Building an authorization model for external means of protection of APCS based on the Internet of things

A A Zaharov, O V Nissenbaum, K Y Ponomaryov, E S Nesgovorov

Tyumen State University, 6, Volodarskogo, Tyumen, 625000, Russia

e-mail: o.v.nissenbaum@utmn.ru

Abstract. In this paper we study application of Internet of Things concept and devices to secure automated process control systems. We review different approaches in IoT (Internet of Things) architecture and design and propose them for several applications in security of automated process control systems. We consider an Attribute-based encryption in context of access control mechanism implementation and promote a secret key distribution scheme between attribute authorities and end devices. Keywords – Internet of things, automated process control, information security, access control.

1. Introduction

Contemporary oil and gas development area has several specific features namely:

- sparse control objects;
- hard environmental and climatic conditions;
- specific social infrastructure in hydrocarbon production areas;
- variety of the automated process control systems (APCS);
- high system reliability requirements;
- high standards of health care and requirements for safety of service staff.

All these features require new approaches to management of production profitability by implementation of technical solutions and special control systems focused on energy-saving technologies, minimization of human labor involved to the production process.

The concept of the Internet of Things (IoT) evolves over time. The key idea is following: it is an information system consisting of various integrated physical entities. In this concept entity is a device that has an ability to transmit data to computer networks (e.g. sensor, smartphone, computer, video camera, etc.). All these devices are connected in the same network; therefore, they can interact with each other and an external environment. There are different options of IoT implementation [1]: production control systems (noise, vibration, pipe deformation, corrosion, soil movement, temperature and pressure measurement can be identified by displacement, pressure sensors, etc.), intelligent energy monitoring system, industrial processes automation, etc.

Distributed networks collecting information from sensors can also be used to control physical secure perimeter. In this case, the Internet of Things concept is applied not to the automated control systems, but to the physical environment in which they are located to build secure perimeter. However, there are many problems and limitations intrinsic to IoT itself, not to several application area. Therefore, we have several problems to consider with IoT itself in light of adaptation to the automated process control system.

It is necessary to keep in mind following IoT requirements, described by E. Leloglu [2]:

- [Requirement 1]
- [Requirement 2]
- [Requirement 3]
- [Requirement 4]
- [Requirement 5]
• resource constraints: In IoT architecture, most of nodes lack of storage capacity, power and CPU, generally using low-bandwidth communication channels. It is challenge to apply some security techniques;

• data volumes: although some IoT applications use brief and infrequent communication channels, there are considerable number of IoT system such as sensor-based, logistics and large scale system that have potentials to entail huge volume of data on central network or servers;

• privacy protection: since a great number of RFID systems are short of suitable authentication mechanism, anyone can tracks tags and find the identity of the objects carrying them. Intruders can not only read the data, but can also modify or even delete data as well;

• scalability: the IoT network consists of a large number of nodes. The proposed security mechanism on IoT should be scalable;

• autonomic control: traditional computers need users to configure and adapt them to different application domains and different communication environments. However, objects in IoT network should establish connections spontaneously, and organize/configure themselves for adapting to the platform they are operating in. This kind of control also involves some techniques and mechanisms such as self-configuring, self-optimizing, self-management, self-healing and self-protecting.

Several scientific sourced focuses a significant attention on issues of access control in IoT networks. There is also a need for detailed and granular information control and an ability to take into account the location coordinates with limited computing resources.

An IoT-system often has a distributed architecture: all objects of the network can extract, process, combine and provide information to other objects. All sensors are able to interact with each other within the wire or wireless network. A distributed network connecting heterogeneous devices is a platform to create complex software products. In order to construct such structure, it is necessary to answer the following questions:

• How to authenticate many devices and sensors in dynamic environment?
• How to implement the access control mechanism?
• How should data providers and processors learn about each other’s true identifiers, properties and network addresses?
• How to achieve connectivity in conditions of heterogeneous network elements with different interaction methods?

2. Main part

Access control is an important point of information systems security, such as computer networks that include data collection sensors. Due to the growing trend of sensor intellectualization, there is a need to distribute access at the application level of the interaction model, which provides support for processes and management of network objects.

It is possible to build an access control system with Attribute-Based Encryption (ABE) cryptographic scheme in distributed networks. ABE schemes were introduced by Sahai and Waters [3]. Multiple attributes, that regulate access to specific information, have to be defined when building systems with Attribute-Based Encryption. Each message in this system has a certain set of attributes. Every user secret key contains access tree with certain attributes. The message data can be decrypted only when message attributes satisfy access tree requirements. This concept is called Key Policy (KP-ABE). Trusted centers issue keys to users and also verify attribute values. Ciphertext Policy (CP-ABE) is an example of another technique in which the access tree is encrypted into a data packet and the user key includes the validation attributes.

Another access control model is based on registration of devices on the authentication server (SA), generating a common secret key. Attribute Authority conduct the same operations. Thus, each node of the system and each trusted center have a common secret key with SA. Access control is achieved by applying attribute encryption, since all messages between devices are encrypted with secret keys based on the access structure. Attributes are different characteristics of the end devices or application area. It
is necessary to consider the method to distribute keys from trusted centers to sensors, because attributes can change in a dynamic environment and in response to new changes there is a need to obtain a new secret key. We will describe this process using the Otway-Rees protocol [4]. We assume that device initiates the transfer of a new set of attributes and AA has a mechanism for authenticating it.

### Table 1. Notifications

| Symbol | Value |
|--------|-------|
| $N$    | Node that requests new key when attribute value has been changed |
| $AA$   | Identifier of Attribute Authority: trusted center that distributes keys |
| $SA$   | Identifier of Service Authority: trusted center that shares keys between AA and $N$ |
| $I$    | Session number identifier |
| $E_N$  | Symmetric-key encryption with key common for $N$ and SA |
| $E_A$  | Symmetric-key encryption with key common for AA and SA |
| $K_{ABE}$ | Key of ABE algorithm based on new attributes of $N$ |
| $attr_{new}$ | New set of attributes |
| $R_N, R_A$ | Random numbers created by $N$ and AA respectively |
| $K$    | Session key |

1. The device $N$ sends to AA the session number, the random number and the set of attributes that are encrypted on the common with SA key.

   $$N \rightarrow AA: I, N, AA, E_N(R_N, attr_{new}, I, N, AA).$$

2. The Attribute Authority transmits the received encrypted SA message, and also encrypts its pseudo-random number with their common key.

   $$AA \rightarrow SA: I, N, AA, E_N(R_N, attr_{new}, I, N, AA), E_A(R_A, I, N, AA).$$

3. SA decrypts received messages, extracts parameters $I, N, AA$ and checks if they match with parameters transmitted in the clear text. If values do not match, SA must abort the protocol session or send a request for resubmission. It also generates a shared session key for $N$ and AA, extracts the attributes and a signature from the message from $N$ and passes them to AA.

   $$SA \rightarrow AA: I, E_N(K, R_N, attr_{new}), E_A(K, R_A, attr_{new}).$$

4. At this stage, AA checks an equality of the received random number generated earlier and checks the session number. After that, it generates a new encryption key based on the received attributes and sends key to $N$ encrypted with a symmetric cipher using the session key obtained from SA. At that moment, AA can approve SA authenticity, otherwise SA would not be able to decrypt the message and return the same pseudo-random number.

   $$AA \rightarrow N: I, E_N(K, R_N, attr_{new}), E_K(K_{ABE}).$$

5. The device $N$ decrypts messages. It retrieves the key containing the access tree (KP-ABE) or the attributes (CP-ABE) using a session key. It is also necessary to check if the set of attributes match the previous values. $N$ verifies $SA$ by checking a pseudo-random number. There may be additional step with $AA$ returning delivery message.
Despite a broad presence of information on the capabilities and models of attribute encryption in the scientific literature, many issues are still open and have to be resolved.

- How to verify the authenticity of attributes during a private key generation?
- How to transfer secret keys in a secure way in a dynamic and open environment?
- What scheme does not have disadvantages of the attribute encryption? For example, how to exclude the possibility of the key sharing by user and transferring its parts to other participants?
- How to hide the attributes of participants and messages in CP-ABE schemes?

There is a large number of documented attribute encryption types [5-9], including papers studying the application of attribute encryption in IoT [10, 11] and most of them implement different approaches to the transformation of data. However, there is no survey evaluating their advantages and disadvantages.

The Internet of things is rapidly developing area, and the number of new devices connected is growing exponentially. Hence, there is an obvious problem with the fact that the network ontology is unknown and changes dynamically. Thus, there is a chance that the services become unavailable and applications cannot find the required devices due to their unavailability (e.g. when changing the geo position) [12, 13].

To solve this problem, it was proposed to use a special software that stores the ontology and handles all requests in the system. Object’s data can be supplemented with special fields to simplify the work of the service. For example, store its attributes (if they do not contain confidential information). When registering a new sensor, all information about it (a unique URI, the subnet segment in which it is located, etc.) is stored in databases. Further, when a request is received from the business logic application, it is redirected to the software service where additional authorization is possible, for example, verifying the access rights to perform the required operation, and in case of authorized operation, the service returns information about the logical or physical location of the requested object.

In the context of a distributed system, each subnet can have its own instance of the entity for a flexibility and scalability. In this case, there is a difficulty with the distribution of information between all nodes of the system and maintaining its relevance. As one of options, routing protocols can be implemented by grouping information about hosts on a set of defined parameters and forwarding it to related entities. In this scheme, the problem of maintaining the relevance of data is critical and require a separate analysis.

The issue of actualization, that is, an authenticated update of device attributes, is put in one way or another in all applied research of ABE. There are various approaches to solving this problem, starting with fairly simple ones, for example, centralized lists of attributes, up to very complex schemes that allow to confirm the updating of attributes by various supervisors within their authority to change one
or another attribute [14]. In the IoT with a decentralized structure, it seems appropriate to apply the latter approach.

3. Conclusion

Modern network concepts, such as the Internet of things, can be used as a system of physical protection for production facilities. In this case, the system is a distributed network for collecting and analyzing data from sensors.

This article describes the problems of a distributed approach of building the Internet of things, which is the most effective in terms of capabilities and the most difficult to implement at the same time. The main problems of this approach are authorization and access control models, registration and authentication mechanisms and ontology schemes for service discovery. The large number of devices and the dynamic nature of the interaction between them are properties of the Internet of things which give rise to additional questions of fault tolerance, control and scalability. In order to build an access control system, it was suggested to use attribute encryption. Introduced a model for distributing secret keys in conditions of a large number of devices and trusted centers.

The merits of attribute encryption are flexible settings of access structures. Attribute based encryption allows encryption of a message between all devices in the network. At the same time if knowledge of the attributes is not secret, it increases privacy risks for specific application areas. The management of cryptographic keys is the bottleneck of ABE in a distributed network. The solving of this problem is the Otway-Riis protocol with a single trusted center for all nodes. Each entity needs to store only one key for communication with this trusted center. However, this scheme generates failover risks due to a single communication node. The shared secret key is generated during the registration process on the trusted the authentication server. It is planned to implement a software prototype in a laboratory, which allows to identify other possible shortcomings.

References

[1] Kupriyanovskiy V P, Namiot D Ye, Drozhzhinov V I, Kupriyanovskaya Yu V and Ivanov M O 2016 Internet of Things in industrial plants Int. Journal of Open Information Technologies 4 (12) pp 69-78
[2] Leloglu E 2017 A Review of Security Concerns in Internet of Things Journal of Computer and Communications 5 pp 121–136
[3] Sahai A and Waters B 2005 Fuzzy Identity-Based Encryption Advances in Cryptology V (Eurocrypt) pp 457–73
[4] Otway D and Rees O 1987 Efficient and Timely Mutual Authentication Operating Systems Review 24 (1) pp 8–10
[5] Waters B 2011 Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization Int. Workshop on Public Key Cryptography 6571 pp 53–70
[6] Ostrovsky R, Sahai A and Waters B 2007 Attribute-based encryption with non-monotonic access structures Proc. of the 14th ACM conf. on Computer and communications security (ACM) pp 195–203
[7] Lewko A 2010 Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques 6110 (Springer Berlin Heidelberg) pp 62–91
[8] Lewko A and Waters B 2011 Decentralizing attribute-based encryption Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques (Springer Berlin Heidelberg) pp 568–88
[9] Wang G, Liu Q and Wu J 2010 Hierarchical attribute-based encryption for fine-grained access control in cloud storage services Proc. of the 17th ACM conf. on Computer and communications security (ACM) pp 37–735
[10] Wang X, Zhang J, Schooler E M and Ion M 2014 Performance evaluation of attribute-based encryption: Toward data privacy in the IoT Communications (ICC) 2014 IEEE Int. Conf. on (IEEE) pp 30–725
[11] Yao X, Chen Z and Tian Y 2015 A lightweight attribute-based encryption scheme for the Internet of Things *Future Generation Computer Systems* **49** pp 12–104
[12] Hachem S, Teixeira T and Issarny V 2011 Ontologies for the internet of things *Proc. of the 8th Middleware Doctoral Symp.* (ACM) p 3
[13] Wang W, De S, Toenjes R, Reetz E and Messner K 2012 A comprehensive ontology for knowledge representation in the internet of things *Trust, Security and Privacy in Computing and Communications (TrustCom) 2012 IEEE 11th Int. Conf. on* (IEEE) pp 98–1793
[14] Chase M 2007 Multi-authority attribute based encryption *Theory of Cryptography Conf.* (Springer Berlin Heidelberg) pp 34–515