ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2024, № 1 (25)

COMPUTER SCIENCE AND CYBERSECURITY, 2024, Iss. 1 (25)

DOI: https://doi.org/10.26565/2519-2310-2024-1-03
УДК 004.056.5

SECURITY IN THE ERA OF WIRELESS INNOVATIONS: ANALYSIS OF POTENTIAL THREATS AND PROTECTIVE MEASURES

Yevheniia Matvieieva[1], bachelor's student at the Faculty of Computer Science,
e-mail: belka.j.0507@gmail.com, ORCID: https://orcid.org/0000-0001-8801-2185
Maryna Yesina[1,2], candidate of Technical Sciences, Associate Professor,
e-mail: m.v.yesina@karazin.ua, ORCID: https://orcid.org/0000-0002-1252-7606
Oleksandr Shumov[2], technical director of JSC «IIT», e-mail: alex.shumoff@gmail.com
[1]*V. N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv, 61022, Ukraine*
[2]*JSC «IIT», Kolomenska Street, 15, Kharkiv, 61166, Ukraine*
Manuscript was received April 2, 2024; Received after review May 2, 2024; Accepted June 3, 2024

Abstract: In today's interconnected world, wireless data transmission technologies have seamlessly integrated into the fabric of modern business operations. As reliance on these technologies grows, so does the imperative to ensure robust cyber security measures. Particularly in the age of wireless innovations, exemplified by the proliferation of the Internet of Things (IoT), the discourse surrounding the security of wireless technologies underscores the necessity of comprehending both established threats and the continuous emergence of new vulnerabilities. This underscores the urgent need for timely detection and mitigation strategies. While the convenience afforded by wireless data transmission technologies grants society unprecedented access to information and facilitates the management of diverse devices, processes, and systems, it also exposes users and modern information and communication systems (ICS) to significant cyber threats and vulnerabilities. Consequently, there arises a pressing need to address these challenges comprehensively. This research dissects contemporary methodologies aimed at restricting access to wireless networks, identifying potential vulnerabilities, and crafting effective responses to cyberattacks. It delves into various facets of cyber security, including data encryption, user authentication mechanisms, traffic monitoring protocols, and anomaly detection algorithms. Furthermore, it delves into the crucial aspect of educating personnel on wireless security practices, equipping them with threat awareness and incident response capabilities. Given the dynamic landscape of cybersecurity technologies and threats, this work seeks to establish a foundational understanding of the security landscape within wireless networks. By doing so, it aims to outline pragmatic strategies for effectively managing security risks, thereby fortifying the resilience of modern organizations and safeguarding critical information assets.

Keywords: *wireless technology, information security, Internet of Things (IoT), vulnerabilities, authentication, quantum cryptography*

In cites: Matvieieva Y., Yesina M., Shumov O. (2024). Security in the era of wireless innovations: analysis of potential threats and protective measures. *Computer Science and Cybersecurity.* 1(25): 35–41. https://doi.org/10.26565/2519-2310-2024-1-03

1. Introduction

One of the most widespread impacts of wireless technologies (*data transfer networks*) is a combination of factors, which are connected to the "weak" strength of the password and/or lack of reliable mechanisms of authentication and authorization. This may lead to unauthorized access to the network and/or confidential data. Some wireless devices use standard passwords or information exchange protocols that contain vulnerabilities caused by "weak" security/ It makes it difficult to ensure the required level of security of existing informational resources. It creates a conditional path for attackers to gain access to the configuration options of the affected network equipment and/or gain access to sensitive information circulating through the compromised device [1].

The presence of vulnerabilities in network protocols of wireless technologies, such as *Wi-Fi* or *Bluetooth*, is also a serious challenge. Unencrypted or poorly secured networks can be easily attacked. As a result, attackers will be allowed to intercept data and/or inject their software.

Security vulnerabilities in wireless networks put both business and personal interests at risk. Effective protection of wireless protection requires awareness of potential threats and the use of up-to-date measures to prevent possible attacks or data leakage. In a business environment, unauthorized access to confidential information may lead to leakage of valuable data, disclosure of commercial secrets, financial losses, or loss of customer trust [6]. Relevant threats may include attacks on remote access systems, attacks on connected IoT devices, etc. [4].

2. Challenges and Opportunities in Wireless Security

Based on the analysis of the latest trends in the development of IT technologies and summarizing the results of known security incidents, it is possible to identify several key challenges and new opportunities that are worth paying attention to:

1. Constant growth in the number of connected wireless devices: integration into average life IoT, increases the number of devices, which creates new attack vectors and increases IS threats.

2. Expansion of the used frequency band: the introduction of new IT technologies determines the need for a greater width of the frequency band, while at the same time complicating the principles of formation of the used signal-code structures and methods of compression of data transmission channels. The combination of these factors creates prerequisites for the emergence of new security challenges in the field of administration of existing channel resources and protection of information circulating (*stored*) in the respective networks [2].

3. Integration of wireless solutions into the information infrastructure of modern cities. This field of activity has a very high pace of implementation, and this may become the main prerequisite for the spread of cyberattacks, which require new, specific (*simplicity, expansion, decentralization of management, low-resource, etc.*) security measures [3].

4. Development of innovative cyber protection technologies. The emergence of new technologies and their mutual integration (*for example, bio- and information technologies*), provides opportunities for creating more effective, multi-level cluster systems for monitoring and protecting information resources and network environments (*for example, blockchain with elements of virtual/augmented reality (VR/AR) or the synthesis of both units and group emulation of their network behavior within created bot farms, etc.*) [8].

Data protection when implementing wireless technologies requires a comprehensive approach. The main protection strategies should include a wide range of technical and organizational measures. These measures, combined with proper access management, ongoing monitoring of current processes, and staff training, are the basic components of a successful wireless security strategy. In this context, it should be noted that with the widespread use of wireless technologies in finance, especially mobile banking [7], the issue of wireless communication security is becoming increasingly relevant.

3. Enhancing Security Measures in Wireless Technology

Network security measures include the use of encryption to protect data transmission over wireless networks, the implementation of appropriate security protocols (*for example, WPA3 in Wi-Fi networks*), and the control and monitoring of network traffic to detect anomalies or possible threats. Along with this, timely software updates, installation of security patches, and use of virtual private networks to protect data transmission are important aspects of network security in a wireless environment [11].

It should be emphasized that the use of wireless networks significantly increases the risk of access to personal (private) information. In this case, the use of data encryption on devices and during information transmission via wireless networks is also an integral part of personal data protection [10]. Encryption ensures the confidentiality and integrity of information when it is transmitted over networks. In addition, an additional step in the preservation of personal data is to limit access to sensitive information. In this sense, users should carefully monitor and control who and under what conditions they provide access to their private data.

From the point of view of further prospects for ensuring security in wireless technologies, the following areas should be highlighted:

1. Quantum cryptography. This direction can significantly change encryption methods (protocols) and provide proportional protection against quantum computers and new algorithms for relevant cyber-attacks [5].

2. Integration of artificial intelligence and machine learning (*AI/LM*) capabilities. The use of AI/LM capabilities to detect network anomalies (*including network behavior anomalies* [12, 13]) in wireless networks and user behavior analysis will allow prompt response to potential threats and/or minimize the consequences of their implementation.

3. Biometric methods of authentication. The simultaneous use of various biometric features (fingerprints, face recognition, retina, etc.) can become a standard for secure access to data devices and important/critical IC control functions).

4. Management of security incidents. The development and implementation of centralized monitoring systems (including based on the broad involvement of AI, ML, AR capabilities, etc.) and rapid response to security incidents [9] should provide opportunities for early detection of IS threats and effective countermeasures against new types of cyber-attacks.

5. Synthesis of new and modification of already existing security protocols, as well as the emergence of new types of electronic services and methods of interaction (*VR, AR, AI, etc.*) of users, both among themselves and when requesting/requesting the necessary information resources.

6. Gradual growth of end-user competencies. Training and increasing the level of competencies in IS issues among ordinary users should become the main component of basic security skills, helping to avoid social engineering attacks and phishing [14, 15].

In general, these directions of development in the field of wireless technologies are most likely to determine the future level of security in the world of wireless solutions, providing more effective and reliable tools and technologies for the protection of information and the functioning of the networks themselves.

Ensuring a high level of security in wireless technologies is an important factor in supporting digital transformation in various sectors of modern society. Security in wireless technology not only protects data and networks, but also influences innovation, and the development of new industries, and drives technological progress, making this aspect critical to today's digital world.

Conclusions

1. Ensuring a high level of IS of wireless technologies not only guarantees the protection of information and related networks. On the other hand, this also has a crucial importance for stimulating innovation and the development of new industries. This data protection activity is essential to the further development of various innovations where wireless technologies become an integral aspect of our daily lives.

2. The security of wireless technologies requires a combination of technical and organizational strategies to effectively prevent possible attacks and ensure the required level of integrity and confidentiality of user data.

3. The development of new information technologies, such as IoT, quantum cryptography, multi-factor biometric authentication systems, and wide integration of AI/ML and AR/VR solutions, indicate the need for continuous improvement of existing strategies and security measures in the field of development and implementation of new wireless technologies.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Kolovanova, E., Melkoziorova, O., & Malakhov, S. (2023). The specifics of exploits and the particularities of countering this threat. *Proceedings of the XXIX International Scientific and Practical Conference.* July 25-27 2023, Warsaw, Poland. 216-224. https://doi.org/10.46299/ISG.2023.1.29 [in Ukrainian]
2. Shi, Q. (2019). Edge computing-enabled internet of things: A review, challenges and open issues. *IEEE Internet of Things Journal*, 6(5), 1615-1630. https://doi.org/10.1109/jiot2019.2892052
3. Elkhodr, M., (2019). A systematic review of industrial wireless sensor networks applications in oil and gas, agriculture and water treatment. *IEEE Access*, (7), 116623-116634. https://doi.org/10.1016/j.csi.2011.03.004
4. Onishchenko, Y., Chukalov, K., Geldt, S., & Kalancha, A. (2023). Methodology of evil websites and add-ons using SQL-injection and countering it. *Proceedings of the XII International Scientific and Practical Conference.* March 28-31, 2023. Florence, Italy. 409-414. https://doi.org/10.46299/ISG.2023.1.12 [in Ukrainian]
5. Kunz, M., Puchta, A., Groll, S., Fuchs, L., & Pernul, G. (2019). Attribute quality management for dynamic identity and access management. *Journal of Information Security and Applications*, (44), 64–79. https://doi.org/10.1016/j.jisa.2018.11.004
6. Earle, A. E., Frost, R. D. (2012). Wireless Security Handbook. (2nd ed.). New York: Auerbach Publications.
7. Muhammad Ehsan Rana, Mohamed Abdulla, Kuruvikulam Arun. (2007). Common Security Protocols for Wireless Networks: A Comparative Analysis. *IEEE Communications Magazine*, 45(4), 143-149. https://doi.org/10.2991/ahis.k.210913.080
8. Lee, I., Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008
9. Pogorila, K., Bogdanova, E., & Kolovanova, E. (2022). An overview of the possibilities and specifics of the implementation of XDR technology, as a means of comprehensively counteracting current threats to information security. *Technologies, tools and strategies for the implementation of scientific research: materials of the IV International Scientific Conference*. Zhovten 7, 2022. Vinnytsia: European Science Platform. https://doi.org/10.46299/ISG.2023.1.22 [in Ukrainian]

10. K. Ramesh Rao, Dr. S.N. Tirumala Rao, Prof. P. Chenna Reddy. (2017) Wireless Communication Security and Privacy issues and Challenges. *International Journal of Computer Science and Information Security (IJCSIS)*, 15(7), 202-209. https://www.academia.edu/34148630/Wireless_Communication_Security_and_Privacy_issues_and_Challenges, ISBN 1947-5500
11. IEEE. (2020). Recommendations for Wireless Network Security. *IEEE Standards Association*. https://standards.ieee.org/ieee/802.11/7028/
12. Arjona, G., Garcia, M. P., Gil, J. A., Gómez, J. A. (2018). Enhancing Network Security Using Software-Defined Networking (SDN). *Journal of Cybersecurity and Privacy*, 1(1), 45-53. https://doi.org/10.3390/electronics12143077
13. Gorbenko, I., Gorbenko, Y., Yesina, M., & Ponomar, V. (2017). Propositions from the new level analysis and acceptance during the competition are decided to overcome new asymmetric post-quantum cryptographic primitives. *Computer Science and Cybersecurity*, (1), 53-70. ISBN: 2519-23-10 https://periodicals.karazin.ua/cscs/issue/view/577/827 [in Ukrainian]
14. Pogorila, K., Lesnaya, Y., Bogdanova, E., & Malakhov, S. (2022). Social engineering as a factor in the implementation of insider threats. *Scientific Collection "InterConf"*, (111), 494-501. https://archive.interconf.center/files/journals/3/issues/11/public/11-12-PB.pdf#page=495.%20ISBN%20978-1-0747-2337-8 ISBN 978- 1-0747-2337-8 [in Ukrainian]
15. Lesnaya, Yu., & Malakhov, S. (2023). Understanding the main changes in the implementation of phishing attacks. Proceedings of the XVII International Scientific and Practical Conference, 453-457. https://doi.org/10.46299/ISG.2023.1.17 [in Ukrainian]

БЕЗПЕКА В ЕПОХУ БЕЗДРОТОВИХ ІННОВАЦІЙ: АНАЛІЗ ПОТЕНЦІАЛЬНИХ ЗАГРОЗ ТА ЗАХОДИ ЗАХИСТУ

Євгенія Матвєєва[1], студентка факультету комп'ютерних наук (бакалаврат);
e-mail: belka.j.0507@gmail.com; ORCID: https://orcid.org/0000-0001-8801-2185
Марина Єсіна[1,2], кандидат технічних наук, доцент; e-mail: m.v.yesina@karazin.ua;
ORCID: https://orcid.org/0000-0002-1252-7606
Олександр Шумов[2], технічний директор АТ «ІІТ»; e-mail: alex.shumoff@gmail.com
[1]*Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна*
[2]*АТ «ІІТ», вул. Коломенська, 15, Харків, 61166, Україна*
Рукопис надійшов 2 квітня 2024 р. Отримано після рецензування 2 травня 2024 р.
Прийнято 3 червня 2024 р.

Анотація: У сучасному взаємопов'язаному світі технології бездротової передачі даних бездоганно інтегровані в структуру сучасних бізнес-операцій. Зі зростанням довіри до цих технологій зростає необхідність забезпечення надійних заходів кібербезпеки. Особливо в епоху бездротових інновацій, прикладом яких є поширення Інтернету речей (IoT), дискурс навколо безпеки бездротових технологій підкреслює необхідність розуміння як усталених загроз, так і постійної появи нових вразливостей. Це підкреслює нагальну необхідність своєчасного виявлення та стратегій пом'якшення. Хоча зручність, яку забезпечують бездротові технології передачі даних, надає суспільству безпрецедентний доступ до інформації та полегшує керування різноманітними пристроями, процесами та системами, вона також наражає користувачів і сучасні інформаційно-комунікаційні системи (ICS) на серйозні кіберзагрози та вразливості. Отже, виникає нагальна потреба у комплексному вирішенні цих викликів. У цьому дослідженні розглядаються сучасні методології, спрямовані на обмеження доступу до бездротових мереж, виявлення потенційних вразливостей і створення ефективної відповіді на

кібератаки. Дана робота розглядає різні аспекти кібербезпеки, включаючи шифрування даних, механізми автентифікації користувачів, протоколи моніторингу трафіку та алгоритми виявлення аномалій. Крім того, робота звертає увагу на найважливіший аспект навчання персоналу методам безпеки бездротового зв'язку, оснащення його засобами поінформованості про загрози та реагування на інциденти. Враховуючи динамічний ландшафт технологій і загроз кібербезпеки, ця робота спрямована на встановлення базового розуміння ландшафту безпеки в бездротових мережах. Окреслюються прагматичні стратегії для ефективного управління ризиками безпеки, тим самим зміцнюючи стійкість сучасних організацій і захищаючи критичні інформаційні активи.

Ключові слова: *бездротові технології, інформаційна безпека, Інтернет речей (IoT), вразливості, автентифікація, квантова криптографія*

Конфлікт інтересів: автори повідомляють про відсутність конфлікту інтересів.

Список літератури:

1. Колованова, Є., Мелкозьорова, О., & Малахов, С. (2023). Специфіка використання експлойтів та особливості протидії цій загрозі. *Proceedings of the XXIX International Scientific and Practical Conference*. July 25-27 2023, Warsaw, Poland. 216-224. https://doi.org/10.46299/ISG.2023.1.29
2. Shi, Q. (2019). Edge computing-enabled internet of things: A review, challenges and open issues. IEEE Internet of Things Journal, 6(5), 1615-1630. https://doi.org/10.1109/jiot2019.2892052
3. Elkhodr, M., (2019). A systematic review of industrial wireless sensor networks applications in oil and gas, agriculture and water treatment. *IEEE Access*, (7), 116623-116634. https://doi.org/10.1016/j.csi.2011.03.004
4. Онищенко, Ю., Чукалов, К., Гельдт, С., & Каланча, А. (2023). Методологія зломів вебсайтів й додатків за допомогою SQL-injection та протидія ним. *Proceedings of the XII International Scientific and Practical Conference*. March 28-31, 2023. Florence, Italy. 409-414. https://doi.org/10.46299/ISG.2023.1.12
5. Kunz, M., Puchta, A., Groll, S., Fuchs, L., & Pernul, G. (2019). Attribute quality management for dynamic identity and access management. *Journal of Information Security and Applications*, (44), 64–79. https://doi.org/10.1016/j.jisa.2018.11.004
6. Earle, A. E., Frost, R. D. (2012). Wireless Security Handbook. (2-nd ed.). New York: Auerbach Publications.
7. Muhammad Ehsan Rana, Mohamed Abdulla, Kuruvikulam Arun. (2007). Common Security Protocols for Wireless Networks: A Comparative Analysis. *IEEE Communications Magazine*, 45(4), 143-149. https://doi.org/10.2991/ahis.k.210913.080
8. Lee, I., Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008
9. Погоріла, К., Богданова, Є., & Колованова, Є. (2022). Огляд можливостей та узагальнення специфіки реалізації XDR-технології, як засобу комплексної протидії актуальним загрозам інформаційної безпеки. *Технології, інструменти та стратегії реалізації наукових досліджень: матеріали IV Міжнародної наукової конференції*. Жовтень 7, 2022. Вінниця: Європейська наукова платформа. https://doi.org/10.46299/ISG.2023.1.22
10. K. Ramesh Rao, Dr. S.N. Tirumala Rao, Prof. P.Chenna Reddy. (2017) Wireless Communication Security and Privacy issues and Challenges. *International Journal of Computer Science and Information Security (IJCSIS)*, 15(7), 202-209. https://www.academia.edu/34148630/Wireless_Communication_Security_and_Privacy_issues_and_Challenges ISBN 1947-5500
11. IEEE. (2020). Recommendations for Wireless Network Security. *IEEE Standards Association*. https://standards.ieee.org/ieee/802.11/7028/
12. Arjona, G., Garcia, M. P., Gil, J. A., Gómez, J. A. (2018). Enhancing Network Security Using Software-Defined Networking (SDN). *Journal of Cybersecurity and Privacy,* 1(1), 45-53. https://doi.org/10.3390/electronics12143077

13. Горбенко, І., Горбенко, Ю., Єсіна, М., & Пономар, В. (2017). Пропозиції з виконання порівняльного аналізу та прийняття в процесі конкурсу рішень щодо переваг певних асиметричних постквантових криптографічних примітивів. *Комп'ютерні науки та кібербезпека*, (1), 53-70. https://periodicals.karazin.ua/cscs/issue/view/577/827 ISBN: 2519-23-10
14. Погоріла, К., Лєсная, Ю., Богданова, Є., & Малахов, С. (2022). Соціальний інжиніринг, як фактор реалізації інсайдерських загроз. *Scientific Collection «InterConf»*, (111), 494-501. https://archive.interconf.center/files/journals/3/issues/11/public/11-12-PB.pdf#page=495.%20ISBN%20978-1-0747-2337-8 ISBN 978-1-0747-2337-8
15. Лєсная, Ю., & Малахов, С. (2023). Узагальнення основних передумов реалізації фішингових атак. *Proceedings of the XVII International Scientific and Practical Conference*, 453-457. https://doi.org/10.46299/ISG.2023.1.17