Швецов Александр Сергеевич
Тюменский Государственный Университет
Кафедра информационной безопасности
Студент группы КБ167
alexander.vosb@gmail.com
Шутова Елена Юрьевна
Тюменский государственный университет
Кафедра иностранных языков и международных коммуникаций
Старший преподаватель
eushutova@mail.ru

БЕЗОПАСНОСТЬ И ИНТЕРНЕТ ВЕЩЕЙ

Shvetsov Alexandr Sergeevich
University of Tyumen
Department of Informational Security
Student of CS167
alexander.vosb@gmail.com
Shutova Elena Yurevna
University of Tyumen
Department of Foreign Languages and Intercultural Communication
Senior lecturer
eushutova@mail.ru

SECURITY AND THE INTERNET OF THINGS

АННОТАЦИЯ. *В статье «Безопасность и Интернет Вещей» Брюса Шнайера затрагивается проблема как отдельно безопасности Интернета Вещей, так и безопасности в целом. Автор описывает риски, связанные с использованием устаревших устройств, их уязвимостями, рыночные и политические проблемы, имеющие прямое отношение к технологической сфере, возможной необходимости обращения вспять тенденции подключения всего к*

интернету, а также размышляет о государственном регулировании как о единственном решении этих проблем.

***КЛЮЧЕВЫЕ СЛОВА**: Интернет Вещей, безопасность, робот мирового масштаба, государственное регулирование, регулирующие органы, распределенные системы.*

***ABSTRACT.** The article «Security and the Internet of Things» of Bruce Schneier touches the problems of IoT security and security on the whole. The author describes perils of using old devices, their vulnerabilities, market and political problems related to technology, the need of reversing trend of connecting everything to the Internet, and government regulation as the only solution to these problems.*

***KEYWORDS**: Internet of Things, security, world-size robot, government regulation, regulatory agencies, distributed systems.*

Over the last few years, Internet of Things has become a hugely discussed topic in the IT sphere. Hundreds of headlines have been captured by IoT over the whole world. Newspapers and magazines strive to tell us how great sensor-embedded devices are with their ability to communicate with each other allowing us to simplify our day-to-day affairs, save our money, health and even other people's lives. Internet of Things has already been applied in business, healthcare, city managing and other fields of life.

We're always in contact with our relatives, friends, colleagues, even if we are far away. Undoubtedly, that connection provides us huge benefits, and most of us can't even imagine their lives without it. However, using connected devices makes us vulnerable to hackers. Rubbing their hands and having their eyes gleaming with malice they search for holes in systems to still other people's personal and sometimes even vital information, say nothing about organizations.

Experts are saying that attacks using Internet of Things has bounced up 280% because hackers become shrewder and savvier.

According to Bruce Schneier, an American cryptographer and computer security specialist, Internet of Things is considered in three parts: sensors, "smarts" and actuators. The sensors collect data about us and include devices such as smartphones,

smart thermostats, street sensors, etc. The actuators affect the environment. Finally, the «smarts» are devices needed to process data, for example, computer processors on the devices and the memory to store the data. All those parts bring to mind the idea of a world-size robot, a mighty and uncontrollable (in a manner) network monster, with its arms embracing the whole planet. The robot is distributed what means it does not have a metal body like those ones ordinary robots have and, moreover, built unintentionally out of the routine objects. It becomes stronger and smarter over the years, so it would be really bad, if someone began to threaten its safety.

Unfortunately, that's happening right now. Threats come in various forms and hackers' manipulations range from stealing personal information to accessing potentially dangerous devices like automobile with cruise-control system. No wonder some of the attacks can lead to mass deaths.

Good for us, such companies like Microsoft, Apple and Google spend a lot of time correcting their code before releasing it. These companies are rich and can afford large professional teams of developers. That's why their devices and software are well secured. But what about small companies? Most of the non-popular companies produce poor secured devices because of the lack of expertise. Besides, such companies sell their products at low prices what means the unsecured devices are all over the planet and many users could become the target of a regular attack.

Bruce Schneier also pays attention to the growing number of connected things. The more devices are in the world network, the more vulnerabilities are born. A vulnerability on one device may cause security holes on the second one which also could threaten the security of the third connected device, and such chains sometimes are really long.

You could ask: "What prevents people from making existing devices more secured?". Actually, there're many problems and one of them is the law. The Digital Millennium Copyright Act (DMCA) has no real power most of the time in respect of piracy and at the same time prohibit editing programs written by their developers excluding the possibility to find and fix errors and vulnerabilities. Besides, as Bruce

Schneier states, some vendors don't even try to secure their products and issue them because "no one will notice", and the DMCA just holds a candle to the devil.

Computer security have largely been left to the market, but it cannot solve all the problems of security. The motivation of markets is profit, they aren't able to handle collective-action problems and deal with economic externalities. So, the opposition to the corporate power is highly needed.

Bruce Schneier believes that technology should get along with policy and accentuate the importance of this cooperation. However, he warns that that will lead to significant government regulation.

With this, he proposes a new government regulatory agency which will combine all the departments, each controlling specific area, for example, National Highway Traffic Safety Administration, Federal Communications Commission, etc. He underlines the problem that each department have different approach and rules and works on its own what prevents proper internet regulation and complicates future development as a whole.

Another interesting fact is worth mentioning: in the world where people try to connect everything to each other, tendency to decentralization is preferable. The main reason of this is that everything is collecting data about us. It makes people really mad. Of course, internet structure rearrangement will be needed but it is not impossible. Another problem is government's aspiration for informational security of a country and keeping information about every citizen to provide safety of society. The goal is praiseworthy but using these methods is disregard of people's liberty.

Approaching the conclusion, Bruce Schneier states that more public-interest technologists are needed. Getting security of IoT right depends on both political and technological sides. But what's more important is having experts in each side working on both.

REFERENCES

1. BRUCE SCHNEIER. Security and the Internet of Things. Available from: https://www.schneier.com/blog/archives/2017/02/security_and_th.html

2. HARALD BAUER, ONDREJ BURKACKY, CHRISTIAN KNOCHENHAUER. Security in the Internet of Things. Available from: https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things

3. Bruce Schneier. Available at: https://en.wikipedia.org/wiki/Bruce_Schneier