Context aware security approach for IoT environments

Giovani Ferreira and Caio Silva
Universal Internet of Things (UIoT)
Tecnology Faculty (FT)
University of Braslia (UFSC)
70910-900 Braslia, DF Brazil
giovani.silva@redes.unb.br, caio.silva@redes.unb.br

***Abstract*—adhaskjdhaksjd**

***Index Terms*—security, quality of context, Internet of things**

I. Introduction

Manzoor [1]

II. Related Concepts

A. Smart Objects

Smart Objects are physical/digital autonomous objects augmented with sensing, processing, and network capabilities able to discover new services, new acquaintances, exchange information, connect to external services, exploit other objects capabilities, and collaborate toward a commom goal [2] [3].

(Ideia: O perigo trazido pelos smart objects que comunicam em muitas tecnologias) Smart objects' threats increases as the amount of communication technology it supports.

The threat represented by the Smart Objects increases as the amount of communication technology it supports.

The amount of communication technologies the smart objects support are directly related to the threat they represent.

The amount of communication technologies the Smart Objects have, potentialize the threats they represent.

Smart Objects' threats are potentiated by the amount of their communication technologies.

Smart Objects' threats are potentiated by the amount communication technologies that they support.

Smart object's threats are potentiated by the amount of communication technologies that it supports. A robust device which communicates in several tecnologies have the opportunity to interact with a lot of devices in the IoT network. These interaction and cooperation capabilities results in generation, distribution and manipulation of sensible data, valuable and confidential, which must not be accessible by unauthorized parties. Ensure that access to information and services is granted only to authorized objects is a key part to guarantee a secure system [4].

B. Context

C. Access Control

The term access control is defined in ISO [5] as means to ensure that access to anything that has value to the organization is authorized and restricted based on business and security requirements. Shirey [6] generalizes this definition stating that access control is a protection of system resources against unauthorized access and the use of system resources is regulated according to a security policy. Also, Venter and Ellof [7] completes these definitions stating that access control is a reactive information security technology because it is used to allow or deny access to a system as soon as an access request is made. Whitman [8] says that in general, all access control approaches rely on as the following mechanisms [6] [5]:

1) Identification: Identification is an act or process whereby an unverified entity - called a supplicant - that seeks access to a resource, presents an identifier to a system so that the system can recognize him and distinguish it from other entities, this identifier must be mapped to one and only one entity within the security domain.

2) Authentication: Authentication is the process of validating a supplicants purported identity and a provision of assurance that a claimed characteristic of an entity is correct.

3) Authorization: Authorization is an approval or a process for granting approval to a system entity to access a system resource.

4) Accountability: Accountability, also known as auditability, ensures that all actions - authorized or unauthorized - of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions.

In IoT environments, smart objects interact with each other requesting services. These services provides information that can be sensible and confidential for the environment. Services with those characteristics must have policies to prevent access to data from unauthorized parties.

An IoT access control system must be aware of specific restrictions:

1) Smart objects are pertinent only in the context of the IoT network that they are inserted
2) Smart objects can have limited computing and memory capacity, being unable to process large keys or compute heavy cryptography algorithms in an acceptable time.
3) The data produced in an IoT environment has no owner, only a storage responsible, and can be requested by every smart object in the network.
4) Smart objects can have sleep schedule that does not allow communication during a time period.

Arduino Uno was selected as test platform, it has an ATmega328 microcontroller, an 8-bit processor with a clock speed of 16 MHz, 2 kB of SRAM, and 32 kB of flash memory [9].

They did the tests with 5 different crypto libraries:

1) AvrCryptolib
2) Relic-Toolkit
3) TinyECC
4) Wiselib
5) MatrixSSL

The performance of encryption with private key was faster for smaller key lengths as was expected. However the increase in the execution time was considerable when the key size was 2048 bits [9]:

TABLE I
MY CAPTION

Key Length (bits)	Execution time (ms); Key in SRAM	Execution time (ms); Key in ROM
64	66	70
128	124	459
512	25,089	27,348
1024	199,666	218,367
2048	1,587,559	1,740,267

Yet, with reasonably long key sizes the execution times are in the seconds, dozens of seconds, or even longer. For some applications this is too long. Nevertheless, the authors believe that these algorithms can successfully be employed in small devices for the following reasons:

- With the right selection of algorithms and libraries, the execution times can actually be smaller. Using the Relic-toolkit with the NIST K163 algorithm (roughly equivalent to RSA at 1024 bits) at 0.3 seconds is a good example of this. - As discussed in [wiman], in general the power requirements necessary to send or receive messages are far bigger than those needed to execute cryptographic operations. There is no good reason to choose platforms that do not provide sufficient computing power to run the necessary operations. - Commercial libraries and the use of full potential for various optimizations will provide a better result than what we arrived at in this paper. - Using public key cryptography only at the beginning of a session will reduce the per-packet processing times significantly.

[10]

New paragraph for: Smart objects can or can not have usual identification like MAC address.

D. Information Security Concepts

1) Integrity: Information has integrity when it is whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being stored or transmitted [8].

2) Confidentiality: According to a definition provided by Whitman (2011), the information has confidentiality when it is protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that only those with the rights and privileges to access information are able to do so [8].

For ISO standard (2009), confidentiality is a property that information is not made available or disclosed to unauthorized individuals, entities, or processes [5].

3) Availability: Availability enables authorized users persons or computer systems to access information without interference or obstruction and to receive it in the required for- mat [8].

Property of being accessible and usable upon demand by an authorized entity [5].

The property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them [6].

4) Authenticity: Authenticity of information is the quality or state of being genuine or original, rather

than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred [8].

Property that an entity is what it claims to be [5].

The property of being genuine and able to be verified and be trusted [6].

[11] [12] [13]

Technology	Max Signal Rate	Nominal Range
Wi-Fi	54 Mb/s	100m
Bluetooth	1 Mb/s	10m
ZigBee	250 Kb/s	10 - 100m
UWB	110 Mb/s	10m
WiMax	75 Mb/s	49Km

E. IoT Security

III. Proposal

IV. Experiments and Evaluation

V. Conclusions and Future work

References

[1] A. Manzoor, H. Truong, and S. Dustdar, "Quality aware context information aggregation system for pervasive environments," pp. 266–271, 2009.

[2] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the internet of things," *Internet Computing, IEEE*, vol. 14, no. 1, pp. 44–51, 2010.

[3] L. Atzori, A. Iera, and G. Morabito, "From" smart objects" to" social objects": The next evolutionary step of the internet of things," *Communications Magazine, IEEE*, vol. 52, no. 1, pp. 97–105, 2014.

[4] M. J. Covington, P. Fogla, Z. Zhan, and M. Ahamad, "A context-aware security architecture for emerging applications," in *Computer Security Applications Conference, 2002. Proceedings. 18th Annual*. IEEE, 2002, pp. 249–258.

[5] ISO, "Information technology security techniques information security management systems overview and vocabulary," International Organization for Standardization, Geneva, Switzerland, ISO 27000:2009, 2009.

[6] R. W. Shirey, "Internet security glossary, version 2," 2007.

[7] H. Venter and J. H. Eloff, "A taxonomy for information security technologies," *Computers & Security*, vol. 22, no. 4, pp. 299–307, 2003.

[8] M. Whitman and H. Mattord, *Principles of information security*. Cengage Learning, 2011.

[9] J. Arkko, H.-M. Rissanen, A. Keranen, and M. Sethi, "Practical considerations and implementation experiences in securing smart object networks," 2012.

[10] O. Garcia-Morchon, S. Kumar, R. Struik, S. Keoh, and R. Hummen, "Security considerations in the ip-based internet of things," 2013.

[11] E. Ferro and F. Potorti, "Bluetooth and wi-fi wireless protocols: a survey and a comparison," *Wireless Communications, IEEE*, vol. 12, no. 1, pp. 12–26, 2005.

[12] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi," in *Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE*. IEEE, 2007, pp. 46–51.

[13] S. J. Vaughan-Nichols, "Achieving wireless broadband with wimax," *Computer*, no. 6, pp. 10–13, 2004.