**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**Західноукраїнський національний університет**
**Факультет комп'ютерних інформаційних технологій**
Кафедра кібербезпеки

БАРАНЮК Володимир Володимирович

# Механізми інформаційної безпеки при розгортанні систем широкосмугового зв'язку Wi-Fi і Wimax / Information Security Mechanisms in Deploying Wi-Fi and Wimax Broadband Communication Systems

спеціальність: 125 – Кібербезпека

освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБм -21
В.В. Баранюк

Науковий керівник
к.т.н., доцент С.В.Івасьєв

Кваліфікаційну роботу
Допущено до захисту:

«____» _____ ___2023 р.

Завідувач кафедри

_____ **В.В.Яцків**

**ТЕРНОПІЛЬ - 2023**

# АНОТАЦІЯ

Кваліфікаційна робота на тему «Механізми інформаційної безпеки при розгортанні систем широкосмугового зв'язку Wi-Fi і Wimax» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека» освітньо-професійної програми «Кібербезпека» написана обсягом 65 сторінок і містить 31 ілюстрацію, 3 таблиці, 1 додаток та 25 джерел за переліком посилань.

Метою кваліфікаційної роботи полягає в дослідженні досліджені вразливостей безпровідних комп'ютерних мереж.

Проведено аналіз вразливостей комп'ютерних мереж з метою підвищення рівня їхньої безпеки. Досліджено атаки на локальну мережу для виявлення потенційних загроз і розробки заходів протидії їм.

Досліджено можливості сканування мережі на вразливості для розробки превентивних заходів і виявлення потенційних ризиків.

Проаналізувано протоколи безпеки Wi-Fi для визначення їх ефективності та розробки рекомендацій щодо покращення захисту бездротових мереж. Проаналізувано протокол безпеки WPA2 Enterprise з метою виявлення можливих слабкостей і розробки заходів для підвищення безпеки. Досліджено можливі атаки на Wi-Fi для розробки методів їхнього виявлення та захисту від них.

Досліджено протокол автентифікації Pkmv1 з метою виявлення слабкостей і можливих напрямків їх виправлення. Досліджено протокол автентифікації Pkmv2 для визначення ефективності і безпеки цього механізму. Проведено дослідження проблеми безпеки протоколів PKMv1 та PKMv2 для забезпечення більш високого рівня захисту мережевих систем, що їх використовують.

Ключові слова: Wi-Fi, Wimax, NTLM, Pkmv1, PKMv2. WPA2.

# ABSTRACT

The qualification work on the topic "Information Security Mechanisms in Deploying Wi-Fi and Wimax Broadband Communication Systems" for obtaining the Master's degree in the specialty 125 "Cyber Security" of the educational and professional program "Cyber Security" is written in the volume of 65 pages and contains 31 illustrations, 3 tables, 1 appendix and 25 sources in the list of references.

The purpose of the qualification work is to investigate the vulnerability of wireless computer networks.

An analysis of the vulnerabilities of computer networks was carried out in order to increase their security level. Attacks on the local network were studied to identify potential threats and develop measures to counter them.

The possibility of scanning the network for vulnerabilities to develop preventive measures and identify potential risks was studied.

Wi-Fi security protocols are analyzed to determine their effectiveness and develop recommendations for improving the protection of wireless networks. The WPA2 Enterprise security protocol was analyzed in order to identify possible weaknesses and develop measures to improve security. Possible attacks on Wi-Fi have been studied in order to develop methods for their detection and protection against them.

The Pkmv1 authentication protocol was studied in order to identify weaknesses and possible directions for their correction. The Pkmv2 authentication protocol was studied to determine the effectiveness and security of this mechanism. The security problem of PKMv1 and PKMv2 protocols has been studied to ensure a higher level of protection for network systems that use them.



Keywords: Wi-Fi, Wimax, NTLM, Pkmv1, PKMv2. WPA2.

ЗМІСТ

# ВСТУП

**Актуальність роботи.** Дослідження цієї теми дозволяє розробляти та вдосконалювати стратегії захисту в інформаційних системах, які використовують бездротові технології для передачі даних. Дослідження механізмів аутентифікації користувачів та пристроїв в бездротових мережах, а також засобів контролю доступу для забезпечення легітимного використання ресурсів дозволить підвищити рівень інформаційної безпеки.

**Мета роботи** полягає в дослідженні вразливостей безпровідних комп'ютерних мереж:

Для досягнення даної мети ставились наступні завдання:

- Провести аналіз вразливостей комп'ютерних мереж.
- Дослідити атаки на локальну мережу.
- Проаналізувати можливості підміни трафіку частково або окремих пакетів даних.
- Дослідити можливості сканування мережі на вразливості.
- Проаналізувати протоколи безпеки WiFI.
- Проаналізувати протокол безпеки WPA2 Enterprise.
- Дослідити вразливості технології Wi-Fi.
- Розглянути інструменти для моніторингу бездротових мереж.
- Дослідити можливі атаки на Wi-Fi.
- Розглянути архітектуру WIMAX.
- Дослідити протокол автентифікації Pkmv1.
- Дослідити протокол автентифікації Pkmv2.
- Провести дослідження проблеми безпеки протоколів PKMv1 та PKMv2.

**Об'єкт дослідження** – процес авторизації та обміну пакетами в безпровідних комп'ютерних мережах Wi-Fi та Wimax.

**Предмет досліджень** – алгоритми та механізми інформаційної безпеки при розгортанні систем безпровідного та широкосмугового зв'язку Wi-Fi і Wimax.

**Методи дослідження базуються** на тестах на проникнення, автоматизації атак на параметри сесії, алгоритмах аналізу запитів.

**Наукова новизна** одержаних результатів визначається наступним чином:

– Формалізовано моделі атак на безпровідні мережі WiFi та виявлено слабкі сторони протоколу PKMv2 для широкосмугового стандарту Wimax.

**Практична цінність** одержаних результатів полягає в тому, що:

- Досліджено системи аналізу стану безпровідних мереж та їхні протоколи безпеки.

**Публікації та апробація результатів досліджень** приведена в:

1. Баранюк В.В., Николишин В.І., Лизун Я.І. Налаштування систем широкосмугового звязку Wi-Fi і Wimax. Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно – інтегровані технології» (АКІТ -2023), Тернопіль, 2023. С. 139 -142.
2. Баранюк В.В. Механізми інформаційної безпеки при розгортанні систем широкосмугового зв'язку .Матеріали науково-практичного симпозіуму "Захист інформації", Тернопіль, 2023. С. 12-15.

# 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

## 1.1 Аналіз вразливостей комп’ютерних мереж

Більшою мірою приділятимемо увагу мережам на базі TCP/IP стека, які можуть використовуватися для роботи всередині невеликої організації.

Для аналізу, які атаки існують для сучасних і не дуже мереж, необхідно провести їх класифікацію, щоб можна було розібратися, в тому як вони працюють і на які частини мережі можуть вплинути.

Найбільш популярною класифікацією атак на мережу є зіставлення атак рівням теоретичної моделі OSI. Тобто всі атаки розглядаються в контексті того, для чого призначений кожен із рівнів[1].

Змінимо принцип, який використовується для класифікації. За основу класифікації візьмемо етапи тестування на проникнення, які зазвичай виробляють визначення найбільш ймовірних сценаріїв атаки зловмисника на мережу організації. Найчастіше тестування на проникнення проводиться у 2 простих етапи. Перший - збір максимально доступної інформації про систему і другий - безпосередньо атака. Якщо говорити при цьому про мережеву взаємодію, то атакою можна вважати і стандартний функціонал, який може використовуватися не за призначенням.

Класифікація виглядає так:

- пошук хостів, які мають доступ до зовнішньої мережі;
- пошук хостів, які не мають доступу до зовнішньої мережі;
- сканування хостів;
- сніффінг (прослуховування трафіку);
- атаки на локальну мережу;
- заміна трафіку частково чи окремих пакетів даних.

Пошук хостів, які мають доступ до зовнішньої мережі. Хоч і насправді складно назвати дії, що робляться в цій групі атаками, проте без застосування

цієї групи навряд чи може бути успішним хоч якийсь намір на безпеку мережі[2].

Набір атак цієї групи можна назвати специфічним типом сканування мережі. Вони дозволяють ідентифікувати, які саме хости доступні ззовні, тобто визначити, чи є зв'язок з ними. Зазвичай ця група реалізується за рахунок спостереження за стандартними механізмами протоколів, які повинні працювати на доступних хостах.

Можна відзначити, що побудова схеми збору даних про мережу здебільшого спирається на звані RFC. Наприклад, RFC 1122 безпосередньо пропонує рекомендації про те, які існують коди для діагностики стану хоста, що бере участь у взаємодії з мережею інтернет. Таким чином, хоча б частково ці вимоги можна застосувати до хостів, які будуть видно ззовні організації.

Для пошуку живих хостів можна скористатися протоколом ICMP. Цей протокол був створений для того, щоб збирати дані про проблеми в мережі. Здійснити збір даних можна, ґрунтуючись на відповідях від хостів. Загалом протокол підтримує близько 15 спеціальних кодів, які визначають, які проблеми виникли в мережі та повідомити про них усім учасникам або тим, хто зіткнувся з проблемою передачі даних. Для операції збору даних про доступність хоста може бути задіяний щонайменше 1 код, який називається echo запит. Якщо уважно вивчити RFC 1122, можна помітити, що деякі хости ще можуть використовувати такі коди ICMP — 13, 15, 17. На підставі хоча б факту відповіді досліджуваного хоста можна судити про його доступність.

Приблизно за тим же принципом можна проводити пошук хостів, якщо використовувати найбільш популярні для мережевої взаємодії протоколи: TCP, UDP, SCTP, HTTP. У цих випадках можуть використовуватися звичайні алгоритми налаштування взаємодії, які передбачаються протоколом у документації. І так само, як і з ICMP, тут будь-які відповіді від цільових хостів інтерпретуватимуться як наявність доступності хоста в принципі.

Всі дослідження можна проводити за допомогою 2 інструментів та їх аналогів:

- masscan - тільки TCP;

- nmap – універсальний, але може бути недостатньо швидким.

Пошук хостів, які не мають доступу до зовнішньої мережі може включати попередній пункт, але, крім нього, цей крок можна поширити, залежно від принципів побудови мережі, на додаткові протоколи та методи отримання даних. Пункт можна поділити на 2 частини. Перша — це пасивний збір даних за можливості прослуховувати трафік: деякі протоколи прикладного рівня можуть розкривати подробиці про те, що передається і ким[3].

Друга частина включає методи на мережу. Здійснюються вони у вигляді використання протоколів:

- ARP – механізм запиту даних про IP адреси та MAC адреси хостів;

- NetBIOS – механізм, який називається Browser. У ньому передається інформація про назву операційної системи та її версії;

- IPv6 — надсилання мультикастових запитів для отримання даних про доступні хости.

Всі види атак можуть бути зроблені інструментами:

- nmap.

- bettercap.

- responder.

## 1.2 Прослуховування трафіку

Атака, яка може бути успішна у випадку або якщо неправильно налаштовано мережеве обладнання, або через особливості топології мережі. Застосовується для вивчення даних у трафіку, а також для отримання даних, які можуть бути використані для підвищення рівня доступу до мережі або на окремих системах, що беруть участь у мережевій взаємодії. У більшості

випадків збір даних можна проводити з операційних систем хостів, хоча і з мережевих пристроїв ті самі дії так само можливі.

Подібні атаки можуть бути здійснені за допомогою:

- wireshark.
- tcpdump.
- bettercap.

## 1.3 Атаки на локальну мережу

Атаки, які в більшості випадків змінюють топологію мережі та заповнюють мережу великою кількістю однотипних пакетів. Робиться це для того, щоб не відбувалося відновлення початкового стану маршрутів мережі.

ARPSpoofing - базовий блок для всіх атак, які мають на увазі зміну трафіку в мережі. Має на увазі відправлення великої кількості пакетів з даними, що дозволяють зловмиснику прикидатися будь-яким хостом у мережі. Найбільш вигідні хости в цьому випадку - gateway або хост, де розміщуються цільові для атаки сервіси[4].

Dynamic Trunking - чи не єдиний ефективний засіб для боротьби зі зміною топології мережі може бути використання стандарту 802.1Q VLAN, то, природно, при його виявленні потрібно перевірити можливість атак на його неправильну конфігурацію. Цей вид атаки передбачає, що при доступі хоча б одного VLAN можна перевести з'єднання в стан, при якому будуть видно всі дані з інших VLAN.

VLAN Hopper — атака, яка дозволяє шукати хости у сусідніх VLAN та надсилати повідомлення.

Double Tagging – атака, яка можлива, якщо атакуючий знає номер VLAN, ip адресу системи жертви. Атакуючий у цьому випадку може запакувати повідомлення для надсилання цільової системи. Недоліком атаки вважатимуться відсутність зворотний зв'язок, оскільки цільова система зможе відправляти відповіді.

Основні інструменти для атак:

- bettercap.

- yersinia — хоч і старий інструмент, але лише в ньому є підтримка пропрієтарних для Cisco протоколів.

- frogger.

- scapy.

- nmap.

- responder — корисний для середовищ із операційною системою Windows.

## 1.4 Підміна трафіку частково або окремих пакетів даних

Атаки цієї групи мають на увазі повний або частковий контроль над інформацією, що передається. Причому в деяких випадках дані проходитимуть через хост атакуючого, а в деяких лише перші пакети.

Заміна сервера DHCP — використовується для контролю надавання адреси для учасників у мережі. Може бути використане для крадіжки даних із додатків[5].

Підміна сервера DNS. Багато програм, які працюють з мережею без належних перевірок, можуть зайво довіряти серверу, який використовується для реалізації роботи програми. Може бути використано для компрометації даних, що відправляються на сервер, при проведенні одночасної атаки на зміну стандартного маршруту всередині мережі.

Підміна gateway – за рахунок механізмів динамічного налаштування маршрутів мережі можна прослуховувати всю інформацію, яка пролітає через мережу.

Підміна сервісів ОС – використання недосконалості протоколів операційних систем та мережевих пристроїв. Найбільш популярна при дії на мережу, учасниками якої є машини під керуванням Windows.

Інструменти для атак:

- bettercap.

- nmap.

- responder.

Спробуємо відтворити дані атаки та спробуємо від них захиститись за допомогою доступних мережевих механізмів ОС та пристроїв.

## 1.5 Сканування мережі на вразливості

Сканування є основним способом збору даних у мережі та дозволяє без знання топології зібрати актуальні дані, а також здійснити пошук сервісів, що працює на хостах. Воно базується на знанні особливостей поведінки хостів та протоколів при порушенні стандартних алгоритмів взаємодії[6].

Кожен протокол, який можна використовувати передачі інформації, зберігає дані у двох частинах. Перша — заголовок, виходячи з якого працюють службові алгоритми протоколу. Тут можуть бути перераховані налаштування з'єднання, описані основні правила обробки та передачі інформації. Схематично ці частини можна так, як на рисунку 1.1.

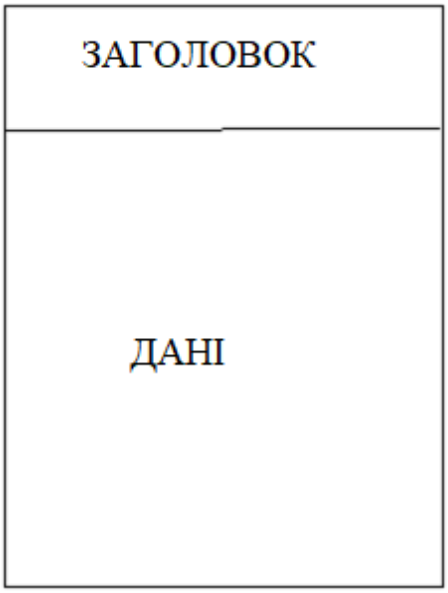


Рисунок 1.1 – Загальна структура пакету

Найпоширеніший протокол, який дозволяє проводити сканування і може бути виявлений практично у всіх сучасних мережах, це протокол TCP. Протокол є одним із основних протоколів найпопулярнішої моделі TCP/IP. Протокол дозволяє налаштовувати з'єднання та контролювати з'єднання протягом усієї взаємодії. І саме цей механізм контролю стану з'єднання використовується більшістю способів сканування. На сьогоднішній день відомі такі варіанти сканування за допомогою TCP протоколу в порядку зменшення ефективності[7]:

1. Connect Scan - звичайний алгоритм налаштування з'єднання, що реалізується мережевими функціями операційної системи.

2. SYN Scan — сканування, яке базується на надсиланні пакетів, що містять лише один встановлений прапор контролю з'єднання — SYN.

3. ACK Scan — сканування, яке ґрунтується на надсиланні пакетів, що містять лише один встановлений прапор контролю з'єднання — ACK.

4. Maimon — сканування, яке ґрунтується на відправленні пакетів, що містять кілька встановлених прапорів контролю з'єднання — FIN/ACK.

5. Null scan — сканування, яке ґрунтується на відправленні пакетів, що не містять жодного прапора, який відповідає за контроль з'єднання.

6. FIN scan — сканування, яке ґрунтується на надсиланні пакетів, що містять лише один встановлений прапор контролю з'єднання — FIN.

7. Xmas Scan — сканування, яке ґрунтується на надсиланні пакетів, що містять на кожен запит різні прапори з усіх доступних для контролю з'єднання.

Кожен із перелічених типів сканування грунтується практично цілком на поведінці хоста щодо керуючих прапорів, які розташовуються в заголовку та відповідають за контроль стану з'єднання.

Перші два види сканування можна знайти в будь-якому інструменті, який надає функції пошуку активних хостів у мережі. Інші типи сканувань через те, що використовують непрямі ознаки стану хостів і сервісів, можуть бути використані лише як додатковий фактор підтвердження правильності

проведення сканування, або для тестування роботи програми або операційної системи з протоколом TCP[9].

Кожен із видів сканування може бути ідентифікований засобами виявлення вторгнень (IDS) та вбудованими алгоритмами аналізу трафіку в мережевому обладнанні. У силу того, що сканування здійснюється на основі легітимного функціоналу протоколу, то алгоритми, що виявляють подібну діяльність, можуть не правильно робити висновок про те, що сканування дійсно відбувається. Тобто нотифікація про проведення сканування може ще свідчити про велику кількість помилок передачі даних у мережі, які можуть виникати внаслідок неправильного налаштування мережного обладнання або поломки[10].

Для тестів використовуватимемо віртуальний стенд на базі VBox, топологія мережі буде побудована на основі типу з'єднання Nat Network. По суті це звичайна мережа з Gateway, який може звертатися в мережу. У мережі будуть знаходитись 3 хости — Kali Linux, Server Debian 20.04 та Windows 10. Для проведення сканування будемо використовувати:

- rustscan.
- masscan.
- nmap.
- naabu.

Rustscan написаний мовою програмування Rust, як запевняють автори, є одним з найшвидших безкоштовних сканерів, доступних на сьогоднішній день. І частково це правда, але насправді цей сканер просто обгортка над nmap. Із заявлених можливостей:

- сканування всіх портів за 3 секунди;

- підтримка движка для автоматизації процесу сканування, можна перенаправляти результати Nmap;

- адаптивне навчання для покращення процесу сканування;

- можливість працювати з адресами, введеними в різних форматах IPv6, CIDR і т.д.

З неочевидних недоліків варто привести обмеження – пулами та CIDR сканувати за допомогою цього інструменту не вийде. Вивалюватиметься помилка `thread 'main' panicked at 'Too many open files.' Вирішити цю проблему можна шляхом використання прапора -b, але в результаті вийде сканувати тільки за однією адресою за один запуск.

Сканер можна встановити різними способами як готовий пакет або як Docker image. На рисунку 1.2 приведено приклад сканування мережі.


Рисунок 1.2 – Сканування засобом Rustscan

Трафік у такому разі виглядає ось так, як показано на рисунку 1.3.

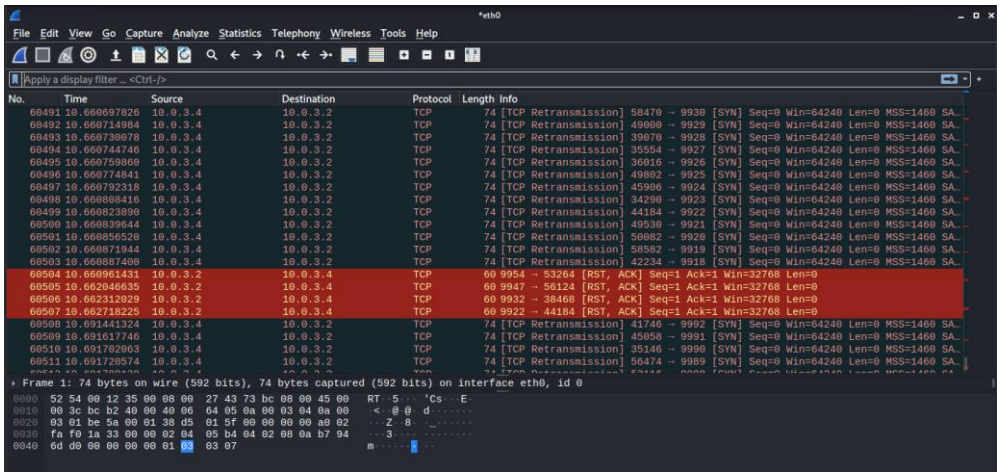


Рисунок 1.2 – Результат тперехоплення трафіку

Інструмент може створювати високе навантаження на мережу. Основні запити, які виконуються за замовчуванням, це запити SYN. Тому блокувати його дії можна досить просто, наприклад, засобами операційної системи через фаєрвол. Для iptables правила можуть виглядати так [11]:

IPTABLES -A INPUT -p tcp -tcp-flags SYN,ACK SYN,ACK -m state -state NEW -j DROP

IPTABLES -A INPUT -p tcp -tcp-flags ALL NONE -j DROP

Masscan - сканер, який можна використовувати для дуже великої кількості хостів та просканувати чи не весь інтернет за лічені хвилини. Можливо, це в першу чергу через власний мережевий стек, який в обхід стека операційної системи самостійно відправляє запити в мережу і займається його обробкою.

Інструмент корисний для виявлення доступних хостів у мережі. Запустити його можна ось так, як показано на рисунку 1.3.


Рисунок 1.3 – Виявлення доступних хостів Masscan

Трафік, який генерує інструмент, містить велику кількість пакетів із встановленим SYN прапором.

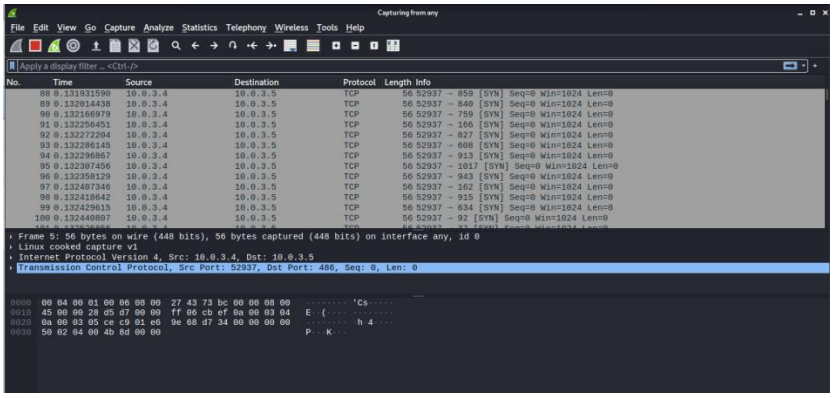


Рисунок 1.4 – Перехоплення результуючого трафіку

Для блокування такої активності можна використовувати ті ж правила на фаєрволлі, які надані в розділі rustscan[12].

Nmap - найпопулярніший інструмент для сканування та, мабуть, найстаріший серед доступних. Він може бути запущений для сканування всіма способами, описаними в розділі `Сканування`. Для цього можна використовувати прапор, який приймає як значення першу літеру в назві типу сканування. Наприклад, SYN сканування можна виконати так, як показано на рисунку 1.5.

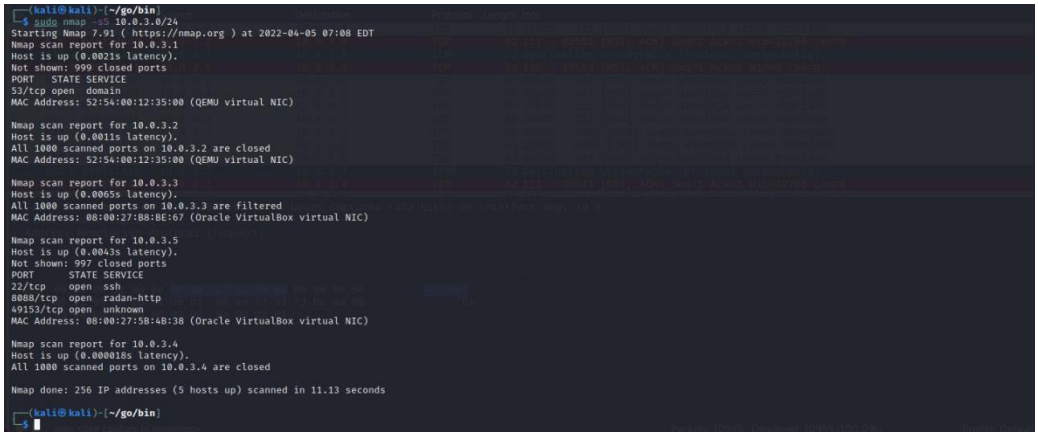


Рисунок 1.5 – Сканування хостів за допомогою Nmap

А трафік для цих типів сканування виглядає так, як зображено на рисунку 1.6. SYN Scan і Connect Scan, nmap це об'єднані типи сканування.

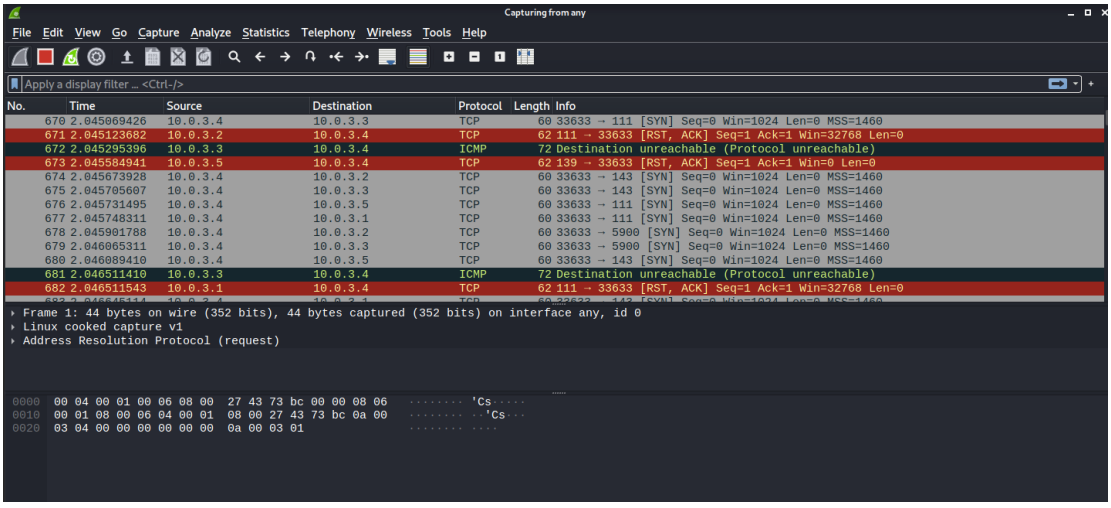


Рисунок 1.5 – Трафік при скануванні nmap

Більшість типів сканувань можна перекрити, якщо скористатися такими правилами для фаєрволу [13]:

IPTABLES -A INPUT -p tcp -tcp-flags SYN,FIN SYN,FIN -j DROP

IPTABLES -A INPUT -p tcp -tcp-flags SYN,RST SYN,RST -j DROP

IPTABLES -A INPUT -p tcp -tcp-flags ALL SYN,RST,ACK,FIN,URG -j DROP

IPTABLES -A INPUT -p tcp -tcp-flags FIN,RST FIN,RST -j DROP

IPTABLES -A INPUT -p tcp -tcp-flags ACK,FIN FIN -j DROP

IPTABLES -A INPUT -p tcp -tcp-flags ACK, PSH PSH -j DROP

IPTABLES -A INPUT -p tcp -tcp-flags ACK,URG URG -j DROP

Naabu - сканер написаний мовою програмування Go. Спрощує процес сканування і по суті використовує лише один тип сканування SYN Scan. Запустити можна так, як показано на рисунку 1.6.


Рисунок 1.6 – Сканування Naabu

Трафік відповідно буде таким, як на рисунку 1.7. Наабу (Naabu) - це відкритий сканер безпеки мереж, який призначений для знаходження вразливостей та збір інформації про відкриті порти, сервіси та інші характеристики мережевих систем. Наабу був розроблений для ефективного

сканування мереж з використанням активного підходу, тобто він взаємодіє з системами у мережі для визначення їхнього стану та ідентифікації можливих вразливостей[14].

Основні особливості Naabu включають:

Активний сканування портів: Naabu використовує активний метод сканування для визначення відкритих портів на цільовій системі. Він відправляє спеціально сформовані запити на цільову систему та аналізує відповіді для визначення стану портів.

Виявлення сервісів: Після визначення відкритих портів, Naabu намагається визначити, які конкретні служби чи сервіси працюють на цих портах. Він аналізує banner-інформацію та інші параметри для ідентифікації програм, які слухають на визначених портах.

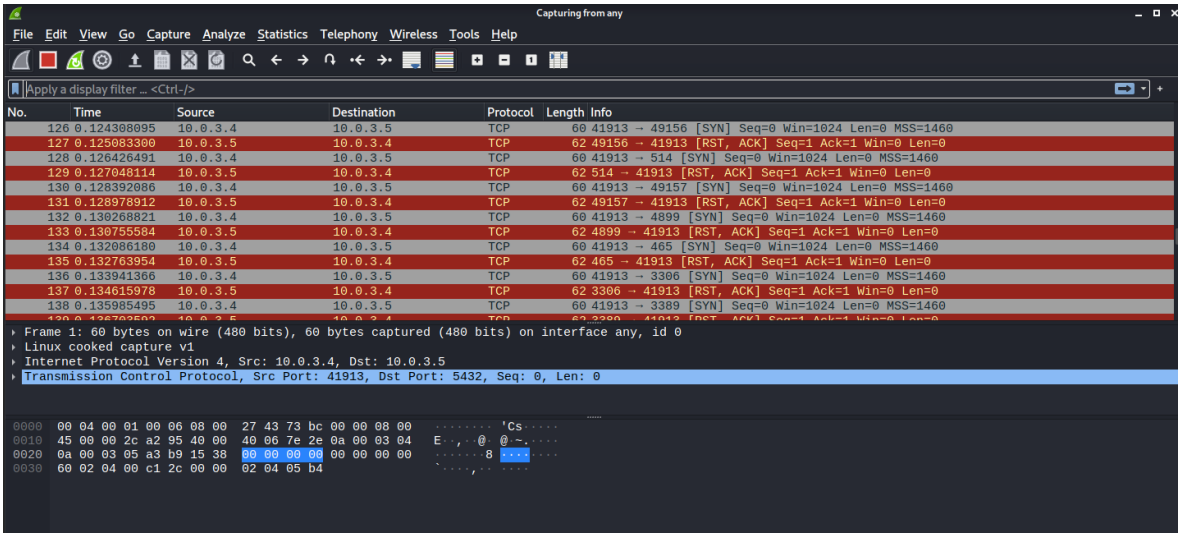


Рисунок 1.7 – Трафік при скануванні Naabu

Виявлення вразливостей: Naabu може також виявляти відомі вразливості, використовуючи інформацію про версії служб та програм, отриману під час сканування. Він може порівнювати цю інформацію з базами даних вразливостей для ідентифікації систем, які можуть бути піддатливими до атак[15].

Підтримка виводу JSON та CSV: Naabu може генерувати результати скану у форматі JSON або CSV, що полегшує автоматизацію та інтеграцію результатів у різні інструменти та системи.

Для ефективного виконання сканування, Naabu використовує потужний інструмент сканування, який може працювати швидко та ефективно в обширних мережах.

Захист від такого сканування можливий з використанням правил з пункту rustscan.

# 2 ДОСЛІДЖЕННЯ БЕЗПЕКИ WIFI

## 2.1 Протоколи безпеки WiFI

Останнім часом з'явилося багато «викривальних» публікацій про зламування будь-якого чергового протоколу чи технології, що компрометує безпеку бездротових мереж.

Будь-яка взаємодія точки доступу (мережі) та бездротового клієнта побудована на:

- Аутентифікації — як клієнт та точка доступу надаються один одному і підтверджують, що вони мають право спілкуватися між собою;

- Шифрування — який алгоритм скремблювання даних, що передаються, застосовується, як генерується ключ шифрування, і коли він змінюється[16].

Параметри бездротової мережі, в першу чергу її ім'я (SSID), регулярно анонсуються точкою доступу в широкомовних пакетах. Крім очікуваних налаштувань безпеки, передаються побажання по QoS, за параметрами 802.11n, швидкості, відомості про інших сусідів та інше. Аутентифікація визначає, як клієнт представляється точці. Можливі варіанти:

- Open — так звана відкрита мережа, в якій всі пристрої, що підключаються, авторизовані відразу.

- Shared — Справжність пристрою, що підключається, повинна бути перевірена ключем/паролем.

- EAP — автентифікація пристрою, що підключається, повинна бути перевірена за протоколом EAP зовнішнім сервером.

Відкритість мережі не означає, що будь-хто охочий зможе безкарно з нею працювати. Щоб передавати в такій мережі дані, необхідно збіг алгоритму шифрування, що застосовується, і відповідно йому коректне встановлення шифрованого з'єднання. Алгоритми шифрування, що використовуються в WiFI наступні[17]:

- None — відсутність шифрування, дані передаються у відкритому вигляді.

- WEP — заснований на алгоритмі RC4 шифр із різною довжиною статичного чи динамічного ключа (64 або 128 біт).

- CKIP — проприєтарна заміна WEP від Cisco, ранній варіант TKIP.

- TKIP — покращена заміна WEP з додатковими перевірками та захистом.

- AES/CCMP – найбільш досконалий алгоритм, заснований на AES256 з додатковими перевірками та захистом.

Комбінація Open Authentication, No Encryption широко використовується в системах гостьового доступу на кшталт надання Інтернету в кафе чи готелі. Для підключення потрібно знати лише ім'я бездротової мережі. Найчастіше таке підключення комбінується з додатковою перевіркою на Captive Portal шляхом редиректу користувача HTTP-запиту на додаткову сторінку, на якій можна запитати підтвердження (логін-пароль, згоду з правилами тощо).

Шифрування WEP скомпрометоване, і використовувати його не можна (навіть у разі динамічних ключів).

Широко зустрічаються терміни WPA і WPA2 визначають, власне, алгоритм шифрування (TKIP чи AES). У силу того, що вже досить давно клієнтські адаптери підтримують WPA2 (AES), застосовувати шифрування за алгоритмом TKIP немає сенсу[18].

Різниця між WPA2 Personal та WPA2 Enterprise полягає в тому, звідки беруться ключі шифрування, які використовуються в механіці алгоритму AES. Для приватних (домашніх, дрібних) застосувань використовується статичний ключ (пароль, кодове слово, PSK (Pre-Shared Key)) мінімальної довжиною 8 символів, що задається в налаштуваннях точки доступу, і у всіх клієнтів бездротової мережі однаковим. Компрометація такого ключа (звільнений співробітник, вкрадений ноутбук) вимагає негайної зміни пароля у всіх користувачів, що залишилися, що реалістично тільки у разі невеликого

їх числа. Для корпоративних застосувань, як випливає з назви, використовується динамічний ключ, індивідуальний для кожного клієнта, що працює в даний момент. Цей ключ може періодично оновлюватися по ходу роботи без розриву з'єднання, і за його генерацію відповідає додатковий компонент — сервер авторизації, і це завжди RADIUS-сервер. Параметри безпеки зведені у цій таблиці 2.1.

Таблиця 2.1 –

| Властивість | Статичний WEP | Динамічний WEP | WPA | WPA 2 (Enterprise) |
|---|---|---|---|---|
| Ідентифікація | Користувач, комп'ютер, карта WLAN | Користувач, комп'ютер | Користувач, комп'ютер | Користувач, комп'ютер |
| Авторизація | Загальний ключ | EAP | EAP або спільний ключ | EAP або спільний ключ |
| Цілісність | 32-bit Integrity Check Value (ICV) | 32-bit ICV | 64-bit Message Integrity Code (MIC) | CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code — CCM) Part of AES |
| Шифрування | Статичний ключ | Сесійний ключ | Попакетний ключ через TKIP | CCMP (AES) |
| Розподіл ключів | Одноразове, вручну | Сегмент Pair-wise Master Key (PMK) | Похідне від PMK | Похідне від PMK |
| Вектор ініціалізації | Текст, 24 біти | Текст, 24 біти | Розширений вектор, 65 біт | 48-біт номер пакета (PN) |
| Алгоритм | RC4 | RC4 | RC4 | AES |
| Довжина ключа, біт | 64/128 | 64/128 | 128 | до 256 |
| Необхідна інфраструктура | Ні | RADIUS | RADIUS | RADIUS |

Якщо з WPA2 Personal (WPA2 PSK) все зрозуміло, корпоративне рішення потребує додаткового розгляду.

## 2.2 Протокол безпеки WPA2 Enterprise

На стороні клієнта спеціальний компонент програмного забезпечення, supplicant (зазвичай частина ОС) взаємодіє з авторизуючою частиною AAA сервером. У цьому прикладі відображено роботу уніфікованої радіомережі, побудованої на легковажних точках доступу та контролері[19]. У разі використання точок доступу «з операційною системою» всю роль посередника між клієнтами та сервером може на себе взяти сама точка. При цьому дані клієнтського супліканта по радіо передаються сформованими протоколом 802.1x (EAPOL), а на стороні контролера вони обертаються в RADIUS-пакети. Схема взаємодії приведена на рисунку 2.1.

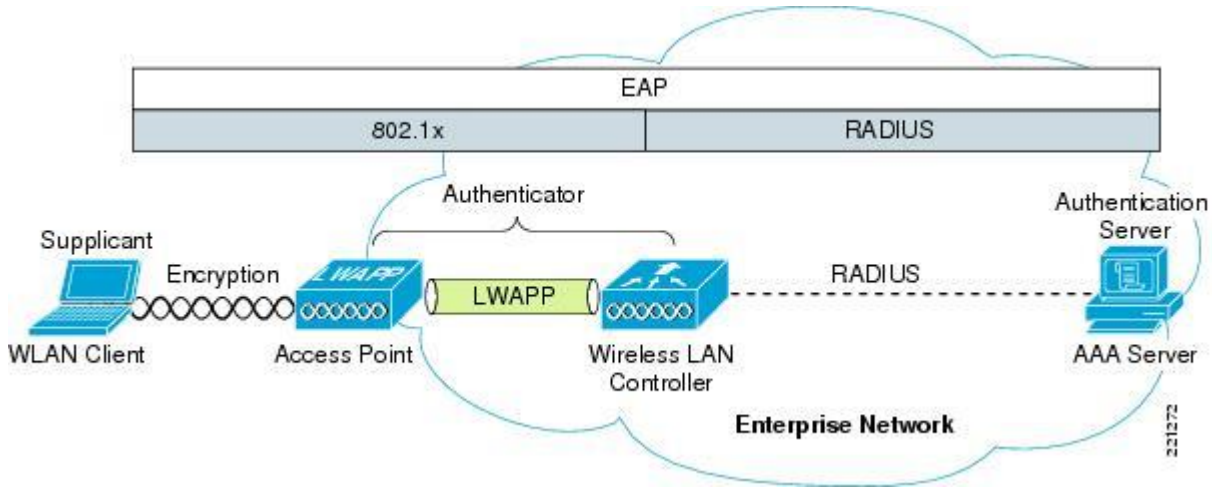


Рисунок 2.1 - Схема застосування механізму авторизації EAP

Застосування механізму авторизації EAP у мережі призводить до того, що після успішної (майже напевно відкритої) автентифікації клієнта точкою доступу (спільно з контролером, якщо він є), остання просить клієнта авторизуватися (підтвердити свої повноваження) у інфраструктурного RADIUS-сервера, як це показано на рисунку 2.2.

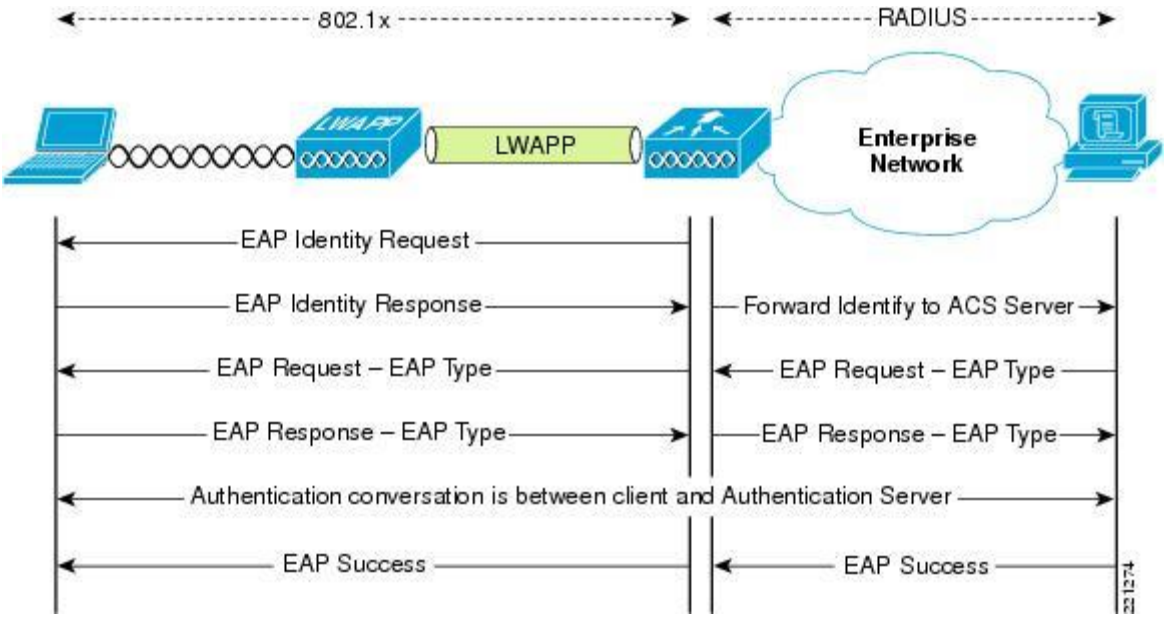


Рисунок 2.2 – Послідовність обміну пакетами за протоколом EAP

Використання WPA2 Enterprise вимагає наявності у мережі RADIUS-сервера. На сьогоднішній момент найбільш працездатними є такі продукти:

- Microsoft Network Policy Server (NPS), колишній IAS – конфігурується через MMC, безкоштовний[20].

- Cisco Secure Access Control Server (ACS) 4.2, 5.3 - конфігурується через веб-інтерфейс, по функціоналу, дозволяє створювати розподілені та відмовостійкі системи.

- FreeRADIUS – безкоштовний, конфігурується текстовими конфігами, в управлінні та моніторингу не зручний.

При цьому контролер уважно спостерігає за обміном, що відбувається, і чекає успішної авторизації, або відмови в ній. При успіху RADIUS-сервер здатний передати точці доступу додаткові параметри (наприклад, в якій VLAN помістити абонента, який йому привласнити IP-адресу, профіль QoS і т.п.). На завершення обміну RADIUS-сервер дає можливість клієнту та точці доступу згенерувати та обмінятися ключами шифрування (індивідуальними, валідними тільки для даної сессії), як показано на рисунку 2.3.

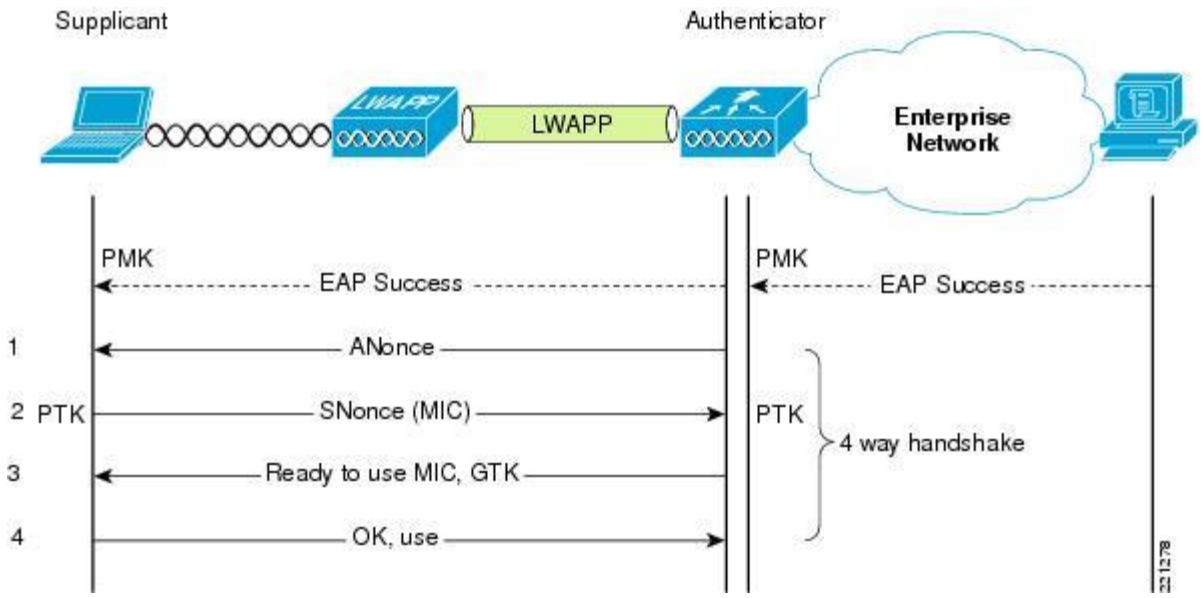


Рисунок 2.3 – 4 кроковий хендшейк

Сам протокол EAP є контейнерним, тобто фактичний механізм авторизації дається відкуп внутрішніх протоколів. На даний момент значного поширення набули такі модифікації протоколу:

- EAP-FAST (Flexible Authentication via Secure Tunneling) – розроблений фірмою Cisco; дозволяє проводити авторизацію за логіном-паролем, що передається всередині TLS тунелю між суппліканом та RADIUS-сервером[21].

- EAP-TLS (Transport Layer Security). Використовує інфраструктуру відкритих ключів (PKI) для авторизації клієнта та сервера (супліканта та RADIUS-сервера) через сертифікати, виписані довіреним центром (CA). Вимагає виписування та встановлення клієнтських сертифікатів на кожен бездротовий пристрій, тому підходить лише для керованого корпоративного середовища. Сервер сертифікатів Windows має засоби, що дозволяють клієнту самостійно генерувати собі сертифікат, якщо клієнт є членом домену. Блокування клієнта легко здійснюється відгуком його сертифіката (чи через облікові записи).

- EAP-TTLS (Tunneled Transport Layer Security) аналогічний EAP-TLS, але під час створення тунелю не потрібний клієнтський сертифікат. У такому

тунелі, аналогічному SSL-з'єднанню браузера, виконується додаткова авторизація (за паролем або ще).

- PEAP-MSCHAPv2 (Protected EAP) — схожий на EAP-TTLS у плані початкового встановлення шифрованого TLS тунелю між клієнтом і сервером, що вимагає серверного сертифіката. Надалі в такому тунелі відбувається авторизація за відомим протоколом MSCHAPv2.

- PEAP-GTC (Generic Token Card) – аналогічно попередньому, але вимагає карт одноразових паролів (і відповідної інфраструктури).

Підтримка будь-якого з EAP методів має забезпечуватися суплікантом на стороні клієнта. Стандартний, вбудований у Windows XP/Vista/7, iOS, Android забезпечує як мінімум EAP-TLS і EAP-MSCHAPv2, що зумовлює популярність цих методів. З клієнтськими адаптерами Intel під Windows поставляється утиліта ProSet, яка розширює доступний список. Це робить Cisco AnyConnect Client (рисунок 2.4).


Рисунок 2.4 – Перелік EAP методів Cisco AnyConnect Client

Усі ці методи (крім EAP-FAST) вимагають наявності сертифіката сервера (на RADIUS-сервері), виписаного центром, що засвідчує (CA). При цьому сертифікат CA повинен бути присутнім на пристрої клієнта в групі довірених (що неважко реалізувати засобами групової політики в Windows).

Додатково EAP-TLS вимагає індивідуального клієнтського сертифіката (рисунок 2.5). Перевірка справжності клієнта здійснюється як за цифровим підписом, так (опціонально) порівняно з наданим клієнтом сертифікатом RADIUS-серверу з тим, що сервер витягнув з PKI-інфраструктури (Active Directory)[22].

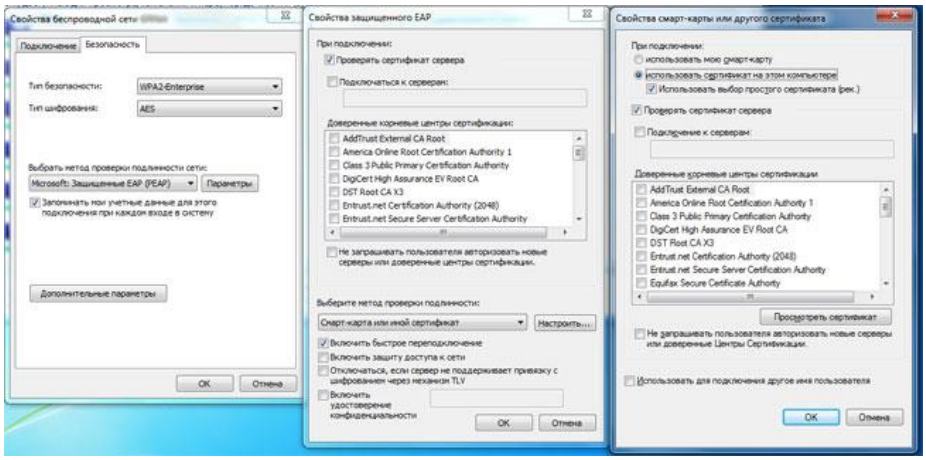

Рисунок 2.5 – Перелік EAP методів доступних у Windows

Зловмисникові, щоб зламати отримати доступ до мережі, яка заснована на WEP, потрібен лише час на перебір IV, і одна з багатьох доступних утиліт сканування.

Для шифрування, заснованого на TKIP чи AES пряме дешифрування можливе теоретично, але практично випадки злому не траплялися.

Звичайно, можна спробувати підібрати ключ PSK або пароль до одного з EAP-методів. Поширені атаки на ці методи не відомі. Можна намагатися застосувати способи соціальної інженерії, або терморектальний криптоаналіз.

Отримати доступ до мережі, захищеної EAP-FAST, EAP-TTLS, PEAP-MSCHAPv2 можна лише знаючи логін-пароль користувача (злом як такий неможливий). Атаки типу перебору пароля, або спрямовані на вразливості в MSCHAP також не можливі або утруднені через те, що EAP-канал клієнт-сервер захищений шифрованим тунелем.

Доступ до мережі, закритої PEAP-GTC, можливий або при зломі сервера токенів, або при крадіжці токена разом з паролем.

Доступ до мережі, закритої EAP-TLS можливий при крадіжці сертифіката користувача (разом з його приватним ключем, звичайно), або при виписуванні валідного, але підставного сертифіката. Таке можливе лише при компрометації центру, що засвідчує, який у нормальних компаніях бережуть як найцінніший IT-ресурс.

Оскільки всі вищезазначені методи (крім PEAP-GTC) допускають збереження (кешування) паролів/сертифікатів, при крадіжці мобільного пристрою атакуючий отримує повний доступ без зайвих питань з боку мережі. Як запобігання може служити повне шифрування жорсткого диска із запитом пароля при включенні пристрою[23].

## 2.3 Вразливості технології Wi-Fi

Технологія бездротової передачі, яка описується набором стандартів IEEE 802.11. Відповідно до стандартів, щоб пристрої могли взаємодіяти один з одним, їх інтерфейси повинні підтримувати одну і ту ж версію набору технологій, які дозволяють ділитися даними по радіоканалу.

Пристрої бездротової мережі ідентифікуються за допомогою Media Access Control (MAC) адресам, група пристроїв, яка взаємодіє за протоколами 802.11 називається Basic Service Set. Ці прості визначення можна знайти в будь-якому пристрої, який можна використовувати для роботи з Wi-Fi.

Звідси походить назва BSSID – ідентифікатор, який може бути використаний для доступу до спільної мережі. По суті це просто MAC адресу пристрою, який використовується як основна для об'єднання всіх учасників.

Для мереж Wi-Fi актуальний цілий ряд атак, які можливі через особливості середовища передачі даних. Серед атак найвідоміші це:

- Man-in-the-Middle(MitM).
- DoS.
- підміна адреси відправки/отримання або просто spoofing.

- frame injection.

- прослуховування.

Так як радіоканал ніяк фізично не можна захистити, такі технології як Wi-Fi використовують цілий ряд додаткових перетворень, які повинні допомогти приховати дані від тих, хто намагається зібрати інформацію з повітря. Найчастіше для цього використовується шифрування та набір алгоритмів, які шифрування дозволяють налаштовувати для всіх учасників мережі.

Основна проблема радіоканалу полягає в тому, що його не так просто обмежувати у просторі. Запущена мережа Wi-Fi стає доступна всім пристроям, які вміють працювати з цим каналом зв'язку. Іноді йдуть на хитрощі та намагаються приховати ідентифікатор мережі або BSSID, але це не завжди може допомогти. Особливо якщо атакуючий матиме на руках сканер на базі SDR[24].

## 2.4 Інструменти для моніторингу бездротових мереж

Насправді, щоб виявити мережі, які розташовані навколо, достатньо перевести бездротовий інтерфейс в режим моніторингу. Це аналог "нерозбірливого" режиму роботи мережевої карти, коли ми працюємо зі сніффером мережі. По суті в режимі монітора також можна скористатися такими сніфферами як WireShark.

Для проведення сканування можна використовувати такі Opensource проекти:

1. bettercap.

2. Kismet.

Обидва проекти спеціалізуються як на атаках на популярні радіо канали, так і дають достатньо інструментів для дослідження цих каналів зв'язку.

Обидва інструменти взаємозамінні і можуть використовуватися окремо, але в рамках статті розглянемо, як ними можна користуватися для моніторингу радіо каналу.

Інструмент Kismet досить старий, входив до стандартного набору операційної системи Kali Linux, зараз його можна встановити, якщо використовується так звана "повна" установка. Додаток позиціонується як сніффер, який може працювати як з картами, які встановлені у звичайні комп'ютери, так і з картами SDR, які можуть приймати сирий сигнал на заданих частотах[25].

До речі, Kismet можна поставити на одноплатний комп'ютер і використовувати його для збирання даних про мережі, що знаходяться у зоні доступу.

Установка програми досить проста, можна знайти її для найпопулярніших операційних систем тут. Програма має один недолік - працює вона виключно на BSD і Linux подібних системах, але при бажанні можна запустити його в WSL для Windows. Однак у цьому випадку можуть виникнути проблеми з доступом до пристроїв.

Після встановлення, щоб програма запрацювала потрібно запустити команду: kismet. Після цього буде такий лог, як на рисунку 2.6.

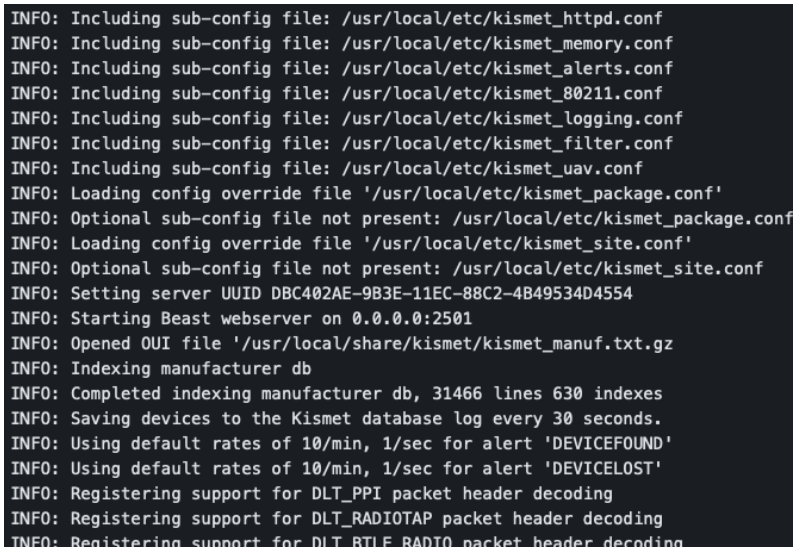


Рисунок 2.6 – Отриманий лог kismet

Після завершення процесу запуску, можна звернутися до активного мережного інтерфейсу пристрою на порту 2501, як показано на рисунку 2.7.

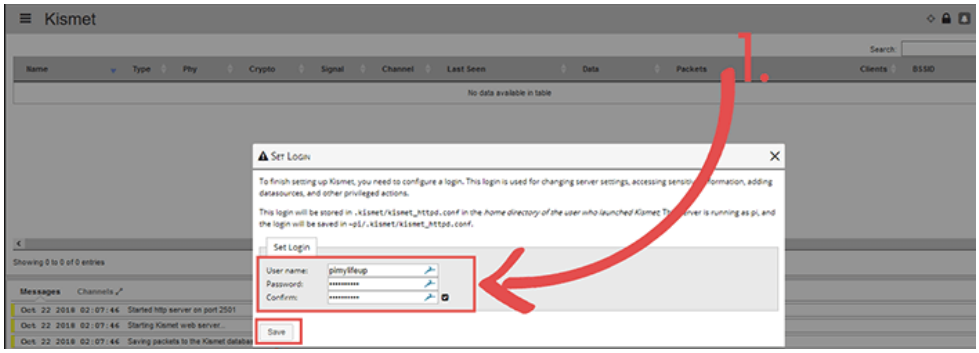


Рисунок 2.7 – Веб інтерфейс kismet

Тепер їх цього інтерфейсу можна запустити моніторинг, який візуалізуватиме всі знайдені дані з радіо каналів навколо.

Щоб вибирати які саме радіоканали моніторитися, потрібно у верхньому правому куті інтерфейсу вибрати контекстне меню і потім включити моніторинг потрібного активного інтерфейсу. У результаті буде аналіз частот, що на рисунку 2.8.

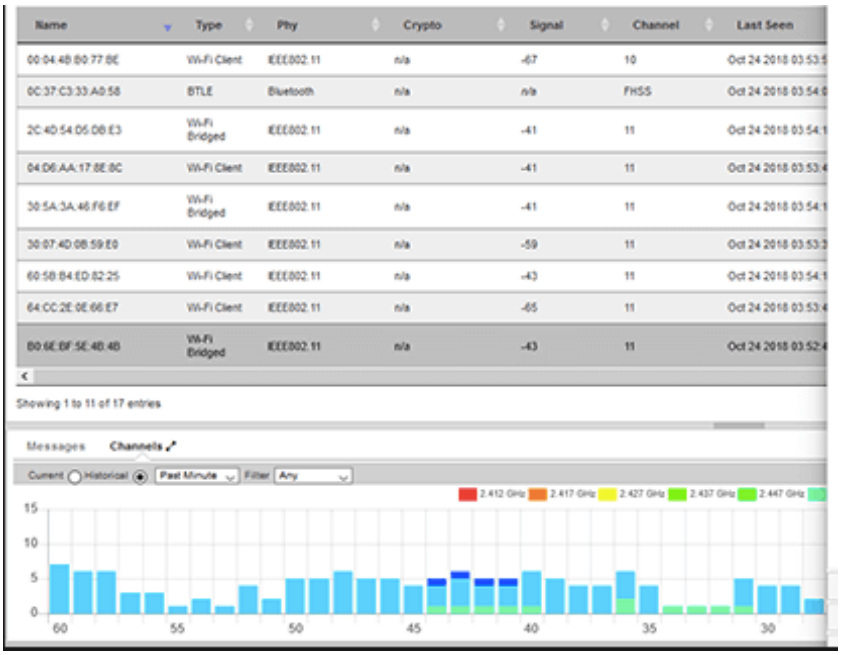


Рисунок 2.8 – Моніторинг Wi-Fi мереж за допомогою kismet

Після такого налаштування не важко знайти сторонні точки доступу і реєструвати аномальну активність в радіо каналі. Це важливо, оскільки більшість атак, які актуальні для Wi-Fi починаються саме з радіоканалу, а потім уже досягають рівня, який дає доступ до даних.

Bettercap - не настільки інтерактивний софт, як kismet, але він і позиціонується як набір інструментів для атаки на бездротові популярні мережі, він включає сніффер, але це тільки одна з його функцій.

Для цього додатка навіть є варіант установки у docker image. Це зручно, але як і з WSL для Windows, доведеться розбиратися з тим, як прокидати пристрої всередину контейнера.

Інструмент можна використовувати в терміналі і це в більшості випадків є кращим способом взаємодії, але також можна використовувати Web UI, для цього потрібно запустити команду в терміналі:

sudo bettercap -eval "caplets.update; ui.update; q"

Команда здійснить оновлення каплета (скрипта для bettercap) і поставить усі необхідні залежності, щоб можна було працювати з Web UI. Після цього потрібно відредагувати дані, що відносяться до логіну та паролю. Всі дані розміщені у файлі bettercap/caplets/http-ui.cap цей файл у будь-якій системі, що підтримується, буде просто знаходитися в директорії установки bettercap. У файлі потрібно прописати логін і пароль і після цього запустити команду:

sudo bettercap -caplet http-ui

Каплет підніме інтерфейс локально і можна потрапити до нього за адресою http://127.0.0.1/, ввівши логін і пароль з минулого кроку. Інтерфейс може виглядати так, як на рисунку 2.9.

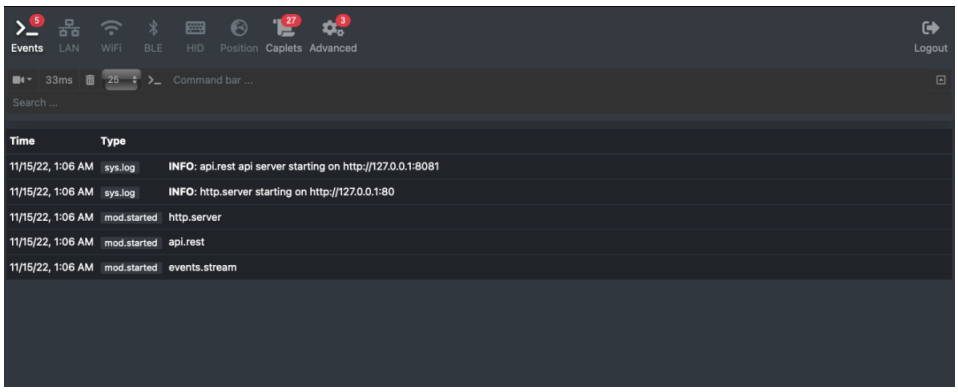


Рисунок 2.9 – Веб інтерфейс Bettercap

Тут інтерфейс простіший, досить просто вибрати цікавий для нас радіо канал і вся інформація буде доступна на екрані. Одна примітка - для сканування потрібно вимкнутись від усіх мереж, які можуть бути активними, потім потрібно вибрати найменування інтерфейсу та запустити збір даних (риунок 2.10).

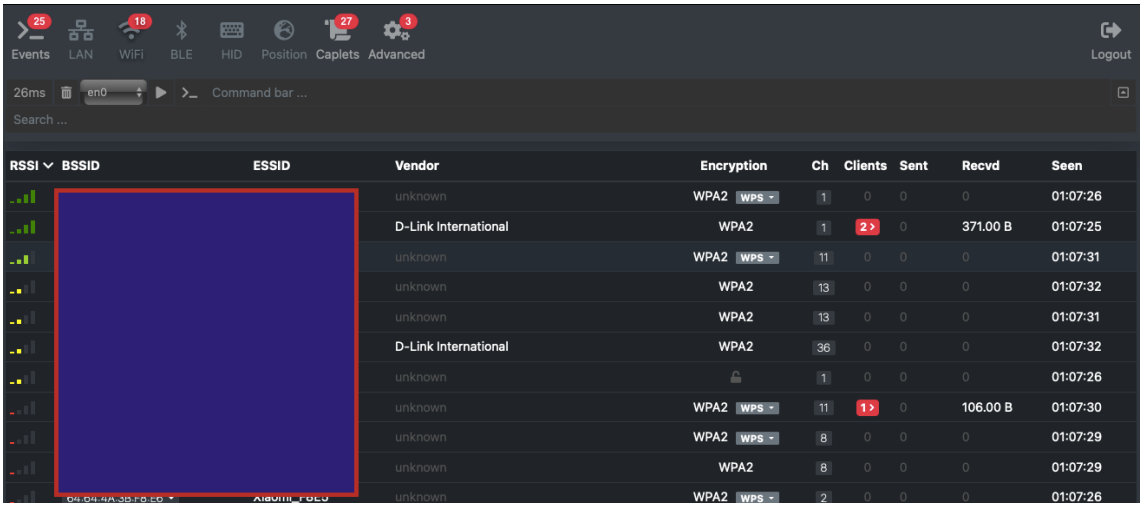


Рисунок 2.10 – Сканування мереж Bettercap

Таким простим способом можна моніторити бездротові мережі та розпочинати дослідження її безпеки.

## 2.5 Атаки на Wi-Fi

Більшість атак, які відомі на бездротових мереж є атаки на механізми автентифікації для доступу до бездротової мережі. Вибираються ці механізми невипадково, оскільки вони перешкоджають безконтрольному підключенню до точки доступу. Весь процес з'єднання з точкою доступу можна схематично зобразити так, як на рисунку 2.11.

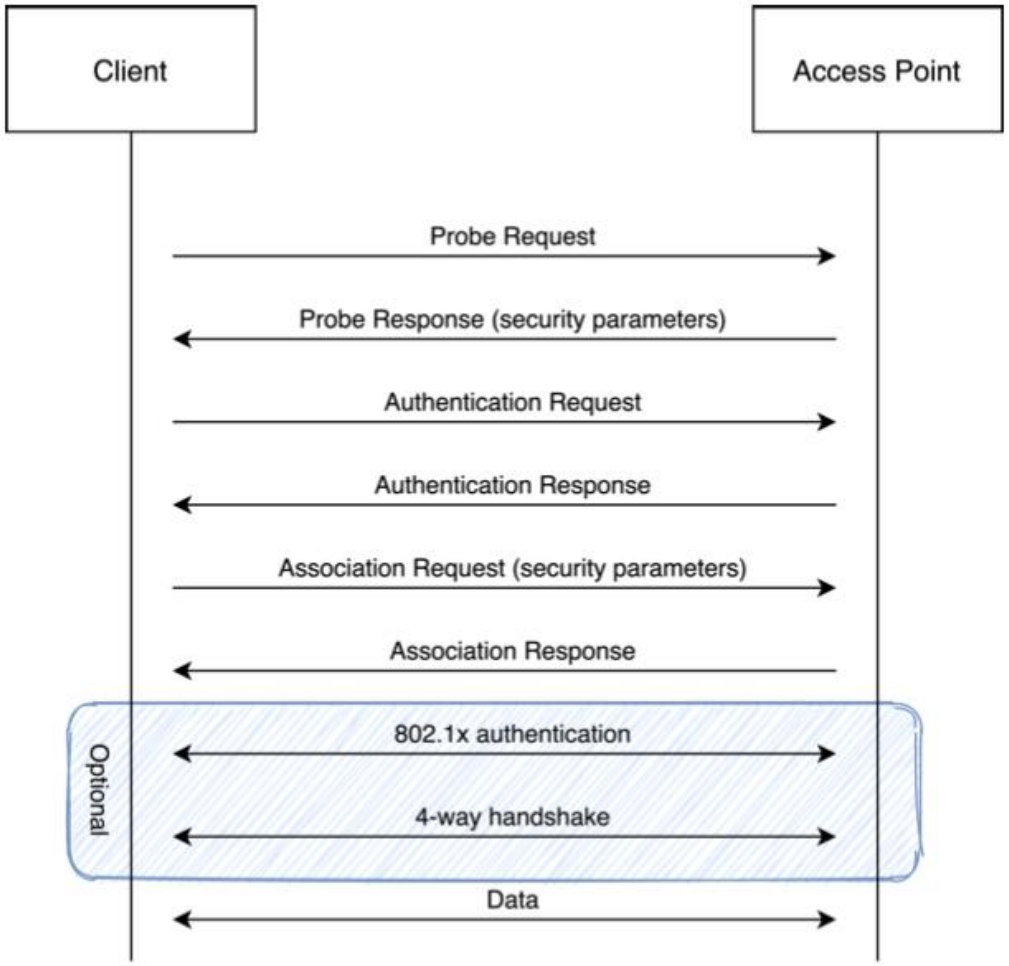


Рисунок 2.11 - Процес з'єднання з точкою доступу

На рисунку позначені саме ті кроки в процедурі коннекта до точки доступу, які відповідають за аутентифікацію. Усі дії, що виконуються в рамках аутентифікації, використовують окремі протоколи, які за допомогою криптографічних алгоритмів дозволяють безпечно надати аутентифікаційні дані користувача для точки доступу.

За час існування Wi-Fi для процедур аутентифікації стали відомі такі протоколи:

- WEP.
- WPA.
- WPA2.
- WPA3.

Всі протоколи відрізняються один від одного набором даних, які потрібні для успішної аутентифікації. Для порівняння можна побудувати таблицю 2.2.

Таблиця 2.2 – Протоколи аутентифікації бездротових мереж

| | **WEP** | **WPA** | **WPA2** | **WPA3** |
|---|---|---|---|---|
| Випущено | 1997 | 2003 | 2004 | 2018 |
| Режими | WEP-OPEN<br>WEP-Shared | WPA-PSK<br>WPA-Enterprise | WPA2-PSK<br>WPA2-Enterprise | WPA3-Personal<br>WPA3-Enterprise |
| Алгоритм шифрування | RC4 | TKIP | AES-CCMP | AES-CCMP<br>AES-GCMP |
| Розмір ключа | 64/128 | 128 | 128 | 128/256 |
| Вважається застарілим | С 2004 | С 2012 | Актуален | Актуален |

Тобто кожен із протоколів використовує свій метод шифрування та валідації даних. По таблиці так само видно, що частина протоколів вважається застарілою і більше не використовується для сучасних пристроїв. Але насправді це не так, пристрої, які вимогливі до живлення, можуть все ще

використовувати старі алгоритми. Отже, атаки можна провести на практиці стосовно кожного протоколу, описаного вище.

Для WEP існують наступні атаки:

- mana attack/evil twin (MiTM).

- FMS Attack (Відновлення ключа).

- Korek Attack (Відновлення ключа).

- PTW Attack (Відновлення ключа).

Усі атаки, окрім MiTM, виконуються на алгоритм шифрування, який використовується протоколом. Нижче наведемо блок-схему з прикладом роботи алгоритму(рисунок 2.12).

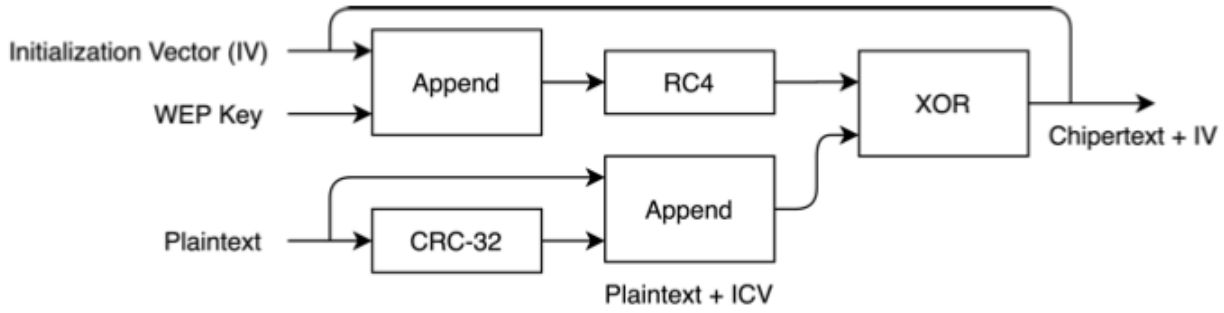


Рисунок 2.12 -Блок-схема роботи алгоритму WEP

Для реалізації атак у мережі є набір інструментів, який досить ефективно може вирішувати завдання відновлення ключа. Єдиною умовою для проведення атаки є необхідність збору даних, що передаються у рамках взаємодії мережі. Тобто потрібно назбирати якомога більше даних з радіоефіру Wi-Fi і просто провести відновлення ключа за даними, які знаходяться у службовій частині інформації, що передається.

Найпопулярнішим інструментом для атак є Aircrack-ng. Усі алгоритми відновлення ключа просто вбудовані у цей набір інструментів.

WPA атаки

Для WPA перелік атак також досить великий:

- Атака за списком паролів (Відновлення ключа).

- перебір WPS.

- EAP-GTC downgrade атака.

Атаки спрямовані або на додатковий механізм аутентифікації, який додано до самого пристрою, або використовується хитрощі у вигляді перехоплення handshake етапу коннекту користувача до точки доступу. На рисунку 2.11 виділені дані, які зберігаються у вигляді дампу.

Інструмент для перебору WPS - Bully, утиліту можна використовувати відразу після завантаження з репозиторію. Брутфорс запускається командою:

bully -b TestBSSID wlan0

Інструмент для перебору за списком Aircrack-ng. Для атаки користувачі повинні пройти процедуру аутентифікації та дані, які були передані в цей момент, збираються за допомогою airmon, а потім в офлайні відбувається брутфорс за заданим списком паролів. Для простоти можна використати rockyou.txt.

EAP-GTC downgrade атаку можна виконувати за допомогою інструменту eaphammer. На сторінці проекту написано, що інструмент працює з WPA2, але його режими також підходять для роботи з WPA-EAP.

WPA2 атаки містять меншу кількість підходів. Оскільки протокол є покращенням вже існуючого протоколу, то частина атак з WPA для нього залишаються справедливими. Цей протокол, на відміну від попередніх, досі актуальний, ним користуються точки доступу за замовчуванням. Криптографія для забезпечення доступу до точки та шифрування даних у мережі досить добре реалізовано в рамках документації, однак імплементація на пристроях містить певні витрати, які використовуються інструментами для отримання даних про ключ доступу та розшифрування трафіку. І так список атак:

- Атака за списком паролів.
- Перебір WPS.
- PMKID Hash атака за списком.
- EAP-GTC downgrade атака.

Результатом кожної з атак є ключ, який дозволяє отримати доступ до Wi-Fi. Інструменти для проведення атак - ті самі, які були перераховані для WPA і додатково Bettercap. Цей інструмент автоматично збиратиме всі дані в дамп і зберігатиме на диск для подальшого брутфорсу. Брут можна здійснювати через пакет aircrack, або через hashcat.

Останній варіант протоколу безпеки WPA3 для Wi-F, хоч і був створений у 2018 році, досі завойовує ринок точок доступу та мережевих карток. Протокол враховує всі недоліки попередніх і теоретично є найзахищенішим. Атак, які б дозволяли відновити ключ шифрування і отримати повний доступ до системи немає. Є тільки варіації атак на відмову в обслуговуванні, в яких може бути здійснений перехід на попередні версії алгоритмів безпеки.

Тобто для пошуку прихованих точок доступу та тесту їх з точки зору безпеки можна використовувати наступний набір інструментів:

- bettercap для проведення mitm атак та атак на відновлення ключа;
- aircrack пакет для проведення відновлення ключа та атак на відмову в обслуговуванні;
- eaphammer для відновлення ключа;
- Bully – для проведення брутфорсу WPS.

# 3 ДОСЛІДЖЕННЯ БЕЗПЕКИ ТЕХНОЛОГІЇ WIMAX

## 3.1 Архітектура WIMAX

WiMAX-802.16 — це новий стандарт, який пропонує широкосмуговий бездротовий доступ із високою пропускною здатністю та швидкістю передачі. Однак, як і всі інші бездротові мережі, WiMAX вразливий до мережевих атак, які порушують радіозв'язок між абонентською станцією (SS), що спілкується, і базовою станцією (BS). З інтеграцією мобільності в стандарті 802.16e-2005 Mobile WiMAX виникають складності у забезпеченні безпечного доступу до цієї мережі. Mobile WiMAX використовує протокол конфіденційності та керування ключами версії 2 (PKMv2), який підтримує надійні механізми взаємної автентифікації, розширений стандарт шифрування (AES) і конфіденційність повідомлень за допомогою коду автентифікації повідомлення на основі хешу (HMAC) або MAC на основі шифру. (CMAC).

На жаль, навіть із розширеними заходами безпеки WiMAX-802.16 Mobile WiMAX все ще вважається вразливим до мережевих атак. Однією з таких загроз є атака MITM, яка спрямована на незашифровані повідомлення керування в початковій точці входу в мережу, будь то фіксований WiMAX (802.16d-2004) або мобільний WiMAX. Зв'язок, у цьому випадку процедура початкового входу в мережу (INE), створює докладні профілі абонентської станції (SS) жертви, включаючи її параметри безпеки та зв'язки з обслуговуючою базовою станцією (BS), імітує законну станцію, а потім змінює повідомлення керування, які наражають мережу на інші деструктивні атаки, такі як атаки відтворення, атаки маскараду та атаки відмови в обслуговуванні (DoS) .

Атака MITM обманює законні станції, які беруть участь у процесі зв'язку, змушуючи їх працювати так, ніби вони все ще спілкуються одна з одною, порушуючи ефективне функціонування мережі [9]. Ключі захисту, такі як ключ авторизації (AK), ключ шифрування трафіку (TEK), ключ

шифрування ключа (KEK) або HMAC (ключ автентифікації повідомлень), які використовуються на підрівні безпеки, забезпечують кращу безпеку для технології WiMAX. Але ризики безпеки, загрози або вразливості все ще доступні для технології WiMAX. Алгоритм протоколу DH є інструментом, який забезпечує взаємну аутентифікацію перед обміном інформацією про керування мережею. При реалізації в мережі WiMAX DH допомагає зберегти SS від шахрайської BS.

Щоб уникнути обмежень традиційних дротових мереж, було докладено багато зусиль для розробки бездротових технологій. Бездротова технологія була розроблена з 19 століття, і в цьому відношенні було зроблено багато розробок. Бездротові мережі базуються на стандарті IEEE 802.11. Стандарт IEEE 802.11 вперше був створений у діапазоні 2,4 ГГц з використанням протоколів, визначених стандартом IEEE 802.11b. На рисунку 3.1 нижче показано мережу WiMAX. SS спілкуються з BS через бездротове з'єднання. Потім базова станція підключається до базової мережі через міжміські канали зв’язку, такі як WiMAX, оптоволоконна мережа або супутник (рисунок 3.1).

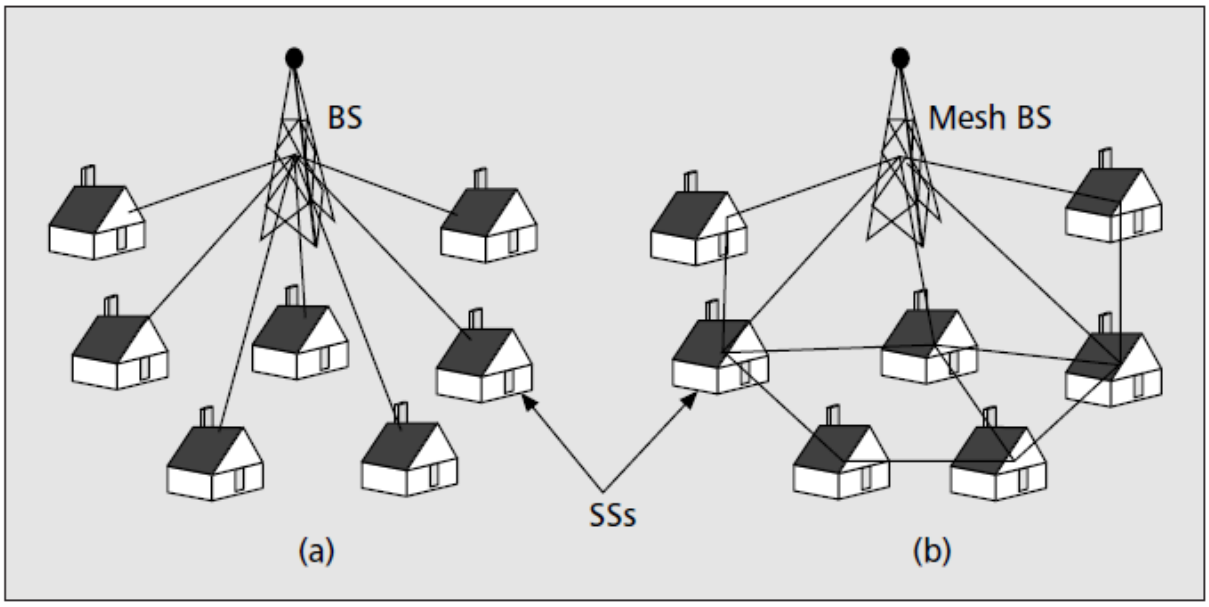


Рисунок 3.1: Мережа WIMAX

Два інші добре відомі стандарти сімейства стандартів IEEE 802.11 — IEEE 802.11a та IEEE 802.11g. Хоча вони забезпечують високошвидкісний стандарт WLAN, зона покриття обмежена. Стандарт IEEE 802.11, комерційно відомий як WiFi, вимагає великої кількості точок доступу WiFi і підключення до дротового вузла. З цієї причини Інститут інженерів з електротехніки та електроніки (IEEE) розробляє новий стандарт для забезпечення великих бездротових мереж.

IEEE 802.16 є стандартом, що забезпечує широкосмуговий доступ як альтернативу кабельному підключенню. WiMAX — торгова назва стандарту IEEE 802.16. Завдяки підтримці мережі Mesh системи WiMAX можна легко налаштувати як бездротові міські мережі (WMAN). Це ще більше покращило можливості WMAN з підтримкою мобільності.

У той час як WiFi і Bluetooth існують уже багато років, WiMAX є молодим стандартом, який розвивається. Для кращого розуміння його принципів подано короткий опис архітектури стандарту. WiMAX означає всесвітню взаємодію для мікрохвильового доступу та є знаком сертифікації сімейства стандартів IEEE 802.16. Він був розроблений для широкосмугового бездротового доступу «точка-багато точок». Його початковою основною метою було не з’єднання кінцевих користувачів із точкою доступу, а з’єднання точок доступу одна з одною. Його можна розглядати як різновид бездротової магістральної мережі, яка є альтернативою кабелю та DSL для забезпечення широкосмугового доступу групам кінцевих користувачів [126]. В останні роки, як відповідь на потреби споживачів і галузі, WiMAX було розширено для підтримки з’єднань між мобільними кінцевими вузлами та базовими станціями. Пристрої WiMAX зазвичай організовані в мережу (рисунок 3.2). Mesh-мережа складається з двох різних типів вузлів, які виконують необхідні завдання маршрутизації: mesh-маршрутизаторів і mesh-користувачів. Той факт, що користувачі сітчастої мережі та маршрутизатори сітчастої мережі можуть виконувати однакові операції і, отже, можуть мінятися ролями, робить сітчасті мережі дуже потужними та гнучкими.

Mesh-мережі зазвичай не обмежуються стандартом IEEE 802.16. Вони призначені для інтеграції інших стандартів, таких як IEEE 802.11 або IEEE 802.15.1, і формують так звані міські та корпоративні мережі. Найважливішими перевагами сітчастих мереж є: масштабованість (рисунок 3.2).

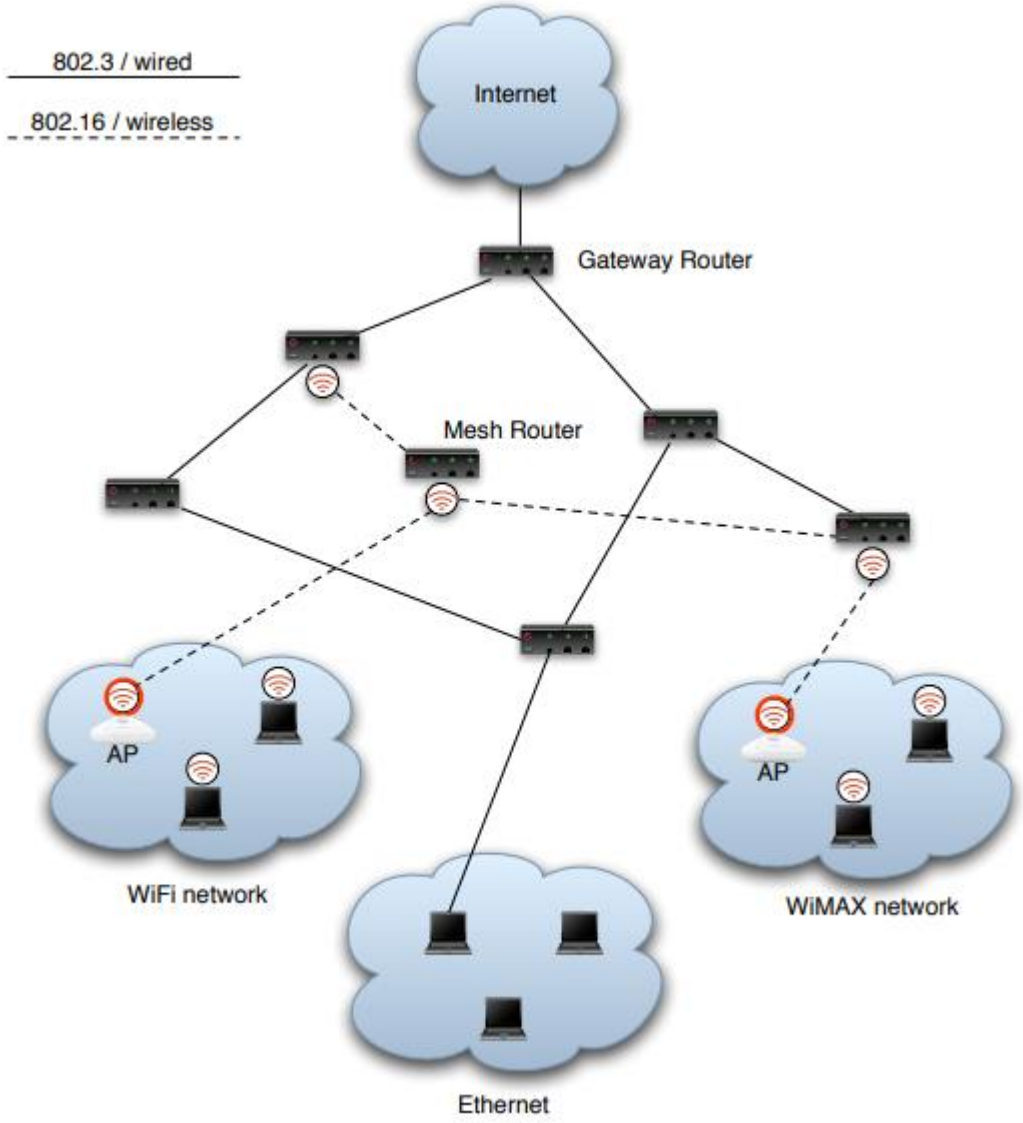


Рисунок 3.2 - Можливе налаштування мережі WiMAX

Вся інфраструктура розроблена таким чином, щоб її можна було масштабувати, оскільки з часом потреба в ресурсах може зрости. Пристрої можуть приєднуватися до мережі та виходити з неї весь час. Маршрутизація може бути самоорганізованою. Підтримується роумінг кінцевих вузлів. Підключення до дротової інфраструктури. Гетерогенні мережі можуть бути

з’єднані між собою за допомогою сітчастих маршрутизаторів. Стандарт IEEE 802.16 використовує діапазон частот від 10 ГГц до 66 ГГц, що вказує на ще одну суттєву відмінність від WiFi, який використовує діапазон 2,4 ГГц. WiMAX здатний охоплювати до 50 км послуг підключення між вузлами без прямої видимості, хоча практично використовувана відстань становить приблизно 5-10 км. Швидкість передачі даних становить до 70 Мбіт/с, що достатньо для одночасного обслуговування близько 60 каналів типу T-1.

Ймовірно, найбільш значні відмінності між стандартами WiMAX і WiFi можна знайти на рівні MAC. WiMAX пропонує значне вдосконалення, оскільки визначає рівень MAC, який підтримує численні специфікації фізичного рівня. Це робить WiMAX чудовою структурою для бездротового широкосмугового зв’язку. Рівень MAC — це так званий рівень MAC планування, на якому пристрої повинні конкурувати за початковий вхід у мережу.

Після приєднання до мережі базова станція виділяє для пристрою часовий інтервал, який може бути змінним, але не повинен використовуватися жодним іншим користувачем. Цей метод пропонує кращу ефективність пропускної здатності та дозволяє базовій станції пропонувати QoS шляхом балансування призначень підключених пристроїв.

Він розроблений для підтримки багатоточкового зв’язку. Він розроблений для багатоточкового зв’язку. Надаються функції самоорганізації. WiMAX спочатку був випущений як IEEE 802.16- 2001 р. у квітні 2002 р. Дослідники почали переглядати дизайн протоколу для існуючої бездротової мережі, ймовірно, IEEE802.11, adhoc та IEEE 802.16 . Усі вони активно працюють над новими додатками для WMAN. EEE 802.16 (2004) забезпечує розширену підтримку NLoS у діапазоні 2–11 ГГц із мережевими з’єднаннями Mesh. Після деяких поправок був випущений IEEE 802.16-2004, також відомий як IEEE 802.16d, який виправив багато помилок і початкових уразливостей безпеки. У 2005 році було випущено стандарт IEEE 802.16e-2005, який уможливив підтримку мобільності в мережах WiMAX і вирішив

додаткові проблеми безпеки. IEEE 802.16j є останньою основною версією цього сімейства стандартів. Це в основному розширює підтримку мобільних пристроїв і не вводить нові функції безпеки.

Рисунок 3.3 ілюструє діаграму архітектури WiMAX. Архітектура протоколу WiMAX складається з двох основних рівнів (рисунок 3.3): - рівень MAC і рівень PHY.

Рівень MAC містить 3 підрівні. Починаючи з базового рівня, перший підрівень — це SS, який шифрує та розшифровує дані, які надходять і виходять із рівня PHY. Цей підрівень використовує для трафіку даних 56-бітне шифрування DES (стандарт шифрування даних), а для обміну ключами використовує шифрування 3DES.

Другий підрівень MAC — це підрівень конвергенції, специфічний для служби (SSCS). Цей підрівень відображає послуги даних вищого рівня на потік послуг і з'єднань рівня MAC.

Третій підрівень — підрівень загальної частини (CPS). На цьому підрівні створено MPDU (блоки даних протоколу MAC). Підрівень CPS визначає правила та механізми для ARQ (запит на автоматичне повторення 10), для контролю з'єднання та для розподілу смуги пропускання доступу до системи.

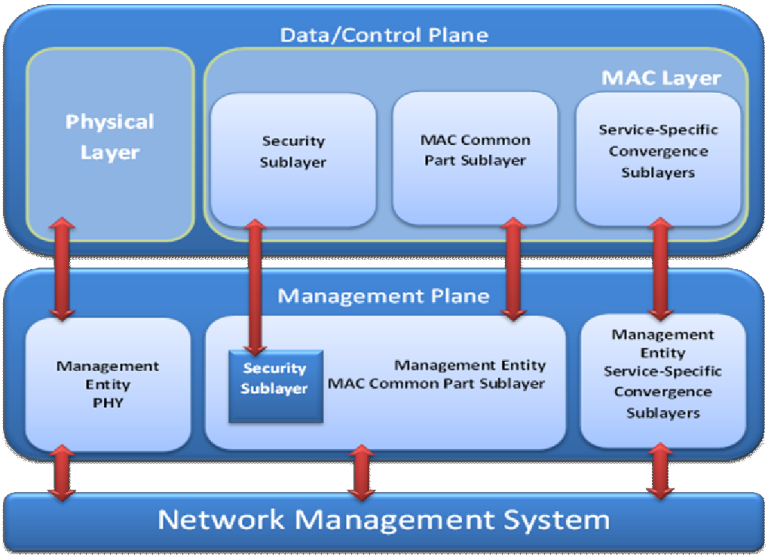


Рисунок 3.3 - Архітектура WiMAX

Він також забезпечує централізацію, доступ до каналів і дуплекс. CS і CAP передаються через MAC SAP (Service Access Point). Рівень PHY — це зв’язок між MPDU та кадрами рівня PHY із кодуванням радіочастотних сигналів під час надсилання та отримання через модуляцію. Архітектура технології WiMAX (рисунок 3.3) була створена таким чином, щоб дозволити її підключення до IP-мереж, які надають послуги Інтернет.

Системи WiMAX були розроблені від початку з урахуванням надійної безпеки. Стандарт включає найсучасніші методи забезпечення конфіденційності даних користувача та запобігання несанкціонованому доступу з додатковою оптимізацією протоколу для мобільності.

Безпека обробляється підрівнем конфіденційності WiMAX MAC. Дані користувача шифруються з використанням криптографічних схем з перевіреною надійністю для забезпечення конфіденційності. Підтримуються як AES (розширений стандарт шифрування), і 3DES (стандарт потрійного шифрування даних). 128-бітний або 256-бітний ключ, який використовується для отримання шифру, генерується на етапі автентифікації і періодично оновлюється для додаткового захисту.

WiMAX надає гнучкі засоби для автентифікації абонентських станцій та користувачів для запобігання несанкціонованому використанню. Структура автентифікації заснована на EAP Internet Engineering Task Force (IETF), яка підтримує різні облікові дані, такі як ім'я користувача/пароль, цифрові сертифікати та смарт-картки.

Термінальні пристрої WiMAX поставляються з вбудованими цифровими сертифікатами X.509, які містять їхній відкритий ключ і MAC-адресу. Оператори WiMAX можуть використовувати сертифікати для автентифікації пристрою та використовувати ім'я користувача / пароль або автентифікацію смарт-карти поверх нього для автентифікації користувача.

WiMAX надає такі послуги безпеки безпосередньо:

- Конфіденційність — захист від підслуховування.

- Цілісність даних — захист даних від підробки під час передачі

- Автентифікація — на рівні користувача та пристрою.

- Авторизація — на рівні сервісу.

Як показано на рисунку 3.4, IEEE 802.16 дозволяє вбудовувати функції безпеки на різних рівнях мережі. З самого початку процесу проектування WiMAX було введено спеціальний рівень як частину рівня MAC. Так званий підрівень безпеки повинен забезпечувати всі необхідні функції безпеки, захищаючи весь зв'язок на вищих рівнях (рисунок 3.5).

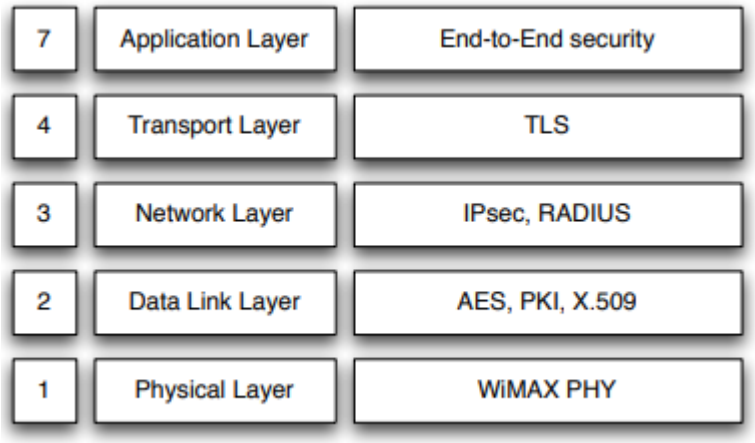


Рисунок 3.4: Підтримувані WiMAX функції безпеки на різних мережевих рівнях

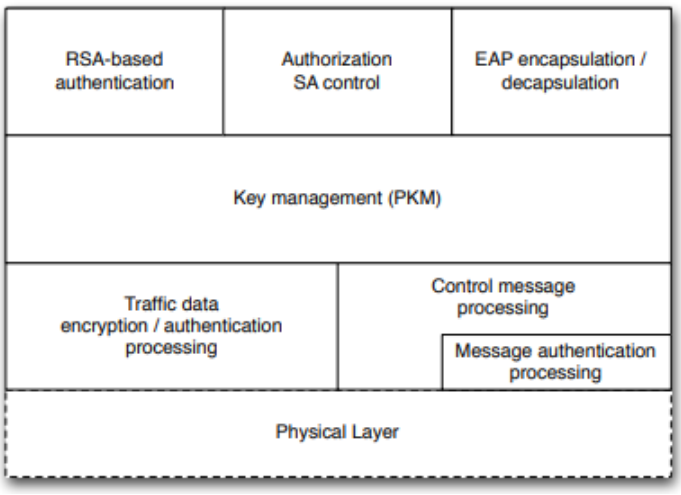


Рисунок 3.5 - Підрівень безпеки WiMAX

Автентифікація та авторизація в WiMAX Автентифікація та авторизація в WiMAX повністю реалізовані на підрівні безпеки. Це

досягається за допомогою так званого протоколу обміну відкритими ключами, який забезпечує автентифікацію та встановлення криптографічних ключів. Обмін ключами та керування ключами загалом мали кілька вразливостей у вихідному стандарті IEEE 802.16. Оскільки стандарт IEEE 802.16e-2005 вирішив більшість цих проблем, буде зосереджено увагу на сучасному стандарті. IEEE 802.16e-2005 визначає два протоколи керування секретними ключами (PKM), PKMv1 і розширену версію PKMv2. В основному вони дозволяють три типи автентифікації:

-Автентифікація на основі RSA — на основі сертифікатів X.509.

- SA control.

- Розширюваний протокол автентифікації (EAP).

Розглянемо аутентифікацію на основі RSA з подальшою автентифікацією EAP. Уся інформація безпеки між сторонами, що спілкуються, є частиною так званих асоціацій безпеки (SA). SA — це набір параметрів, які використовуються для автентифікації, авторизації та шифрування. Спільна інформація залежить від вибраного криптографічного набору та зазвичай включає ключі шифрування та вектори ініціалізації (IV), необхідні для процесу шифрування. IEEE 802.16e-2005 визначає три різні типи SA:

- Первинна SA Кожна абонентська станція (SS) встановлює первинну SA під час процесу ініціалізації.

- Статичний SA Вони надаються в межах кожної базової станції (BS).

- Динамічний SA Вони встановлюються та усуваються на льоту у відповідь на ініціювання та завершення певних потоків послуг. Кожна SS встановлює ексклюзивну первинну SA зі своєю BS і динамічними SA для кожного нового потоку послуг. Термін служби SA обмежений стандартом. Кожна нова SA повинна отримати новий дозвіл перед її створенням.

Таблиця 3.1 - Огляд криптографічних ключів, що використовуються в WiMAX

| Key Name | Description | Derived from |
|---|---|---|
| AK<br>Authorization Key | Shared private key<br>(between SS and BS) | not clearly defined by<br>the standard |
| KEK<br>Key Encryption Key | Key used for encrypting<br>TEKs in the key exchange | derived from the AK |
| TEK<br>Traffic Encryption Key | Used for encrypting all<br>end to end traffic | derived from the AK |
| PK<br>Public Key | public key of the<br>BS and the SS respectively | stored in the X.509 certificate<br>of the BS and SS respectively |

Протокол конфіденційності та керування ключами версії 2 (PKMv2) використовується для безпечної передачі ключового матеріалу з базової станції на мобільну станцію, періодичної повторної авторизації та оновлення ключів. Цілісність бездротових керуючих повідомлень захищена за допомогою схем дайджесту повідомлень, таких як CMAC на основі AES або HMAC на основі MD5.

Для підтримки швидкої передачі обслуговування WiMAX дозволяє MS використовувати попередню аутентифікацію з конкретною BS для прискорення повторного входу. Схема тристороннього рукостискання підтримується для оптимізації механізмів повторної аутентифікації підтримки швидкої передачі обслуговування, одночасно запобігаючи будь-які атаки типу «людина посередині».

## 3.2 Протокол автентифікації Pkmv1.

PKM встановлює загальний ключ під назвою «Ключ авторизації» (AK) між абонентом (SS) і базовою станцією (BS). Після того, як цей спільний AK встановлено між сторонами, з нього виходить ключ шифрування ключа (KEK). Потім цей KEK використовується для шифрування наступних обмінів PKM ключами шифрування трафіку (TEK). Усе шифрування корисного навантаження базується на TEK. Таблиця 3.1 надає витяг криптографічних ключів, які використовуються в WiMAX. Рисунок 3.6 ілюструє протокол

автентифікації та авторизації, який спочатку був інтегрований у IEEE 802.16-2001. SS використовує перше повідомлення для надсилання сертифіката виробника X.509 до BS, що дозволяє йому перевіряти свою ідентичність за допомогою центру сертифікації (CA) (рисунок 3.6).

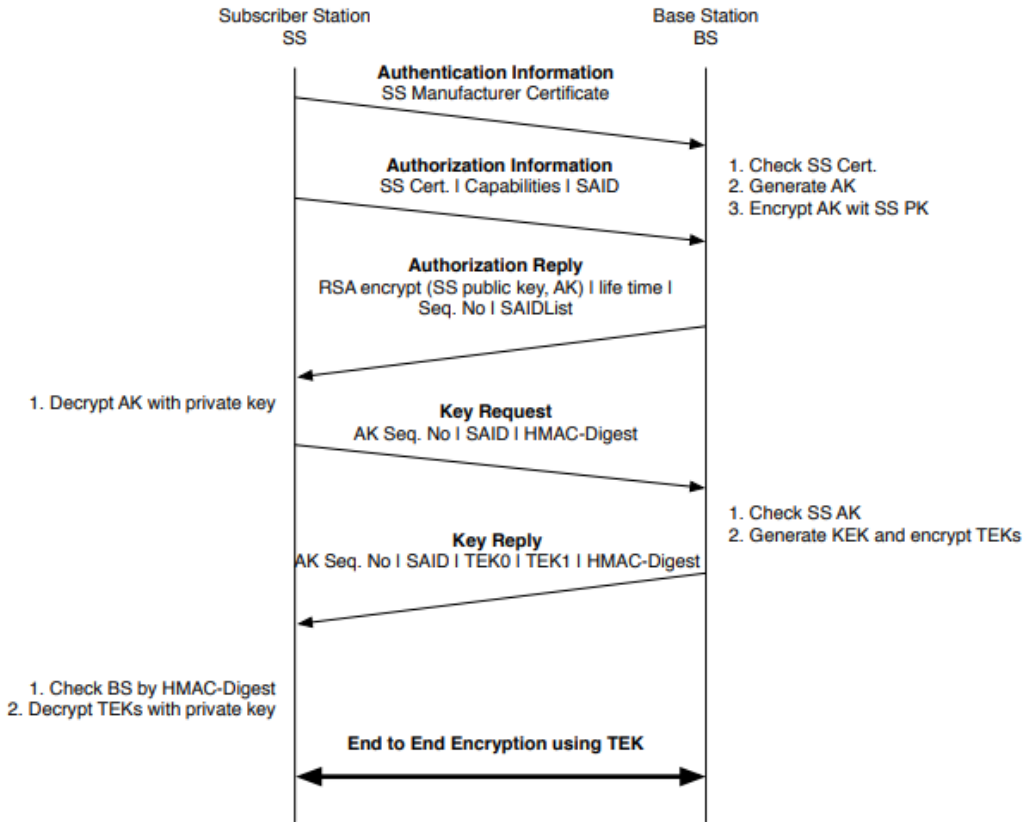


Рисунок 3.6 - WiMAX Privacy Key Management Protocol (PKM) v1

Друге повідомлення надсилається одразу після першого та містить сертифікат X.509 SS, його можливості безпеки та ідентифікатор первинної асоціації безпеки (SAID). Використовуючи відкритий ключ (PK) сертифікатів SS, BS може сконструювати відповідь авторизації, включаючи ключ авторизації (AK). Наступні повідомлення призначені для встановлення ключів, необхідних для шифрування. PKMv1 не має взаємної автентифікації, оскільки лише SS надає сертифікат.

SS використовує інформаційне повідомлення автентифікації, щоб передати BS свій сертифікат X.509, який ідентифікує його виробника. BS використовує цей сертифікат, щоб визначити, чи є SS надійним пристроєм.

BS може використовувати це повідомлення, щоб дозволити доступ лише до пристроїв визнаних виробників відповідно до своєї політики безпеки. SS надсилає повідомлення 2, назване запитом на авторизацію, відразу після повідомлення 1 (рисунок 3.7). Повідомлення 2 складається з сертифіката SS X.509 із відкритим ключем SS, його можливостей безпеки, які насправді є алгоритмами автентифікації та шифрування, які підтримують SS, і ідентифікатора асоціації безпеки (SAID), який є ідентифікатором безпечного з'єднання між SS і BS.

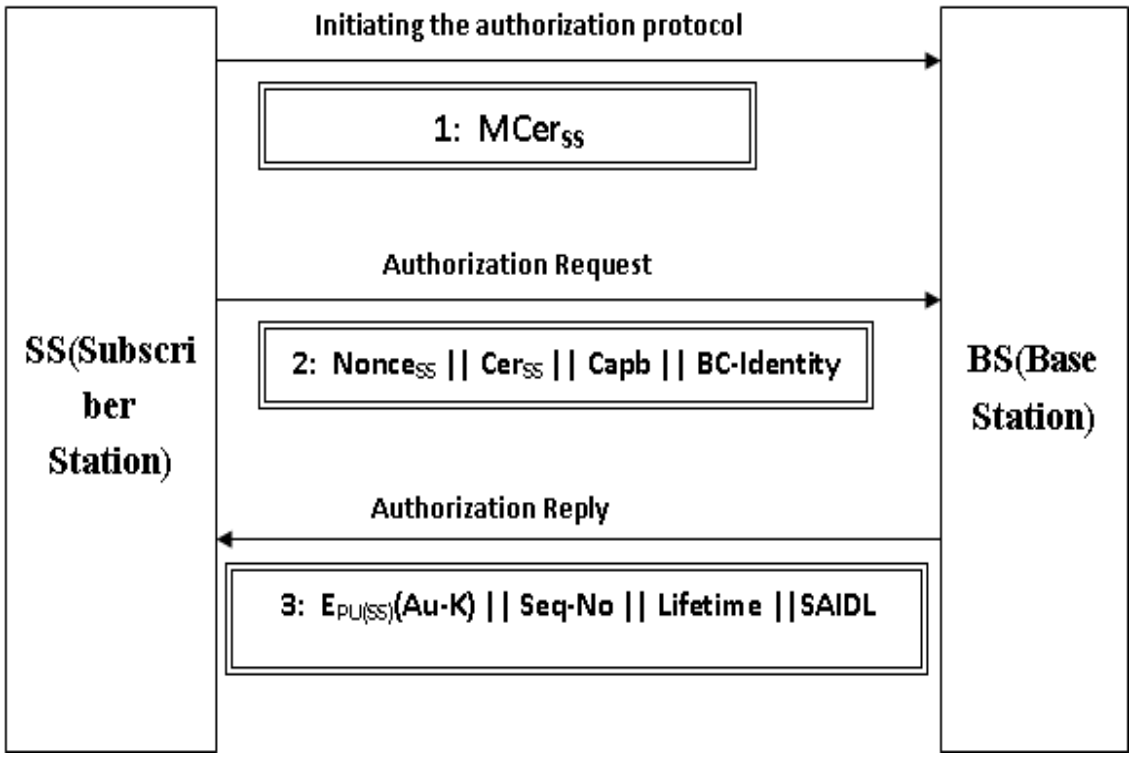


Рисунок 3.7 - Діаграма PKM v1

де на рисунку 3.7:

$MCer_{ss}$ - сертифікат виробника SS.

$Nonce_{ss}$ - номер, обраний SS для ідентифікації.

$Cer_{ss}$ - Сертифікат, що належить SS.

Capb Можливості безпеки SS.

BC-Identity Security можливості SS.

$E_{pu(ss)(}$Au-K) - Ключові функції автентифікації.

$Seq_{-NO}$ - Порядковий номер.

Lifetime - ресурс АК.

SAIDL - Ідентифікатор асоціації безпеки .

Використовуючи сертифікат, BS визначає, чи авторизувати SS; і відкритий ключ SS, який також міститься в сертифікаті, дозволяє BS створити повідомлення 3 . У разі успіху, а саме SS авторизовано після того, як BS перевірить свій сертифікат, BS відповідає повідомленням 3, відповіддю авторизації. Це повідомлення містить АК, зашифрований за допомогою Rivest, Shamir і Adelman (RSA) протокол шифрування з відкритим ключем, який використовує відкритий ключ SS, отриманий у попередньому повідомленні, час життя АК як беззнакове число в секундах, порядковий номер для АК як 4-бітне значення та список дескрипторів SA, кожен з яких включає SAID і шифр SA.

## 3.3 Протокол автентифікації Pkmv2

IEEE 802.16e-2005 представив покращену версію протоколу керування конфіденційними ключами під назвою PKMv2, спрямовану на забезпечення взаємної автентифікації на основі сертифікатів X.509 і виправлення вразливостей PKMv1. Як показано на рисунку 3.7, відповідь авторизації розширюється сертифікатом BS, цифровим підписом і випадковими початковими числами від SS і BS відповідно. Ці додаткові параметри мають на меті захистити протокол від повторних атак і атак man in-the-middle. PKMv2 також дозволяє використовувати коди автентифікації повідомлень на основі шифру (CMAC) замість хешованих кодів автентифікації повідомлень (HMAC). На додаток до автентифікації на основі RSA WiMAX дозволяє використовувати розширюваний протокол автентифікації (EAP). Метод EAP може використовувати певний тип облікових даних, наприклад сертифікат X.509 у випадку EAP-TLS (рисунок 3.8) або модуль ідентифікації абонента (SIM-карта) у випадку EAP-SIM.

.

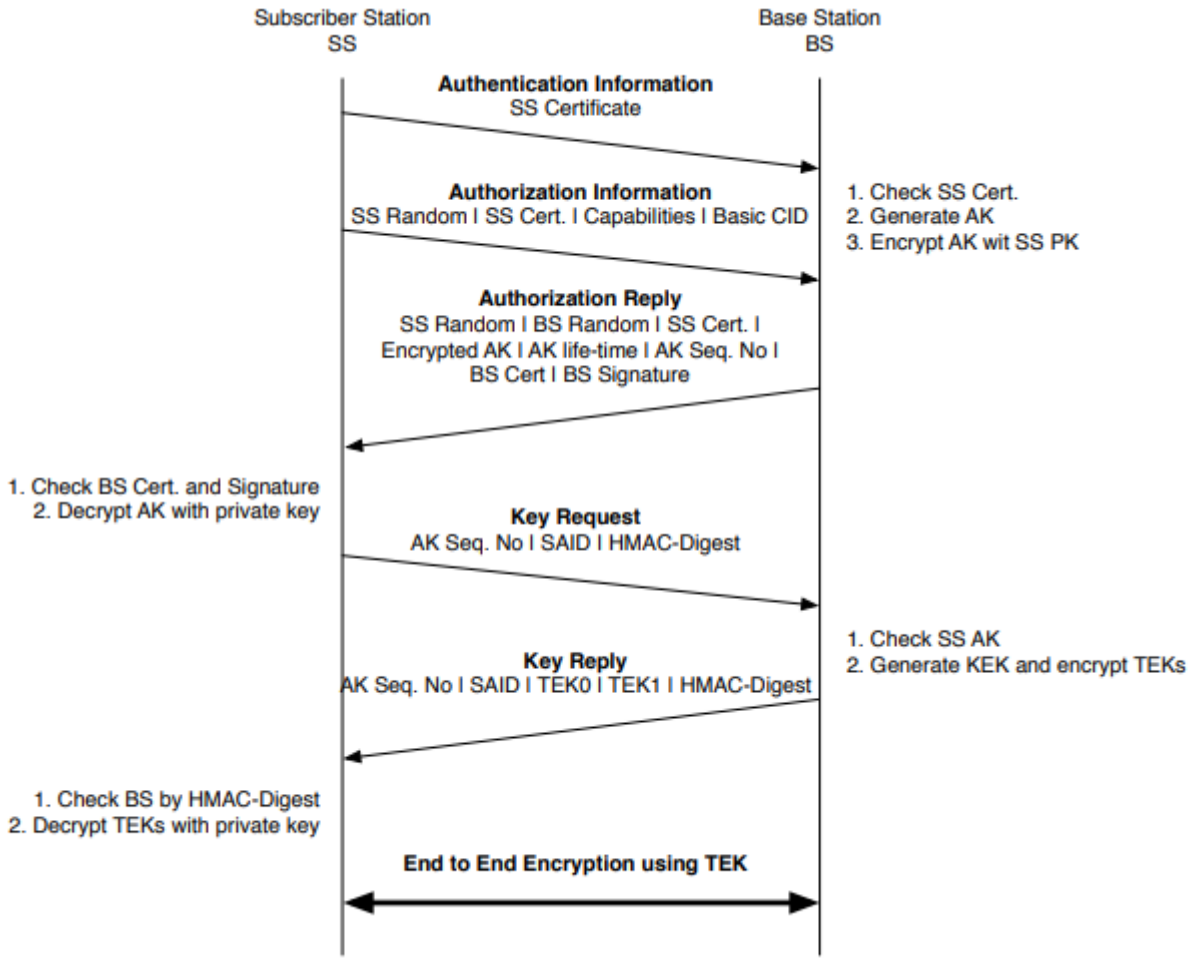


Рисунок 3.8 - WiMAX Privacy Key Management Protocol (PKM) v2

Визначення протоколу EAP знаходиться за межами стандарту WiMAX і може бути отримано з RFC 4017.

SS перевіряє подібність шляхом порівняння надісланих N з отриманими N у повідомленні відповіді авторизації. Потім він витягує PAK, оскільки тільки авторизований SS може витягти PAK.

Це можна використовувати як доказ авторизації. Нарешті, останнє повідомлення цієї автентифікації надсилається SS для підтвердження автентифікації BS. SS включає випадкове число BS Nb, отримане в повідомленні відповіді авторизації, яке використовується для підтвердження подібності, MAC-адресу SS і криптографічну контрольну суму повідомлення (рисунок 3.9).

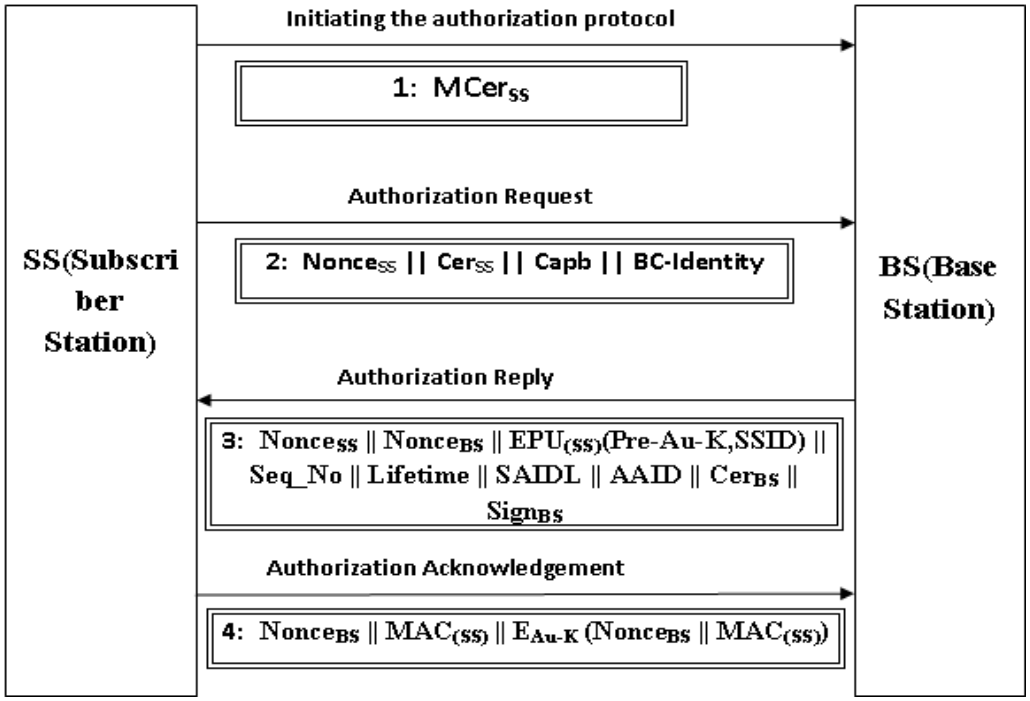


Рисунок 3.9 - Діаграма PKMV 2

$MCer_{ss}$ - Сертифікат виробника SS.

$Nonce_{ss}$ - Номер, обраний SS для ідентифікації.

$Nonce_{BS}$ - Номер, обраний BS для ідентифікації.

$Cer_{ss}$ - Сертифікат, що належить SS.

$Cer_{BS}$ - Сертифікат, що належить BS.

Capb - Можливості безпеки SS.

BC-Identity Security можливості SS.

$E_{pu(ss)}$(Au-K) - Ключові функції автентифікації.

$Seq_{-NO}$ - Порядковий номер.

Lifetime - Ресурс АК.

SAID - Security Association Identity.

MAC $_{(ss)}$ - MAC-адреса SS.

Початковий стандарт визначав шифрування на основі стандарту шифрування даних (DES) із довжиною ключа за замовчуванням 56 біт.

Рисунок 3.10 ілюструє процес шифрування IEEE 802.16-2001. DES працює в режимі з'єднання шифрованих блоків (CBC) з використанням TEK як ключа шифрування, вектора ініціалізації, отриманого з IV SA та значення поля в заголовку PHY. Обидва ці останні названі значення передбачувані. IEEE 802.16e-2005 представив використання розширеного стандарту шифрування (AES) у режимі лічильника з режимом CBC-Message Authentication Code (CCM) для автентифікації та AES у режимі лічильника (CTR) для цілей шифрування (рисунок 3.10). AES-CCM і AES-CTR працюють швидше, ніж 3DES, і рівень безпеки є значним.

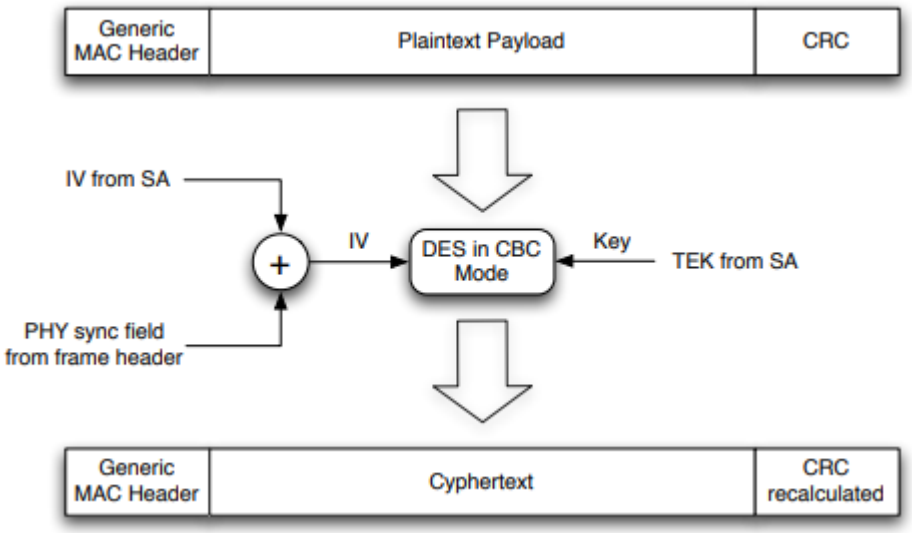


Рисунок 3.10 – Схема шифрування DES, що використовується в стандарті

Останній стандарт IEEE 802.16e-2005 містить нову версію (PKMv2) протоколу, яка усуває недоліки першої версії. PKMv1 не має можливості для взаємної автентифікації. Крім того, PKMv2 підтримує два різні механізми автентифікації: SS і BS можуть використовувати автентифікацію на основі RSA або розширюваного протоколу автентифікації (EAP) [21]. Це тому, що автентифікація на основі RSA застосовує цифрові сертифікати X.509 разом із шифруванням RSA. Тому автентифікація стає більш безпечною. Потік обміну повідомленнями в аутентифікації на основі RSA показано наступним чином:

SS ініціює процес взаємної аутентифікації на основі RSA, надсилаючи два повідомлення. Перше повідомлення містить сертифікат виробника X.509.

Друге повідомлення із запитом авторизації містить сертифікат SS X.509, 64-бітне випадкове число SS Ns, список можливостей безпеки, які підтримує SS, SAID і підпис SS. Якщо SS автентифікована та авторизована для приєднання до мережі, BS надсилає повідомлення авторизації у відповідь. У повідомленні відповіді BS містить отримане 64-бітне випадкове число SS Ns, своє власне 64-бітне випадкове число Nb, 256-бітний ключ попередньої первинної авторизації (pre-PAK) [3], зашифрований відкритим ключем SS, Час життя ключа prePAK і його порядковий номер, список SAID (один або більше), сертифікат BS'sX.509 і підпис BS у відповіді авторизації.

## 3.4 Проблеми безпеки протоколів PKMv1 ТА PKMv2

WiMAX спочатку був розроблений для вирішення проблеми «останньої милі». Робоча група IEEE 802.16 намагалася уникнути помилок у проектуванні, як це було зроблено, визначивши стандарти WiFi, включивши вже існуючий стандарт, Специфікації інтерфейсу служби передачі даних через кабель (DOCSIS). DOCSIS розроблено для вирішення проблеми «останньої милі» для дротових з’єднань. Цей факт дозволяє припустити, що він може не працювати без проблем у бездротових мережах. Результатом стало те, що IEEE 802.16-2001 не зміг належним чином захистити бездротові канали. Основними недоліками безпеки початкового стандарту є наступні:

- Зашифровано лише транспортування даних, залишаючи кадри керування вразливими для атак.

- Зосередження уваги на шифруванні корисного навантаження пакетів залишило протокол авторизації знехтуваним і, отже, вразливим.

- Стандарт дозволяв односторонню автентифікацію, залишаючи багато лазівок для атак із повторенням.

- Декільком частинам стандарту, пов’язаним із безпекою, таким як генерація ключів, бракувало чітких визначень, і тому вони могли бути реалізовані недосконалими постачальниками обладнання.

- Потрійний DES використовувався в режимі CBC. Хоча сам DES більше не є незламним, дуже короткі ключі, які використовуються в IEEE 802.16-2001, є серйозною вразливістю. Крім того, процес шифрування (риунок 3.11) демонструє серйозну помилку через використання передбачуваних векторів ініціалізації (IV). Режим CBC потребує випадкового IV для захисту схеми.

- Уразливості, створені слабкою схемою шифрування та відсутністю взаємної автентифікації, дозволяють кілька атак на конфіденційність і цілісність.

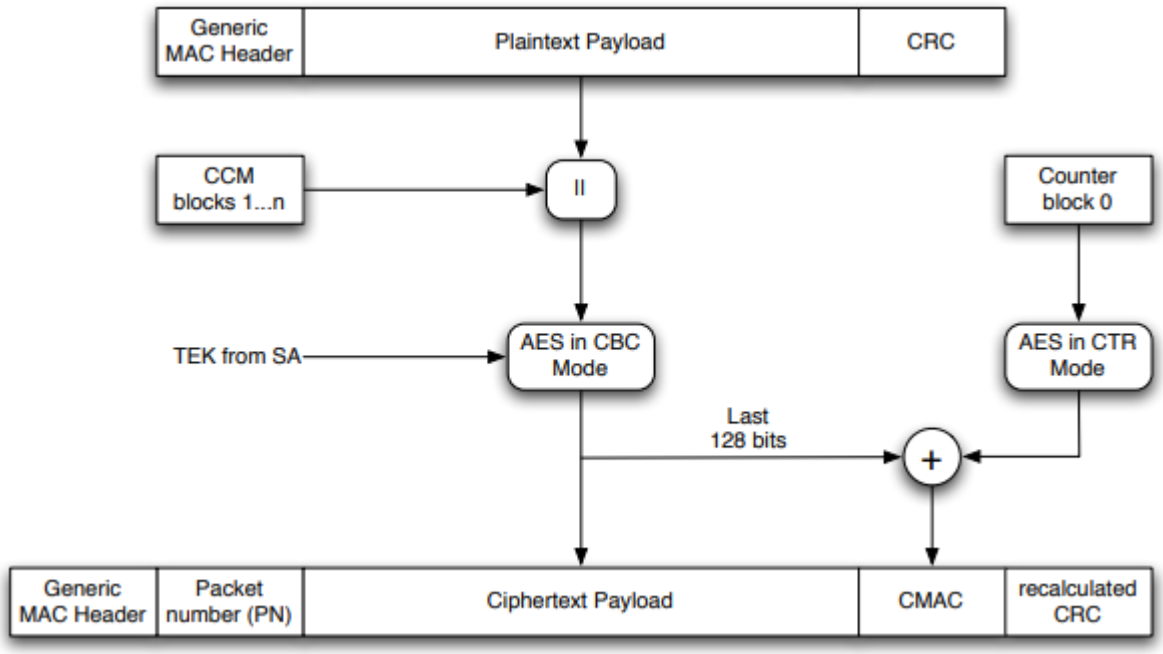


Рисунок 3.11 - Процес шифрування IEEE 802.16e-2005 на основі AES

Крім того, це залишає топологію мережі підданою атакам на сітчасту мережу. IEEE 802.16e-2005 виправляє ці помилки, описані вище, за допомогою таких механізмів:

- Шифрування кадрів керування.

- Покращення протоколу автентифікації шляхом впровадження PKMv2.

- Реалізація взаємної автентифікації на основі PKI.

- Більш точне відтворення визначень генерації ключів.

- Заміна DES-CBC на AES-CBC.

Представлення AES-CCM для автентифікації повідомлень. Як згадувалося раніше, IEEE 802.16e-2005 все ще є молодим стандартом, і зараз навколо нього проводиться багато досліджень, пов’язаних із безпекою. Як показала історія пов’язаних бездротових мереж, це дослідження виявить додаткові вразливості та недоліки конструкції.

Незважаючи на те, що цей захист був інтегрований у початковий дизайн WiMAX, кілька серйозних уразливостей було виявлено незабаром після випуску першої версії. Ці недоліки були виправлені в наступних стандартах. Фактична версія, IEEE 802.16e-2005 все ще є молодим стандартом, і зараз навколо нього проводиться багато досліджень, пов’язаних із безпекою. Як показала історія пов’язаних бездротових мереж, це дослідження виявить додаткові вразливості та недоліки конструкції.

PKMv1 ТА PKMv2 мають недолік безпеки. Взаємна автентифікація відбувається в PKMv2 лише після передачі керуючої інформації. Тут стане в нагоді алгоритм DH. DH спочатку проводить автентифікацію перед передачею обміну управлінською інформацією. Обмін ключами Діффі-Хеллмана (DH) — це криптографічний протокол, який дозволяє двом сторонам, які не мають попередньої інформації одна про одну, разом установити спільний секретний ключ через незахищений канал зв’язку. Потім вони використовують цей ключ для шифрування наступних комунікацій за допомогою шифру з симетричним ключем. Схема була вперше публічно опублікована Вітфілдом Діффі та Мартіном.

Обмін Діффі-Хеллмана сам по собі не забезпечує автентифікацію сторін, що спілкуються, і, отже, чутливий до атаки "людина посередині". Щоб запобігти такому типу атак, як правило, необхідний метод взаємної автентифікації сторін, що спілкуються між собою. Як показано на малюнку

3.9, SS надсилає повідомлення запиту до BS, яке містить сертифікат. Потім BS відповідає на виклик. Зв'язок дозволений лише тоді, коли між SS і BS отримано спільну відповідь. Номер nonce — це криптографічний номер, який використовується лише один раз для автентифікації. Будучи шифруванням RSA, P може шифрувати nonce, а користувач A може дешифрувати, щоб отримати nonce.

Протокол обміну ключами Діффі-Хеллмана спочатку підтримує неавтентифіковані ключові угоди між станціями, які бажають спілкуватися. Станціям не потрібно знати ідентифікаційні дані одна одної, щоб створити спільний секретний ключ шляхом обміну своїми повідомленнями відкритого ключа у відкритому каналі. Це становить загрозу, оскільки шкідлива станція може обмінюватися власним відкритим ключем із законною базовою станцією (BS) або може обмінюватися ним із законною мобільною станцією (MS), щоб згенерувати спільний ключ, який використовується для цілей шифрування. Це ставить під загрозу безпеку всієї мережі WiMAX, тому автентифікація об’єкта перед впровадженням протоколу обміну ключами Діффі-Хеллмана є життєво необхідною. Основна версія протоколу Діффі-Хеллмана реалізована, як описано нижче:

Припустимо:

$$PkMS = GN\mathbf{b} \bmod \mathrm{P} \qquad 3.1$$

$$PkBS = GN\mathbf{a} \bmod \mathrm{P} \qquad 3.2$$

де:

- PkMS є відкритим ключем мобільної станції.
- PkBS є відкритим ключем базової станції.
- G і P — це глобальні змінні, які називаються простими числами.
- G — первісний корінь P.
- «Na» і «Nb» є особистими ключами MS і BS відповідно.

У базовій версії DH після відповідного обміну відкритими ключами MS і BS обчислюють спільний ключ шифрування, як показано в рівняннях 3.7 і 3.9. Щоб реалізувати взаємну автентифікацію, AS надсилає Na до BS, BS обчислює AKB. Потім BS надсилає інший унікальний номер Nb до SS. Подібним чином SS розраховує AKS. Якщо AKS дорівнює AKB, AS вважає це повідомлення, надіслане BS. AK як у SS, так і в BS розраховується таким чином:

$$AK = GN\mathbf{b} \bmod P = GNa \bmod P \qquad 3.3$$

Наведене вище рівняння 3.3 ілюструє реалізацію протоколу DH. Перший етап реалізації модифікованого протоколу Діффі-Хеллмана для стримування атаки MITM передбачає аутентифікацію сутності принципалів, які бажають спілкуватися через мережу WiMAX . Мобільна станція (MS), яка стверджує, що є законною, отримує виклик (Nb) від обслуговуючої базової станції (BS). Він обчислює рішення виклику, використовуючи свою криптографічну функцію, а потім надсилає результат і його ідентичність до BS. BS підтверджує рішення MS і надсилає маркер прийняття як доказ автентифікації. Після отримання MS надсилає виклик (Na) до BS, яка обчислює відповідне рішення на основі криптографічної функції MS і надсилає його до MS.

MS, у свою чергу, перевіряє рішення та надсилає назад маркер прийняття до BS як доказ успішної автентифікації. Нарешті досягається успішна взаємна автентифікація сутності. У цій моделі передбачається, що тільки законна BS і законна MS мають знання про криптографічну функцію, яка використовується для обчислення виклику, надісланого під час виконання протоколу. Таким чином, зловмисник у мережі не в змозі вивести правильне значення даного виклику і, таким чином, ізольований як зловмисник у мережі. Рисунок 3.5 ілюструє процедуру впровадження запропонованого протоколу.

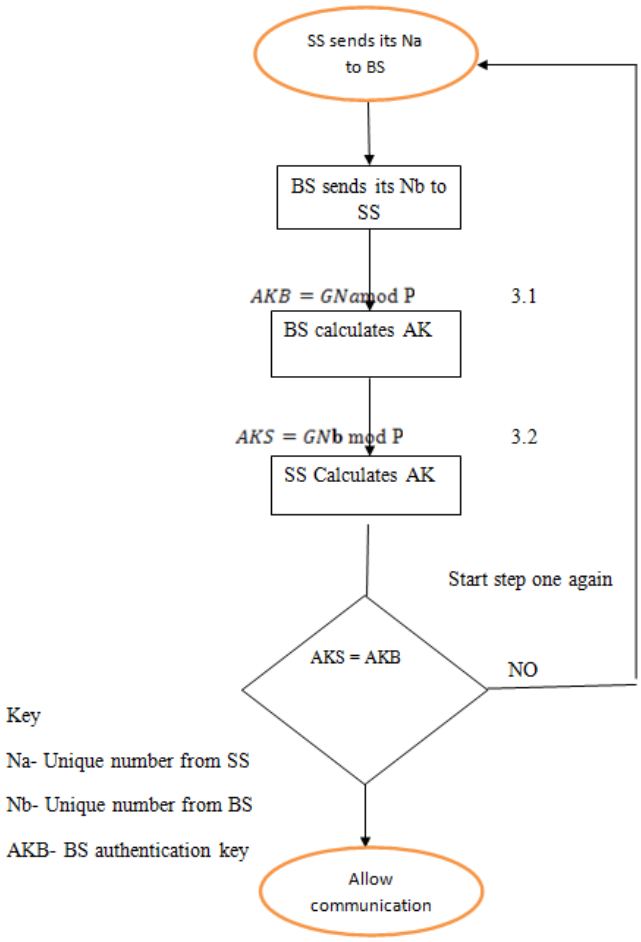


Рисунок 3.12 - Запропонований протокол DH

SS надсилає номер Na до BS. Потім BS надсилає інший унікальний номер Nb до SS. BS розраховує унікальний ключ автентифікації, використовуючи номер, отриманий від SS. SS також обчислює унікальний ключ автентифікації, використовуючи номер, отриманий від BS. Два результати, отримані в результаті обчислень, повинні бути однаковими, щоб автентифікація пройшла успішно. Зв'язок дозволений, лише якщо ключі автентифікації однакові. В іншому випадку зв'язок буде припинено, якщо AKS і AKB не збігаються.

З розгортанням бездротового зв'язку в останні роки питання безпеки в бездротових мережах також стають все більшим занепокоєнням. Конфіденційність або конфіденційність є фундаментальними для безпечного спілкування, яке забезпечує стійкість до перехоплення та прослуховування. Автентифікація повідомлення забезпечує цілісність повідомлення та

автентифікацію відправника, що відповідає атакам на безпеку модифікації повідомлення та уособлення. Атака відтворення повідомлень є однією з найпоширеніших атак на аутентифікацію та протоколи встановлення аутентифікованих ключів. Якщо повідомлення, якими обмінюються в протоколі автентифікації, не містять відповідних ідентифікаторів свіжості, тоді зловмисник може легко пройти автентифікацію, відтворивши повідомлення, скопійовані з законного сеансу автентифікації.

Навіть якщо технологія WiMAX має складні методи автентифікації та авторизації та дуже надійну техніку шифрування, вона все одно вразлива до різних атак або загроз, таких як глушіння, скремблування, MITM або атаки під впливом води. Алгоритм протоколу Diffie Hellmann вводить взаємну автентифікацію між BS і SS перед обміном будь-якою інформацією управління. Для цього дослідження було обрано WiMAX, оскільки це нова технологія, яка зараз розгортається в багатьох частинах світу завдяки своїй широкосмуговій потужності. Ця технологія забезпечує середовище для спілкування багатьох гаджетів. Шахрайський BS може видати себе за справжнього BS, щоб обдурити обладнання SS. Отже, протокол DH актуальний у WiMAX, оскільки він дозволяє взаємну автентифікацію перед обміном конфіденційною мережевою інформацією. Порушення комунікації зловмисником часто призводить до великих збитків у бізнесі. Тому безпека мережі дуже важлива.

# ВИСНОВКИ

Проведено аналіз вразливостей комп’ютерних мереж з метою підвищення рівня їхньої безпеки. Досліджено атаки на локальну мережу для виявлення потенційних загроз і розробки заходів протидії їм. Проаналізувано можливості підміни трафіку частково або окремих пакетів даних з метою розробки ефективних методів виявлення і захисту від подібних атак.

Досліджено можливості сканування мережі на вразливості для розробки превентивних заходів і виявлення потенційних ризиків.

Проаналізувано протоколи безпеки Wi-Fi для визначення їх ефективності та розробки рекомендацій щодо покращення захисту бездротових мереж. Проаналізувано протокол безпеки WPA2 Enterprise з метою виявлення можливих слабкостей і розробки заходів для підвищення безпеки. Досліджено вразливості технології Wi-Fi з метою забезпечення більш ефективного захисту від потенційних загроз. Розглянуто інструменти для моніторингу бездротових мереж для підвищення здатності виявлення аномалій і вразливостей. Досліджено можливі атаки на Wi-Fi для розробки методів їхнього виявлення та захисту від них.

Розглянуто архітектуру WIMAX для зрозуміння потенційних загроз і вдосконалення систем безпеки в мережах WIMAX. Досліджено протокол автентифікації Pkmv1 з метою виявлення слабкостей і можливих напрямків їх виправлення. Досліджено протокол автентифікації Pkmv2 для визначення ефективності і безпеки цього механізму. Проведено дослідження проблеми безпеки протоколів PKMv1 та PKMv2 для забезпечення більш високого рівня захисту мережевих систем, що їх використовують.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Баранюк В.В., Николишин В.І., Лизун Я.І. Налаштування систем широкосмугового звязку Wi-Fi і Wimax. Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно – інтегровані технології» (АКІТ -2023), Тернопіль, 2023. С. 139 -142.

2. Баранюк В.В. Механізми інформаційної безпеки при розгортанні систем широкосмугового зв'язку .Матеріали науково-практичного симпозіуму "Захист інформації", Тернопіль, 2023. С. 12-15.

3. Z.You, X.Xie, W.Zheng," Verification and Research of a WiMAX authentication protocol Based on SSM", ICETC, pp. 22-32, 2010.

4. H.Tseng, R.Hong, W.Yang,"A chaotic maps-base key agreement protocol that preserves user anonymity", IEEE ICC, vol. 3, pp. 67-70, 2009.

5. S.Sidharth, M.P.Sebastian," A Revised Secure Authentication Protocol for IEEE 802.16 (e)", International Conference on Advances in Computer Engineering, pp. 34-42, 2010.

6. K.C.Chen, J.Boberto and B. De Marca, *Mobile WiMAX*. John Wiley & Sons Ltd, p. 56, 2008.

7. K. Jensen, L.Kristensen, L. Wells," Coloured Petri Nets and CPN Tools for Modeling and Validation of Concurrent Systems", Department of Computer Science, pp. 112-122, 2008.

8. M.Barbeau, "WiMAX/802.16 Threat Analysis," in *Proceedings of ACM Q2SWinet'05*, Montreal, Quebec, Canada, 2005, pp. 8-15.

9. H.Tseng, R.Hong, W.Yang,"A chaotic maps-base key agreement protocol that preserves user anonymity", IEEE ICC, pp.44, 2009.

10. J.Huang, C.Tser," Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations", IEEE journal, Vol. 34, issue. 6, pp.45, 2011.

11. M.Bogdanoski, P.Latkoski, A.Risteski, and B.Popovski, "IEEE 802.16 Security Issues: A Survey," in *16th Telecommunications forum TELFOR 2008*, Belgrade, Serbia, pp. 123, 2008.

12. M.Holbal, T, Welzer," An Improved Authentication Protocol Based on One-Way Hash Functions and Diffie-Hellman Key Exchange", International Conference on Availability, Reliability and Security, 2009, pp. 87.

13. R.K.Guha, Z.Furqan, and S.Muhammad, "Discovering Man-In-The-Middle attacks in authentication protocols," in *MILCOM 2007*, Orlando, FL, October 29-31, 2007, pp. 56.

14. [14] A.M.Taha, A.T. Abdel, and S.Tahar, "Formal Verification of IEEE 802.16 Security Sublayer Using Scyther Tool," in *IEEE International Conference on Network and Service, N2S '09*, 2009, pp. 1-5.

15. P.Narayana et al., "Automatic Vulnerability Checking of IEEE 802.16 WiMAX Protocols through TLA+," in *Proceedings of the 2nd IEEE Workshop on Secure Network Protocols*, November, 2006, pp. 44-49.

16. T.Han, N.Zhang, K.Liu, B.Tang, and Y.Liu, "Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions," in *IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 2008, pp. 828-833.

17. M. Bogdanoski, P.Latkoski, A.Risteski, B.Popovski," IEEE 802.16 Security Issues: A Survey", Telecommunication forum, 2008.

18. F.Leu, Y. Huang, C.H.Chiu," Improving security levels of IEEE802.16e authentication by Involving Diffie Hellman PKDS", International Conference on Complex, Intelligent and Software Intensive Systems, pp. 67-74, 2010.

19. K.C.Chen, J.Boberto and B. De Marca, *Mobile WiMAX*. NY: John Wiley & Sons Ltd, pp. 134, 2008.

20. E.M. Clarke, O.Grumberg, and D.A. Peled, *Model Checking*. California: The MIT press, 1999, PP. 121.

21. E.Liu, K.Huang and L.Jin,"the design of trusted access scheme base on identity for WiMAX network" IEEE computer society (International Workshop on Education Technology and Computer Science), 2009, PP. 66.

22. E.Liu, K.Huang and L.Jin,"the design of trusted access scheme base on identity for WiMAX network" IEEE computer society (International Workshop on Education Technology and Computer Science), 2009, PP. 28.

23. J.Huang, C.Tser," Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations" IEEE, 2011, PP. 89.

24. S.Sidharth, M.P.Sebastian," A Revised Secure Authentication Protocol for IEEE 802.16 (e)", International Conference on Advances in Computer Engineering, pp. 34-42, 2010.

25. B. Diffie and M.Hellman, *An overview of Public Key Cryptography*, in IEEE communication magazine, November 1978, vol 16, no. 6.