Advances in Economics, Business and Management Research, volume 156
2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020)

Legal Enforcement of Cybersecurity of Wearable Mobile Devices in Healthcare

Minbaleev A.V.[1,2], Nikolskaia K.Yu.[2,*] Zhernova V.M.[2]

[1]*Kutafin Moscow State Law University (MSAL), Moscow 125993, Russian Federation*
[2]*South Ural State University, Chelyabinsk 454080, Russian Federation*
[*]*Corresponding author. Email: nikolskaya174@gmail.com*

ABSTRACT
Wearable devices are becoming popular, their sales are growing, the number of people who purchase and use them is growing. The market is filled with all kinds of wearable products.
Wearable devices are able to store and exchange user information with other electronic devices, for example, a phone, tablet, computer, etc. The huge amount of wearable devices generates a huge amount of unprotected information. Since at the moment there are no standardized algorithms for secure data transmission for these devices. The information is not protected from intruders who use security vulnerabilities in wearable devices that arose during their development.
This article explains the insecurity of wearable mobile devices. Their vulnerabilities are considered with examples. Using specific examples of hacking wearable devices makes it possible to clearly demonstrate their insecurity. Algorithms for solving problems arising during their development will also be presented. It also provides an overview of the legal mechanisms for wearable cybersecurity.
Keywords: *wearable mobile devices, DDoS attacks, cybersecurity*

1. INTRODUCTION

Wearable mobile devices are devices that you can carry and that can exchange data via bluetooth or the Internet [1]. Collectively, wearable mobile devices can be called the Internet of Things. Wearable mobile devices mean, for example, smart watches, pacemakers, fitness trackers, smart toys and much more. Wearable mobile devices can also be described as accessories. Wearable devices are becoming more and more popular at the moment, covering a large number of industries in which they are used. For example, any athlete knows about fitness bracelets or smartwatches that have the functions of a pedometer, heart rate monitor. Medicine is actively introducing sensors for taking patient readings, for example, body temperature, heart rate, respiration, sugar level, etc. [2].
Therefore, companies such as Google, Apple, Samsung, Microsoft and others are engaged in the development and implementation of wearable technologies in manufacturing, medicine, agriculture and other industries. Security is a major concern for wearable mobile devices. Although the data is protected by encryption, pin-code or user authentication mechanisms, these methods become useless when many users do not follow the manufacturer's standard recommendations. One of these recommendations is to replace the password originally set on the device. Wearable mobile devices are one of the most personalized devices. All received data refer to a specific person. For example, fitness bracelets that measure your health readings can be easily compromised, i.e. your data becomes known to an outsider. For example, the captured movement data can be useful to robbers. Information about the user's life, which he does not want to advertise, can be used by advertisers to promote their products. Any personal information can be used for personal gain. If a person uses something closely related to himself, then he should have confidence in the protection of his personal data. Everyone has the right to the inviolability of their private life. If we do not create a safe environment for wearable mobile devices soon, we will have to abandon such useful devices in our life. Another problem is the lack of legal mechanisms to ensure the cybersecurity of wearable mobile devices.

2. METHODOLOGY

A. Wearable devices and their vulnerabilities

One of the most powerful DDoS attacks in the entire history was carried out using a botnet, which consisted of IoT devices [3]. DDoS attack (Distributed Denial of Service) is a complex of actions of an intruder aimed at partial or complete disabling of an Internet resource or server [4]. DDoS attacks are aimed at disrupting the operation of one or more protocols by "bombarding" a network resource with requests. This leads to partial or complete failure of the site, application, server, etc. A two-week attack on the website of renowned cybercrime journalist Brian Krebs. It was carried out using a botnet of hacked cameras. The next large-scale DDoS attack using Mirai occurred against the American provider Dyn, which resulted in access problems for a number of popular services such as Twitter, GitHub, Soundcloud and Spotify. After some time, the source code of a malicious algorithm

called Mirai was published, which led to the emergence of new botnets based on it. Mirai exploited an obvious vulnerability in IoT devices - standard passwords that many users do not change. The system scans for available devices, tries to brute-force access, taking default passwords such as admin or 123456 as a basis. In addition, some devices had built-in accounts that are used for debugging. Users do not have access to them. Before the release of products, they are usually removed, but sometimes experts forget about it by mistake.

In the aftermath of the aforementioned incidents, governments in many countries are seriously concerned about the security of the Internet of Things. The US Secretary of Homeland Security and the Department of Homeland Security urged manufacturers to maximize the security of their devices from hacking. The US Federal Trade Commission (FTC) has filed a lawsuit against the Taiwanese company D-Link, accusing it of insufficient security of its products, as the manufacturer's devices were used by cybercriminals in botnets.

The number of IoT devices is growing every day. As a result, the number of large-scale DDoS attacks carried out using these devices will also grow.

2.1 Smart watch

Smart watches are a wonderful invention of humanity. With them, you can track the location of children, make emergency calls, measure the distance traveled and much more. However, with the growing demand for these devices, the interest in them from intruders has also increased.

The Norwegian Consumer Council has published a report highlighting safety concerns for children who use smartwatches. This report was published ahead of the publication of the decision of the Federal Network Agency of Germany to ban the sale of smart watches. The agency said that gadgets with a built-in tracking function violate applicable law. Together with a security firm, the Norwegian Consumer Council analyzed four smartwatch firms available online and in Norwegian stores, called Gator 2, Tinitell, Viksfjord, and Xplora. The technical testing of the chaos was carried out by the information security company Mnemonic. Testing found serious security flaws in three of the four devices tested. The company found, for example, that the two devices have flaws that could allow a potential intruder to take control of applications. Thus, having gained access to data on the location of children in real time, their historical location, and personal data, as well as even give them the opportunity to contact children directly, without the knowledge of the parents. One of the watches also functioned as a listening device, allowing a parent or stranger with some technical knowledge to observe the child's surroundings without any clear indication on the watch. Two of the watches had additional vulnerabilities for so-called location spoofing. This means they could allow an intruder to manipulate the location data sent from the watch to the app on the parent's phone. Consequently, an intruder could create the impression that the watch is not at its actual location.

Under the guidance of Professor Romit Roy Choudhury, students from the Department of Electrical and Computer Engineering at the University of Illinois have developed an app called Motion Leaks through Smartwatch Sensors (MoLe). The app uses the clock accelerometer and gyroscope to build a virtual 2D map of the keyboard. The program measures the time between each press and the offset vector of the brush, based on which it assumes which key is pressed. It disguises itself as some kind of standard pedometer to gain access to all the necessary sensors, accelerometer and gyroscope. Thus, the development team clearly demonstrated the danger of using such devices: intruders can steal passwords and other data by creating such an application.

Copenhagen University student Tony Beltramelli presented his master's thesis entitled "Deep-Spying: Spying using Smartwatch and Deep Learning". In it, he introduced a new attack method that allows intruders to extract sensitive information, such as credit card numbers, or access a telephone PIN from motion sensors in wearable devices. The thesis is based on the MoLe application described above. The student used a machine learning algorithm called "Recurrent Neural Network - Long Short-Term Memory". The data is first transmitted to the smartphone connected to the watch via Bluetooth, and the latter already sends it to a remote server for processing.

B. Fitness bracelets

Fitness bracelets have become an integral part of modern life. With their help, you can monitor various functions of the body. For example, the saturation of the body with oxygen, the number of steps taken, pulse, pressure. On the one hand, this kind of data can hardly be called purely medical, but on the other hand, it can be used for personal gain. Also, fitness bracelets are often targeted by intruders to organize a bot-no. With the help of which it will then be possible to conduct a DDoS attack.

In the article "How I hacked my fitness bracelet" Roman Unuchek talks about the vulnerabilities of the fitness bracelet, which he discovered during the experiment. The author decided to conduct a series of experiments after his Android Wear App was randomly synchronized with someone else's fitness bracelet. The user of the fitness bracelet did not even notice that they were connected to his device. To transfer information from a fitness bracelet to a phone, in most cases, they use Bluetooth LE technology (also known as Bluetooth Smart). The researcher made his own application that automatically searched for Bluetooth LE devices, tried to connect to them, and get their list of services. To receive data, you need not only connection, but also authentication. In six hours of scanning, the researcher was able to connect to 54 devices. Despite the fact that the devices are already connected to smartphones and it is assumed that it is impossible to establish a connection with an already connected device, in fact, it is possible to block the communication between the previously paired bracelet and the official application and connect. When the authentication process starts, the fitness bracelet vibrates and waits for a button press in order to force it to

authenticate, you can restart the process many times until the user presses the button. Or until it moves back to more than 6 meters - the real maximum distance for connections in most cases. After the authentication is completed, the data becomes available for removal and commands such as changing the date and time can be easily executed on the device. The article notes that in some cases it is possible to connect to a fitness bracelet easily and without the user's knowledge. The possibility of using Trojan-Ransom on wearable devices is also noted. An intruder can take control of your bracelet and make it vibrate constantly. And to turn off vibration demand money.

C. Pacemakers

A free group of researchers from the Catholic University of Leuven, the University of Birmingham, and Gasthuisberg University Hospital presented a paper "On the (in) security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them". The team examined 10 different pacemakers and cardiac defibrillators and found that such devices can be compromised remotely, as well as harm the wearer. The researchers conducted black box testing. This means that before the start of the tests they did not know anything about the internal structure of the devices and they were not studied beforehand. This method allows simulating novice intruders who have no initial knowledge of the system specification. In the report, the researchers say that they managed to significantly increase the rate of battery discharge of devices, steal personal data of patients that are stored by pacemakers, and also transmit arbitrary commands to modern implantable cardiac defibrillators. Implantable cardiac defibrillators can not only send electrical signals to the patient's heart to regulate its activity, but also in the event of an emergency, have the ability to transmit stronger electrical signals. The authors note that an intruder can transmit a command to create a strong electrical pulse, which can be fatal. An intruder is only five meters away from the device to launch an attack. The authors also argue that an intruder does not have to approach the patient personally; it is enough to install beacons in advance in strategic places where he often happens (for example, in a hospital or at a public transport stop).

Researchers of the MedSec startup and representatives of the investment firm Muddy Waters Capital have presented a joint analytical report. The report describes the vulnerabilities of St. Jude Medical. The researchers said that a remote attack on cardiac equipment is possible from a distance of fifteen meters. Representatives of St. Jude Medical reported that this claim is false, as the device can only be accessed from a distance of no more than two meters. They also denied other accusations and called them a lie. However, no third party expertise was provided. Expertise for checking security against attacks is currently not spelled out anywhere in technical regulations. Ultimately, the Food and Drug Administration (FDA) became interested in the situation. Independent researchers have confirmed the findings of the MedSec researchers. They discovered vulnerabilities in the manufacturer's medical equipment. The Industrial Control Cyber Emergency Response Team (ICS-CERT) in the United States mentions three vulnerabilities in Abbott Laboratories pacemakers (Abbott Laboratories at the time acquired St. Jude Medical) manufactured before August 2017. The most dangerous of the three vulnerabilities (CVE-2017-12712) relates to the authentication algorithm in the pacemaker: the authentication key and timestamp can be compromised or tampered. This allows an intruder to send unauthorized commands to the pacemaker over the radio channel. The second vulnerability (CVE-2017-12714) could significantly reduce the battery life of a pacemaker. Pacemakers do not limit the number of commands that can be received. This allows an intruder to re-send commands, which will reduce the battery life of the pacemaker. St. Jude Medical updated its devices for the first time due to premature battery drain, a result of vulnerabilities that prematurely drained pacemaker batteries when two people died in Europe. The third vulnerability (CVE-2017-12716) was that when information is transmitted to home monitoring systems, unencrypted information about the patient is transmitted through the radio channel. In addition, the information was stored unencrypted in the memory of the pacemakers themselves. As a result, the FDA recalled 465,000 pacemakers related to MedSec's research.

D. Neuroimplants

At the moment, the most common type of implants are those with a brain stimulation system (DBS) [5]. These implants consist of implanted electrodes that are placed in the brain. The electrodes are linked by wires that run under the skin. The wires carry signals from the implanted stimulator. The stimulator consists of a battery, a small processor, and a wireless antenna. The antenna allows doctors to program the stimulator. The principle of operation is the same as that of a pacemaker, the only difference is that it interacts directly with the brain. DBS targets different areas of the brain. It is a tool for treating a huge range of diseases. However, there is a risk that the wireless control of such devices may be subject to cyber attacks [6]. An example of a cyberattack is changing the stimulation settings, which will immobilize patients with Parkenson's disease. These kinds of hacks are quite difficult to carry out, as they require a high level of technological competence, however, they are quite feasible. The article Securing Wireless Neurostimulators analyzed the safety of wireless brain implants [7]. These implants are used to relieve the symptoms of diseases such as Parkinson's syndrome, diabetes, cancer, etc. The researchers conducted a safety analysis using reverse engineering. They interfered with the communication between the implant and its controller. As a result, it became known that the transmitted data is not encrypted and not authenticated. A number of radio-controlled attacks have been carried out to compromise the safety and privacy of patients. The article proposed a security architecture for secure communication between the controller and the implant. The architecture is based on the use of the patient's physiological signal to generate a

symmetrical key in the neurostimulator. The generated key is transmitted through the patient's body - the controller can read the electrical signals of the neuroimplant through touch. Data exchange takes place through a secret channel with data compression. In the article, the authors proved the safety of the architecture used. Neuroimplants are gaining popularity. When they are officially approved for streaming patient care, the risk of cyberattacks on them will increase. Therefore, before introducing such technologies into mass operation, it is necessary to ensure technical security and create mechanisms for legal regulation and responsibility for cybercrimes using neuroimplants.

3. OVERVIEW OF LEGAL METHODS TO ENSURE MOBILE WEARABLE DEVICE CYBERSECURITY IN HEALTHCARE

By collecting data with the help of gadgets, manufacturers of wearable mobile devices can access personal information and health information of users, analyze data, and sell analytics results, while getting more profit [8]. And all of this is legal, as most privacy policies are vague. For example, such a function as API provides third-party integration for data access [9]. One of the reasons for the existence of ambiguous privacy policies is that there are currently no regulations and laws that would protect customer privacy and restrict the use of personal information by wearable mobile devices. However, some countries are seeking to establish regulatory mechanisms for these types of devices. For example, in Australia they are working on the creation of such legislation. The Australian Privacy Principles (APP) under the Privacy Act govern the processing of personal information by Australian government agencies and certain private sector entities. [10] This document states that an organization that is subject to the action of APP, when collecting personal information from users for a specific purpose, should not use this data for other purposes without the consent of the client or in certain exceptional situations. These are the first steps towards creating effective principles to restrict data trade [11]. The privacy law only applies to private companies and government agencies in Australia with an annual turnover of A$ 3 million or more. [12] Thus, small, private organizations may still use personal information for other purposes. Due to limited enforcement capabilities, Australian agencies can only take action against manufacturers and service providers physically located in Australia. Since most of the world's most renowned wearable device manufacturers are headquartered in the United States, they are not required to comply with this document. Manufacturers of wearable mobile devices may store personal information, including health data from users around the world, and must comply with US regulations only. With regard to health information in the United States, the Health Insurance Portability and Accountability Act 1996 (HIPAA) governs the legitimate use and adequate protection of healthcare organizations. However, as in Australia, the emergence of manufacturers of wearable devices is not clearly classified [13]. This means that manufacturers of wearable mobile devices can store and process personal and health information of users and are not subject to regulations. This puts users at high risk of data privacy breaches.

In 2009 in China, an article was introduced into the Criminal Code. It is called selling or illegally providing citizens' personal information. This article governs the collection, processing, and storage of confidential information that has been collected from any technical device. However, the maximum liability is 3 years in prison.

After analyzing the regulations of various countries, we can conclude that so far no one understands how to regulate the relationship associated with confidential data created by wearable mobile devices. In a number of countries, individual attempts are being made to introduce articles into already existing laws on the protection of confidential data. However, there are a number of problems. One of them is associated with the lack of international technical regulations for the development of such devices. Such regulations must be adopted at the international level. This will create competitive products that are standardized and can be used everywhere. For example, when shipping pacemakers to different countries, there must be confidence in their protection protocols.

4. DISCUSSION OF RESULTS

From the results of this study, a number of conclusions can be drawn to determine the most common.

- At the moment, all current regulations cannot effectively limit and regulate the processing of personal health information by manufacturers of wearable mobile medical devices.
- It is necessary to supplement regulatory legal acts and legislative acts to standardize methods for collecting, storing and processing personal medical data. Wearable mobile medical device companies should be clearly categorized and regulated in accordance with each country's privacy policy.
- The collection of data should only be carried out with the consent of the users. Since medical information is one of the most critical categories of personal data in any country.
- Companies should develop clear and understandable privacy rules. These rules must be communicated to the user. The rules must clearly indicate how personal data will be collected, stored and for what purpose they will be processed.
- Regulations and laws always play a passive role in relation to emerging technologies and lag far behind them. This happens because it is very difficult to predict the modification of certain technologies or their appearance in general. However, it is necessary to close the gap between them as much as possible. This is possible if government agencies actively cooperate with manufacturing companies.

- There is a need to strengthen cooperation between government and manufacturers of wearable mobile medical devices. This collaboration is essential as it prioritizes customer needs and defines clear policies that can be easily adapted as technology advances.

5. CONCLUSIONS

The market for wearable mobile medical devices is growing rapidly. The data privacy issue is the main issue at the moment. The privacy issue is becoming a major obstacle to the mass adoption of wearable mobile medical technologies for users. This is because users' awareness of data privacy is increasing. The realization that such devices can pose a threat to data confidentiality will over time become an obstacle to the development of the market in this area. The privacy issue associated with wearable mobile medical devices requires careful consideration and regulation by various parties. While wearable mobile devices provide undeniable benefits to users of such devices, privacy protection should not be compromised. The user needs a guarantee that their data will be reliably protected and have not been transferred or disclosed. Manufacturers of wearable mobile medical devices need to take all possible steps to protect user privacy. On the part of the legislature, there is a need to expedite the process of creating regulations to regulate the use of wearable mobile medical devices for both personal and business purposes, in order to eliminate the risks of privacy breaches in the framework of regulatory compliance.

ACKNOWLEDGMENT

The reported study was funded by Grants Council of the President of the Russian Federation according to the research project No. MD-2209.2020.6.

REFERENCES

[1] K. W. Ching, M. (Mandy) Mahinderjit Singh, Wearable Technology Devices Security and Privacy Vulnerability Analysis, International Journal of Network Security & Its Applications, 8(3) (2016) 19-30. DOI: 10.5121/ijnsa.2016.8302

[2] J. M. Franklin, G. Howell, S. Ledgerwood, J. L. Griffith, Security Analysis of First Responder Mobile and Wearable Devices. DOI: 10.6028/NIST.IR.8196

[3] A. Boyko, V. Varkentin, T. Polyakova, Advantages and Disadvantages of the Data Collection's Method Using SNMP, Proceedings of the International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 2019, Vladivostok, Russia. DOI: 10.1109/FarEastCon.2019.8934069

[4] E. Nazarenko, V. Varkentin, T. Polyakova, Features of Application of Machine Learning Methods for Classification of Network Traffic (Features, Advantages, Disadvantages), Proceedings of the International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 2019, Vladivostok, Russia. DOI: 10.1109/FarEastCon.2019.8934236

[5] N.E. Oueslati, H. Mrabet, A. Jemai, A. Alhomoud, Comparative Study of the Common Cyber physical Attacks in Industry 4.0. In Proceedings of the 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), Tunis, Tunisia, 20–22 December 2019; pp. 1–7.

[6] M. Hammoudeh, G. Epiphaniou, S. Belguith, D. Unal, B. Adebisi, T. Baker, A. Kayes, P. Watters, A service-oriented approach for sensing in the Internet of Things: Intelligent transportation systems and privacy use cases. IEEE Sens. J. 2020.

[7] E. Marin, D. Singelée, B. Yang, V. Volski, Guy A. E. Vandenbosch, B. Nuttin, B, Preneel, Securing Wireless Neurostimulators, CODASPY '18, March 19–21, 2018, Tempe, AZ, USA.

[8] A. Seeam, O. S. Ogbeh, Xavier J.A. Bellekens, Sh.P. Guness, Threat Modeling and Security Issues for the Internet of Things, IEEE Nextcomp, 2019, At: Mauritius. DOI 10.1109/NEXTCOMP.2019.8883642.

[9] H. Mrabet, S. Belguith, A. Alhomoud, A. Jemai, A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. Sensors 2020, 20(13), 3625. DOI: 10.3390/s20133625.

[10] Office of the Australian Information Commissioner: Privacy fact sheet 17: Australian Privacy Principles (2014), Electronic resource.

[11] 11. A. Daly, The Law and Ethics of 'Self Quantified' Health Information: An Australian Perspective. Int. Data Priv. Law (2015).

[12] Federal Register of Legislation, Australian Government: Privacy act 1988 (2015).

[13] K.H. Bromberg, D.A. Cranston, Wearable technology: taking privacy issues to heart. New York Law J. (2015).