The Internet of Things Cybersecurity Standardization

MILICA D. ĐEKIĆ, Subotica

Professional Paper
UDC: 343.533::004
DOI: 10.5937/tehnika1904603D

The Internet of Things (IoT) landscape is a quite fast growing marketplace with so many open questions coming on with. The main challenge to this area is still its security and so many current and incoming professionals need to tackle such a concern through. As it's well-known, the IoT solutions would rely of a wide variety of digital, embedded and mechatronics systems coping with the exposing to the web. So many experts would make an advice to pay attention to cybersecurity at the project's initiation, so there would be a plenty of hard work to research and development (R&D) teams to proceed with those requirements. If the role of R&D members is to deal with the cybersecurity demands – would that mean that the expert's community should ask those professionals about their opinion on any kind of technological standardization? The best known international standards would come from the Switzerland's standardization body being called the International Standard Organization (ISO). There would also be some concerns how trusted emerging technology got and so many organizations worldwide would try to put that question into the legal frameworks. Apparently, the international standardization of the IoT cyber defense is something that should get stressed out through a lot of official meetings and discussions. In this paper, we would attempt to provide a comprehensive insight how the international standardization works in the practice and why it is important to standardize the current tendencies.

Key words: *Internet of Things, cybersecurity, standardization, trust, intelligence, etc.*

1. INTRODUCTION

Through the history of human kind, people would deal with more or less unified solutions. The industrialization of the world would begin at the end of 18th century and since then the people would see the need to better organize their processes, products and services. Even much before the industrialization, the man kind would figure out that their tools, food and water must deal with some kind of the order. Here we come to the term being the quality! So far, the human beings would realize that something could be more or less qualitative and for such an attribute many would be willing to pay quite much. It's well-known, that the social establishment through the history would cope with the high quality stuffs for their time, while the common people would lead so ordinary life. [6, 7] However, the modern epoch is not very different from the previous ages and even today we would deal with some sort of order in our lives and businesses. In other words, the good organization became the ultimate goal to any targeted group and many would recognize the significance of playing by the rules. The main reason for accepting the rules is the people's well-being, progress and prosperity. On the other hand, if we organize our industries to cope with some kind of procedures suggesting to their implementers to go step by step, we would see that such a requirement can only increase our productivity and effectiveness. The main point here is more we produce the bigger profit would be!

So, would the standardization be about the quality only? In our opinion, it's a quite trickery question for a reason that such a topic could get somehow correlated with the control. By control, we would not mean any sort of security activity, but rather we would see so as a simplification of some process, product and service. The point is if we distinguish anything we need to assess to so simple criteria, we would get the outcomes that would satisfy our needs and the final consumers would get happy with such a result. Differently saying, any sort of standardization is about

Author's address: Milica Đekić, Subotica, Vase Pelagića 39a

e-mail: milicadjekic82@gmail.com

Paper received: 08.05.2019.

Paper accepted: 22.05.2019.

the good quality management and even if we talk about the technological standards – we would get that those demands would insist on the good quality of the cutting-edge services as well as appropriate quality of the technological solutions. Right here, we should get aware that the standards would change with time and as human kind progresses – we would cope with the new and new standardization requirements. The human race would strive for better and better advancements and that's quite encouraging, because that's how we progress and develop our communities. For instance, there would be a lot of standards getting correlated with the legal risk management and the purpose of those documents is to make the order and improve the quality even in the legal regulations field. Apparently, the standardization is somehow about the control, but not in defense senses – and mostly in the adequate assessing manners.

The ISO standards regarding cyber defense of any sort of risk management would be the good reflection of the ongoing need to improve those areas of our work and activities. The standardization is quite important in terms of putting things into order and such an approach could greatly simplify our management in any area. Also, so many standard implementers would deal with the quality of food and water and those guys would know how to estimate if any product would meet the current needs. In addition, so many people would want to know if the standardization is something that would challenge our skills and make us learn and explore more, better and deeper. The fact is every new generation would appear as somehow being more progressive than the previous ones and for such a reason – it's quite natural to expect that the next generation standards would be more progressive as well. [16, 17] From this perspective, we should realize that the deep understanding of standardization is something we need so alarmingly. The reason for that is it could be the way to guide our progress and development. The standardization may appear as a quite profitable business, but anyone being led with the deep moral and ethical insights would know that it's something that is supposed to bring the benefits to the human kind. Finally, through this effort – we would try to make a closer look at the standardization trends and tendencies as well as some kind of needs regarding the IoT marketplace that should also get unified and better explained.

2. WHAT ARE THE NEW TENDECIES?

There are some predictions that by 2020 the word would have approximately 50 billion IoT devices being connected to the global network. This number may seem as fascinating for a reason that the international marketplace could get flooded with these new products. The trick with the IoT technology is that it would only be the digital transformation of the existing improvements combining with itself the internet connectivity. In other words, the command signal being used to manage some system or process would use a TCP/IP connection in order to get sent through the network. [6, 7] In our opinion, this emerging advancement got an opportunity to become the part of mass usage because of its cost-effectiveness and probably simplicity. Few decades back the world would get seen as a global village that would use the web communications in order to make people being in touch. Some experts would suggest that then we would deal with the internet of people and as that tendency went to the history – we would get the new paradigm being the IoT. The IoT would assume the application of the internet channel for making the connected devices talking to each other.

The main question here is how we could design such a solution and the answer to that question is not that simple at all. It requires a lot of engineering skills and it can be quite time consuming to produce such a system and synchronize all the devices to work as a whole. Every single project would start with the good preparation and before you make a decision on to run anything – you should do the good market's research that should indicate the current needs as well as trends within your targeted group. In other words, you must know who would potentially buy your product and once you determine so you would get in position to proceed with much deeper technological research. Further, it's quite necessary to investigate how you could develop your engineering solution and how much it would cost you. Apparently, it's recommended to estimate your budget and define the deadlines for any project's step. Also, you should take care about the possible tolerance in sense of project's schedule because there could get some constrains which could limit you in your project's realization. The IoT design is not the easy task and through your journey you would need to think about both – hardware and software approach.

The role of R&D teams is quite challenging and those guys should know how to resolve heaps of concerns. In addition, resolving the engineering problems seeks the certain level of creativity, innovative thinking and so many brilliant ideas. In other words, it would appear that so soon we would fully rule over such a technology and even developing economies would get the capacity to tackle the IoT projects. According to some sources, so many less developed societies would produce their first IoT solutions several years back, but they would not get aware how competitive their results are. Here we come to the next phase of our project's cycle and that is the good promotion, presentation and marketing of the final solution. On the other hand, any technological outcome should get tested, assessed and approved by the creditable certification body and it's so important to take into account such a detail in your planning process. [1, 3, 5] In other words, that could also cost somewhat and impact the final price of your product. Finally, it's obvious why the standardization in any production cycle matters and how such an approach could optimize your working process as well as quality of your ultimate solution.

3. THE ROLE OF CYBER DEFENSE

As we have suggested before, the IoT technologies still struggle with their cyber defense requirements. By so many researchers and IT security managers, cybersecurity is something that needs to get taken into consideration at the beginning of any project. This is normally case in the developed economies and those folks would cope with so straightforward procedures and rules that would offer them a chance to obtain their projects. On the other hand, the situation in the developing part of the world is far more different and those guys need the huge support in order to meet the international demands. People could get more or less developed affinity about some area and in so poor countries the population would not get an option to cope with the IT technologies. Those people would not even hear about the IoT wave being the part of the industry 4.0. Next, the progressive societies would lead the human kind in its intent to become more and more advanced. The situation in the Southeastern Europe is more as in any developing country. Those communities would follow the requirements of the developed world and non-European Union members would need to invoke the good legal regulations as well as plans and strategies in order to get a deeper insight about the cyber defense tendencies over the globe. In other words, our communities still need to learn hard about the international trends and attempt to understand the significance of cybersecurity in a development of the technological project.

The fact is there is a big knowledge about cybersecurity in the progressive countries and so many skillful people worldwide would try to transform those experiences into carefully prepared standards, procedures and policies in order to improve the quality of their processes, products and services. Indeed, there are a plenty of methods to explore how vulnerable the IoT systems are and those findings could get applied in order to define some countermeasures in cyber terms. [2, 5, 8] Here we come to the IoT cybersecurity standardization and its impacts to both society and economy. The need for cybersecurity nowadays is so huge and right here; we would not provide the cases of threatened IT safety and security regarding the IoT solutions. On the other hand, we could try to deal with some impacts of those activities including cyber sabotage, espionage and psychological operations. There are strong indications that all of these got possible in sense of IoT solutions. Also, it's important to mention that the IoT solutions are getting the segment of critical infrastructure and in that fashion it's important to realize why we must highlight the role of cyber defense in such a field.

4. THE INTERNET OF THINGS TOOLS

In this effort, we would attempt to provide a brief overview why the IoT search engines as Shodan and Censys matter in the better IT protection. Also, we would want to appeal on the standards developers to take into account these technological advancements before they start to write their standards for a reason that could offer much higher quality of the technical service. [16, 17, 18] The IoT crawlers are so convenient tools for exploring the IoT network worldwide and discovering its vulnerabilities as well. So many security researchers would cope with these solutions and figure out that their applications are nearly limitless. In other words, in order to develop the good IoT cybersecurity standardization framework you need to deeply correspond with the security industry. The IoT search engines could serve as the intelligence collectors and once you cope with those findings you would get a chance to better understand the weaknesses of your technology. It's quite interesting that these crawlers would give you an opportunity to see all the pluses and minuses of the critical infrastructure and its IT safety and security. This may get significant from the strategic perspective because once you make a standardization of the entire IoT complex you would get capable to offer more qualitative usage to those improvements.

5. THE NEED FOR STANDARDIZATION

With about 50 billion IoT devices worldwide so soon – there is the strong need for an appropriate standardization of this area. The point is we need to be safe when we use the IoT technologies and for such a reason the unification of that marketplace may play the crucial role in the future. The process of standardization takes time and the standardization by itself it's not only about the standards implementation and maintainace, but rather about the good research as well as development, so far. There is the entire procedure from the standards initial draft until their final approval. [1, 2, 6] This sort of concern is usually stressed out through so many discussions, meetings and public commenting sessions. The feasible collaboration between the standardization bodies and security industry can make a significant progress in the IoT cybersecurity area. The industry 4.0. landscape could seem as a quite dynamic and complicated one and indeed, it is – but we should know as any technological revolution brought the new ideas and approaches – even this transformation can require the novel rules and standards. We are definitely in progress with something emerging that should get managed smartly and intelligently in order to take a full advantage over its outcomes. For such a reason, there is the entire tendency that would dictate the requirements for this new exciting field of science and technology.

6. SOME INERNATIONAL IMPACTS

The international standardization is from a strategic importance to the global community. It can greatly accelerate the world's economy and make significant impacts to the entire human society. There is the enormous need for the experts in such an area and the fact is that the standards R&D departments demand the powerful support from the standards implementers. The role of the standards R&D teams is to make the standards and the implementers should spread them worldwide.

This may appear as a quite profitable business and the point is everyone is beneficial in such a game. [6, 7] The international standardization is something getting deeply correlated with the progress and if so many people over the globe receive the skill how to deal with such an improvement – they would undoubtedly get appreciated and needed by their communities. The interest for the IoT cybersecurity standardization is the consequence of the modern tendencies and industrial revolution, so we should pay a great attention to the trends coming on so soon.

7. DISCUSSIONS

The IoT cybersecurity standardization is an emerging question in so many developed economies and there are some indications that such a trend could get from the interest to the entire international community. The ISO has developed so many technical, organizational and cybersecurity standards and what we miss at this moment is much deeper approach to the 4th industrial revolution.

The fields of that boom are artificial intelligence, deep learning, cryptocurrencies, industrial internet of things and much more. In other words, all these areas need the good standardization as well in order to serve for the good purposes to the human race.

8. CONCLUSION

Through this effort, it's quite clear that the entire planet is going through some sort of technological breakthrough. The need for strategic thinking and planning is so demanding and as tendencies suggest – there would be the huge need for those sorts of professionals. The future may appear as so promising, so let it be like that!

9. ACKNOWLEDGEMENTS

The author is so deeply thankful to her family for all its love, care and support through her life, education and career.

REFERENCES

[1] Ablon L, Libicki M. C, Golay A, *Markets for Cybercrime Tools and Stolen Data*, Sponsored by Juniper Networks, 2014, Web source: http://www.-rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

[2] Beaver K, Davis P. T, *Hacking Wireless Networks for Dummies*, Wiley Publishing, 2005, Web source: https://cdn.preterhuman.net/texts/underground/hacking/Hacking_Wireless_Networks_For_Dummies_2005.pdf

[3] Bergman M. K, *The Deep Web: Surfacing Hidden Value, White paper*, 2000, Web source: http://jornalggn.com.br/sites/default/files/documentos/2011_bergman_7_cafarella_informationretrieval_presentation1_2.pdf

[4] Charney S, *Rethinking the Cyber Threat: A Framwork and Path Forward*, Microsoft, 2009.

[5] Chaliand G. and Blin A, The History of Terrorism, University of California Press, 2007, Web source: https://wikileaks.org/gifiles/attach/177/177597_History%20of%20Ter.pdf

[6] CRS Report for Congress, *Critical Infrastructure and Key Assets: Definition and Identification*, 2004, Web source: https://www.fas.org/sgp/crs/RL32631.pdf

[7] James P, Jenson M. And Tinsley H, Understanding the Threat: What Data Tell Us about U.S. Foreign Fighters, START, 2015, Web source: https://www.-start.umd.edu/publication/understanding-threat-what-data-tell-us-about-us-foreign-fighters

[8] *RFID Security*, The Government of the Hong Kong Special Administrative Region, 2008, Web source: http://www.infosec.gov.hk/english/technical/files/rfid.pdf

[9] Payne S. P, *A Guide to Security Metrics*, SANS Institute, Web source: https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55, 2007,

[10] Puhe M, Edelmann M, Reichenbach M, *Integrated urban e-ticketing for public transport and touristic sites*, Final report, Science and Technology Options

Assessment, Web source: http://www.europarl.-europa.eu/RegData/etudes/etudes/join/2014/513551/IPOL-JOIN_ET(2014)513551_EN.pdf, 2014,

[11]Ponemon Institute LLC, *Cost of Data Breach Study: Global Analysis*, Ponemon Institute Research Report, 2015, Web source: https://nhlearningsolutions.com/-Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF, 2015

[12]Symantec, *Internet Security Threat Report*, 2016, Web source: https://www.symantec.com/content/-dam/symantec/docs/reports/istr-21-2016-en.pdf

[13]S. Weine and B. H. Ellis, *Lessons Learned from Mental Health and Education: Identifying Best Practices for Addressing Violent Extremism*, STA-RT, 2015, Web source: https://www.start.umd.edu-/pubs/START_LessonsLearnedfromMentalHealthAndEducation_FullReport_Oct2015.pdf

[14]Weine S. and Ellis B. H, *Supporting A Multidisciplinary Approach to Addressing Violent Extremism*, START, 2015

[15]Aleksandar Rodic, Gyula Mester, Ivan Stojković, *Qualitative Evaluation of Flight Controller Performances for Autonomous Quadrotors*, pp. 115-134, Intelligent Systems: Models and Applications, Endre Pap (Ed.), Topics in Intelligent Engineering and Informatics, Vol. 3, Part. 2, TIEI 3, ISSN 2193-9411, ISBN 978-3-642-33958-5, DOI 10.1007/978-3-642-33959-2_7, Springer-Verlag Berlin Heidelberg, 2013.

[16]Gyula Mester, Aleksandar Rodic, *Sensor-Based Intelligent Mobile Robot Navigation in Unknown Environments*, International Journal of Electrical and Computer Engineering Systems, Vol. 1, No. 2, pp. 1-8, ISSN: 1847-6996, 2010.

[17]Gyula Mester, Szilveszter Pletl, Gizella Pajor, Zoltan Jeges, *Flexible Planetary Gear Drives in Robotics*. Proceedings of the 1992 International Conference on Industrial Electronics, Control, Instrumentation and Automation - Robotics, CIM and Automation, Emerging Technologies, IEEE IECON '92, Vol. 2, pp. 646-649, ISBN 0-7803-0582-5, DOI: 10.1109/IECON.1992.254556, San Diego, California, USA, November 9-13, 1992.

REZIME

STANDARDIZACIJA VISOKOTEHNOLOŠKE BEZBEDNOSTI INTERNETA STVARI

Obzorje Interneta Stvari (IS) je brzo narastajuće tržište sa jako mnogo otvorenih pitanja koja pristižu. Glavni izazov za ovo polje je još uvek njegova bezbednost i mnogo sadašnjih i dolazećih profesionalaca treba da se izbori sa tim problemima. Kao što se zna, IS rešenja se oslanjaju na digitalne, umeštene i mehatroničke sisteme koji su otvoreni prema web-u. Jako mnogo stručnjaka u toj oblasti sugeriše da treba obratiti pažnju na visokotehnološku bezbednost na samom početku projekta, što znači mnogo napornog rada za istraživačko-razvojne timove. Ovim se dovode u vezu tehničke nauke, bezbednost i standardizacija kao neizostavni učesnici u razvoju projekta. Najpoznatiji međunarodni standardi dolaze iz Švajcarske i dobro su poznati kao ISO standardna rešenja. Glavno pitanje je koliko možemo da verujemo novim tehnologijama i to je nešto što danas ulazi u zakonske okvire. Dakako, međunarodna standardizacija visokotehnološke bezbednosti IS-a je nešto što mora da prođe kroz panel diskusije i zvanične sastanke. U ovom radu, pokušaćemo da damo sveobuhvatan uvid u to kako međunarodna standardizacija funkcioniše u praksi i zašto je bitno standardizovati savremene tendencije.

Ključne reči: *Internet stvari, visokotehnološka bezbednost, standardizacija, poverenje, saznanja, itd.*