The Internet of Things Security Challenges

MILICA D. ĐEKIĆ, Subotica

Professional paper

UDC: 343.53:004.738.5

343.9

DOI: 10.5937/tehnika2005678D

The Internet of Things (IoT) is a quite recent paradigm going a decade back to the past. With the development and deployment of wireless technologies this new advancement has taken the part in the consumers' lives and businesses. In other words, the IoT is a pretty convenient way to correlated devices with each other and make them communicate in such a network. This is feasible using the internet connection and differently saying, all IoT devices forming the IoT asset got their IP addresses. From this perspective, it's quite clear that this technology got a lot of advantages and the users may feel so thankful for being the part of an IoT community. On the other hand, the consumers would spend less time thinking about the possible security concerns being linked to this new improvement. In this paper, we intend to discuss how secure our IoT infrastructure is, what its strategic implications are and why cyber industry should invest more time and effort in order to better research and develop this concept. In addition, we would try to deal a bit more with the IoT crawlers as the tools for investigating the IoT network and being so handy for both – researchers and hacker's groups.

Key words: cyber defense, IoT, intelligence, security, technology, industry 4.0, etc.

1. INTRODUCTION

Approximately two decades back the internet would cope with its global boom. So many people worldwide would become the residents of a global village and it would be quite easy to make a contact with the folks on the other side of the globe in a sub-second period of time. From today's point of view, we would talk about the Internet of People (IoP) being so popular topic in the 2000s. Nowadays that concept would get less mentioned probably because it would get widely accepted everywhere. Some experts would say that once the people stop talking about some topic that means either that area became well-accepted or it went to the history. At this moment, we have the similar situation with the IoT paradigm. Everyone would talk about such a technological solution and indeed, you would find a lot of its resources on the web or within the expert's channels [7-9]. In other words, the people would recognize the significance of that new technology and they would attempt to cope with so.

Also, the researchers, scientists and engineers wo-

ldwide would get aware of the IoT security concerns and they would put a lot of effort on in order to contribute to the better understanding of such an issue. In our opinion, the new tendency in the IoT development and deployment would be paying more stage, it's important to get that defense staffs must be the good thinkers. The similar logics could get applied to the cyber defense. It's also about the risk management, but in this case – such a risk would get linked to the cyberspace. In essence, we hope this brief introduction has given the useful insight into topics we want to discuss through this paper and also we believe that the expert's community could find this effort as a good starting point to some further investigations.

2. THE RELATED WORK

Many researchers would tackle the issues being correlated with the IoT field and they would undoubtedly give a big contribution to that area. The security of an IoT technology is a quite new challenge to that branch of science and technology. In [2] we would find a quite comprehensive approach to all security concerns being linked with the IoT landscape. Also, some authors would make so many good recommendations how the IoT environment could become much safer place to operate in. The US National Institute of Science and Technology (NIST) would put a lot of efforts to explain how significant the standardization

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

e-mail: milicadjekic82@gmail.com

Paper received: 07.09.2020.

Paper accepted: 17.09.2020.

of the IoT advancements could be [7]. Indeed, the standardization of this technology could take a huge part in the coming technological endeavors because if we deal with the unified IoT landscape, we could better control so or in other words – make it being more secure. Although the IoT marketplace is rapidly growing, it's getting obvious that the economical impacts of this technology would get so suitable to many people worldwide. By some prognoses, there will be about 50 billion IoT devices by the 2020 [2, 5, 6]. This rising curve of such a marketplace may indicate that we could get less secure in cyber terms if we do not adopt the best practices for dealing with those challenges [2].

3. THE INTERNET OF THINGS PARADIGM

The IoT is a quite recent concept that would change our points of view in sense of our skillfulness and way of thinking. That paradigm would revolutionize the entire world and it would deal with the advantages offering them to make a breakthrough on the marketplace. The fact is the IoT is still developing and as it appears from a today's perspective – it would take some time in order to get widely accepted. Right here, we would talk about the skills we need to deal with such a technology as its end users. Some sources would claim that this 4th technological revolution could increase our math-logical IQ. Why would that be the truth? First, if we take into consideration all complexity of the modern technological solutions and how skillful the end user should be in order to learn to take advantage over those equipments. Through this section, we would mention the technological revolution [2, 5, 6]. By many, that phenomenon would cover on the factories, industry assets and manufacturing complexes only. In this case, that revolution would happen at your home, in your everyday life and it would even become the part of your privacy. In other, words the quite near future would bring us so many computer geeks who would be the member of such a big global network.

So, what is the difference between the previous technologies and the IoT or in other words, what makes the IoT being so special in comparison with the other solutions? It's so important to know that the IoT is the network of devices that would correlate so many gadgets that would communicate with each other using the web signal. It would also include something that we know as a smart technology. In the practice, the civilian's usages of the IoT would consist of the web cameras, smart home equipment, health's condition monitoring devices and so on. Through this review, it's quite obvious that the people would need the skills in order to deal with such a technology. There is the good saying suggesting that the simplicity is an ultimate sophistication. We would fully agree with so! Well, in

order to use the IoT hardware and software – you would do that so simply, but you would need some skills as well as the high engineering IQ. It's not that easy at all to connect your gadgets to the network or to use your smart application or even to troubleshoot some technical problem [2]. In all these cases, you would need to deal with the good skills and even if you call your Help Desk – you would need the skill to explain your concern to your operator and understand what he has to advise to you.

The common thing to all these IoT solutions is that they would deal with their own IP address. In other words, getting your own IP address means that you would get your own access to the internet. In so many developed economies, there would be the entire wireless signal infrastructure within the urban centers and the people would so greatly use those benefits. For instance, if you go out for a recreation to some green area – you would get the access to the web which would support your mobile device to deal with your gadget monitoring, say, your heart rate. Doing your recreation every single day, you would get in position to compare your day by day statistics being stored to your application analytics and you would so accurately know if you are progressing with your training. The good way to deal with some sort of situational awareness, right? The situational awareness is so ongoing topic to many armed forces worldwide and there are some indications that the competitive armies could try to adopt the IoT technology so soon. In conclusion, there is a wide spectrum of the potential IoT usages and through this effort – we would discuss only some of them.

4. THE INTERNET OF THINGS SEARCH ENGINES

There are so many crawlers on the web and the consumers are well-familiar with the Google, Yahoo, Bing and much more. The most known of them is certainly the Google which would pick up the data from the so called – surface internet. On the other hand, there are a plenty of Darknet search engines and the best-known there is the Tor. The role of this article is not to make any comparison between the surface and deep internet, but rather to suggest that there are also some crawlers being available online that could get used to investigate the global IoT network. The most known and so popular of them are the Shodan and Censys that could get found on the following web locations www.shodan.io and www.censys.io, respectively. These crawlers could represent the convenient way to the security researchers who would want to investigate the vulnerabilities of the IoT network, report them and in such a manner, contribute to the possible improvements of those solutions.

The both IoT crawling systems are mostly commercial which means that you need to pay something in order to take a full advantage over them. For instance, the Shodan would deal with the banners and get back some results. In addition, we would find so many explanations on how these two search engines work, but we are not completely confident to stand behind any of them because we are aware of that the marketers could try to hide their business secrets. Also, some sources would claim that the Censys would apply the so called Z-map in order to make a wide search of the web [5, 6]. This could also be the marketing trick which aim is to attempt to camouflage how such a system works for real. In addition, the domain name being .io would indicate that the website would cope with the input and output ports, so far. In essence, the trick is if you enter some keyword into both of the crawlers' web pages – you would get the real collection of IP addresses with some geo-location details that would suggest you using some algorithm what it got accessible through such a search.

On the other hand, what it is also important to know is that you need to register in order to get the access to those search engines' capacities. The media would go that far away calling the Shodan the most dangerous crawler of today, because they would believe that the cybercrime syndicates could misuse that product. The inventor of that solution would try to protect himself claiming that there is no place to fear because his project is for security researchers only. However, the fact is that the hackers could open on the fake accounts and try to exploit the people online which devices would get visible through those search engines. Once the cyber criminals get in possession of any IP address, they could use the hacking tools to simply make a breach into such an infrastructure. In order to login to anyone's computer the hackers need some authentication details or, in other words, the username and password. Testing the Shodan's capabilities we would easily notice that some people over the globe would use so weak authentication putting, let's say, username or admin and password or 1234 as their authentication information. Finally, it's quite obvious that there are the ways to make a breach into someone's IoT network and further, through this article, we would attempt to explain what the risks are and how we could put them under control.

5. THE WAYS TO PROTECT YOUR INTERNET THINGS NETWORK

As we would see through the previous chapter – there would be the very few difficulties to discover and exploit someone's IoT asset. Researching the IoT crawlers we would obtain the findings that would undoubtedly indicate that it's feasible to get an access to

someone's web camera being in his bedroom or in the children room. As it's so clear – there are a plenty of ways for exploiting those weaknesses and people should get aware of all security concerns before they decide to apply any IoT solution. Being the part of an IoT family is the convenience for real as well as the risk, so our advice is to learn to manage that risk somehow. There are some best practice recommendations that would support you in securing you IoT asset and as we said before the NIST would give some useful tips and tricks in its report [7]. Before you begin to research any area of technology – it's good to know that there are a lot of web resources that could get quite helpful, but also think about the expert's channels which could provide you with the quite qualitative information.

Through this discussion, we would realize that the authentication could get one of the most obvious weaknesses within your IoT network. So, we would recommend you to deal with the strong authentication and periodically change your login information. This could work for both – your personal and business life! Any loss of your private or business details could cost you a lot and the cybercrime underground would know that publishing those data could compromise someone's reputation. So frequently, they could try to get the money from their victims in return to their silence and if they do not make a deal – they would find the way to sell their catch on the black market. Anyway and anyhow, someone would get ready to offer the money for their findings! So many Law Enforcement agencies would cope with this sort of a crime and one of the helpful ways to protect your critical data is to invest into the education and training of your Police members. Also, we would try to advise the governmental and non-governmental institutions to try to deal with the awareness rise campaigns in order to prepare their people for the possible cyber threats.

Next, we would try to discuss how you should set up your asset in order to hide your IP address and make it being less visible in terms of the potential cyber incidents. For example, if you adjust your Firewall to rely mostly on its outbound communications rather than on its inbound ports – you would make your IoT experience being more secure. In the web resources [2], we would find the quite handy explanations suggesting that the IoT crawlers would cope with the inbound ports only and if you transfer your web traffic to the outbound ports – you would get invisible to the IoT search engines. The both – inbound and outbound communications would be two-directional and in case of inbound traffic you would receive the signal from the web and send your response to the global network, while in the case of outbound communications – you would do the reverse thing.

Also, what it is significant to mention here is that you should think how to hide your IP address. In other words, your private IP address should be different from your public IP address. The private IP address is something being correlated to your physical device and the public IP address is something that would appear on the web about you. In addition, there are so many good tools on the internet that could get applied in order to play with your IP address. In such a sense, we would mention some online location offering you an opportunity to mask your IP or you can simply use the gadgets such as the Virtual Private Networks or VPNs that could provide you a chance to cope with the different public IP addresses. In other words, many experts would see this approach as some kind of a camouflage and they would warmly recommend to everyone to try that method on. At the end, the security is about the risk management as we would mention before, so get aware of all possible risks, threats and challenges that could make your cyber experience being less suitable. Additionally, any IT breach into your IoT infrastructure could cost you a lot and before you decide to make any step on – try to make a cost-benefit analysis and you would get that the investment into a cyber defense would cost you less than potential damage being the consequence of the hacker's attacks.

6. THE INTERNET OF THINGS AS THE PART OF A CRITICAL INFRASTRUCTURE

The critical infrastructure is any plant, object or asset being from a vital or strategic importance to its nation or country. Some of helpful examples of the critical infrastructure are airports, telecommunication systems, internet infrastructure, industry assets, government agencies and so on. Any sort of discontinuity in operation of these assets could seriously affect the lives of people belonging to that territory. In other words, in order to distract the work of any critical asset the threats could try to apply the diverse ways of sabotage and diversion. For instance, try to imagine how severe impacts the water or electricity restrictions could have on lives and work of some nation's members. So, the question here could be how we can correlate this sort of strategically significant infrastructure with the IoT networks. The answer to this question is quite simple – the majority of critical infrastructure would deal with its devices being connected to the global web.

If you try to do a search using, say, the Shodan IoT crawler – you would notice that it would offer you an option to look for the Industrial Control Systems (ICS), Programmable Logic Controllers (PLCs) or Supervisory Control and Data Acquisition (SCADA) systems and much more. Applying the simple search via Shodan and targeting these solutions – you would get a

plenty of the IP addresses and geographical locations suggesting you where those systems could get found. In other words, just try to imagine how devastating the impact of possible cyber sabotage to these assets could be. Also, many would remember the Stuxnet operation being conducted by the US and Israeli defense forces to the Iranian nuclear program [7, 8]. In such a case, the highly sophisticated computer worm has caused the malfunction of all the PLCs being used in that complex.

To wrap up this section, it's so important to suggest that the critical infrastructure would greatly rely on the IoT technologies and many would see so as the 4th industrial revolution. It's also good to mention that critical infrastructure could include anything being from vital importance even for an economy of some country and right here, we would indicate those could be even the small businesses. The reason why some agencies would classify that sector into the critical infrastructure is that the significantly high percentage of the country's GDP would depend on those enterprises. So, if you know that the both – private and public sectors – are adopting the IoT solutions, it's quite obvious why we would deal with such a technology even in the commerce also being the part of the nation's strategic infrastructure. Finally, we would want to suggest that the IoT security is still the open concern and it would probably take some time before the cyber industry develop some responses to the ongoing situations. In any sense, the IoT is – indeed – the part of the critical infrastructure and its role would become more important as its marketplace is growing, so the need for the good cyber defense would rise promptly.

7. THE INTERNET THINGS SECURITY STRATEGIES

The best way to prevent something is to accept so. In other words, if we want to deal with the cyber breaches within the IoT network – we should try to accept either they exist or they can happen. Once you get aware that there is a certain risk you are supposed to manage – you would handle any situation in much easier manner [2]. Through this effort, we would talk about some measures that could get applied in order to protect your IoT asset and right here, we would like to highlight that the best way to tackle the problem is to aware the people that the problem exists in the practice. This does not mean that everyone using the IoT technology would cope with the hacker's attacks, but rather he would accept the possibility of such an occurrence.

In other words, it's useful to know that the investment in the human resources is the best possible investment. Why? If you teach the people how to manage some situation you would create the active

workforce that would combat to protect your infrastructure. Once the cyber defense becomes the part of our working routine – there will be fewer headaches to any business.

To summarize, in order to maintain your cyber risk at an acceptable level you should know that it could be so important to invest into your staffs' education and training.

Once the people get aware of all the challenges and learn how to resolve the real concerns or in other words, when they gain that skill – it would be less difficult to deal with the IoT greatest challenge being the security. So, the best practice plans, frameworks and strategies are expected as a response to the current situation!

8. THE DISCUSSION

Through this discussion, you could easily get an impression that we live in the IoT age. Well, that's partially accurate because there are also so many other technologies being present on the marketplace. Anyhow, the IoT technology is something that would have the quite promising usages in the near future. It's a convenient way to improve our skills and make us a bit smarter in a technological sense [2, 5, 6].

Also, what we need to care of the most is the IoT security being the huge challenge to a today's cyber community. The potentials of this advancement are nearly limitless and its marketplace is getting bigger and bigger every single day offering the realistic opportunities to a business community. Finally, as we are still talking about this solution that means we did not fully adopt it yet.

Once we stop mentioning so that would indicate that it got completely accepted. In other words, the expert's groups still need to put a lot of effort on in order to better understand this area of science and technology.

9. THE CONCLUSION

Some researchers would suggest that the best method to defeat from a threat is to understand it. Right here, we would suggest that we do not fully understand

all the challenges of the IoT technology, so we should put lots of effort on in order to bridge that gap.

We would mention that the biggest challenge to this technological improvement is its security and it's well known that there is the certain cyber skill shortage worldwide. In conclusion, it would seem that our track to any solution could take much more time once we take into consideration all the findings of this discussion.

10. THE ACKNOWLEDGEMENTS

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

REFERENCES

- [1] CSA. Security Guidance for Early Adopters of the Internet of Things (IoT), 54 p., April 2015.
- [2] Djekic M, *The Internet of Things: Concept, Applications and Security*, Lambert Academic Publishing, 2017.
- [3] PubNub, A New Approach to IoT Security - 5 Key Requirements to Securing IoT Communications, 8 p., 2015.
- [4] Symantec. An Internet of Things Reference Architecture, 22 p., 2016 .
- [5] The Censys website being available at <https://censys.io/>
- [6] The Shodan website being available at <https://www.shodan.io/>
- [7] The US Department of Homeland Security. Strategic Principles for Securing the Internet of Things (IoT), Version 1.0, 17 p., November 15, 2016.
- [8] Maede Zolanvari, *IoT Security: A Survey*, University press, 2015.
- [9] GFCE – Global Forum on Cyber Expertise. Internet of Things (IoT) Security, 21 p., October, 2019.

REZIME

BEZBEDONOSNI IZAZOVI INTERNETA STVARI

Internet Stvari (IS) je prilično nova paradigma koja ide čitavu deceniju unazad u prošlost. Sa razvojem bežičnih tehnologija ova nova rešenja su uzela učešća u potrošačkim životima i poslovnom okruženju. Drugim rečima, IS je prilično zgodan način da se povežu uređaji međusobno, kao i da se ostvari komunikacija u takvoj mreži. Sve ovo je moguće primenom internet konekcije ili drugačije rečeno, svi IS uređaji koji čine IS infrastrukturu imaju svoju IP adresu. Sa ovog stanovišta, prilično je jasno da ova tehnologija ima mogo prednosti i sami korisnici mogu da se osećaju bezbrižno što su deo IS zajednice. S druge strane, korisnici mogu da u mnogome manje brinu o mogućim bezbednosnim problemima koji su skupčani sa ovim novotarijama. U ovom radu, nameravamo da prodiskutujemo koliko su bezbedna IS postrojenja, koje su njihova strateške implikacije i zbog čega visokotehnološka indsutrija treba da uloži više vremena i truda u istraživanje i razvoj ovog koncepta. U dodatku, pokušaćemo da obratimo pažnju na IS pretraživače koji služe kao alatke za ispitivanje IS mreže i koji su podjednako zgodni kako za istraživače, tako i za hakerske grupe.

Ključne reči: visokotehnološka bezbednost, IS, saznanje, bezbednost, tehnika, industrija 4.0, itd.