Security challenges of the Industry 4.0

Adam U Mentsiev¹,³, Elina R Guzueva¹ and Tamirlan R Magomaev²

¹ Faculty of information technology, Chechen State University, 32 Sheripov Street, Grozny, 364024, Russia
² Department of Information Systems in Economic, Institute of Digital Economics and Technological Entrepreneurship, GTSU named after Acad. M.D. Millionschikov, 100 Isaev Avenue, Grozny, 364061, Russia
³ E-mail: a.mentsiev@chesu.ru

Abstract. Industry 4.0 or the fourth industrial revolution is defined as the latest digital transformation that our manufacturing and production industry is going through during the modern day and will continue to do so for the next decade or so. But with this transformation, there are a number of challenges associated and most of these challenges are related to cybersecurity. This research is based on a gap analysis which identifies these challenges that stand in the way of Industry 4.0 revolution. These challenges related to security and privacy fall under different categories and each needs to be discussed. Some of these categories include people, processes and technologies. The paper then also provides recommendations to each of this challenge of every category. The recommendations are also based on the people they are addressed to. Before to dive into these security and privacy challenges there also considered what this fourth industrial revolution is and how is it going to change our industry.

1. Introduction

Any revolution is a result where previously existing causal relationships can no longer work according to the previous algorithm. The Fourth Industrial Revolution or Industry 4.0 is no exception. However, it should be noted that this revolution has its own specifics. So, we can safely say that the main factor of the industrial revolution is applied research, which entails the development of science in this area.

In order to understand the security and privacy challenges faced by Industry 4.0 we need to understand what this fourth industrial revolution is and what are some of its main characteristics which give rise to these challenges. Industry 4.0 as defined earlier is the digital transformation of our present manufacturing and production industry. Some of the major technologies that are at the core of industry 4.0 include Internet of Things IoT, cloud computing, cyber physical systems and finally artificial intelligence [1].

The phenomena of industry 4.0 started from a German revolution whose goal was to revolutionize the German industry and make it more competitive as compared to other countries and the term was called “Industrie 4.0”. This phenomenon soon became global and started being used interchangeably with the fourth industrial revolution. The development of this industry suggests that enterprises will switch to a new type of process management. The main task is the execution of the process. Networked machines will autonomously adjust production processes in accordance with specified parameters and do this quickly, efficiently and without errors.

Some of the major factors that characterize industry 4.0 include:
1. To make the manufacturing and production processes more automated than ever before.
2. To decrease human interaction in the manufacturing process by bridging the gap between physical and digital systems, this way humans do not have to operate physical systems and can give them command by using digital systems. These systems are called cyber-physical systems.
3. To help all the machines involved in the process connect with each other, share information and take decisions based on that data due to the internet of things,
4. To shift the control of the complete manufacturing process from a control process down to every smart machine, which takes its own decision and can be controlled locally,
5. To enhance the use closed loop data models i.e. models that improve their output based on the feedback from their previous performance, and
6. To increase the trend of personalization and/or customization of products during the manufacturing process according to the customer needs. [2,3]

Now, a basic understanding of the fourth industrial revolution and some of the factors that characterize it has developed, it will be easier to understand the reason behind the security challenges that stand in the way of industry 4.0.

2. Security Challenges of the Industry 4.0

2.1. Lack of IT/OT Security Expertise and Awareness
As identified above, this challenge is due to the people who are either involved in the manufacturing processes that are undergoing change or are involved in the security of the digital part of it. In both cases, there is a severe lack of information security expertise. People who are involved in the manufacturing process usually have no clue of what security measures need to be taken and people who are dealing with the security part of the process, do not completely understand the manufacturing process to secure it in a way that it is not vulnerable to any outside attacks.

For a person to understand the complete process, he/she needs to be qualified in a number of areas including IT and OT security, embedded systems and network security etc. and it is becoming increasing difficult to find such individuals who are qualified in all the above mentioned fields. [4]

Even if to find a good security specialist who is qualified in all these areas and fully understands your manufacturing processes as well, it is very essential that all your employees who are involved in the manufacturing process also have a thorough understanding of the security processes and they make security a priority instead of treating it as a feature. To add to all these problems, most companies that are undergoing the fourth industrial revolution have chosen to take the easier path which is the deployment of security services on top of their processes instead of training their current employees who work on manufacturing. There are a number of reasons for that which include, employees lacking the ability to understand and learn the newer security systems and the cost of trainings being extremely high. These days the number of trainings which are dedicated to cybersecurity are becoming less and less in number and more and more expensive when it comes to the cost [5].

2.2. Lack of Policies and Funds to Focus on Security
The industry that is at the forefront of the fourth industrial revolution is still to this day reluctant to focus on the need for security. This is obvious from the absence or lack of policies and organizational rules that ensure that when manufacturing a product privacy and security are given number 1 priority. No matter how much we emphasize on it, the industry just has not started to see privacy and security as an absolute need. To this day it is considered to be an add-on or a luxury feature for most operators, which brings us to our next point. [6]

For the same reason that industries and operators refuse to give security a priority over other things, they have also cut back on funds and are very reluctant to invest or spend more when it comes to R&D related to security challenges that are being faced in the present day. This poses a number of challenges as the cybersecurity technology will no longer propagate and get better as it is supposed to.
A good example of companies not spending enough money on security solutions is let’s say when a company decides to migrate its information systems on to the cloud instead of storing it locally. Now such a migration takes place when a company realizes the amount of sources that are being wasted on storing the information locally and so one of the biggest motivation behind this move is usually the finances that can be saved on migration to cloud services. So how would a company be willing to spend on cloud security if its sole reason to move its information systems on cloud were to save money [7].

2.3. Liability over Products
The next security related challenge that is being faced by the operators of Industry 4.0 is related to the second category which is processes. The challenge here that we are talking about is the liability for Industry 4.0 cybersecurity. In order to manufacture a smart product that can be connected to the internet via the internet of things (IoT), a large number of stakeholders are involved in the process. These stakeholders include everyone from the manufacturing brand, the companies that supply one of the many parts of that are being put together to manufacture that particular smart device, it includes the security teams working on the security systems installed in that smart device, the software teams that program that device and many more in the supply chain. This huge number of stakeholders end up apportioning liability issues in case a security incident involving that smart device occurs and thus can prove to be a major challenge in the implementation of Industry 4.0. [8]

2.4. Lack of Uniform Standardization
Science has grown so much over the past few centuries. Hundreds and thousands of reports, books and standards have been published that make it easy to work on these technologies but that is not the case with Industry 4.0 security. Unlike IoT or other new technologies which have complete standardization available and makes it easier for a user to follow these standards to implement their projects, Industry 4.0 security has very little or no standards presents in the market. The only standards that are being used by the current operators of Industry 4.0 are either fragmented or are not agreed upon by the research community working on Industry 4.0. [9].

2.5. Technical Constraints of the Devices
Since the Industry 4.0 is meant to be the digitalization of the already existing manufacturing processes i.e. it would not be a completely new system instead same things that were being done manually would now be done digitally. This means that digital platforms will be added onto the existing platforms, which is the only possible solution because otherwise we will have to build an entirely new industry from the ground up. So while this is an easy way to implement Industry 4.0 it has some associated challenges. Most of these devices that are already in use or that are still being manufacturing using the old techniques have some technical constraints that present a lot of security challenges.

Most of these devices have very limited operating power, so much so that they cannot even perform some very basic operations. This is done for a number of reasons and one of the biggest amongst those reason is keeping the prices steadier.

The second biggest technical constraint is that all these devices that are already in operation lack the infrastructure to support any protective mechanism of any kind. All these devices were made with one major operation in mind and no heed was paid to the protective part of these devices. Not only that, to this day a lot of new devices being made lack this basic protective infrastructure. Lastly, even if some devices do have some processing power and are capable of performing small tasks such as a fridge measuring temperature and sending it to its control unit, these devices still lack the ability to perform more advanced security such as encryption or authentication because even though these tasks may sound simple, they require a lot of processing power which these machines simply do not have [8].
3. Conclusion and recommendation

In order to ensure the successful implementation of industry 4.0 in our world, there are certain measures that need to be ensured to overcome the security challenges and move forward with the fourth industrial revolution. These recommendations include:

- People should be made more aware of the importance of security and privacy in all the modern devices and by people we mean the manufacturers and operators of industry 4.0. More and more specific trainings need to be carried out in order to prepare workers with specialized skills.
- Organizations need to focus on making policies and rules that make security the number 1 priority in manufacturing processes and they also need to allocate funds in order to ensure successful growth and upgradation of security systems.
- Operators of industry 4.0 also need to clarify the liability issues that might arise due to a security incident involving the smart devices and for that all the stakeholders need to come together and decide upon who is going to be liable for which part of the device. Uniform standards also need to be set in order to provide the operators of industry 4.0 with guidelines to follow.

Last but not least, such devices need to be manufactured that are not bound by any technical constraints that meddle with the security process. Devices should come with more computing power to perform advanced security tasks even if that means a slight bump in prices because security is more crucial than anything else.

References

[1] Prinsloo J, Sinha S and von Solms B 2019 A Review of Industry 4.0 Manufacturing Process Security Risks Applied Science 9 1-31
[2] Scoop I 2019 Industry 4.0: the fourth industrial revolution – guide to Industrie 4.0 Retrieved from https://www.i-scoop.eu/industry-4-0/
[3] Magomedov I A, Magomadov V S, Rahimov A A, Alikhadzhiev S Kh and Gudaev M-A A 2019 FMMA and FMECA for analysis of reliability of a wind turbine Journal of Physics: Conference Series 1399(5) 1-5
[4] Anderson E 2019 3 CHALLENGES OF INDUSTRY 4.0 AND HOW TO ADDRESS THEM Retrieved from https://www.forescout.com/company/blog/3-challenges-of-industry-4-0-and-how-to-address-them/
[5] Magomadov V S 2019 Deep learning and its role in smart agriculture Journal of Physics: Conference Series 1399(4) 1-5
[6] Evans J 2018 Be prepared for the security challenges of Industry 4.0. Retrieved from Orange Business Services Retrieved from https://www.orange-business.com/en/blogs/be-prepared-security-challenges-industry-40
[7] Mentsiev A U, Gerikhanov Z A and Isaev A R 2019 Automation and IoT for controlling and analysing the growth of crops in agriculture Journal of Physics: Conference Series 1399(4) 1-5
[8] Morgan J 2014 A Simple Explanation Of 'The Internet Of Things' Retrieved from http://forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#6724d4741d09
[9] Alani M M and Alloghani M 2019 Security Challenges in the Industry 4.0 Era In book: Industry 4.0 and Engineering for a Sustainable Future Publisher: Springer, Cham
[10] Balamurugan C and Satheesh R 2017 Development of Raspberry pi and IoT Based Monitoring and Controlling Devices for Agriculture Journal of Social, Technological and Environmental Science 6 207-15