Proposed Model to Implement High-Level Information Security in Internet of Things

Sergio Duque Castilho
School of Electrical and Control Engineering.
Estácio de Sá College, FAESO.
Ourinhos, Brazil.
sergiocastilho@uol.com.br

Eduardo P. Godoy
Bauru School of Engineering.
Sao Paulo State University, UNESP
Bauru, Brazil.
epgodoy@yahoo.com.br

Tayane W. L. Castilho
Bauru School of Engineering.
Sao Paulo State University, UNESP
Bauru, Brazil.

And Fadir Salmen
São Paulo Technology College
Ourinhos, Brazil.

***Abstract*— Internet of Things (IoT) connect different types of devices to control different things or simply read data from then, such as room temperature, location, pressure and others, in a variety of application domains using the World Wide Web. This is a challenge for technology and Information Security (IS). Therefore, this paper surveys advances in IoT-based with an eye towards security, where discusses the technologies used in devices, the risks to which these devices are exposed to stay directly connect to a global network, the TCP/IP Network Layers Model that is used in this connection. The main objective of this paper is to propose an implementation models of security based on ISO 7498-2 for residential and industrial use in IoT. Mitigate risk is a major job for users of this technology because all Internet-connected device runs the risk of having their availability or integrity data transmitted corrupted.**

Keywords—Internet of Things; IoT; Information security; Protocols.

I. INTRODUCTION

The Internet has grown in importance for all users, this growth is due to its evolution, where initially computers were connected, it focused on connecting people in social networks and finally with technological advancement, it came to all things, being the so-called Internet of things (IoT).

IoT is as a global infrastructure to be used for society, enabling advanced services through connectivity [11]. Complete informing as reported by [17], it is a worldwide net with heterogeneous elements (or things) with an address for identification, in function of the volume of connected objects that use the Protocol of Internet Version 6 (Ipv6).

Thus, IoT starts to be constituted not only by equipment with high power of processing as computers, smartphone or laptops but more and more of elements such as sensors of different types and use, actuators that take decisions based on the sensors data, household appliances, and others.

These emergent devices will have each one its individual identification, in other words, its IP address [20].

As well as the Internet of computers and Internet of people, the security remains a challenge, with several incidents been reported daily.

With IoT, considering the increasing number of devices, there is a great probability of increasing the vulnerability and possible problems, assuming that everything connected to the Internet can be hacked sooner or later

So, is it possible to establish a good level of security to exchange and store information in IoT devices?

To solve the problem above, some authors have proposed several hypotheses, some of them implement new layers of security and others some politics of control.

The implementation of all possible, already developed, control security protocols in the different layers of the Internet Reference Model, also known as TCP/IP (Transfer Control Protocol/Internet Protocol) can provide an excellent level of confidentiality and integrity of the information if implemented in a group, not only in one layer.

Therefore, this article proposes a new IoT Security Implementation Model to increase security in data transmitted and makes the devices already installed compatible with this model. Review and discuss the cyber security of the main protocols used in IoT Network Model Layers, understand the principals used technologies and the security in different layers of the TCP/IP already implemented and its relation with the OSI model.

II. LITERATURE REVIEW

Access everything and be able to control your devices at any time from any location was a dream for a few and today is a reality for many with IoT.

The ITU-T [11] presents one of the several definitions of IoT and inform that it will make abundant use of things, and these can be any real device or information from the virtual world, providing the most different types of service for different applications while providing security and privacy. So, the applications include various types of service, such as

978-1-5386-2859-1/17/$31.00 ©2017 IEEE

intelligent transport systems, smart home, health monitoring among others.

Evans [7] informs that in 2003 the world had about 6.3 billion people and the number of connected equipment was less than 0.08 per person;in 2010, this number had increased to 1.84 equipment per person, and after that, in 2020 there will be 6.58 devices per person for a total of 7.6 billion people and 50 billion connected devices. This expansion will happen thanks to IoT.

Before talking about the importance of IoT, it must be necessary to understand the differences between the Internet and World Wide Web (Web). The Internet is the physical part, consisting of switches, routers and other equipment and their primary function is to transport information from one point to another.

The Web is the layer of the application that works on the Internet, it provides an interface that makes the information usable for any users [7].

Internet spread around the world using the wired technology but the need for mobility, accessibility, and facilities to install made users choose wireless technology [14]. Kaur and Monga [14] make a comparison between the two technologies and cites the main used in wireless networks, especially Wi-Fi, a registered trademark of Wi-Fi Alliance, used in Wireless Local Area Networks (WLAN).

A. *IoT proposed layer model*

IoT has a large list of proposed layer models, one of those models was proposed by Atzori et al. [3], composed by layers of Application, Network, and Perception. One more complete model, with five layers, was proposed by Khan et al. [15] their model contains the Perception layer where the physical objects are.

The Network Layer is also called intermediate transmission. The Middleware or Service Management layer that delivers different types of data. The Application Layer provides the user's requested service and finally the Business Layer that will provide graphics or monitor services. These layers can be seen in Table 1.

TABLE I. FIVE LAYER MODEL

Layer Number	***Layers***	***Services***
1	Business Layer	Graphics and Monitoring
2	Application Layer	Provides the requested service
3	Middleware layer	Data delivery
4	Network Layer	Secure transmission
5	Perception Layer	Physical objects, Sensors

The Network Layer transfers information of the devices sensors to the system safely, to be processed by systems in the layer above. On this layer, there are different types of technology used as a Zigbee, WiFi, IEEE 802.11 HA, 6LoWPAN and RFID.

B. *IoT protocols and standards*

The RFID systems are usually in the perception layer, they are simple systems known as Tags(sensors), with low power and processing consumption [12].

The RFID network architecture has base stations and sensors, the latter is responsible for data acquisition by measuring certain parameters, such as ambient temperature and access the Internet via the base station [13].

To address the sensors in a network, one of the ways is to map its address using hash and implemented in the last 64 bits of the IPv6 as described by the authors above. Thus, these devices can be accessed directly on the Internet, through the base station.

Zwave is a proprietary standard communication technology, wireless based on radio frequency (RF)operating at 921.4 MHZ and designed specifically for applications of control and monitoring by reading status in residential and commercial environments. It uses a mesh topology and 231 devices can be connected to each other and operate as a repeater [2].

Zigbee is an open standard technology for Personal Area Network (PAN) based on IEEE802.15.4 with 250 kbps transfer rate. When operating at a frequency of 2.4 GHZ, this technology allows connecting small devices for data collection or control with low power consumption.

The devices can be configured in three network topologies: tree, star or mesh. A ZigBee system consists of several components.

The most basic are the device classified as a Full-Function Device (FFD), or a Reduced Function Device (RFD) [9]. The Zigbee network must include at least one FFD, operating as a network coordinator in the PAN. The FFD can operate in three modes: a Network Coordinator Personal Area (PAN). An RFD is intended for applications that are extremely simple and does not need to send large amounts of data. An FFD can talk to RFDs or FFDs while an RFD can only talk to an FFD [10].

Sakane et al. [13] propose one IEEE 802.15.4 devices address translation method for Ipv6 translation by a Lightweight Directory Access Protocol (LDAP) as proposed, these devices may be identified directly from the Internet.

The newly launched IEEE 802.11 ah is an emerging standard for wireless local area network (WLAN) operating in open sub-bands 1GHz.

Thanks to the favorable propagation characteristics of the low-frequency spectrum, this standard can supply a better transmission distance when in compared with the conventional 802.11 abg operating at 2.4 GHZ or 5 GHZ. It may be used for various purposes including the large network sensor areas (Sun et al. 2013). This standard defined by the Wi-Fi Alliance named Wi-Fi Harlow has different transfer rates and can reach up to 1,000 meters away.

The 6LoWPAN is an adaptation layer to low cost and limited power wireless communication device that can be connected to the IPv6 networks.

These networks include devices that work together connecting the physical real-world environment, for example, wireless sensors, with the virtual world.Thus the devices based on IEEE 802.15.4 can be connected to the Internet without the need for intermediate entities such as gateways or proxies [25].

Essentially 6LoWPAN means IPv6 Over LowPower Wireless Personal Area Networks and consists of an adaptation layer, which allows the IEEE 802.15.4 packets transport data over IPv6 [16].

The 6LoWPAN is completely based on IP protocol, this means that a device can be accessed from anywhere in the world (if properly configured), by a standard computer.

This is a huge advantage, despite its consequences for Information Security(IS) [30].

C. *Information security and protocols*

The different types of devices to be connected to different technologies, as described above, bring the awareness of the cybernetics security.

Experts are generally familiar with the Internet security of computers including mobile devices. Security in IoT will be a great challenge [20], an inquiry say that approximately 17% (seventeen percent) of the specialists inform that it will be a relative disaster on the IS, to approximately 48% (forty-eight percent) said it will have the same Internet security level of the devices and finally 21% that will be a great opportunity to improve the standard of safety throughout the current Internet.

The challenge is great because anything connected to the Internet can be hacked and manufacturers of devices for IoT not set standards or protocols for secure operations [21].

Today the IS in networks of computers are not exactly a disaster but it presents several faults, that if maintained in the control devices they will possibly cause some disaster.

IS according to Vuorinen and Tetri [27] ”aims to protect the relationship between the user’s desire and file”, this security is based on the three pillars: confidentiality, integrity, and availability.

Confidentiality and integrity are based on the idea that only an authorized user must be able to access and edit protected information.

Availability refers to the requirement of accessibility, in other words, the information must be available and modifiable when needed by authorized users.

The risk in IS is the probability of a threat to exploit a vulnerability in a system.

The risk not only exists with the possibility of attackers taking control of IoT devices connected to the network, but also related to the huge quantities of storage and increasing amount of data being generated by these devices, with extensive collection capabilities that are increasingly being introduced in areas generally considered private, even intimate, as organizations, homes, cars, and through technologies used in clothing and ingestible sensor [28].

In the industrial availability is the most important pillar of a system that should prevent any unnecessary delay in production, that results in lost productivity and revenue.

This includes in particular protection against Denial of Service (DoS) attacks in cyberspace against production systems. Another important point is don’t cause injury to the human beings,so the IS integrity of the industry should be maintained

Digital attacks on IoT devices connected to the Internet not only present risks in the digital world but also create physical risks to the owners of the devices, I.e. the risk of injury and even death.

This is best understood when you consider that there will be an estimated 10 million cars self-steerable connected to the Internet running on the road within a few years [28].

Cyber security is routinely cited by policymakers and consistently is at the top of their meeting. Governments around the world have (at least officially), seeking to secure their systems in cyberspace, implementing strategies and creating new laws to guide and regulate its use so as achieving a high-level security, Europe has achieved progress IoT segment and further supported its regulation in various sectors such as energy, vehicles and residential [22].

Depending on your role and specific environment, one of the industrial communications systems must meet a subset of security objectives in terms of the types of attacks described below [6].

- DoS: or denial of service attack which objective is to interrupt the availability. This type of attack can be performed at the physical layer with interference or in transport layer with mass sending packages to the same IP address.
- Eavesdropping: attacks the confidentiality capturing and if possible checking the contents of the packages.
- Man-in-the-middle: attacks the confidentiality placing between the transmitter and receiver, capturing and changing the transmitted content.
- Malicious Software: this type of attack violates the availability, are programs that run intentionally or unintentionally by the user, that lodge, and double seeking information, there is a list of this type of software: viruses, worms, trojans, ransomware, spyware and adware.

These attacks are performed by users with great knowledge of programming and protocols in the system that will be attacked, commonly known as Hackers [24].

The implementation of security in IoT is usually studied in layers, Table 2 lists the layers of the Open Systems Interconnection (OSI), with the Internet layer model and the

most used protocols used [18]. The TCP/IP model predates the OSI model at the date of creation [5].

The ISO 7498-2 standard informs the main points to implement security in the different layers of the TCP/IP model as shown in Table 3. Some layers may not always provide itself security services but can make use of appropriate security services provided by below layers [19].

Thus, security can be established in all the different layers of the TCP/IP model, used in IoT.

Many of these implementations were made in IPv6, this protocol is gradually being deployed around the world, replacing IPv4, both launched by the Internet Engineering Task Force (IETF).

The main difference between the two protocols are two, the first is the amount of available address as the first has 3; $4*10^{38}$, the second contains only $4*10^{9}$ currently fully used. Thus understanding and mitigate security challenges become a necessity for the numbers of devices to be connected.

The second is the ability to automatically configure IP addresses on the new nodes, which reduces the administrative burden of setting them manually.

A set of new protocols, called Neighbor Discovery (ND), this new feature allows automatic configuration for devices with IPv6 implemented, permitting a plug-and-play manner of work. This capability is necessary for future IPv6 applications with a large number and variety of devices [4]. This possibility is used in the IoT 6LoWPAN protocol.

The implementation of security at the network layer can be improved with the IP Security (IPSec), created by the IETF, it is parts of ofIPv6 protocols, defined by a set of RFCs which may optionally be added to IP packets to ensure the confidentiality and integrity of data.

The confidentiality and integrity are achieved by using an Authentication Header (AH) and the encapsulation of the data transmitted Encapsulating Security Payload (ESP) to protect the contents of payload like Fig. 1.

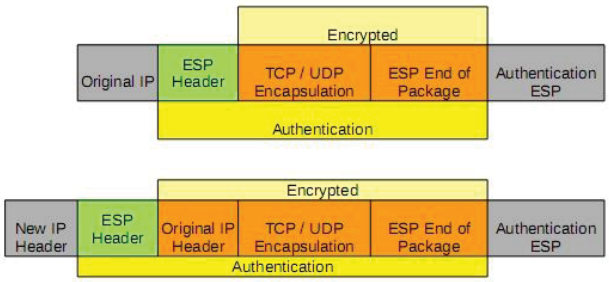

Fig. 1. Encapsulation of the Data Transmitted.

Raza et al. [23] were the first to propose the implementation of the 6LoWPAN-IPsec, an IPsec specification for 6LoWPAN including settings for AH and ESP in the length of headers. It is a safe basic model for end-to-end communication.

UDP is a protocol of the Transport Layer used in packet switching for data transport. It is a very simple protocol and contains only the source port number, destination port number, message size and an optional checksum. The UDP does not have any secure algorithm to the source and destination.

Sitenkov et al. [26] proposed a Datagram Transport Layer Security (DTLS) designed to operate under UDP.

Many Internet applications use UDP as a transport protocol because of the simple use and little overhead to the IP packet. That is the reason why UDP is preferred by IoT.

The Remote Authentication Dial-In User Service(RADIUS) is a centralized service for administration and user authentication that uses the UDP protocol.

Many Internet Service Providers (ISPs) use RADIUS to authenticate thousands, or even millions of users, that are added and deleted continuously throughout the day, and users authentication information constantly changes.

The centralized administration of users in this scenario are an operational requirement, and it is in accordance with Table 3.

TABLE II. PROTOCOLS OF OSI MODEL AND TCP/IP MODEL

OSI Model	Internet	Protocols
Application (Layer 7)	Application	HTTP, HTTPS, RADIUS Server
Presentation (Layer 6)		FTP
Session (Layer 5)		HTTP, HTTPS
Transport (Layer 4)	Transport	TCP, UDP, ICMP, IGMP
Network (Layer 3)	Internet	IP, IPV6, Ipsev, ARP, ICMP, 6LoWPAN (adaptation for IPV6)
Data Link (Layer 2)	Network Interface	Ethenet, Frame Relay, WiFi, L2TP (VPN)

TABLE III. OSI MODEL AND SECURITY ARCHITECTURE (ISO7498-2)

Internet	Protocols	Security
Application	HTTP, HTTPS, RADIUS Server	Access control
	FTP	No Repudiation
	HTTP, HTTPS	Authentication
Transport	TCP, UDP, ICMP, IGMP	Access control, traffic confidentiality
		Authentication of data in origin and destination
Internet	IP, IPV6, Ipsev, ARP, ICMP, 6LoWPAN (adaptation for IPV6)	Traffic and Connection
Network Interface	Ethenet, Frame Relay, WiFi, L2TP (VPN)	
Physical	IEEE 802.15.4 (ZigBee), Wi-Fi HaLow	

HTTPS is a protocol of Application Layer, widely used for secure communication over the network in this layer. When a device sends data to a server, it behaves as a browser to establish an HTTPS connection over the Internet.

Gaurav et al. [8] show the handshaking phase to establish a secure connection in a direct HTTPS communication between a device and the server, this connection can be established even by a single IoT device.

The discussion above makes clear that there are some ways to establish the security of storing or transmitting information when users seek the same information directly on devices or when these devices store their information on servers for future use.

On the other hand, various authors propose new beds to provide security, including Yang, X. et al [29], who presented a security model with three layers to IoT containing the perception layer, network, and application.

The perception layer is the most important layer for architecture, it recognizes devices around and gathers data from the surrounding environment via sensors used. However, the data flow through these wireless sensors makes them vulnerable to attacks, resulting in several security risks in this layer.

Alhamedi et al. [1] propose creating an independent single layer that will suit most security mechanisms required differently from the other layers.

The proposal layer is placed between the physical layer and link, as a filter for sending and receiving data. Furthermore, the proposed layer is designed to be lightweight in order to be used by the resource limited devices.

III. Results And Proposals

The use of IoT devices in the home environment will have a great expansion if it is going be simple to install (plug-andplay), as the connection of mobile devices like a smartphone on the residential environment is.

To become a tendency, Wi-Fi Harlow (802.11 ah) is supposed to be as simple as it is nowadays with Wi-Fi standard (802.11 a, b, g, n) and if possible implemented in the same router.

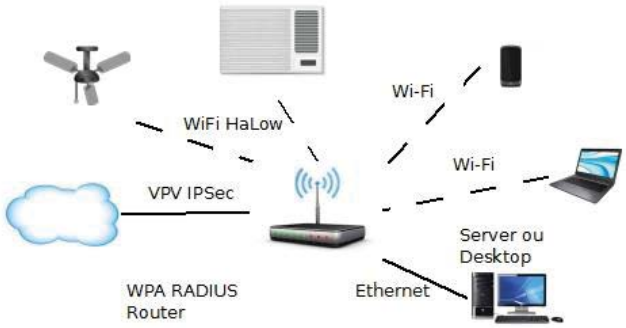

Fig. 2. IoT Model of home users with Wi-Fi and Wi-Fi HaLow on a single route.

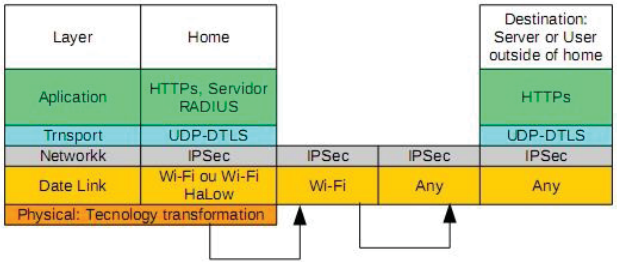

Fig. 3. Security protocols used in end-to-end communication.

The proposed security implementation can be applied in two ways, one for industrial use and one for home use as described below.

To establish a high-level security in the household is necessary to implement the considerations presented in Table 3, as shown in Fig 2, where a single router configured with IPSec and RADIUS for a private messenger, control IoT devices and provides access to fixed and mobile devices, enabling the exchange of information between them.

This configuration without the use of IoT devices is already widely used and can offer a hight level information and home control security.

A protocol layers to establish a communication between any two points on long distance using the model to implement a high level of security can be seen in Fig. 3, the communication in Network layer between these points.

The Physical layers in Fig 3 will be used for the possible transformations of other technologies such as ZigBee or ZWave directly in IPSec, 6LoWPAN-IPSec, Wi-Fi Harlow or Wi-Fi and connect directly to the router in any place.

The destination of the information in Fig 3 can be a cloud storage or the owner of the process accessing your home in long distance, for example, starting from the application layer and reaching the same layer on your local server which will control and store the information of local devices.

Another possibility is direct access to the IoT device via IPSec or 6LoWPAN-IPSec using VPN tunneling, authenticating directly to the configured RADIUS server on the router, in this case, the use of the local server is not necessary.

In the Industrial case the security proposal is similar to residential, but with the obligation of the local server use, preventing direct access from outside users to IoT devices, data will be stored and collected on a server using all the proposed security in different layers.

Mostly Industry will use Physical layers in Fig. 3 to allow the junction of different technologies.

IV. Conclusions

The IoT is one way with no return, multiple devices will be connected to the network in a short period and with a high probability of confidentiality or availability loss, due to a misconfiguration in your security.

The proposed implementation of a security sequence based on existing protocols and technologies on the ISO 7498-2 model allows a significant improvement in security, making highly secure residential or industrial environment.

The Physical layers in the proposed model will serve for the adjustment of different technologies already implemented, making them directly accessible on the Internet or allowing data to be stored directly on the site server.

Many proposals were made, but the concern for security has not been considered.

This work begins with a security model to an implementation model, making it a safe environment for home and industrial user with little knowledge in Information Security.

Equipment with low power battery that only send information, like tags for commercial use don't need security, in this case the IS can be implemented in the receiver.

Many proposes have already been implemented in parts, for future works recommend all implementation using Wi-Fi Harlow with 6LoWPAN-IPSec in low power equipment for security test.

ACKNOWLEDGMENT

Thanks to the help and support of São Paulo Technology College; Estácio de Sá College computer labs (Ourinhos, Brasil) and all the people who contributed in some way to the work.

REFERENCES

[1] Adel H. Alhamedi, Vaclav Snasel, Hamoud M. Aldosari, and Ajith Abraham. Internet of Things Communication Reference Model Adel. In International Conference on Computational Aspects of Social Networks (CASoN), pages 61–66, 2014.

[2] Z-Wave Alliance. Z-Wave. 2015. [online ¡http://z-wavealliance.org//¿ accessed 10. April 2015].

[3] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The Internet of Things: A Survey. Comput. Netw., 54(15):2787–2805, 2010.

[4] Ferdous A Barbhuiya, Santosh Biswas, and Sukumar Nandi. Detection of neighbor solicitation and advertisement spoofing in IPv6 neighbor discovery protocol. Proceedings of the 4th international conference on Security of information and networks - SIN '11, page 111, 2011.

[5] J D Day and H Zimmermann. The OSI reference model. Proceedings of the IEEE, 71(12):1334–1340, 1983.

[6] EC-Council. Ethical Hacking & Countermeasures. Booklet, pages 1–19, 2012.

[7] Dave Evans. The Internet of Things - How the Next Evolution of the Internet is Changing Everything. CISCO white paper, (April):1–11, 2011.

[8] Kumar Gaurav, Pravin Goyal, Vartika Agrawal, and Shwetha Lakshman Rao. IoT Transaction Security. 2015.

[9] Jose A Gutierrez, Edgar H Callaway, and Raymond L Barrett. Low-rate wireless personal area networks: enabling wireless sensors with IEEE 802.15. 4. IEEE Standards Association, 2004.

[10] Dae-Man Han and Jae-Hyun Lim. Smart home energy management system using IEEE 802.15. 4 and zigbee. IEEE Transactions on Consumer Electronics, 56(3):1403–1410, 2010.

[11] ITU-T. Overview of the Internet of Things. Recommendation Y2060, International Telecommunication Union, Geneva, 2012.

[12] Rune Hylsberg Jacobsen, Qi Zhang, and Thomas Skjdeberg Toftegaard. Internetworking Objects with RFID. In Cristina Turcu, editor, Deploying RFID - Challenges, Solutions, and Open Issues, pages 319–334. InTech, 2011.

[13] Steffen Elmstrøm Holst Jensen and Rune Hylsberg Jacobsen. Integrating RFID with IP Host Identities. Book Radio Frequency Identification from System to Applications, InTech, 2013.

[14] Navpreet Kaur and Sangeeta Monga. Comparsions of Wired and Wireless Networks: A Review. International Journal of Advanced Engineering Technology, V(II):34–35, 2014.

[15] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. Future internet: The internet of things architecture, possible applications and key challenges. In Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012, pages 257–260, 2012.

[16] Nandakishore Kushalnagar, Gabriel Montenegro, and Christian Schumacher. IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals. Technical report, 2007.

[17] H Ma, L Liu, A Zhou, and D Zhao. On Networking of Internet of Things: Explorations and Challenges. IEEE Internet of Things Journal, 3(4):441–452, 2016.

[18] Christoph Meinel and Harald Sack. The Foundation of the Internet: TCP/IP Reference Model. In Internetworking, pages 29–61. Springer, 2013.

[19] D I N Norm. ISO 7498: Information Processing Systems Open Systems Interconnection Basic Reference Modell, 1983.

[20] John Pescatore and Gal Shpantzer. Securing the Internet of Things Survey. SANS Institute InfoSec Reading Room, pages pp. 1–22, 2014.

[21] Antigone Peyton. The Connected State of Things: A Lawyer's Survival Guide in an Internet of Things World. Catholic University Journal of Law and Technology, 24(2):5, 2016.

[22] Tim Polk and Sean Turner. Security challenges for the internet of things. In Workshop on Interconnecting Smart Objects with the Internet, Prague, 2011.

[23] Shahid Raza, Simon Duquennoy, Tony Chung, Dogan Yazar, Thiemo Voigt, and Utz Roedig. Securing communication in 6LoWPAN with compressed IPsec. In 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), pages 1–8. IEEE, 2011.

[24] REGNER SABILLON, JEIMY CANO, VICTOR CAVALLER, and JORDI SERRA. Cybercrime and Cybercriminals: A Comprehensive Study.

[25] S Sakane, Y Ishii, K Toba, K Kamada, and N Okabe. A translation method between 802.15.4 nodes and IPv6 nodes. In International Symposium on Applications and the Internet Workshops (SAINTW'06), pages 4 pp.–37, jan 2006.

[26] Denis Sitenkov, Supervisors-Ludwig Seitz, Shahid Raza, and G¨oran Selander. Access Control in the Internet of Things. Master's thesis, 2014.

[27] J Vuorinen and P Tetri. Paradoxes in Information Security. IEEE Potentials, 35(5):36–39, 2016.

[28] Rolf H Weber and Evelyne Studer. Cybersecurity in the Internet of Things: Legal aspects. Computer Law & Security Review, 2016.

[29] Yang X., Li Z., Geng Z., and Zhang H. A multi-layer security model for internet of things, 2012.

[30] A Yushev, A Sikora, and E J Sebastian. Open source 6Lo protocol stack for wireless embedded systems. In 2016 Wireless Telecommunications Symposium (WTS), pages 1–7, 2016.