International Journal of Engineering & Technology, 7 (4.36) (2018) 700-706

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A systematic Study of Security Challenges and Infrastructures for Internet of Things

N. Koteswara Rao[1*], Gandharba Swain[2]

[1]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.
[2]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.
E-mail:gswain1234@gmail.com
**Corresponding author E-mail: rao0007@gmail.com*

Abstract

The proliferation of smart objects with capability of sensing, processing and communication has grown in recent years. In this scenario, the Internet of Things (IoT) connects these objects to the Internet and provides communication with users and devices. IoT enables a huge amount of new applications, with which academics and industries can benefit, such as smart cities, health care and automation. In this environment, compose of constrained devices, the widespread adoption of this paradigm depends of security requirements like secure communication between devices, privacy and anonymity of its users. This paper presents the main security challenges and solutions to provide authentication and authorization on the Internet of Things.

1. Introduction

The next leap in Internet growth is grounded in the Internet of Things (IoT) paradigm which encompasses hardware, software, and service infrastructure that connects physical objects, called things, to the computer network [1]. According to [2], the basic idea of IoT is the presence of a diversity of objects that interact and cooperate with each other in order to achieve a common goal by sharing information using single addressing methods and standardized communication protocols.

The integration between sensors and actuators on the Internet forms the technological basis for the concept of intelligent environments in which the information generated by an object can be shared between several platforms and applications [3]. The concept of intelligent environments encompasses different technologies, such as wireless sensor networks (RSSF) and integrated radio frequency identification (RFID) systems to track states of things, such as location, temperature, movement, etc. [2].

Another important concept in the IoT scenario is the Web of Things (WoT). The main feature in WoT is the adoption of protocols widely used in web applications, such as HTTP, whose main gain is the ease of integration between WoT services and other services and systems available on the Internet [4] . With the increased adoption of IoT and WoT applications, concern for information security will increase the success of the use of this emerging technology and so will be based on the level of security that the environment can provide for users, such as confidentiality of the data trafficked, as well as the privacy of users.

IoT presents unique requirements that require differentiated approaches to safety. According to [5], adding security mechanisms to embedded devices with computational constraints can be challenging. Given the heterogeneity of devices, developing security mechanisms that can be executed on different platforms is an important requirement for IoT. Finally, the authors state that physical access to devices is facilitated by the type of environment in which objects are inserted. Thus, not only the logical but also physical protection of these devices is required.

Among the set of security requirements for IoT, we can highlight: the identity management of users and devices; the confidentiality of the data exchanged in the communication; the availability of resources and systems; and network access control to ensure only authorized devices [5].

You can meet these security requirements through an authentication and authorization infrastructure. With this infrastructure, identity management can be deployed to prevent unauthorized users or devices from accessing resources, preventing legitimate users or devices from accessing resources for which they are not authorized, and allowing legitimate users or devices to have access to resources authorized [8]. Although authentication and authorization of users is well addressed in the literature, authentication and authorization of devices is not well characterized and, according to [9], is a research challenge in this scenario.

The purpose of this paper is to discuss the security challenges and authentication and authorization infrastructures that provide Internet identity management for Things. The following key issues are discussed in this chapter: single sign-on (SSO) of users and devices, management of trust relationships between different administrative domains, and interoperability between authentication and authorization mechanisms.

2. Overview of internet of things

The next step in the growth of the Internet is the integration of day-to-day physical objects (things) into communication networks. In 206, there were approximately 1.5 billion personal computers and more than 1 billion mobile phones with Internet access. By 2020, something between 50 and 60 billion devices are expected to be connected to the Internet. [5] say that at IoT there are things like clothes, furniture, cars, smartcards, medical devices, consumer meters and industrial machines. The IoT paradigm integrates a wide range of concepts and areas, such as: electronics, automation, communication networks, biotechnology, mechanics and materials technology [6].

According to the report [1], IoT can bring changes to society in general in the way the individual relates to the environment, as well as in the way business processes will be carried out. In addition to communication and information anytime, anywhere, in IoT is also possible connectivity for anything.
According to [1], the advances and convergence of micro electromechanical systems technologies, wireless communication and digital electronics have resulted in the development of miniature devices with the ability to feel, compute and communicate over a wireless network over short distances. From this scenario derives the concept of intelligent environments. Several countries are developing Smart Cities projects, which offer innovative experiences in transportation, environmental preservation, coexistence and energy savings. Worldwide, we recognize the potential of IoT technology to create intelligent environments through smart objects [7].
Characteristics of the Internet of Things:
IoT can be characterized as a worldwide network of interconnected things / objects / devices that behave as active entities

- Things (devices) in IoT often have resource constraints such as RAM or ROM, processing power, and power [8]
- Communication mechanisms of some devices, mostly wireless, have low transmission power and low data rate [9]
- There are a lot of things (devices) with short cycle of life, which requires a high management capacity [10]
- Integrates heterogeneous things (devices), which demands a concern regarding interoperability between them [11]
- The network has a dynamic topology because many nodes enter and leave the network frequently [11, 12]
- It can be characterized as an environment containing a large number of invisible computing devices or devices that collaborate with the user, ie a pervasive and ubiquitous environment [12]
- At IoT, users can interact with things in their physical and virtual environment in a variety of ways [11]

According to [13], things in IoT have five main features and an optional one. These are:

- **Existence:** things that exist in the real world can also exist in the virtual world (IoT), through embedded communication devices
- **Self-awareness:** all things have, explicitly or implicitly, an identity that describes them. Things can process information, make decisions, and behave autonomously
- **Connectivity:** Things can start communicating with other entities. In this way, communication with entities in your vicinity or in remote environments is possible.
- **Interactivity:** Things can interoperate and collaborate with a variety of heterogeneous entities, whether human or virtual or real machines. In this way, they produce and consume a wide variety of services
- **Dynamicity:** Things can interact with each other at any time, place or way. These can enter and exit a network as they wish, not being limited to a single physical location, and can use a wide variety of interfaces
- **Environmental science:** Sensors can allow things to perceive the characteristics of their environment, for example, network overload or water radiation. This feature is optional because not all things have this capability, such as an object with an RFID tag.

In [1] author further state that the IoT environment culminates in the generation of huge amounts of data that need to be stored, processed and presented in an efficient and easy to interpret manner. The authors state that the concept of Cloud Computing completes the IoT concept in order to provide ubiquitous sensing. A cloud infrastructure where you can store a large amount of data and provide that data for which applications can be built, with requirements for availability, processing capacity and on-demand resource allocation is required for intelligent environments to be scalable and highly available.
As an example of this integration (Cloud and IoT), the European OpenIoT project aims to provide open-source middleware for the development of IoT applications using the cloud-based model. Objects connected to the Internet can be accessed by IoT services in the cloud. For example, the sensing of this object can be a service provided in the cloud (Sensing as a Service). Through the use of IoT services, users can configure and develop IoT applications. The project also aims to provide infrastructure and IoT applications in the cloud, forming a cloud of things.
To understand the IoT paradigm, author in [2] present the main concepts, technologies and standards involved, from three perspectives, namely:

- **Vision orientation to things:** Consider things as simple items, for example, Radio-Frequency IDentification (RFID) tags, but not just these simple things. It deals with aspects such as single and global addressing (for direct access to things via the Internet) and the univocal identification of things. One of the relevant points of this view is that, for the actual realization of IoT, the need to increase the intelligence of things (conceive smarts things) is contacted;
- **Internet-orientation to vision:** Responsible for the necessary protocols and how these should be adapted to allow the exchange of information between things in IoT. In this vision are the researches and standards that deal with the adaptation of the IP protocol to the IoT environment;
- **Vision orientation to Semantics:** The amount of things connected to the network (Internet of the Future) is bound to be very high. This view includes issues such as representation, storage, search and organization of the large amount of data generated in IoT. In this context, semantic technologies should play a fundamental role, since they will be used for modeling things, for extracting data knowledge, for reasoning about the data generated in IoT, for creating semantic execution environments and for defining the architecture that will accommodate IoT requirements.

3. Requirements and security threats on the internet of things

According to [13], security is identified as one of the obstacles to be transposed into the effective use of the Internet of Things. By providing security to IoT applications, through an authentication and authorization infrastructure, it is necessary to ensure the autonomous behavior of objects and the interoperability between them.

3.1. IoT Security requirements

Considering the characteristics of IoT, author in [14, 13] point out several security requirements for the Internet of Things and indicate which security properties should be guaranteed, these being:

- **Confidentiality:** sensitive data from users or organizations may be contained in the Internet transactions of Things and therefore the confidentiality of such data must be assured;
- **Integrity:** data stored and transmitted must not be altered, removed or included by unauthorized users or devices;
- **Availability:** Keeping the Internet services / resources of Things available for access by authorized users and

devices at any time and from anywhere, thereby providing access to data on an ongoing basis;

- **Authenticity:** need for mutual authentication, since IoT data are used for different decision-making and action processes, and it is necessary that both the resource / service consumer and the provider be authenticated.
- **Privacy:** refers to the need to provide users with the means for them to control the exposure and availability of their own data and information and to have greater transparency about how and by whom their data is used.

In [15] author points out some other security requirements that need to be guaranteed in IoT, among them:

- **Identity Management:** handles the identification and authentication of users and devices / things in a system. It also controls access to the resources of this system by associating access rights and restrictions, according to the established identity (authentication and authorization)
- **Secure data communication:** includes authentication of communication pairs, ensuring the confidentiality and integrity of transmitted data, preventing repudiation of a transaction and protecting the identity of entities
- **Secure network access:** guarantees the possibility of network connection or access to a service only for authorized devices and
- **Resistance to Violation:** maintains security aspects, even when the device is physically accessed by an attacker.

According to [3], IoT's large scale and scope increase user interaction options with systems, leading to the need to extend current privacy, security, and identity management models to include how users interact with objects. In this sense, the requirements are also raised that it should be possible to identify objects in a unique way, that is, to differentiate one object from the other, besides allowing the unique authentication of objects in IoT [4].

Finally, authors in [16] and [13] highlight the requirement of fault tolerance, which in general scenarios, refers to the system does not fail and function normally, even in the presence of a fault. In the Internet of Things, fault tolerance consists of the system recovering data transmission and repairing the network structure (Ex. its topology) autonomously, even in the presence of faults in nodes or network links.

3.2. Threats and attacks in the IoT

In [17], the authors confirms that the IoT allows computational systems become ubiquitous and transparent to users. This transparency, together with the ubiquity, are potential threats to the privacy of users, as well as enforces difficulties to ensure the confidentiality and integrity of data that travels. The sharing of devices with other people is one of the major security threats against the privacy of users, because data can easily be obtained by persons not authorized, once that this person would have physical access to the device [18].

In [19], the authors confirms that before the existence of the IoT, corrupted digital systems were mostly incapable of acting in the physical world, but in the scenario of IoT, corrupted devices can act and influence the physical world directly. For example, a device that has the smoke sensor should alert a control center whenever it detects smoke in the environment. If this device is corrupted, you can issue false alerts or even may fail to issue alerts before a real situation of danger with smoke.

In the scenario of the Internet of Things, when a node sends data to another node in the network or even for a node is accessible through the Internet, these data can be stored temporarily in the intermediate nodes that act as routers. Thus, between the source and destination of a particular information, there may be several intermediate nodes which, if they are malicious, can change the information in transit or still do not forward the information to the final destination [20].

Authors in [20] feature a division of the types of attacks on the Internet of Things in five categories listed below:

- **Physical attacks :** are attacks that violate the device hardware and are difficult to perform, because the material needed to perform the attacks is expensive. The packaging of a chip, micro-probing and layout are reconstruction techniques used for this type of attack
- **Attacks on the communication channel:** attacks based on data retrieved from the devices responsible for operations of cryptanalysis. These data are obtained through analysis of delay, the radiation emitted, power consumed, among other sources, that allow the key criptografiused to be inferred
- **Crypatanalysis Attacks :** attacks with focus on the ciphertext, seeking to find the key of encyprion thus obtain the text in clear. One of the attacks in this category is the attack of the Man in the middle (Man in the Middle - MITM)
- **Software Attacks:** software attacks exploit vulnerabilities of software present on the device. Includes attacks of exploitation of buffer overflowbuffer overflow () and the use of Trojan horse programs, worms and viruses to inject malicious code into the system
- **Network Attacks:** in the middle without fithe transmission is broadcast by diffusion () and thus there are vulnerabilities inherent to the medium itself. In this category are attacks such as the capture and analysis of traffic (eavesdropping), denial of service (Denial of Service (DoS), corruption of messages, attacks of routing, among others

Authors in [21] point out that wireless networks, such as those used in IoT, are prone to various types of attacks, such as: eavesdroping, which violates the ownership of confidentiality; masking, in which one knot pretends to be another, thus hurting the property of authenticity; and denial of service, which violates the availability property. On denial of service, [11] cite the dynamic topology of the network, lower bandwidth and energy constraints as vulnerabilities that provide this type of attack.

Authors in [22] points out security concerns related to the entry of devices on the network are described. At the moment of entering the network, information about cryptographic keys, domain parameters and other configurations can be captured by malicious entities and they could use this information to intercept and forward data in a way not to be perceived, characterizing a man in the attack middle. In addition, if the key establishment protocol is compromised, not only will the confidentiality of the communication be compromised, but also the authenticity of the participating nodes may be at risk, since often the communicating nodes do not have prior knowledge of each other. According to the authors, it is possible to carry out the resource exhaustion (DoS) attack, since in this environment computational and energy resources are limited.

Authors in [11] point out that the attack of man in the middle can lead to the old message attack, in which the attacker seeks to use old messages (intercepted) to communicate with other devices, in order to obtain answers of those devices that initially would not be for him, but for the sender of the original message.

Author in [23] indicate the possibility of corrupting identification or localization messages in IOT architectures using the 6LoWPAN protocol. Corrupting such messages would lead to network security failures, since an attacker could send false update messages about the location of a node, causing messages not to reach their destination or be sent to the malicious node. This would still allow for denial-of-service attacks by mass mailing (flood).

In [24] authors address two other types of attacks: shared key and sybil. In shared-key attack, the attacker knows the key distribution

mechanism of the environment and, knowing that two nodes are close, assumes that they share the same key space. The attack occurs when the key shared by the devices can also be inferred by the attacker, compromising the security of the system. The sybil attack is characterized when a malicious node assumes multiple false identities in order to steal or forge the identity of a legitimate node.
Finally, authors in [8] also point out the existence of a key control attack, in which one of the participants in the communication forces the other participants to choose cryptographic keys within a restricted set of values or even a predetermined value. In this way, the attacker influences the process of choosing cryptographic keys in order to facilitate obtaining the control over the data trafficked.

4. Authentication and authorization on the internet of things

Authentication and Authorization (access control) are known as central elements to treat security in distributed systems. A way to provide these controls is through an infrastructure for authentication and authorization (IAA) which provides the management of identities (Identity Management (IDM). IDM can be understood as the set of processes and technologies are used to ensure the identity of an entity (user or device), ensure the quality of the information of an identity (identificators, credentials and attributes) and to provide authentication procedures and authorisation [4]. The entities involved in a system of IdM are: (i) user or device, an entity that uses a service provided by a service provider; (ii) the identity provider (Identity Provider -IDP), responsible for maintaining the database of domain users and validate your credentials (authenticate users); and (iii) the provider of services (Service Provider - SP), which provides resources or services to users.
In the IoT, the devices can belong to more than one network or administrative domain, scenario that [19] call Internetwork of things. This situation can affect the functioning of the procedures for authentication and authorization, in function of the mobility of these devices between different networks.

4.1. Authentication of Users

The Internet of Things, users interact with many smart devices or 22015099 headaches services (Service Providers (SPs) to get some useful service for them. To allow a user to access an object/device in the IoT, many times, it is necessary that this pass through an authentication process.
Some studies in the literature follow the model of centralized authentication, based on a third party environment. In [25] author proposes the use of LDAP (Lightweight Directory Access Protocol) in conjunction with Kerberos authentication mechanism, to provide a single authentication (Single Sign On) users in the IoT.
In [26], for which a user to access a service provider, this must submit an access token signed (issued) by a third party environment (Authorized Server - AS) for both the user and the SP. Each user needs to make an initial registration to this central server (AS), which should provide an identity indicator and password. To obtain the access token (capability), the user must authenticate to the, making use of your password. The SP verifies signing the token and analyzes the content of the same to complete the process of user authentication.

4.2. Device authentication

In [11] author propose a mutual authentication method for IoT focused on devices that are in a single domain. A device, upon joining the network, receives a pair of asymmetric keys and a domain parameter from a Key Distribution Center (KDC). This domain parameter was used by the KDC in the process of generating the key pair delivered to the device, based on an Elliptic Curve Cryptography (ECC) protocol. Thus, when two devices wish to communicate within the domain of the same KDC, they use the ECCDH protocol to establish a private key, which will be used for communication between them. The basis for establishing this key is the domain parameter and the public key of each of the devices.
After the establishment of this private key, the authentication process between the devices occurs. This process takes place through a response challenge protocol, based on the established private key, a timestamp and a random number generated by one of the parties to the communication. The ability presented by each of the devices is also used in the authentication process. The skill is a token that contains the device identity, a set of access rights, and a hash of the two previous fields. This hash is applied with the CBC MAC method to ensure message integrity. Finally, the device that will be accessed verifies that the ability token sent by the other device is equal to what it has stored. If yes, and if the challenge-response result is correct, the mutual authentication process is complete and successful.
In [27] author present a security architecture For IoT based on the Datagram Transport Layer Security (DTLS) and make use of digital certificates in the process of authentication of devices. In this architecture, are proposed three actors: publisher - a device producer; subscriber - consumer device resources; and access control server - Equipment with greater computational power and responsibility to enforce access control to the resources of the devices producers.
Two scenarios are presented, one in which the producing devices have Trusted Platform Modules (TPMs) and one in which the devices do not have TPMs. For the first scenario, the producer is able to make full DTLS handshake with the consumer of the resource, and mutual authentication is performed through X.509 certificates, issued by a Certification Authority (CA), recognized by both.
For the second scenario (devices with restrictions), producer authentication is done through the use of a pre-shared key (PSK) of the TLS encryption suite. In this scenario, the device has a random set of pre-installed data, called protokeys, that are used to generate the PSK of a session. In the authentication process, the producer generates a session identity, consisting of its identity and some randomly generated data at the time of authentication. Then, a PSK is generated by applying an HMAC function on this session identity, keyed in this process to protokey.
The resource consumer, in turn, must authenticate to the access control server, which is aware of protokeys and the session identity of the producer. Thus, the access control server is able to generate the PSK of the producing device for that session and pass it on to the consumer. In this way, the access control server validates the consumer's identity for the producer, as well as validating the identity (session) of the producer to the consumer. Therefore, the access control server must be a trusted third party in this architecture.
According to [2], IoT's intelligent object constraints demand for lighter security mechanisms. The use of digital certificates for device authentication is in many cases considered impractical. In this work, the authors aimed to prove that, with some modifications in the DTLS protocol handshake process, the use of digital certificates becomes a viable method of authentication in many IoT scenarios.

4.3. Authorization

Access control mechanisms are needed to ensure that resources are available only to individuals authorized by the access control policy. A subject can be a process, a person or a device that you want to perform some action on a resource. In the IoT, the implementation of this type of mechanism should take into account the dynamics of the environment, with a large number of

devices and users, as well as the presence of devices with limited computational resources.

In the context of the IoT, among the studies analyzed, it is observed that the Access control mechanisms deploy by known models and already employed in Internet, namely:

- **Discretionary Model:** for example, in [28] author propose a mechanism based on access control list (Access Control List - ACL) to allow people to share their devices in the WoT with other users through existing social networks. The owner of the device requires permissions for each device and for each user with whom you want to share it. An approach using ACLs is costly for a user to keep when this has many devices and many users with whom you wish to share.
- **Model based on roles (Role Based Access Control (RBAC):** [8, 16] adopt the RBAC model that is widely accepted in the Internet and known for its simplicity to manage permissions and users. However in [11] author indicate that RBAC has limited granularity and the way in which it deals with the delegation of duties is not suitable for large-scale environments, such as the environment of the IoT.
- **Capability Based Access Control - CBAC:** the holder the ability (authorization token) is able to interact with an object by means of as well defined operations. The information about the identity of the user or device is transformed into a skill, that still combines the access rights of this user/device. This model provides good scalability, since there is no need to confront the identity of the user with an access control list, or lists of roles and permissions. In this model, it has a smaller number of information stored in the entity responsible to enforce access control. In [11] authors follow this model in their infrastructure for authorization.
- **Attribute Based Access Control (ABAC):** the authorization decision is taken from a set of attributes of the subject, the object of the operations requested and the conditions of the context facing the access control policies, rules or relationships that describe the operations allowed for a given set of attributes. Han and Li make use of ABAC model in the IoT, adapting it to deal with the delegation of attributes in this scenario. According to the authors, it is possible to realize some benefits from the use of ABAC in scenarios such as IoT, when the subject does access to an object outside of its administrative domain. In this case, access control lists (ACL- Access Control List) or the RBAC roles are not applicable, since these are strongly linked to the context of the holder of the resource. In [29] also fit the ABAC model for the scenario of IoT, combining a targeted approach to workflow (WABAC). In this model, so that a decision is taken to access control, are considered the attributes of three actors: (i) the subject, whoever wants to perform an action on a resource, which can be a user, an application or a mobile phone, having attributes as an identification, an IP address or email address, etc; (ii) the feature, which can be, for example, a service, a fact or an intelligent device, having attributes such as geographical location, identification or Date of creation, etc; and (iii) the environment, which refers to the context in which access to the information happens, having attributes such as the date or the level of network security.

5. Infrastructure for authentication and authorization applied to the IoT

In [29] author described the main patterns and solutions to provide identity management for the classical Internet, Future Internet, Cloud and Experimental Networks, respectively. This section presents the main standards and solutions being used in the context of the Internet of Things.

5.1. Security specifications for web services

The Security Assertion Markup Language (SAML), based on XML language define syntax and rules for creating, requisition and transport information on authentication, authorization and attributes through assertions of security . The eXtensible Access Control Markup Language (XACML) aims to describe access control policies in a format that is interoperable. In the specification of XACML, is also described a protocol to conduct inquiries about access control decisions. The SAML AND XACML standards are widely used in Web Services. The use of these in the IoT is also possible, as can be seen in the works, below.

In [29] have an access control model based on attributes and instructed to Workflow (WABAC), in which permissions are generated for users according to their attributes, attributes of resources, the environment and the current task. In the proposed solution, the SAML is used for the transport of the attributes of the subject and the xacml is used as the language for description of access policies and for taking a decision on which users, based on the SAML assertions, can access which resources.

Initially, before the subject requesting access to the system, it must have a SAML attributes, issued by an authority of attributes. Then, the SAML is inserted in the header of a SOAP request is sent to the system. Upon receiving the request, the system generates the tasks related to the requisition and puts them in a ready state. So one of the tasks is enabled, the Policy Enforcement Point (PEP) gets the attributes of the subject, the task information and assembles a purchase requisition XACML authorization, which is sent to the Policy Decision Point (PDP). It is up to the PDP take the authorization decision based on authorization policies, in the state of the job, and if you need more attributes, will get them through the Policy Information Point (PIP).

Domenech and Wangham proposed an infrastructure for authentication and authorization (IAA) to IoT that makes use of patterns SAML AND XACML.

5.2. Authentication of users with OpenID and windows card space

OpenID is a single sign-on (SSO) protocol that allows users to authenticate to sites (service provider) using the OpenID (account) identifier they desire. OpenID also allows the user to control the information that will be shared with the applications. In OpenID, when a user provides their identifier, it is immediately redirected to their OpenID provider, which performs authentication using the authentication method, which is supported in the indicated OpenID provider. After confirmation of the data, the user is redirected to the service provider, along with its attributes.

Windows CardSpace is a meta-system that allows users to choose, from a portfolio of identities they possess, the one that best fits the context of a given service provider, regardless of the system that originated such identity. CardSpace is a component of Microsoft's .Net platform, designed to provide users with a consistent experience of using multiple digital identities through the use of a specialized user agent called an identity selector. When a service provider requests the authentication and attributes of a user, the CardSpace identity selector transmits the requested information into a digitally signed security token, and this set of attributes can be generated and signed by the user or a provider of external identities, which manages the identity selected by the user.

The use of OpenID, Windows CardSpace and the SAML standard in the Things Internet scenario, for user authentication only, is treated in the Hydra middleware. The authors' proposal is that

there is a complement between technologies to provide a secure identity management solution, in which one technology complements the other.

5.3. OAuth and OpenID connect

OAuth is an authentication and authorization framework that allows a user to share web resources (delegate access to a resource) with third parties without having to share their authentication credentials. With the OAuth protocol it is possible to authorize access to these resources for a given time.
In version 2.0 of the OAuth protocol, four roles are defined: resource owner, resource server, client, and authorization server. One of the possible interactions between the roles has the following steps:

1. The client requests the authorization of the owner of the resource
2. The resource owner checks the client data and returns the authorization permission, represented by an authorization credential from the resource owner
3. The client uses the authorization credential to request the authorization server access token;
4. The authorization server authenticates the client and validates the authorization credential and, if valid, issues an access token
5. The client requests the resource (application) to the resource server and authenticates using the access token
6. The resource server checks the access token, if valid, provides the client resource.

OpenID Connect 1.0 is an identity layer over the OAuth 2.0 protocol. This OpenID integration with OAuth allows a client to verify the end-user identity based on the authentication performed by the Authorization Server, as well as to obtain user profile information, from an interoperable and REST-based solution [6].
According to [6], OpenID Connect 1.0 enables clients of various types, including Web, mobile, and JavaScript clients, to request and receive information about end-user authentication sessions. The specification is extensible, allowing, for example, encryption of identity data and discovery of OpenID Connect providers.
A work in progress that involves the use of OpenID Connect in the WoT scenario is being developed by [7]. The objective of this study is to evaluate the impacts caused by a health care system through the use of a user-centered IdM system. User and device authentication and establishment of trust relationships between users, OAuth server (IdP), and resource server 3 are provided by the OpenID Connect 1.0 authentication and authorization (IAA) infrastructure.
Another work in progress[12], proposes an infrastructure for the provision of physical devices on the Web (WoT) through a service bureau. To control and provide authentication and authorization to access these devices, the solution proposed by the authors is the use of OpenID Connect. In this case, an OpenID Connect server, external to the bus, is responsible for providing end-user authentication that attempts to access the resources (things) made available on the service bus.

6. Conclusion

The possibilities of Internet applications of Things are numerous, and among these there is potential to create intelligent environments through smart objetcts, objects that have the ability to feel and act on the environment in which they are inserted. The differentiated and often restrictive features of IoT, such as its distributed nature, the ease of physical access to objects and objects with restricted computational resources, make security provision a challenge. This paper examined security in the Internet of Things, focusing on authentication and authorization aspects in this scenario. Devices on IoT constantly generate, transmit, modify, and store data, and this information is often confidential to its users. These devices can belong to more than one network (domain) and can travel across more than one domain, which affects authentication and access control approaches.

References

[1] Communities, “Future networks and the internet: Early challenges regarding the internet of things”, Technical report, CTEC, (2008).
[2] Atzori L, Iera A & Morabito G, “The internet of things: A survey”, *Computer Networks*, (2010), pp.2787–2805.
[3] Gubbi J, Buyya R, Marusic S & Palaniswami M, “Internet of things (IoT): A vision, architectural elements, and future directions”, *Future Generation Computer Systems*, (2013), pp.1645–1660.
[4] Guinard D & Trifa V, “Towards the web of things: Web mashups for embedded devices”, *Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web*, Vol.15, (2009), pp.1-8.
[5] Babar S, Stango A, Prasad N, Sen J & Prasad R, “Proposed embedded security framework for internet of things (iot)”, *2nd IEEE International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*, (2011), pp.1–5.
[6] Xiang C & Li X, “General analysis on architecture and key technologies about internet of things”, *IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS)*, (2012), pp.325–328.
[7] Schaffers H, Komninos N, Pallot M, Trousse B, Nilsson M & Oliveira A, “Smart cities and the future internet: Towards cooperation frameworks for open innovation”, *Lecture Notes in Computer Science, The Future Internet*, Vol.6656, (2011), pp.431–446.
[8] Hummen R, Ziegeldorf JH, Shafagh H, Raza S & Wehrle K, “Towards viable certificate-based authentication for the internet of things”, *2nd ACM workshop on Hot topics on wireless network security and privacy*, (2013), pp.37–42.
[9] Mahalle P, Babar S, Prasad NR & Prasad R, “Identity management framework towards internet of things (iot): Roadmap and key challenges”, *Recent Trends in Network Security and Applications*, (2010), pp.430–439.
[10] Fongen A, “Identity management and integrity protection in the internet of things”, *Third IEEE International Conference on Emerging Security Technologies (EST)*, (2012), pp.111–114.
[11] Mahalle PN, Anggorojati B, Prasad NR & Prasad R, “Identity establishment and capability based access control (iecac) scheme for internet of things”, *IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, (2012), pp.187–191.
[12] Hanumanthappa P & Singh S, “Privacy preserving and ownership authentication in ubiquitous computing devices using secure three way authentication”, *IEEE International Conference on Innovations in Information Technology (IIT)*, (2012), pp.107–112.
[13] Roman R, Najera P & Lopez J, “Securing the internet of things”, *Computer*, Vol.44, No.9, (2011b), pp.51–58.
[14] Alam S, Chowdhury MM & Noll J, “Interoperability of security-enabled internet of things”, *Wireless Personal Communications*, Vol.61, No.3, (2011), pp.567–586.
[15] Babar S, Mahalle P, Stango A, Prasad NR & Prasad R, “Proposed security model and threat taxonomy for the internet of things (iot)”, *In Volume 89 of Communications in Computer and Information Science*, (2010), pp.420–429.
[16] Xu X, “Research on safety certification and control technology in internet of things”, *IEEE Fourth International Conference on Computational and Information Sciences (ICCIS)*, (2012), pp.518–521.
[17] Akram H & Hoffmann M, “Laws of identity in ambient environments: The hydra approach”, *IEEE Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, (2008a), pp.367–373.
[18] Jindou J, Xiaofeng Q & Cheng C, “Access control method for web of things based on role and SNS”, *IEEE 12th International Conference on Computer and Information Technology (CIT)*, (2012), pp.316–321.
[19] Liu J, Xiao Y & Chen CP, “Authentication and access control in the internet of things”, *32nd International Conference on Distributed Computing Systems Workshops*, (2012), pp.588–592.
[20] Conzon D, Bolognesi T, Brizzi P, Lotito A, Tomasi R & Spirito MA, “The virtus middleware: An xmpp based architecture for

secure IoT communications", *21st IEEE International Conference on Computer Communications and Networks*, (2012), pp.1–6.

[21] Bonetto R, Bui N, Lakkundi V, Olivereau A, Serbanati A & Rossi M, "Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples", *IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks*, (2012), pp.1–7.

[22] Mahalle PN, Anggorojati B, Prasad NR & Prasad R, "Identity authentication and capability based access control (iacac) for the internet of things", *Journal of Cyber Security and Mobility*, Vol.1, No.4, (2013a), pp.309–348.

[23] Jara AJ, Marin L, Skarmeta AF, Singh D, Bakul G & Kim D, "Secure mobility management scheme for 6lowpan id/locator split architecture", *IEEE Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, (2011), pp.310–315.

[24] Nguyen TD, Al-Saffar A & Huh EN, "A dynamic id-based authentication scheme", *IEEE Sixth International Conference on Networked Computing and Advanced Information Management (NCM)*, (2010), pp.248–253.

[25] Li N, Wang Q & Deng Z, "Authentication framework of iiedns based on ldap & Kerberos", *3rd IEEE International Conference on Broadband Network and Multimedia Technology*, (2010), pp.695–699.

[26] Konidala DM, Duc DN, Lee D & Kim K, "A capability-based privacy- preserving scheme for pervasive computing environments", *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, (2005), pp.136–140.

[27] Kothmayr T, Schmitt C, Hu W, Brunig M & Carle G, "A dtls based end-to-end security architecture for the internet of things with two-way authentication", *IEEE 37th Conference on Local Computer Networks Workshops*, (2012), pp.956–963.

[28] Guinard D, Fischer M & Trifa V, "Sharing using social networks in a composable web of things", *8th IEEE International Conference on Pervasive Computing and Communications Workshops*, (2010), pp.702–707.

[29] Zhang G & Liu J, "A model of workflow-oriented attributed based access control", *International Journal of Computer Network and Information Security (IJCNIS)*, Vol.3, No.1, (2011), pp.47–53.