A REQUIRED SECURITY AND PRIVACY FRAMEWORK FOR SMART OBJECTS

Antonio Skarmeta, José L. Hernández-Ramos, Jorge Bernal Bernabe
Department of Information and Communications Engineering
Computer Science Faculty, University of Murcia (Spain)

ABSTRACT
The large scale deployment of the Internet of Things (IoT) increases the urgency to adequately address trust, security and privacy issues. We need to see the IoT as a collection of smart and interoperable objects that are part of our personal environment. These objects may be shared among or borrowed from users. In general, they will have only temporal associations with their users and their personal identities. These temporary associations need to be considered while at the same time taking into account security and privacy aspects. In this work, we discuss a selection of current activities being carried out by different standardization bodies for the development of suitable technologies to be deployed in IoT environments. Based on such technologies, we propose an integrated design to manage security and privacy concerns through the lifecycle of smart objects. The presented approach is framed within our ARM-compliant security framework, which is intended to promote the design and development of secure and privacy-aware IoT-enabled services.

Keywords—Internet of Things, Security, Privacy, Trust

1. INTRODUCTION

The application of security mechanisms to manage the life cycle of smart objects has received an increasing attention from the research community. Millions of interconnected constrained devices are starting to set up open and dynamic environments, which are difficult to be managed directly by humans. Indeed, this trend is expected to have increased in the coming years to reach between 50 and 100 billion of devices by 2020 [1]. In these environments, traditional operational procedures for bootstrapping, authentication and authorization are becoming obsolete, since they were not designed to deal with the inherent requirements of IoT ecosystems, in terms of scalability, heterogeneity, flexibility and us-ability.

The extension of technology to everyday devices implies the extension of identity management foundations to the physical world, in order to foster the deployment of Machine-to-Machine (M2M) communications [2] in which smart objects will be able to interact with each other, as an integral part of the IoT paradigm. In this sense, the IoT will require more lightweight, decentralized and end-to-end verification and authentication of the new devices deployed in a network, and, on the other hand, extension of the trust domain to such devices. This drives the need of new self-managing models to allow IoT smart objects to establish trust relationships among each other, while dealing with the new security and privacy concerns, which are inherent in these uncontrolled environments.

To this means, this work proposes the design of an integral approach for managing security and privacy concerns throughout the life cycle of a smart object. The design of the proposed approach is framed within our security framework [3] that is based on the Architectural Reference Model (ARM) [4], in order to realize the M2M vision of the IoT paradigm, while security and privacy are preserved. Specifically, in this work, we consider the use of the Handle System [5] as distributed information system for identification and resolution purposes of smart objects, an approach that is being currently considered by the ITU. Furthermore, we base our proposal on the use of the Protocol for Carrying Authentication for Network Access (PANA) [6], which is being currently used by ZigBee Alliance and ETSI M2M as IoT boot-strapping protocol. Moreover, we propose the use of partial identities as mechanism in order to conceal and minimize the private information revealed on a daily basis operation. The partial identities are implemented by applying anonymous credential systems (e.g. Idemix [7]), which allow to prove a subset of the attributes associated to the whole identity. Such privacy-preserving identity management mechanism could be integrated with other recent proposals, such as our Distributed Capability-based Access Control (DCap-BAC) [8] approach, in order to establish the notions of a secure and privacy-preserving M2M-enabled IoT.

The remainder of this work is organized as follows: Section 2 provides a general overview of concepts related to identity management in IoT. Section 3 introduces some of the main security and privacy challenges of the life cycle of smart objects, and an overview of the main interactions of our security framework to cope with such concerns. Subsequently, section 4 proposes the use of different candidate technologies that are currently considered by standardization bodies to cope with security issues in IoT environments. Furthermore, Section 5 focuses on the

---

This work has been sponsored by European Commission through the FP7-SMARTIE-609062 and the FP7-SOCIOTAL-609112 EU Projects.
privacy-preserving mechanisms that are envisioned to support secure and privacy-aware M2M communications. Finally, Section 6 concludes the paper with some remarks and an outlook of our future work in this area.

2. IDENTIFICATION AND IDENTITY FOR SUPPORTING SECURITY

2.1. Identities and Partial Identities in IoT

In the IoT ecosystem, identity management foundations must be extended to consider smart objects as entities with communication capabilities. While such smart objects may have different networking identifiers, they have also to possess their own identity to be distinguished from other devices. This identity could make reference a core identifier but also to specific features or attributes that point to the object. Furthermore, smart objects could act on behalf of a user. These objects could then be aware of the identity of their owners disclosing sensitive information to other devices. The identity management should be distributed in order to authenticate objects between each other but, at the same time, centralized enough to be able to establish a hierarchical approach where identity credentials could be issued and authenticated securely enabling a global digital trust environment.

Privacy concerns are also of paramount importance in IoT, where mechanisms for anonymity making use of partial identities are required. A partial identity is a subset of the attributes that comprise the complete or real identity of the user. Thus, an identity of a particular user or object may be composed of different partial identities. Each of these partial identities can be used to identify the user or the object in different circumstances according to the context or social situation. The real identity is the union of all the attributes of the partial identities of the user or object. Partial identities may comprise not only traditional user personal attribute values like names, identifiers, and addresses, but also object attributes, such as hardware features or software version. Thus, IoT ecosystems require suitable identity management solutions to cope with new challenges due to inherent nature and requirements of IoT, where the identities of a huge amount of heterogeneous smart objects need to be properly managed.

2.2. Object Naming, Resolution, Networking and Addressing

In order to achieve a real IoT, an essential feature is to give support to finding smart objects in order to be addressable, named, and finally discovered. In the IoT paradigm, smart objects cannot be configured with respect to a fixed set of services. This is mainly due to the changing dynamics of the IoT system resulting from the mobility of such devices, as well as the changing availability of services due to constraints on the underlying resources and devices. Therefore, a real need exists for a suitable infrastructure to be in place that allows addressing, naming and discovery of IoT services:

- **IoT Addressing:** an IoT address refers to an identifier of a smart object and/or its virtual representation. This feature entails the assignment and management of addresses/identifiers for smart objects.

- **IoT Naming:** it refers to mechanisms and techniques for assigning names to objects and supporting their resolution/mapping to IoT addresses. IoT Naming provides the means to identify smart objects through a resolution mechanism of a name according to a naming system. Additionally, names can be organized according to taxonomies or classifications in a hierarchical fashion and according to a well-defined naming system.

- **IoT Discovery:** it refers to the process of locating and retrieving IoT resources in the scope of a large and complex space of smart objects.

Previous concepts are closely related, given that the adherence to certain choices and solutions (e.g., standards, mechanisms, algorithms, tools) for one area (e.g., choice of addresses/identifiers) can directly affect the respective choices and solutions in the other areas (e.g., naming system used). As a consequence, the consideration of solutions for one area cannot be seen as isolated from the others.

2.3. Handle and Identifiers

The realization of the concepts described in the previous section implies the need for suitable infrastructures to enable addressing, naming and discovery procedures for the IoT ecosystem. Indeed, currently there are different proposed Internet identifier services addressing some of these aspects. X.500 [9] is the OSI Directory Standard defined by the ISO and the ITU. It defines a hierarchical data model with a set of protocols to allow global name lookup and search. In the same direction, The Lightweight Directory Access Protocol (LDAP) [10] was developed as a more lightweight alternative, but bringing different problems related to the hierarchical data model, as well as to the complex search/query process. Addressing some of these main concerns, the Handle System (HS)\(^1\) is a general purpose distributed information system that provides efficient, extensible, and secure identifier and resolution services for use on networks, such as the Internet [5]. While X.500 or LDAP could also be used, HS provides additional features, outperforming previous approaches due to its flexibility to enrich the resolution infrastructure with security aspects. Furthermore, HS could be used in tandem with LDAP providing efficient name resolution service, and extended search capabilities, respectively [11]. It is part of the Digital Object Architecture (DOA). A Digital

\(^1\) www.handle.net
Object (DO) has a machine and platform independent structure that allows it to be identified, accessed and protected.

The HS was developed initially with digital documents in mind, but it has evolved into a generic implementation of the DOA, supporting multiple object types, not just ’digital documents’. It is being taken into account by the ITU under ITU-T Recommendation X.125. The HS incorporates an operational security system based on both private/public key pairs and passwords. It allows for the storage and resolution of a set of attributes to a particular identifier, including an infrastructure for authentication, signing, integrity checking, public key operations as well as an authorization mechanism to restrict the access to the attributes. A handle consists of a prefix and a local identifier. The syntax of the DO is a set of pairs (type, value). As with the Domain Name System (DNS) with its DNS Resource Directory (DNSRD), the Handle Resolver (i.e. handle server) will provide a set of such pairs, some of which include well-known data types, like URIs, INET HOST addresses, etc. The pairs can be hierarchic, so that a DO contains descriptions and identifiers of other DOs in its parameters. Clearly, some of the parameters may contain IPv6 addresses, but there may be several such addresses depending on different views of the parameters.

The attributes managed by Handle and associated to an identifier can be exploited by an identity management system in order to allow the usage of partial identities associated to such attributes. A claim-based anonymous credential system, e.g. Idemix [7], can interact with Handle to generate credentials based on the attributes associated with the smart object. Subsequently, the smart object can derive partial identities from such a credential to operate against other smart objects in a privacy-preserving way. Specifically, we envision the use of Handle for three main purposes:

- Restricting the access to Handle attributes to authorized smart objects, based on a public key infrastructure through the use of X.509 certificates.
- Anonymous credential provisioning and partial identity management based on the attributes that are registered in the HS.
- Generation of authorization credentials to enable M2M secure communications, based on handle attributes to make access control decisions.

3. TOWARDS A SECURITY FRAMEWORK FOR SMART OBJEKT LIFE CYCLE

The secure management of the life cycle of IoT smart objects imposes the need for considering architectural approaches, taking into account the inherent requirements of the application of security and privacy-preserving mechanisms on IoT scenarios. Towards this end, IoT-A [4] was a large-scale European project focusing on the design of an Architectural Reference Model (ARM), in order to optimize the interoperability among isolated IoT domains. Based on ARM, our security framework [3][12] is intended to address security and privacy concerns in the IoT paradigm, by instantiating and extending the security functional group of ARM. Consequently, such framework promotes its applicability and inter-operability in a wide range of IoT scenarios, in which security and privacy are required.

Under the complete view of our IoT security framework, as well as the main stages of the life cycle of smart objects [13], below we provide an overview of the main interactions that are required to address security and privacy concerns through such phases. It should be pointed out that, while it has been proposed in our framework, for the sake of clarity, the interactions of the Group Manager functional component are not addressed in this work [14]. Figure 1 shows the required interactions to manage security during the smart objects life cycle. The description of these interactions is split according to the main stages of it. In particular, the life cycle begins when a smart object is installed and commissioned during the bootstrapping process. We propose to extend this phase so the smart object is also registered (bootstrapping and registration), and consequently, it can be discovered by other smart objects. This discovery process is shown in the figure through the Discovery and provisioning stage, in which a smart object additionally tries to obtain the required security credentials for a secure and protected access. In case this process is successfully completed, both devices can communicate with each other during the Operation stage, in which a smart object tries to get access to the discovered device by using the credentials previously obtained.

At this point, note that, while it is not shown, we assume smart objects are supplied with statically configured cryptographic material (e.g. symmetric keys or X.509 certificates) before the bootstrapping process. Such cryptographic material can be configured by the manufacturer (or the device’s owner), and it can be considered as the root identity that is employed for bootstrapping procedures. During this stage, the smart object is commissioned and connected to the network, which implies an authentication and authorization process that is required before starting the sending or receiving of data. Specifically, the purpose of this process is twofold. On the one hand, the smart object can be registered in order to be discovered by other smart objects to communicate with each other. This functionality is already considered by the ARM through the IoT Service Resolution functional component, and it can be carried out by an infrastructure entity (e.g. based on Handle). On the other hand, a success authentication and authorization process could derive other cryptographic material to be employed by the smart object during its operation. In particular, we
envision that anonymous credentials (e.g. based on Idemix) associated with identity attributes that are demonstrated during the bootstrapping, could be supplied during this process. However, while smart objects could use such credentials for privacy-preserving communications, the creation of an anonymous credential would be linked to the root identity of the smart object. This process is intended to preserve the accountability of the anonymity condition, in order to avoid the misuse or abuse of it.

After the smart object has been successfully bootstrapped, it enters the operation phase by providing (or trying to get access to) the services for which it has been manufactured. At operational level, security guarantees that only trusted and legitimate smart objects can communicate with each other. Consequently, the application of security and privacy-preserving mechanisms is crucial to ensure a proper and effective operation of the smart object. For these interactions, we assume the existence of two smart objects acting as a producer (providing a service), and a consumer (trying to get access to such service). In addition, we assume that these smart objects have already carried out the process previously described. Before starting the operation stage, the consumer initiates a discovery process to know the services being provided by the producer. This step involves authentication and authorization procedures, in order to determine whether the consumer is authorized to find that service or not. Furthermore, such authentication mechanism can consider privacy concerns of the consumer through the use of partial identities, which can be derived from the anonymous credential. Furthermore, we envision the extension of the discovery step in order that the consumer, in the case of a successful authentication and authorization process, can get the required credentials for a secure M2M communication with the producer smart object. Once this process is completed, such credentials are used by consumers to access a resource being hosted by the producer. On the one hand, from a consumer perspective, the operation stage can take into account privacy concerns through the selection of a different partial identity (or pseudonym), according to contextual information being sensed. On the other hand, from the producer perspective, the evaluation of authorization credentials presented by the consumer could consider additional information, such as trust and reputation scores associated to the requesting smart object [15].

4. LIGHTWEIGHT SECURITY MECHANISMS FOR IOT ENVIRONMENTS

Having highlighted the main required interactions of our IoT security framework have been highlighted, below we give an overview of candidate technologies being currently considered by different standardization bodies, and how they can be integrated to achieve the functionality previously described. The integration of these mechanisms is intended to provide a holistic view to support security and privacy
aspects, which can be leveraged by smart objects during their life cycle.

4.1. Security Bootstrapping

The bootstrapping process usually consists of a set of procedures in which a node is installed and commissioned within a network. Optionally, this stage can include authentication and access control mechanisms to get security parameters for trusted operation. For a successful and secure bootstrapping process, well-known mechanisms need to be on the basis. Additionally, in the context of IoT constrained scenarios, the application of such procedures needs to be analysed due to implicit requirements of these environments. Towards this end, [16] provides some design considerations that must be taken into account in the design of an appropriate IoT bootstrapping protocol. In addition, [17] presented three main alternatives for the security bootstrapping of IoT devices: Host Identity Protocol Diet Exchange (HIP-DEX) [18], PANA [6] and 802.1X.

Currently, PANA is widely accepted as the main candidate for IoT security bootstrapping, and it is being employed by ZigBee Alliance in conjunction with EAP-TLS as authentication protocols. In this work, we consider that smart objects are initially equipped with an identity certificate (e.g. a X.509 certificate), which contains a set of attributes associated with the smart object (e.g. manufacturer or hardware features). Then, we propose the use of PANA as a signaling protocol enabling smart objects, in an on-demand way, to make smart objects to apply for security credentials that can be used for secure M2M communications during their operation.

4.2. Operational Security

At operational level, security guarantees that only trusted and legitimate instances of an application running in the IoT can communicate with each other, through the use of the corresponding security mechanisms at the application layer. Specifically, CoAP [19] defines a security binding to DTLS [20] through the use of pre-shared keys, raw public keys or certificates. However, it does not cover the use of authorization and access control mechanisms at the application level. Towards this end, our Distributed Capability-Based Access Control model (Capac) has been postulated as a realistic approach to be used on IoT scenarios [8]. This approach is based on linking access privileges or capabilities to smart objects, which are identified by their public key. Capac is based on the use of authorization tokens, containing capability that were previously granted to the holder, as well as a set of access conditions to be locally verified by the end device when the token is presented. Specifically, it makes use of the JavaScript Object Notation (JSON) [21] as representation format for the capability token, which is attached in access requests by using the Constrained Application Protocol (CoAP) [19].

In addition to the main authentication and authorization for communication between two smart objects, given the global scale of the IoT, it is likely that smart objects often operate as groups of entities (e.g. interacting or collaborating for a common purpose). Indeed, we consider the concept of group as essential in the IoT to cope with environments with a high number of smart objects interacting with each other, and the application of security mechanisms involving groups of devices with dynamic and ephemeral relationships as a challenging aspect. In this sense, the CipherText-Policy Attribute-Based Encryption (CP-ABE) [22] has been recently proposed as a highly flexible cryptographic scheme, which provides the ability to define groups and subgroups of smart objects according to different combinations of identity attributes. Indeed, unlike the use of symmetric key cryptography, in which groups of entities must be preconfigured, a smart object could encrypt each piece of data under a different combination of attributes, allowing for the creation of dynamic groups or subgroups. For example, a smart object could encrypt information so that only the set of objects from the same manufacturer or the same owner could decrypt the information. The application of CP-ABE for IoT scenarios is currently considered in our framework, through the design of our proposed Group Manager functional component, as well as the interactions with other security components.

4.3. Supporting Security and Privacy features in the Life Cycle of Smart Objects

After the overview of the main security and privacy technologies addressing different aspects of the life cycle of smart objects, this section shows an overview of how some of the above mentioned technologies previously described could be integrated into addressing such requirements.

According to the main stages described in the previous section, the life cycle of a smart object begins with the bootstrapping/registration phase. For this stage, we consider the use of PANA due to its flexibility enabling the execution of different authentication mechanisms or EAP methods. Once the smart object is successfully authenticated through its root identity (for example, by using a X.509 certificate), we propose to extend this phase so the smart object is registered through the use of the Handle infrastructure to be discovered by other smart objects. This process may involve the registration of attributes or additional information that is contained in the smart object’s certificate. After this process, the device could try to obtain an Idemix credential that is associated with the information previously registered in the Handle server. Indeed, it can use the issuance Idemix protocol as specified in [7].

In the discovery and operation stages, a smart object (acting as a consumer) tries to access a resource being hosted by another (acting as a producer). For this purpose, firstly, it discovers the device by querying the Handle server. It should
be pointed out that this process may require authentication and authorization procedures according to the information that was registered during the bootstrapping and registration stage of the smart object producer. In addition to the discovery, the consumer tries to obtain the credentials that are required for a secure and M2M operation. In this case, we propose to extend the semantics of PANA notification messages so that a device can apply for DCapBAC tokens to get access to a resource being hosted by another device. Obtaining these credentials implies an authorization process driven by infrastructure components, which are responsible for generating DCapBAC tokens to authorized smart objects. For this purpose, we propose the use of CoAP/DTLS or HTTPS as communication protocols, and the eXtensible Access Control Markup Language (XACML) [23] as standard access control technology. Finally, after the smart object consumer obtains the required DCapBAC token, it can make use of a CoAP-DTLS exchange attaching the credential for a secure and protected M2M communication.

5. PRIVACY-PRESERVING M2M SUPPORT

The realization of the IoT ecosystem implies moving towards automated and self-managing security mechanisms, which allow IoT devices to set up trust relationships with each other with a low degree of human intervention. Furthermore, given the M2M nature of these emerging scenarios, the application of current privacy-preserving technologies needs to be reconsidered and adapted to be deployed in such a global ecosystem, addressing aspects such as Privacy by Design (PbD) [24], in order to give people maximum control over their personal data. As already mentioned, privacy-enhancing technologies provide means to achieve anonymity, data minimization, unlinkability as well as other techniques to provide confidentiality and integrity of sensitive data. In this regard, the usage of partial identities as privacy-preserving identity management scheme, allows users to define a subset of the personal attributes, from their real identity, in order to identify them in a given context. In order to realize this vision, some solutions rely on the notion of Anonymous Credential Systems [25] to deal with privacy concerns. Through the use of these technologies, a consumer smart object could try to get access to a producer device by proving a subset of identity attributes from their whole identity, without the involvement of an on-line Trusted Third Party (TTP) in charge of authenticating the subject.

The use of partial identities and anonymous credential systems, which has been previously proposed, could be combined with authorization mechanisms, such as our DCapBAC approach [8]. Specifically, in the original DCapBAC proposal privacy aspects are not considered, since it is based on the use of X.509 certificates, which are used to identify smart objects making use of authorization tokens. These considerations were addressed in our recent work [26] by enhancing DCapBAC with anonymity features, in order to deal with privacy concerns through the integration with Idemix [7].

Specifically, with this approach, the smart object (acting as a producer) could use its Idemix credential obtained during the bootstrapping/registration phase to get an Anonymous DCapBAC token from the Capability Manager (the entity that is responsible for generating these credentials) in a privacy-preserving way. Specifically, the Idemix proof generated by the producer could be associated with a particular partial identity (i.e. a subset of identity attributes), which could be used for authorization purposes by the Capability Manager and the PDP. Such proof should also contain a pseudonym generated by the smart object to be specified in the token. Then, the smart object can make use of such anonymous token, to get access to the producer smart object through the Idemix proving protocol. This process allows the consumer to prove it is the entity associated with the token while concealing any other identity attributes. The integration of this mechanism to the scenario proposed in the previous section is being currently designed and implemented, and it represents part of our ongoing work in this area.

6. CONCLUSIONS AND FUTURE WORK

The realization of IoT scenarios imposes significant security and privacy concerns due to the extension of Information Technology to our everyday lives. These aspects must be addressed by considering the whole picture of this paradigm, so the enormous envisioned potential can be leveraged by the society in the context of the future Smart Cities. Physical objects of our surrounding environment are being enabled with intelligence and communication abilities transforming them into smart objects. In this work, we have reviewed the main security and privacy challenges that are inherent in an IoT ecosystem. These implications are considered crossing all the stages of the life cycle of a smart object. We claim the need to consider architectural approaches to cope with these challenges in order to design appropriate mechanisms for emerging environments. By considering our previous work in this area, and some promising technologies that are currently being contemplated for deployment in IoT scenarios, we have provided the design of an integrated approach in order to capture such requirements. This scenario is being developed under our ARM-compliant security framework, with the aim of providing a holistic security approach as a step forward to realizing the vision of a secure and privacy-preserving IoT.

REFERENCES

[2] Zubair Md Fadlullah, Mostafa M Fouda, Nei Kato, Akira Takeuchi, Noboru Iwasaki, and Yousuke Nozaki,


