Securing DataTweet IoT Architecture Elements

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

***Abstract*—Security and privacy are two of the most important aspects driving the consumer adoption of the Internet of Things (IoT) based products. In our previous works, we have introduced a data-driven IoT architecture known as DataTweet. This paper examines how to secure DataTweet IoT architecture elements. The contribution of the paper is in – (i) introducing a security framework into DataTweet IoT architecture and (ii) protect IoT data and thing metadata to preserve consumer privacy.**

Keywords—Internet of Things; Privacy; Security.

I. Introduction

The Internet of Things (IoT) paradigm is set to connect around 30-50 Billion of physical devices creating an enormous ecosystem. The "always connected" devices will generate huge quantity of data about our homes, power consumption, environment, physical conditions, mobility pattern and much more. Smart and secure treatment of the raw data can produce high level intelligence which allows consumer of the IoT products and services to take intelligent decision and react to the surroundings. Unprotected treatment of the data can potentially compromise consumer privacy. At the same time, the inexpensive devices can be used to control high value assets in a smart manufacturing unit or equipments in industrial IoT scenario. IoT services expose such devices or things, their interfaces, generated data and means to communicate and control to the Internet and web. Several academic and industrial studies have pointed out the vulnerabilities and insecure products[1] and services found in IoT ecosystems[2]. The cross-domain nature of IoT further complicates security concerns. For cross-domain and cross-platform interactions, there are no single vendor or provider who develops and maintains all hardware and software security components used in IoT. Therefore, establishing a security framework to cover vertical as well as horizontal IoT scenarios is challenging both in research and engineering terms.

Recently, the IEEE IoT Initiative[3], AGILE IoT[4] and Eclipse IoT Working Group[5] conducted a developer survey [1] which revealed that the top three developer concerns are security, interoperability and connectivity. This establishes security, privacy and trust as top concerns of the IoT ecosystems. Standard Development Organizations (SDO) and IoT alliances around the world are focusing their efforts on securing the ecosystem.

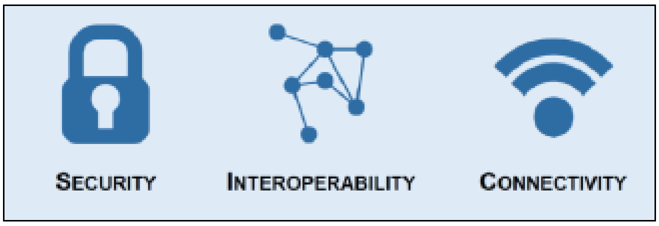

Fig. 1. Top three concerns of IoT developers.

Previously, we have introduced a generic and data driven IoT architecture (shown in Figure 2) called DataTweet [2]. The data centric approach is effective to combat the issues related to fragmentation and data silos in the ecosystem. Under this mechanism, we study the IoT data cycle (data generation, communication, processing & storage, consumption and actuation). The overall vision is to explore ubiquitous and consumer centric IoT services. The DataTweet architecture is flexible, scalable and generic enough to support a multitude of scenarios including (i) mobile crowd sensing for smart cities [3], (ii) integration of connected vehicles & intelligent transportation systems (ITS) [4] and (iii) personalized healthcare in smart homes leading to ambient assisted living (AAL) [5]. So far we have investigated the interoperability and connectivity aspects of the Figure 1 with access control functions to restrict the usage to authorized consumers.

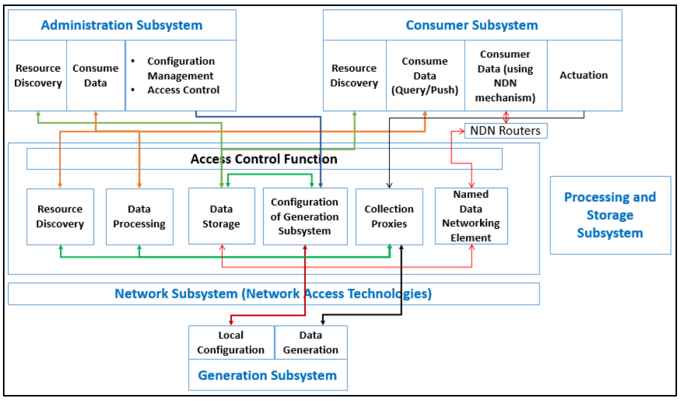

Fig. 2. DataTweet IoT architecture and its elements.

In this paper, the several security aspects of the architecture are studied. A security framework is integrated into the DataTweet architecture securing the elements as well as protecting the IoT data. The main contributions of the paper are – (i) identification of the security concerns, (ii) securing DataTweet elements, (iii) protect IoT data throughout the different stages of operation (of the IoT data cycle) and (iv) integrating a novel security framework.

[1] http://www.kaspersky.com/about/news/virus/2015/Kaspersky-Lab-Researcher-Discovers-Security-Issue-in-His-Fitness-Wristband
[2] http://www.forbes.com/sites/moorinsights/2015/09/15/the-internet-of-insecure-things
[3] iot.ieee.org
[4] http://agile-iot.eu/
[5] https://www.eclipse.org/org/workinggroups/m2miwg_charter.php

Rest of the paper is organized as follows. Section II addresses the security concerns, the mechanisms to secure DataTweet elements and IoT data. Section III describes combining the mechanisms into a security framework and integrating it into DataTweet architecture. The new architecture thus addresses all the top three concerns of Figure 1. Finally, Section IV concludes the paper.

II. Securing DataTweet Elements

This section highlights the mechanisms undertaken to secure the subsystems of the architecture and their elements.

A. Generation Subsystem

It includes things (sensors and actuators) which generate sensing data and react to the environment based on commands. The things belong to a wide range of domains including home automation, healthcare, fitness and automotive. In turn they generate data about consumers, their surroundings, habits, locations etc. For generation subsystem (GS), we propose to secure the sensor metadata content that is transmitted to the processing and storage subsystem (PSS). DataTweet proposes a data centric architecture and services which are independent of the infrastructure. This leads us to assume that a secure communication link may not be always available between the GS and PSS. Following a secure bootstrapping, the security keys to encrypt raw sensor metadata are shared. Similarly, for actuation, encrypted instructions are sent from the PSS to GS over the same interface. The mentioned keys are generated and exchanged following Elliptic Curve Cryptography (ECC).

The local configuration of the GS can also be updated through the secure bootstrapping. Authorized users (as determined by the access control function in the PSS) are allowed to update the configuration details of GS.

Therefore, on the GS we introduce a secure bootstrapping element to configure encryption keys and local configuration.

B. Processing and Storage Subsystem

The PSS includes functional elements to allow resource discovery [6], data processing [7], data storage, collection proxy [8], configuring GS and Named Data Networking (NDN) element [9]. We discuss the security mechanisms adopted for each element.

1) Resource Discovery

Authorization and authentication based attempts to make resource discovery secure has been studied in [10], [11]. To restrict unauthenticated devices from registering and being discovered, thing authentication and access control systems should be incorporated. ECC is used for security key generation, exchange as well as encryption and decryption of discovery metadata exchange. For access control (AC) RBAC is utilized. As an alternative, we can also use DCapBac [14] that enforces capability based access control rules before things and their metadata are accessed.

2) Secure Data Management and Storage in IoT

For the data management part, the fundamental principles for information security must be incorporated. Confidentiality ensures privacy of data generated at GS as well as the high level intelligence derived at the data processing unit of PSS. Integrity protects IoT data from being changed by unauthorized users and/or things. This is particularly applied to actuators. Integrity of commands sent to actuators must be ensured otherwise critical infrastructure can be damaged. Similarly, sensor configuration details are important for enabling resource discovery and automatic management of GS components. Integrity of the Availability of IoT data from PSS data storage unit is necessary especially in real time and emergency situations. These three principles are the main security requirement for the data and configuration management [12] and local storage in PSS. It allows external consumers to access the functionalities through web services and APIs. The external security threats can range from unauthorized data access & modification, unauthorized actuator control to denial of service attack. To address these challenges, we need security mechanisms to support link access control, encryption, integrity measures and detection and prevention of DoS attacks [15], [16] embedded into PSS.

3) Collection Proxies

The collection proxies assist PSS in communicating with GS over different communication technologies and protocols. Our current architecture allows HTTP and CoAP based communication with SenML protocol being used for sensor and actuator metadata transfer and CoRE Link Format for exchanging GS configuration. But the communication link is not secure which makes it vulnerable to a variety of attacks including compromise of integrity and Man-in-the-Middle attack. To secure the collection proxies is, lightweight and secure CoAP [13] is integrated at both PSS and GSS.

4) Data Dissemination

Depending on the consumer and administrative subsystems requirement, PSS may disseminate raw data coming from GS or the derived intelligence from local data storage. We utilize named data networking (NDN) philosophy which includes security components like signature (hash function, digest) and signed information (publisher ID, key locator).

III. DataTweet Security Framework

Based on the identification of security concerns in previous section and mechanisms to secure the subsystem components, we look into creating DataTweet security framework. It is integrated with the original architecture and is depicted at Figure 3.

When a GS comprising of sensor/actuator is connecting to the PSS for the first time, the secure provisioning takes place. Open Mobile Alliance Lightweight M2M Technical Specifications describe an industry agreed method on secure provisioning. It is used to exchange keys. Following that, encrypted sensor metadata and actuation instructions are exchanged over secure CoAP. This ensures security of the communication protocol and data.

In PSS, the same secure provisioning element utilizes ECC mechanisms for key generation and exchange. This is at the south interface that handles the communication with physical things. The north interface takes care of the interaction with administration and consumer subsystems and employs authentication and authorization tools leading to strict access control. Additionally, the local storage of PSS is secured. The administration subsystem (AS) determines the policies for access control, secure provision (at south interface) and configuration. The CS is runs on Android powered smartphones and is provided with authentication tokens necessary for resource discovery and then consuming data & actuation. The data dissemination with NDN elements [9] has its own security mechanisms in-built.

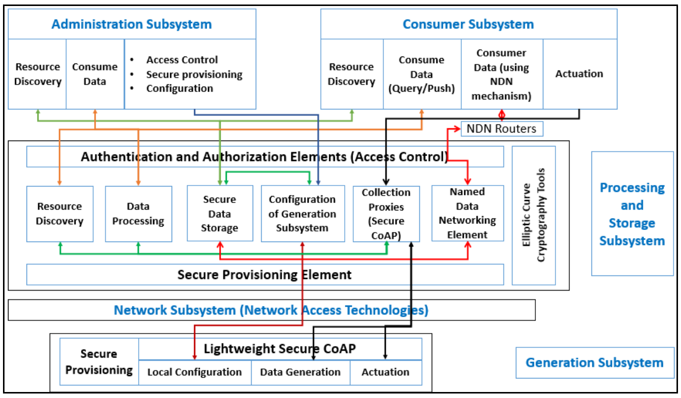
Administration Subsystem
Resource Discovery
Consume Data
Access Control
Secure provisioning
Configuration
Consumer Subsystem
Resource Discovery
Consume Data (Query/Push)
Consumer Data (using NDN mechanism)
Actuation
NDN Routers
Authentication and Authorization Elements (Access Control)
Resource Discovery
Data Processing
Secure Data Storage
Configuration of Generation Subsystem
Collection Proxies (Secure CoAP)
Named Data Networking Element
Elliptic Curve Cryptography Tools
Processing and Storage Subsystem
Secure Provisioning Element
Network Subsystem (Network Access Technologies)
Secure Provisioning
Lightweight Secure CoAP
Local Configuration
Data Generation
Actuation
Generation Subsystem

Fig. 3. DataTweet IoT architecture and its elements.

IV. Conclusion

The essence of ubiquity coupled with horizontal nature of IoT pose many challenges in terms of security, privacy, trust and reliability. Physical things used many IoT scenarios are not protected by conventional firewalls which increase probability of being compromised. The cross platform interaction in IoT ecosystem further challenges security. This paper presents the approach taken to study the security concerns of DataTweet IoT architecture elements. Since we focus on a data centric approach, we have integrated mechanisms to secure resource discovery, IoT data and configuration of things as well as the data communication protocols. Strict access control is in place to restrict the access to IoT data, thing metadata and other services to authorized consumers. All the security components are integrated into the DataTweet architecture as parts of the security framework. This successfully embeds security elements into the DataTweet IoT architecture to protect consumer privacy. As future work, we are investigating how to prevent DoS attack against DataTweet.

Acknowledgment

This work is supported by French research project DataTweet (ANR-13-INFR-0008).

References

[1] IoT Developer Survey, April 2016 available at - http://iot.ieee.org/images/files/pdf/iot-developer-survey-2016-report-final.pdf

[2] S. K. Datta, C. Bonnet, R. P. Ferreira da Costa and J. Haerri, "DataTweet: An Architecture Enabling Data-Centric IoT Services," IEEE Region 10 Symposium (Tensymp), 2016, Bali.

[3] S. K. Datta, R. P. Ferreira da Costa, C. Bonnet, and J. Haerri, "oneM2M Architecture Based IoT Framework for Mobile Crowd Sensing in Smart Cities," European Conference on Networks and Communications (EUCNC), 2016 25th, Athens, 2016.

[4] S. K. Datta, R. P. Ferreira da Costa, J. Haerri and C. Bonnet, "Integrating Connected Vehicles in Internet of Things Ecosystems: Challenges and Solutions," International Workshop on Smart Vehicles: Connectivity Technologies and ITS Applications (SmartVehicles), 2016 3rd, Coimbra, 2016.

[5] S. K. Datta, C. Bonnet, A. Gyrard, R. P. Ferreira da Costa and K. Boudaoud, "Applying Internet of Things for personalized healthcare in smart homes," Wireless and Optical Communication Conference (WOCC), 2015 24th, Taipei, 2015, pp. 164-169.

[6] S. K. Datta, R. P. F. Da Costa and C. Bonnet, "Resource discovery in Internet of Things: Current trends and future standardization aspects," Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, Milan, 2015, pp. 542-547.

[7] A. Gyrard, S. K. Datta, C. Bonnet and K. Boudaoud, "Cross-Domain Internet of Things Application Development: M3 Framework and Evaluation," Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on, Rome, 2015, pp. 9-16.

[8] S. K. Datta, C. Bonnet and N. Nikaein, "An IoT gateway centric architecture to provide novel M2M services," Internet of Things (WF-IoT), 2014 IEEE World Forum on, Seoul, 2014, pp. 514-519.

[9] S. K. Datta and C. Bonnet, "Integrating Named Data Networking in Internet of Things Architecture," Consumer Electronics-Taiwan (ICCE-TW), 2016 IEEE International Conference on, Nantou, 2016.

[10] P. P. Pereira, J. Eliasson and J. Delsing, "An authentication and access control framework for CoAP-based Internet of Things," IECON 2014 - 40th Annual Conference of the IEEE Industrial Electronics Society, Dallas, TX, 2014, pp. 5293-5299.

[11] S. K. Datta, "Towards securing discovery services in Internet of Things," 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, 2016, pp. 506-507.

[12] J. M. Bohli, A. Skarmeta, M. Victoria Moreno, D. García and P. Langendörfer, "SMARTIE project: Secure IoT data management for smart cities," Recent Advances in Internet of Things (RIoT), 2015 International Conference on, Singapore, 2015, pp. 1-6.

[13] S. Raza, H. Shafagh, K. Hewage, R. Hummen and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," in IEEE Sensors Journal, vol. 13, no. 10, pp. 3711-3720, Oct. 2013.

[14] Jose L. Hernandez, Antonio J. Jara, Leandro Marinc and Antonio F. Skarmeta G6meza. DCapBAC: Embedding Authorization logic into Smart Things through ECC optimizations. International Journal of Computer Mathematics, 1-22,2014.

[15] A. Arış, S. F. Oktuğ and S. B. Ö Yalçın, "Internet-of-Things security: Denial of service attacks," 2015 23nd Signal Processing and Communications Applications Conference (SIU), Malatya, 2015, pp. 903-906.

[16] P. Kasinathan, C. Pastrone, M. A. Spirito and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, 2013, pp. 600-607.