World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

A security view for LIDO

Taoufik Ben Hassine *

National School of Computer Science, Manouba University, 2010 Manouba, Tunisia.

World Journal of Advanced Research and Reviews, 2022, 16(02), 660–664

Publication history: Received on 26 September 2022; revised on 27 October 2022; accepted on 30 October 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.16.2.1129

Abstract

This article deals with cybersecurity and specially IoT security. We add a seven view to the Internet of Things (IoT) universal modelling language called "LIDO". "LIDO" has six (6) different views each represents an aspect of the IoT domain. Security deals with tree aspects: Confidentiality, Integrity, Availability (CIA). This CIA triad model is a safety model that is intended to guide strategies for data security inside the places of a society or corporation. The "OSI" propose a model made of seven security layers that satisfies this CIA triad Model. We present in this article a layered IoT security view based on standards. We have retained this OSI model in seven layers to build the security view. The most delicate layer that we can't control is the "human layer". To address this lack, we propose to set up an ethic which regulates the conscience and the behavior of man. We propose to include this ethic that educators and security specialists will define in the textbooks of generations to come.

Keywords: "LIDO"; Cybersecurity; IoT; Security layered Architecture; Security View

1. Introduction

Day by day security is becoming more and more important in our local and especially global information systems. Systems are becoming data-centric. Among our data there are those which are classified as private and which must be accessed only by some ones. The global situation has made systems, although heterogeneous, interact, cooperate and collaborate. Web services are often the supporting infrastructure for these interactions. C++, C sharp and java as multi-purpose languages for example offer a very powerful instruction set allowing access to local and global systems. C++ is a smart extension of the older, more installed C language. These multi-platform languages allow greater interoperability between different systems by implementing different communication protocols. Although it is desirable that systems cooperate for the good of everyone, the risks of insecurity can multiply and one system can contaminate another.

LIDO the language we propose to design IOT solutions consists of a metamodel and a textual notation. The metamodel is made of platform-independent concepts and metaphors and thus makes it possible to think of both open local systems and global systems welcoming them. These days we can no longer think of a system whether local or global without thinking about the security aspects and more precisely data security. This is all the more urgent as the IOT knows the phenomenon "BIG DATA" while waiting for that of "BIG IDEAS". Therefore, a seventh view, a "Security View", must be added to the six views already offered by LIDO. In this article we propose to develop this view.

* Corresponding author: Taoufik Ben Hassine
National School of Computer Science, Manouba University, 2010 Manouba, Tunisia.

2. “LIDO” a Smart and Clement Modelling Language

2.1. What is "LIDO"?

"LIDO" is a language designed to be used by different people from different backgrounds experiencing different development cultures [7]. These people have chosen to work as a team to solve the development problems of the IOT. Each of them comes with their own skills and their own incapabilities. "LIDO" offers a metamodel that advocates a global horizontal culture framing any other specific vertical culture. This horizontality of "LIDO" allows the mix of developer profiles. This thus allows the constitution of a heterogeneous and integrated team.

2.2. "LIDO" in the development process

"LIDO" is a language that allows the entire development team, including the end users, to discuss and exchange design and implementation ideas about an IoT solution [8]. After multiple brainstorming team sessions and discussions with end users the developers of an IoT solution start from the "LIDO" metamodel called "MODIDO" [6]. Of course, they must have undergone training on the concepts conveyed by the metamodel. They will create a model of their solution by deriving the metamodel to retain the concepts that suit their problem. Their model will thus be made up of instances of these concepts. After having agreed on the model of the solution, the development team moves on to its textual notation which describes by means of a grammar and an editor the elements constituting the hardware and software architecture of the final solution. A technological software tool supporting "LIDO" allows in conclusion to transform the description of the solution in the textual notation into an automatically generated code. This process has been experimented in a smart agriculture application and it gave respectable results.

3. The imperatives the IOT new Security View

3.1. What is "Cybersecurity"?

“To choose a definition is to plead a cause” said The Analytic Philosophe Charles Leslie Stevenson (1908–1979). Cybersecurity is a broadly used term, whose definitions are highly variable, often subjective, and at times, uninformative [1]. Cybersecurity affects all the organizational, structural, infrastructural and human aspects that have a relationship with security. This security concerns humans, their hardware and software equipment connected to the Internet. This security therefore concerns the cybernetic space of man and everything to which he is entitled in an exclusive or shared way. What we are aiming for in this article is IoT cybersecurity.

3.2. What security are we aiming for?

What interests us in this article is the security of IoT data and processes. IoT cybersecurity mainly affects the data and the sensors that capture it and the processes for processing this data and their locations: local or cloud servers. An effective cybersecurity method has numerous layers of defense spread across the networks, computers, programs, or information that one aims to keep non-toxic [2]. The methods used to ensure IoT security must on the one hand be sufficiently flexible and permissive for those we are trying to protect and on the other hand sufficiently and intelligently selective with respect to whom we must protect ourselves. The definitive objective of cybersecurity is to defend the data from actuality stolen or co-operated. To attain this, we aspect at 3 important goals of cybersecurity.

- Defensive the Privacy of Information
- Conserving the Integrity of Information
- Controlling the Obtainability of information only to approved users

These objectives practice the confidentiality, integrity, availability (CIA) triad, the base of entirely safety agendas. This CIA triad model is a safety model that is intended to guide strategies for data security inside the places of a society or corporation [2]

3.2.1. Confidentiality

Confidentiality concerns all data and processes that must be hidden from non-rights holders. For this, we can encrypt them, make the verification of those who are entitled to them more sophisticated. A multi-factor or biometric authentication are even better.

3.2.2. Integrity

Integrity is an important CIA triad model element. Integrity ensures that data is not modified in a corrupt manner. The data must respect its domain values and be consistent with the state of all other related data.

3.2.3. Availability

The availability of data and the continuity of services is an important criterion for the security of a system. websites, for example, must be available to provide web services or to serve HTML web pages. The security of a website or an IoT data server or processing server must prevent and respond to any Denial of Service (DoS) attack.

4. Architectural choices for the IoT Security View

Ransomware, phishing, denial-of-service attacks, credential stuffing — the list of potential cyberattacks just continues to grow. According to a study by the University of Maryland, Internet-connected systems experience an attempted cyberattack every 39 seconds. That's more than 2,200 attacks daily [3].

A common misconception among those outside the cybersecurity sector is that a single technology – a single action or software or strategy – can make an organization "secure" [4]. Indeed, threats of a security nature are innumerable and require multi-disciplinary skills. This is why multi-layered protection is needed to thwart the diversity of attack types that can occur and endanger the cyber IoT system.

4.1. The OSI standard model

The International Standards Organization (ISO) developed the Open Systems Interconnection (OSI) model with its seven layers of cybersecurity as a reference to show the various layers on a network and how everything was interconnected. The OSI model's seven hierarchical layers are the: Human Layer, Perimeter Layer, Network Layer, Endpoint Layer, Application Layer, Data Layer, and Mission Critical Layer. Each layer represents a different stage in network communication, from someone typing on a keyboard to the data your system uses for applications.

The top layer is "The Human Layer". People are, hands down, the weakest link in almost every way possible when it comes to cybersecurity. In fact, according to reports, upwards of **90%** of all security breaches are caused by humans. The best approach to keeping the human layer secure is education and training. Getting an education program set up to train employees on the benefits of good cybersecurity habits regularly can significantly reduce the likelihood of a successful attack [5].

The second layer is Data Security: Data security controls protect the storage and transfer of data. The third layer is Application Security: Applications security controls protect access to an application, an application's access to your mission critical assets, and the internal security of the application. The fourth layer is Endpoint Security: Endpoint security controls protect the connection between devices and the network. The fifth layer is Network Security: Network security controls protect an organization's network and prevent unauthorized access of the network. The sixth layer is Perimeter Security: Perimeter security controls include both the physical and digital security methodologies that protect the business overall.

The Bottom layer is the "Mission Critical Assets" Layer. This is anything your business can't survive without. This layer is for everything vital to your system. Everything that in case of loss or malignant alteration can lead to the death of your system. It's at the bottom of the hierarchy because the whole system rests on it. Keeping track of and monitoring the seven layers of security can be a challenge. Even if you have a dedicated IT team, there are a lot of pieces that need to be watched, and it's easy for something to get missed [5].

4.2. Our priorities for the Security View Model

We opt for standards because they are the result of different experiences based on strategies from different platforms in the security world. Standards and norms often attract different security solution's providers who want a larger local and global market share. The most important reason for our choice of standards is that these standards and norms capitalize on and synthesize word historical security experience and especially allow interoperability, integrability and often portability of solutions. These criteria of integrability and portability lead researchers in security and in other fields to unite and to constitute increasingly large communities in number and capacity of influence for a security salvation benefiting the entire planet.

We insist on the imperative of increasing the capacities of man to assume his role in this security shared by all. Indeed, technicality alone cannot achieve the objectives of sustainable and effective security, even when using the latest technology such as artificial intelligence. Deep learning provided by artificial intelligence can contribute to better experiencing and resolving security. But before learning machine safety, must we first teach it to humans?

Indeed, man must be in control of his cyber security. Security cannot be ensured unless people are aware of what is at stake. To do this, we recommend setting up an ethic that regulates the minds and behavior of people.

5. The LIDO IoT Security View

The LIDO IoT Security View represents the different components of a "Business System" and the different security layers protecting them. The layers are described in the section titled "The ISO Standard Model". These components are:

Users: A user is the end user the Human or the application used by him.

Networks: A network connects all the other components of the system via connectors and ports.

Devices: Devices are sensors, actuators or any other electronic equipment dealing with data capturing from physical objects.

Physical Objects: Physical objects are real word objects or things that are embedded with devices or attached to devices. This allows them to acquire digital skills integrating them into the digital and virtual worlds. For these reasons we also call them augmented objects.

Storage Servers: Storage servers are here to store data on disks and other storage units.

The LIDO IoT Security View illustrated in Figure 1 describes all these components and layers.

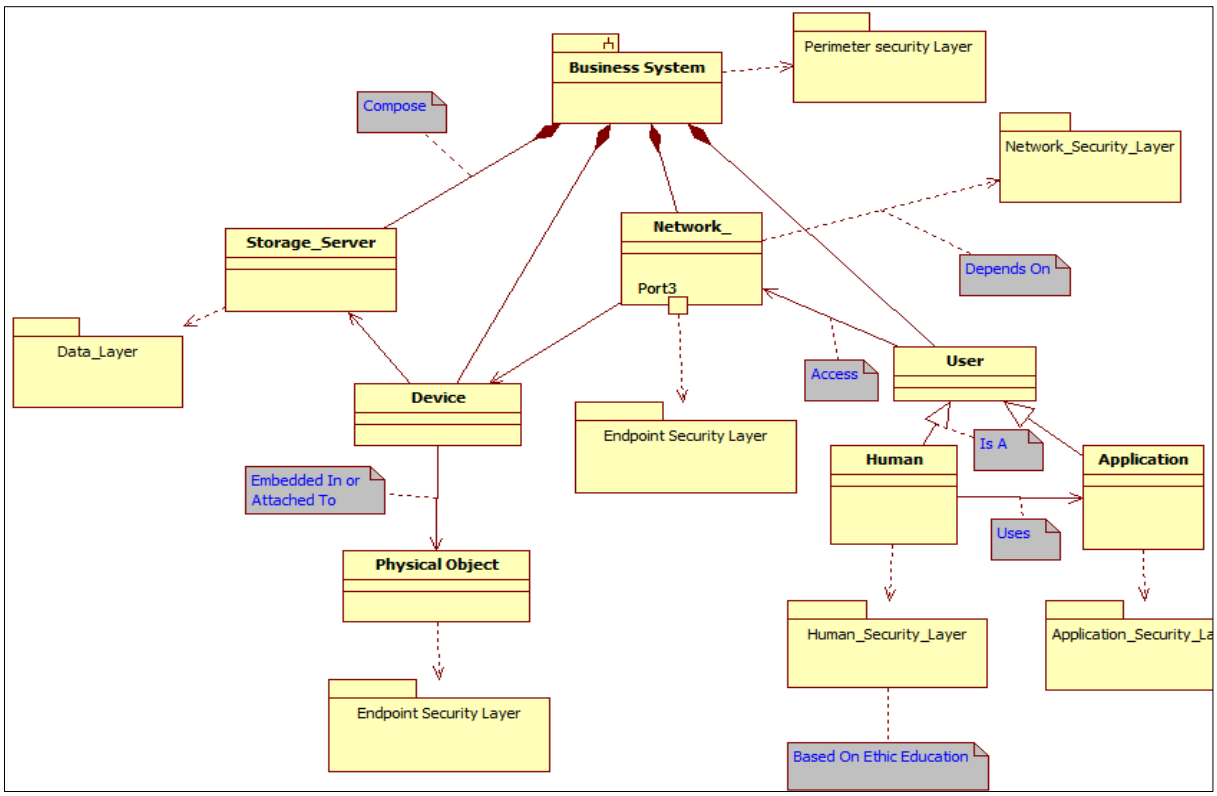

Figure 1 IOT Security View For LIDO

6. Conclusion

We present in this article a layered IoT security view based on standards. We have retained the OSI model in seven layers to build the security view. The most delicate layer that we can't control is the “human layer”. To address this lack, we propose to set up an ethic which regulates the conscience and the behavior of man. In this article, we have tried to imagine what kind of security can we reserve for IoT cyber systems. We have illustrated this in an IoT security view complementary to "LIDO". We have opted for a layered architecture which also respects the standards. The most important layer is the “Human Layer”. This layer must be considered apart from any advanced techniques. Our contribution to this end is to propose to set up an ethic which regulates the conscience and the behavior of man. This is only possible through education and teaching from an early age to be able to live together in a world that is traveling towards digital. Security is the business of all individuals, groups or societies. We win all individuals and societies to work together so that security and especially cybersecurity is guaranteed. This work can be extended and specialized to study physical security as it relates to citizens.

Compliance with ethical standards

Funding

There is no financial interest to report. This submitted work is original and has not have been published elsewhere in any form or language.

References

[1] Diakun-Thibault, Nadia. (2014). Defining Cybersecurity. Technology Innovation Management Review. 2014.

[2] Sheth, Mrs & Bhosale, Sachin & Kurupkar, Mr & Prof, Asst. (2021). Research Paper on Cyber Security. CONTEMPORARY RESEARCH IN INDIA (ISSN 2231-2137): SPECIAL ISSUE : APRIL, 2021.

[3] Jeff Pracht, from “MainStream Technologies” A Layered Security Architecture Offers the Strongest Protection from Cyber Threats, November 30, 2021, https://www.mainstream-tech.com/layered-security-architecture/

[4] Siobhan Climer , Mishaal Khan, from “Mindsight” , What Are The 7 Layers Of Security? A Cybersecurity Report, July 14, 2020, https://gomindsight.com/insights/blog/what-are-the-7-layers-of-security/

[5] ManHattanTechSupport , “The seven layers of IT security” January 21 2021

https://www.manhattantechsupport.com/blog/the-seven-layers-of-it-security/

[6] HASSINE, Taoufik Ben, KHAYATI, Oualid, et GHEZALA, Henda Ben. An IoT domain meta-model and an approach to software development of IoT solutions. In: 2017 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC). IEEE, 2017. p. 32-37. [2]

[7] Taoufik Ben Hassine. A Language & an Approach for the Development of IoT Solutions. American Journal of Electrical and Computer Engineering. Vol. 6, No. 1, 2022, pp. 1-14. doi: 10.11648/j.ajece.20220601.11

[8] Taoufik Ben Hassine “Démarche pour la construction de solutions pour l'internet des objets”, Editions Universitaires Européennes, ISBN : 978-613-8-44249-3