WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

IOT Security Standards and Indicators Analysis

Ahmed Mohamed Maher[1], S.Suganya[2]

[1]Mcs computer sciences Rathinavel Subramaniam college of arts and science, Coimbatore, India

[2]Mca, Ph.D, Asst. Prof Department of computer sciences Rathinavel Subramaniam college of arts and science, India

A B S T R A C T

That's where technical standards come in. Standardizing products allows devices to work together, making the products easier to use and more appealing to end users. It also creates competition among manufacturers, which reduces prices and gives consumers a choice. But what's in it for the manufacturer?
Often, companies want to lock you into their products so that you solely use their brand. But most companies don't make every type of product. Door lock companies don't usually make dishwashers. Automotive product companies don't usually make medical devices. So, allowing devices to work together actually expands the market for the manufacturer without having to develop products outside of their specialization. It also allows for smaller niche products to work with more widespread ones. Beyond that, making devices more versatile and easier to use makes these devices more appealing in general so that all manufacturers sell more products. As for the price, the best way for companies to keep prices up is to produce newer, better and more innovative products, which benefits the consumer as well.

Keywords:IoT; Standards; indicators; cryptography; security framework.

1. Introduction

Imagine a world in which you can tell your phone you're leaving work, and your washing machine automatically starts the laundry at home so that it's ready for the dryer when you arrive. Or your oven begins preheating so that you can pop a pizza in when you get home. Or, on cold days, your car automatically starting and warming up for your drive home. Imagine coming home from the grocery store, and your hands are full. No worries! The camera above your door has recognized you, and your door has unlocked and is already swinging open for your convenience.
Actually, you don't have to imagine these scenarios anymore; they're happening now. It is estimated there will be 30 billion IoT connected devices by 2020 and 75 billion devices by 2025. But with all these devices from dozens of manufacturers exploding onto the scene, how will they all work together? Today, many of them don't—but it's essential that they do.

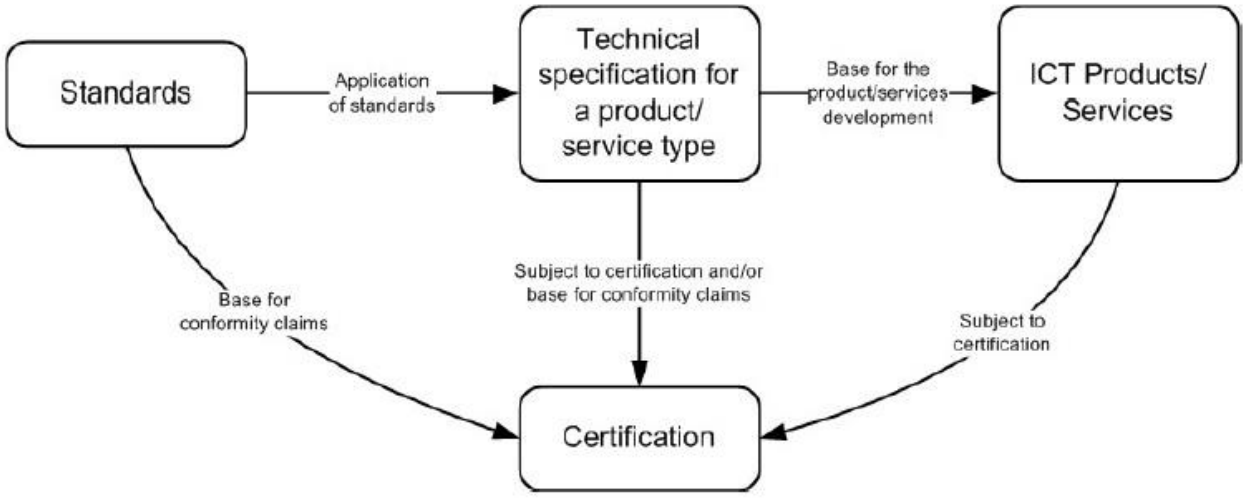
Spearheading IoT Standards for Interoperability and Security

Where do standards come from? For standards related to IoT, an organization has been created called the Open Connectivity Foundation (OCF). OCF is committed to consumers, businesses and industries to deliver a standard communication platform to ensure interoperability and security for IoT devices. These standards will span multiple industries, including smart homes, automotive, industrial, scientific and medical, to name a few.
OCF's goal is for devices from various manufacturers to operate together seamlessly and securely. Currently, OCF's membership includes roughly 400 member organizations, including major software companies, service providers and silicon chip manufacturers. OCF has developed specifications and is using an open-source platform called IoTivity (hosted by the Linux Foundation) that can be embedded in IoT devices. IoTivity is used to create middleware that will allow various clients and servers to communicate with one another. The communications occur in software, so the physical connections (e.g., Wi-Fi, Bluetooth, Zigbee, Z-wave, ethernet) aren't an issue.
But OCF isn't just about interoperability. The latest release of the OCF platform incorporates PKI security. At a time when security is often taken for granted or is an afterthought for new technologies, OCF is committed to the highest level of security possible for such low-power limited processing devices. Why is this important? We may not think that hacking a lightbulb is a big deal, but the weakest link in a network is often the biggest target for hackers. Once they're in, they can cause irreparable damage. Therefore, every device on the network needs to be secured. Not to mention the fact that you probably don't want someone else to be able to unlock your doors, turn off your security devices or control your medical device or vehicle without your knowledge or consent!

Furthering IoT Standards Development with CableLabs and Kyrio

So where do CableLabs and Kyrio fit in? CableLabs has been in the business of developing standards and certifying products for the cable industry for the past 30 years. Kyrio, as a subsidiary of CableLabs, is reaching out to other industries to help develop new technologies. The combination of experience in standards development, as well as certification testing, makes CableLabs and Kyrio a natural fit with the OCF.

For the past few years, CableLabs and Kyrio have been heavily involved with OCF. Our involvement ranges from acting as a standing member of the board, to chairing the security working group, to participating in various working groups such as certification and interoperability testing. Kyrio is also one of seven authorized test labs (ATLs) in the world and have performed certification testing for several of the first devices to be certified. In addition to OCF certification testing, we also offer development support to manufacturers that need to get their implementations ready for certification.



2. Analysis of standards and indicators

The requirements listed in the ENISA report "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures" have been mapped to an existing identifiable standard that if followed would allow the requirement to be satisfied. The detailed, requirement by requirement, mapping is given in Annex A. The simplified analysis yields that there is no significant standards gap - every requirement can be met by an existing standard. The problem is that this is neither the correct nor the expected answer. Standards exist for many different elements of making a device or service secure. However, when referring to IoT, one refers to an ecosystem of not only devices and services. Moreover, the context of use of IoT, its high scalability and other particularities further complicate the field and require more generic and flexible approaches. Therefore, for example the gap in IoT device standards for security is that the standards are not treated holistically so it is possible to deliver a device to the market that can authenticate its user, that can encrypt data it transmits, that can decrypt data it receives, that can deliver or verify the proof of integrity, but which will still be insecure. Similarly, the organisation developing the IoT product or service may have the development processes defined in management guidelines such as those of ISO-27000 but still delivers an insecure product. The challenge for regulators and suppliers alike is to bring only secure IoT devices to the market and this requires a different approach, which will have to be flexible enough to accommodate for the nature of the dynamic IoT ecosystem. Accepting that it is often speculation, there is a necessary challenge to imagine how society will be in a few years from now and to consider the threats to society at that time. In order to frame this, the broad assumption is that ICT will reach further into society with more connectivity, further augmentation of everyday life through ICT, and this will demand an ICT and cybersecurity response. The concerns of the next few years however stretch far beyond the remit of only security technology and many of the recommendations in the present document extend to gaining better understanding of the societal understanding of how ICT, and in particular, ICT incorporating cybersecurity impacts daily life. Whereas this checklist of security requirements for IoT security and its mapping to specific standards can serve as a springboard towards holistic and effective IoT security, it should be noted that the intricacies of the IoT ecosystem call for more flexible approaches. Not only are the underlying technological challenges calling for adaptive, context- and risk-based solutions, but also the IoT market constraints have to be taken into account, so as not to hamper competitiveness and innovation.

3. The certification opportunity

The overall purpose of standards from the perspective of the market is twofold in defining what a standard is intended to achieve: (1) interoperability, and (2) confidence. The conventional role of standards in achieving interoperability is discussed in some length in Annex A and is not repeated here. The role of standards in the domain of trust is less well defined and in a security context is difficult to state in simple terms. When referring to the IoT, one should not only consider individual devices. The inherent connectivity and interdependencies of devices, services, people, process and data call for holistic approaches. Accordingly(3), this implies a much more holistic view of the role of the device as opposed to a relatively closed view of what standard does

it comply to for say encryption. Standards can be used for developing technical specifications in a specific context of a product type, and provide a framework for security evaluation of products. Such general concept is presented in figure 1 below.

15408 Evaluation criteria for IT security, widely recognized as 'Common Criteria' (CC)2. CC consists of 3 parts including:

- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components

Based on the security model discussed in part 1 one can develop technical specifications, called – in CC

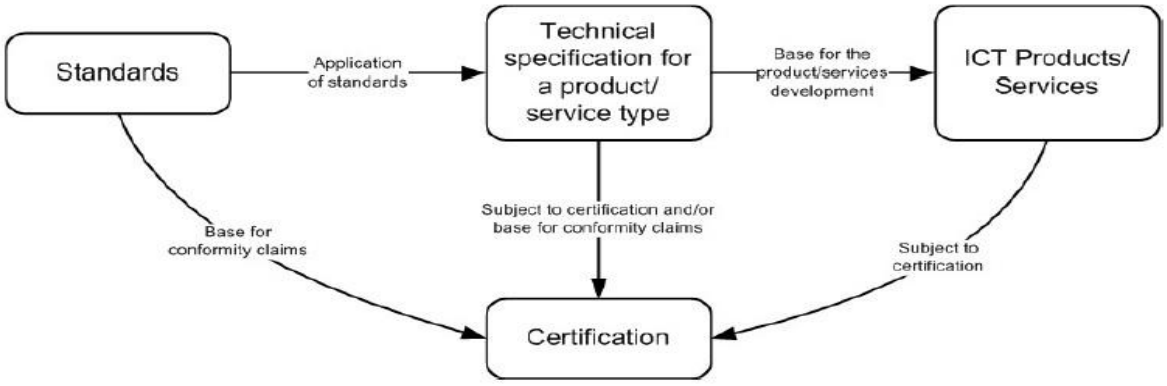


Fig. 1 - framework for security evaluation of products

language – 'protection profiles' (PP) for the product type, or 'security target' (ST) for a given product. Such specifications contain security requirements according to the formal taxonomy given in part 2 of CC, and simultaneously create the evaluation requirements by using security assurance components given in part 3 of CC.The evolution of CC from PP/ST through cPPs (collaborative Protection Profiles) and into the proposed "Direct Rationale" approach from the Common Criteria group does provide a framework for a wider(4), holistic view of security and therefore of confidence. The "Direct Rationale" approach provides a way of producing comprehensive security specifications for products, which is simpler than a traditional one hence it could be potentially applied in the IoT for preparing good technical specifications, giving simultaneously the ground for providing requiring solid and proven confidence the product meets security requirements.

The opportunity to drive market confidence in security of IoT may be developed from the work outlined in evolution of the Common Criteria (see also a detail examination in Annex B) to propose to all ICT security developing SDOs (5), to work towards cPPs and from there to work in the Direct Rationale cPP development. Evidently, the example use case of CC can be considered for other standards when it comes to IoT. As mentioned, there is a growing call for flexible and adaptive solutions in this environment and therefore a complete analysis is beyond the scope of this report. There is an opportunity to develop standards that have to be testable and that will be cited in the certification chain as proof of assurance. A subtle assertion is that if you comply with a standard, and that standard is properly maintained, then conformance is sufficient. Less obvious is that the proof of security
assurance will require many standards to be conformed to.

4. Mapping of requirements to standards

General overview

In the context of IoT devices, a broad generalisation of the role of standards is that their role is to provideinteroperability of "things". It is also a broad generalisation that standards provide requirements to be metand do not provide instructions on how to implement a requirement. For security standards thesestatements apply as a broad interpretation but with the slight modification that many security standards,or more likely the security functions defined in standards, give assurance of the interoperability of "things"when subject to attack by hostile parties. Thus standards may address functionality (e.g. an encryptionalgorithm), application of that functionality (e.g. use of specific encryption mode (say counter mode)), andcontextual use of that functionality(6) (e.g. application of encryption to provision of confidentiality protectionservices). Entities involved in cryptographic security that are required to interoperate will also require sharing knowledge and functionality that will include the identification of keys and algorithms. Thus security standards have to address simple mechanical interconnection, semantic and syntactic shared meaning, and management of attributes and organisations to react to security transgressions in an appropriate manner.

Organisational interoperability

There is a class of organisational management standards in security that defines roles within organisationsthat seek to enforce a "need to know". From a security perspective when two organisations share datathey may transfer data securely by having a common Communications Security (ComSec) framework, butthe ComSec exchange cannot make any inference on how data is treated prior to, or after, transfer(7). Thusthe local IT security policy of the sending and receiving organisations is trusted to be equivalent and thistrust may be reinforced by external measures.

Syntactic interoperability

Syntax derives from the Greek word meaning ordering and arrangement. The English language sentencestructure of subject-verb-object is a simple example of syntax, and generally in formal language syntax is the set of rules that allows a well formed expression to be formed from a fundamental set of symbols. In computing science syntax refers to the normative structure of data. In order to achieve syntacticinteroperability there has to be a shared understanding of the symbol set and of the ordering of symbols(8).In any language the dictionary of symbols is restricted, thus in general a verb should not be misconstruedas a noun for example (although there are particularly glaring examples of misuse that have becomenormal use, e.g. the use of "medal" as a verb wherein the conventional text "He won a medal" has nowbeen abused as "He medalled").

Semantic interoperability

Syntax cannot convey meaning and this is where semantics is introduced. Semantics derives meaning from syntactically correct statements. Semantic understanding itself is dependent on both pragmatics andcontext. There are a number of ways of exchanging semantic information although the success is dependent on structuring data to optimise the availability of semantic content and the transfer ofcontextual knowledge (although the transfer of pragmatics is less clear). The most obvious examples ofsemantic containers for syntactically correct information are protocols whereby the protocol (e.g. anshared state as a means of identifying context and this is often embedded in protocol (e.g. anauthentication protocol may go through states that include "Identified", "Challenge issued", "Responsepending" prior to finalising on the state "Authenticated").

Electrical and mechanical interoperability

Quite simply a device with a power connector using, for example, a Type IEC 60906-2 connection cannotaccept power from anything other than a Type IEC 60906-2 connector. Similarly, for example, a serial port complying to USB-Type-A will not be able to connect with a USB-Type-C lead. In addition to simplemechanical compatibility there is a requirement to ensure electrical interoperability covering amongstothers the voltage level(9), amperage level, DC or AC, frequency if AC, variation levels and so forth.

Radio communication interoperability

Radio (wireless) communication requires shared knowledge of frequency band, modulation technique,symbol rate, power, and so forth. In general radio communication can be characterised as broadcast andunreliable. The nature of the physical media requires that radio protocols make provisions to maximise linkreliability(10), most often achieved using various forms of Forward Error Correction in the Link Layer (layer 2 ofthe OSI stack).

5. Conclusions

The requirements listed in the ENISA report “Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures” have been mapped to an existing identifiable standard that if followed would allow the requirement to be satisfied. The detailed, requirement by requirement, mapping is given The simplified analysis yields that there is no significant standards gap - every requirement can be met by an existing standard. The problem is that this is neither the correct nor the expected answer. Standards exist for many different elements of making a device or service secure. However, when referring to IoT, one refers to an ecosystem of not only devices and services. Moreover, the context of use of IoT, its high scalability and other particularities further complicate the field and require more generic and flexible approaches. Therefore, for example the gap in IoT device standards for security is that the standards are not treated holistically so it is possible to deliver a device to the market that can authenticate its user, that can encrypt data it transmits, that can decrypt data it receives, that can deliver or verify the proof of integrity, but which will still be insecure. Similarly, the organisation developing the IoT product or service may have the development processes defined in management guidelines such as those of ISO-27000 but still delivers an insecure product.

REFERENCES

1. Verikoukis, C.; Minerva, R.; Guizani, M.; Datta, S.K.; Chen, Y.; Muller, H.A. Internet of Things: Part 2.IEEE Commun. Mag. 2017, 55, 114–115.
2. Silva, J.S.; Zhang, P.; Pering, T.; Boavida, F.; Hara, T.; Liebau, N.C. People-Centric Internet of Things.IEEE Commun. Mag. 2017, 55, 18–19.
3. Hasan, M.; Islam, M.M.; Islam, I.; Hashem, M.M.A. Attack and Anomaly Detection in IoT Sensors in IoT Sites Using Machine Learning Approaches. Internet Things 2019, 7, 100059.
4. Yang, Y.; Wu, L.; Li, G.Y.L.; Zhao, H. A survey on security and privacy issues in internet-of-things.IEEE Internet Things J. 2017, 4, 1250–1258.
5. Ling, Z.; Luo, J.; Xu, Y.; Gao, C.; Wu, K.; Fu, X. Security vulnerabilities of the internet of things: A case study of the smart plug system. IEEE Internet Things J. 2017, 4, 1899–1909.
6. Cheng, C.; Lu, R.; Petzoldt, A.; Takagi, T. Securing the Internet of Things in a quantum world. IEEE Commun. Mag. 2017, 55, 116–120.
7. Allho , F.; Henschke, A. The Internet of Things: Foundational ethical issues. Internet Things 2018, 1, 55–66.
8. Kawamoto, Y.; Nishiyama, H.; Kato, N.; Shimizu, Y.; Takahara, A.; Jiang, T. E
ectively collecting data for the location-based authentication in the Internet of Things. IEEE Syst. J. 2017, 11, 1403–1411.
9. Garcia-de-Prado, A.; Ortiz, G.; Boubeta-Puig, J. COLLECT: Collaborative Context-aware service-oriented architecture for intelligent decision-making in the Internet of Things. Expert Syst. Appl. 2017, 85, 231–248.
10. Fussler, C.; James, P. Eco-Innovation: A Break thorough Discipline for Innovation and Sustainability; Pitman: London, UK, 1996.