IoT Information Security Evaluation for Developers and Users

Lohana Santos Medeiros, Fábio Zuvanov, Flávio Luis de Mello, Edilberto Strauss

***Abstract*— The accelerated growth of Internet of Things (IoT) exposes many unsecured issues related to design and usage of devices leading to a new technological security paradigm. This paper presents an evaluation method and corrective actions to be carried out in order to make the usage of IoT devices safer. This method combines both the developer's perspective and user's perspective, thus differing from current guides. The proposed evaluation method is divided by categories, each one composed of security control clauses and their corresponding action recommendation. The user perspective of such evaluation method was applied into a service company, and the developer perspective into an IoT device manufacturer. These experiments produced useful perceptions on such view points. The evaluation provided an opportunity to enhance manufacturer security awareness and improve user experience with IoT devices.**

***Index Terms*— Internet of Things, Information Security, Good Practices, Evaluation**

I. Introduction

THE strict definition of IoT (Internet of Things) is not a consensus, but the term is usually described as a collaborative ecosystem of context-aware, intelligent and automated device connected to network for specific purpose. Over the years, the accelerated growth of such connected

devices produced a large amount of data. Besides, it can be observed that the main target of IoT industry is the creation of smart environments, self-conscious and autonomous devices.

This increasing number of devices creates new opportunities of business and processes, but it is a challenge to infrastructure capacity, and mainly, to security.

The IoT ecosystem is an environment subjected to different security risks: malicious manipulation of the information flow of network connected devices; usage of tampering devices for acquiring sensitive data; loss of consumer privacy; slowdown of Internet functionality through large-scale distributed denial of service attacks; and potential disruptions to critical infrastructure. It is expected that in 2020 there will be 50 billion of connected devices [1], and since 2008 there has been more of such devices than human beings. This must be perceived with severe concern since commonly used IoT devices contain serious security vulnerabilities. It is important to understand IoT devices security risk because of what such equipments have access to. However, there are many basic security controls which, once put in place, can raise the security posture of a device. There are several vulnerabilities considered trivial and also relatively easy to remediate without affecting the user's experience.

This paper proposes information security evaluation for developers, manufacturers and users of IoT devices. It aims to present not only the main features one must be aware of, but also what must be done. The proposed method evaluates devices in order to identify faults and mitigate risks that this kind of technology brings to the life of people and companies, improving the confidence level, privacy and sustainable growth.

II. Related Work

MANY researches have been carried out on IoT security issues. Riahi et al. [2] explain that IoT calls for a new paradigm of security, which will have to consider the security problem from a holistic perspective, including new actors and their interactions, and thus propose a systemic approach tosecurity. Roman et al. [3] also call attention to the convenience and economy provided by IoT devices, and that this scenario will require novel approaches to ensure its safe and ethical use. Abomhara and Køien [4] discuss the existing security threats, and open challenges in the domain of IoT. Wenjun et al. [10] and Kim [11] studied honeynet management tools. Alagheband and Aref [12] analyzed key management models for heterogeneous networks. Bera et al. [13] presented an integrated security framework. Chamberlain et al. [5] evaluate the need for balancing security, reasonable installation and maintenance efforts. The authors explain that security is a crucial issue, but if the security infrastructure is not relatively easy to use, it will ultimately be compromised by users who are insufficiently motivated to deal with the complexity of ensuring security. Oh and Kim [6] state that current IoT security requirements are insufficient.

Submitted for review on November 21th, 2017. This work was supported in part by Machine Intelligence and Computer Models Laboratory of Federal University of Rio de Janeiro (IM^{2}C/Poli/UFRJ) under grant Poli 19.257 of Coppetec.

Lohana Santos Medeiros is system auditator at SulAmérica insurance company, Brazil (email: lohanamedeiros@gmail.com).

Fabio Zuvanov (M.Sc.) is Business Developer Director focused on Digital Transformation projects, leading Artificial Intelligence and Internet of things (IoT) initiatives for Intel' Energy Industry customers in Brazil (email: fabio.zuvanov@intel.com).

Flávio Luis de Mello (D.Sc.) is associate professor at the Electronics and Computer Department from Polytechnic School at Federal University of Rio de Janeiro, Brazil (email: fmello@poli.ufrj.br).

Edilberto Strauss (Ph.D.) is associate professor at the Electronics and Computer Department from Polytechnic School at Federal University of Rio de Janeiro, Brazil (email: strauss@poli.ufrj.br).

Theypropose security requirements of IoT by analyzing heterogeneity, resource constraint, dynamic environment, and suggest IoT network, cloud, user, attacker, service and platform as key elements for device security.

Attacks and vulnerabilities are widely studied. Nawir et al. [7] report the eventual attacks to IoT devices during safety-critical operations causing them to be in the shutdown mode. They created a taxonomy of security attacks within IoT networks to assist IoT developers for better awareness of the risk of security flaws, so that new protections shall be incorporated. Wurm et al. [8] identify backdoors and analyze security of hardware, software, and networks from commercial/industrial IoT devices. They provide experimental proof that security vulnerabilities are a common problem for most devices, and indicate solutions to help IoT manufacturers secure their products. Abomhara and Køien [9] not only classify threat types, but also analyze and characterize intruders and attacks to IoT devices and services. Sonar and Upadhyay [14] discuss different Distributed Denial of Service attack and its effect on IoT. Pan et al. [15] identify andclassify possible cyberphysical attacks and connect such attacks with variations in manufacturing processes and quality inspection measures. Their taxonomies also provide a scheme for linking emerging IoT-based manufacturing system vulnerabilities to possible attacks and quality inspectionmeasures.

Consequently, there are many frameworks and methodologies concerning IoT security. Koivu et al. [16] analyze different security solutions for IoT devices and propose techniques for further analysis. Their study provides guidance on implementing security solutions for both existing and coming IoT devices, by providing analysis and defining the Complexity of Implementation score for each solution. Pérez et al. [17] present a research project in which is defined a methodology to experiment, validate and certify different technological solutions in large-scale conditions. The Online Trust Alliance [18] produced the IoT Trust Framework, serving as a product development and risk assessment guide for developers, purchasers and retailers of IoT devices. It includes forty principles, segmented into four key categories.

This framework includes instructions on how to approach design and implementation choices that produce quality, secure, and affordable products. NIST [19] published a standard report that contains an IoT Security Guidance designed to help preventing exploitation of vulnerabilities and facilitating the creation of a disciplined, structured systems security engineering activities. DHS [20] explains these risks concerning IoT and provides a set of non-binding principles. It suggests good practices to raise security levels of IoT devices and systems. OWASP [21] also published an IoT Security Guidance that focus on IoT manufacturers, developers and consumers and categorizes the IoT security in ten principles.

III. IoT Security Evaluation

THERE are two main agents that contribute to IOT security: (1) device manufacturers and developers; (2) device users. The former are pressured by the time to market, producing fast implementation that bypasses basic security principles. The latter are usually unaware of security issues, and sometimes are even negligent about such issues. For this reason, it is important to encourage the use of security knowledge to make smarter decisions and perform tasks in new situations. Good practices provide instructions that have shown to work well, succeeding in achieving objectives, and that are replicable. In this section, IoT security evaluation is described in order to supply a recommendation security model.

The proposed evaluation helps manufacturers and developers to design their devices according to security and privacy good practices, and also proposes safer usage of such devices. The scheme is based on several frameworks [18, 19, 21] but it offers a different approach. It provides a model evaluation for both users and manufacturers/developers. Moreover, it also provides recommendations to improve the information security ecosystem, according to the results obtained from the evaluation model.

Thus, this evaluation is divided into two perspectives: manufacturer/developer and user. Each perspective is composed of four categories containing good practices items, which aim to estimate compliance. These estimations result into a criticality evaluation. This is illustrated at Figure 1.

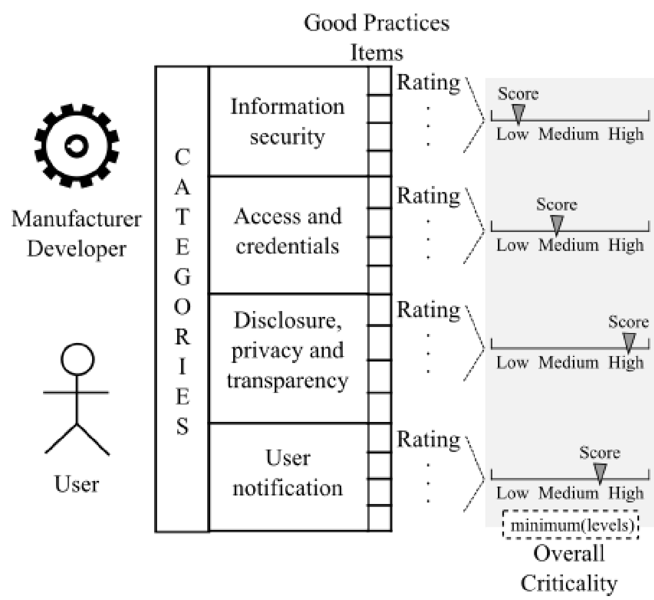

Fig. 1. IoT Security Evaluationscheme.

The good practices items are mapped over categories such as: Information security; Access and credentials; Disclosure, privacy and transparency; User notification. These categories are analyzed in separate because each one of them evaluates the criticality under different visions. The overall criticality for the whole perspective is given by the higher category criticality.

Moreover, the criticality level for each category is classified as low, medium and high. This level is associated with a score value obtained by the sum of the good practices items ratings. This scaling method is based on Likert Scaling [Carifio07], that is, it reproduces a level of agreement or disagreement on a symmetric agree-disagree scale for a series of statements.

Therefore, good practice items compliances are rated according to the following:

- Total Compliance: one point to the item when the practice is completely adherent to the feature being rated;
- Partial Compliance: two points if the featured being rated is not completely fulfilled;
- No Compliance: three points when practice has no conformity to the rating feature.

A. Manufacturer/developer perspective

This perspective helps the manufacturer/developer to produce more secure IoT devices. Each good practice is associated with actions that must be triggered so that a better compliance is obtained.The criticality level is obtained according to the compliance with such practices. Tables I to IV present the set of good practices and actions for each category under manufacturer/developer perspective.

TABLE I
INFORMATION SECURITY GUIDANCE FOR MANUFACTURER/DEVELOPER PERSPECTIVE

Category: Information Security		
Good Practice	Action	
IS1: Devices and applications have security protocols and updated cryptography.	If there is a web interface, then enable HTTPS protocol to protect data transfer The software applications must use encrypted communication between devices Stored data must be encrypted Use certified cryptography and avoid proprietary encryption Applications must have a default encryption method	
IS2: Devices, applications and servers arechecked against vulnerabilities impact.	Web interface implementation must be tested against XSS, SQLinjection and CSRF vulnerabilities. Firewalls must be enabled to protect all interfaces. Improve application response against attacks such as buffer overloading, fuzzing and denial of service.	
IS3: There are robust mechanisms for distributing updates and vulnerabilities corrections	Updates must not change user configurations (security and privacy) User must be able to authorize and reject updates All applications must be able to be remotely updated All applications must be able to be remotely patched whenever vulnerabilities are identified Updates and installations must be fully verified signed	
IS4: There is an evaluation of security risks and compliance of service and cloud providers	All outsourcing service must be tested against XSS, SQLinjection and CSRF vulnerabilities All outsourcing service must provide encrypted data transfer All mobile applications used by IoT devices must implement encrypted data transfer	
IS5: Applications prerequisites demand a minimum usage of physical inputs and outputs hardware interfaces	Applications must be development to demand a minimum amount of external interfaces (eg.: USB and slot cards)	
Criticality Level		
Low [5,7]	Medium [8,12]	High [13,15]

TABLE II
ACCESS AND CREDENTIALS GUIDANCE FOR MANUFACTURER/DEVELOPER PERSPECTIVE

Category: Access and Credentials		
Good Practice	Action	
AC1: Strong authentication is used by default	Applications must reject weak passwords Use multi-factor authentication Implement mechanisms such as blocking account and password expiration New user login and password must be provided at the first usage of IoT device	
AC2: Administrative passwords are not used for other purposes than administrative tasks	Developed applications must limit administrative resources to a local interface with a single passwords Developed applications must implement multi user usage with segregate functionalities	
AC3: Password recover mechanisms must be implemented using manufacturer support or multi-factor authentication	Mechanisms for password recover must be secure and supported by IoT manufacturer	
AC4: There are countermeasures to be triggered against brute for attacks and abusive logins attempts	Implement user account blocking or deactivation after a certain number of invalid logins Accept only strong passwords using uppercase, lowercase, numbers and special characters	
AC5: Users are notified of passwords redefinitions and outliers login attempts in the device	Web interfaces and mobile applications must be developed so that password changes and non-standard access are informed to users All applications must perform a log of security events	
AC6: Authentication credentials are stored encrypted	Passwords stored on device and at the cloud must be encrypted using salt and hash methods	
Criticality Level		
Low [6,9]	Medium [10,14]	High [15,18]

TABLE III
DISCLOSURE, PRIVACY AND TRANSPARENCY GUIDANCE FOR MANUFACTURER/DEVELOPER PERSPECTIVE

Category: Disclosure, Privacy and Transparency		
Good Practice	Action	
DPT1: Data collection is limited to what is necessary to device operation	Evaluate what are the necessary data for device well functioning Make sure that just low sensible data are collected	
DPT2: Data retention policy and stored personal information lifetime are public available	Guarantee that privacy policy and data retention are implemented, updated and deployed for all personnel	
DPT3: User can reject imposed manufacturer policy at anytime	The consequence of rejecting security policies must be clearly reported to user, and also the impacts on product resources and functionalities Users must be able to decide what data will be collected and the reasons for demanding such data	
DPT4: Applications collect just anonymized information for storing at servers	Personal data must be protected using cryptography when stored and transmitted Consumer collected data must be anonymized Just authorized personnel can access personal data	
Criticality Level		
Low [4,6]	Medium [7,9]	High [10,12]

TABLE IV
USER NOTIFICATION GUIDANCE FOR MANUFACTURER/DEVELOPER PERSPECTIVE

Category: User Notification		
Good Practice	Action	
UN1: There is a communication process to inform the users about security problems, privacy issues, product termination and device discontinuity	Applications must be developed so that alerts and notifications are generated whenever a security event occurs Security issues must be notified at product official website, through email, SMS or any other user communication channel	
UN2: There is a communication process to inform users about security events and operational faults	Create mechanisms to allow users choosing the notifications about security events and operational faults that he desires to receive Notifications must be implemented over several communication channels such as email, SMS or any other user communication channel	
Criticality Level		
Low [2]	Medium [3,5]	High [6]

B. *User perspective*

This perspective aims to make users aware of IoT technology and to show them the main issues they must be concerned about. The user must be well informed about security issues and risks he is exposed to, so that this user consumes the technology consciously and reduce side effects. Tables V to VIII present the set of good practices evaluators and actions for each category under user's perspective.

TABLE V
INFORMATION SECURITY GUIDANCE FOR USER PERSPECTIVE

Category: Information Security		
Good Practice	Action	
IS1: Device webpage secure protocol is enabled	The device system must be enabled for HTTPS, or HSTS (Strict Transport Security), or AOSSL (Always On SSL)	
IS2: IoT device has its firmware and software always updated	Keep activated the checking for updates option Check if updates are being periodically applied	
IS3: Regular analysis of notifications and messages are made	Enable any functionality concerning the log of events related to security issues Make periodic analysis of unidentified events	
IS4: External input/output port are disabled when not in use	At the web administration interface deactivate any physical ports that are not being used	
IS5: IoT device is not connected to the same network of critical services	Use network segmentation technologies such as firewalls in order to separate IoT devices from critical operations If there is a firewall available in IoT device, enable it	
Criticality Level		
Low [5,7]	Medium [8,12]	High [13,15]

TABLE VI
ACCESS AND CREDENTIALS GUIDANCE FOR USER PERSPECTIVE

Category: Access and Credentials	
Good Practice	Action
AC1: Unique and strong passwords are used, specially for IoT administrative access	Change standard login and password for strong keys If available, enable the periodic password modification requirement
AC2: Multi-factor authentication are used to access devices	Enable the authentication option for using multi-factor authentication
AC3: Just the amount of user accounts necessary to use IoT are registered	IoT accounts must provide access to functionalities compatible with user profile Whenever a new user account is created, functionalities segregation must be observed If system provides privilege definition for users, consider the minimum user privileges for accomplishing user tasks Restrict the administrative resources of IoT system
AC4: System	Block or disable guest accounts

authentication is protected against brute force attacks	Block or disable the device after a certain number of consecutive unsuccessful logins	
Criticality Level		
Low [4,6]	Medium [7,9]	High [10,12]

TABLE VII
DISCLOSURE, PRIVACY AND TRANSPARENCY GUIDANCE FOR USER PERSPECTIVE

Category: Disclosure, Privacy and Transparency		
Good Practice	Action	
DPT1: The data used by IoT device are not sensible	Do not insert sensible information into the system that are not necessary Revise the data used by devices such as user identification and personal data Enable cryptography using robust methods When sensible data are necessary, understand the risks about its usage	
Criticality Level		
Low [1]	Medium [2]	High [3]

TABLE VIII
USER NOTIFICATION GUIDANCE FOR USER PERSPECTIVE

Category: User Notification		
Good Practice	Action	
UN1: Messages and notifications reporting issues on security, privacy, product life cycle are checked and analyzed	Enable the mechanisms of alerts and notifications related to security issues Follow instruction from manufacturer about security issues and product life cycle termination	
Criticality Level		
Low [1]	Medium [2]	High [3]

IV. EVALUATION TEST

THISsection illustrates how the design concept of IoT security evaluation is feasible. Note that, along this article, the term good practice was used instead of best practice. As observed by Bardach [23], the work necessary to guarantee a practice to be the best is rarely possible and hardly ever done. Most of the time, such practices may be called good or smart practices, offering insights into solutions that may work for most situations. Therefore, this paper presents evidences that the good practices evaluation proposed here produces reasonable results. In order to support its viability, the IoT security evaluation test was applied to an IoT device manufacturer and to a service company. Before assigning such test, both companies were interviewed about their auto-evaluation on IoT devices security.

The manufacturer/developer perspective was tested into a 12 years' experience IoT developing company, which defines itself as being concerned about security and privacy. It says that several efforts have been implemented to improve security and privacy in its products, but there were still some course of actions to be performed, such as data encryption. Table IX abridge the conformity evaluation.

TABLE IX
DEVELOPING COMPANY IOT SECURITY EVALUATION

Rating	Score	TroubleSpot
IS1 = 2	10 Medium	Stored data are not encrypted
IS2 = 3		There is no policy against attacks to the device
IS3 = 2		Software updates are automatic and signed, but firmware update is not
IS4 = 2		Server is not tested against cross-side scripting
IS5 = 1		Default policy demands a minimum usage of external ports
AC1 = 3	10 Medium	Strong authentication is not required
AC2 = 1		Administrative and ordinary views have no functionalities in common
AC3 = 1		Password recover implements a double check test
AC4 = 2		Blocking and deactivation are implemented but strong passwords are not required
AC5 = 1		All identified non-standard access are reported and security logs are made
AC6 = 2		Standard AES encryption is used, with symmetric key
DPT1 = 1	6 Low	No sensible data are collected
DPT2 = 1		Policy is public available, but is not certain that all users really understand it
DPT3 =2		User reject of manufacturer policy implies device limited functioning
DPT4 = 2		All data are anonymous, but stored and transmitted data are not encrypted
UN1 = 1	3 Medium	Security, privacy and termination issues are communicated at website and customers mailing list
UN2 = 2		Users can configure events notification, but logs must be analyzed
Overall Criticality		Medium

Most categories evaluated were classified with medium criticality, and the majority of trouble spots are not hard to solve. Moreover, simple actions such as strong password requirement, salt and hash encryption, and an active notification system would improve categories conformity value, as well as reduce the overall criticality. This diagnose is compatible with a company described as concerned with IoT security.

Furthermore, the user perspective was tested into a service company which has IoT devices such as smart TVs, IP security cameras, smartphones and IP phones. The company is not worried about IoT security and does not have any policy concerning such devices. In fact, the low interest on such subject forced a scope reduction of this analysis, restricting it to IP security cameras. Table X resumes the conformity evaluation that was performed.

TABLE X
USER COMPANY IOT SECURITY EVALUATION

Rating	Score	Trouble Spot
IS1 = 3	13 High	Device does not support secure protocols
IS2 = 3		Firmware is not updated and there is no software update
IS3 = 2		Events logging is enabled but there is no evidence that such log were ever analyzed
IS4 = 2		External ports cannot be disabled, but there are no overplus ports
IS5 = 3		Device is connected to the same network of servers and employees computers
AC1 = 3	10 High	There is a weak password composed of five numbers
AC2 = 3		There is no multi-factor access control
AC3 = 1		There are an administrator account and users accounts
AC4 = 3		Device firmware ignores brute force attacks
DPT1 = 1	1 Low	No personal or corporative data are required
UN1 = 2	2 Medium	Manufacture provides notification reports but there is no evidence that such information were ever analyzed
Overall Criticality		High

Good practices IS1, AC2, AC4 indicate features that cannot be improved, since cameras do not support such characteristics. This is a consequence of a bad decision made by the time devices were purchased, and the only mitigation available is substitution. Besides, devices may comply with other good practices if their corresponding mitigation actions are taken. Concerning DPT1, devices are in accordance with the good practice, but, it is important to understand that the access to internal company images, or even images of its day by day operation are sensible too. Solving the compliance issues from all other categories will mitigate this problem with peculiar sensible data. The high criticality obtained is compatible with a company that is not concerned with IoT security.

Both tests resulted into criticalities that are well-suited to companies' profile. They provide evidence that the IoT security evaluation was adequately assembled and implemented. The actions triggered helpful and contextualized recommendations, thus supporting process redesign. These allow the identification of improvements to be made in order to get a better information security ecosystem.

V. CONCLUSION

ITis important that the process of developing IoT device be secure in order to supply confidence to users who adopt it. On the other hand, users are usually considered the weakest link in the information security chain since they lack knowledge on technology, and sometimes do not know risks concerning such technology. However, by taking into account the IOT security evaluation, these risks can be mitigated.

This work described an information security IoT test for both manufacturers/developers and users. The proposed evaluation allows analyzing the compliance with each good practice, which triggers actions to mitigate problems. Therefore, the evaluation makes advises to prioritize the actions that are necessary to be implemented and configured. Moreover, the IoT security evaluation also enables a risk analysis of IoT device and makes explicit the eventual absence of important features.

As future works, it is suggested an increment on the number of validation tests to guarantee statistical results. It is also interesting to evolve the evaluation to a framework, and therefore, it is necessary to follow up the triggered action taken by companies, and then, analyze the enhancement of categories criticality.

REFERENCES

[1] Tully, Jim. “Analysts to Explore the Value and Impact of IoT on Business”, In: Gartner Symposium/Itxpo, November 10, 2015.

[2] Riahi, A.; Challal, Y.; Natalizio, E.; Chtourou, Z. Chtourou; Bouabdallah, A. "A Systemic Approach for IoT Security," 2013 IEEE International Conference on Distributed Computing in Sensor Systems, Cambridge, MA, pp. 351-355, 2013. doi: 10.1109/DCOSS.2013.78

[3] Roman, R.; Najara, P.; Lopez, J. "Securing the Internet of Things," In Computer, v. 44, n. 9, pp. 51-58, Sept. 2011. doi: 10.1109/MC.2011.291

[4] Abomhara, M.; Køien, G. M. "Security and privacy in the Internet of Things: Current status and open issues", 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, pp. 1-8, 2014. doi: 10.1109/PRISMS.2014.6970594

[5] Chamberlain, Roger D.; Chambers, Mike; Greenwalt, Darren; Steinbrueck, Brett; Steinbrueck, Todd. "Devices Can Be Secure and Easy to Install on the Internet of Things", In: Integration, Interconnection, and Interoperability of IoT Systems, Ed. Gravina, Raffaele; Palau, Carlos E.; Manso, Marco; Liotta, Antonio; Fortino, Giancarlo. Springer International Publishing, pp.59-76, 2017. doi: 10.1007/978-3-319-61300-0_4

[6] Oh, S. R.; Kim, Y. G. "Security Requirements Analysis for the IoT," 2017 International Conference on Platform Technology and Service (PlatCon), Busan, pp. 1-6, 2017. doi: 10.1109/PlatCon.2017.7883727

[7] Nawir, M.; Amir, A.; Yaakob, N.; Lynn, O. B. "Internet of Things (IoT): Taxonomy of security attacks," 2016 3rd International Conference on Electronic Design (ICED), Phuket, pp. 321-326, 2016. doi: 10.1109/ICED.2016.7804660

[8] Wurm, J.; Hoang, K.; Aria, O.; Sadeghi, A. R.; Jin, Y. "Security analysis on consumer and industrial IoT devices," 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macau, pp. 519-524, 2016. doi: 10.1109/ASPDAC.2016.7428064

[9] Abomhara, M.; Køien, G. M. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks", Journal of Cyber Security and Mobility, v.4, n.1, pp. 65-88, 2015. doi: 10.13052/jcsm2245-1439.414

[10] Fan, Wenjun; Fernández, David; Du, Zhihui. "Versatile virtual honeynet management framework", IET Information Security, v.11, n.1 , pp.38-45, 2017. doi: 10.1049/iet-ifs.2015.0256

[11] Kim, I. S.; Kim, M. H. "Agent-based honeynet framework for protecting servers in campus networks", IET Information Security, v.6, n.3, pp.202-211, 2012. doi: 10.1049/iet-ifs.2011.0154

[12] Alagheband, M. R.; Aref, M. R. "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," IET Information Security, v.6, n.4, pp.271-280, 2012. doi: 10.1049/iet-ifs.2012.0144

[13] Bera, P., Ghosh, S. K.; Dasgupta, P. "Integrated security analysis framework for an enterprise network - a formal approach," IET Information Security, v.4, n.4, pp.283-300, 2010. doi: 10.1049/iet-ifs.2009.0174

[14] Sonar, Krushang; Upadhyay, Hardik. "A Survey: DDOS Attack on Internet of Things", International Journal of Engineering Research and Development, v. 10, n. 11, pp.58-63, November 2014.

[15] Pan, Yao; White, Jules; Schmidt, Douglas C.; Elhabashy, Ahmad; Sturm, Logan; Camelio, Jaime; Williams, Christopher. "Taxonomies for

Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems", International Journal of Interactive Multimedia & Artificial Intelligence, v.4, n.3, pp.45-54, 2017.

[16] Koivu, A. et al., "Software Security Considerations for IoT," 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, pp. 392-397, 2016. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.93

[17] Pérez, S.; Martínez, J. A.; Skameta, A. F.; Mateus, M.; Almeida, B.; Maló, P. "ARMOUR: Large-scale experiments for IoT security & trust," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, pp. 553-558, 2016. doi: 10.1109/WF-IoT.2016.7845504

[18] OTA. "IoT Trust Framework v2.5", Online Trust Alliance / Internet Society, 2017.

[19] Ross, Ron; McEvilley, Michael; Oren, Carrier. “Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems”, NIST Special Publication 800-160, National Institute of Standards and Technology, November, 2016. doi: 10.6028/NIST.SP.800-160

[20] DHS. “Strategic Principles for Securing the Internet of Things”, U.S. Department of Homeland Security, version 1.0, November 2016.

[21] OWASP. “Manufacturer IoT Security Guidance”, Open web application security project, 2016.

[22] Carifio, Perla. "Ten Common Misunderstandings, Misconceptions, Persistent Myths and Urban Legends about Likert Scales and Likert Response Formats and their Antidotes", Journal of Social Sciences, v.3, n.3, pp.106–116, 2007. doi:10.3844/jssp.2007.106.116.

[23] Bardach, Eugene. "A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving", Thousand Oaks, CA: Sage, 2011.

Lohana Santos Medeiros received her MBA in Governance, Projects and Information Technology Services from the Federal University of Rio de Janeiro - UFRJ (2017), certified in information security foundation based on ISO IEC 27002 (2015) and Bachelor's degree in information systems from the University Castelo Branco (2015).

She currently works with systems auditors at SulAmérica, a large company in the insurance industry, having participated in works in cloud computing (Google Apps for Business), business continuity plan, disaster recovery plan, security in bring your own device, and personally identifiable information.

Fábio Zuvanov received his MSc. in Business Management from the Brazilian Institute of Capital Markets - IBMEC (2004), Undergraduate degree in Systems Engineering from the State University of Rio de Janeiro- UERJ (1998).

He currently works as Business Developer Director focused on Digital Transformation projects, leading Artificial Intelligence and Internet of things (IoT) initiatives for Intel’ Energy Industry customers in Brazil, an American multinational corporation and technology company headquartered in Santa Clara, California, in the Silicon Valley. It is the world's second largest and second highest valued semiconductor chip makers based on revenue

Flávio Luis de Mello received his DSc. in Theory of Computation and Image Processing from the Federal University of Rio de Janeiro - UFRJ (2006), MSc. in Computer Graphics from the Federal University of Rio de Janeiro - UFRJ (2003), Undergraduate degree in Systems Engineering from the Military Institute of Engineering - IME (1998).

He developed command and control systems and implemented military messages interchange applications during twelve years as a Brazilian Army officer. He was responsible for developing software applications based on machine learning and knowledge reasoning from Mentor Group.

Dr Mello currently is Associate Professor at the Electronic and Computer Engineering Department (DEL) of Polytechnic School (Poli) at the Federal University of Rio de Janeiro (UFRJ). He is head of the Machine Intelligence andComputing Models Laboratory (IM^{2}C).

Edilberto Strauss received his PhD. in Computer Science from the Imperial College of Science Technology and Medicine of London (1996), MSc. in Computer Graphics from the Pontifical Catholic University of Rio de Janeiro – PUC-Rio (1992), Undergraduate degree in mechanic engineering from the Federal Center of Technological Education Celso Suckow da Fonseca (1986).

He was the Coordinator of the Computation and Information Engineering under graduation of Federal University of Rio de Janeiro (UFRJ) and was responsible for the course foundation. He was substitute teacher at Imperial College and Fluminense Federal University.

Dr Strauss currently is Associate Professor at the Electronic and Computer Engineering Department (DEL) of Polytechnic School (Poli) at the Federal University of Rio de Janeiro (UFRJ) since 2000. He is the head of Information Technology Master Business Administration courses called Executive Information Technology, Computation and System Engineering, and Governance Projects and Services.