ISSN 2277-3061
Volume 15 Number 04
INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Security Frameworks: A Study on Different Approaches for the Internet of Things

Luan Oliveira, Zair Abdelouahab, Breno Sousa, Denivaldo Lopes
UFMA, PPGEE, Avenida dos Portugueses, s/n,
Cidade Universitária, CEP 65085-580, São Luís MA Brazil
luan.oliveira.c@gmail.com
UFMA, DEEE, Avenida dos Portugueses, s/n,
Cidade Universitária, CEP 65085-580, São Luís MA Brazil
zair@dee.ufma.br
UFMA, DEEE, Avenida dos Portugueses, s/n,
Cidade Universitária, CEP 65085-580, São Luís MA Brazil
breno_fabricio23@hotmail.com
UFMA, DEEE, Avenida dos Portugueses, s/n,
Cidade Universitária, CEP 65085-580, São Luís MA Brazil
dlopes@dee.ufma.br

ABSTRACT

This paper provides an overview of some of the major works that focus on the use of security frameworks for Internet of Things environment to facilitate the development of applications for this scenario. The Internet of things or "IoT" is characterized by a high heterogeneity degree of devices and network protocols, where all kinds of communications appear to be possible, even unauthorized ones. As a result, requirements such as reliability, connectivity, privacy and security are becoming increasingly more critical. This paper discusses the applicability and limitations of the main existing security frameworks in the context of the Internet of Things.

Indexing terms/Keywords

Internet of Things, Frameworks, Security.

TYPE (METHOD/APPROACH)

Survey

INTRODUCTION

Due to various types of technologies created for the internet in order to connect more people and different devices, the challenge is to facilitate the interaction of these heterogenous objects with the real world. This feature of connecting and representing real physical objects through an Internet connection is the so-called Internet of Things (IoT) [1]. It offers new project opportunities for interactive applications containing static documents, real-time information concerning the places and objects of the physical world [16].

However, technological challenges required by this connectivity need to be addressed, including interoperability between devices, autonomy of systems, security issues, privacy and trust. Security mechanisms, such as encryption, privacy and trust are needed to protect data traffic or information between devices and the Internet. Encryption provides privacy in communication between two entities without the participation of unauthorized entities [3]. Authentication is a service that performs the mutual identification between two entities to communicate with each other. [4].

Since there are a variety of applications and devices in the IoT scenario, mechanisms to facilitate the development of applications with these requirements are increasingly necessary. One possible solution is to use frameworks to perform these tasks. Thus, facilitating the creation of software for various devices in situations where security requirements are necessary since in most cases the complexity of software development requires greater effort by the developer to achieve the purpose.

In this paper, we discuss some security frameworks for the Internet of Things, and in particular, security techniques employed in such solutions, analyzing possible strengths and limitations. It is organized as follows: section 2 and 3 present a review of the main concepts of security, privacy and trust in the Internet of Things. Section 4 shows the work done in the area of security frameworks for Internet of Things. Finally, in section 5, we present the conclusion of a report of possible working improvements that can contribute to a better security solution for the Internet of Things.

INTERNET OF THINGS

IoT has emerged as a new computing paradigm that aims to facilitate and enable smart and heterogeneous devices to communicate through the World Wide Web (Internet) [2]. Each device (thing) is an autonomous entity and has its own operating characteristics [5]. These devices are characterized as nodes in the network, and may or may not have a centralizing entity responsible for their management.

With the possibility of communication between different devices, it has brought new perspectives on solving problems in different areas of knowledge, as well as in entertainment areas. The exchange of information between these multitudes of devices creates a massive amount of information to be managed carefully. The use of communication protocols is a crucial factor in IoT, because it is a new paradigm, some options may behave unsatisfactorily in certain situations.

Another factor of great importance in IoT is security. In the literature we can find a variety of proposed solutions, however they also have limitations in most cases. The following section presents concepts about security in IoT.

SECURITY, PRIVACY AND TRUST IN THE INTERNET OF THINGS

The security factor in computing environments is a key point to guarantee the proper functioning of a system. Following this premise, IoT devices must have mechanisms that meets this need.

The author [17] reports the concepts of security, privacy and trust. It states that information security should ensure integrity, confidentiality and authentication in computer systems. But the concept of privacy is related to the system's ability to keep information private, accessible only to authorized users. Finally, the trust is more complex to be defined in the literature, however, this is related to the metric definition of business, technical, legal, and regulatory assessment methodologies of certain systems.

As highlighted in [5], ensuring the protection of devices in IoT is an arduous and time consuming task, because its architecture is designed to handle billions of objects intercommunicated with each other, generating often a huge amount of data to be managed. This amount of information can be a magnet for badly intentioned people. The devices can be constantly under attacks, thus requiring a better attention to the security mechanisms for such components. In this context, [5] reported that the authors in [7, 8, 14] highlighted some of the challenges faced in IoT as:

- Heterogeneity influences the security of the network protocol services in IoT devices;
- Identity management of the devices is difficult because of the large number of connected devices;
- The large volume of data generated by devices in IoT is a major threat to privacy because the information must be managed so that the privacy of its content must be guaranteed;
- The number of devices as well as the heterogeneity affects the trust and governance of such devices. Trust is affected in two ways: trust relationships between different devices, and the actions they can perform; and trust in the user point of view of the system, as users should be able to manage their things so as not to feel under some unknown external control. In relation to governance, on the one hand, it offers stability, support for political decisions, and the possibility of defining common frameworks and interoperability mechanisms. On the other hand, the government can easily become excessive, encouraging a super controlled environment.
- As IoT evolves, devices belonging to this paradigm become attractive to potential attacks, therefore, it is necessary that they have the ability to be faults tolerants.

However, the search for new security mechanisms and methods must be a constant task because threats are always in a process of evolution as the IoT paradigm is improved.

FRAMEWORKS FOR INTERNET OF THINGS

The heterogeneity of internet of things technologies, the large number of devices and systems, and the different types of users and roles create significant challenges in this context. In particular, security requirements, authentication, reliability, confidentiality, integrity, privacy and context management are difficult to solve, even with the huge volume of existing work. In the literature there are various ways to provide these requirements [11], [12], [9], [10] and [13]. Some related works are listed below.

The VIRTUS Middleware: A XMPP Based Architecture For Secure IoT Communications

The work proposed by [11] presents the middleware VIRTUS, which is event-driven and is based on the XMPP protocol (eXtensible Messaging and Presence Protocol) having security mechanisms that contribute to interoperability such as the servers federation and mapping over HTTP. In VIRTUS, the TLS (Transport Layer Security) and SASL (Simple Authentication and Security Layer) are used to ensure integrity and confidentiality of messages and authentication of the parties involved, respectively. Figure 1 shows the modules of VIRTUS middleware.

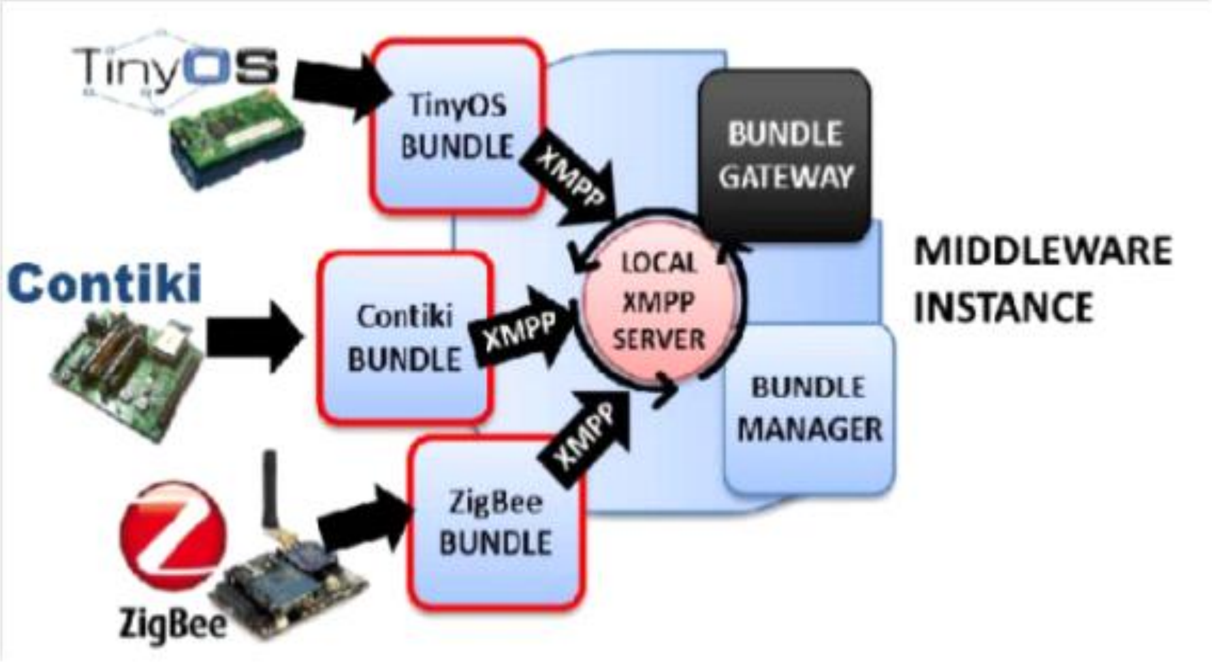

Fig. 1: The VIRTUS middleware [11]

Figure 1 illustrates the modules present in VIRTUS [11] middleware as described below:

- **Custom modules**: also called bundles (eg Zigbee bundle), are used to enable communication between devices with computational constraints and the VIRTUS Server, translating the specific messages from device technology to XMPP. They are usually deployed as an intermediary between the device and the rest of the middleware;
- **VIRTUS Server**: used to manage the communication between the middleware components. There is a server for each network (domain) where the middleware is implemented;
- **Manager**: manages the connection between various middleware modules. It also provides a list of available modules and makes managing dependencies;
- **Gateway** communicates with the local instance of VIRTUS Server, as well as remote middleware instances. This component is the intermediary between any application that wants to communicate with any device within the middleware.

The middleware considers the existence of three distinct types of devices: devices with many features such as servers that implement all the middleware; restricted devices such as smartphones that implement the client XMPP modules to interact with other modules and simple devices such as sensors and RFID tags which has its encapsulated messages in XMPP format by another device with more computing resources. The intra-domain and inter-domain communication is done through exchange of XMPP messages, but there are modules that allow communication with other architectures, such as with Web Services.

A Service Infrastructure for the Internet of Things based on XMPP

The work proposed by [12] provides a service platform based on the XMPP for the development and provision of pervasive infrastructure services. The paper is based on two case studies (robot control and e-mobility) in IoT scenario, demonstrating the real-time capability of the architecture. The work focuses on Services Platform (XMPP based Service Platform) that provides an execution environment for multiple services dynamically. It is based on a data concentrator, a portion of the service execution environment, a service platform that connects with various real-world objects. The platform connects the services with several real-world objects such as sensors and mobile devices. Another feature is the device management which handles the provisioning of applications for mobile devices as well as the management of users and devices. The paper addresses security issues, authentication with the XMPP protocol. Figure 2 shows the architecture of the work.

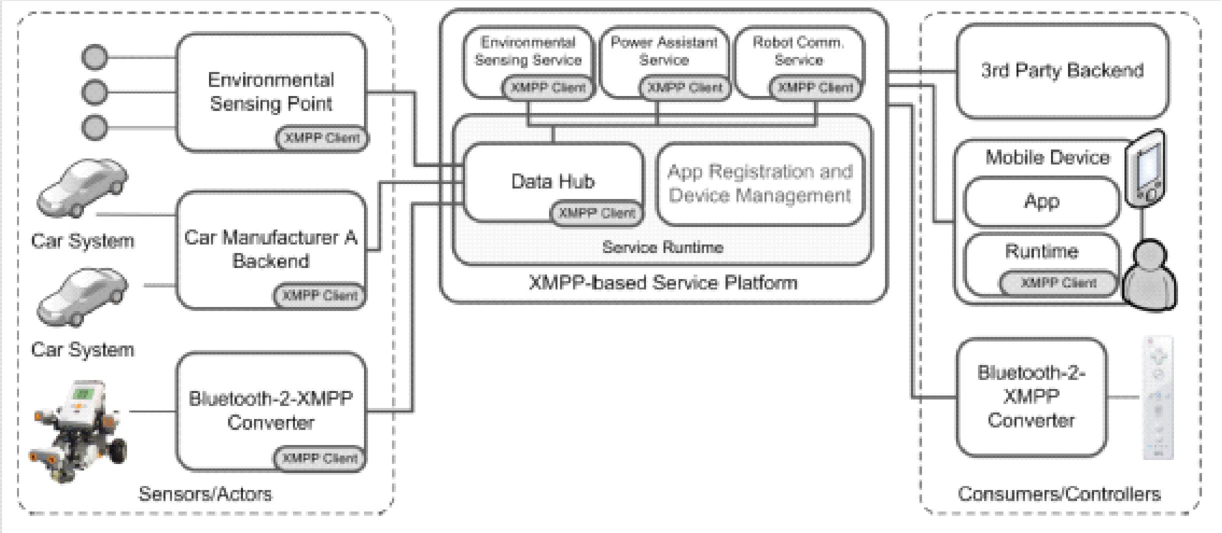

Fig. 2: Framework Architecture [12]

SCondi: A Smart Context Distribution Framework Based on a Messaging Service for the Internet of Things

The work proposed by [9] presents a context distribution framework based on Internet of Things. It provides an effective and reliable mechanism for distributing context information. The mechanism defines the use of security requirements using a context channel which provides an adaptive and reliable abstract communication, disseminating and collecting information from service providers. Furthermore, the context channel filter provides authentication and authorization to achieve security of information.

It uses a messaging service that supports the MQTT protocol (MQ Telemetry Transport) in TCP / IP networks. The structure of Scondi supports anonymous communication between message publishers and subscribers, providing reliable delivery based on MQTT's QoS (Quality of Service) in heterogeneous environments and wireless networks.

SecKit: A Model-based Security Toolkit for the Internet of Things

The work proposed by [10] presents a model based on a set of security tools that are integrated into a management framework for devices in IoT, supporting the specification and evaluation of security policies to allow the protection of user data. This work is applied to a Smart City case study to demonstrate its viability and performance. To allow security requirements, threat scenarios, trusts, and control policies usage are met. The project is based on a security management modeling. Thus, allowing a user with the possibility to design completely a set of custom security and privacy policies. SecKit can be used to specify and enforce privacy policies, data retention, access control, non-repudiation, and trust management. The defined metamodels include data, time, identity, rules, context, structure, behavior, risk, trust and meta rules implemented using the Eclipse Modeling Framework (EMF).

Service-Oriented Security Framework for Remote Medical Services in the Internet of Things Environment

The work proposed by [13] provides a secure oriented services structure for medical environments. The model supports dynamic security features in accordance with telemedicine insurance services. IoT. Security features (confidentiality, integrity, availability, privacy) are covered in the architecture. The work provides confidentiality via authentication of each device accessing a security and encryption channel, and privacy trough a secure transmission and exchange of health information through encryption and hash algorithm. It deals with the availability of information, given that sensitive data is related to the life of a patient.

Analysis and Comparisons

The solution proposed by [10] addresses the issue of trust with a set of associated specifications. It also uses metamodels to address security management issues such as privacy, context information and confidentiality policies. The works [9] [11] [12 [13] deal with authentication to check the users identity accessing the system. Reliability is treated in [9] using MQTT's QoS (Quality of Service) ensures reliable delivery across heterogeneous environments and wireless networks. The use of SSL security protocol / TLS is addressed in [10] with XMPP as the supporting technology. The use of SSL / TLS also ensures integrity, confidentiality, authenticity and non-repudiation, when configured correctly. The work of [13] achieves privacy with specific rules to access data by each user or medical staff. Context information of different types are collected in works [9] [10] using an abstract architecture. Confidentiality is guaranteed in [11] [10] and [13] guarantees authentication and secure transmission through encryption and hash algorithm. Due to the variety of types of devices in IoT such as wireless sensors, smart phones, computers and devices etc, heterogeneity is an important issue to address. The work [9] [11] [12] provide adaptable architectures to satisfy this requirement. Table I shows a comparison of Internet of things security frameworks presented in section 4. This comparison takes into account the use of trust, authentication, reliable mechanisms communication, SSL / TLS, privacy, context aware information collection, confidentiality and adaptation to different devices.

Table I: Security Frameworks for the Internet of Things

	[11]	[12]	[9]	[10]	[13]
Trust	-	-	-	x	-
Authentication	x	x	x	-	x
Reliability	-	-	x	-	-
SSL/TLS	x	-	-	-	-
Privacy	-	-	-	x	x
Context Aware information collection	-	-	x	x	-
Confidentiality	x	-	-	x	x
Adaptation to different devices	x	x	x	-	-

CONCLUSION

In this paper, we have presented some of the main security frameworks for the Internet of Things. These works provide heterogeneous communications environments, security to information integrity through authentication and confidentiality.

A possible extension to the above work is to integrate the best solutions in a single facility. To achieve this goal, it is possible to provide a component that implements the standard SSL technology to provide a secure channel of communication, a context analyzer to set the device status to the environment that is connected, and reliability features, user and devices management.

ACKNOWLEDGMENTS

Financial supports of CAPES and FAPEMA are gratefully acknowledged.

REFERENCES

[1] GARTNER. 2015. Internet of Things definition. Available at: http://www.gartner.com/itglossary/internet-of-things. Accessed on: 20/1/2015.

[2] GENDREAU, A. "Situation Awareness Measurement Enhanced for Efficient Monitoring in the Internet of Things". In Proceedings of the 15th IEEE Region 10 Symposium (TENSYMP), 82-85.

[3] Leeuwen, J. 1990. Handbook of theoretical computer science: algorithms and complexity (Vol. 1). Elsevier.

[4] [4] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. 1996. Handbook of applied cryptography. CRC press.

[5] ROMAN, R. et al.. 2013. On the features and challenges of security and privacy in distributed internet of thing". Computer Networks: The International Journal of Computer and Telecommunications Networking, 57 (July 2013), 2266-2279.

[6] BHATTASALI, T. et al. 2013. Study of Security Issues in Pervasive Environment of Next Generation Internet of Things. In Computer Information Systems and Industrial Management, Springer Lecture Notes in Computer Science, 206-217

[7] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I.S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, P. Doody, 2011. Internet of Things Strategic Research Roadmap, Cluster of European Research Projects on the Internet of Things, CERP-IoT

[8] S. Turner, T. Polk, 2011. Security Challenges For the Internet of Things, in: IAB Interconnecting Smart Objects with the Internet Workshop, Prague, Czech Republic.

[9] PARK, Jongmoon; LEE, Myung-Joon. 2014. SCondi: A Smart Context Distribution Framework Based on a Messaging Service for the Internet of Things. Journal of Applied Mathematics, 1-8, Hindawi Publishing Corporation.

[10] NEISSE, Ricardo et al. 2015, SecKit: A Model-based Security Toolkit for the Internet of Things. Computers & Security, 54 (October 2015), 60-76

[11] CONZON, Davide et al. 2012. The virtus middleware: An xmpp based architecture for secure iot communications. In: Proceedings of the 21th IEEE Conference on Computer Communications and Networks (ICCCN), 1-6.

[12] [BENDEL, Sven et al. 2013. A service infrastructure for the Internet of Things based on XMPP. In: Proceedings of the 2013 IEEE International Pervasive Computing and Communications Workshops (PERCOM Workshops),. IEEE,. p. 385-388

[13] LEE, Jae Dong et al. 2015. Service-Oriented Security Framework for Remote Medical Services in the Internet of Things Environment. Healthcare informatics research, 21 (October 2015), 271-282.

[14] R. Roman, P. Najera, J. Lopez, 2011. Securing the internet of things, IEEE Computer 44 (9) 51–58.

[15] Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady 2004. Security in embedded systems: Design challenges, ACM.Transactions on Embedded Computing Systems (TECS) , Volume 3 (August 2004).

[16] T. C. de França, P. F. Pires, L. Pirmez, F. C. Delicato, and C. Farias. 2014. Web das coisas: Conectando Dispositivos Físicos Ao Mundo Digital, minicourse, Federal University of Rio de Janeiro.

[17] SICARI, S. et al. 2015. Security, Privacy And Trust In Internet Of Things: The road ahead. Computer Networks, 76 (January 2015), 146–164

[18] Spector, A. Z. 1989. Achieving Application Requirements. Distributed Systems, ACM