troubleshooting processes for such problems.

INTRODUCTION

It is no secret that in the course of time there is a rapid and growing global trend towards the Internet of Things (IoT) at all levels of government and commerce. The common definition was that the IoT involves heterogeneous objects and connectivity [1]. However, to reach the goal of the IoT there is a need for a model describing the communication between these heterogeneous objects, such as the TCP/IP model. Much discussion was done by a group of researchers from more than 20 large industrial companies and research institutions to lay a common “architecture” for the Internet of Things: the IoT Architecture project (IoT-A) [2]. The heterogeneity of smart devices along with the currently existing infrastructure raises the impossibility of having a single design protocol that fits all application domains. Therefore, a more abstract model is needed. The general Communication Reference Model suggested by [2] gives this general abstract framework that comprises a minimal set of unifying concepts, axioms and relationships for understanding significant relationships between the entities of an environment. However, the suggested Communication Reference Model is still unable to address the interoperability issues between heterogeneous objects; like security and privacy.

Security Requirements for IoT

In the security hierarchy of information transmission process, we have to guarantee the confidentiality, integrity, authenticity and instantaneity of data and information, which mainly refers to the security of telecommunication network and corresponds to the security of transmission hierarchy in the Internet of Things [3]. While Figure 1 illustrates these requirements.

Figure 1. Security Requirements for IoT.

The Problem History

The history from the OSI and TCP/IP reference models (Figure 2) to the IoT-A. As a step forward to address a solution for the security issues, this research proposes a new adopted security layer to be added to the IoT-A. The following sections give a brief introduction to the security requirements and a history for the OSI and TCP/IP reference models as roots to the IoT-A.

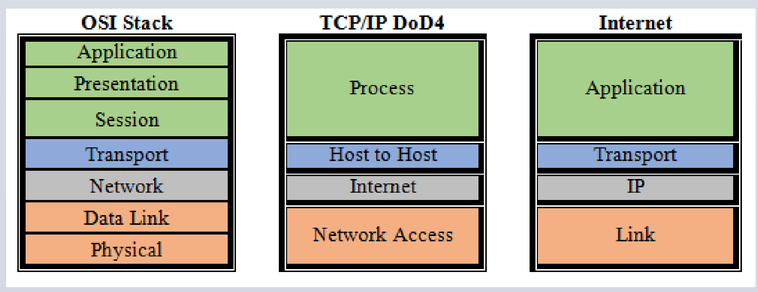

Figure 2. OSI Layers to TCP/IP Model and Internet Stack Model

The IoT Architecture Project (IoT-A) [4] [2], which is a project funded by the European Union and conducted between 2010 and 2013, was the startup for setting such IoT model. More than 50 scientists and researchers contributed to the development of the Communication Reference Model for the IoT which is called “IoT Communication Reference Model”.

IoT-A team decided to focus on the ISO/OSI stack, the US Department of Defense 4 layer model (DoD4) , and the Internet stack, as roots to provide the IoT reference model. The previous models are not able to address the interoperability issues between heterogeneous objects like security. However, this model can be layered on top of one another with our vision to form a new model. The interoperability aspects required for the IoT-A model are illustrated in Figure 3.

The Problem Definition

From the security perspective, the current proposed research investigates the first of the roots of the IoT, which is the OSI model, the security reference model of which is defined in (ISO 7498-2), as illustrated in Table 1. The model is designed around the seven layers (based on OSI reference model ISO 7498-1) [5]. Although the security needs are well-recognized in traditional internet domains, it is still not fully understood how existing security protocols and architectures can be deployed in IoT [6].

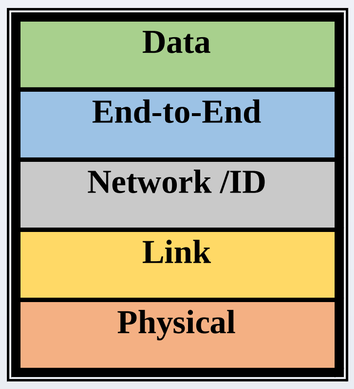

Figure 3. IoT-A Communication Reference Model and its aspects.

OSI Layers (ISO 7498-1)	Security Model (ISO 7498-2)
Application	Authentication
Presentation	Access Control
Session	Non-Repudiation
Transport	Data Integrity
Network	Confidentiality
Data Link	Assurance / Availability
Physical	Notarization / Signature

Table 1. The Security Model

The Proposed Security Layer

The proposed security layer is based on the idea reported in [7] and it is intended to create an independent single layer that will meet most of the required security mechanisms which have been distributed over other layers. The proposed layer will be placed between the Link layer and Physical layer as a filtration layer before the processes of sending and receiving data. Moreover, the proposed layer planned to be lightweight to be suitable for constrained and limited resources devices (those having limited CPU processing capability, a small footprint memory, and limited energy sources) Figure 4.

To show how this layer works after adding it to the communication model, Figure 5 illustrates a scenario of End-to-End Communications through the IoT Communication Reference Model with the proposed security layer.

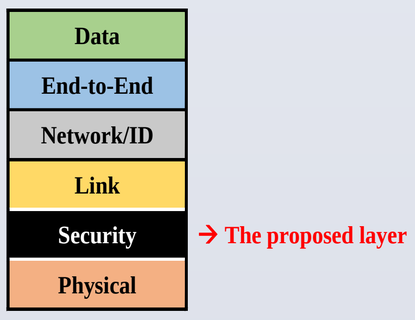

Figure 4. Illustration of the model with the proposed Security Layer.

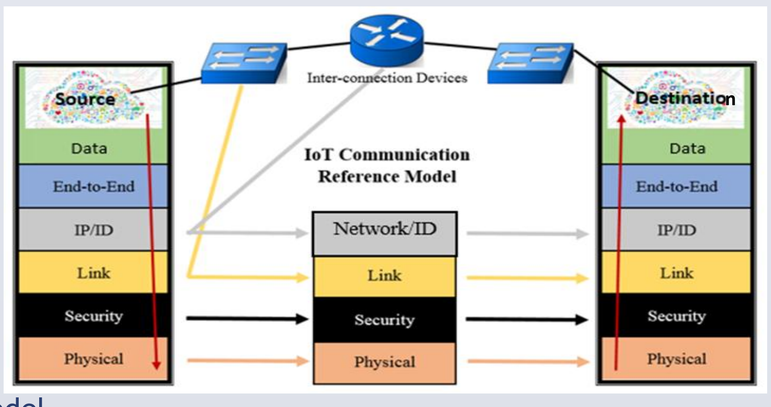

Figure 5. Security scenario from End-to-End

Conclusions

Everything and everyone will someday be connected to the Internet of Things. The history of the network is known and the security problems which still exist are visible. This paper stated a brief summary of the current IoT communication security along with the important security requirements for the future of this new era. Moreover, the paper specified the need for a new Security Layer to be added to the current IoT Communication Reference Model. The advantages of that layer may include Link and End-to-End security. Also, it may increase the throughput performance of other layers, since they will relay on the security layer for the data validation and confirmation of its sources. Furthermore, it would be very helpful for the troubleshooting designers as all problems will be gathered in one place.

REFERENCES

1. Van Kranenburg, Rob, and Alex Bassi. "IoT challenges." Communications in Mobile Computing vol. 1, no. 1, pp. 1-5, 2012.

2. Bassi, Alessandro, Martin Bauer, Martin Fiedler, Thorsten Kramp, Rob Van Kranenburg, Sebastian Lange, and Stefan Meissner. Enabling things to talk. Springer, 2013.

3. Li, Lan. "Study on security architecture in the Internet of Things." In Measurement, Information and Control (MIC), International Conference on, vol. 1, pp. 374-377. IEEE, 2012.

4. http://www.iot-a.eu/public

5. Oladayo Bello, Sherali Zeadally: Communication Issues in the Internet of Things (IoT) Springer-Verlag, London, 2013.

6. Glenn Surman: Understanding Security Using the OSI Model. SANS Institute InfoSec Reading Room, 2002.

7. Adel H. Alhamedi, Hamoud M. Aldosari, Vaclav Snasel, Ajith Abraham. "Internet of things communication reference model." Computational Aspects of Social Networks (CASoN), 6th International Conference on. IEEE, 2014.