Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
Кафедра радіотехнічних систем
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Метод та програмне забезпечення захисту безпровідної мережі Wi-Fi

Виконав: студент VI курсу, групи РАм-61

спеціальності 172 Електронні комунікації та радіотехніка
(шифр і назва спеціальності)

(підпис) Кміть С.О. (прізвище та ініціали)

Керівник (підпис) Дунець В.Л (прізвище та ініціали)

Нормоконтроль (підпис) Хвостівська Л.В. (прізвище та ініціали)

Завідувач кафедри (підпис) Дунець В.Л. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)

Кафедра радіотехнічних систем
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дунець В.Л.
(підпис) (прізвище та ініціали)
«29» листопада 2024 р..

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 172 Електронні комунікації та радіотехніка
(шифр і назва спеціальності)

Студенту Кміту Сергію Омеляновичу
(прізвище, ім'я, по батькові)

1. Тема роботи Метод та програмне забезпечення захисту безпровідної мережі Wi-Fi

Керівник роботи Дунець Василь Любомирович, к.т.н., доцент, завідувач кафедри РТ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «29» листопада 2024 року № 4/7-1146

2. Термін подання студентом завершеної роботи 26 грудня 2024р.

3. Вихідні дані до роботи Об'єкт дослідження:

Предмет дослідження:

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ.

Розділ 1. Аналітична частина

Розділ 2. Основна частина

Розділ 3. Науково-дослідна частина

Розділ 4. Охорона праці та безпека в надзвичайних ситуаціях.

Висновки

Перелік використаних джерел

Додатки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці			
Безпека в надзвичайних ситуаціях			

7. Дата видачі завдання 29 листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи		
2.	Підбір джерел по темі кваліфікаційної роботи		
3.	Переклад та опрацювання джерел по темі кваліфікаційної роботи		
4.	Виконання дослідження по темі кваліфікаційної роботи		
5.	Оформлення розділу «Аналітична частина»		
6.	Оформлення розділу «Основна частина»		
7.	Оформлення розділу «Науково-дослідна частина»		
8.	Оформлення розділу «Охорона праці та безпека в надзвичайних ситуаціях»		
9.	Підготовка графічного матеріалу		
10.	Оформлення кваліфікаційної роботи		
11.	Нормоконтроль		
12.	Перевірка на плагіат		
13.	Попередній захист кваліфікаційної роботи		
14.	Захист кваліфікаційної роботи		

Студент _____ Кміть С.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Дунець В.Л.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Метод та програмне забезпечення захисту безпровідної мережі Wi-Fi // Кваліфікаційна робота освітнього рівня «Магістр» // Кміть Сергій Омелянович // Тернопільський національний технічний університет імені Івана Пулюя, факультет прикладних інформаційних технологій та електроінженерії, кафедра радіотехнічних систем, група РАм-61 // Тернопіль, 2024 // С. 75, рис. – 35, табл. – 2, додат. – 3, бібліогр. – 20.

Ключові слова: АЛГОРИТМ, АТАКА, АУТЕНТИФІКАЦІЯ, БЕЗПРОВІДНА ІНФРАСТРУКТУРА, ВАЛІДНІСТЬ, ДЕТЕКТОР, ЕФЕКТИВНІСТЬ, ЗАХИСТ, ІДЕНТИФІКАТОР, ІНФОРМАЦІЙНА БЕЗПЕКА, КЛЮЧ, КЛІЄНТ, КОНФІДЕНЦІЙНІСТЬ, МЕРЕЖА, МЕТОД, НАДІЙНІСТЬ, ПАКЕТ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ПРОТОКОЛ БЕЗПЕКИ, РАДІОКАНАЛ, СЕРВЕР, СЕРТИФІКАТ, ТОЧКА ДОСТУПУ, ТРАФІК, ФАЛЬШИВА ТОЧКА ДОСТУПУ, ЦІЛІСНІСТЬ, ШИФРУВАННЯ.

Кваліфікаційна робота присвячена вирішенню актуальної науково-практичної проблеми розробки стратегій для гарантування інформаційної та функціональної безпеки безпровідної інфраструктури. Це виконується за допомогою апаратного розділення абонентів, з метою підвищення рівня захищеності від різноманітних загроз безпеки. Розглядаються теоретичні основи, методи, моделі та засоби, спрямовані на забезпечення надійної функціональності безпровідних систем та мереж.

В першому розділі кваліфікаційної роботи:

– Розглянуто питання аутентифікації в безпровідних мережах Wi-Fi.

– Проведено аналіз існуючих протоколів безпеки, які застосовуються в мережах.

– Досліджено проблему запобігання недозволеному доступу підроблених клієнтів до ТД та ефективності заходів захисту від можливих атак, спрямованих на підроблення ТД.

– Проаналізовано ефективність існуючих методів та засобів захисту, які можуть забезпечити безпеку Wi-Fi клієнтів від потенційних загроз, що виникають як з боку самої мережі, так і з боку клієнта.

Результати дослідження вказують на те, що наявні методи не забезпечують повноцінного захисту від ФТД.

В другому розділі кваліфікаційної роботи розроблено концепцію, яка дозволяє проводити аутентифікацію клієнтів ТД. Ця модель може бути використання як для базової аутентифікації клієнтів, так і для впровадження аутентифікації ТД і клієнтів.

В третьому розділі кваліфікаційної роботи розроблено комплекс програм, що включає клієнтську та серверну частини. Клієнтська частина, спроектована для ОС Android, забезпечує аутентифікацію ТД за допомогою ВК. У майбутньому можна розглянути можливість реалізації першочергової довіри клієнта до ТД, використовуючи сертифікати X.509 або модель, що застосовується в протоколі Pretty Good Privacy (PGP).

ANNOTATION

Method and software for securing a wireless Wi-Fi network // Qualification work of the educational level «Master» // Kmit Serhii Omelianovych // Ternopil Ivan Puluj National Technical University, Faculty of Applied Information Technologies and Electrical Engineering, Department of Radio Engineering Systems, group RAm-61 // Ternopil, 2024 // P. 75, fig. – 35, tabl. – 2, annexes. – 3, references – 20.

Keywords: ALGORITHM, ATTACK, AUTHENTICATION, WIRELESS INFRASTRUCTURE, VALIDITY, DETECTOR, EFFICIENCY, PROTECTION, IDENTIFIER, INFORMATION SECURITY, KEY, CLIENT, CONFIDENTIALITY, NETWORK, METHOD, RELIABILITY, PACKAGE, SOFTWARE, SECURITY PROTOCOL, RADIO CHANNEL, SERVER, CERTIFICATE, ACCESS POINT, TRAFFIC, ROGUE ACCESS POINT, INTEGRITY, ENCRYPTION.

The qualification work is devoted to solving the urgent scientific and practical problem of developing strategies to ensure the information and functional security of wireless infrastructure. This is done by means of hardware separation of subscribers in order to increase the level of protection against various security threats. The theoretical foundations, methods, models, and tools aimed at ensuring reliable functionality of wireless systems and networks are considered.

The first section of the qualification paper:

– The issue of authentication in wireless Wi-Fi networks is considered.

– The analysis of existing security protocols used in networks is carried out.

– The problem of preventing unauthorized access of fake clients to the AP and the effectiveness of protection measures against possible attacks aimed at counterfeiting the AP is investigated.

– The effectiveness of existing methods and means of protection that can ensure the security of Wi-Fi clients from potential threats arising from both the network itself and the client is analyzed.

– The results of the study indicate that existing methods do not provide full protection against Rogue AP.

In the second section of the qualification work is developed concept that allows authenticating clients of the AP. This model can be used both for basic client authentication and for implementing authentication of the AP and clients.

In the third section of the qualification work, a set of programs is developed that includes client and server parts. The client part, designed for Android OS, provides authentication of the AP using PK. In the future, it is possible to consider the possibility of implementing the client's primary trust in the AP using X.509 certificates or the model used in the Pretty Good Privacy (PGP) protocol.

ЗМІСТ

ВСТУП

Актуальність теми. Для обміну інформацією між користувачами все частіше використовують безпровідні мережі. Зазвичай їх встановлюють в аеропортах, готелях, ресторанах, університетах, на підприємствах з метою забезпечення з'єднання користувачів із мережами постачальників інтернет-послуг. Також ці мережі використовуються для об'єднання просторово розташованих підмереж в єдину загальну мережу, тобто у випадках, коли кабельне підключення підмереж є неможливим або небажаним.

Ці зміни спричинюють зростання вразливості світу перед новими деструктивними впливами, такими як виклики, загрози і фактично непомітні кібернетичні злочини в галузі ІТ. Це призводить до збільшення частоти атак та завдання збитків внаслідок витоку інформації. Оскільки основи такої діяльності наразі неформалізовані достатньо, питання забезпечення інформаційної та функціональної безпеки безпровідних мереж набуває особливої актуальності.

Вирішенню проблеми інформаційної та функціональної безпеки, включаючи безпровідні мережі, приділяється увага видатних науковців, як вітчизняних, так і закордонних, а також їхніх наукових шкіл. Серед них зазначаються імена В.М. Богуша, В.Л. Бурячка, В.В. Домарева, А. Карлсона, О.Г. Корченка, Г.Т. Маркова, М.В. Степашкина, С.В. Толюпи, В.О. Хорошка та Я.С. Шифрина, а також інших вчених.

Наявність розбіжностей в існуючих даних визначає актуальність теми кваліфікаційної роботи освітнього рівня «Магістр», і отже, вирішення завдання забезпечення безпеки Wi-Fi мережі має значущі наукові та практичні аспекти.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи є обґрунтування стратегій захисту Wi-Fi мережі для запобігання несанкціонованому доступу та забезпечення інформаційної безпеки.

Для досягнення поставленої мети потрібно виконати ряд завдань, зокрема:

– Проаналізувати відомі методи захисту Wi-Fi мережі для обґрунтування наукового напряму дослідження.

– Обґрунтувати методологію та концепцію захисту Wi-Fi мережі від несанкціонованого доступу.

– Розробити програмний комплекс захисту Wi-Fi мережі для клієнтської та серверної частини, орієнтований на мобільні пристрої з ОС Android.

– Провести процес валідації розробленого методу та концепції захисту Wi-Fi мережі від несанкціонованого доступу.

Об’єкт дослідження. Основним об’єктом дослідження є процес впровадження заходів для облаштування захисту Wi-Fi мережі від недозволеного доступу.

Предмет дослідження. Розгляд методів, спрямованих на забезпечення інформаційної безпеки Wi-Fi мережі та захист її від несанкціонованого доступу.

Практичне значення одержаних результатів. Вперше створено схему захисту Wi-Fi мережі на основі взаємної ідентифікації між користувачами та точками доступу, використовуючи модель протоколу Pretty Good Privacy.

Наукова новизна отриманих результатів. Полягає у вдосконаленні практичних і теоретичних підходів та моделей забезпечення функціональної і інформаційної безпеки в мережах зв’язку, що базуються на використанні апаратного розділення абонентів

РОЗДІЛ 1. АНАЛІТИЧНА ЧАСТИНА

1.1. Аналіз стану проблеми

Безпровідні ТД набувають найбільшої популярності як засіб підключення до IP-мереж, таких, як Інтернет. Згідно з прогнозом компанії Cisco щодо глобального мобільного трафіку на період 2015-2020 років [1], до 2016 року глобальний IP-трафік перетне рубіж у 1 Збайт (1000 Ебайт), а до 2019 року ця кількість збільшиться до 2 Збайт. У 2014 році 54% трафіку становило провідне підключення, а 46% – безпровідне. Проте до 2019 року передбачалося зростання частки Wi-Fi і мобільного трафіку до 66% від загальної кількості, з яких 13% становив чистий мобільний трафік, а 53% – чистий Wi-Fi трафік. На рисунку 1.1. наведено динаміку зміни обсягу трафіку від різних технологій доступу.

Рис. 1.1. – Прогноз компанії Cisco щодо зміни IP-трафіку різних технологій доступу в період з 2014 по 2019 рік

Згідно з тим самим прогнозом від компанії Cisco [2], кількість безпровідних ТД Wi-Fi зросте з 64,2 мільйонів у 2015 році до 841,3 мільйонів у 2021 році. Підвищення обсягу безпровідного трафіку пояснюється передусім простотою впровадження WLAN, зростанням популярності електроніки, такої як смартфони, планшети, тощо, а також розвитком технологій, таких як Connected Car (Wi-Fi в автомобілі) та інші.

Незважаючи на очевидний ріст популярності WAP) Wi-Fi і збільшення кількості користувачів, в існуючих схемах аутентифікації між клієнтами та ТД існують певні недоліки. Наприклад, більшість адміністраторів WAP залишають незмінними ключі аутентифікації, налаштовані за замовчуванням. Деякі ТД, з іншого боку, залишаються відкритими зазначенням виробника. У додаток до цього існують методи злому захищених ТД Wi-Fi, які дозволяють отримати паролі аутентифікації за прийнятий час. Ці дії створюють можливість для проведення атак, таких як “злий двійник” (англ. “Evil twin”), яка включає в себе створення ФТД (англ. “Rogue AP”), що виглядає як справжня [3]. Це дозволяє зловмисникові збирати особисті дані користувачів.

У контексті невеликих мереж, захищених за протоколами WEP або WPA/WPA2 Personal, керування доступом до безпровідної точки можна регулювати шляхом обмеження доступу за MAC-адресами та застосуванням методу конфіденційності для цієї точки. Втім, перший метод можна легко уникнути шляхом фальсифікації MAC-адреси. Виявлення прихованих ТД стає нескладним завдяки можливості визначення їх під час прослуховування радіоканалу.

Отже, виникає необхідність взаємної аутентифікації між клієнтами та ТД Wi-Fi.

1.2. Загальна проблематика аутентифікації в безпровідних мережах Wi-Fi

Завжди традиційна мережна взаємодія передбачала використання провідних мереж, що ґрунтується на роботі комутаторів. Останні, у свою чергу,

маршрутизують пакети на відповідний порт призначення, забезпечуючи при цьому обмежений доступ до інших хостів (див. рисунок 1.2.).

Для того щоб перехопити чужий трафік, зловмисник повинен здійснити фізичне підключення до комутатора, отримати адміністративні права на цьому пристрої або використати метод атаки MITM з фізичним втручанням між пристроями мережі (докладний розгляд аспектів безпеки провідних мереж виходить за межі даної кваліфікаційної роботи).

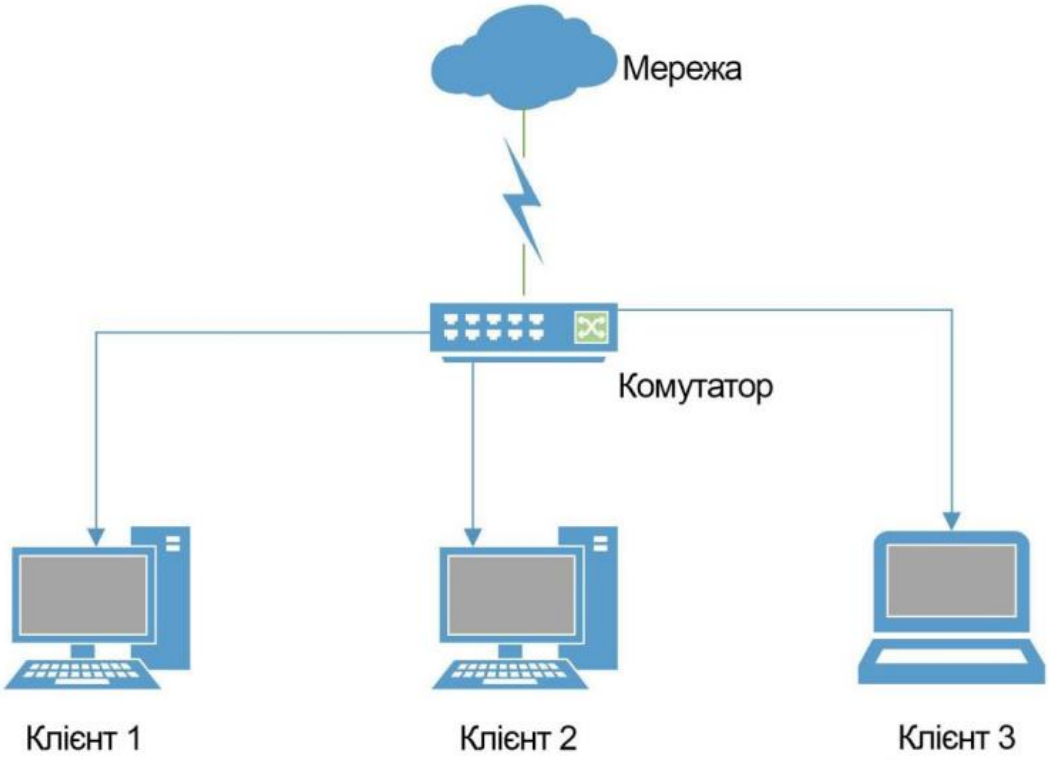


Рис. 1.2. – Принцип функціонування комутаторів

Безпровідні мережі передають дані за допомогою радіохвиль високих частот, зокрема в дециметровому діапазоні 2,4 ГГц та сантиметровому діапазоні 5 ГГц. Оскільки це радіосигнал, його доступність для пристроїв фізично необмежена, що дозволяє отримання даних будь-яким пристроєм у зоні поширення сигналу (див. рисунок 1.3). У стандартному режимі, також відомому як клієнтський або управлінський режим, мережеве обладнання отримує лише пакети, призначені саме йому. Проте існує ряд ПЗ (Commview for WIFI [4],

aircrack-ng [5]та інші), яке дозволяє перевести безпровідні мережні адаптери в режим моніторингу, що надає можливість пристрою отримувати й аналізувати весь мережевий трафік.

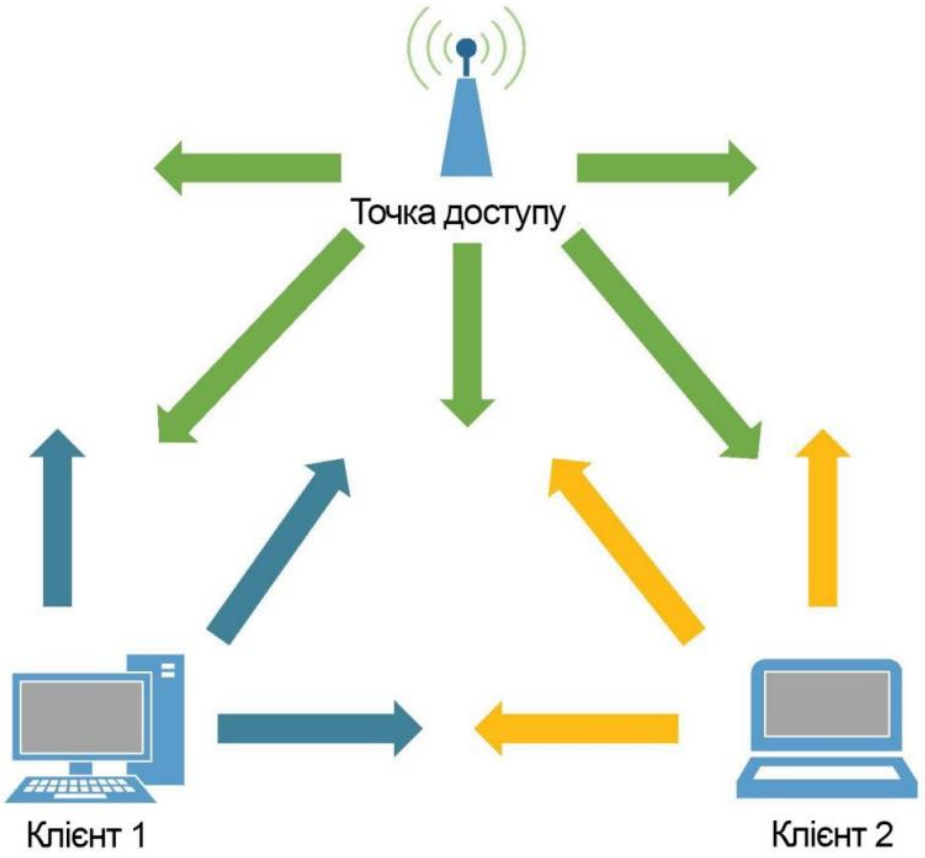


Рис. 1.3. – Принцип функціонування WAP

Враховуючи це, виникла необхідність аутентифікації клієнтів для регулювання радіодоступу до ТД та LAN, а також для шифрування трафіку, що передається між клієнтами та транспортними засобами передачі даних. З цією метою було розроблено декілька протоколів безпеки, які відповідають за аутентифікацію та шифрування інформації, а також кілька методів, які забезпечують додатковий контроль доступу до мережі.

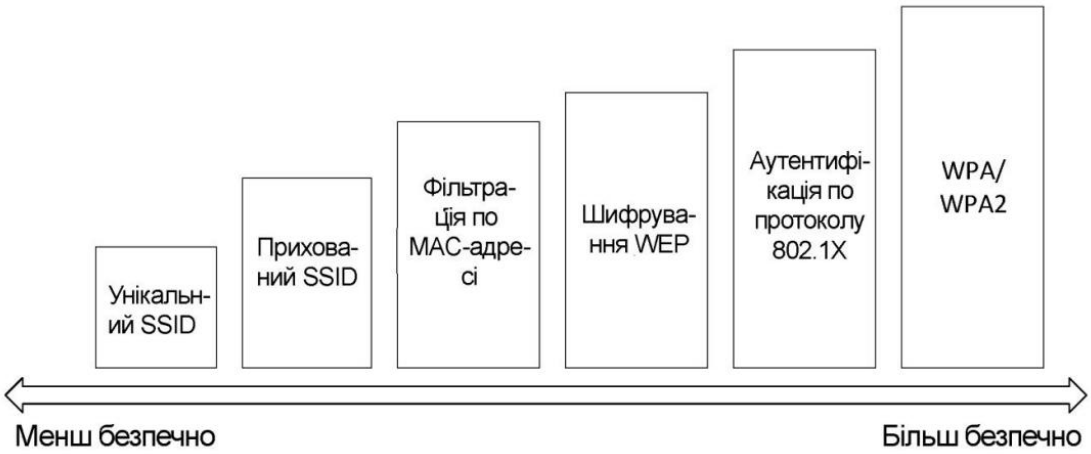


Рис. 1.4. – Методи забезпечення безпеки WAP

На рисунку 1.4. представлено різноманітні методи забезпечення безпеки WAP в залежності від рівня безпеки.

1.3. Різновиди аутентифікації клієнтів та точок доступу

Основним елементом взаємодії будь-якої безпровідної мережі, включаючи ТД та їхніх клієнтів, є процес аутентифікації. Це визначає, як ТД ідентифікує клієнта, перевіряє його права на взаємодію та забезпечує відповідне підтвердження. Також ключовим аспектом є шифрування: вибір алгоритму, методи генерації ключів та їхнє регулярне оновлення. Існує кілька варіантів аутентифікації [6], зокрема відкрита аутентифікація, аутентифікація за відкритим ключем та аутентифікація через протокол 802.1X. Перші два підходи визначаються стандартом 802.11 і мають свої ризики, тоді як останній описаний у стандарті IEEE 802.11i-2004. Цей стандарт визначає процедури керування ключами та взаємної аутентифікації 802.1X, об’єднані під терміном RSNA, або міцне безпечне мережеве спілкування [7].

1.3.1. Відкрита аутентифікація

Метод “Open” є найпростішою формою аутентифікації, де єдиним вимогам є знання клієнтом ідентифікатора SSID ТД. Клієнт ініціює запит на

авторизацію до ТД, яка, в свою чергу, автоматично встановлює з'єднання з пристроєм у мережі. Цей метод, який не є справжньою аутентифікацією, використовується відкритими мережами або в тих, що захищені протоколом WEP. На рисунку 1.5 подано процес відкритої аутентифікації клієнтів у мережі.

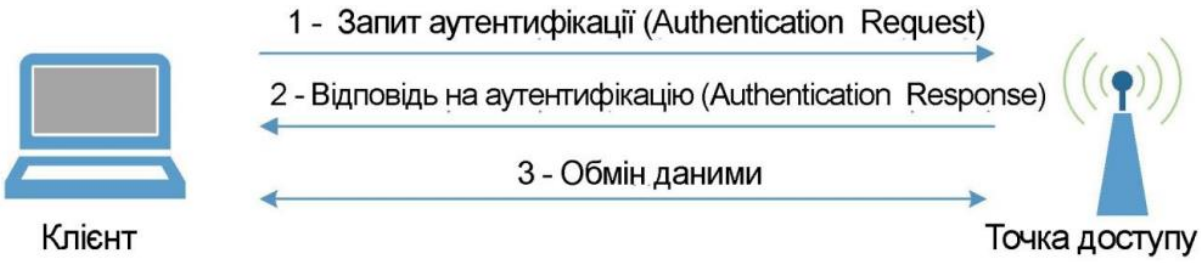


Рис. 1.5. – Процес відкритої аутентифікації

На етапі початкового зв'язку клієнт подає запит на проведення аутентифікації, після чого ТД перевіряє валідність ідентифікаційних даних клієнта, а на третьому етапі клієнт успішно приєднується до мережі ТД.

1.3.2. Аутентифікація за допомогою загального ключа

Метод Shared Keys передбачає перевірку валідності клієнта, який підключається, на основі спільного ключа (пароля). Процедура аутентифікації включає чотири етапи. Починаючи з запиту на аутентифікацію від клієнта до ТД, відповідь на запит надсилається текстовим повідомленням. Клієнт, отримавши це повідомлення, шифрує його за допомогою ключа WEP і надсилає зашифровану відповідь назад до ТД. ТД розшифровує отримане повідомлення, і в разі збігу з відправленим, аутентифікація вважається успішною.

Рис. 1.6. – Алгоритм аутентифікації по загальному ключу

На рисунку 1.6. наведено схему аутентифікації по загальному ключу.

1.3.3. Використання протоколу IEEE 802.1X для аутентифікації

Протокол мережі IEEE 802.1X виступає як метод аутентифікації на основі протоколу PEA, який уповноважує стандарт IEEE 802.1X та описує його як EAPOL [8]. EAPOL є канальним протоколом, що дозволяє передавати Air-пакети між користувачем і аутентифікатором, використовуючи MAC-адреса. Стандарт 802.1X встановлює контроль доступу до мережі на основі портів для аутентифікації та авторизації пристроїв і визначає механізми керування ключами. Порт тут розглядається як єдина точка приєднання до LAN. 802.1X визначає три учасника взаємодії:

– Аутентифікатор – мережевий пристрій, який вимагає аутентифікації (комутатор або WAP).

– Пристрій, що просить доступ до мережі та потребує аутентифікації – прохач або клієнт.

– Сервер аутентифікації – пристрій, який здатний аутентифікувати клієнта на підставі певних даних.

У ролі такого сервера виступає AAA-сервер, який виконує аутентифікацію, авторизацію та збір інформації про використані ресурси за відповідним протоколом [9]. (див. рисунок 1.7.).

Однією з найвідоміших реалізацій системи AAA є протокол RADIUS, який визнано стандартом у даній області. Для використання цього протоколу на сервері аутентифікації потрібно налаштувати відповідний сервер RADIUS (наприклад, Freeradius [10]). Прохач і аутентифікатор взаємодіють за допомогою протоколу EAPOL, аутентифікатор та сервер обмінюються даними через протокол транспортного рівня RADIUS (див. рисунок 1.7).

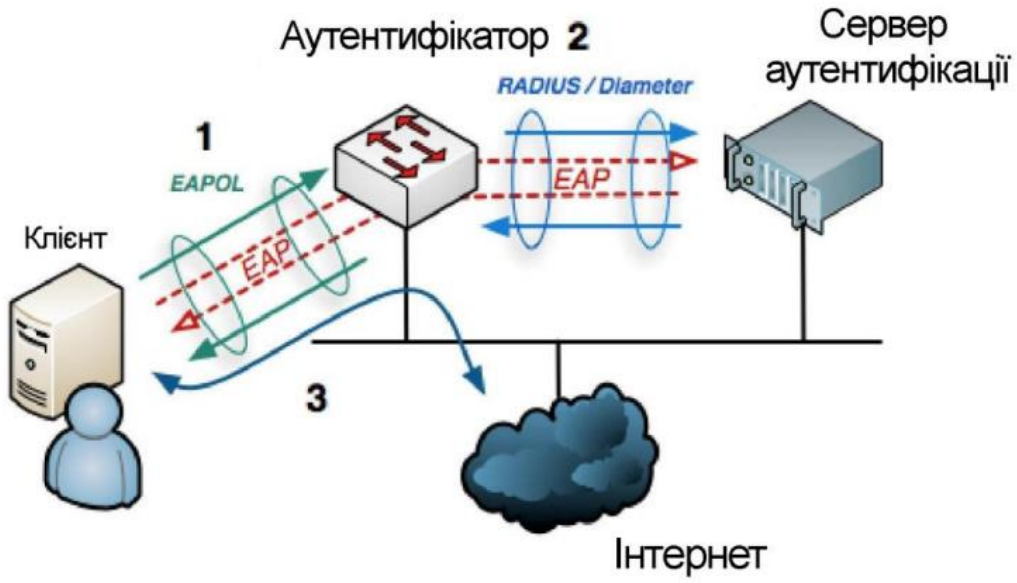


Рис. 1.7. – Структура мережі з установленою аутентифікацією згідно з протоколом 802.1X

Аутентифікатор взаємодіє з “управляючими” і “неуправляючими” портами, які є логічними (віртуальними) сутностями, проте використовують одне фізичне підключення до ЛКМ (див. рисунок 1.8.). Перед аутентифікацією доступний лише “неуправляючий” порт. Через нього дозволений лише трафік EAPOL-пакетів, а після успішної аутентифікації активується “управляючий” порт.

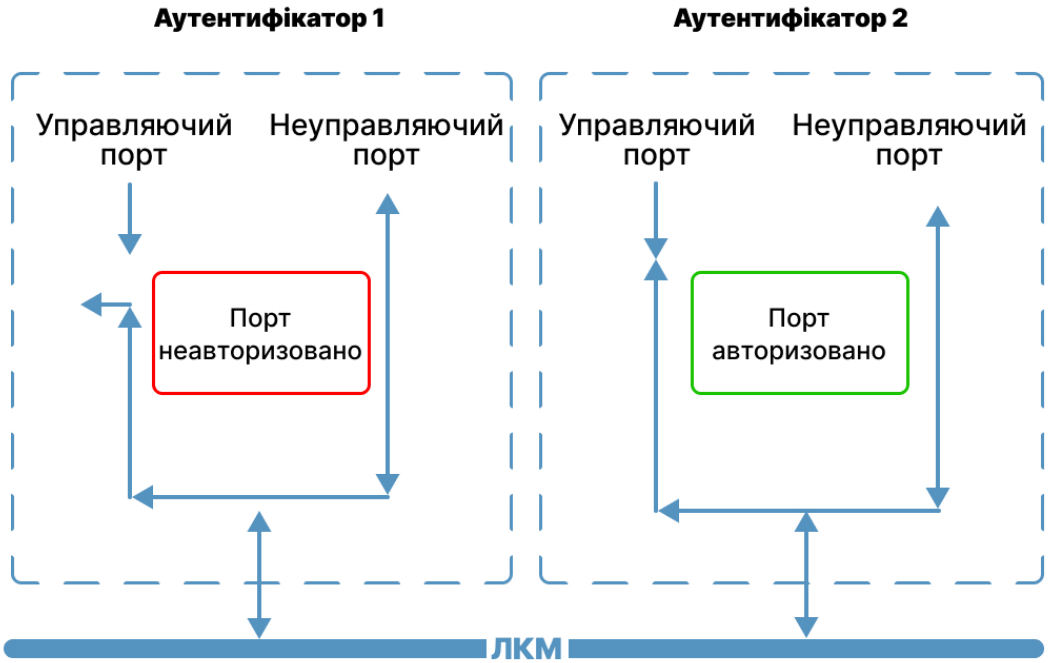


Рис.1.8. – Управляючі та неуправляючі порти

Протокол EAP представляє собою транспортний механізм, спеціально розроблений для процесів аутентифікації і не визначає конкретних методів. Цей протокол виступає в ролі фреймворку, який забезпечує безпечну передачу ключів, формати повідомлень та загальні методи, необхідні для реалізації протоколів. EAP функціонує поверх канальних протоколів, таких як PPP (Point-to-Point Protocol) або IEEE 802 (наприклад, Ethernet), і це відбувається без застосування IP [11]. Протокол має кілька основних реалізацій, описаних у стандартах IETF (у різних RFC), а також додаткові реалізації, втілені фірмами, наприклад, Cisco. Як вже було зазначено, стандарт 802.1X адаптує протокол EAP для застосування в провідних і безпровідних мережах, що дозволяє використовувати різноманітні варіації протоколу EAP для взаємної аутентифікації. Конкретні типи аутентифікації, які використовуються, визначаються компаніями, що розробляють мережеве обладнання та ПЗ. Застосування стандарту 802.1X гарантує взаємну аутентифікацію клієнтів та серверів аутентифікації у безпровідних ЛКМ [12]. Схема аутентифікації за стандартом 802.1X у безпровідних мережах представлено на рисунку 1.9.

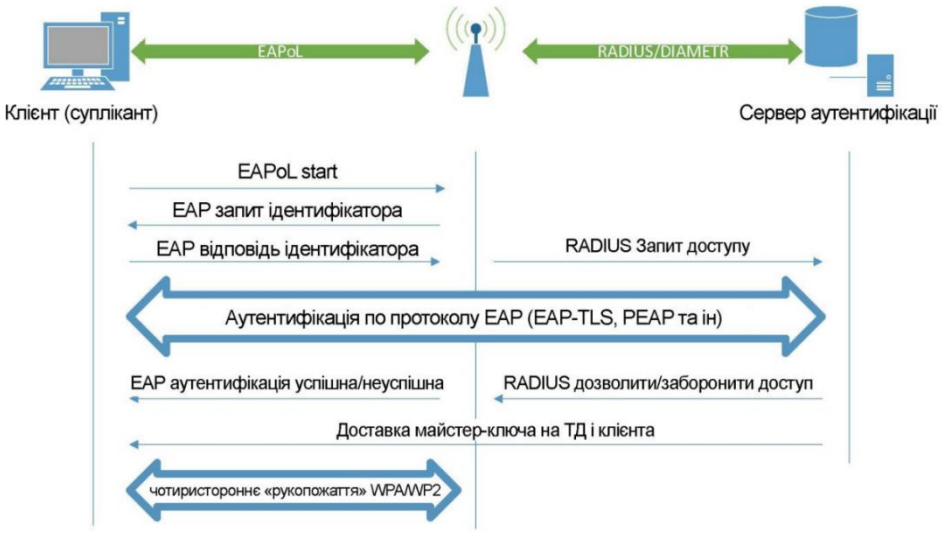


Рис. 1.9. – Аутентифікація згідно з протоколом 802.1X у безпровідних мережах

Також доступні інші варіанти рішень. Наприклад, компанія Cisco впроваджує в свої пристрої методи аутентифікації, такі як аутентифікація за MAC-адресою та CCKM аутентифікація [13].

1.4.Протоколи забезпечення безпеки в безпровідних мережах Wi-Fi

1.4.1 Протокол WEP

Протокол WEP, ухвалений IEEE в 1997 році та введений як частина стандарту 802.11 [14], вважається застарілим на сьогоднішній день і був заміщений протоколом WPA2 у 2004 році. Початково призначений для забезпечення рівня безпеки, аналогічного провідним з'єднанням, і захисту від перехоплення трафіку, він не відповів своєму завданню через концепційні недоліки. Завдяки проектним помилкам, він вразився рядом атак, і для отримання ключа та подальшого дешифрування трафіку необхідно захопити достатню кількість пакетів, використовуючи спеціальні інструменти, наприклад, aircrack-ng [15]. Процес відбору ключа займає лише кілька хвилин. Головними недоліками є коротка довжина ключа шифрування (40 або 104 біта) і використання одного ключа для шифрування всіх даних (практично це означає побітову операцію XOR із псевдовипадковим ключем).

Протокол WEP використовується як метод шифрування даних. Однак для клієнтської аутентифікації вздовж цього протоколу можуть застосовуватися дві різні стратегії: відкрита аутентифікація та аутентифікація за загальним ключем. При відкритій аутентифікації, яка була детально описана в розділі 1.2.1, клієнт не надає жодних аутентифікаційних даних для входу в мережу. Тим не менше, для подальшої взаємодії з мережею ТД, ключі WEP повинні збігтися. На рисунку 1.10. наведено схему процесу відкритої аутентифікації при застосуванні протоколу WEP.

Рис. 1.10 – Процес відкритої аутентифікації за використання протоколу WEP

У випадку аутентифікації за загальним ключем ТД починає процес, висилаючи клієнту певний текстовий рядок у відповідь на запит аутентифікації. У своїй реакції клієнт передає зашифрований текст, що містить WEP-ключі. ТД розшифровує отриманий текст, використовуючи свій WEP-ключ, і порівнює розшифрований текст зі зразком. Якщо тексти збігаються, ТД проводить аутентифікацію клієнта та дозволяє йому приєднатися до мережі [16]. Відповідна схема подана на рисунку 1.6. Важливо відзначити, що аутентифікація за загальним WEP-ключем менш безпечна, оскільки зловмисник може прослуховувати радіоканал, отримати вихідний текст від ТД та зашифрований текст від клієнта, і провести порівняння для отримання вихідного ключа [17].

1.4.2. Протоколи WPA і WPA2

Протокол WPA вирішив замінити протокол WEP у 2003 році для швидкого усунення існуючих вразливостей. Організація Wi-Fi Alliance впровадила цей перехід відзначивши терміновість закриття вразливостей. У той же період робоча група IEEE 802.11 пристосувала стандарт 802.IX до нового стандарту 802.Ш, де в 2004 році був представлений протокол WPA2. WPA2 впроваджує методи аутентифікації, керування ключами та шифрування, які були визначені як обов'язкові в стандарті 802.1 П. Основною відмінністю між протоколами WPA2 і WPA є алгоритм шифрування трафіку між клієнтом і ТД. У випадку WPA використовується алгоритм TKIP, тоді як у випадку WPA2 – це CCMP, що базується на стандарті AES (Advanced Encryption Standard). Оскільки протокол WPA2 обов'язково підтримується тими ж пристроями, що й протокол WPA з 2006 року [18], а далі буде розглянуто саме WPA2.

На відміну від протоколу WEP, WPA2 володіє як аутентифікаційними, так і шифрувальними функціями. Аутентифікація може відбуватися за допомогою одного з двох методів:

– Використання попередньо розподіленого ключа безпеки – WPA2 Personal, також відомий як режим WPA2-PSK.

– Застосування протоколу 802.IX – WPA2 Enterprise, що також ідентифікується як режим WPA2-EAP.

Перед розглядом варіантів аутентифікації важливо висвітлити різновиди ключів, які формуються під час обох процесів:

1. MSK використовується для отримання PMK.

2. PMK є основним 256-бітним ключем, що використовується для забезпечення безпеки взаємодії між ТД та клієнтом. Він випливає безпосередньо або з раніше розподіленого ключа MSK (WPA2 Personal) або через методи EAP (WPA2 Enterprise).

3. Тимчасовий парний ключ (PTK) – це 512-бітний ключ, який застосовується для аутентифікації та шифрування даних. Його визначають

через перетворення ключа PMK та інших даних за допомогою псевдовипадкової функції. PTK складається з трьох частин:

3.1. Ключ підтвердження ключа (KCK) використовується для перевірки цілісності пакетів.

3.2. Ключ шифрування ключа (KEK) використовується для шифрування групового тимчасового ключа (GTK).

3.3. TK використовується для шифрування трафіку.

На рисунку 1.11. наведено розподіл ключа PTK на вказані компоненти.

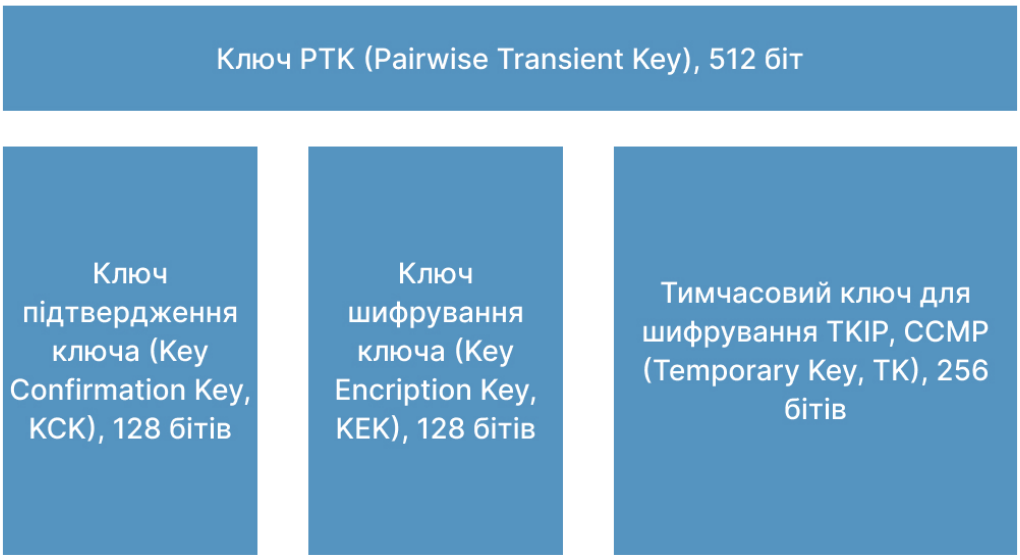


Рис. 1.11. – Складові компоненти PTK ключа

4. Майстер-ключ групи (GMK) представляє собою 256-бітний допоміжний ключ, використовуваний для отримання групового тимчасового ключа (GTK).

5. Груповий тимчасовий ключ (GTK) – це 256-бітний ключ, який використовується для шифрування широкомовного та багатоадресного трафіку, що передається від ТД до клієнтів. Він формується за допомогою перетворення групового майстер-ключа (GMK).

Режими аутентифікації відрізнятимуться у визначенні параметрів для взаємної аутентифікації та в управлінні ключем PMK. Основною метою

кожного типу аутентифікації є встановлення того, щоб ТД та безпровідний клієнт могли переконатися, що вони обидва володіють спільним парним майстер-ключем PMK. Для передачі майстер-ключа використовується протокол канального рівня EAPOL у обох методах аутентифікації.

1.4.3. WPA2 Personal

Протокол захисту WPA2 Personal спроектовано для використання в невеликих і середніх мережах, наприклад, в домашніх мережах, де кількість клієнтів невелика. За використання WPA2 Personal визначається єдиний пароль для всієї мережі, який встановлюється для ТД. Цей пароль представляє собою відкритий текст, що складається від 8 до 63 ASCII-символів. Обмеження на 63 символи введено з метою відмежування паролю від попередньо розподіленого ключа PSK, довжина якого становить 256 біт і відображається як 64 шістнадцяткових символи. У цьому випадку пароль діє як MSK. Для створення PMK на стороні клієнта та ТД пароль передається на вхід у функцію формування ключа на основі PBKDF2 пароля, яка використовує алгоритм HMAC-SHA1 для отримання хеш-значення вхідної послідовності. Функція PBKDF2 повторює обчислення хеш-значення HMAC 4096 разів, отримуючи таким чином 256-бітний PSK ключ.

Отриманий PSK ключ застосовується як PMK ключ. Після цього ініціалізується процес чотиристороннього обміну рукостисканням (див. рисунок 1.12.).

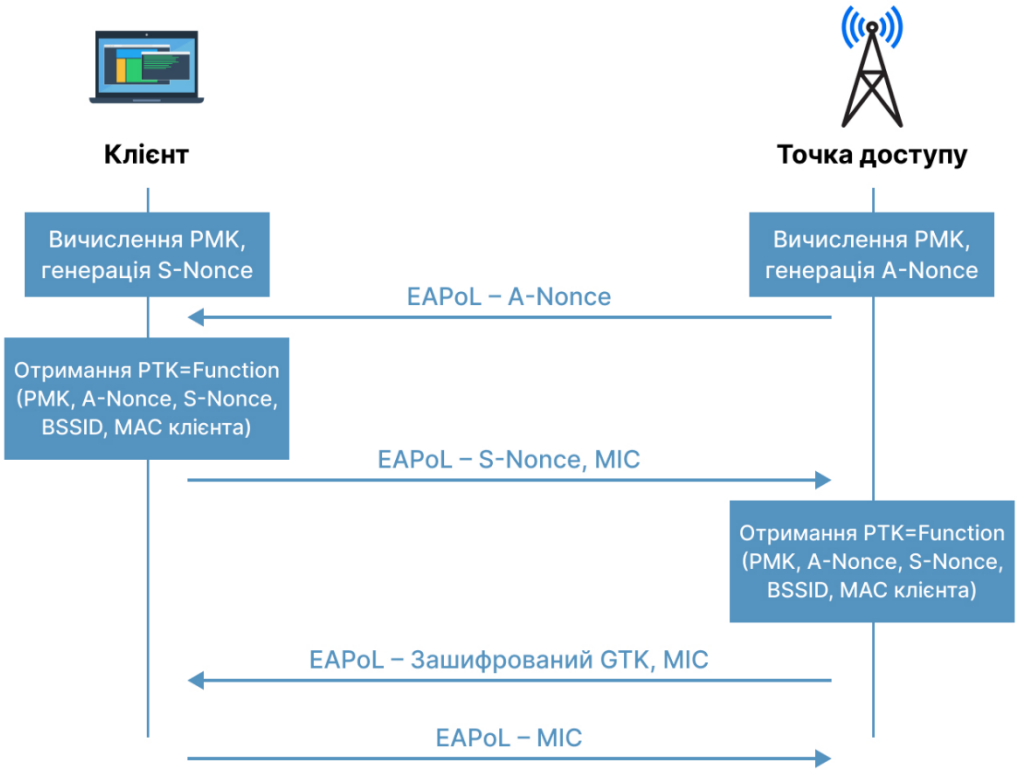


Рис. 1.12. – Схема чотиристоронього обміну рукостисканням протоколу WPA2-PSK

У початковому повідомленні ТД передає клієнту випадкову послідовність з 32 байт, відому як A-Nonce, а також MAC-адресу. У відповідь на це клієнт передає свою випадкову послідовність також з 32 байт, що називається S-Nonce, а також MIC, який додається до повідомлення для захисту від атак. Таким чином, клієнт і ТД володіють наступною інформацією: A-Nonce, PMK, основний SSID ТД (тобто її MAC-адреса) і MAC-адреса клієнта. Ці п’ять параметрів об’єднуються в рядок, який передається на вхід функції PBKDF2, і обчислюється так само, як PSK ключ. Отриманий PTK ключ має довжину 512 біт. Весь процес генерації PMK і PTK ключів наведений на рисунку 1.13.

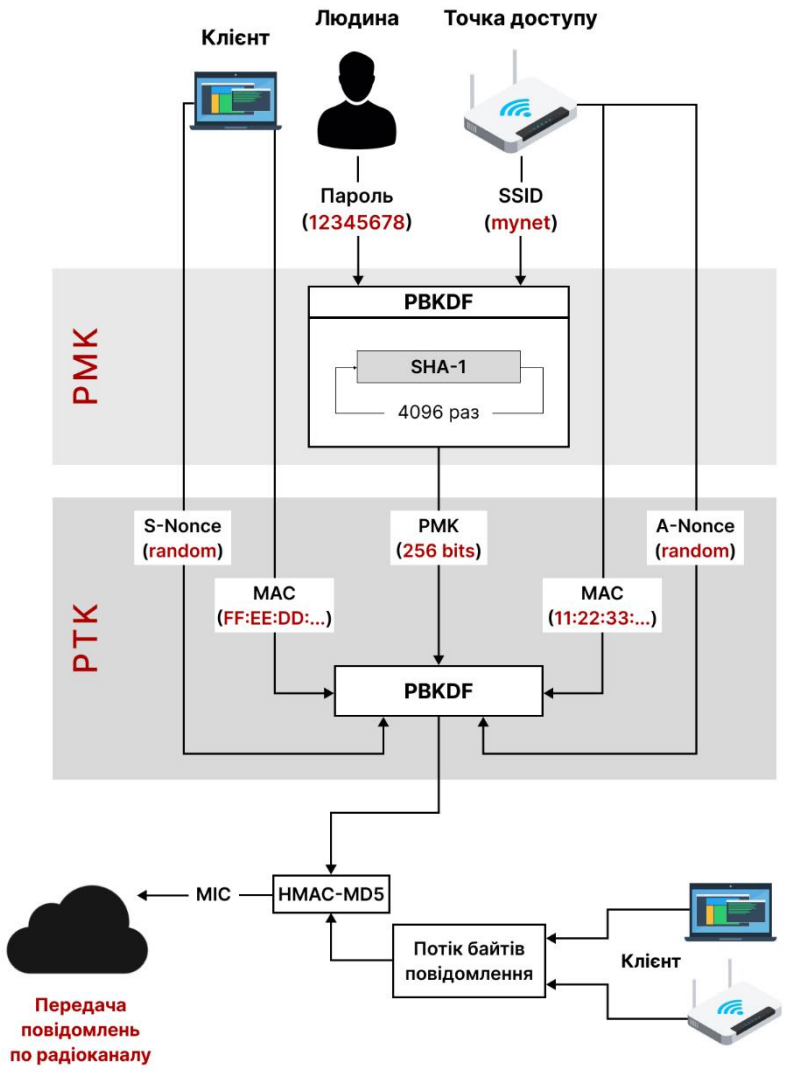


Рис. 1.13. – Процес генерації ключів PMK і PTK

GTK ключ призначений для зашифрування трафіку загального та багатоадресного спрямування від ТД до клієнтів, тому його створює та передає лише ТД. Цей ключ генерується на основі взаємного підтвердження та шифрується за допомогою KEK. У першому повідомленні ТД передає клієнту GTK ключ, зашифрований за допомогою KEK, а також MIC, що використовує KCK. Клієнт відповідає повідомленням із власним MIC. Під час початкового встановлення GTK ключа цей процес відбувається під час 4-стороннього, як наведено на рисунку 1.12.

PTK ключ застосовується для двох цілей: проведення аутентифікації та як симетричний ключ шифрування. Аутентифікація полягає в перевірці збігу

паролів. У процесі 4-етапного рукостискання, починаючи з другого етапу (тобто етапу відправлення S-Nonce клієнтом), до повідомлення додається MIC для підтвердження ідентичності. MIC обчислюється за допомогою HMAC-MD5, де ключем є PTK, що виступає соллю. Отже, PTK застосовується як для шифрування потоку даних, так і для створення контрольної суми. У випадку, якщо використовувалися однакові PTK, розшифрований MIC буде співпадати з обчисленим. В іншому випадку, якщо MIC не збігається, це вказує на використання різних PTK, що в свою чергу означає відмінність PMK і, отже, різні початкові паролі.

Після встановлення загального PTK ключа, ТД передає клієнту GTK ключ і MIC, а клієнт реагує шляхом висилання ACK повідомлення. Взаємна аутентифікація вважається успішною, якщо на кожному етапі 4-стороннього рукостискання, починаючи з другого фрейму, всі наступні рукостискання виявилися успішними [19].

1.4.4. WPA2 Enterprise

У безпровідних мережах, які використовують систему попередньо розподіленого ключа, існує важливий недолік. У випадку компрометації ключа або необхідності відкликання доступу для одного з клієнтів, необхідно змінити ключ як на стороні аутентифікатора, так і на стороні всіх клієнтів. Крім того, в разі перехоплення трафіку зловмисник має можливість здійснити офлайн-атаку для підбору пароля. Успішне одержання та захоплення 4-стороннього рукостискання між клієнтом і ТД дозволяє розшифрувати трафік клієнта мережі. Такі недоліки роблять неприйнятним застосування WPA-PSK у [20] корпоративних мережах, де може бути значна кількість клієнтів і ТД.

При застосуванні схеми аутентифікації WPA2 Enterprise процес стає більш складним і включає залучення стороннього сервера аутентифікації (див. рисунок 1.7). У порівнянні з попередньо розподіленим ключем, аутентифікація тепер відбувається відповідно до принципів стандарту 802.1X (див. п. 1.1.3.) та виконується на сервері. Протокол 802.1X, як вже було зазначено в пункті 1.1.3.,

враховує участь трьох сторін: клієнта, аутентифікатора та сервера аутентифікації.

Щодо безпровідних мереж Wi-Fi, учасником, що подає запити, є безпровідний клієнтський пристрій, тоді як ТД виступає в ролі аутентифікатора. У свою чергу, сервером аутентифікації зазвичай є RADIUS-сервер. Процес аутентифікації включає прийом ТД EAPoL-пакетів з запитами та відповідями від клієнта, які потім переадресовуються до відповідного RADIUS-сервера.

У WPA2 Enterprise, зазвичай, для аутентифікації не використовується розподілений ключ. Замість цього клієнт повинен представити особисті дані, формат яких залежить від конкретної реалізації протоколу EAP (ім’я користувача і пароль, токен, сертифікат, одноразовий пароль, тощо). RFC 4017 визначає методи, які рекомендується впроваджувати у безпровідних мережах: EAP-TLS, EAP-TTLS, PEAP, EAP-SIM [21].

Основними протоколами є EAP-MD5 і EAP-TLS. Процес EAP-MD5 включає в себе використання алгоритму MD5 для створення хеш-значення особистих даних (пароля), яке надсилається на сервер і порівнюється зі збереженим хеш-значенням. Цей метод має обмеження, оскільки забезпечує лише односторонню аутентифікацію, де тільки сервер перевіряє клієнта. Часто EAP-MD5 не використовується через ці обмеження та вразливість, оскільки аутентифікація розпочинається безпосередньо після підключення, що може піддавати атакам як клієнтів, так і мережу. Найбільш безпечним методом є EAP-TLS. Для взаємної аутентифікації використовуються x.509 сертифікати як на стороні клієнта, так і на стороні сервера. На рисунку 1.14 зображено повний процес аутентифікації методом EAP-TLS. Незважаючи на високий рівень безпеки, EAP-TLS використовується не так часто через необхідність розповсюдження сертифікатів для кожного з клієнтів.

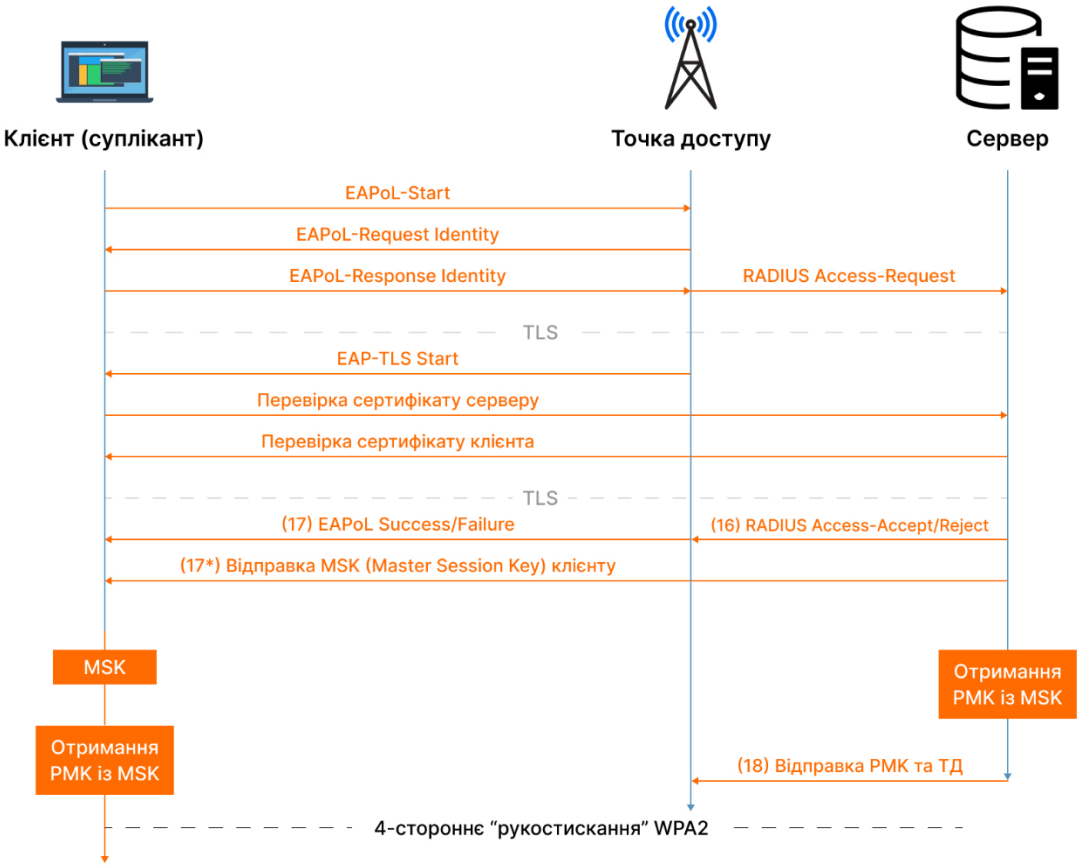


Рис. 1.14. – Аутентифікація EAP-TLS

З метою поєднання зручності аутентифікації клієнтів за особистими даними та забезпечення безпеки, були розроблені тунельні методи PEAP (Protected EAP, захищений EAP) і EAP-TTLS (Tunneled TLS, тунельований TLS) як розширення методу EAP-TLS. Обидва методи використовують EAP-TLS для аутентифікації лише сервера та встановлюють захищене TLS-з'єднання між клієнтом і сервером, використовуючи x.509 сертифікат сервера, аналогічно до механізму встановлення https-з'єднань. Клієнт спочатку переконується у валідності сертифіката сервера, після чого використовуються "внутрішні методи" для аутентифікації клієнтів.

Основна відмінність між методами EAP-TTLS і PEAP полягає і їхній внутрішній структурі. У PEAP можуть використовуватися такі "внутрішні методи", як EAP-MSCHAPv2 (який передає зашифрований пароль та підтримується виключно Microsoft), EAP-GTC (передається одноразовий

пароль та підтримується виключно Cisco), EAP-TLS (передається сертифікат клієнта та підтримується виключно Microsoft). З іншого боку, EAP-TTLS підтримує різні застарілі методи, такі як PAP, CHAP і інші, внаслідок його ранньої розробки. Фактично EAP-TTLS і PEAP ідентичні за суттю, проте перший був створений компаніями Certicom та Software Funk, тоді як PEAP є спільним продуктом Cisco та Microsoft. Завдяки активній маркетинговій кампанії останніх, PEAP став найбільш поширеним протоколом [22].

Графічне порівняння тунельованих і базових методів аутентифікації наведено на рисунку 1.15.

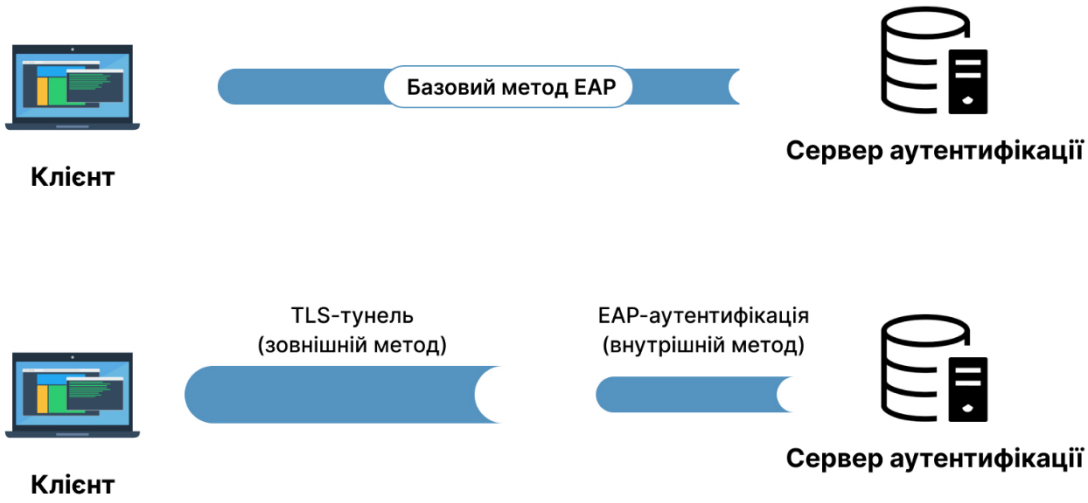


Рис. 1.15. – Порівняння методів аутентифікації з використанням тунелювання та базового підходу

Після успішної аутентифікації між клієнтом і сервером, наступним кроком є встановлення сеансових ключів. Для кожного користувача та кожної окремої сесії генеруються унікальні ключі для підвищення рівня безпеки. В залежності від використаного методу EAP, PMK ключ може бути обчислений або на клієнтський і серверній стороні, або лише на стороні сервера аутентифікації, після чого передається на клієнтську сторону через захищений канал. Сервер отримує AAA ключ розміром 512 біт, відомий як MSK, який обчислюється на основі даних, отриманих під час аутентифікації через

протокол EAP. Наприклад, при використанні EAP-TLS, ключ встановлюється так: після аутентифікації клієнт генерує PMK, який шифрує на відкритому ключі сервера та відправляє йому. PMK, секретний рядок, випадковий рядок клієнта та випадковий рядок сервера, застосовуючи псевдовипадкову функцію TLS-PRF, перетворюються в AAA ключ. PMK ключ, який є першими 256 бітами AAA ключа, подальше передається сервером на ТД [23]. Після цього ініціюється 4-стороннє рукостискання, аналогічне WPA2 Personal.

1.4.5. Процес підключення до WAP

Для установлення з'єднання з мережею стандарту 802.11, обслугованою ТД, клієнт повинен спочатку визначити її на одному з 14 каналів. Існують два можливі варіанти сканування каналів для виявлення мережі [24]:

1. Пасивний режим: пристрій слухає всі канали на наявність пакетів-маяків (Beacon-фреймів). ТД періодично розсилає Beacon-фрейми, що вказують на її присутність (див. рисунок 1.16, а). У цих фреймах міститься інформація про підтримувані швидкості, канали, алгоритми шифрування, керування ключами, тощо. Клієнт періодично сканує радіочастотний діапазон для виявлення Beacon-фреймів та прийняття рішення щодо оптимального підключення [25]. Цей метод є неефективним і має недоліки, такі як можливість пропуску Beacon-фрейму, якщо час очікування на якомусь каналі обмежений [26].

2. Активний режим: пристрій також сканує кожен канал, але не очікує Beacon-фреймів. Сканування відбувається за допомогою Probe-запитів для отримання інформації про ТД. Ці запити розсилаються на широкомовний MAC-адрес з нульовим SSID (рис. 1.16, б). У пакеті Probe-запиту може бути вказаний SSID мережі. ТД отримує Probe-запит, перевіряє, чи є хоча б одна сумісна з нею швидкість передачі, і відповідає Probe-відповіддю, яка містить інформацію, аналогічну тій у Beacon-фреймах (SSID, підтримувані швидкості передачі, тощо). Після отримання клієнтом широкомовного Probe-запиту, він вибирає ту мережу із всіх Probe-відповідей, яка найбільше відповідає його налаштуванням.

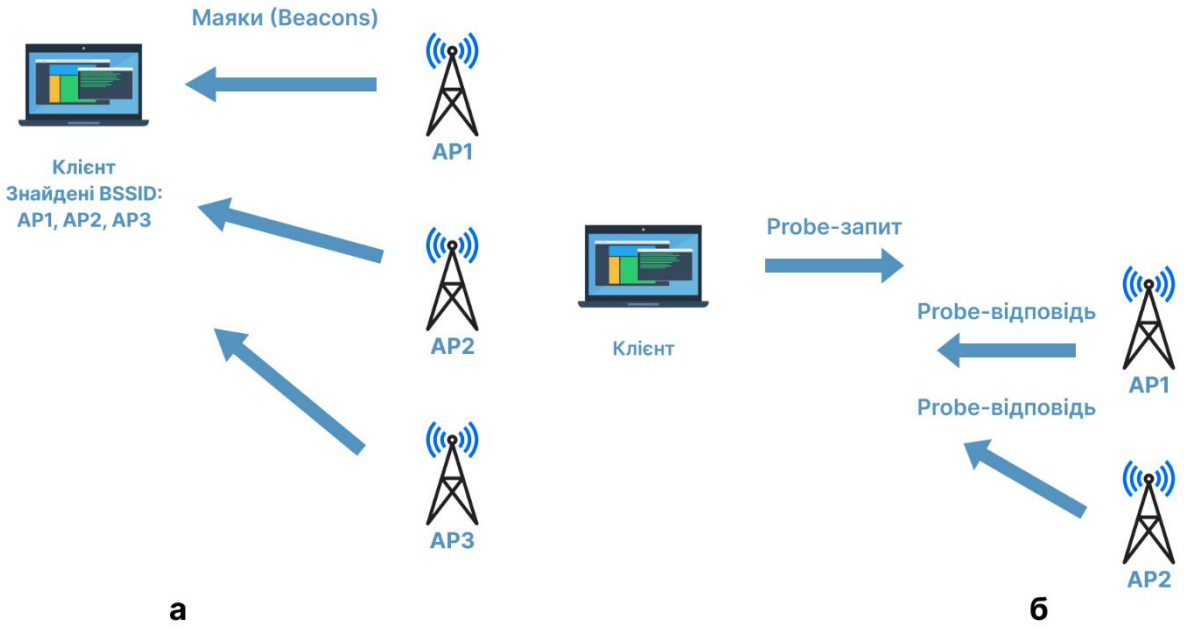


Рис. 1.16. – Пасивний (а) та активний (б) режим сканування мережі Wi-Fi

Після виявлення мережі відбувається взаємодія через обмін пакетами аутентифікації та асоціації з обраною ТД (див. рисунок 1.17). Пакети аутентифікації забезпечують низькорівневу аутентифікацію на рівні протоколу 802.11, тобто на канальному рівні. Цей вид аутентифікації відрізняється від аутентифікації за стандартом 802.1X та протоколом WPA2, які починають діяти лише після того, як клієнт пройшов аутентифікацію та асоціювався за протоколом 802.11. Первісно аутентифікація 802.11 була розроблена для протоколу WEP, але, як зазначено в розділі 1.2.1, протокол WEP був визнаний як небезпечний і застарілий. У зв’язку з цим у пакеті аутентифікації майже завжди встановлюється тип 0, що означає відкриту аутентифікацію, і вона завершується успішно. У випадку, якщо ТД отримує від неаутентифікованого клієнта пакети, відмінні від аутентифікації або Probe-запитів, вона висилає клієнту пакет деаутентифікації, переводячи клієнта в стан неаутентифікованого та неасоційованого. Аутентифікація 802.11 дозволяє клієнту аутентифікуватися в багатьох ТД, що спрощує роумінг та подальшу асоціацію з ними, оскільки клієнт може бути асоційований тільки з однією ТД. Запит на асоціацію містить

обрані типи шифрування, якщо вони необхідні, а також інші дані 802.11, необхідні для сумісності. Якщо ТД отримує від авторизованого клієнта, але неасоційованого, пакети, відмінні від асоціації, то вона висилає клієнту пакет дісоціації, переводячи клієнта в стан авторизованого, але неасоційованого. Після успішного завершення процесів аутентифікації та асоціації 802.11 ТД створює ідентифікатор асоціації для даного клієнта [27].

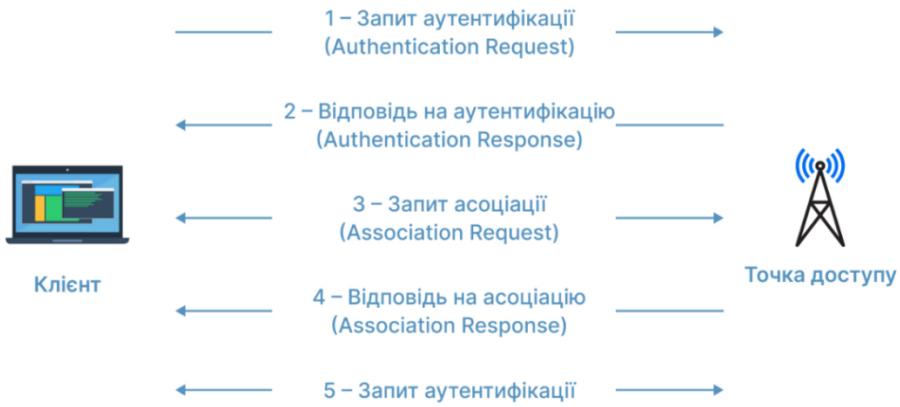


Рис. 1.17. – Процес аутентифікації та асоціації у безпровідних мережах

Лише після цього розпочинаються процеси аутентифікації та створення динамічних WPA2/802.1X ключів. На рисунку 1.18 наведено послідовність обміну пакетами у випадку аутентифікації за стандартом WPA2.

D-LinkIn_e1:7b:d0	Apple_2e:9c:62	802.11	167	Probe Response, SN=156, FN=0, Flags=........
Apple_2e:9c:62	D-LinkIn_e1:7b:d0	802.11	41	Authentication, SN=841, FN=0, Flags=........
D-LinkIn_e1:7b:d0	Apple_2e:9c:62	802.11	30	Authentication, SN=157, FN=0, Flags=........
Apple_2e:9c:62	D-LinkIn_e1:7b:d0	802.11	107	Association Request, SN=842, FN=0, Flags=...
D-LinkIn_e1:7b:d0	Apple_2e:9c:62	802.11	81	Association Response, SN=158, FN=0, Flags=..
D-LinkIn_e1:7b:d0	Apple_2e:9c:62	EAPOL	133	Key (Message 1 of 4)
Apple_2e:9c:62	D-LinkIn_e1:7b:d0	EAPOL	155	Key (Message 2 of 4)
D-LinkIn_e1:7b:d0	Apple_2e:9c:62	EAPOL	195	Key (Message 3 of 4)
Apple_2e:9c:62	D-LinkIn_e1:7b:d0	EAPOL	133	Key (Message 4 of 4)

Рис. 1.18. – Послідовність обміну пакетами між клієнтом і ТД Wi-Fi при наступній аутентифікації та формуванні ключі за протоколом WPA2

1.5. Обґрунтування методів захисту мережі

Всі наявні заходи захисту від атаки ФТД можна класифікувати залежно від того, на якому рівні взаємодії використовуються ці заходи, а саме на рівні клієнта чи мережі.

1.5.1. Розгляд атаки підробленої точки доступу

У вищезгаданих протоколах безпеки для Wi-Fi мереж використовуються різноманітні методи аутентифікації. Проте жоден із цих методів не враховує можливість аутентифікації клієнтом ТД, що утворює простір для атак типу “підроблена ТД (англ. Rogue Access Point)”. Залежно від вибраного протоколу та методу аутентифікації ця атака може мати критичне значення.

Rogue Access Point атака виконується наступним чином: зловмисник отримує інформацію про ТД до якої клієнт раніше приєднувався, і формує ідентичну ТД з аналогічними налаштуваннями (див. рисунок 1.19). Залежно від протоколу безпеки, який використовується для аутентифікації в мережі, зловмиснику потрібно визначити та сконфігурувати відповідні параметри. Далі зловмисник намагається відключити клієнта від поточної ТД (якщо він не підключений) або просто намагається підключити клієнта до своєї підробленої мережі.

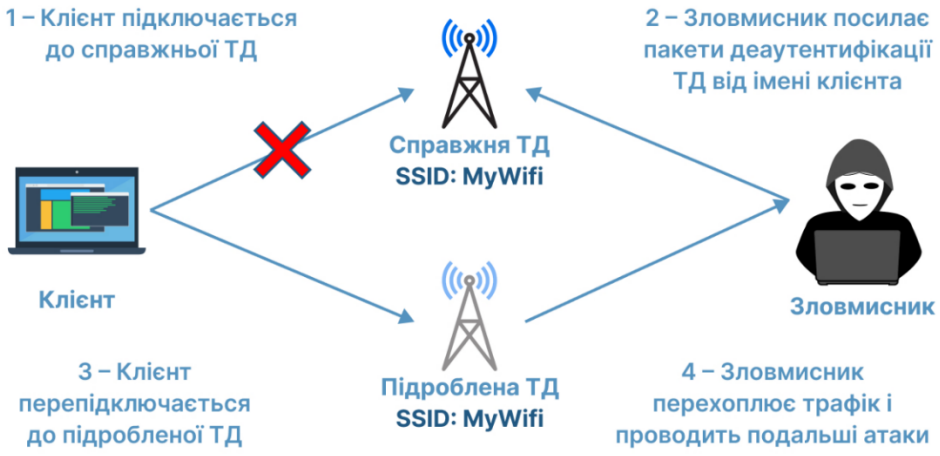


Рис. 1.19. – Принцип імітації Rogue Access Point атаки

Існує декілька можливих сценаріїв:

1. Клієнт у даний момент підключений до певної Wi-Fi мережі, і атакуючий намагається незаконно підключити його до ТД, яка обслуговує ту ж саму мережу.

2. Клієнт знаходиться в режимі підключення до однієї Wi-Fi мережі, тоді як зловмисник створює ФТД, намагаючись привести його в оману.

3. Клієнт не має активного з'єднання з будь-якою Wi-Fi мережею.

4. Використання методу перебору публічно доступних відомих ТД.

В залежності від конкретного сценарію, зловмисник повинен виконати додаткові дії. У випадку, коли клієнт не знаходиться в жодній з мереж, атакуючому достатньо налаштувати мережі, до яких клієнт раніше підключався, для того щоб процес підключення став прозорим для потенційної жертви. У двох інших випадках у зловмисника є два можливі варіанти підключення клієнта до його ФТД:

1. Відправка пакетів, які містять дані для аутентифікації, клієнту.

2. Здійснення DoS-атаки на ТД.

У будь-якому випадку ФТД має мати сильніший сигнал, ніж оригінальна, щоб привернути увагу потенційної жертви. В іншому випадку, при спробі повторного асоціювання клієнт автоматично підключиться до правомірної ТД. Після успішного підключення жертви до ФТД, зловмиснику необхідно відтворити автентичні умови, щоб переконати клієнта в його легітимності.

У відкритих мережах це завдання вважається досить простим, оскільки вони не вимагають жодного процесу аутентифікації, і достатньо представити клієнтові правомірний SSID ідентифікатор.

При підключенні до загальнодоступної мережі клієнт стає особливо вразливим у порівнянні з іншими методами аутентифікації. У випадку мереж, що використовують протокол WEP та здійснюють аутентифікацію на основі пакетів 802.11 (див. розділ 1.3.), зловмисникові потрібно знати загальний ключ. Як вже було зазначено у розділі 1.1.2., WEP протокол визнано небезпечним через можливість відновлення загального ключа шляхом аналізу перехоплених

мережних пакетів за короткий проміжок часу, використовуючи відповідне ПЗ, для прикладу, aircrack-ng. Таким чином, захист, який забезпечується WEP протоколом, малоефективний в порівнянні з захистом у загальнодоступних мережах, і таку мережу можна відносно легко піддати атакам.

У безпечних мережах, що використовують WPA/WPA2 протокол, зламати захист і успішно пройти аутентифікацію є значно важке завдання. У випадку WPA2 Personal, зловмисник повинен мати інформацію про MAC-адресу ТД (BSSID), SSID і PSK. Для отримання PSK ключа, тобто пароля до мережі, зловмисник повинен зафіксувати процедуру 4-стороннього рукостискання. Проте, складність вгадування пароля прямо залежить від його довжини. Зазвичай використовуються словники або генератори паролів для вгадування. Таким чином, значно складніше вгадати пароль, який складається з 16 унікальних символів, ніж пароль з 8 повторюваних символів. У таблиці 1.1 наведено статистику вгадування WPA2-PSK паролю за допомогою 8 відеокарт AMD 290X зі швидкістю приблизно 1,5 млн WPA-паролів за секунду (в порівнянні зі швидкістю вгадування 94 млрд MD5-хешів за секунду) та на 4-ядерному процесорі Intel Core-i7 3840QM із тактовою частотою 3,8 ГГц із швидкістю вгадування 4800 WPA-паролів за секунду [28].

Таблиця 1.1

Залежність часу перебору WPA-PSK паролів від їхньої довжини та складу

Склад пароля	Час, необхідний для перебору всіх можливих значень	
	Intel Core-i7 3.8 ГГц	AMD 290X
Пароль із 8 літер латинського алфавіту	268 / (4700 * 3600 * 24) = 514 днів	268 / (1500000 * 3600) = 38.7 годин
Пароль із 10 цифр	1010 / (4700 * 3600 * 24) = 24.6 дня	1010 / (1500000 * 3600) = 2 години

Продовження таблиці 1.1

Пароль із 10 літер латинського алфавіту	2610 / (4700 * 3600 * 24 * 365) = 952 років	2610 / (1500000 * 3600 * 24 * 365) = 3 роки
Пароль із 12 цифр	1012 / (4700 * 3600 * 24 * 365) = 6.7 років	1012 / (1500000 * 3600 * 24) = 7.7 днів
Пароль із 14 цифр	1014 / (4700 * 3600 * 24 * 365) = 674.6 років	1014 / (1500000 * 3600 * 24 * 365) = 2.1 років

З цього випливає, що при достатній довжині пароля немає сенсу вести спроби вгадування, оскільки ймовірність успіху дуже низька. Тим не менш, адміністратори часто залишають паролі за замовчуванням або встановлюють їх короткими для зручності запам’ятовування. У відкритих мережах паролі можуть надаватися обслуговуючим персоналом за запитанням клієнта. Це вказує на те, що в певних умовах загальний пароль WPA2-PSK може бути вразливим. У випадку виявлення атак або визначення, що один із користувачів внутрішньої мережі є зловмисником, і здійснює атаки, існують два можливих варіанти обмеження доступу: обмеження за MAC-адресою або зміна ключа для всієї мережі WPA2-PSK. Проте MAC-адреси можна змінювати на різних ОС (особливо на ОС сімейства Linux, якими часто користуються зловмисники), і зміна ключа для всієї мережі WPA2-PSK може призвести до складнощів через потребу в його розповсюдженні серед користувачів.

У сценарії WPA2 Enterprise, де аутентифікація базується на протоколі EAP, безпека з’єднання залежить від вибраного методу аутентифікації між клієнтом і сервером Radius, а також від правильності конфігурації аутентифікації як на сервері, так і на клієнтському пристрої. Зазначені у пункті 1.2.2 методи EAP-TLS, PEAP, EAP-TTLS використовують сертифікати на стороні сервера (EAP-TLS також на стороні клієнта). За винятком інфраструктурних вразливостей, пов’язаних з роботою TLS (наприклад, злам

центру сертифікації, використання слабких алгоритмів генерації ключів, втрата ЗК через шкідливе ПЗ на сервері, тощо), для успішної атаки ФТД необхідно, окрім самої ТД, сконфігурувати підроблений сервер аутентифікації, в який необхідно внести сертифікат TLS. Якщо неможливо отримати сертифікат та ЗК справжнього сервера аутентифікації, зловмисник може використовувати або власний завірений сертифікат, який неможливо перевірити, або дійсний сертифікат, який може розкрити його справжню ідентичність. У разі завіреного сертифіката, при правильній конфігурації клієнт буде попереджений про те (див. рисунок 1.20), що неможливо перевірити валідність сертифіката, і користувач повинен буде вирішити, чи довіряти серверу аутентифікації. Отже, успіх атаки значною мірою залежить від фактору людського втручання. В даному випадку зловмисник може тільки сподіватися, що користувач прийме підроблений сертифікат, що сприяє той факт, що багато організацій встановлюють довірені сертифікати. Зокрема, за відсутності недоліків методів EAP на основі TLS, існує низка інших методів, використання яких підвищує ймовірність успішної атаки.

Для прикладу, було виявлено, що метод LEAP має слабкість у відношенні до атаки на перебір паролів, особливо при використанні його в автономному режимі.

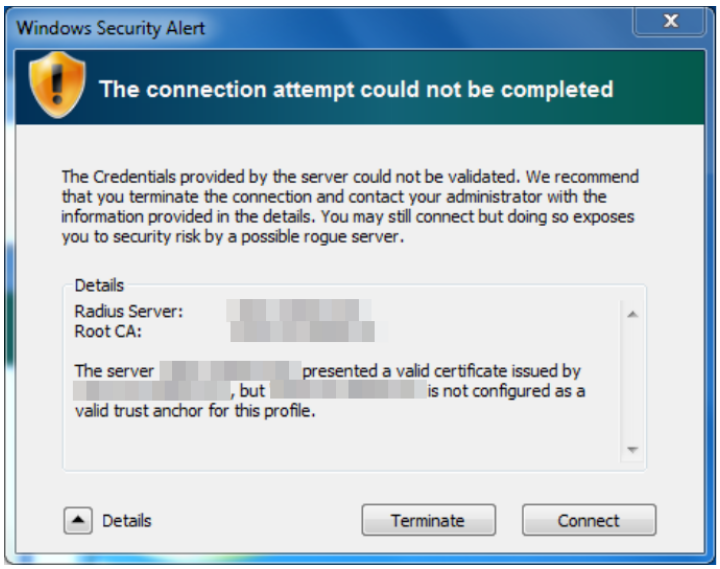


Рис. 1.20. – Сповіщення користувача щодо неможливості верифікації автентичності сертифіката сервера в ОС Windows

У випадку успішного з’єднання клієнта з ФТД, зловмиснику відкривається можливість виконання Man-in-the-middle атак. Приклади реалізації таких атак можуть бути наступні:

1. Захоплення трафіку, включаючи використання сторонніх утиліт, які уникають захисту жертви. Наприклад, атака sslstrip, що використовує однойменну утиліту. Зловмисник обходить HSTS та SSL-трафік.

2. Різні форми підмін (ARP, DNS і інші) та атаки (DoS, DHCP, тощо).

3. Сканування конкретних хостів мережі для подальших атак.

4. Таким чином, існує загроза успішного виконання атаки ФТД на клієнтські пристрої у випадку відсутності або неправильному використанні більшості протоколів безпеки Wi-Fi та їх типів. Складність створення ФТД в конкретній мережі залежить від використовуваного протоколу безпеки, що забезпечує аутентифікацію в даній мережі. Однак, якщо користувач коли-небудь підключався до мережі, в якій захист був наданий неправильно або взагалі відсутній, і якщо зловмисник володіє параметрами безпеки однієї з мереж, до якої клієнт підключався, це збільшує ймовірність успішної атаки ФТД.

1.5.2. Захисні заходи на рівні мережі

У відкритих та персональних мережах цей метод безпеки, як правило, не використовується, але знаходить успішне застосування у корпоративних мережах. Різні виробники, такі як Cisco, Tp-link, Zyxel, Aruba та інші, вбудовують в свої пристрої підтримку виявлення, запобігання та захисту від ФТД.

У корпоративних мережах можна виділити два сценарії використання ФТД. У першому випадку ФТД працює як незалежний вузол мережі (див. рисунок 1.21, а), у другому вона підключається безпосередньо до комутатора або контролера LAN (див. рисунок 1.21, б). Іноді такі ТД відомі як інтерферуючі.

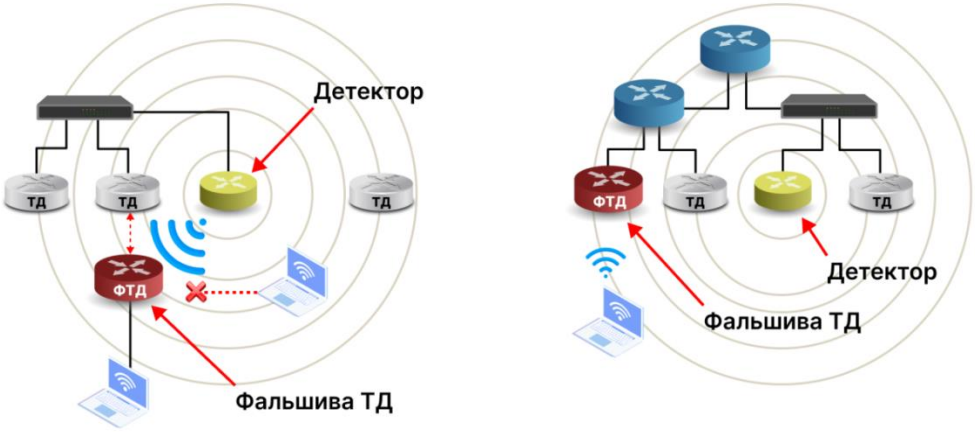


Рис. 1.21. – Розгляд можливих сценаріїв встановлення ФТД в корпоративних мережах: а – сценарій, коли ФТД є автономною; б – сценарій, де ФТД підключена до внутрішньої мережі

У простій конфігурації контролера безпровідної мережі встановлюються списки довірених ТД, базуючись на їхніх MAC-адресах, тоді як всі інші автоматично вважаються недовіреними. Далі адміністратор самостійно вживає заходів безпеки на основі виявлених недовірених ТД. Більш продуктивним вирішенням є конфігурація однієї з ТД у режимі моніторингу, де вона сканує радіочастотний спектр і виявляє підозрілі ТД. Якщо ФТД не підключена до LAN, детектор заважає її роботі, наприклад, висиланням широкомовних пакетів, щоб унеможливити підключення клієнтів до ФТД (див. рисунок 1.22, а). У випадку з’єднання за допомогою провідного підключення виникає можливість призупинити її функціонування через відключення порту комутатора (див. рисунок 1.22. б).

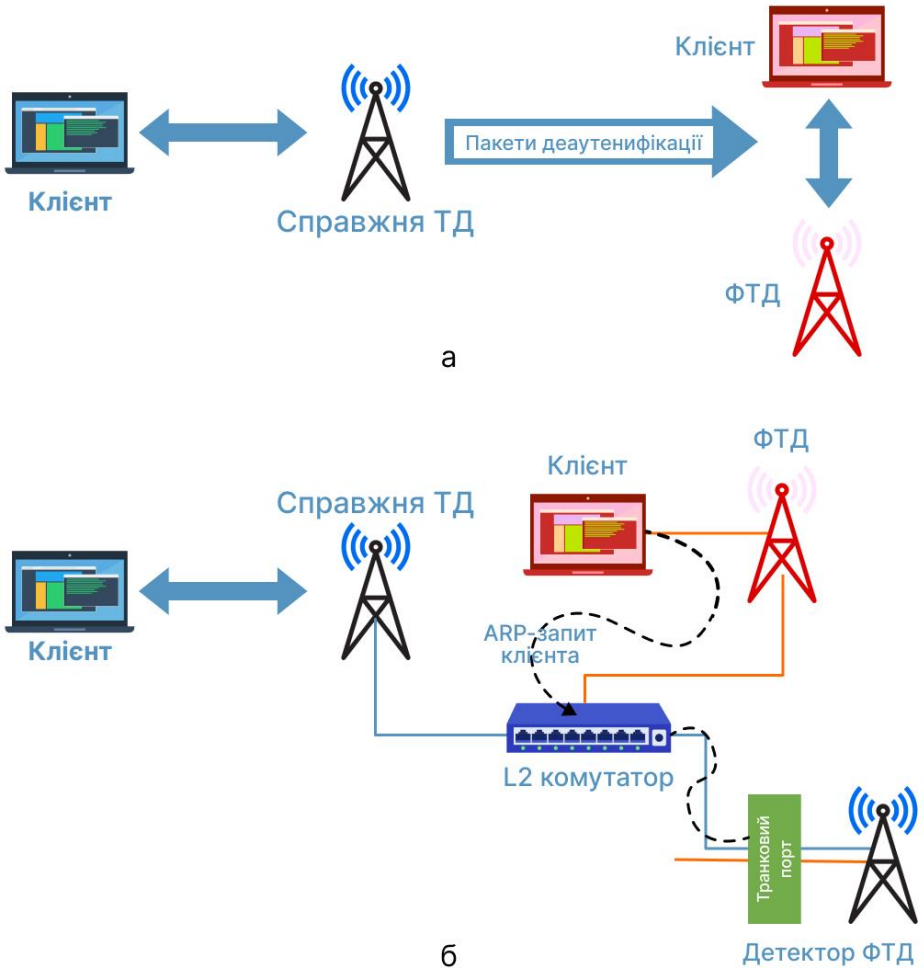


Рис. 1.22. – Заходи захисту від ФТД: а – ФТД непідключена до провідної мережі; б – ФТД підключена до провідної мережі

На сьогоднішній день Cisco володіє передовими технологіями у сфері безпеки безпровідних з’єднань, особливу увагу приділяючи технології WIPS (Wireless Intrusion Prevention System), яка включає в себе виявлення ФТД [29]. Визначення того, чи є ТД фальшивою, та її критичність базуються на SSID, який вона транслює, інформації про з’єднання точки з провідною мережею, а також на списках і статистиці, яку зберігає спеціальна станція (Cisco Prime Infrastructure, CPI) для уникнення помилок першого роду. Процес керування ФТД складається з трьох етапів:

1. Виявлення.

Спеціальна ТД переводиться в режим моніторингу, скануючи ефір для збору даних, таких як SSID, MAC-адреси точки та її клієнтів, IP-адреси, канали тощо. Отримані дані передаються контролеру.

2. Класифікація.

Точки-детектори намагаються відповідати даним про ФТД, отримані через безпровідний канал, з тими, які отримані через провідний канал. Їх розташовують на транковому порту для прослуховування всього провідного трафіку з усіх VLAN. Якщо MAC-адреса ФТД або одного з її клієнтів виявлено в провідній мережі, точка розглядається як критична. Крім того, Cisco винайшла протокол RLDP, який допомагає визначити, чи підключена ФТД до провідної мережі, підключаючись до неї як клієнт і висилаючи дані через протокол RLDP на CPI.

3. Усунення.

Визначається місцезнаходження ТД, встановлюються перешкоди та відключаються порти.

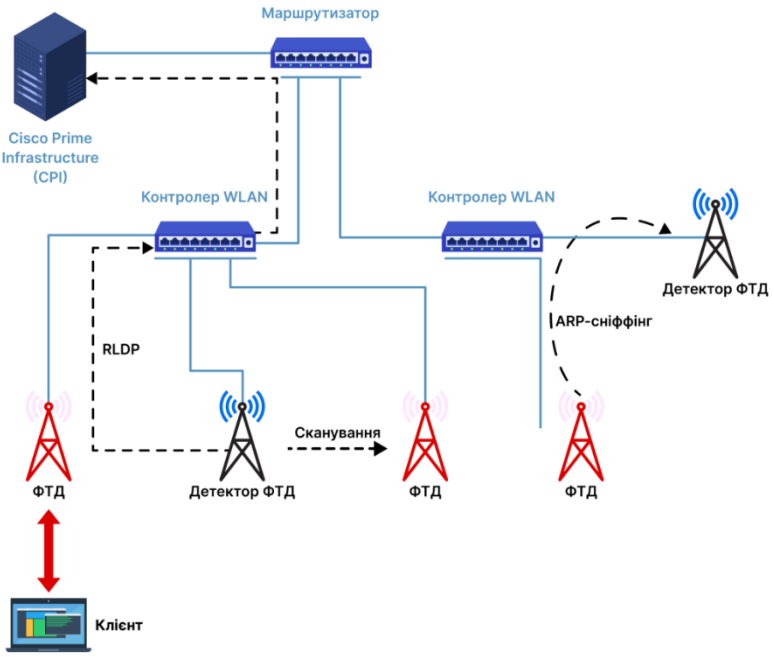


Рис. 1.23. – Технології виявлення ФТД компанією Cisco

На рисунку 1.23. представлені всі застосовувані технології Cisco для виявлення ФТД у LAN.

1.5.3. Захисні заходи на рівні клієнта

Клієнтський пристрій може застосовувати два методи захисту від атаки ФТД: запобігання його підключенню або захист його від такого підключення. Щодо захисту від підключення до ФТД, користувач може вжити наступних заходів:

– Відключення автоматичних підключень до мереж Wi-Fi. Ця функція активується по-різному в залежності від ОС. Зазвичай це налаштування застосовується окремо для кожної мережі, до якої пристрій може підключатися. Наприклад, в iOS користувач повинен вручну натискати “Забути цю мережу”, щоб вимкнути автоматичне підключення. У Windows це налаштовується через “Панель керування” (для версій до Windows 10) або через “Параметри мережі” (в Windows 10/11). Аналогічні дії виконуються для вимкнення автоматичного підключення й в інших ОС. На рисунку 1.24. наведено, як ця функція працює в iOS 9 (рисунок 1.24. а) і Windows 10 (рисунок 1.24. б).

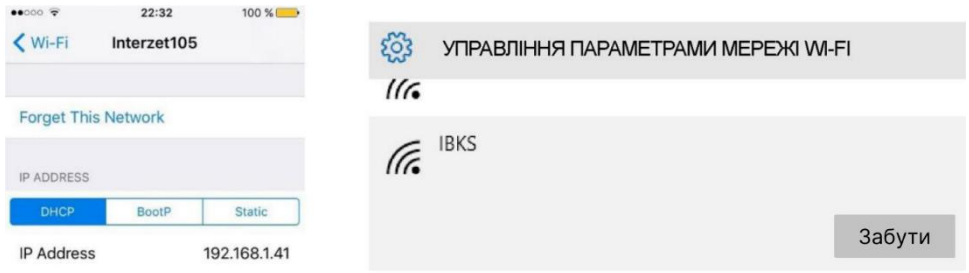


Рис. 1.24. – Вимкнення автоматичного з’єднання в ОС iOS (а) та ОС Windows 10 (б)

– Активація фільтрації з’єднань через ПЗ. Наприклад, в ОС Windows цю конфігурацію можна налаштувати за допомогою вбудованого інструменту netsh:

```
netsh wlan add filter permission=block ssid=WLAN
networktype=infrastructure
```

В ОС Linux аналогічні налаштування можна здійснити за допомогою вбудованого інструменту iptables, проте можливість блокування обмежена лише за MAC-адресами:

```
Iptabes –A INPUT –m mac –mac-source <MAC> -j DROP
```

– Застосування інших програмних засобів. Наприклад, інструменти, які надають можливість самостійно визначати сумнівні ТД. Один із таких інструментів – Waidps [30], розроблений на мові програмування Python і спрямований на виявлення атак та проведення аудиту ТД. Його функціонал включає визначення та повідомлення користувача у кількох сценаріях:

1. Виявлення ТД із однаковим SSID (ESSID), що може свідчити про атаку ФТД.

2. Реєстрація потоку пакетів деаутентифікації, що може свідчити про те, що зловмисник намагається відключити клієнта і перепідключити його до свого контрольованого пристрою.

3. Виявлення того, що пристрій клієнта перепідключився до іншої ТД, що вказує на проведення процедури переасоціації.

Іншим прикладом зовнішніх інструментів, використовуваних для виявлення ФТД, є Evilapdefender [31], яка спроможна виявити недостовірні ТД за декількома параметрами:

– Однаковий SSID, але інша адреса BSSID.

– Той самий SSID, але різні атрибути (канал, метод шифрування, протокол і аутентифікація).

– Однаковий SSID і атрибути, але різні параметри, що передаються у beacon-фреймах.

Покрім інструментів, які використовуються для виявлення ФТД, можна використовувати програми, такі як Smart Wi-Fi Toggler [32]. Це ПЗ дозволяє

пристроям з ОС Android 2.3 і новішими версіями автоматично включати та вимикати безпровідний адаптер в залежності від географічного положення пристрою. Проте цей метод може захистити від ФТД лише в тих місцях, які користувач не визначив як зони підключення до Wi-Fi, що створює можливість для атак в районах, таких як дім чи робоче місце.

– Підключатися тільки до мереж, що захищені протоколами EAP, і уникати підключення до мереж, сертифікати яких не є довіреними.

– Вимикати безпровідний адаптер. Цей метод є найбільш радикальним, але водночас найбільш ефективним.

Ці методи вважаються запобіжними. Крім цього, користувач може захищати свої дані після встановлення з'єднання з ТД. Такі заходи схожі на ті, які використовуються для забезпечення конфіденційності та цілісності особистих даних. Один із основних та універсальних методів захисту полягає у використанні VPN-з'єднань. Покрім захисту на рівні мережі та каналу, безпеку даних можна підняти на більш високий рівень за допомогою протоколу TLS, тобто використовувати виключно HTTPS-з'єднання. З цією метою Electronic Frontier Foundation, спільно з The Tor Project, розробила розширення "HTTPS Everywhere" [33] для браузерів, таких як Chrome, Opera, Firefox, яке вимагає, щоб всі запити до веб-ресурсів виконувалися лише через захищене з'єднання.

Усі розглянуті вище методи захисту від ФТД вирішують вказану проблему, але вони або не є універсальними, або мають специфічне призначення, що може ускладнити їх використання. Наприклад, може статися відключення автоматичного з'єднання з відомими мережами або потреба використання платних VPN-сервісів. Деякі компанії обмежують швидкість і обсяг дозволеного трафіку. В цьому контексті виникає потреба в розробці та впровадженні методу захисту від ФТД, який спеціально спрямований на вирішення цієї конкретної проблеми та успішно з нею впорається.

1.6. Висновок до першого розділу

В першому розділі кваліфікаційної роботи освітнього рівня “Магістр”:

– Розглянуто питання аутентифікації в безпровідних мережах Wi-Fi; Проведено аналіз існуючих протоколів безпеки, які застосовуються в мережах; Досліджено проблему запобігання недозволеному доступу підроблених клієнтів до ТД та ефективності заходів захисту від можливих атак, спрямованих на підроблення ТД; Проаналізовано ефективність існуючих методів та засобів захисту, які можуть забезпечити безпеку Wi-Fi клієнтів від потенційних загроз, що виникають як з боку самої мережі, так і з боку клієнта.

Результати дослідження вказують на те, що наявні методи не забезпечують повноцінного захисту від ФТД.

РОЗДІЛ 2. ОСНОВНА ЧАСТИНА

2.1. Модель ідентифікаційної взаємодії між клієнтами та ТД Wi-Fi

На даний момент більшість протоколів захисту, які здійснюють ідентифікацію, обмежуються проведенням ідентифікації лише між клієнтом мережі та самою мережею SSID. У цьому випадку зловмисник намагається з’єднати клієнта із підробленою центральною ТД.

У такому сценарії протоколи не забезпечують ідентифікацію доступних точок мережі, в яких ідентифікований клієнт чи користувач, і відповідно, забезпечують обмін даними персонального характеру в цій мережі.

Для вирішення завдання щодо проблем доступності ФТД необхідно:

– Запровадити процедуру ідентифікації кожної конкретної точки, до якої підключений клієнтський пристрій.

– Забезпечити взаємозалежну ідентифікацію точок мережі для індивідуальної ідентифікації кожного клієнта окремо в мережі. Особливо у випадку невеликих та середніх мереж, які використовують протокол WPA2 без сервера ідентифікації, обмежений доступ до мережі забезпечується за допомогою унікального клієнтського MAC-адреса.

У цьому контексті розглядається загальна модель ідентифікації, коли клієнт визначає ТД до мережі, оскільки цей сценарій є узагальненим. Процес ідентифікації клієнтом мережевої точки відбувається аналогічним чином.

Для здійснення ідентифікації ТД пропонується використовувати криптосистему, а саме алгоритм шифрування повідомлень клієнта за допомогою ключа відкритого типу. Це рішення сприяє вирішенню завдання довіри через використання ЦП. У криптографії з ВК використовується пара ключів: відкритий (публічний) і закритий (приватний). ЗК залишається конфіденційним, оскільки його розголошення може призвести до компрометації криптографії, у той час як ВК передається вільно. Електронний

ЦП створюється за допомогою ЗК, а його перевірка виконується відповідним ВК.

Щодо аутентифікації клієнтами ТД, модель виглядає наступним чином (див. рисунок 2.1.):

1. Клієнт вибирає довірену ТД.

2. Клієнт отримує ВК даної ТД і запам’ятовує його.

3. При наступному підключенні, перед початком передачі трафіку, клієнт проводить аутентифікацію:

a. Клієнт надсилає випадкову послідовність байтів ТД.

b. ТД підписує цю послідовність байтів своїм ЗК і висилає результат підпису клієнту.

c. Клієнт перевіряє підпис за допомогою ВК ТД, підтверджуючи, що у ТД вірний ЗК.

4. При успішній аутентифікації клієнт починає передачу трафіку до ТД, в іншому випадку підключення відхиляється.

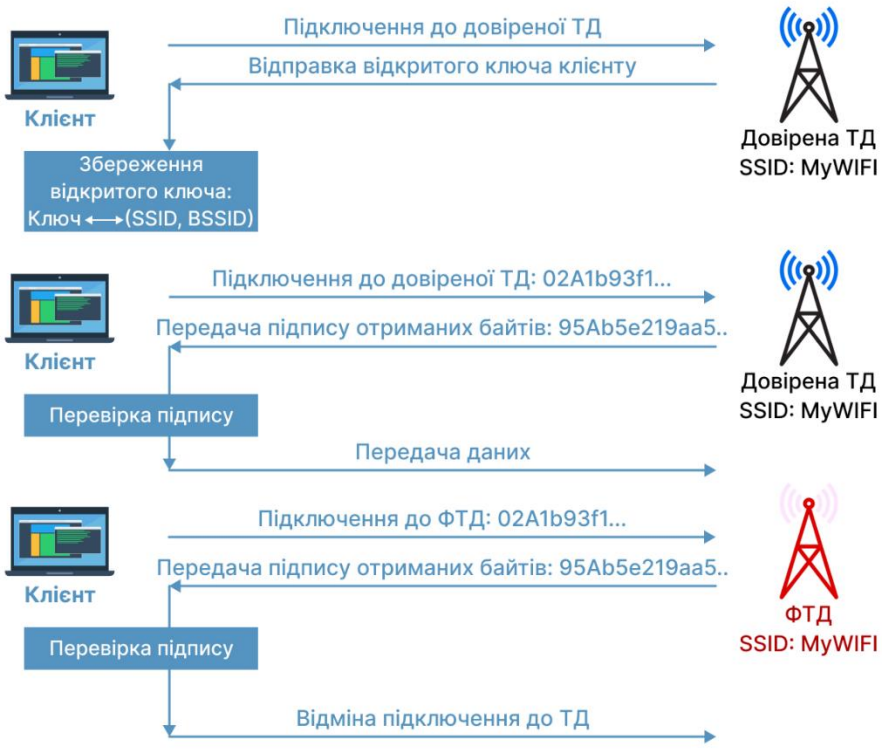


Рис. 2.1. – Модель аутентифікації ТД безпровідними Wi-Fi клієнтами

Існує маса криптографічних алгоритмів з ВК, які використовуються для створення та перевірки ЦП, таких як схема RSA, схема Ель-Гамаля, DSA, EdDSA, ECDSA та інші. Оскільки передбачається, що як на клієнтові, так і на ТД (у випадку взаємної аутентифікації) зберігатиметься пара відкритий-закритий ключ, і кількість таких підключень може бути значною, першою вимогою при виборі алгоритму є мінімізація довжини ключів для економії пам’яті. Однак, оскільки цільовими є мобільні пристрої, обраний алгоритм повинен також забезпечувати швидкодію. Відомо, що алгоритми, які базуються на еліптичних кривих, забезпечують високу швидкодію і аналогічний рівень криптостійкості порівняно з алгоритмами, що базуються на числах. Для прикладу, розглянемо алгоритм DSA і його реалізацію на еліптичних кривих – ECDSA. Криптостійкість DSA ґрунтується на складності завдання дискретного логарифмування, тоді як криптостійкість ECDSA базується на тому ж завданні, але застосованому до теорії еліптичних кривих. Це призводить до ускладнення можливості здійснення атак на ECDSA, зменшуючи при цьому довжину ключів та обчислювальних ресурсів для генерації підписів. Звісно, довжина ВК для алгоритмів, що базуються на еліптичній криптографії, становить 32 байти (ЗК – 64 байти, але в стислому вигляді також 32 байти), а довжина підпису – 64 байти. На рисунку 2.2 наведено залежність довжин ключів між алгоритмами RSA/DSA та ECDSA/EdDSA.

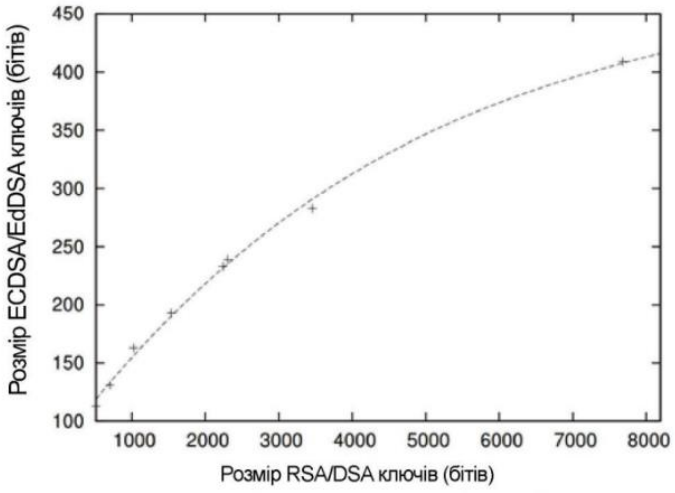


Рис. 2.2. – Зв’язок між розмірами ключів для алгоритмів RSA/DSA та ECDSA (в бітах)

Отже, для проведення процедури аутентифікації рекомендується використовувати протоколи з підтримкою еліптичних кривих, такі як ECDSA або EdDSA. ECDSA, що є найбільш використовуваним алгоритмом, має реалізації на різних еліптичних кривих, серед яких Curve25519 вирізняється як оптимальна з точки зору швидкості та криптостійкості. Алгоритм EdDSA, розроблений Данилом Бернштейном, представлений реалізацією на еліптичній кривій Ed25519 (еквівалентною Curve25519) і вважається найшвидшим та безпечним криптографічним методом з ВК [34]. Слід відзначити, що приріст продуктивності між цими алгоритмами невеликий, тож обрання одного чи іншого не виявляє чітких переваг.

Викладену вище модель аутентифікації можна впроваджувати на різних рівнях протоколу TCP/IP:

– На канальному рівні в пакетах аутентифікації 802.11.

– На транспортному рівні через засоби TCP-сокетів.

– На прикладному рівні через протоколи HTTP і веб-сокетів.

Як було зазначено в розділі 1.3., під час підключення відбувається взаємодія через обмін пакетами аутентифікації 802.11. Відповідний фрейм аутентифікації зображено на рисунку 2.3.

Рис. 2.3. – Структура фрейму аутентифікації

Фрейм складається із чотирьох основних полів:

1. Ідентифікатор алгоритму аутентифікації: 0 – для відкритої аутентифікації, 1 – для аутентифікації за допомогою розподіленого WEP ключа.

2. Порядковий номер фрейму в послідовності аутентифікації.

3. Код статусу: 0 – у випадку успішної аутентифікації, 1 – у випадку невизначеної помилки.

4. Текст аутентифікації. Це поле використовується у фреймах 2 і 3 для аутентифікації першого типу (див. рисунок 2.3.).

Як зазначено в розділі 1.1.2., коли застосовується аутентифікація нульового типу, відбувається обмін двома пакетами, а при використанні першого типу – чотирма пакетами аутентифікації. Таким чином, теоретично можна додати нові типи аутентифікації 802.1. Запропоновано впровадити три додаткові типи аутентифікації:

– Тип 2 – аутентифікація клієнтом ТД.
– Тип 3 – аутентифікація ТД клієнта.
– Тип 4 – взаємна аутентифікація між ТД та клієнтом.

Для другого типу обміну передбачено взаємодію через відправку пакетів запиту та отримання відповіді. У пакеті запиту клієнт вказує тип аутентифікації (тип 2) і включає поле тексту аутентифікації, яке містить унікальну послідовність байтів, згенеровану випадковим чином. У відповідь на цей запит клієнт отримує ЦП даного тексту, який також розташований у полі тексту аутентифікації, та перевіряє його автентичність. Після перевірки ЦП клієнт приймає рішення щодо подальшої асоціації з ТД. Якщо підпис виявляється правильним, клієнт вирішує продовжити асоціацію, інакше він надсилає ТД пакет із запитом аутентифікації. На рисунку 2.4 наведено схему аутентифікації клієнтом ТД.

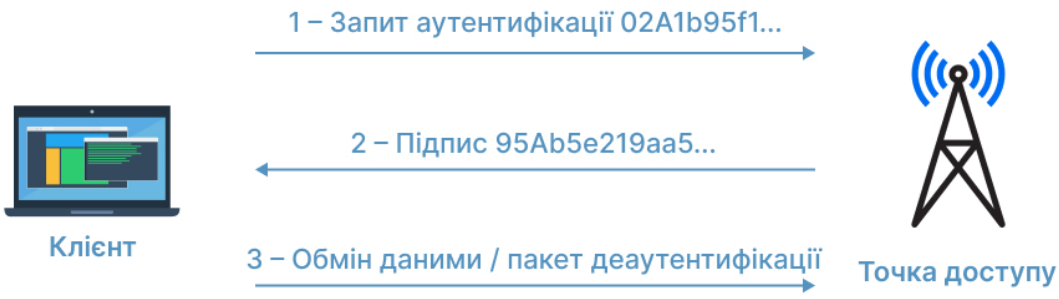


Рис. 2.4. – Схема аутентифікації клієнтом ТД

У випадках аутентифікації типів 3 та 4 взаємодія вже відбуватиметься за допомогою чотирьох пакетів. Тип 3 залишається аналогічним до вже існуючої схеми, описаної в пункті 1.1.2., з винятком того, що передача даних від клієнта до ТД буде виконуватися не зашифрованим загальним ключем, а підписаною клієнтом послідовністю байтів. Тип 4 відрізнятиметься тим, що в кожному з чотирьох пакетів буде включене поле “Текст аутентифікації”:

1. Перший пакет, що містить запит на авторизацію від клієнта до ТД, включатиме випадкову послідовність байтів клієнта.

2. Другий пакет, переданий від ТД клієнтові, буде включати випадкову послідовність байтів ТД.

3. Третій пакет, переданий від клієнта до ТД, буде містити підписані клієнтом байти ТД. Якщо підпис є вірним, то ТД переходить до кроку 4; в іншому випадку вона відправляє клієнту пакет аутентифікації.

4. Четвертий пакет, переданий від ТД до клієнта, буде містити ЦП переданих випадкових байтів клієнта.

На рисунку 2.5. наведено схему взаємної аутентифікації на канальному рівні.

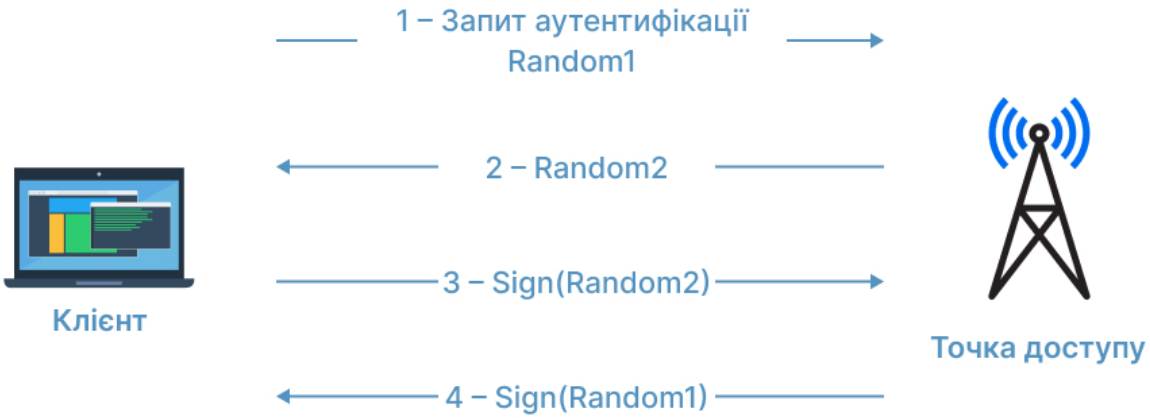


Рис. 2.5. – Схема взаємної аутентифікації на канальному рівні

Перевага такого підходу полягає у тому, що структура пакетів аутентифікації 802.11 вже практично готова для інтеграції цієї схеми, і для її реалізації знадобиться мінімальна кількість модифікацій. Більш того, якщо

внести зміни до самого стандарту 802.11, схема аутентифікації може стати універсальною для всіх пристроїв. Проте, недоліком цього підходу є потреба в зміні конфігурацій на численних вже наявних пристроях.

Обидва інші методи реалізації (через TCP-сокети та веб-сокети) мають схожий характер і виконують ті ж самі послідовності обміну даними, що і при використанні технології на канальному рівні. Однак є різниці у реалізації цих технологій (див. рис. 2.6.). Обидва підходи вимагають реалізації у вигляді додаткового ПЗ і працюють напряму з API ОС. Їх перевагою є простота реалізації як на стороні клієнта, так і на стороні сервера. Здається, що реалізація через веб-сокети має деяку перевагу, оскільки їх легше настроювати, і більшість ТД підтримують графічні інтерфейси для керування, що дозволяє вносити зміни в прошивку роутерів досить просто.

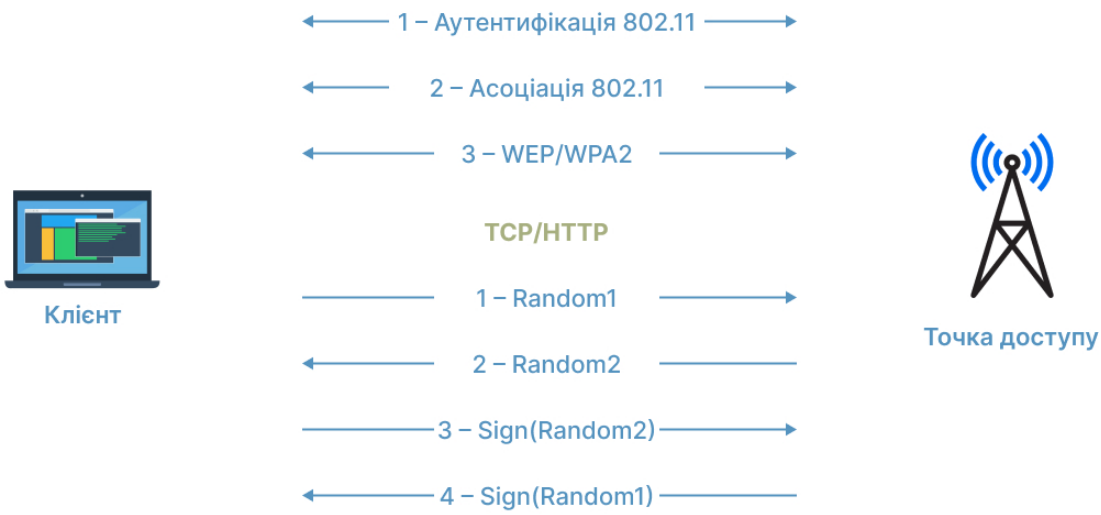


Рис. 2.6. – Схема взаємної аутентифікації між клієнтом і ТД за допомогою TCP-сокетів чи WEB-сокетів

Однак, незважаючи на простоту розгортання, обидва підходи мають кілька недоліків:

– Перевагою цих підходів у реалізації без змін існуючих протоколів канального рівня є їхній недолік в універсальності, оскільки можливість

реалізації додатка під певну платформу буде залежати від доступних функцій API.

– Обидва підходи можуть функціонувати лише після того, як клієнт підключився до самої ТД стандартними засобами і отримав IP-адресу, призначену мережі, яку обслуговує ТД. Це через те, що протокол TCP-сокети реалізований через однойменний протокол, що працює поверх IP, а веб-сокети реалізовані над HTTP (як його розширення), отже, працюють поверх TCP. Розроблене ПЗ повинне контролювати обмін даними та блокувати передачу даних на стороні клієнта, якщо ТД не була аутентифікована, і водночас забороняти клієнту доступ до мережі, якщо він не пройшов аутентифікацію.

Це ускладнює впровадження взаємної аутентифікації та аутентифікації клієнта ТД.

2.2. Висновок до другого розділу

В другому розділі кваліфікаційної роботи розроблено концепцію, яка дозволяє проводити аутентифікацію клієнтів ТД. Ця модель може бути використання як для базової аутентифікації клієнтів, так і для впровадження аутентифікації ТД і клієнтів.

РОЗДІЛ 3. НАУКОВО-ДОСЛІДНА ЧАСТИНА

З метою відображення функціонування наведеної у пункті 3 схеми аутентифікації між безпровідними клієнтами та ТД Wi-Fi був створений програмний комплекс, який реалізує аутентифікацію клієнтів у ТД за допомогою ЦП, генерованих та перевіряються алгоритмом з ВК EdDAS. Даний комплекс включає в себе серверну та клієнтську частини. Для створення та перевірки ЦП використовується алгоритм EdDAS, реалізований на еліптичній кривій Ed25519. Довжина відкритих ключів складає 256 біт, а довжина підпису – 512 біт.

3.1. Серверна архітектура програмного комплексу

Серверна частина є консольною програмою, що емулює функціонал ТД. Вона здатна управляти активацією та деактивацією безпровідного інтерфейсу Wi-Fi на пристрої, а також забезпечує взаємодію з сервером аутентифікації. Розроблена в середовищі Node.JS мовою JavaScript, програма повністю кросплатформна під різні ОС, які підтримують середовище виконання Node.js (Windows, Linux, Mac OS та інші), за винятком частини, відповідальної за конфігурацію Wi-Fi, оскільки вона є платформозалежною. Управління Wi-Fi в ОС Windows реалізовано через виклик вбудованих команд консольної утиліти netsh. Для ОС Linux конфігурування Wi-Fi виконується за допомогою сторонньої бібліотеки wireless-tools [35], яка, в свою чергу, викликає стандартні команди Linux. Важливо відзначити, що для демонстрації конфігурування, увімкнення та вимкнення Wi-Fi можна проводити за допомогою вбудованих засобів ОС без використання розробленого ПЗ. Інтерфейс серверної частини зображено на рисунку 3.1.

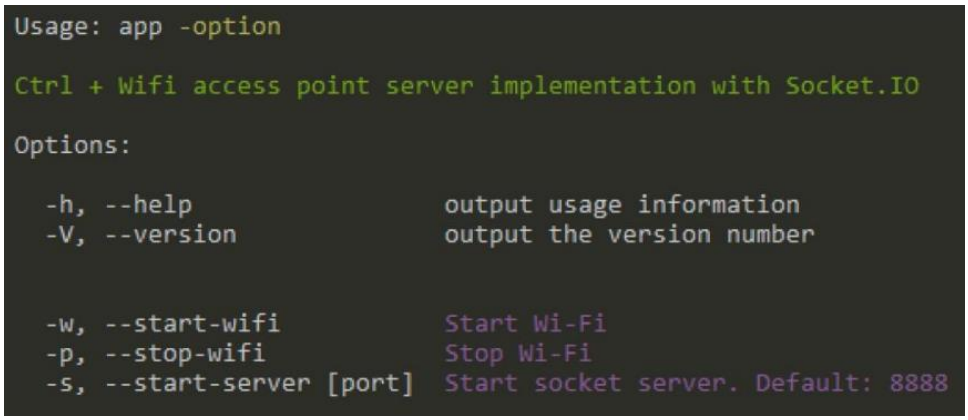


Рис. 3.1. – Інтерфейс серверного модулю розробленого програмного пакету

Аутентифікаційний компонент був розроблений за допомогою бібліотеки socket.io [36], яка впроваджує функціональність веб-сокетів. Для активації сервера достатньо запустити його на конкретному порту і налаштувати обробники вхідних повідомлень, як це подано в лістингу 3.1.

Лістинг 3.1 – Налаштування сервера та обробників вхідних повідомлень

```
const server = io.listen(
require("http").createServer(app).listen(PORT), options);

server.sockets.on("connection"), function (socket) {
socket.on("deriveKey"), function () {
socket.emit("deriveKeyResponse", {
key: key.getPublic("hex")
});
});

socket.on("checkKey", function (data) {
const signature = key.sign(data).toHex();
socket.emit("checkKeyResponse", {encodedString: signature});
});
});
```

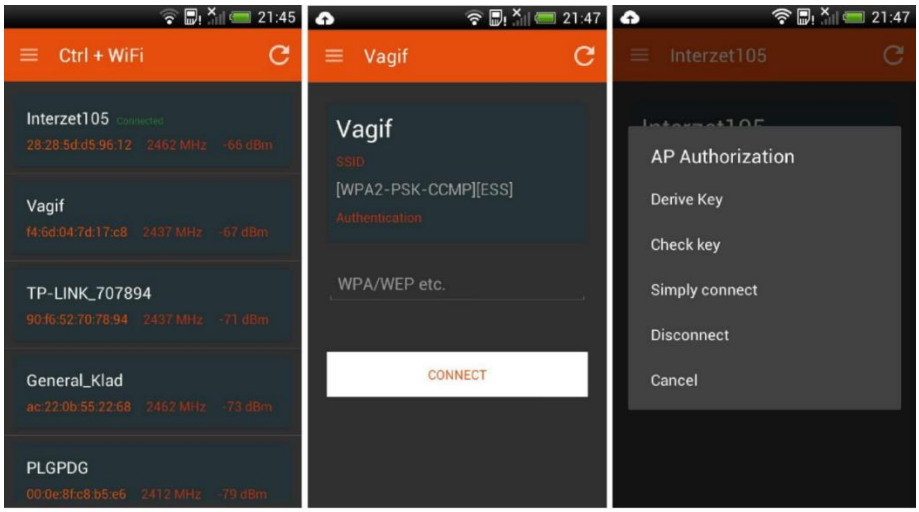
Сервер аутентифікації здійснює обробку двох типів подій:

1. Отримання ВК ТД (подія “deriveKey”). При виникненні цієї події сервер аутентифікації генерує ВК і ЗК, надсилаючи ВК ТД клієнту.

2. Перевірка ВК ТД (подія “checkKey”). Під час настання цієї події ТД отримує від клієнта певну послідовність байтів, підписує її за допомогою алгоритму EdDSA на своєму ЗК і надсилає підпис клієнту.

3.2. Функціонал та особливості клієнтської частини

Клієнтська частина розроблена на мові Kotlin і представлена у вигляді мобільного додатка з графічним інтерфейсом для пристроїв з ОС Android версії 4.0.3 і вище (використовувалось API Level 15). При старті додатка ініціюється локальний сервіс VPN, який функціонує у фоновому режимі. Цей сервіс виступає у ролі спрощеного міжмережевого екрана та блокує передачу даних до транспортного рівня, за винятком тих, що адресовані IP-адресі та порту сервера аутентифікації, до моменту авторизації ТД через додаток. Після успішної авторизації інформація про аутентифіковану ТД додається до локальної БД, дозволяючи передачу трафіку до неї. Основний інтерфейс додатка пропонує список доступних Wi-Fi мереж і забезпечує інформацію про них, таку як MAC-адреса видимої ТД, частота каналу в мГц та рівень сигналу в дБ мВт (див. рисунок 3.2, а). Вибравши конкретну мережу зі списку, відкривається інтерфейс, де можна встановити з'єднання з нею (див. рисунок 3.2, б). Після авторизації до ТД клієнт отримує її ключ, може підключитися безпосередньо або відмінити підключення (див. рисунок 3.2, в). У випадку першого підключення клієнта до ТД, він може отримати ВК на основі власної довіри.



а б в

Рис. 3.2. – Головний екран інтерфейсу: а – перелік доступних безпровідних мереж Wi-Fi; б – інтерфейс обраної ТД; в – інтерфейс для вибору дій для подальшої взаємодії з ТД після її підключення

Ключ заноситься до локальної БД та порівнюється із SSID мережі та MAC-адресою точки, які відображаються у розділі “База ключів” (див. рисунок 3.3.). З цього розділу їх можна вибрати, щоб використовувати під час наступних підключень, та перевірити, чи існує відповідний дійсний ЗК для ТД.

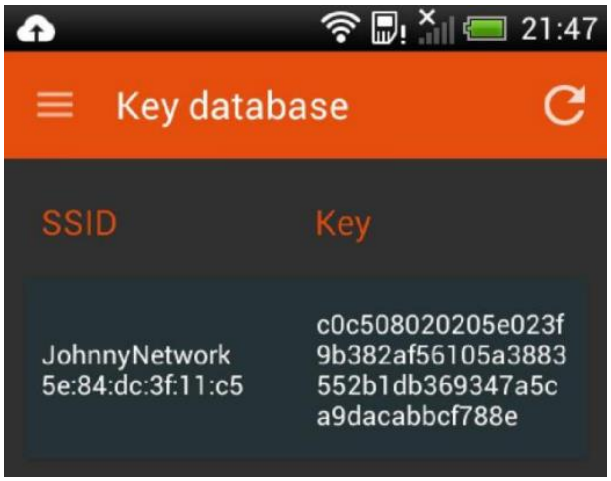
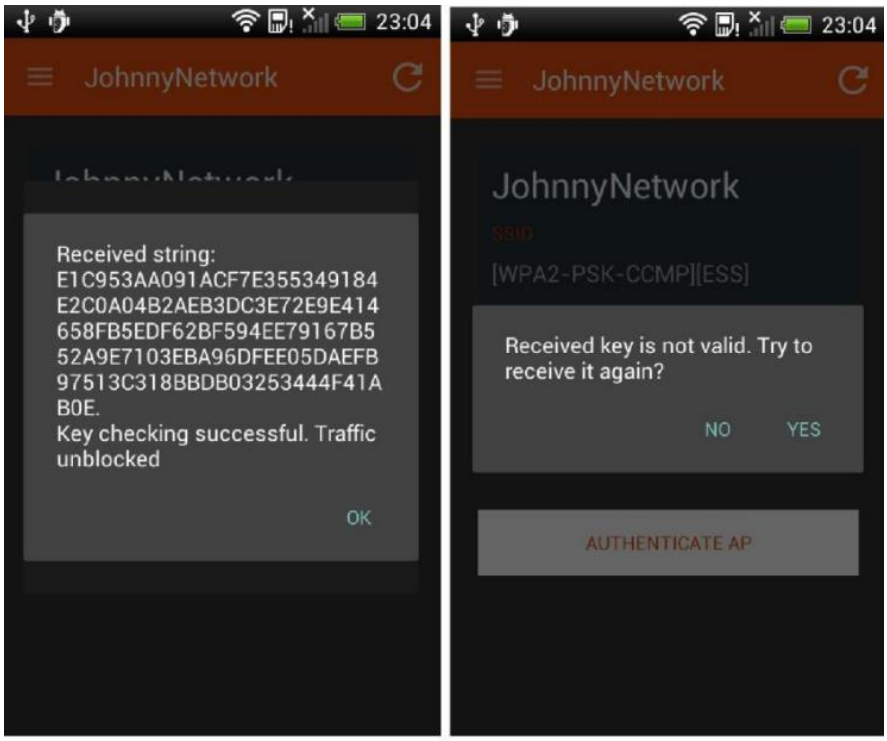


Рис. 3.3. – Інтерфейс локального сховища порівняльних мереж та ТД разом із ВК

Для проведення авторизації у ТД та передачі довільної послідовності байтів клієнт встановлює з’єднання з веб-сервером ТД. Взаємодія здійснюється через веб-сокети, реалізовані за допомогою тієї ж бібліотеки Socket.IO [37]. У випадку успішної аутентифікації відбувається обмін даними з ТД (див. рисунок 3.4, а), в іншому випадку виникає запит на повторну перевірку ключа або відміна підключення (див. рисунок 3.4. б).



а б

Рис. 3.4. – Висвітлення вікон при успішній (а) та невдалій (б) аутентифікації ТД

Якщо змінити порядок байтів, на основі яких формуються ЗК і ВК ТД за допомогою алгоритму EdDSA, то отриманий ВК, який зберігається на стороні клієнта, не буде відповідати відповідному ЗК, що зберігається на стороні ТД. Це призведе до невдалої перевірки підпису переданого повідомлення на стороні ТД, і користувач буде інформований про це. Наприклад, якщо спочатку використовувався ЗК для генерації ВК на ТД, і його значення було таким: 693e3cab5f693e3cab5f693e3cab5f, то відповідні ВК матимуть вигляд:

$$\text{ВК}_{\text{ТД}} = c0c508020205e023f9b382af56105a3883552b1db369347a5ca9dacabbcf788e$$

Тепер, змінивши ЗК на нове значення, наприклад: 693e3cab5f693e3cab5f693e3cab5d, отримаємо нові пари ВК:

$$\text{ВК}_{\text{ТД}} = 6da1d9401a981766d913ed939c3ae9319e5b86c9783a615a7bc95fc6b2756f12$$

В БД клієнта все ще залишиться оригінальне значення ВК для ТД (див. рисунок 3.4). Таким чином, при перевірці підпису користувач буде сповіщений про те, що ЗК на стороні ТД не вдалося перевірити (див. рисунок 3.4, б).

3.3. Висновок до третього розділу

В третьому розділі кваліфікаційної роботи розроблено комплекс програм, що включає клієнтську та серверну частини. Клієнтська частина, спроектована для ОС Android, забезпечує аутентифікацію ТД за допомогою ВК. У майбутньому можна розглянути можливість реалізації першочергової довіри клієнта до ТД, використовуючи сертифікати X.509 або модель, що застосовується в протоколі Pretty Good Privacy (PGP).

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Під час роботи з радіотехнічними системами враховано всі небезпечні фактори ризику (перевищений рівень шуму та вібрацій, електротравматизм, негативний вплив освітлення освітлення та інші), які би негативно впливали на рівень безпеки обслуговуючого персоналу в процесі експлуатації системи.

Оскільки система, живиться безпосередньо від електромережі, тому необхідно максимізувати рівень електробезпеки обслуговуючого персоналу шляхом адекватного дотримання правил роботи з електроприладами, зокрема системою, які прописані в стандарті ГОСТ 12.1.030-81 «ССБТ. Електробезпека. Захисне заземлення. Занулення» [38].

Із врахуванням вище сформульованого припущення, встановлена необхідність розроблення рекомендації по питанням охорони праці при роботі з радіотехнічною системою шляхом аналізу негативного впливу електричного струму на обслуговуючий персонал при роботі із системою, способів нормування та захисту від його дії.

Внаслідок дії електричного струму на організм обслуговуючого персоналу під час експлуатації блоку може виникнути загальна (електричний удар) або місцева електротравма (опіки, електричні знаки, електрометалізація шкіри, механічні пошкодження). Розрізняють три ступені впливу струму при проходженні через організм людини (змінний струм) [38]:

- відчутний струм – початок болісних відчуттів (до 0-1,5 мА);
- невідпускний струм – судоми і біль, важке дихання (10-15 мА);
- фібриляційний струм – фібриляція серця при тривалості діє струму 2-3с, параліч дихання (90-100 мА).

На рисунку 4.1 зображено основні фактори, які впливають на організм людини при ураженні електричним струмом.

Рис. 4.1. Фактори впливу електричного струму на людину

Правильне визначення необхідних засобів та заходів обслуговуючого персоналу від ураження електричним струмом необхідно враховувати гранично допустимі значення напруг дотику та струмів, що проходять через тіло людини по шляху "рука - рука" чи "рука - ноги" (таблиця 4.1) (регламентується ГОСТом 12.1.038-82).

Таблиця 4.1

Гранично допустимі значення напруги дотику та сили струму, що проходить через тіло людини

Вид струму	Нормоване значення	Тривалість струму, сек					
		0,1	0,2	0,5	0,7	1	Більше1
Змінний, 50 Гц	Напруги дотику, В (не більше)	500	250	100	70	50	36
	Сила струму, мА (не більше)	500	250	100	70	50	6

Основне завдання електробезпеки - мінімізувати можливість негативного впливу електричного струму на людину. Досягти цієї мети можна за допомогою таких заходів і засобів: 1) безпечною і надійною конструкцією елементів системи; 2) організаційними та технічними заходами щодо безпечної

експлуатації системи та використання електричної енергії; 3) технічними засобами захисту.

У даному випадку це досягнуто шляхом конструктивного виконання складових системи класу I, який відповідає вимогам технічних умов і стандарту ГОСТ 12.1.030-81. Згідно класу I складові системи мають робочу ізоляцію і виконаний таким чином, що підключити його до електричної мережі можна лише після під’єднання корпусу до заземлювача (нульового захисного провідника), а при від'єднанні від мережі - корпус відключається від заземлювача (нульового захисного провідника) в останню чергу.

Стан ізоляції струмопровідних частин відповідає правилам використання системи. Цими правилами передбачене періодичне випробування ізоляції 2 рази на рік у приміщеннях зі складними умовами, підвищеною вологістю і 1 раз на рік у приміщеннях з нормальним середовищем. Ізоляція створює великій опір, який перешкоджає протіканню через неї струму. Опір ізоляції складових системи становить не меншим 0,5 МОм (згідно вимог ГОСТ 12.1.030-81). Якщо опір ізоляції знижується на 50% від початкового, мережу або ізоляцію необхідно замінити.

При роботі в приміщеннях без підвищеної небезпеки напруга складових системи повинна бути не більше 220 В. При роботі в приміщеннях з підвищеною небезпекою і за межами приміщень напруга складових системи повинна бути не більше 36 В. В особливих умовах дозволяється використовувати блок з напругою до 220 В, але при наявності захисного відключення або надійного заземлення корпусу з використанням захисних засобів (діелектричні рукавички, килимки, калоші).

Захисне заземлення - навмисне електричне з'єднання із землею металевих струмопровідних неструмоведучих частин, на яких може з’явитися напруга. Заземлення - це сукупність заземлювача і заземлювальних провідників. Заземлювачі можуть бути штучні (створені спеціально для заземлення блоку) і природні. Для штучних заземлювачів застосовують вертикальні і горизонтальні електроди. Вертикальні - зі стальних прутів діаметром 10-12мм, кутової сталі

розміром 40х40 мм або стальних труб діаметром 30-50мм, довжиною 2,5-3 м. Вертикальні електроди з'єднують стальною штабою розміром 4х12 мм або круглим дротом діаметром не меншеб мм. Опір заземлюючого пристрою не повинен перевищувати 4-10 Ом (перевіряється щорічно).

Таким чином врахувавши вище сформульовані рекомендації по питанням охорони праці при експлуатації радіотехнічної системи буде забезпечено небезпечні умови праці обслуговуючого персоналу.

4.2. Безпека в надзвичайних ситуаціях

Підприємтсво з випуску радіотехнічних систем (ДРС) є пожежонебезпечним, тому акуальним є забезпечення протипожежного захисту робітників та службовців, які на них працюють. Заходи протипожежного захисту здійснюються з дотриманням вимог глави 13 Кодексу цивільного захисту України від 02.10.2012 р. №5403-VI.

Всі заходи організаційно-технічного характеру протипожежного захисту на виробництві на об'єкті можна підрозділити на організаційні, технічні, режимні та експлуатаційні [36].

Забезпечення пожежної безпеки є складовою частиною виробничої або іншої діяльності посадових осіб, працівників підприємств та підприємців. Це повинно бути відображено у трудових договорах (контрактах) та статутах підприємств.

Керівник підприємства з випуску ДРС повинен визначити обов'язки посадових осіб щодо забезпечення пожежної безпеки, призначити відповідальних за пожежну безпеку окремих будівель, споруд, приміщень, дільниць, технологічного та інженерного устаткування, а також за утримання і експлуатацію технічних засобів протипожежного захисту. Обов’язки щодо забезпечення пожежної безпеки, утримання та експлуатації засобів протипожежного захисту мають бути відображені у відповідних посадових документах (функціональних обов'язках, інструкціях, положеннях тощо).

На кожному підприємстві з урахуванням його пожежної небезпеки наказом (інструкцією) повинен бути встановлений відповідний протипожежний режим, в тому числі визначені:

• можливість (місце) паління, застосування відкритого вогню та побутових нагрівальних приладів;

• порядок проведення тимчасових пожежо небезпечних (в тому числі зварювальних) робіт;

• правила проїзду та стоянки транспортних засобів;

• місця для зберігання і допустима кількість сировини, напівфабрикатів та готової продукції, які можуть одночасно знаходитися у виробничих приміщеннях і на території (у місцях зберігання);

• порядок прибирання горючого пилу та відходів, зберігання промасленого спецодягу і шмаття, очищення повітроводів вентиляційних систем від горючих відкладень;

• порядок відключення від мережі електрообладнання у разі пожежі;

• порядок огляду і зачинення приміщень після закінчення роботи;

• порядок проходження посадовими особами навчання та перевірки знань з пожежної безпеки, а також проведення з працівниками протипожежних інструктажів та занять з пожежно-технічного мінімуму з призначенням відповідальних за їх проведення;

• порядок організації експлуатації і обслуговування наявних технічних засобів протипожежного захисту (протипожежного водопроводу, насосних станцій, вогнегасників тощо);

• дії працівників у разі виявлення пожежі.

Для об'єктів з перебуванням людей вночі інструкції мають передбачати два варіанти дій відповідно у денний та нічний час.

Усі працівники при прийнятті на роботу і за місцем здійснення професійної діяльності повинні проходити інструктаж з питань пожежної безпеки (вступний, первинний, повторний на робочому місці, позаплановий та цільовий). Посадові особи до початку виконання своїх обов'язків і періодично

один раз на 3 роки мають проходити навчання і перевірку знань з питань пожежної безпеки.

Отже, організаційні заходи пожежної безпеки передбачають: організацію пожежної охорони на об'єкті, проведення навчань з питань пожежної безпеки (включаючи інструктажі та пожежно-технічні мінімуми), застосування наочних засобів протипожежної пропаганди та агітації, проведення перевірок, оглядів стану пожежної безпеки приміщень, будівель, об'єкта в цілому та ін.

До технічних заходів належать: суворе дотримання правил і норм, визначених чинними нормативними документами при реконструкції приміщень, будівель та об'єктів, технічному переоснащенні виробництва, експлуатації чи можливому переобладнанні електромереж, опалення, вентиляції, освітлення і т. п.

Заходи режимного характеру передбачають заборону куріння та застосування відкритого вогню в недозволених місцях, недопущення появи сторонніх осіб у вибухонебезпечних приміщеннях чи об'єктах, регламентацію пожежної безпеки при проведенні вогневих робіт тощо.

Експлуатаційні заходи охоплюють своєчасне проведення профілактичних оглядів, випробувань, ремонтів технологічного та допоміжного устаткування, а також інженерного господарства (електромереж, електроустановок, опалення, вентиляції).

4.3. Висновки до розділу 4

У підрозділі з охорони праці розроблено рекомендації по питанням охорони праці при роботі з радіотехнічною системою шляхом аналізу негативного впливу електричного струму на обслуговуючий персонал при роботі із системою, способів нормування та захисту від його дії.

У підрозділі з безпеки в надзвичайних ситуаціях проаналізовано заходи організаційно-технічного характеру протипожежного захисту на виробництві радіотехнічної системи.

ЗАГАЛЬНІ ВИСНОВКИ

В ході виконання кваліфікаційної роботи було проведено аналіз існуючих протоколів безпеки в Wi-Fi мережах, з основним упередженням на запобігання вторгнення підроблених клієнтів до ТД і виконання атак ФТД. Результати вказують на те, що більшість протоколів забезпечують аутентифікацію клієнтів в мережі, але не гарантують аутентифікацію ТД. У зв’язку з цим були ретельно розглянуті існуючі засоби та методи захисту, які могли б захистити клієнтів Wi-Fi від ФТД, незалежно від напряму, чи то з боку мережі, чи з боку клієнта. Під час аналізу було виявлено, що існуючі засоби та методи не завжди забезпечують повноцінний захист від ФТД.

Відтак, було розроблено схему, призначену для аутентифікації клієнтів ТД, яка може використовуватися для додаткової аутентифікації клієнтів та виступати як взаємна аутентифікація. Для демонстрації ефективності розробленої схеми було реалізовано програмний комплекс, який включає в себе клієнтську та серверну частини. Клієнтська частина була створена для ОС Android і дозволяє аутентифікувати ТД за допомогою ВК. Далі можна розглядати як напрямки майбутньої роботи кілька аспектів, зокрема, питання вихідної довіри до ТД зі сторони клієнта, яке може бути вирішено, наприклад, за допомогою сертифікатів X.509 або через модель, аналогічну тій, яка використовується в протоколі PGP, відомій як Web Of Trust. У цій моделі багато учасників взаємодії, які вже відомі клієнту, можуть встановити певний рівень довіри до конкретної ТД з певною ймовірністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Програмне забезпечення Aircrack-ng. 2015. URL: http://www.aircrack-ng.org/.

2. Authentication Types for Wireless Devices. 2008. URL: http://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuth enticationTypes.html#wp1034623.

3. Changhua He, John C Mitchell. Security Analysis and Improvements for IEEE 802.11i. 2004. URL: http://seclab.stanford.edu/pcl/mc/papers/NDSS05.pdf.

4. 802.1X: Port-based network access control. 2010. URL: http://standards.ieee.org/getieee802/download/802.1X-2010.pdf.

5. AAA protocols. 2013 URL: http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-1/user/guide/acsuserguide/rad_tac_phase.html.

6. FreeRadius. Enterprise Wi-Fi / IEEE 802.1X. 2015. URL: http://freeradius.org/enterprise-wifi.html.

8. Extensible Authentication Protocol (EAP). 2004. URL: https://tools.ietf.org/html/rfc3748.

7. Cisco Wireless LAN Security Overview. 2006. URL: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/prod_brochure09186a00801f7d0b.html.

8. The Working Groupfor WLAN Standards. 2016. URL: http://www.ieee802.org/11/.

9. WPA2™ Security Now Mandatory for Wi-Fi CERTIFIED™ Products. 2006. URL: http://www.wi-fi.org/news-events/newsroom/wpa2-security-now-mandatory-for-wi-fi-certified-products.

10. IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements. 2004. URL: http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.

11. IETF RFC 4017. Extensible Authentication Protocol (EAP) Method

Requirements for Wireless LANs. 2005. URL: https://www.ietf.org/rfc/rfc4017.txt.

12. Understanding the updated WPA and WPA2 standards. 2005. URL: http://www.zdnet.com/article/understanding-the-updated-wpa-and-wpa2-standards/.

13. Типи фреймів мережі стандарту IEEE 802.11. 2011. URL: http://wi-life.ru/texnologii/wi-fi/wi-fi-frames-management-control-data -

14. What are passive and active scanning. 2016. URL: http://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning.

15. Wi-Fi мережі: проникнення та захист. 3) WPA. OpenCL/CUDA. Статистика подбора. 2014. URL: https://m.habrahabr.ru/post/226431/.

16. Cisco Rogue Management. 2013. URL: http://www.cisco.com/c/en/us/td/docs/wireless/technology/roguedetection_deploy/Rogue_ Detection.html.

17. Ed25519: high-speed high-security signatures. URL: https://ed25519.cr.yp.to/.

18. Palianytsia, Yurii, Vasyl Dunets, and Liliia Khvostivska. “Modeling of Phased Array Antenna for Data Transmission in Urban Environment.” Proceedings of the 3rd International Workshop on Information Technologies: Theoretical and Applied Problems, 22-24 November 2023, Ternopil, Ukraine, edited by Lytvynenko I.V. and Lupenko S.A., ITTAP-2023, 2023, pp. 370-381.

19. Дунець В.Л., Хвостівська Л.В., Паляниця Ю.Б. Математичне, алгоритмічне та програмне забезпечення оцінювання завадозахищеності каналів зв’язку з балансною модуляцією. Збірник наукових праць Вісник НУ пВГП, серія технічні науки, випуск 4 (104), 2023. - С. 95-107. ISSN: 2306-5478.

20. Liliya Khvostivska, Mykola Khvostivskyy, Vasyl Dunets, Iryna Dediv. “Mathematical and Algorithmic Support of Detection Useful Radiosignals in Telecommunication Networks”. Proceedings of the 2nd International Workshop on Information Technologies: Theoretical and Applied Problems, 22-24 November 2022, Ternopil, Ukraine, ITTAP 2022, 2022, pp. 314-318. ISSN 1613-0073

ДОДАТКИ

Додаток А

Назва додатка А

УДК 004.056
С.О. Кміть, к.т.н В.Л. Дунець

АНАЛІЗ МЕТОДІВ ЗАХИСТУ МЕРЕЖ Wi-Fi

P.P. Protsyk, Ph. D. V.L. Dunets

ANALYSIS OF PROTECTION METHODS OF THE Wi-Fi NETWORKS

Функціонування більшості сучасних підприємств базується на використанні комп'ютерних мереж. Для ефективного вирішення задач, пов'язаних із мобільністю та масштабністю мережі, доцільно використовувати бездротові комп'ютерні мережі стандарту IEEE 802.11. В той же час використання бездротових мереж створює нові виклики, пов'язані з розробкою систем захисту від кіберзагроз. Якщо захисту мережі не приділити належної уваги може трапитись втрата конфіденційної інформації користувачів, втрата доступу до ресурсів і дисків користувачів Wi-Fi-мереж і ресурсів LAN, спотворення інформації, що проходить в мережі, впровадження підроблених точок доступу і т.п. [1]

Класифікувати методи захисту бездротової мережі можна за різними ознаками, в першу чергу існують методи фізичного, технічного та програмного захисту. В даному дослідженні акцент робиться на останньому, як такому, що є найбільш прогресивним. Методи програмного захисту у свою чергу поділяються на методи обмеження доступу, методи автентифікації і шифрування [1].

Одним із методів обмеження доступу є фільтрування MAC-адрес. Даний метод дозволяє визначити список пристроїв і дозволити лише цим пристроям доступ до вашої мережі Wi-Fi (whitelist), або навпаки заборонити певним пристроям доступ (blacklist). На жаль, цей метод ефективний лише в теорії, на практиці такий захист проблемно налаштовувати і дуже легко обійти. MAC-адреси можуть легко підробляти (клонувати) в багатьох операційних системах, тому будь-який пристрій може претендувати на одну з дозволених унікальних MAC-адрес. Вони надсилаються повітрям, коли кожен пакет даних переходить до пристрою та з нього, оскільки MAC-адреса використовується для того, щоб кожний пакет даних потрапляв на правильний пристрій. Тож цей метод, хоча і існує, проте не забезпечує ефективного захисту мережі.

Ще одним методом обмеження доступу є режим прихованого SSID. SSID (Service Set Identifier) – це ідентифікатор мережі, який за замовченням надсилається маршрутизатором або точкою доступу бездротової мережі у режимі broadcast, тобто всім. Зазвичай точки доступу мережі Wi-Fi надсилають своє мережеве ім'я як один з інформаційних елементів, які входять до деяких кадрів керування, ці елементи, або маяки, з інформаційним елементом, ідентифікатором якого є 0. Приховати SSID, тобто припинити його транслювати в ефір, також вважається одним із методів захисту. Проте, на мою думку, це ще один не ефективний і скоріше теоретичний метод захисту. Один із фахівців Microsoft Стів Райлі про даний метод висловився так: «SSID – це мережеве ім'я, а не пароль. Бездротова мережа має SSID, щоб відрізняти її від інших бездротових мереж поблизу. SSID ніколи не розроблявся, щоб бути прихованим, і тому не забезпечить вашу мережу будь-яким захистом, якщо ви намагаєтесь сховати його» [2]. Даний метод не є ефективним, через те, що ідентифікатор "прихованої" мережі дуже легко знайти з допомогою короткочасного програмного сканування всіх доступних мереж в радіусі доступу.

Наступним методом обмеження доступу є статична IP-адресація. Цей метод захисту полягає у відключені динамічного призначення локальних IP-адрес центральною станцією

(маршрутизатором), натомість вимагаючи від користувачів вручну налаштовувати відповідні параметри мережі (адресу, маску, DNS-сервер, шлюз, тощо). Про те цей метод також не є досить ефективним, адже не забезпечує достатнього захисту від злому. До того ж, такий спосіб адресації значно ускладнює адміністрування мережі, зокрема в частині додавання нових вузлів та погіршує масштабування мережі, що неприпустимо в бездротових мережах, адже вони, навпаки, мають покращувати цей параметр. Тож загалом вищеописані методи обмеження доступу сьогодні не є ефективними при побудові системи захисту від кіберзагроз бездротових мереж.

Наступна категорія методів захисту - це методи автентифікації. До них належать відкрита автентифікація, автентифікація зі спільним ключем (WEP, WPA) і автентифікація за допомогою RADIUS-сервера.

Відкрита автентифікація дозволяє будь-якому бездротовому пристрою автентифікуватись, а потім намагатися встановити зв'язок з точкою доступу. Це не завжди означає, що одразу після автентифікації буде надано доступ до мережі. Після автентифікації може бути запитано пароль, ключову фразу, додаткові ідентифікаційні дані, тощо. Проте, такий метод автентифікації також не захищає мережу від зловмисників і може використовуватись лише на точках доступу, що відділені від основної мережі додатковими засобами захисту, наприклад брандмауером.

Автентифікація зі спільним ключем (WEP, WPA). Даний метод автентифікації є найпопулярнішим, а його ефективність залежить від стандарту захисту, який використовується для його реалізації. Під час автентифікації за допомогою спільного ключа, ключі клієнта та точки доступу повинні співпадати. Першим стандартом захисту з використанням спільного ключа був WEP (Wired Equivalent Privacy), проте попри свою гучну назву (Захист еквівалентний дротовому) цей стандарт має слабкі місця, через які процес несанкціонованого доступу до мережі стає дуже простим. До переваг даного алгоритму можна віднести лише швидкодію та простоту реалізації. Що ж стосується недоліків, то основним є те, що на сьогодні існують дієві методи атаки на цей алгоритм, що робить його використання не доцільним в сучасних системах. Тому цей стандарт хоч і підтримується більшістю маршрутизаторів, проте з 2004 року офіційно вважається застарілим. На зміну стандарту WEP прийшов стандарт WPA (Wi-Fi Protected Access) і цей стандарт виключив можливість простого способу атаки через прослуховування трафіка і, відповідно, прибрав необхідність повторно використовувати ключі шифрування. В основі стандарту WPA лежить протокол тимчасової цілісності ключів TKIP (Temporary Key Integrity Protocol). TKIP динамічно генерує новий 128-бітний ключ для кожного пакета і тим самим запобігає WEP-скомпрометованим типам атак. TKIP та відповідний стандарт WPA реалізують три нові функції безпеки для вирішення проблем безпеки, що виникали в WEP-захищених мережах [1]. По-перше, TKIP реалізує ключову функцію змішування, яка поєднує таємний корінний ключ з вектором ініціалізації, перш ніж передавати його до ініціалізації. По-друге, WPA реалізує лічильник послідовності, щоб захистити мережу від повторних атак. Пакети, що надходять не по встановленому порядку, будуть відхилені точкою доступу. По-третє, TKIP реалізує 64-розрядну перевірку цілісності повідомлень (MIC). TKIP гарантує, що кожен пакет даних надсилатиметься з унікальним ключем шифрування. Змішування ключів збільшує складність розшифровування ключів, надаючи зловмиснику суттєво менше даних, які були зашифровані за допомогою будь-якого одного ключа. Перевірка цілісності повідомлення запобігає прийняттю підроблених пакетів. У WEP було можливим змінити пакет, вміст якого був відомий, навіть якщо він не був розшифрований. Проте, незважаючи на ці зміни, слабкість захисту деяких з цих доповнень дозволила створити нові, хоч і більш складні, способи атак. Протокол TKIP не вважається надійним і офіційно не підтримується стандартом 802.11 з 2012 року [2].

Із різноманітності методів захисту для побудови бездротової Wi-Fi мережі найбільш ефективним є комбінація використання стандарту захисту WPA2 та протоколу шифрування CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) з

використанням складного ключа доступу (наприклад 14-и значного набору випадкових цифр та літер).

WPA2 виправила помилки попереднього стандарту і в основі даного стандарту лежить протокол шифрування CCMP, який в свою чергу базується на принципово новому алгоритмі шифрування AES (Advanced Encryption Standard). AES працює на принципі проектування, відомому як мережа заміщення-перестановки, що поєднує як заміщення, так і перестановку, і швидко працює як у програмному, так і в апаратному забезпеченні. Хоч і дана модель захисту не є досконалою і її ефективно та відносно просто можна атакувати при використанні слабкого кодового слова (паролю), такого як словникове слово, простий набір цифр, тощо. Вдала атака на мережу, захищену за стандартом WPA2 з ключем, розміром 256 біт хоча і можлива теоретично, проте вимагає високої кваліфікації зловмисника, спеціального програмного/технічного забезпечення, та, що найголовніше, значного проміжку часу. Проте, і ці методи організації захисту не є досконалими і, окрім програмного захисту, потрібно також враховувати необхідність постійного моніторингу роботи мережі, організацію технічного та фізичного захисту [3].

Автентифікація за допомогою RADIUS-сервера. Remote Authentication Dial In User Service (RADIUS) або Віддалений ідентифікаційний набір в службі користувача - це протокол, що забезпеує трирівневу систему: автентифікація, авторизація та облік і використовується для віддаленого доступу до мережі. Ідея полягає в тому, що існує сервер, який виконує функції «охоронця», перевіряючи ідентифікацію через ім'я користувача та пароль, які вже заздалегідь визначені користувачем. Сервер RADIUS також може бути налаштований для виконання політик та обмежень користувачів, а також запису облікової інформації, такої як час підключення для таких цілей, як платіж. Такий метод захисту досить надійний, проте вимагає додаткового обладнання, налаштування та може застосовуватись лише в комбінації з іншими методами захисту. Такий підхід захисту бездротових мереж, як правило застосовують у великих корпоративних мережах.

Провівши аналіз та порівнявши особливості методів захисту слід зауважити, що технології обмеження доступу не є надійними при побудові систем захисту комп’ютерних мереж стандарту IEEE 802.11, а що стосується методів авторизації та шифрування, то лише використання комбінації сучасних протоколів/алгоритмів та коректне налаштування мережевого обладнання дозволяє отримати прийнятний рівень безпеки.

Література

1. О. Юдін, Г. Конахович, О. Корченко, Захист інформації в мережах передачі даних: підруч. К.: Вид-во ТОВ НВП “ІНТЕРСЕРВІС”, 2009, 714 с.
2. ««S. Riley, Myth vs reality: Wireless SSIDs». [Електронний ресурс] [Веб-сайт]. - Режим доступу: https://blogs.technet.microsoft.com/steriley/2007/10/16/myth-vs-reality-wireless-ssids. [дата звернення: 14.04.2019].
3. Кіберполіція: захист мереж WI-FI - на дуже низькому рівні, 2017. [Електронний ресурс]. Режим доступу: https://www.ukrinform.ua/rubric-technology/ 2281044-kiberpolicia-zahist-merez-wifi-na-duze-nizkomu-rivni.html [дата звернення: 14.04.2019].