Proceedings of the International Conference , "Computational Systems for Health & Sustainability"
17-18, April, 2015 - by R.V.College of Engineering,
Bangalore,Karnataka,PIN-560059,INDIA

SECURITY OF SMART OBJECTS IN IoT

[1]Divyashree HJ, [2]Shanchiher Nikunj, [3]Manjunath CR
[1, 2, 3]School of Engineering and Technology, Jain University

Abstract The internet of things involves people interacting with the technological environment based on what we considered things as "smart objects" allowing sharing of information through communication on internet. As the concept of IoT and its application is growing rapidly, the security aspect becomes very important and critical which has to be looked upon with severe importance. Security is needed anywhere where computation happens. Since the IoT allows various objects or devices to connect to internet forming a network communicating with each other or with the human user, the usage of large scale of objects on the network and the heterogeneity of those objects plays as a major security issue. Therefore, we focus on the security and privacy aspects regarding the issues, the various challenges that are being faced, and try to study the feasible solutions for the above security challenges, and also using few applications as examples. According to the observations made, it is found that there are two main approaches as referred in the existing papers which are systemic and cognitive approach. Due to the large number of interactions between things, a systemic and cognitive approach and decentralized approach seems to be an appropriate choice for IoT security.

Keywords—smart objects, systemic and cognitive, decentralised approach.

I. INTRODUCTION

"A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in internet environment." Incorporating IoT into our lives introduces many benefits into several domains such as health-care, transportation, safety and business. With the uninterrupted evolution of technology, new opportunities have been created to set up new experiences and practices in our everyday life. Information and intelligence became distributed and passive entities are turning out to be active participants of our lives when connected to the Internet. In this new context, it became possible for objects, services and applications to make decisions and to react according to a given situation in their environment.
Some of the commonly known examples of Internet of things are as follows

- Today's vehicles, for example, have multiple networks to control engine function, safety features, communications systems, and so on.
- Commercial and residential buildings also have various control systems for heating, venting, and air conditioning, telephone service, security and lighting.

The Internet of Things is a complex paradigm in which people interact with the technological ecosystem based on smart objects through complex processes. Therefore the security, privacy and trust with respect to the smart object is necessary to ensure their efficient behavior in the technological ecosystem. Hence Smart objects play an important role in IoT, and also security of these smart objects become necessary.The IoT has gained much research attention the last few years due to the plethora of applications it supports for improving and simplifying peoples' lives. Everyday objects are being interconnected, communicate with each other and exchange the information they sense, and thus become "smart". However, users and service providers are reluctant to exploit this IoT potential without assurance for the safety of private information. With Smart Objects new security and privacy issues arise, like data integrity, information privacy, trust and safety.. While in recent years many technological challenges have already been solved through the extension and adaptation of wireless technologies, security and privacy still remain as the main barriers for the IoT deployment on a broad scale. Some of the challenges that we are addressing in this study are

1. Smart object identification and location.
2. Authentication and authorization.
3. Privacy, security and trust.
4. Smart object interaction.

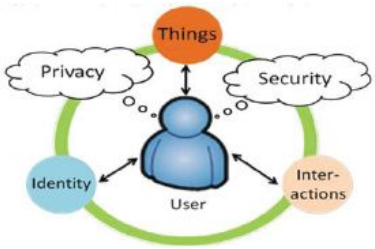


Figure 1

1. SMART OBJECT IDENTIFICATION

The main challenge of object identification is to ensure the integrity of records used in the naming architecture. Although the Domain Name System (DNS) provides name translation services to Internet users, it is an insecure naming system. It remains vulnerable to various attacks, such as DNS cache poisoning attack, and man-in-the-middle attack. This poisoning attack injects counterfeit DNS records into victims' cache and directly compromises the resolution mapping between naming architecture and addressing architecture. Therefore, without the integrity protection of the records, the entire naming architecture is insecure. Domain Name Service Security Extension (DNSSEC, IETF RFC4033) is deployed as the security extensions of DNS. DNSSEC can ensure the integrity and authenticity of a Resource Record (RR), and atthe same time serve as a vehicle for the distribution of cryptographic public keys. Although DNSSEC seems to be a remedy for naming services, it is still challenging to deploy DNSSEC properly in IoT. DNSSEC incur high computation

and communication overhead and may not be suitable for IoT devices. A new naming service is desirable.

2. AUTHENTICATION AND AUTHORIZATION

Although public-key cryptosystems have advantage for constructing authentication schemes or authorization systems, the lack of a global root certificate authority (global root CA) hinders many theoretically feasible schemes from actually being deployed. Without the global root CA, it becomes very challenging to design an authentication system for IoT. Furthermore, it may be infeasible to issue a certificate to an object in IoT since the total number of objects is often huge. Therefore, the concept of delegated authentication and delegated authorization must be taken into consideration for IoT.

3. PRIVACY SECURITY AND TRUST

The challenges can be divided into two categories: data collection policy and data anonymization. Data collection policy describes the policy during data collection where it enforces the type of collectable data and the access control of a "Thing" to the data. Through the data collection policy, the type and amount of information to be collected is restricted in the data collection phase. Since the collection and storage of private information is restricted, privacy preservation can be ensured. The second challenge is data anonymization. To ensure data anonymity, both cryptographic protection and concealment of data relations are desirable. Given the diversity of the "Things", different cryptographic schemes may be adopted. For example, lightweight cryptographic schemes are more suitable to devices that have resource- constraints. The second category, concealment of data relation, investigates the removal of direct relations between the data and its owner. This also can be achieved by applying data encryption where scrambled data has resistance against data analysis. However, information needs to be shared amongst "Things" in IoT; therefore, computation on encrypted data is another challenge for data anonymization. To cope with the problem, some of research works in homomorphic encryption may be applicable.

4. SMART OBJECT INTERACTION

The interactions of the four IoT components i.e., person, intelligent object, technological ecosystem, and process in IoT, highlight a systemic and cognitive dimension within security of the IoT. The interaction of people with the technological ecosystem requires the protection of their privacy. Similarly, their interaction with control processes requires the guarantee of their safety. Processes must ensure their reliability and realize the objectives for which they are designed. We believe that the move towards a greater autonomy for objects will bring the security of technologies and processes and the privacy of individuals into sharper focus. Furthermore, in parallel with the increasing autonomy of objects to perceive and act on the environment, IoT security should move towards a greater autonomy in perceiving threats and reacting to attacks

II. APPROACHES

The challenges mentioned above can be restrained by certain approaches which can decrease the risk that is caused in IoT and achieve a secure smart environment. According to the observations made, it is found that there are two main approaches as referred in the existing papers which are systemic and cognitive approach and decentralized approach.

A. Systemic and cognitive approach

Due to the large number of interactions between things, a systemic and cognitive approach seems to be an appropriate choice for IoT security. To become fully secure, they propose a three dimensional pyramid-shaped model, where process, people, technology and organization are at the vertexes. We include in our approach a cognitive dimension in order to give the flexibility to the system to be able to analyze different situations and perform the most suitable measures to guarantee reliability and security. The systemic and cognitive approach for IoT security, is made up of four nodes, namely person, people, technology, and intelligent object. To guarantee conformity in conception and implementation of secure applications, all these nodes must cooperate.

We consider a scenario that involves a home owner, who plays the role of people, sensors and actuators within the house perform the role of intelligent objects, communication means and protocols depict the technological ecosystem and remote monitoring of heater represents the process. In this scenario, the home owner needs to identify the right sensor or actuator to adapt the ambient temperature to his/her preferences. The actuator has to trust the originator of the command to react correctly. This process should not involve anyone else, then, privacy must be guaranteed. Safety of people and equipment when performing this action must be a priority to protect people's health. Finally, the smart object must ensure its immunity against physical or logical intrusion.

The four planes within which the interactions among the nodes take place through the interactions that are visible in Fig. 2, where we give a 2D perspective of each group of nodes. These planes are specified according to the relationships among the different triads of nodes.

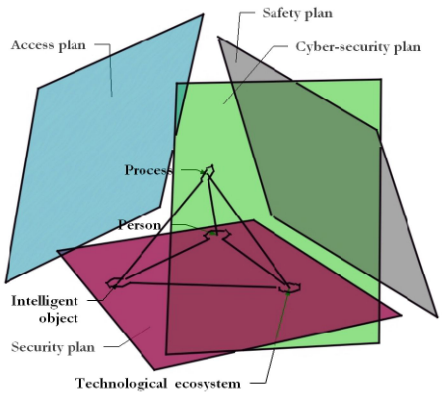


Figure 2

- Safety plane - The Safety plane concerns process, person and technological ecosystem and involves the following

tensions: privacy, safety and reliability. In this plane, the technological choice made by a person to perform a given process like analyzing, storing or distributing data must be done in a safe and reliable manner.

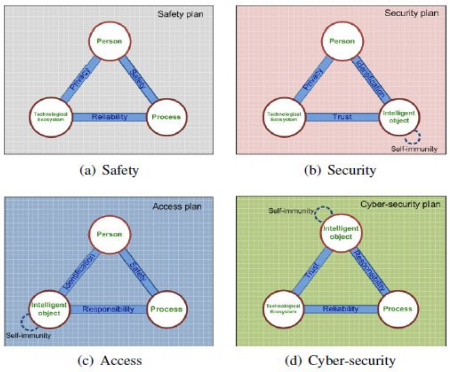
- Security plane - The Security plane includes person, technological ecosystem and intelligent object and details related tensions namely: trust, privacy and identification. In the IoT, all kinds of objects and equipment are connected together through different technologies and networks. Then, users can profit to develop and benefit from new services and applications.

- Access plane - The Access plane contains process, person and intelligent object and implies their connected tensions: identification, safety and responsibility. The intelligent objects are able to interact with other networked entities (objects and/or persons) and store information related to a specific process. This interaction must be developed in a fluent manner that identifies correctly the intelligent objects, respects safety rules of humans and equipment and precise convenient access rules and responsibilities for each entity.

- Cyber-security plane - The Cyber-security (Fig. 2(d)) plane includes process, technological ecosystem and intelligent object. The tensions considered for this plane are responsibility, trust and reliability. The objective is to produce an effort to ensure security properties of the IoT cyber environment against security risks.

The main features of the actors involved in our model, namely: person, process, technological ecosystem and intelligent object, and we highlight the role of each actor.

Person: Security concerns are always depending on people's interest and intentional/unintentional behavior. They must be conscious of the necessity of having security background including objectives, risks, practices, choices, loyalties and skills. Concretely, humans must accomplish the tasks related to security rules management, which consists of:



(a) Safety (b) Security

(c) Access (d) Cyber-security

Figure 3

- Addressing security practices and rules to develop an efficient security policy documentation.

- Auditing security practices and rules effectiveness including personnel, documentation and technical control procedures.

- Implementing practices and rules in operational mode.

Process: The process node is about a mean or a way to perform tasks in the IoT environment according to specific security conditions. Process must be in accordance with effective security policies to guarantee a sufficient level of security at different IoT architecture layers. A set of standard areas to consider when performing a secure process

- Information Security Risk Assessment.
- Information Security Strategy.
- Security Controls Implementation.
- Security Monitoring.
- Security Process Monitoring and Updating.

Technological ecosystem: The third node is about the technological alternatives taken to guarantee acceptable IoT security level describes five categories of information security elements:

- Security Design and Configuration;
- Identification and Authorization;
- Enclave internal;
- Enclave boundary;
- Physical and environmental.

Intelligent object: The intelligent object is quite a new node that refers to an object like sensing node (camera, X-ray machine, etc.), an RFID reader or tag (detecting the presence of a person, an animal or an object) involved in a given application. This object is enhanced by electronic features to interact with other objects. It becomes able to collaborate, share and exchange information about its environment, and react to specific events by performing adequate functioning.

The above approach the Internet of Things is a complex paradigm in which people interact with the technological ecosystem based on smart objects through complex processes. The interactions of these four IoT components, person, intelligent object, technological ecosystem, and process, highlight a systemic and cognitive dimension within security of the IoT. The interaction of people with the technological ecosystem requires the protection of their privacy. Similarly, their interaction with control processes requires the guarantee of their safety. Processes must ensure their reliability and realize the objectives for which they are designed. We believe that the move towards a greater autonomy for objects will bring the security of technologies and processes and the privacy of individuals into sharper focus.

B. Decentralised approach

A distributed capability-based access control mechanism which is built on public key cryptography in order to cope with some of these challenges. Specifically, our solution is based on the design of a lightweight token used for access to CoAP Resources, and an optimized implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) inside the smart object. The feasibility of the approach is promising in order to cover more complex scenarios in the future, as well as its application in specific IoT use cases.

Distributed CapBAC This proposal makes use of capability-based access control model (CapBAC), whose description, motivation and advantages against other models for IoT scenarios can be found further. Work is based on technologies specifically designed for IoT environments, facilitating a distributed approach in which smart things themselves are able to make fine-grained authorization decisions. These decisions are based on local conditions, providing context-awareness in the authorization process. This work suggests the use of public key cryptography whose characteristics fit the requirements of IoT regarding scalability and interoperability. The highly optimized version of ECDSA is implemented within the smart object ensuring end-to-end authentication, integrity and non-repudiation, without the intervention of any intermediate entity.

The basic operation of our proposed distributed capability based access control, we clarify the different steps of the process.

• Issue Capability Token. As initial step, the Issuer entity, usually instantiated by the device owner, issues a capability token to the Subject to be able to access that device. Additionally, in order to avoid security breaches, the Issuer signs this token by using ECDSA, whose value is attached to the capability token.

• Access Request. Once the Subject has received the capability token, it attempts to access the device. For this purpose, it generates a CoAP request, in which the token is attached. The inclusion of the token into the request has been carried out using the payload field, and the Content-Format header to indicate the representation format of the payload inside the request. In addition, the Request-Uri option is used to indicate the specific resource to be accessed in the Device. Finally, the Subject also signs the CoAP request itself using ECDSA algorithm, whose value is attached to that message by adding a new header called Signature.

• Get Authorization Decision. When the Device receives the access request, the authorization process is carried out. First, the application checks the validity of the token as well as the rights and conditions to be verified. Then,due to the cost of these operations, the Issuer signature is verified and Subject is authenticated.

• Return Authorization Decision. Finally, once the authorization process has been completed, the Device generates a CoAP response based on the authorization decision. In the case of a unauthorized request, a Unauthorized 4.01 response is returned, indicating that the Subject is not authorized to perform the requested action. Otherwise, the value of the answer will depend on the content of the request.

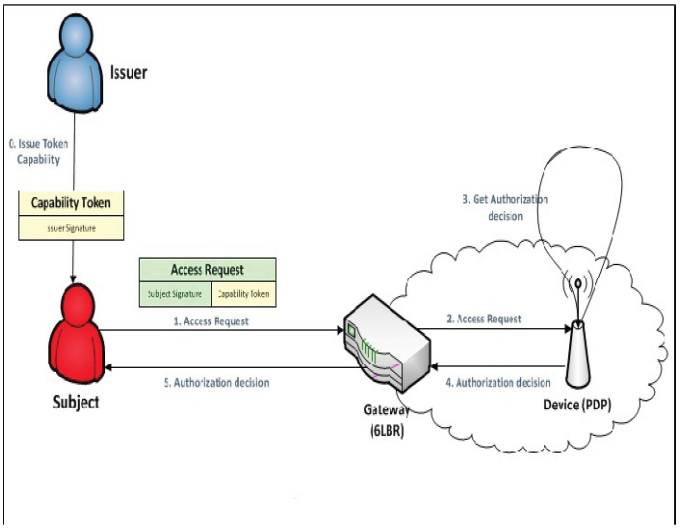


Figure 4

CONCLUSION

With the increasing autonomy of objects to perceive and act on the environment, IoT security should move towards a greater autonomy in perceiving threats and reacting to attacks i.e. when the number of smart objects are increased we need to integrate more security example for smart cities. Thus we need a distributed or a decentralized approach which enhances the secure behavior of these smart/intelligent objects and provide safety, privacy and trust. Further the data involved in these huge number of smart devices need to be analyzed and aggregated which also is a major challenge.

The huge amount and particularly sensitive information generated by users and smart objects, and the proliferation of emerging services affecting our everyday lives, create the need to properly address security and privacy issues.A distributed approach to control access to this sensitive information has been presented in order to cope with the challenges about security and privacy previously described, further when more features are added to the distributed systems it might be suitable for different cases of IoT.

REFERENCES

[1] Antonio F. Skarmeta, Jos´e L. Hern´andez-Ramos, M. Victoria Moreno"A decentralized approach for Security and Privacy challenges in the Internet of Things",

[2] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, "IoT Security: Ongoing Challenges and Research Opportunities"

[3] Dr. Ovidiu Vermesan SINTEF Norway, Dr. Peter Friess Belgium,"Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems".

[4] Arbia Riahi_, Enrico Natalizioy, Yacine Challaly, Nathalie Mittonz, Antonio Ierax,"A systemic approach for IoT security"

[5] Henrich C. P¨ohls, Vangelis Angelakis, Santiago Suppan, Kai Fischer, George Oikonomou, Elias Z. Tragos, Rodrigo Diaz Rodriguezk "Building a Reliable IoT upon Privacy- and Security- enabled Smart Objects and Theodoros".