СЕКЦІЯ
«ФІЗИКА»

Підсекція комп'ютерних наук та кібербезпеки

УДК 544.421.43:544.421.032.76:544.431.122.2:547.541:547.636.3

ЕКСПЛУАТАЦІЯ ТИПОВИХ ВРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ МЕРЕЖ НА ПРИКЛАДІ МІКРОКОНТРОЛЕРА ESP32

О. І. Барибін, В. В. Бражний

Сьогодні однією із самих актуальних проблем в сфері інформаційно-обчислювальних систем є захист інформації в безпровідних мережах, дійсно, мало хто мислить своє життя без того ж самого Wi-Fi. Останнім часом безпровідні мережі передачі даних стають все більш популярними. Однією з причин можна назвати те, що при розумній ціні вони забезпечують достатню для більшості додатків швидкість передачі даних. Основною перевагою бездротових мереж є відсутність кабельної інфраструктури, що дозволяє реалізувати мережевий проект в коротші терміни і зменшити витрати на побудову системи.

Серед існуючих бездротових мереж, найбільш широко використовується Wi-Fi мережа, побудована за технологією, описаною в стандарті IEEE 802.11. Ця мережа працює на частоті 2,4 та 5 ГГц.

На відміну від кабельних мереж, безпровідні вважаються більш вразливими. Адже традиційні провідні локальні мережі, такі як IEEE 802.3 (Ethernet), можуть бути захищені методами обмеження доступу в будівлю, доступу до пасивного та активного мережевого обладнання. Безпровідні мережі не можуть бути захищені подібним чином, оскільки, на відміну від звичайних провідних мереж, середовище передачі даних в цих мережах представляє собою радіоефір. Будь-який бажаючий, що знаходиться в зоні дії мережі, потенційно може прослуховувати середовище і получати дані що передаються. Таким чином, в випадку з безпровідними мережами механізми фізичної безпеки не можуть бути застосовані.

Згідно з стандартом IEEE 802.11 існують такі основні механізми захисту безпровідних мереж, як шифрування та аутентифікація. Але в цих механізмах захисту існують і постійно виявляються нові вразливості, за допомогою яких можна обійти захист і получити конфіденційні дані.

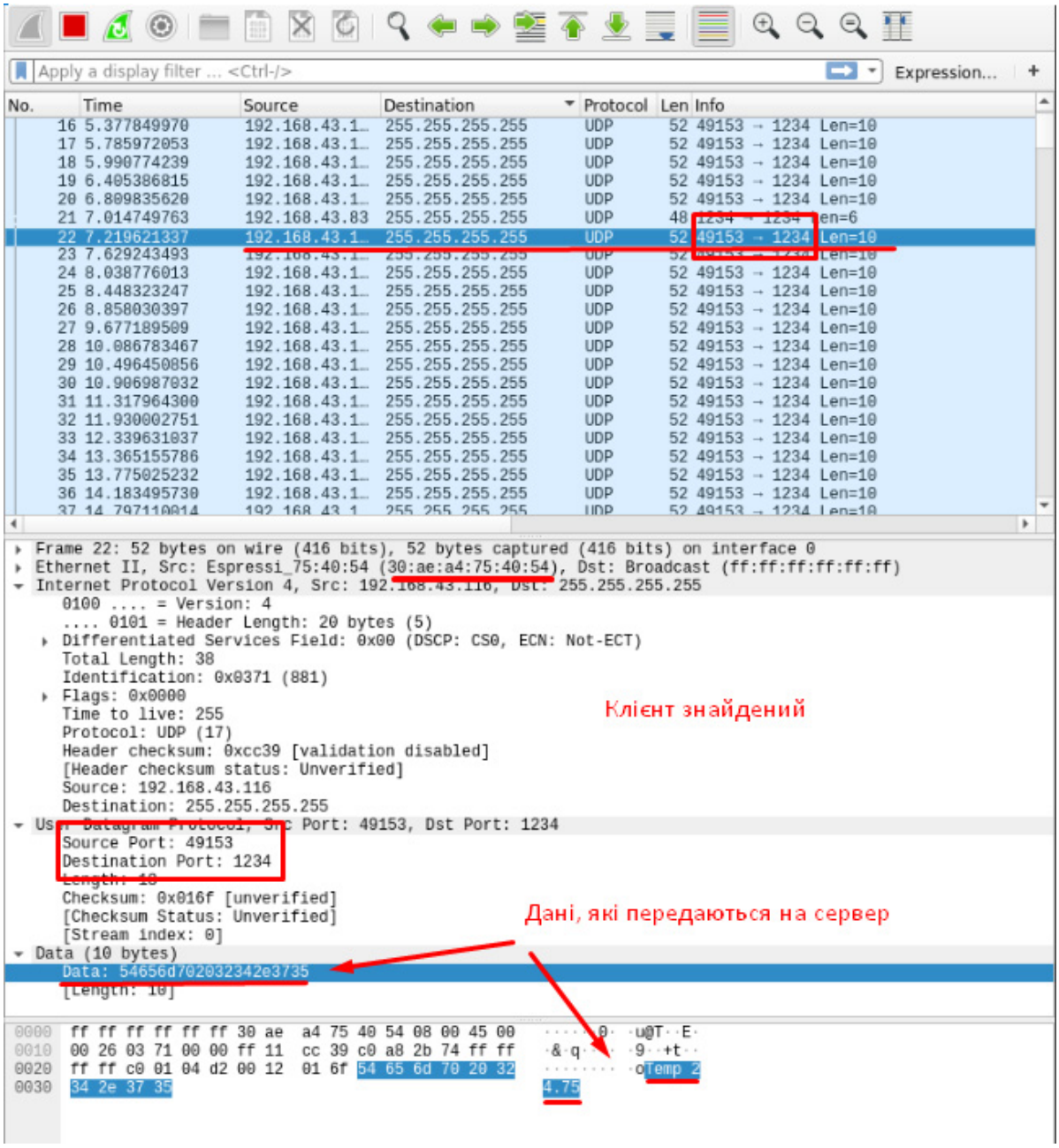
В рамках використання безпровідних мереж в сучасному високотехнологічному суспільстві все більш популярним стають технології Інтернету речей (Internet of Things – IoT) – це мережа зв'язаних через всесвітньою мережу Інтернет об'єктів, які можуть збирати дані і обмінюватися зібраними даними. У зв'язку із поєднанням великої кількості технологій в рамках IoT на сьогоднішній день немає структурованого підходу до забезпечення відповідної інформаційної безпеки на загальному рівні, а лише для конкретних рішень. Зокрема одним з найбільш використовуваним у непромислових пристроях IoT є мікроконтролер ESP 32, загрози інформаційної безпеки щодо якого в першу чергу будуть пов'язані з використання вразливостей бездротових мереж, що обумовлює актуальність теми курсової роботи.

Таким чином метою даної роботи є дослідження можливостей використання вразливостей бездротових мереж під час використання ESP 32.

Відповідно до сформульованої мети завданнями роботи є :

- виділити основних існуючих вразливостей безпровідних мереж;
- проаналізувати та запропонувати інструментарій для використання окреслених вразливостей;
- дослідити можливості використання вразливостей під час використання ESP 32.

З врахуванням усіх завдань роботи було експлуатовано типові вразливості бездротових мереж на прикладі мікроконтролера esp32 (рис. 1).



В даній роботі:

1. Виділено основні актуальні вразливості безпровідних мереж на основі аналізу стандартів, топології, механізмів захисту, переваг та недоліків безпровідних технологій передачі даних безпровідних мереж.

2. Враховуючи наявний інструментарій, який використовується для компрометації бездротових мереж, запропоновано в якості основних інструментів використовувати: Airmon-ng, Airodump-ng, Besside-ng, Aircrack-ng, Wireshark, Aireplay-ng, Arduino.

3. На основі тестування бездротової мережі на злам та на заміну трафіку, який передається ESP 32, сформульовано вектор атаки, який дозволяє клонування пристрою на основі використання компонентів бездротових мереж з відомими вразливостями.

Література

1. Pathan A. K. Securing Cyber-Physical Systems. London: CRC Press, 2015. 236 p.
2. Misra S., Maheswaran M., Hashmi S. Security Challenges and Approaches in Internet of Things. 2017. 106 p.
3. Aziz B., Arenas A., Crispo B. Engineering Secure Internet of Things Systems. Croydon : CPI Group, 2016. 56 p.
4. Gilchrist A. INDUSTRY 4.0 THE INDUSTRIAL INTERNET OF THINGS. Nonthaburi : Apress, 2016. 100 p.
5. Hu F. Security and Privacy in Internet of Things (IoTs). London : CRC Press, 2016. 203 p.
6. Macaulay T. RIoT Control. London: Elsevier, 2017. 13 p.
7. Russell B., Van Duren D. Practical Internet of Things Security. BIRMINGHAM : Packt, 2016. 94 p.
8. The Internet of things with ESP32. URL : http://esp32.net/ (Last accessed: 05.01.2019).
9. Wi-Fi, від англійського Wireless Fidelity, 2009. URL : https://wiki.cuspu.edu.ua/index.php/Wireless_Fidelity/ (Last accessed: 05.01.2019)
10. Колыбельников А. И. Обзор технологий беспроводных сетей. *Московский физико-технический институт*, 2012. 3 с.
11. Макаренко А. Ю., Парфенова А. О., Могильний С. Б. Бездротові технології передачі даних WI-FI, BLUETOOTH TA ZIGBEE. *Національний технічний університет України «КПІ»*, 2010. 127 с.
12. Сайко В. Г., Оксіюк О. Г., Дікарєв О. В. Основи цифрового оброблення сигналів в системах цифрового радіозв'язку. Київ, 2016. 113 с.
13. Шовкута В. А., Флоров С. В. Аналіз механізмів захисту та вразливостей бездротових WI-FI мереж. *ДВНЗ «Національний гірничий університет»*, 2016. 10 с.
14. Parrot Security OS – альтернатива Kali Linux, 2017. URL : https://habr.com/company/pentestit/blog/337712 (дата звернення: 05.01.2019).
15. Airmon-ng, 2014. URL : https://tools.kali.org/wireless-attacks/airmon-ng (дата звернення: 05.01.2019).
16. Airodump-ng, 2017. URL : https://tools.kali.org/wireless-attacks/airodump-ng (дата звернення: 05.01.2019).
17. Besside-ng, 2017. URL : https://tools.kali.org/wireless-attacks/besside-ng (дата звернення: 05.01.2019).
18. Aircrack-ng, 2014. URL : https://tools.kali.org/wireless-attacks/aircrack-ng/ (дата звернення: 05.01.2019).
19. Wireshark, 2014. URL : https://tools.kali.org/information-gathering/wireshark (дата звернення: 05.01.2019).
20. Aireplay-ng, 2017. URL : https://tools.kali.org/wireless-attacks/aireplay-ng (дата звернення: 05.01.2019).
21. Arduino, 2014. URL : https://tools.kali.org/hardware-hacking/arduino (дата звернення: 05.01.2019).

УДК 81.33+004

СИСТЕМА АНАЛІЗУ «USER STORY» НА БАЗІ БІБЛІОТЕКИ NLTK

О. І. Барибін, О. В. Соловей

У сучасному світі прискорення темпів розвитку інформаційних технологій призводить до необхідності використовувати гнучкі підходи до розробки програмних продуктів. Від того, які технології використовує компанія, будуть залежати її конкурентні переваги на ринку. Однією з найбільш актуальних проблем є саме формулювання вимог до програмного