The Internet of Things Security

MILICA D. DEKIĆ, Subotica

The Internet of Things (IoT) is a quite new concept covering on digital systems being correlated with each other. The first role of the Internet was to connect people, while this new paradigm serves in terms of connecting devices. Those solutions could get connected to each other using a standard web signal or applying another sort of communication channels. It’s estimated that the IoT has included around 4.9 billion devices by the end of 2015, while it’s expected that there would be 25 billion IoT devices in 2020.

The purpose of this paper is to provide a comprehensive overview about how this concept works and try to deal with some of a security’s aspect of this useful paradigm.

Key words: cybersecurity, Internet of Things, web, defense, technology, etc

1. INTRODUCTION

The modern technological progress has challenged many scientists, researchers and engineers to provide their full effort in investigating these new tendencies. The global picture has changed since we deal with cyber technologies and such a concept made us dependent on computers, web and mobile devices. The current trend is that the entire society got dependent on emerging advancements and the quite interesting fact is that these new technologies would not gain their popularity in a legal world only, but rather in illegal domains [1, 6]. This tendency would require from Defense Forces to produce a highly skillful workforce that would be capable to respond to these new requirements.

It’s not an easy task to investigate a cybercrime or another way of illegal behavior on the web. The forensic detectives doing those cases are supposed to be well-trained in order to resolve many complicated problems. Resolving the case in a forensic manner would demand collecting the evidence, analyzing their meaning and preparing skillful reports which would explain what happened for real. Also, it’s necessary for the members of a Justice System to be well-educated in sense to deal with this sort of the cases. The fact is that whatever anyone does in a cyberspace would leave the trace to forensic detectives which would usually know how to re-construct what occurred in a practice.

In other words, as the entire society got dependent on new technologies – even the malicious actors would cope with that sort of tendency [1, 2]. The majority of modern investigations need a good preparation before anyone runs the case and lots of brainstorming and discussions that would clarify how professionals should approach a certain issue.

Finally, we would come to that new concept being called the Internet of Things. Practically, it’s nothing else – but the part of our technological evolution. We would call that paradigm like so, because it would indicate that many devices got connected with each other through some sort of a big network.

Through this article, we also intend to provide a better insight into all challenges of this novel concept as well as talk a bit more about security’s aspects being vitally important in understanding how these systems work and how they could be protected. The Internet of Things is a trend that would improve our technological development and deployment and also open up many security’s questions being the challenges for tomorrow.

2. WHAT IS THE INTERNET OF THINGS?

The Internet of Things is a fast-growing marketplace deserving the attention of financial investors and economic strategists because of its robustness and flexibility. For a quite small investment this marketplace promises the quite big returns in a short period of time. The Internet of Things in a technological manner represents a set of electronic devices being connected...
to communicate with each other. The main advantage of such a solution is its convenience, while the supreme weaknesses could be security by their nature. When we talk about the Internet of Things – we would mean by that a technological evolution that would bring us this new concept through the past decade.

As time goes on – a technology would become more and more sophisticated and at this stage of its development and deployment – we would live this IoT age. The primary role of the Internet was to connect people with each other and then we would talk about the Internet of People, while this modern paradigm deals with the devices being connected to each other and we talk about the Internet of Things. The typical examples of solutions being used as a part of the Internet of Things are industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), embedded systems and smart equipment [6, 7]. It’s well-known that many home solutions would use sensors, computers and networks to correlate our home devices to each other making a freaky place out of our accommodation in case we face up any sort of cyber incidents.

Right here, we would mention why it’s important to make your IoT network being the secure one. First, you would avoid any sort of sabotage, hacking or cyber espionage and second, you would deal with less flaws through your work. Through this paper, we intend to discuss a bit deeper the applications of the Internet of Things and its security’s challenges. Right now, it’s sufficient to suggest that the IoT security is about a well-researched design and following the best practice. Many reputable international institutes and organizations would deal with some sorts of researches suggesting how we should manage a risk in terms of the Internet of Things. As we would mainly rely on computers, web and mobile technologies through this technological improvement – we would obviously cope with some of cyber defense best practices. Finally, it’s significant to add that the Internet of Things is inseparable part of cybersecurity, so we should always have that in mind.

3. THE MAIN APPLICATIONS OF THE INTERNET OF THINGS

The role of the Internet of Things is to make electronic and electrical devices work together as a network. Many today’s solutions got exposed to the web and the majority of them would use the internet signal or another way of communication to deal with each other. There are some highly sophisticated tools serving as IoT search engines that got capacity to find the IoT devices being connected to the web. It’s getting clear that it’s not suitable at all if anyone would spy on anyone’s bedroom or children’s room using the weaknesses of their web-cameras. It’s well known that the organized crime groups, human trafficking rings or even terrorist organizations would pay well to obtain confirmed information about the situation within someone’s home, office or critical asset.

On the other hand, some of the main applications of the Internet of Things could be within smart homes, industrial infrastructure, and intelligent equipment being based on microcontroller-driven solutions or any other devices using the internet channel to talk to each other. Some of the best known tools for searching the Internet of Things are Shodan and Censys. Their web addresses are www.shodan.io and www.censys.io suggesting that they are registered as input/output (I/O) domains. This sort of indication would correlate these scary searching tools with the I/O ports serving as a link to the IoT devices being connected to computing units [4, 5]. These types of search engines could provide an IP address of any devices being visible to them on the web and in such a case – it’s highly recommended to protect your port’s data transfer.

For instance, computers would deal with the incoming ports being called the inbound ones and the outcoming ports being named the outbound ones. The IoT search engines would scan all inbound ports being correlated with their web servers and provide such information to their users who would obtain the IP address and using some of the hacker’s gadgets with a remote administration’s option cause some of cyber incidents. The well-known hacker’s tools being used for connecting to someone’s IT asset are Radmin and Advanced IP scanner that got ability to search through the computer’s network and remotely connect to a device being online. So, even if your inbound ports are not set up to hide your computer and its equipment from the IoT search engines – it could be useful to rely on a strong authentication offering you an opportunity to smartly choose your username and password that would protect your IT infrastructure.

A great deal of the complications may appear if anyone using, say, the Shodan tool obtains the information about some ICS or SCADA systems and try to connect to those assets in order to take a remote control over them. As it’s known, these systems are the part of a critical infrastructure being strategically significant to some country. Many research institutes would deal with these sorts of challenges and provide great efforts in terms of the best practice documentations [2, 3, 7]. So, it’s strongly advisable to follow some of those suggestions and try to protect your infrastructure. Finally, we would make a brief overview of hacker’s tools being used to take control over their targets. For instance, these gadgets could make a file transfer secretly causing you lose confidential information
from your network. On the other hand, they may shut down your computer or make it work as a hacker’s tool commands. In addition, the hackers could spend lots of time with your machine trying to steal as much information as possible before they make a decision to take any step on.

4. THE SECURITY’S CHALLENGES OF THE INTERNET OF THINGS

As we would see through the previous section, the Internet of Things is coping with many security’s challenges. For example, the IoT searching tools like a Shodan could offer an opportunity to malicious actors find the quite vulnerable computers worldwide. Also, once the hackers target those machines, they may start exploiting them offering their service on the black market. The primary purpose of IoT search tools is to serve to researcher’s community as they seek from their users to register in order to use the advantages of those products. On the other hand, some of IP addresses being available through a Shodan tool would use a quite weak authentication. For instance, it’s not a rare case that searching a Shodan – you would find computers or IoT devices applying usernames and password such as admin and 1234 or username and password.

In addition, some hackers could also break into the rest of systems simply trying to guess their authentication details [4, 5]. Once you get hackers within your asset, you would begin dealing with lots of troubles. The hackers are so commonly correlated with the black market and regularly deal with the organized crime groups, terrorist organizations or any other threats to our private and business safety and security. As we would suggest before, the Internet of Things marketplace is an extremely fast-growing place and if we do not take any care about its defense – we would get too many people worldwide being exposed to a risk. Some media would call a Shodan being the scariest search engine of today and we believe the similar attribute could be given to a Censys as well. These two tools illustrate a pretty powerful side in case of threat’s applications.

The fact is that there would always be people who would attempt to threaten someone’s safety and security and who would sell so confidential information about someone’s life and business. The good thing to an investigation is that these actors would always leave a trace in a cyberspace and such a case would be resolved effectively. From another point of view, it’s necessary to think about the potential consequences of successfully committed crime and their impacts to lives of possible victims. Obviously, new technology would support us in resolving any case, but the point is we should think how to prevent a crime even happens [7]. Some of the best practices would suggest us to raise awareness about all harmful effects being correlated with emerging systems. For example, it’s not that bad idea to organize some sort of education and training about all the risks being addressed to using cyber solutions. This would certainly assist us greatly in better understanding of all pluses and minuses of those technological advancements and explain to end users how they could stay assured. In case of Republic of Serbia, we would advise the Law Enforcement agencies such as a Ministry of Interior Affairs (MIA) to try to implement some of those projects into its communities.

5. THE SOCIO-ECONOMICAL IMPACTS OF THE INTERNET OF THINGS

As it’s already indicated, the IoT marketplace is a fast-growing environment with the tendency to become more than 5 times bigger during the period of 5 years. Some studies would claim that we can expect more than 25 billion devices being connected to an Internet of Things by 2020. From such a perspective, it’s getting obvious how huge the impact of these new technological advancements could be on the global population [1, 2]. Through this paper, we would discuss some security’s requirements this technology should follow in a coming future in order to remain safe to the majority of its users.

On the other hand – from an economical perspective – it’s getting clear that an IoT business deserves an attention of many financial experts and potential investors. It’s definitely a field offering great returns for a short period of time. So, if anyone would intend to invest into the IoT marketplace – there would be a big possibility that he could make a significant profit. As it’s known, Serbia is a small country with still developing economy, social values and life’s standards to its residents, but it’s a quite good idea that some of the financial resources of this country could be directed to an IT industry and specifically – to an IoT business.

Finally, we would want to recommend to Serbian authorities to cope with the international standards being correlated to a cyber defense and create some of campaigns to their communities that would teach people how to deal with the best practice in terms of computer and network security [4, 5]. Some IoT solutions would rely on mobile technologies making these sorts of improvements getting portable and easily accessible remotely. Also, there are many suitable tools offering an option of cyber tracking that would definitely threaten a safety and security of those device’s owners. At the end, we would strongly advise Serbian Defense Forces to work hard coping with these new tendencies in security and providing much safer environment to their people.
6. DISCUSSIONS

The Internet of Things may appear as one of stages in an overall Human Kind’s technological evolution. It’s a new concept only to people who are not familiar with a history of science and technology and a quite obvious step in evolution to those who got aware of any novel tendencies. For such a reason, an impact of technology to a global society could be unavoidable as well as consequences of such a trend to an international defense community. The new technologies would become an inevitable part of our lives and get similarly important to both – legal and illegal segments of society.

As it’s already discussed, we all would become dependable on emerging technologies and at least use computer with the internet connection to send an e-mail or read the news. The similar situation would be with an illegal part of community which would also rely on these technological solutions. In other words, to get the bad guys – you should think like them [1, 2, 3]. For such a reason, we would see cyber skills being so important to the Police Forces of tomorrow making them capable to resolve any criminal scenario.

7. CONCLUSION

The purpose of this article is to aware an expert’s community in Serbia about new technological tendencies and their security. Cyber defense is not only about the security of devices, equipment or solutions using the web, but rather it deals with the population’s safety and defense. In other words, all segments of the human society are closely connected to each other and these new trends require from everyone to develop a good learning curve in order to gain awareness about today’s challenges.

REFERENCES


REZIME

BEZBEDNOST INTERNETA STVARI


Ključne reči: visokotehnološka bezbednost, Internet Stvari, web, održana, tehnologija, itd