МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний технологічний університет
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

21-22 квітня 2022 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 21-22 квітня 2022 р**.** - Одеса, Видавництво ОНТУ, 2022 р. – 251 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова - д.т.н., проф., **Єгоров Б.В.**, ректор ОНТУ

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНТУ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНТУ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м.Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц., Київський національний університет імені Тараса Шевченка

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНТУ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНТУ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНТУ,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ “Львівська політехніка”,
Жуков І.А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською та англійською мовами.
Редактор збірника Котлик С.В.

Розділ 2.
Управління, обробка та захист інформації

UDC 004.056:[004.056:355.451]

OVERVIE OF MODERN CYBER RISKS OF IOT TECHNOLOGIES

KULIA YULIIA (yuliia.kulia@nure.ua),
Kharkiv National University of Radio Electronics

This work is devoted to assessing current cyber risks of the IoT (Internet of Things) and best practices for protection against them. The use of IoT devices in botnets is considered.

There are millions of "smart" Internet-connected devices that make up IoT, from mobile phones to computers, home thermostats, CCTV cameras and coffee makers.

The Internet of Things has both advantages and disadvantages. To begin with, IoT devices often do not have built-in legacy security features that prevent hackers from accessing them. In addition to the privacy and security concerns that arise from these security vulnerabilities, the greater danger is that these devices may be used by hackers to create a botnet that is a network of malware-infected devices without the user's knowledge.

There are a number of cyber risks in the world of IoT devices [1]. Some of the major cyber threats to the IoT currently include the following risks:

1. lack of regular updates and weak update mechanisms;
2. weak password protection;
3. unprotected interfaces. Interface vulnerabilities allow hackers to hack IoT devices and then infiltrate users' LANs;
4. malware. After infecting IoT devices with malicious software, they can be used in DDoS (Distributed Denial of Service) attacks [2], the use of such devices is a modern trend in the formation of botnets. Such attacks are, for example, SYN (Syncronized) flood or UDP (User Datagram Protocol) flood;
5. unencrypted data. Lack of encryption can allow threat takers to intercept packets from a network of devices through middle-aged attacks or other methods of interfering with the network and gaining access to sensitive data. Uncrypted data and networks are a pressing issue that is causing catastrophic company breaches.

Among the best practices of protection against attacks on IoT can be identified several [3].

1. Change the default router settings. Most people forget to rename the router and leave the name by default. This can compromise the security of private Wi-Fi (Wireless Fidelity). It is recommended that you change a name that does not contain personal information. Wi-Fi is the first line of defense that needs to be protected from hackers, as many IoT devices are connected to it.
2. Disconnect IoT devices when they are not needed. You should know all the necessary functions of the IoT device. Most modern devices can connect to the Internet, such as refrigerators and TVs. However, this does not mean that you need to connect them to the Internet. It is recommended to get acquainted with the functions of the devices and find out exactly which device requires an Internet connection to work.
3. Choosing a strong password. For reliable protection, the principle of "three out of four" should be used, ie use at least three parameters - three out of four in the password - uppercase and lowercase letters, numbers, special characters.
4. Avoid using Universal Plug and Play. Although Universal Plug and Play (UPnP) has its uses, it can make printers, routers, cameras, and IoT devices vulnerable to cyber attacks. The principle of UPnP development is to make it easier to connect devices to the network without additional configuration and help them automatically detect each other. However, this is more beneficial to

hackers than users, as they can detect all IoT devices outside the local network. Therefore, it is better to completely disable UPnP.

5. Constant updating of firmware and installed software. Updating your device's IoT software ensures that your device has the most up-to-date security settings. In addition, it helps the system eliminate security flaws in older versions of software.

Despite the risks, it is unlikely that IoT will cease to spread in homes, offices, etc. Because of this, hackers will not go anywhere. Therefore, the most important thing is to remember the safety of your devices. Understanding their vulnerabilities and using the right protection tools is necessary to counter threats in the changing world of IoT.

Referens

1. Cyber Threats Haunting IoT Devices in 2021 [Online]. Available: https://securityboulevard.com/2021/09/cyber-threats-haunting-iot-devices-in-2021/.

2. Reo J. DDoS Hackers Using IoT Devices to Launch Attacks [Online]. Available: https://www.corero.com/blog/ddos-hackers-using-iot-devices-to-launch-attacks/.

3. Swamini K. How to secure IoT devices and protect them from cyber attacks [Online]. Available: https://internetofthingsagenda.techtarget.com/post/How-to-secure-IoT devices-and-protect-them-from-cyber-attacks.

UDC 004.491.22

TYPES OF INTERNET FRAUD

MELNIK M.V., KIM YE.R. (e.kim@turan-edu.kz)
Turan University, Kazakhstan

In the modern world, in connection with the development of mobile and Internet communications, new “social” relations have been built. Every day, more and more people prefer to buy goods or services online. Thanks to online shopping, people save a lot of time, since there is no need to go for the goods, there is a home delivery function. With non-cash payment, bonuses are accrued, which can later be used to purchase a particular product. But with the development of the World Wide Web, there are such unpleasant phenomena as fraud in its various forms.

Scams on the Internet have grown in scope, going beyond the banal mailing list. There are scammers in almost all spheres of human activity. With the advent and development of the worldwide network, their activities have acquired new forms of fraud.

Fake online stores, various charitable fundraisers, phishing, viral content are some of the most popular methods of online deception.

Since purchases through online stores are in great demand, scammers create fake pages on social networks, under the guise of one-day shops. After making a certain number of purchases, these stores disappear, or the purchased goods are radically different from those declared.

Today, phishing attacks are still relevant. Proof of this is the statistics of Kaspersky Lab. In 2019, there were 492,432,555 activations of the Anti-Phishing system by Kaspersky Lab users when they tried to navigate to phishing sites. This is 245,626,777 attempts more than in 2018. In general, 19.34% of computer users of Kaspersky Lab were attacked [1].

Phishing attacks have new targets. During the period 2018-2019, 142 phishing attacks were registered against universities in 17 countries around the world. Of these, more than half of higher education institutions are located in the US - 83, in the UK - 24, and 9 each in Canada and Australia. Fraudsters mainly stole a large number of important documents, including a study in the field of nuclear energy.

For seven months of 2020, 11 thousand cyber attacks were recorded in Kazakhstan. This is 23.4% less than in the same period last year (14.4 thousand). It should be noted that this decrease is

XXII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

21-22 квітня 2022 р

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.