Journal of Scientific & Industrial Research
Vol. 78, November 2019, pp. 751-754

Authentication Phase of Security Bootstrapping in the Internet of Things Networks Based on a Trusted Zone

N Nazemi[1]* and M T Manzuri[2]

[1]Computer Engineering Department, Sharif University of Technology Tehran, Iran,

[2]Computer Engineering Department, Sharif University of Technology, Tehran, Iran

Received 23 September 2018; revised 15 May 2019; accepted 18 September 2019

Internet of Things (IoT) represents enabling all things in such a smart way that those things be accessed any time and anywhere through the Internet. Presence of IoT as a novel way of networking, opens up new concernsaround the communication and network world. A secure establishing in such a diffused network is a great concerns of the researchers. Due to Smart things' resource-constraints and power-limitation the former ways of securing networks cannot be applicable in IoT. Thus, security bootstrapping has introduced a solution for establishing security in the first instance of deploying the network. In this study, we have proposed a security bootstrapping solution which can be applied in IoT environment. This security bootstrapping focused on the authentication phase of security as a basis. Our solution is based on having a unique device identifier, which physical address was chosen. Devices can automatically introduce themselves to the router of IoT network by their unique identifier with the minimum of human intervention. Besides, we suggest that an IoT Center to be a trusted medium between the manufacturer of smart things and the buyers. Therefore, we make a connection between the router and the IoT Center.

Keywords: Internet of Things, Security Bootstrapping, Media Access Control (MAC) Address, Authentication

Introduction

Kevin Ashton was the inventor of "IoT" term in 1991. Internet of Things (IoT) has introduced the global architecture based on sharing information among things (consist of sensors, actuators and embedded communication devices) throughout the environment via Internet. The communication between these things as well as the services provided by IoT, are better to be without direct human intervention[1]. Technologies such as RFID (Radio Frequency Identification) and WSN[2] (Wireless Sensor Networks) have been considered as enabling technologies for hardware components of IoT. Cloud based storage solutions is one of the most important enabling technologies for middleware component of IoT. There are several application domains which will be impacted by the emergence of Internet of Things such as Smart Home and Public Infrastructure[3]. Content of this paper is extracted from the author's master[4] thesis which is updated and refreshed with ideas and materials that have been discovered recently and explained in related works. Following security bootstrapping part, in this section, discusses the concerns in bootstrapping and associated security which is followed by this paper's main motivation and discussing the related work in literature review. All detailed steps and concepts have been explained in materials and methods section. Result and discussion section explains the outcome and discusses the related security measurements. In final section, proposed scenario and related elements of this paper are concluded.

Security Bootstrapping

Security is an essential issue in IoT domain. The fact that the devices have limitation in communications and memory and energy consumption– they are mostly battery powered. So the security solution should[4,5]:

- Be lightweight[6] on the resources have low computing complexity (because maximum payload size of IEEE 802.15.4 is 128 bytes[7])
- Satisfy the security requirements
- Be easy-to-use and no need of human intervention
- Be able of commissioning different things from different manufacturers

*Author for Correspondence
Email: Niousha.Nazemi@alum.sharif.edu

By the reasons above, IoT proposes new way of commissioning and bootstrapping of devices, that is, deployment of devices without need of maintenance time or human intervention. So we combine authenticating and bootstrapping solution in order to implement Security Bootstrapping. Since we want to have an open attended environment, authentication is the basis of other security mechanisms, like authorization, integrity check and secure configuration, we should have a reliable device authentication method[4,6].

Literature review

To enable an efficient authentication and bootstrapping process, the secure bootstrapping mechanism of the IETF 6TiSCH protocol faced an extension by[5] in a way that authentication keys are distributed within the trusted nodes that authenticate themselves through a joint proxy/helper to a centralized entity that enables Join Registrar/Coordinator (JRC) authentication that concludes a zero-touch authentication mechanism for IoT devices bootstrapping as a part of IETF 6TiSCH target. A new ECQV certificate issuance protocol is proposed in[8] that identifies the security issues of the former PAuth Key protocol. Integrating into the secure join protocol of the IEEE 802.15.4 that a Cryptographically Generated Address (CGA) is used for security bootstrapping to obtain the MAC address of smart objects from its ECDH public key to secure the ally and certificate issuance protocol which is the basis of the protocol design.

Motivation

Since the smart things are mostly headless (without any monitor or keyboard as an interface) using a secured method of bootstrapping and managing the things centrally with minimum user interaction outlines our research goal.

Materials and methods

Our scenario has seven steps. First step is sending beacon frames by Pan Coordinator (Edge router). Second step is connecting to the network by the smart things. In third step edge router receives the MAC address and creates an array, made of combination of hashed MAC addresses of devices and national code of device owner. Then edge router sends them to the IoT center. The fourth step is processing of each request by IoT Center Web-service. IoT center finds the manufacturer of the device by checking first six digits of its MAC address. The fifth step is fulfillment of each request by each vendor site. During this step the vendor checks its CRM (Customer Relationship Management) database. The sixth step is transmitting vendor web service response to edge router by IoT center. The seventh step is allocating IP to the devices by the edge router. Fig. 1 shows the diagram of Business Processing Model and Notation (BPMN) of the proposed method.

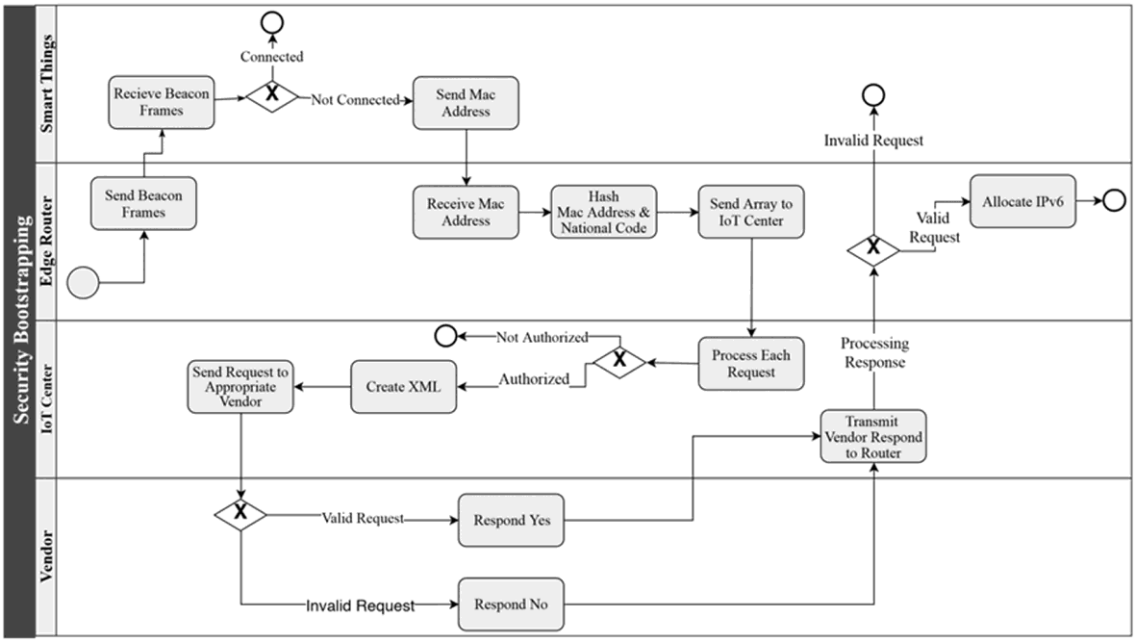

Fig. 1 — BPMN Model of the Proposed Method

Results and Discussion

Our solution includes three components: Router, IoT Center and Smart Things. We have chosen raspberry pi as router of scenario and implemented 6 Low PAN boarder router in it, in order to be interfaced between our IPv6 Network (for example, Smart Home or any IoT environment) and Internet. Raspberry pi as a cost efficient and small size computer, has been known recently and is highly recommended for implementing IoT scenarios. In our project we have used Pi 3 board in model B. According to our scenario, end user should register themselves once only in IoT Center website, in order to join the service. We have assumed that there are some vendors who joined IoT center. So they have the sale's information of each user in the DB of their CRM. On the other hand, end user has entered their National code in the router, for example national code of '0032957306' has been entered from customer A. Customer A has bought a device by MAC address 80:e6:50:1f:a6:d4. In first step, smart things send their MAC address to the router in order to make our scenario possible and whereas we have no real things, we've developed a test-page which simulates MAC address in it. The MAC addresses, which are the transmitted MAC addresses by the smart things around the edge router, in this page will be forwarded to the router. User A places their new device near the router and expects their device joins the network automatically. In second step, router sends the MAC address and the national code which is set in their configuration. we see the function that takes place in the router, calls the server .php file of the web-service of IoT Center. In the code snippet in Fig. 2, IoT center web-service receives the MAC address and national ID. It looks for the brand name of the device (according to the first 6bits of a MAC address which determines the company name) and then check whether that company is one of the members of the IoT center. Next, It finds the related brand web-service and forwards the message including MAC and national code. We have chosen apple as one of the Vendors which the stated MAC addresses were sent to it, in the CRM Data Base of Apple Company, operation of verifying the 'MAC-national code' combination is checked. Then company web-service sends its result to the IoT Center server, IoT center forwards the massage to the router. Fig. 2 presents the result of process. As it is shown, at the end, the only MAC address which was allocated to user A got IP address. The first IP address is router's IP. Other received MAC addresses got NULL reply, that is, they weren't allowed to join the network.

Security Measurement

Communicating between the web services, happens by secure cryptographic algorithm named TLS/SSL (Transport Layer Security/ Secure Sockets Layer). We

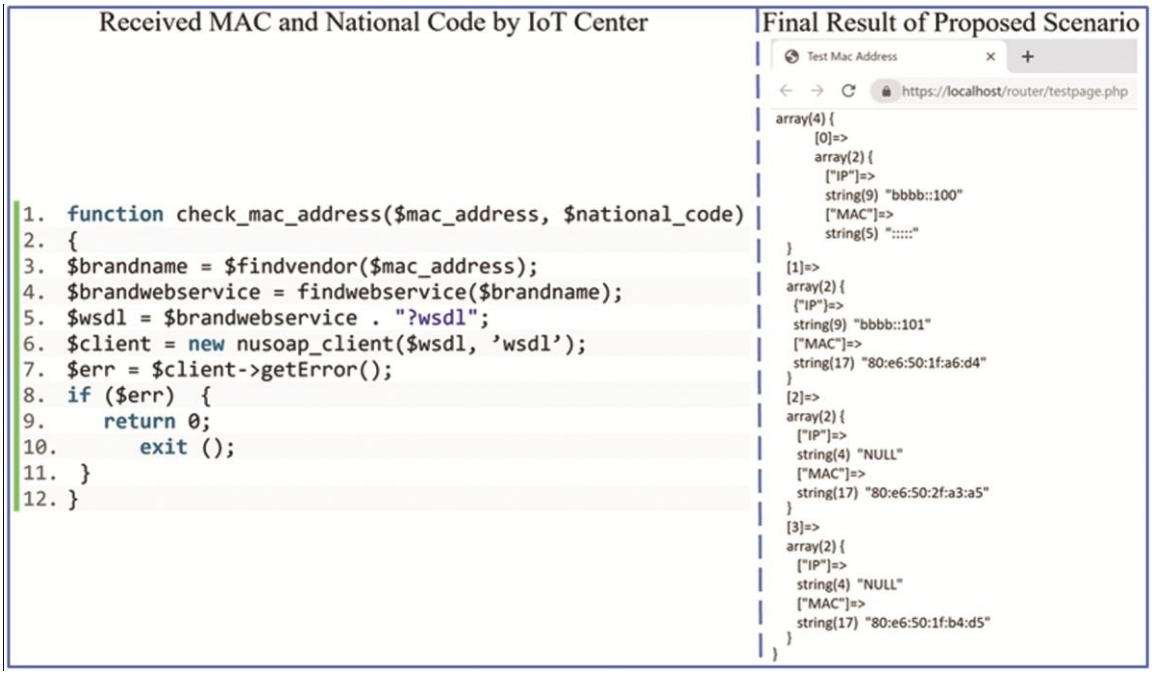

Fig. 2 — Received MAC and National Code by IoT Center, andFinal Result of Proposed Scenario

used TLS1.2 and SSL3.0 in our project. TLS/SSL provides privacy and data integrity between two communicating computer or between a client and a server. In our scenario in each level of communication, the one which calls the web- service is client and the one replies, is the server. Using TLS/SSL helps us prevent man-in-the-middle attack (the type of attacks used for eavesdropping) and also makes the reliable connection by using the message authentication code.

Conclusions

The present study tries to improve the security bootstrapping of smart things in IoT by implementing the security policy in the second layer, that is link layer. Our proposed scenario has four main elements which includes Smart things intend to connect to network, edge router transfers securely and keeps the sensitive information confidential from smart things to the IoT Center which is approved by both side of vendors and customer. It processes data and determines proper vendor site then calls their web services and vendor portal that is responsible for checking validation of request by its CRM databases. We use combination of the MAC address of smart things and national ID of the smart things' owner for our authentication method in Vendor portal. In considering of what was explained in the study about the good features of a security bootstrapping solution our proposed method is having the minimum load on the sensors. All to be done by a sensor is only sending its MAC address and it didn't involve in process of authenticating. The solution is easy-to-use from end-user perspective. All the owners have to do is registering themselves in the IoT Center website and everything else will be done automatically. The type of smart thing does not matter in our solution. Any device from any manufacturer can be authenticated through this method. The only requirement is joining the company to the IoT Center Service. In addition, the logic behind our scenario is the Unique ID of device and Unique ID of owner. Then, changing the Unique ID of device from MAC address to any other unique identifier could be applied to our scenario and having a UID of a device which is standard and globally accepted by all manufacturers would not be a concern.

Acknowledgements

We would like to thank DSP Laboratory (seehttp://dspl.ce.sharif.edu/) at Sharif University of Technology for providing equipment and required tools, Dr. Tajgardoon for his expert advice, Mr. Sajjad Meshki for his technical assistance and Mr. Soroush Jafari for his insightful comments and support throughout this work.

References

1 Schoder D, in Internet of Things A to Z: Technologies and Applications, edited by Q F Hassan (John Wiley & Sons, Hobokon) 2018, 1-50.

2 Parwekar P and Rodda S, Localization of sensors by base station in wireless sensor networks, *J Sci Ind Res*, **77**(2018)83-86.

3 Asghar M H, Negi A & Mohammadzadeh N, Principle application and vision in internet of things (IoT), in Int Conf on Comput Commun & Auto (IEEE, Noida) 15-16 May 2015.

4 Nazemi N, Simulation and evaluation of the security sub-layer for IoT, MSc Thesis, Sharif University of Technology International Campus, Kish Island, Iran, 2016.

5 Aydin H, Goermues S & J in Y, A distributed user authentication mechanism for IETF 6TiSCH protocol, in 87thVeh Technol Conf Spr (IEEE, Porto) 3-6 June 2018.

6 Devi L, Shantharajah S P and Kumar A N, Authenticated and security maintenance in wireless sensor network by filtering injected false data, *J Sci Ind Res*, **75**(2016)713-719.

7 Nagarajan R and Dhanasekaran R, Fault-tolerant wireless communication system for process control in wind power stations, *J Sci Ind Res*, **75**(2016)51-55.

8 Park C, A secure and efficient ECQV implicit certificate issuance protocol for the internet of things applications, *IEEE Sens J*, **17**(2017)2215-2223.