Securing IoT Platforms

Soumya Kanti Datta and Christian Bonnet
Communication Systems Department, EURECOM, Sophia Antipolis, France
Emails - {dattas,bonnet}@eurecom.fr

***Abstract*— Ensuring adequate security features for the Internet of Things (IoT) Platforms is often challenging. This paper focuses mechanisms to engineer authentication, authorization, and trust among the IoT Platform elements. JSON Web Token (JWT) based authentication and authorization are described. Trust is established by mutual certificate based authentication. We have shown how these security features have been incorporated in the EURECOM IoT Platform.**

I. INTRODUCTION

With a rapid rise of use of sensors in our daily lives, security risks pertaining to the Internet of Things (IoT) are also continuously growing and changing [1]. Cyber criminals are able to take possession of poorly secured IoT devices, turn them into Botnets, and launch massive Distributed Denial of Service (DDoS) attacks. The goal of this paper is to describe the security mechanisms adopted in our EURECOM IoT Platform[1]. It has evolved from a monolithic, IoT gateway centric architecture [2] to a secure, end-to-end architecture with multiple Human Machine Interfaces (HMI) (shown in Fig. 1). The Cloud infrastructure hosts the IoT common service functions (CSFs) [3] which are deployed as loosely-coupled microservices. An Edge Server provides functionalities like local data validation, processing, and actuation. The north interface of the Cloud interacts with client applications through a web-based dashboard and an Android application through HTTP and MQTT protocol bindings. Meanwhile the south interface interacts with the IoT devices and the Edge Server over HTTP only.

Among the many security properties, this paper focuses on authentication, authorization, and trust [4], [5] aspects of the IoT Platforms.

II. JWT BASED AUTHENTICATION AND AUTHORIZATION

Two primary security and access control concerns relate to authentication and authorization. Although they are well studied aspects, this paper proposes to utilize the relatively new JSON Web Token (JWT)[2] based authentication and authorization. The IoT devices as well as client applications must authenticate themselves in order to receive a JWT. All successive interaction with the IoT Platform must include the JWT in "x-access-token" header of HTTP and the communications must take place over HTTPS.

Since the Cloud based web services are deployed as microservices, initially NGINX was utilized as the default entry point to the Cloud. But since NGINX is a reverse proxy,

[1] https://iotplatform.eurecom.fr/
[2] https://jwt.io/

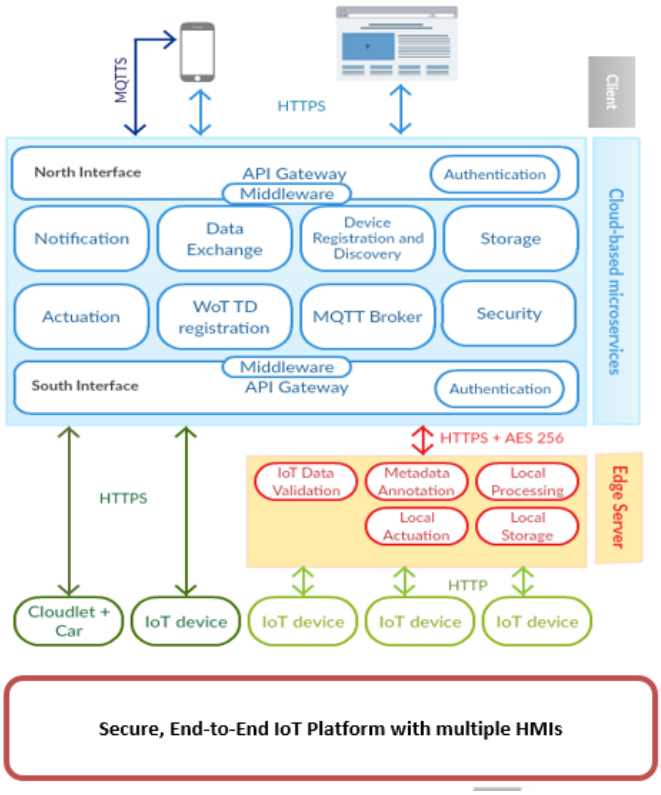

Fig. 1. EURECOM IoT Platform architecture.

it can only analyze the path of the web service to which a GET or POST request is made. But authentication must be performed before a client application or an IoT device can be authorized to access any protected resources (e.g. web services or database). NGINX does not support adding authentication feature and adding that to all microservices would not be an optimized solution. Thus, the EURECOM IoT Platform utilizes the API Gateway which provides the same functionalities as the reverse proxy but allows adding (i) authentication service for clients to obtain the JWT, and (ii) a middleware which validates the JWT (token-based authentication and authorization) before the incoming request is routed to the appropriate web service. The generated JWT for a successful authentication is stored in a Cloud database to keep a record of valid tokens. Each of the generated tokens are valid until the client has logged-out or the token has expired. The database blacklists such invalid tokens. Following JSON based schema is utilized when saving a

token in the database (Fig. 2).

```
{
token:
        {type: String, unique: true, required: true},
        token_id: {type: String, unique: true, required: true},
        user  id: {type: String},
        device_id: {type: String},
        blacklist: {type: String, required: true}
}
```

Fig. 2. JSON based schema used for JWT database.

The above schema contains the token string, the token unique id with a specification of the id either of the client application or the IoT device. The blacklist attribute is added to the invalid tokens. This attribute also protects the IoT Platforms resources against hijacked tokens. The steps for authentication and middleware-based checks for JWT are shown in Fig. 3.

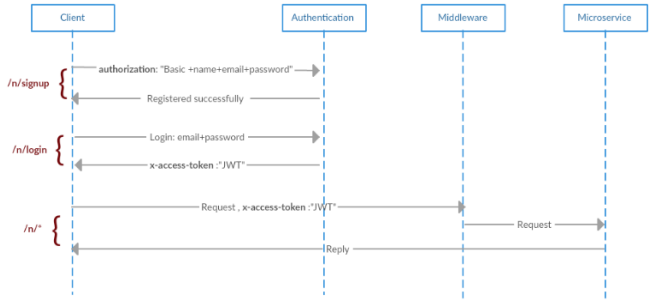

Fig. 3. Steps for authentication.

III. Trust Among IoT Platform Elements

The IoT Platforms in general connect several IoT devices as well as 3rd-party client applications. Thus there is a strong need to establish trust among the IoT Platform elements to know with certainty that data exchange happens among trusted elements. SSL/TLS provides a mechanism to establish the trust using mutual certificate based authentication. In a two-way, mutual SSL authentication, the IoT device or a client application first verifies the identify of the IoT Platform and vice-versa. This is presented in Fig. 4. Establishing the secure connection channel for data exchange using this method requires the following six steps - (i) a client (e.g. application or IoT device) requests access to a protected resource, (ii) the server (the IoT Platform in this case) presents its SSL certificate to the client, (iii) the client verifies the server's SSL certificate, (iv) if the previous verification

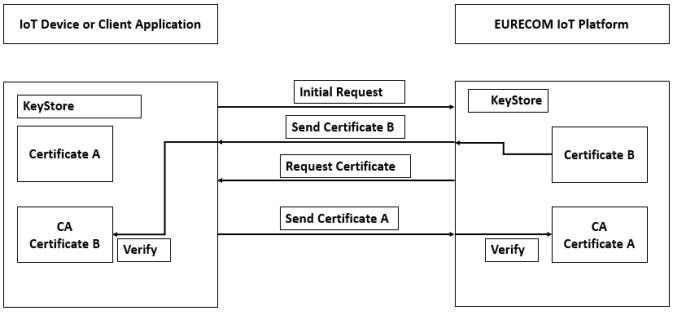

Fig. 4. Mutual certificate based authentication.

is successful, the client then sends its SSL certificate to the server, (v) it verifies the received certificate, and (vi) if the last verification is successful, the server allows access to the protected resource as requested by the client.

The EURECOM IoT Platform has a SSL certificate issued by Terena with a well known Certificate Authority. But the IoT devices connected to the Platform are installed with Self-Signed Certificate.

IV. Conclusion

In a nutshell, the paper discusses two important security factors for the IoT Platforms and how they are implemented in the EURECOM IoT Platform. The mechanisms described in this paper are replicable which can ease their adoptions across the IoT ecosystems. As for future work, we are implementing other security and privacy features suggested in OWASP IoT project.

Acknowledgment

This work is supported by AFA SCHEIF Project. EURECOM acknowledges the support of its industrial members, namely, BMW Group, IABG, Monaco Telecom, Orange, SAP, and Symantec.

References

[1] S. K. Datta and C. Bonnet, "Securing datatweet iot architecture elements," in *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, pp. 1–3, Oct 2016.

[2] S. K. Datta, C. Bonnet, and N. Nikaein, "An iot gateway centric architecture to provide novel m2m services," in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 514–519, March 2014.

[3] J. Swetina, G. Lu, P. Jacobs, F. Ennesser, and J. Song, "Toward a standardized common m2m service layer platform: Introduction to onem2m," *IEEE Wireless Communications*, vol. 21, pp. 20–26, June 2014.

[4] S. Prez, J. A. Martnez, A. F. Skarmeta, M. Mateus, B. Almeida, and P. Mal, "Armour: Large-scale experiments for iot security amp; trust," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 553–558, Dec 2016.

[5] F. D. Hudson, "Enabling trust and security: Tippss for iot," *IT Professional*, vol. 20, pp. 15–18, Mar 2018.