# A Fuzzy Model for Knowledge Base IoT Information Security Evaluation

Flávio Luis de Mello

***Abstract*—Internet of Things (IoT) accelerating growth exposes many unsecured issues related to the design and the usage of network integrated devices. This paper presents a fuzzy evaluation method, based on both IOT hardware/software developers' and users' knowledge, creating an novel model to aid correctness actions over security procedures, in order to increase the IOT safeness usage. This method combines both the developer's and user's perspectives, creating an integrated adaptive evaluation attached to the Information Technology security standards and best practices guidelines. 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 was defined by an IoT device manufacturer. The obtained results have shown that the evaluation method enhances both the manufacturer security awareness and the IOT users experience in the improvement of security IoT issues.**

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

## I. Introduction

THE IoT (Internet of Things) strict definition 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, leading the creation of smart environments, self-conscious and autonomous devices. Such characteristic creates new opportunities of business and processes, but also it deals with both infrastructure challenges capacity and the security issues.

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 the usage of Internet connected devices leads security vulnerabilities.

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 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 a fuzzy approach to information security evaluation for developers, manufacturers and users of IoT devices based on Medeiros et al. [2] estimation method. 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.

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.

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).

## II. Related Work

MANY researches have highlighted some important issues concerning this work. Riahi et al. [3] explain that IoT calls for a new paradigm of security, while Roman et al. [4] 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 [5] discuss the existing security threats, and open challenges in the domain of IoT. Bera et al. [11] presented an integrated security framework, and Chamberlain et al. [6] evaluate the need for balancing security, reasonable installation and maintenance efforts. Oh and Kim [7] state that current IoT security requirements are insufficient and propose 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. [8] report the eventual attacks to IoT devices during safety-critical operations causing them to be in the shutdown mode. Wurm et al. [9] identify backdoors and analyze security of hardware, software, and networks from commercial/industrial IoT devices. Abomhara and Køien [10] not only classify threat types, but also analyze and characterize intruders and attacks to IoT devices and services. Sonar and Upadhyay [12] discuss different Distributed Deny of Service attack and its effect on IoT. Pan et al. [13] identify and classify possible cyberphysical attacks and connect such attacks with variations in manufacturing processes and quality inspection measures.

Moreover, there are many frameworks and methodologies concerning IoT security. Koivu et al. [14] analyze different security solutions for IoT devices and propose techniques for further analysis. Pérez et al. [15] 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 [16] produced the IoT Trust Framework, serving as a product development and risk assessment guide for developers, purchasers and retailers of IoT devices, including forty principles, segmented into four key categories.

This framework is a continuing research from Medeiros et al. [2] and on some regulatory agencies NIST [17] 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 of systems security engineering activities. DHS [18] explains these risks concerning IoT and provides a set of non-binding principles. OWASP [19] 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 [16,17, 19] 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 (linguistic variables) containing good practices items, which aim to estimate compliance. These estimations result into a fuzzy criticality evaluation. This is illustrated at Figure 1.

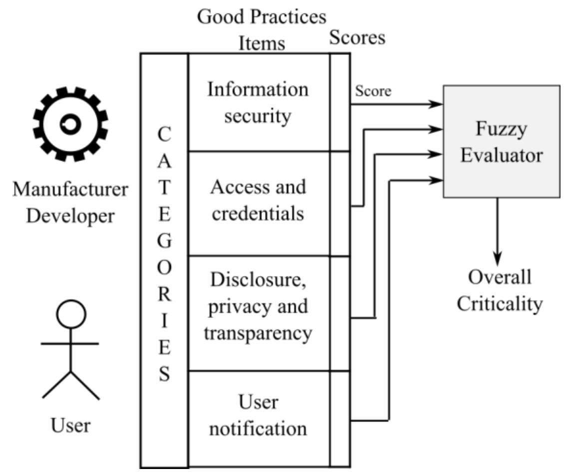



Fig. 1. IoT Security Evaluation scheme.

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 fuzzy value obtained by the fuzzy evaluator.

Moreover, the security level for each category are fuzzy value called Secure and Insecure obtained through a membership function that maps the score of the items compliance. The score is computed by the sum of points given to a good practice, and such 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.

Let the linguistic variables Information Security, Access and Credentials; Disclosure, Privacy and Transparency; User Notification be abbreviated by IS, AC, DPT and UN, respectively. The membership functions for those four linguistic variables are given at the next subsections. Moreover, let the domain of the output variable, criticality, be composed by the following terms: negligent, fragile, manageable, desirable. The proposed evaluation described in this paper used Zadeh operators for constructing the fuzzy rules. Thus, such rules are defined as:

If IS(insecure) and AC(insecure) and DPT(insecure) and UN(insecure) Then Criticality(negligent)

If IS(secure) and AC(insecure) and DPT(insecure) and UN(insecure) Then Criticality(fragile)

If IS(insecure) and AC(secure) and DPT(insecure) and UN(insecure) Then Criticality(fragile)

If IS(secure) and AC(insecure) and DPT(insecure) and UN(secure) Then Criticality(manageable)

If IS(secure) and AC(secure) and DPT(insecure) and UN(insecure) Then Criticality(manageable)

If IS(secure) and AC(insecure) and DPT(secure) and UN(insecure) Then Criticality(manageable)

If IS(secure) and AC(secure) and DPT(secure) and UN(secure) Then Criticality(desirable)

There are several traditional methods to perform defuzzyfication, but the one used in this work is quite simple. The overall criticality is given by the term with the highest value. The tie-breaking criterion is to choose the lower precedence term from this list order: Negligent < Fragile < Manageable < Desirable.

### *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. The membership function is also described.

TABLE I. INFORMATION SECURITY GUIDANCE FOR MANUFACTURES/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<br>The software applications must use encrypted communication between devices<br>Stored data must be encrypted<br>Use certified cryptography and avoid proprietary encryption<br>Applications must have a default encryption method |
| IS2: Devices, applications and servers are checked against vulnerabilities impact. | Web interface implementation must be tested against XSS, SQL injection and CSRF vulnerabilities.<br>Firewalls must be enabled to protect all interfaces.<br>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)<br>User must be able to authorize and reject updates<br>All applications must be able to be remotely updated<br>All applications must be able to be remotely patched whenever vulnerabilities are identified<br>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, SQL injection and CSRF vulnerabilities<br>All outsourcing service must provide encrypted data transfer<br>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) |
| ***Membership Function*** | |

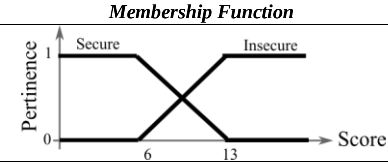



TABLE II. ACCESS AND CREDENTIALS GUIDANCE FOR MANUFACTURES/DEVELOPER PERSPECTIVE

| **Category: Access and Credentials** | |
|---|---|
| ***Good Practice*** | ***Action*** |
| AC1: Strong authentication is used by default | Applications must reject weak passwords<br>Use multi-factor authentication<br>Implement mechanisms such as blocking account and password expiration<br>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<br>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<br>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<br>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 |
| ***Membership Function*** | |

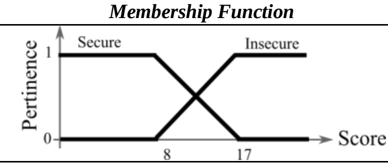



TABLE III. DISCLOSURE, PRIVACY AND TRANSPARENCY GUIDANCE FOR MANUFACTURES/DEVELOPER PERSPECTIVE

| **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<br>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 |

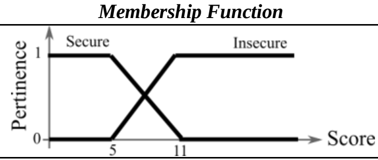
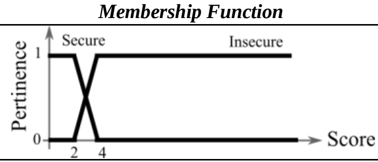
| | |
|---|---|
| DPT3: User can reject imposed manufacturer policy at anytime | The consequence of rejecting security policies must be clearly reported to user, and also the impacts on product resources and functionalities<br>Users must be able to decide what data will be collected and the reasons for demanding such data |
| DPT4: Applications collect just anonymized information for storing at servers | Personal data must be protected using cryptography when stored and transmitted<br>Consumer collected data must be anonymized<br>Just authorized personnel can access personal data |
| ***Membership Function*** | |
|  | |



TABLE IV. USER NOTIFICATION GUIDANCE FOR MANUFACTURES/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<br>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<br>Notifications must be implemented over several communication channels such as email, SMS or any other user communication channel |
| ***Membership Function*** | |
|  | |



## 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. The membership function is also described.

TABLE V. INFORMATION SECURITY GUIDANCE FOR USER PERSPECTIVE

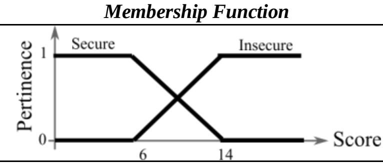
| **Category: Information Security** | |
|---|---|
| ***Good Practice*** | ***Action*** |
| IS1: Device webpage secure protocol is enabled | The device system must be enabled for HTTPS, or HSTS (Strict Transport Security), or AOSSL (Always On SSL) |
| IS2: IoT device has its firmware and software always updated | Keep activated the checking for updates option<br>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<br>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<br>If there is a firewall available in IoT device, enable it |
| ***Membership Function*** | |
|  | |



TABLE VI. ACCESS AND CREDENTIALS GUIDANCE FOR USER PERSPECTIVE

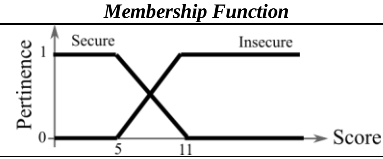
| **Category: Access and Credentials** | |
|---|---|
| ***Good Practice*** | ***Action*** |
| AC1: Unique and strong passwords are used, specially for IoT administrative access | Change standard login and password for strong keys<br>If available, enable the periodic password modification requirement |
| 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<br>Whenever a new user account is created, functionalities segregation must be observed<br>If system provides privilege definition for users, consider the minimum user privileges for accomplishing user tasks<br>Restrict the administrative resources of IoT system |
| AC4: System authentication is protected against brute force attacks | Block or disable guest accounts<br>Block or disable the device after a certain number of consecutive unsuccessful logins |
| ***Membership Function*** | |
|  | |



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<br>Revise the data used by devices such as user identification and personal data<br>Enable cryptography using robust methods<br>When sensible data are necessary, understand the risks about its usage |
| ***Membership Function*** | |

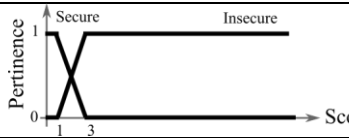
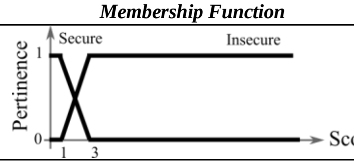



TABLE VIII. USER NOTIFICATION GUIDANCE FOR USER PERSPECTIVE

| **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<br>Follow instruction from manufacturer about security issues and product life cycle termination |
| ***Membership Function*** | |




## IV. EVALUATION TEST

THIS section illustrates the usage of IoT security evaluation with fuzzy logic. Note that, along this article, the term good practice was used instead of best practice. The work necessary to guarantee a practice to be the best is rarely possible and hardly ever done [20]. 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 such thesis, 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 for each category, based on secure (S) and insecure (I) terms.

TABLE IX. DEVELOPING COMPANY IOT SECURITY EVALUATION

| **Rating** | **Pertinence** | **Trouble Spot** |
|---|---|---|
| IS1 = 2 | 0.4286 (S) | Stored data are not encrypted |
| IS2 = 3 | 0.5714 (I) | 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 | 0.7778 (S) | Strong authentication is not required |
| AC2 = 1 | 0.2222 (I) | 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 | 0,8333 (S) | No sensible data are collected |
| DPT2 = 1 | 0.1667 (I) | 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 | 0.5000 (S) | Security, privacy and termination issues are communicated at website and customers mailing list |
| UN2 = 2 | 0.5000 (I) | Users can configure events notification, but logs must be analyzed |
| Negligent = 0,1667<br>Fragile = 0,1667<br>Manageable = 0,2222<br>Desirable = 0,4286 | | ***Overall Criticality*:**<br>Desirable |

The categories Access and Credentials (AC) and Disclosure, Privacy and Transparency (DPT) presents a high pertinence with the secure (S) concept. The Information Security category presents a small tendency to be insecure (I) and User Notification (UN) indicates no inclination toward secure or insecure characteristics. It seems that 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. The overall criticality is Desirable.

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 for each category, also based on secure (S) and insecure (I) terms.

TABLE X. USER COMPANY IOT SECURITY EVALUATION

| **Rating** | **Pertinence** | **Trouble Spot** |
|---|---|---|
| IS1 = 3 | 0.1250 (S) | Device does not support secure protocols |
| IS2 = 3 | 0..8750 (I) | 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 | 0.1667 (S) | There is a weak password composed of five numbers |
| AC2 = 3 | 0.8333 (I) | 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 = 2 | 0.5000 (S)<br>0.5000 (I) | No personal or corporative data are required, but there are indoor images processed by the device |
| UN1 = 2 | 0.5000 (S)<br>0.5000 (I) | Manufacture provides notification reports but there is no evidence that such information were ever analyzed |
| Negligent = 0,5000<br>Fragile = 0,1667<br>Manageable = 0,1250<br>Desirable = 0,1250 | | ***Overall Criticality*:**<br>Negligent |

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. Both categories Information Security (IS) and Access and Credentials (AC) present a bias to be considered insecure (I). The other two categories are neutral for secure (S) and insecure (I) linguistic terms. The criticality obtained is compatible with a company that is not concerned with IoT security, and thus, the overall criticality is Negligent.

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

THE process of developing an IoT solution must 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 to follow up the triggered action taken by companies, and then, analyze the enhancement of categories criticality. With the evolution of technology in mobile devices, there is a model of work increasingly used in organizations, BYOD (Bring Your Own Device), which allows the user to use their own mobile device at work. It seems that the experience obtained with the construction of this IoT security evaluation can be used to propose a BYOD security framework.

## References

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

[2] Medeiros, Lohana Santos ; Zuvanov, Fabio; Mello, Flávio Luis de; Strauss, Edilberto . IoT Information Security Evaluation for Developers and Users. Journal of Information Security and Cryptography (Enigma), v. 4, p. 16-22, 2018. doi: 10.17648/enigma.v4i1.63

[3] 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

[4] Roman, R.; Najara, P.; Lopez, J. "Securing the Internet of Things," In Computer, vol. 44, no. 9, pp. 51-58, Sept. 2011. doi: 10.1109/MC.2011.291

[5] 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

[6] 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

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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.

[13] 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.

[14] 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

[15] 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

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

[17] 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

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

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

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

**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 and Computing Models Laboratory (IM$^2$C).