Далеко не всі мед заклади можуть собі дозволити потрібне обладнання, тривалий процес дозрівання тканин - це з мінусів, плюсами ж є перспектива створення органів для: Трансплантації та лікування дефіциту донорських органів, можливість друкувати тканини з клітин пацієнта, створення хрящів, кісток, шкіри, судин для Реконструктивної медицини, а також зниження вартості лікування у майбутньому.

Біодрук має величезний потенціал кардинально змінити медицину та наукові дослідження. Очікується, що технологія дозволить створювати повноцінні живі органи для трансплантації, що допоможе вирішити проблему нестачі донорів і значно знизить ризик відторгнення, адже органи створюватимуться з клітин самого пацієнта. Також біодрук відкриє можливість персоналізованої медицини, коли тканини та імпланти точно відповідатимуть індивідуальним особливостям людини. Крім того, у перспективі лікарі зможуть друкувати тканини безпосередньо у тілі пацієнта під час операцій, що прискорить загоєння ран і відновлення пошкоджених ділянок. Загалом біодрук стане основою нової епохи регенеративної медицини, суттєво розширюючи можливості Лікування та підвищуючи якість життя людей.

Література

1. Michele Conti, Michele Marino. Bioprinting From Multidisciplinary Design to Emerging Opportunities, Academic Press, Elsevier, 2022.-P. 19-49.

2. Mitchell Maika G. Bioprinting: techniques and risks for regenerative medicine. London, San Diego, Cambridge, Oxford, 2017.-P. 123-140.

3. Yang Wu, Jerry Fuh and Ibrahim Tarik Ozbolat. 3D Bioprinting in Tissue and Organ Regeneration, 2023.-P. 247-264.

4. Що таке біодрук URL:
http://ua.insta3dm.com/info/what-is-3d-bioprinting-simply-explained-f-71989890.html

5. Перспективи біодруку URL:
https://easy3dprint.com.ua/uk/3d-druk-dlya-meditsini/

6. Принцип роботи біопринтингу URL:
https://www.imena.ua/blog/3d-bioprint-part-1/

УДК 004.7.056

Д.С. Матюк; М.В. Деркач, канд. техн. наук, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

NetScope: ПЕНТЕСТІНГ БЕЗДРОТОВИХ МЕРЕЖ

D.S. Matiuk, M.V. Derkach, Ph.D., Assoc. Prof.

NetScope: WIRELESS NETWORK PENTESTING

Бездротові мережі можуть бути розгорнуті та працювати у різних середовищах: комерційних, урядових, освітніх, а також у звичайних житлових будинках. До того ж технології бездротової передачі сигналу особливо сприяють концепції Інтернету речей (Internet of Things, IoT), на яку переходять все більше пристроїв, що підвищують наш комфорт перебування в Інтернеті [1].

В результаті кількість бездротових мереж, як і кількість об'єктів для атак, буде тільки збільшуватися. Клієнти та організації повинні розуміти всі ризики використання бездротових мереж та знати, як зловмисники атакують ці системи. Пентестери повинні гарантувати, що ці мережі мають необхідну кількість елементів керування безпекою та у їхній конфігурації відсутні помилки. Для цього використовують сканери

вразливостей, фреймворки пентестування та аналізу трафіку, що виявляють конфігураційні похибки й відомі CVE. Складність мереж і різноманітність протоколів (Wi-Fi, ZigBee, Bluetooth, радіочастного діапозону 2.4 ГГц) для ефективного захисту вимагають багаторівневих контрзаходів, які охоплюють як активні, так і пасивні вектори атак, що призводить до комбінування програмних й апаратних інструментів, які здатні перевіряти рівень захищеності точок доступу, контролерів, клієнтських пристроїв, виявити вразливості бездротових мереж [2]. Розробка апаратної платформи надає змогу проводити польові випробування, швидко розгортати точки атаки та мінімізувати час налаштування.

Наразі, розроблено пристрій для тестування безпеки бездротових мереж NetScope, що здатен виявляти вразливості, зокрема WPA/WPA2, відкриті точки доступу, слабкі паролі, застарілі протоколи шифрування, WPS; здатний автоматично виявляти бездротові мережі та підключені пристрої; проводити атаки, включаючи атаки деавтентифікації, спам-маяки, а також клонувати мережі. Це доступне та портативне рішення для швидкої оцінки безпеки бездротових мереж у реальних умовах, особливо корисне для навчальних закладів, державних підприємств, малих фірм, які не мають власних фахівців або ресурсів для регулярного тестування на проникнення мережевих з'єднань. Основною перевагою розробки є повна автономність пристрою. Він не потребує встановлення додаткового програмного забезпечення чи підключення до живлення. Модульна структура дозволяє розширювати функціонал, наприклад, додавати підтримку нових протоколів чи типів тестів. Результати пентестінгу можуть бути доступні через вебінтерфейс, що спрощує аналіз і створення звітів. Ще одна перевага — низька собівартість у порівнянні з аналогічними комерційними рішеннями.

Фактично NetScope здатен виявляти вразливості до MITM-сценаріїв, підміни точок доступу та інших загроз у бездротових мережах. Принцип дії наступний: для початку пристрій проводить сканування, на екрані якого з'являється перелік доступних в радіусі дії мережевих з'єднань з вказаною потужністю сигналу, використаним номером каналу та протоколом безпеки для захисту бездротових мереж; далі розроблений пристрій проводить пентест для обраної мережі.

Для прикладу в межах етичного хакінгу для проведення пентесту розроблений пристрій NetScope спрямовує деаутентифікаційні пакети проти точки доступу TEST, зв'язок різко стає нестабільним (рис. 1). Це свідчить про можливість проведення атаки, оскільки поки мережа слабшає, зловмисник може розгорнути підроблену точку з тією ж назвою (SSID). Якщо зловмисник ще й знатиме спільний пароль для доступу до мережі (PSK), може реалізувати атаку «Evil twin», тобто розгорнути фальшиву точку доступу, і в приватній мережі весь трафік жертви проходитиме через атакуючий вузол, що дозволяє проводити MITM-сценарії: перехоплення логінів, паролів і зміни контенту.

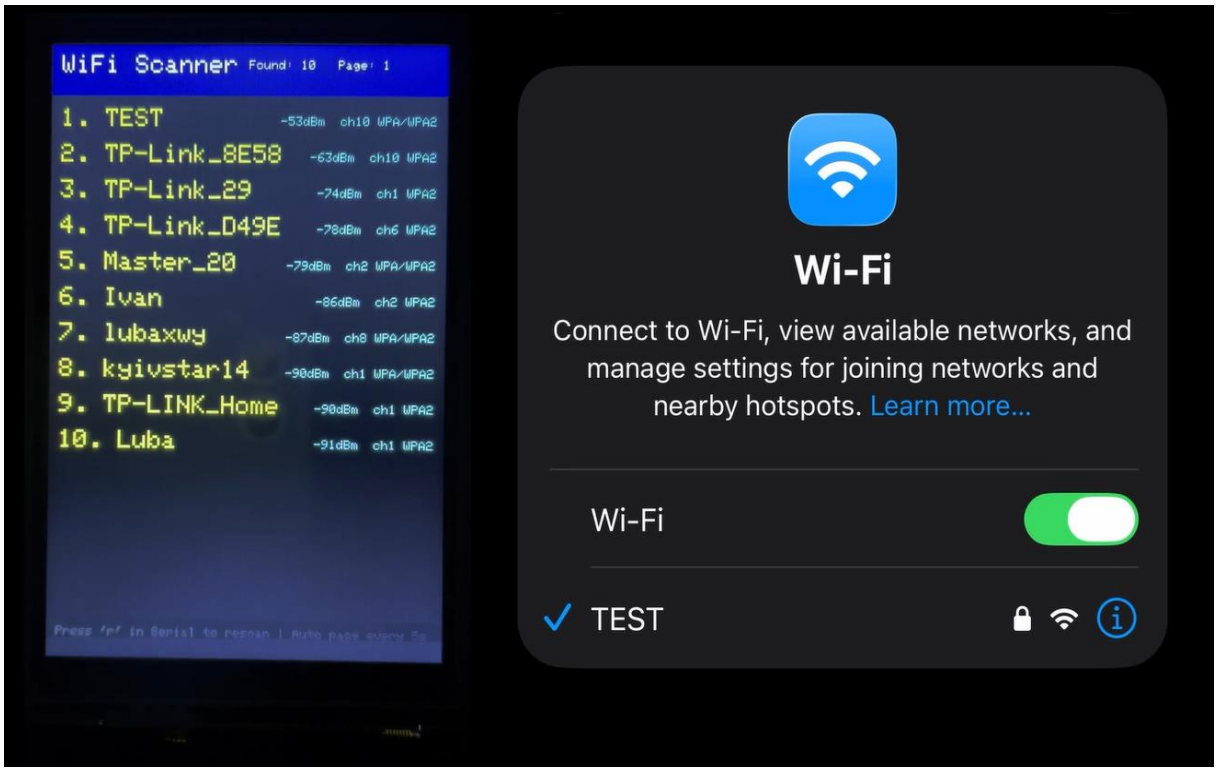

Рисунок 1. Приклад пентесту бездротової мережі

Тобто, завдяки розробленому пристрою можна проводити тестування і оцінку безпеки бездротових мереж, а саме визначати чи піддається мережеве з'єднання атакам, які призводять до відмови або до різних типів MITM-атак, що несуть істотний ризик компрометації трафіку, особливо в корпоративному сегменті.

В цілому пристрій NetScope вирішує актуальну проблему, зокрема дозволяє оперативно перевірити безпеку бездротових мереж у будь-якому місці; забезпечує зниження ризиків витоку даних шляхом швидкої діагностики вразливостей у реальних умовах та може бути використаний як: навчальний інструмент для здобувачів вищої освіти за спеціальністю «Кібербезпека та захист інформації», польовий пристрій для аудитів безпеки, інтегрований компонент систем моніторингу підприємств або смарт-будівель.

Література

1. Sachenko A.O., Kochan V.V., Bykovyy P.Ye., Zahorodnia D.I., Osolinskyy O.R., Skarga-Bandurova I.S., Derkach M.V., Orekhov O.O., Stadnik A.O., Kharchenko V.S., Fesenko H.V. Internet of Things for intelligent transport systems: Practicum. Ministry of Education and Science of Ukraine, Ternopil National Economic University, Volodymyr Dahl East Ukrainian National University, National Aerospace University "Kharkiv Aviation Institute", 2019. 135 p. ISBN 978-617-7361-92-2. URL: https://aliot.eu.org/wp-content/uploads/2019/10/ALIOT ITM3 IoT-for-Int-TransSys_web.pdf

2. Derkach, M., Matiuk, D., Skarga-Bandurova, I., & Zagorodna, N. CrypticWave: A zero-persistence ephemeral messaging system with client-side encryption, in: Cyber Security and Data Protection, vol. 4042, 2025, P.316–323.