The Framework for Authentication and Authorization for Constrained M2M Devices

Sardorjon Vakkosov, Jung-Il Namgung, Soo-Hyun Park
Ubiquitous System Lab., Graduate School of FIS,
Kookmin University, Seoul, South Korea

Abstract

M2M technology enables us to control "Things" and collect various kinds of information from "Things". M2M is defined as a technology that enables electronic and mechanical devices to communicate with each other seamlessly and perform actions without human intervention. In this paper, we review some security solutions for M2M devices and show our light weight framework which is responsible for security of constrained M2M devices. In addition to the above-mentioned ones, we propose the framework can be applied for constrained environment and give conclusion and future works.

1. Introduction

Today we are residing in a world of communication. Mass of machines and devices are connecting to one another wirelessly. Machine-to-machine (M2M) communication is viewed as one of the next frontiers in wireless communications [1]. Due to the advent of new standards for low power wireless communications and the desire for mobile operators to find new sources of revenue, it is only recently that M2M wireless communications are gaining greater attention [2].

As networked machines become more popular around our living, information security on these devices becomes an important issue [3]. Unfortunately, the nature of the complex and heterogeneous environment in M2M makes the security issues very challenging. Furthermore, most nodes are resource constraint, which makes the property of lightweight necessary for M2M security mechanisms.

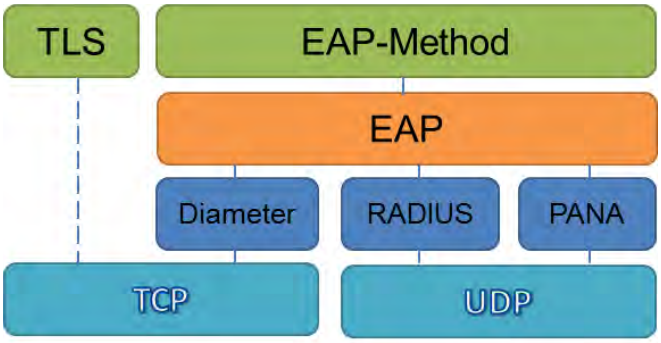
Messages from/to devices can be easily attacked if no security mechanism is used. Hence, a lightweight authentication and authorization mechanism is needed to protect the messages. Authentication and authorization are not only the crucial measures to ensure the security of the received data, but also the premises of many security services.

The remainder of this paper is organized as follows. Section II gives the related works. Proposed framework is described in Section III. Framework evaluation descried in Section IV. Finally, Section V concludes and highlights directions for future work.

2. Related Works

For some reasons M2M application is extremely convenient to attacks, especially in the constrained environment: its nodes spend most of the time unattended; and thus, the probability of physically attacking to them is high. Mostly, network communications are wireless, which makes eavesdropping extremely simple. Furthermore, most of the M2M devices are characterized by low capabilities in terms of both energy and computing resources and thus, they cannot implement complex schemes in order to support security.

Due to the reasons listed above, security is considered as the main barrier to be overcome among academia and industry in next years for a global deployment of M2M. Over recent years security problems have been solved by the extension and adaptation of protocols. Most access authentication protocols are based on Extensible Authentication Protocol (EAP). EAP is an authentication framework. It offers EAP methods in order to provide authentication. There are many EAP methods, such as: LEAP [4], EAP-TLS [5], EAP-PSK [6], EAP-AKA [7] and



(Figure 1) Secure protocol stack

Figure 1 shows secure protocol stack. EAP offers its methods in order to provide authentication. Protocols like Diameter [8], RADIUS [9], PANA [10] are the protocols that provide transferring messages related with EAP. The protocols use TCP or UDP in order to transfer their messages.

This stack has advantages for providing security but it has some disadvantages for constrained environment. In order to solve that kind of challenges vendors, standardization organizations and working groups are offering their solutions. Particularly, IETF working groups like IPv6 over Low power WPAN (6LoWPAN) and Constrained RESTful Environments (CoRE) are working on adaptation of existing protocols into constrained environment. CoRE WG proposed an application layer protocol called Constrained Application Protocol (CoAP) [11] for resource constrained devices.

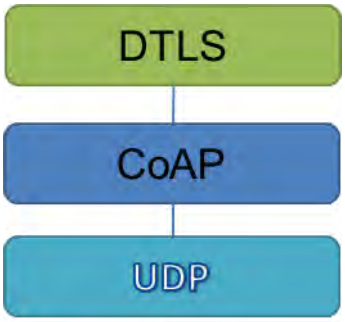
Some security threats and corresponding solutions of 3GPP are discussed in [12], but the mechanism and procedure have not yet been developed. A new group message authentication protocol has been discussed in [13]. An authentication and access control scheme for the layer

perception is given in [14]. Moreover, in [15], authors present OpenPANA and open source contribution, which implements the standard PANA. It can be used for any PANA implementation and can be applied to M2M applications. A group authentication and key agreement protocol, called EG-AKA is proposed in [16], for machine-type communications combining elliptic curve Diffie-Hellman (ECDH) based on EAP framework.

Previous works address general security solutions of M2M applications, while our work focuses on lightweight versions of security solutions for constrained environments.

3. Proposed lightweight Framework

The deployment of constrained M2M devices on uncontrolled systems results new requirements to emerge. The major problems related to security concern authentication and data integrity.



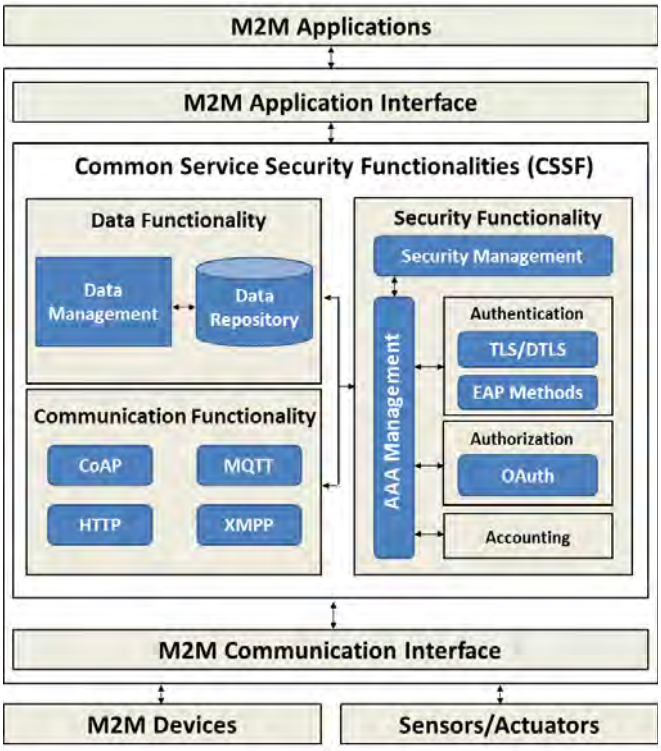
(Figure 2) Proposed protocol stack

Figure 2 shows our proposed protocol stack. The proposal is based on a simplified Datagram Transport Layer Security (DTLS) [17]. CoAP is used as an application layer protocol. This protocol, based on the same RESTful principles as HTTP, allows the realization of embedded services but accommodated to the requirements of constrained devices and networks. Finally, UDP is utilized as a transport layer protocol.

Figure 3 shows the adaptation of our proposed framework into M2M service scenarios. Our framework has been implementing OneM2M security standards and includes interface in order to deploy it M2M applications. In other words, M2M applications can utilize our Common Service Security Framework (CSSF) through M2M Application Interface. On communication stage M2M devices and Sensors/Actuators utilize different kind of networks in order to send/exchange their messages using CSSF. CSSF has M2M Communication Interface for supporting those network types.

CSSF consists of three functional components: Data Functionality, Communication Functionality and Security Functionality. Data Functionality addresses Data related activities. It is includes Data Management and Data Repository. On one hand, Data Repository is responsible for storing CSSF related data. On the other hand, Data Management offers functions concerning the stored data.

Communication Functionality component refers networking stage. While communication is being considered and analyzed it is important to choose convenient protocol.



(Figure 3) Common Service Security Framework

Security Functionality addresses safety and security of the whole system. Normally, M2M devices spend most of the time unattended. So that, the probability of the physical attacks to them is high. In order to provide security of the date stored in those devices CSSF purveys security mechanisms. Furthermore, eavesdropping to the wireless networks is not too difficult. For that reason, our framework offers lightweight solutions in order to protect communication. CSSF is designed to communicate with Communication Functionality in order to support different authentication mechanisms. Besides, it has interactions with authentication, authorization, and accounting (AAA) infrastructures.

4. Evaluation of the framework

In terms of reliability, our lightweight Common Service Security Framework provides a flexible approach, offering the lightweight authentication and authorization mechanisms, in order to keep secure communication.

Through the authentication, M2M nodes shall be verified and it will prevent eavesdropping. Besides, the framework offers OAuth-based Authorization which can be invoked by any subscribed host or M2M device. It can be thought of as a remotely triggered switch that filters incoming requests and decides whether to serve them or not. The design goal of the OAuth-based Authorization is to relieve M2M devices from handling a large amount of authorization-related information and processing all incoming requests. By outsourcing these functionalities, devices can keep their application logic as simple as possible, thus meeting the requirements for keeping the memory usage as low as possible, which is extremely important for constrained devices.

With the Real Time feature, M2M applications can

maintain a persistent real-time socket communication link between the device and the backend. Real-time communication ensures instant event notification in either direction. On one hand, supplying Real-time functionality causes increasing of network usage. On the other hand, it requires proper security mechanism. Our CSSF framework offers lightweight authentication and authorization mechanisms that make sufficient supplying Real-time functionality into constrained environment applications.

In order to verify reliability and Real-time service integration of our proposed framework we are planning to emulate effects on internal attacks compared with other security frameworks.

5. Conclusion and Future Works

The deployment of M2M applications are growing and lead the way to new business cases. It is also creating new requirements to the security solutions. The adaptation of M2M applications into constrained environment requires lightweight mechanisms because of its devices. Constrained M2M devices have low capabilities in terms of both energy and computing resources. Hence, they cannot implement complex security schemes. In this paper, we discussed related works for providing security and offer our lightweight framework. The framework proposes lightweight security mechanisms in order to embed the safety of date on constrained M2M devices and to prevent eavesdropping. Future work is focused on the adaptation of existing lightweight protocols into our framework. Specifically, CoAP protocol implementation into our test board is our next work. Furthermore, we planned to analyze other lightweight security solutions addressing other components of the proposed framework, in order to provide a comprehensive security approach for constrained M2M environment.

6. Acknowledgments

This research was supported by Department of Financial Information Security (BK21+ Future Financial Information Security Specialist Education Program Group), Kookmin University.

The work is a part of the results of the research "Development of the wide-band underwater mobile communication systems" supported by Ministry of Oceans and Fisheries, Korea.

References

[1] Inhyok Cha, Yogendra Shah, Andreas U. Schmidt, Andreas Leicher, and Michael Victor (Mike) Meyerstein, “Trust in M2M Communication”, IEEE Vehicular Technology agazine, September 2009.

[2] Berta Carballido Villaverde, Rodolfo De Paz Alberola, Antonio J. Jara, Szymon Fedor, Sajal K. Das, and Dirk Pesch, “Service Discovery Protocols for Constrained Machine-to-Machine Communications”, IEEE Communications Surveys & Tutorials, vol. 16, no. 1, First quarter 2014.

[3] Jie-Ren Shih, Yongbo Hu, Ming-Chun Hsiao, Ming-Shing Chen, Wen-Chung Shen, Bo-Yin Yang, An-Yeu Wu, Senior Member, IEEE, and Chen-Mou Cheng, “Securing M2M With Post-Quantum Public-Key Cryptography”, IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 3, no. 1, March 2013.

[4] Wenju, Liu, et al. "An analysis of the improved EAP-AKA protocol." 2010 2nd International Conference on Computer Engineering and Technology. Vol. 1. 2010.

[5] Aboba, Bernard, and Dan Simon. "Ppp eap tls authentication protocol." (1999).

[6] Bersani, Florent, and Hannes Tschofenig. "The EAP-PSK protocol: A pre-shared key extensible authentication protocol (EAP) method." (2007).

[7] Arkko, Jari, and Henry Haverinen. "Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA)." (2006).

[8] Calhoun, Pat, et al. "Diameter base protocol." *Work in Progress* (2003).

[9] Willens, Steve, et al. "Remote authentication dial in user service (RADIUS)." (2000).

[10] Forsberg, D., et al. "RFC 5191 protocol for carrying authentication for network access (PANA)." *Network Working Group* (2008).

[11] Shelby, Zach, Klaus Hartke, and Carsten Bormann. "The Constrained Application Protocol (CoAP)." (2014).

[12] 3GPP TR 33. 868 V0. 5. 0, Security aspects of Machine-Type Communications, 2011.

[13] S. Laur and S. Pasini, “Sas-based group authentication and key agreement protocols,” in Public Key Cryptography-PKC, pp. 197–213, Springer, 2008.

[14] Ye, Ning, et al. "An efficient authentication and access control scheme for perception layer of internet of things." *Int. J. Appl. Math. Inf. Sci* 8 (2014): 1617-1624.

[15] Marin-Lopez, R., and F. Vidal-Meca. "An open source implementation of the protocol for carrying authentication for network access: OpenPANA." *Network, IEEE* 28.2 (2014): 49-55.

[16] Jiang, Rong, et al. "EAP-based group authentication and key agreement protocol for machine-type communications." *International Journal of Distributed Sensor Networks* 2013 (2013).

[17] Rescorla, Eric, and Nagendra Modadugu. "Datagram transport layer security." (2006).