Security Education in the IoT Reference Architecture

Evelina Pencheva
The author is with the Faculty of Telecommunications, Technical University of Sofia, Kl. Ohridski 8, 1000 Sofia
Bulgaria
iia@tu-sofia.bg

ABSTRACT: *This work has addressed the security education in the Internet of Things. It describes the communication between one to other device and service access issues. The limitations in web services have impact on the security aspects of IoT. The newer security functions are discussed with a functional system of IoT reference architecture. The mutual authentication and service agreement signing are explained further.*

Keywords: Internet of Thing, Reference Architectural Model, constrained Web Services, security, privacy

Received: 12 Janaury 2022, Revised 10 March 2022, Accepted 28 March 2022

DOI: 10.6025/isej/2022/9/1/1-7

1. Introduction

Internet of Things (IoT) is defined as a network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. Th infrastructure is based internet evolution and network developments. It offers specific object identification, sensor and connectivity capabilities as a basis for development of independent federated services and applications. Services are expected to feature a high degree of autonomous data capture, transfer event network connectivity and interoperability [1], [2], [3].

One of the most challenging topics in such an interconnected world of objects including systems, sensors and services are security and privacy aspects. Without confidence that safety of private information is assured and adequate security is provided, users will be unwilling to adopt the IoT technology that invisibly integrates into their environment and life [4], [5].

IoT security features diverse challenges. Heterogeneous interactions in IoT include different communication patterns such as: human-to-human, human-to-thing, thing-to-thing, or thing-to-things. Communication protocols that enable information exchange between devices and users must provide integrity, authenticity, and confidentiality at different layers [6]. While the confidentiality of data captured from the physical world and represented in the digital world may rely on communication infrastructure, sensor privacy mainly targets the physical world [7]. Actuators execute actions in the physical world triggered in the digital world and the integrity, authenticity, and confidentiality of data sent to an actuator mostly depend on communication security, while the privacy on actuators is highly specific to the scenario [8]. Moreover, security mechanisms for storage device must be extended to provide adequate protection of user privacy [9].

Confidentiality and integrity of devices for interaction with humans in the physical world must insure that no third party has access to the device internal data and that device privacy depends on communication privacy [10]. Integrity and authenticity of processing that provide data mining and service are based on device and communication integrity and on the correct design and implementation of the respective algorithms [11]. Localization and tracking are required to mange the mobility of the physical world. Identities provide unique physical object identification in the digital world. While the authenticity of these functions depends on the communication authenticity and device integrity, the confidentiality in this context features high sensitivity [12].

Services and applications security spans on different perspectives. It covers information, functional, operational and deployment views [13]. Access policies can accompany service description and information about services and software components must be hidden or made anonymous in order to protect the service provider privacy. Security related functions need to be implemented to manage the above mentioned issues. IoT system operation and deployment should follow specific best practices [14], [15].

The aim of the research is to analyze existing solutions for security functions concerning IoT service and application and to suggest some enhancements to the IoT Reference functional model [16].

The paper is structured as follows. In Section 2, related works in the area of IoT service security are discussed. Section 3 presents the new security functions in the IoT Reference functional model that extend the authentication in service discovery and add service selection supplement service agreement. The conclusion summarizes the contribution.

2. Related Works

Things in Internet of Things may be regarded as interconnected nodes in a Building Automation Control (BAC) system. The nodes vary in functionality and usually are constrained devices demanding low energy consumption.

Multiple control protocols for the IoT are developed. Key roles for BAC systems play the ZigBee standard [17], BACNet [18], or DALI [19]. Due to requirement for Internet Protocol (IP) connectivity the focus is on an all-IP approach for system control. Nowadays, the standardization activities are focused on design of new protocols for resource constrained networks of smart things. The 6LoWPAN standardization work includes definitions of methods and protocols for the efficient transmission and adaptation of IPv6 packets over IEEE 802.15.4 networks [20]. A framework for resource-oriented applications running on constrained IP network is developed in [21]. A lightweight version of the HTTP protocol, the Constrained Application Protocol (CoAP), uses UDP services and enables efficient applicationlevel communication for things [22].

IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) require simple service discovery network protocols to discover, control and maintain services provided by devices [20]. 6LoWPAN applications often require confidentiality and integrity protection. This can be provided at the application, transport, network, and/or at the link layer. Given the constraints, first, a threat model for 6LoWPAN devices needs to be developed in order to weigh any risks against the cost of their mitigations while making meaningful assumptions and simplifications. Some examples for threats that should be considered are man-in-the-middle attacks and denial of service attacks. A separate set of security considerations applies to bootstrapping a 6LoWPAN device into the network (e.g., for initial key establishment). This generally involves application level exchanges or out-of-band techniques for the initial key establishment, and may rely on application-specific trust models. Beyond initial key establishment, different protocols (TLS, IKE/IPsec, etc.) for subsequent key management as well as to secure the data traffic must be evaluated in light of the 6LoWPAN constraints. One argument for using link layer security is that most IEEE 802.15.4 devices already have support for Advanced Encryption Standard (AES) link-layer security. For network layer security, two models are applicable: end-to-end security, e.g., using IPsec transport mode, or security that is limited to the wireless portion of the network, e.g., using a security gateway and IPsec tunnel mode. The disadvantage of the latter is the larger header size, which is significant at the 6LoWPAN frame messages. To simplify 6LoWPAN implementations, it is beneficial to identify the relevant security model, and to identify a preferred set of cipher suites that are appropriate given the constraints.

Constrained RESTful Environments (CoRE) Link Format defines Web Linking using a link format by constrained web servers to describe hosted resources, their attributes, and other relationships between links [21]. The CoRE Link Format can be used by a server to register resources with a resource directory or to allow a resource directory to poll for resources. Based on the HTTP Link Header field, the CoRE Link Format is carried as a payload and is assigned an Internet media type. "RESTful" refers to the Representational State Transfer (REST) architecture. A well-known URI is defined as a default entry point for requesting the links hosted by a server.

The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks [22]. The nodes often have 8- bit microcontrollers with small amounts of ROM and RAM, while constrained networks such as 6LoWPAN often have high packet error rates and a typical throughput of tens of kbit/s. The protocol is designed for device-to-device applications and provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP easily interfaces with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead and simplicity for constrained environments.

Host Identity Protocol Diet EXchange (HIP DEX) is a variant of the HIP Base EXchange (HIP BEX) specifically designed to use as few crypto primitives as possible yet still delivering the same class of security features as HIP BEX [23]. The design goal of HIP DEX is to be usable by sensor devices that are code and processor constrained. Like HIP BEX it is expected to be used together with another suitable security protocol, such as the Encapsulated Security Payload. HIP DEX can also be used directly as a keying mechanism for a MAC layer security protocol as it is supported by IEEE 802.15.4.

Security features and components are well defined in IoT Reference Architecture [16]. Layering approach is adopted to describe communication security and service security which are foundation for IoT service access and resolution service. Resolution is a service by which a given identification is associated with a set of addresses of information services and interaction services. Information services allow querying, charging and adding information about the thing in question, while interaction service enable direct interaction with the thing by accessing software resources of the associated devices. Resolution is based on a priori knowledge achieved by service discovery. Discovery is a service to find unknown services based on a rough specification of the desired result. It may be utilized by a human or another service. The discovery execution considers credentials for authorization. The security related functional components provide secure discovery of an IoT service and restricted discovery.

Secured discovery of an IoT service restricts the discovery of service to those users or applications that are authorized to know about it, including the creation of a new pseudonym (to ensure privacy of a user). As to [16] secured service discovery includes the following functional components: user authentication and assertion of his identity and discovery of person related IoT services for authorized personnel. The later functional components cover authorization to general access to discovery, service discovery based on service specification, filtering of discovery results, creation and deployment of new pseudonym. Secure direct discovery of IoT service is applied when the related credentials have to be processed prior to the discovery. In this case, first the user is authenticated and a list of credentials is provided based on the user identity. Then the user may communicate directly with an isolated discovery component performing the following actions: credentials presentation, service discovery and restricted access based on credentials.

Both scenarios for IoT service discovery presented in [16] rely on authentication authority and guarantee the user related security aspects. In some case, service authentication is also a matter of concern, for example, how to authenticate requests coming from other Web Services. So, where appropriate, authentication in IoT must be mutual including both user and service authentication. Moreover, for charging purposes, there is a need for the authenticated user to confirm the intention to use the discovered IoT service by signing a service agreement. The signing of service agreement is to ensure non-repudiation, or in other words to prevent the user from denying he or it has used the service. Typical service agreement presentation and signing is done by digital signature.

Section 3 presents the suggested elaboration of the IoT security model at application level, which faces the above mentioned issues.

3. Elaboration of the IoT Security Model

The suggested use cases related to secure IoT service access are shown in Figure 1. The access to IoT service includes Initial Access, Application level Authentication, Service Discovery and Service Selection use cases.

Before using IoT services, the user and the Service Repository authenticate each other. Authentication prevents from unauthorized access. Once authenticated, the user selects the service interface to be used. To ensure non-repudiation, the Service Repository can request signing of a service agreement before allowing the IoT to be used. Only after the authentication, service selection, and signing of the service agreement have been done the user start can using the actual IoT service. Apart from

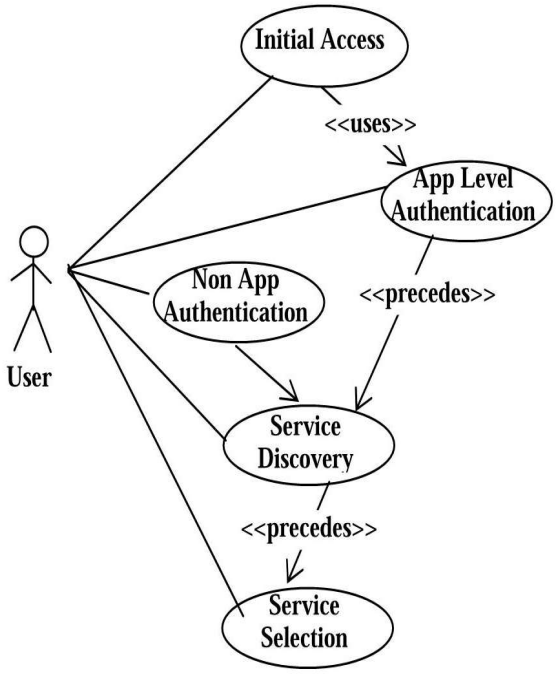

Figure 1. Use cases for secure IoT service access

providing security, the authentication and service selection process also allows IoT service providers to define permission profiles for different users. The amount of privileges can be made to depend on the level of trust awarded to the user.

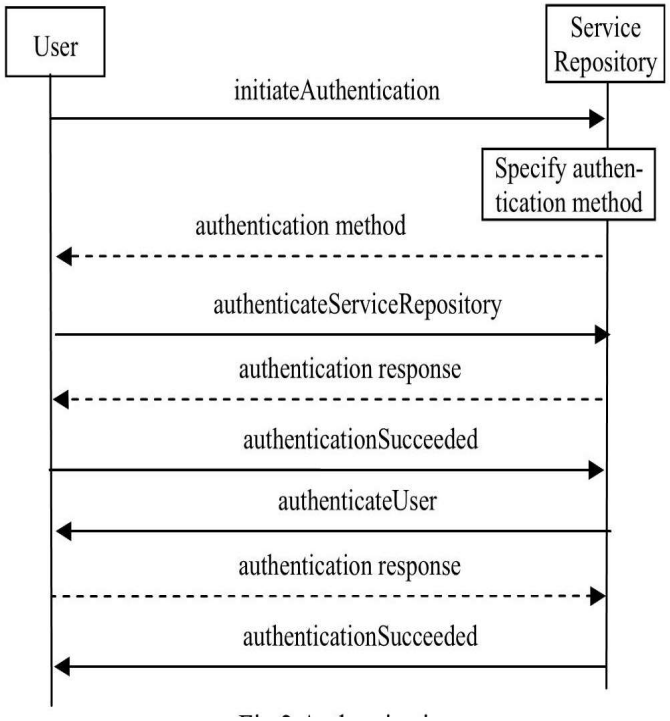

Figure 2. Authentication

Figure 2. shows the sequence diagram related to authentication use case

The steps are as follows

1. At initial contact, the User requests authentication by invoking the initiateAuthentication operation. The Service Repository replies with an indication of the authentication operation to be used. An agreed authentication method is used. If more than one authentication operations are supported, the initiateAuthentication operation serves to tell which operation to use.

2. The User requests authentication from the Service Repository by invoking authenticateServiceRepository operation. When the Service Repository has successfully authenticated itself, the User acknowledges this with the authenticationSucceeded operation.

3. Once the User has authenticated the Service Repository, the Service Repository requests authentication from the User by invoking authenticateUser operation. The security mechanisms are symmetric. Not only the Service Repository authenticates the User, but the User authenticates the Service Repository also.

Figure 3 shows the service discovery and signing of service agreement.

The steps are as follows:

1. After the Service Repository and User have successfully authenticated each other, they agree on an algorithm to be used for signed exchanges by invoking selectSigningAlgorithm operation.

2. The User may not know the services available and may request a list of service types by invoking listServiceTypes operation.

3. The User may need to examine the leading properties of selected services using describeServiceTypes operation.

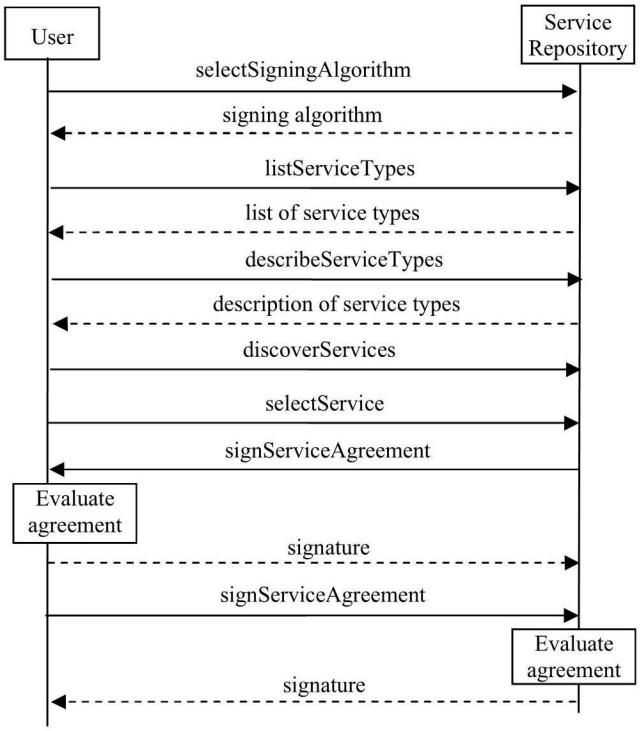

Figure 3. Service discovery, service selection and signing of service agreement

4. The core operation, discoverServices informs the Service Repository of the required service using parameters serviceTypeName and servicePropertyList as well as the maximum number of matches the User wishes to receive. The Service Repository returns a list of IoT services meeting the requirements and their service properties.

5. Using the selectService operation, the User informs the Service Repository of the ServiceID of the IoT service it wishes to select. The Service Repository provides a token that is private to the User.

6. The User and Service Repository sign a service agreement electronically by invoking signServiceAgreement operation. Once the service agreement has been successfully signed by both sides, the User can start using the IoT service.

4. Conclusion

The paper studies security aspects of IoT services. Based on the analysis on current standards and research work, security issues at the application, transport, network, and/or at the link layer in constrained networks are discussed. Some weaknesses in authentication and authorization of IoT service security are identified. As countermeasures mutual authentication procedure between the user and IoT service, as well as service selection procedure are suggested. In addition to increased security, the suggested authentication and service selection procedures allow differentiation of IoT service users.

Acknowledgement

The research is in the frame of Project DDBY02/13/17.02.2010 funded by National Science Fund, Bulgarian Ministry of Youth, Education and Science.

References

[1] ITU Internet Reports. The Internet of Things (2005) (Ed. 2005).

[2] Infso, D. Networked enterprise & RFID INFSO G.2 Micro & Nanosystems, in cooperation with the WG on RFID of the ETP EPOSS, '"*Internet of Things in 2020. Roadmap for the Future,* vol 1, pp. 1–27 (2008).

[3] Bekiarski, A., Altimirski, E. & Pleshkova, S. (2010) Multimedia surveillance station for audio-visual objects tracking with mobile robot. *In: Proceedings of the of International Conferences of Systems*, Greece, pp. 240–247.

[4] Galluccio, L., Morabito, G. & Palazzo, S. (2011) On the potentials of object group localization in the Internet of things. *In: Proceedings of the of IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks WoWMoM'*2011, pp. 1–9 [DOI: 10.1109/WoWMoM.2011.5986489].

[5] Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S.L., Kumar, S.S. & Wehrle, K. (2011) Security challenges in the IP-based Internet of things. Wireless Personal Communications, 61, 527–542 [DOI: 10.1007/s11277-011-0385-5].

[6] Pleshkova, S. (2011) Algorithm of feature estimation for real time objects detection in thermal images. *In: Proceedings of the of International Conference on Computational Intelligence, Man-Machine Systems and Cybernetics. CIMMACS:* Jakarta, pp. 209–215.

[7] Park, S. et al. (2011). "IPv6 over Low Power WPAN Security Analysis", Internet Draft.

[8] Weber, R.H. (2010) Internet of Things – New security and privacy challenges. Computer Law and Security Review, 26, 23–30 [DOI: 10.1016/j.clsr.2009.11.008].

[9] Li, T. & Chen, L. (2012) Internet of things: Principle, framework and application. *Future Wireless Networks and Information Systems, Springer LNEE, 144, 477–482.*

[10] Serbanati, A., Medaglia, C., Ceipidor, U. "Building Blocks of the Internet of Things: State of the Art and Beyond" (2011), Chapter 20. In: edited book "*Deploying RFID - Challenges. Solutions, and Open Issues*.

[11] Roman, R., Najera, P. & Lopez, J. (2011) *Securing the Internet of things. Computer*, 44, 51–58 [DOI: 10.1109/MC.2011.291].

[12] Mayer, C. (2009) Security and privacy challenges in the Internet of things. *Electronic Communications of the EASST*, 17, 1–12.

[13] Castellani, A.P., Gheda, M., Bui, N., Rossi, M. & Zorzi, M. (2011) Web services for the Internet of things through CoAP and EXI. *In: Proceedings of the of IEEE International Conference on Communications Workshops*, pp. 1–6 [DOI: 10.1109/iccw.2011.5963563].

[14] Suo, H., Wan, J., Zou, C. & Liu, J. (2012) Security in the Internet of things: A review. *In: Proceedings of the of International Conference on Computer and Electronics Engineering ICCSEE*, Vol. 3, pp. 648–651 [DOI: 10.1109/ICCSEE.2012.373].

[15] Kranenburg, R. et al. (2011) The Internet of things. In: *Proceedings of the of Berlin Symposium on Internet and Security*.

[16] FP7 project Internet of things – Architecture (2012). "Introduction to the Architectural Reference Model for the Internet of Things". www.iot-a.eu/arm/d1.3.

[17] ZigBee. www.zigbee.org/.

[18] Ramon, S. (2011) ZigBee alliance completes ZigBee building automation standard, BACnet. Default.aspx?Contenttype=ArticleDet&tabID=332&moduleId= 806&Aid=354&PR=PR. www.zigbee.org/.

[19] DALI. www.dalibydesign.us/dali.html.

[20] Kushalnagar, N., Montenegro, G. & Schmacher, C. (2007) IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals. RFC, 4919.

[21] Shelby, Z. (2012). Constrained RESTful Environments (CoRE) Link Format, RFC, Vol. 6690.

[22] Shelby, Z. et al. (2012). Constrained Application Protocol (CoAP), Internet Draft.

[23] Mozkowitz, R. (2011). "HIP Diet Exchange (DEX)", Internet Draft.