Захист інформації в інформаційних комунікаційних системах

УДК 519.718.2

Р.І. Банах, А.З. Піскозуб

Національний університет «Львівська політехніка», Львів

ДІАГНОСТИЧНА МОДЕЛЬ СИСТЕМИ-ПРИМАНКИ БЕЗДРОТОВОЇ МЕРЕЖІ СТАНДАРТУ IEEE 802.11

Проведено детальний аналіз існуючих метотодів і механізмів захисту точкок бездротового доступу стандарту IEEE 802.11 (Wi-Fi) та наявні в них вразливості для обладнання сигменту SOHO. Розроблено алгоритм оцінки умовної захищеності системи-приманки для бездротових мереж стандарту IEEE 802.11. Сформульовано вимоги до налаштувань систем-приманок задля створення умов для подальшої взаємодії зі зловмисником належного рівня кваліфікації і наявності потрібного апаратного забезпечення у останнього.

Ключові слова: *система-приманка, діагностика, оцінка вибору конфігурації, метод аналізу ієрархій.*

Вступ

Постановка задачі та аналіз досліджень. Задача будь-якої системи-приманки – піддатись атаці або несанкціонованому дослідженню зі сторони зловмисників, що згодом дозволить вивчити їх стратегію та визначити перелік засобів, за допомогою яких можуть бути нанесені удари по стратегічних об'єктах автоматизованої системи (АС) [1]. Система-приманка являє собою ресурс, який не несе ніякої користі окрім як відвернення уваги від справжніх інформаційних об’єктів, а при взаємодії зловмисника з нею інформація збирається задля подальшої обробки.

Відкритим є питання правильності конфігурування таких систем, особливо це стосується систем-приманок які імітують бездротові мережі, оскільки їх клієнти є мобільними, а контрольована зона часто не є обмеженою [2]. Не правильна конфігурація системи-приманки може стати безкорисним навантаженням у середині АС, особливо це стосується системи приманки для бездротової мережі стандарту IEEE 802.11. Система-приманка із низьким чи відсутнім рівнем захисту може викликати підозру у досвідченого зловмисника, у гіршому ж випадку вона стане легкою здобиччю порушників метою яких є лише доступ до ресурсу Інтернет. З іншого боку, використання системи-приманки із максимальним рівнем захисту також не має сенсу, оскільки така модель стане не приступною фортецею для зловмисника [3–5].

Метою роботи є розробка діагностичної моделі для систем-приманок бездротових мереж стандарту IEEE 802.11, яка допоможе оцінити поточну конфігурацію точки доступу на імовірність використання відомих вразливостей з боку зловмисників.

В рамках поставленої мети було сформульовано наступні завдання: розробити модель порушника для мереж стандарту IEEE 802.11 та описати логічну послідовність його дій; оцінити можливість обходу механізмів захисту наявних у сучасних точках доступу стандарту IEEE 802.11; запропонувати варіації конфігурацій для систем-приманок стандарту IEEE 802.11, які збільшать імовірність взаємодії зі зловмисником потрібного рівня кваліфікації задля вивчення методів, засобів, та вектора атаки останнього.

Основна частина

Опис існуючих механізмів захисту технології бездротового зв’язку IEEE 802.11 та їх вразливості. У первинному виданні стандарту IEEE 802.11 не було задекларовано жодного метода автентифікації. Із відкритою системою з’єднання встановлюється шляхом передачі двох повідомлень.

Розглянемо цей процес на прикладі двох пристроїв A та B. Пристрій A стверджує свою ідентичність до пристрою B, відправивши запит на автентифікацію. Пристрій B надсилає пристрою A результат його запиту, який може бути як позитивним так і негативним. Оскільки не існує ніяких критеріїв для достовірності то результатом неодмінно буде успішна автентифікація.

Деякі виробники реалізовували захист лише за рахунок фільтрування MAC адрес клієнтських пристроїв. Та дана реалізація не гарантує повної захищеності такої мережі, оскільки, не прикладаючи великих зусиль, MAC адреса клієнтського пристрою зловмисника може бути змінена на адресу, яка є у списку «білих» MAC адрес на точці доступу. Окрім того, даний метод приносить незручності у випадку, якщо мережа масштабується.

Для того, щоб отримати доступ до мережі, клієнт при підключенні повинен вказати її ідентифікатор (англ. Service Set Identifier, SSID). Ще одним методом, який дозволяв сховати мережу від сторонніх очей, вважалось приховування SSID. Під час сканування діапазону бездротової мережі стандарту IEEE 802.11 зловмисник може отримати дані про SSID точки доступу, навіть тієї, у налаштуваннях якої встановлений прапорець на функції «не транслювати SSID». Це відбувається тому, що кожен пакет, який відправляється клієнтом до точки доступу, несе в собі інформацію про MAC адресу відправника (клієнта), MAC адресу отримувача (точки доступу) та SSID отримувача. Для отримання такої інформації зловмиснику всього лише потрібно перевести мережеву картку у режим моніторингу і увімкнути фільтр пакетів які надходять на точку доступу із прихованим SSID.

Метод автентифікації Wired Equivalent Privacy (WEP) був введений вже у специфікації стандарту 802.11b, але страждав від цілого ряду серйозних вразливостей. Вразливості WEP були виправлені у специфікації стандарту 802.11i. Метою IEEE 802.11i було підвищення таких ключових завдань захисту інформації як цілісність, доступність та конфіденційність. Завдяки процесу автентифікації за допомогою загального ключа (англ. Shared key) автентифікованими можуть бути лише ті клієнти, які його знають. Загальний ключ розповсюджується між пристроями за допомогою певного механізму поза рамками стандарту IEEE 802.11. Автентифікація здійснюється після чотиристоронннього процесу рукостискання:

1. Пристрій A відправляє запит на авторизацію пристроєві B.
2. Пристрій B готує випадковий 128-октетний текст (challenge text) використовуючи псевдовипадковий числовий генератор і відправляється пристроєві A.
3. Пристрій A шифрує challenge text використовуючи шифр RC4 (тим самим методом, що і кадри з даними).
4. Коли пристрій B отримує зашифрований кадр, він перевіряє його цілісність. Якщо значення ICV (англ. Integrity check value, значення перевірки цілісності) є вірним, то він перевіряє challenge text, і у випадку, якщо він збігається з оригінальним, то пристрій B відправляє статус код про успішність процесу авторизації.

ICV обчислюється для кожного кадру M. ICV це 32-бітний CRC (англ. Cyclic redundancy check, циклічна перевірка надлишковості), таким чином із кадру з відкритим текстом M отримуємо $ICV=CRC_{32}(M)$. ICV конкатенується з відкритим текстом пакету M і формує пакет P = M | ICV. Потік ключів генерується з використанням псевдовипадкового числового генератора із ключа WEP (K_{WEP}) і 24-бітного вектора ініціалізації (англ. Initialization vector (IV)). Новий вектор ініціалізації використовується для кожного кадру. Та проблемою є те, що вектори ініціалізації перевикористовуються через кожні 24^2 кадри. Вектор ініціалізації передує ключеві K_{WEP}, для того, щоб сформувати передкадровий ключ $K = I \mid K_{WEP}$. Пакет P шифрується за допомогою шифру RC4. Шифроване повідомлення отримується за допомогою операції XOR по відношенню до передкадрового ключа K та пакету P:

$$C = P \oplus K .$$

У початковому вигляді ключ WEP був довжиною в 40 бітів, що згодом почало вважатись не достатнім для захисту. Тому згодом довжину ключа було збільшено до 104 бітів.

Ключовий потік K може бути відновлений за допомогою використання функції XOR по відношенню до відкритих повідомлень і шифртексту. Таким чином, загальний ключ є найбільш вразливим під час процесу автентифікації, оскільки відкритий challenge text і зашифрована відповідь передаються одним і тим же ж каналом. Великим недоліком є і те, що один і той самий ключ використовується як для автентифікації, так і для шифрування. Ця проблема поглиблюється в результаті використання статичних ключів, заміна яких відбувається мануально і, як правило, не часто.

Довжина вектора ініціалізації складає 24 біти і вважається не достатньою. У мережах із великою кількістю трафіку буде часто виникати колізія вектора ініціалізації. Відповідно до цього імовірність його вгадування збільшується відносно кількості колізій.

У стандарті 802.11 реалізовано два механізми – це Pre-shared key (PSK) та 802.1x. На PSK загальний ключ встановлюється на точці доступу. Взаємна автентифікація встановлюється, використовуючи чотиристоронній процес рукостискання. Зазвичай ключі встановлюються на бездротовий пристрій мануально. Очевидно, що для мереж із великою кількістю клієнтів використання одного і того ж ключа для всіх клієнтів є не доцільним, тому для них використовується механізм 802.1x, а PSK, своєю чергою використовується у мережах типу SOHO (Small or home office). Саме про такі мережі далі і піде мова.

Незважаючи на покращення безпеки, у специфікації стандарту 802.11i було визначено, що використання застарілих апаратних засобів стандарту IEEE 802.11 буде і надалі використовуватись протягом деякого часу. Програмне забезпечення на застарілих пристроях використовувало WEP, а відповідно і шифр RC4. Для того, щоб уникнути неправильного використання WEP, а саме неправильного планування ключів, колізій вектора ініціалізації та фальшування пакетів, у 802.11i було визначено підпротокол Temporal Key Integrity Protocol (TKIP). TKIP працює як обгортка навколо шифрування WEP, забезпечуючи більш складну функцію перемішування ключів. 128 бітний покадровий ключ шифрування RC4 отримується з тимчасового ключа (TK) клієнт-

ського MAC адресу і вектора ініціалізації. Вектор ініціалізації у TKIP діє як лічильник послідовності для захисту від атаки повторення

Функція змішування TKIP працює у двох фазах. У першій фазі TKIP-mixed передає адресу і ключ (TTAK), обчислений з TK, MAC адреси (TA), і лічильника послідовності TKIP (TSC). Покадровий ключ WEP_{SEED} генерується у другій фазі, використовуючи TTAK, TA та TSC. WEP_{SEED} проходить процес інкапсуляції WEP поряд з відкритим текстом кадру M. WEP бере ключ RC4 та вектор ініціалізації з WEP_{SEED}. Тому WEP_{SEED} використовується замість ключа WEP і вектора ініціалізації WEP. WEP обчислює ICV і зашифровує M для створення кадру шифртексту.

TKIP включає в себе 64-бітну перевірку цілісності повідомлення MIC для кожного каджу. Алгоритм який використовується для обчислення MIC називається Michael. Його метою є запобігання атак яким був піддається WEP. MIC обчислюється за допомогою таких даних, як адреса джерела (SA), адреса призначення (DA), поле пріоритету (Pr), трьох зарезервованих октетів (Rsvd) і відкритого тексту (M) кадру MAC:

$$MIC = Michael(SA \mid DA \mid Pr \mid Psvd \mid M) .$$

TSC використовується для захисту проти атаки повторення. Кадри у яких послідовність не зростає – ігноруються отримувачем.

Хоч Michael і є покращенням CRC, який використовується у WEP, та він не є безвідмовним і все одно існує імовірність компрометації цілісності повідомлень. Це відбувається через конструктивні обмеження, що накладаються на реалізацію, яка вимагає підтримки застарілих апаратних засобів. Як наслідок, в TKIP імплементовано протидію задля зменшення імовірності фальшування і лімітування відносно інформації про ключ. Якщо виникає підозра на атаку, то операції TKIP призупиняються на 60 секунд, парні ключі генеруються повторно. Такі контр-заходи застосовуються у випадку, якщо протягом однієї хвилини з'являються два кадри із не коректним MIC.

Ключ RC4 та вектор ініціалізації, які використовуються в WEP_{SEED}, звертається до процесу інкапсуляції WEP. WEP використовує це для генерації ICV і шифрування MPDU та MIC. Не зважаючи на те, що реалізація TKIP є складнішою за WEP, все ж MIC є досить слабким відносно підробки повідомлень. Тим не менше, він являє собою краще, що може бути досягнено на застарілому обладнанні. Протокол TKIP імплементований в методі автентифікації Wi-Fi Protected Access (WPA).

Згодом було запропоновано нову версію метода автентифікації WPA, яка базувалась на протоколі CCMP. CCMP – це протокол, який базується на режимі лічильника протоколу AES з перевіркою автентичності ланцюжка повідомлення шифр-блоку (CBC-MAC). За допомогою режиму лічильника забезпечується конфіденційність, а CBC-MAC використовується для забезпечення цілісності. Алгоритм шифрування AES є набагато стійкішим за RC4, який використовується у WEP та TKIP. Проте він не може функціонувати на застарілому обладнанні.

Клієнт отримує доступ до мережі з методом автентифікації WPA2, пройшовши чотиристоронній процес рукостискання. Та проблема даного методу полягає у тому, що цей пакет може бути отриманий будь-якою бездротовою карткою, яка працює у режимі моніторингу на частотах 2.401 - 2.483 ГГц.

Коли клієнт або точка доступу збирається перезавантажуватись або клієнт покидає зону покриття, відправляється спеціальний кадр деавтентифікації, який не проходить перевірку автентичності. Це означає, що будь-який пристрій який працює за стандартом 802.11, і є в зоні покриття конкретної точки доступу – може відправити згенерований кадр деавтентифікації, в результаті чого отримати пакет рукостискання.

Маючи пакет рукостискання, зловмисник може запустити лобову атаку на цей пакет, перебуваючи навіть на відстані від точки доступу.

Для того, щоб ускладнити задачу по дешифруванню пакету рукостискання рекомендується встановлювати складні паролі.

Для середньостатистичного користувача бездротової мережі сегменту SOHO є набагато зручнішим варіант, у якому підключення відбувається за допомогою простого паролю.

Для того, щоб спростити схему авторизації і водночас зробити лобову атаку на методи автентифікації WPA/WPA2 не доцільною, було запропоновано механізм Wi-Fi Protected Setup (WPS). WPS дозволяє користувачеві майже автоматично отримати доступ до мережі. Згодом після введення його в експлуатацію, було виявлено, що сам механізм є вразливим до атаки грубої сили.

Пін-код, за допомогою якого і проводиться автентифікація, складається з восьми цифр, які при переборі можна розбити на дві частини, оскільки при відгадуванні першої половини пін-коду точка доступу почне відправляти повідомлення про те, що друга половина не є вірною. Окрім того остання цифра є контрольною сумою перших семи цифр, і може бути відновлена за формулою:

$$f(n) = f\left(\left[\left[\frac{n}{10}\right]/10\right]\right) + 3(n \bmod 10) + \left(\left[\frac{n}{10}\right] \bmod 10\right).$$

Отримавши $f(n)$, можемо отримати контрольну суму (останній символ пін-коду) S_C:

$$S_C = (10 - f(n) \bmod 10) \bmod 10 .$$

Відповідно до цього зловмисникові потрібно перебрати всього лиш $10^4 + 10^3$ варіантів.

Підстави до формування критеріїв діагностичної моделі системи приманки бездротової мережі стандарту IEEE 802.11 полягають у оцінці складності обходу методів їх захисту. Як вже було

згадано вище, кожен із методів захисту може бути скомпрометований в залежності від навичок та технічного забезпечення зловмисника. Точка доступу, а у нашому випадку система-приманка, захист якої є повністю відсутнім, або не достатнім, може стати легкою здобиччю для осіб, які мають на меті скористатись безкоштовним ресурсом Інтернет або ж викликати підозру у досвідчених зловмисників.

Як вже було зазначено вище – найслабшим із методів автентифікацій є WEP, а отже його використання точкою доступу імовірно буде сприйматись як помилка з боку адміністратора мережі або наявність в мережі застарілого обладнання.

Комбінація певних факторів може зменшити імовірність взаємодії зловмисника із системою приманкою. Наприклад, присутність підключеного клієнта обов'язкова у більшості конфігурацій точки доступу, інакше проведення атаки буде не реальним. В результаті збору метаданих з діапазону частот 2.401— 2.483 ГГц за допомогою мережевої картки, яка працює в режимі моніторингу, зловмисник може цілком або частково отримати дані про точку доступу і її клієнтів.

Згадана вище вразливість методів автентифікації WPA/WPA2 також може бути проведена лише за наявності підключеного клієнта. Виключенням може бути лише варіант конфігурації з увімкнутим механізмом WPS, лобова атака на який не потребує наявності підключеного клієнта, оскільки перебір PIN коду відбувається лише по відношенню до точки доступу.

Для атаки на метод автентифікації WPA зловмисникові необхідно отримати спеціальний пакет рукостискання між точкою доступу і клієнтом, який знає ключ до мережі. Такий пакет перехоплюється зловмисником у момент підключення клієнта до мережі.

Ситуація ускладнюється у випадках конфігурацій, де присутні такі механізми як прихований SSID, увімкнене фільтрування MAC адресів або увімкнутий метод автентифікації WPA2 із вимкненим WPS, і відсутні підключені клієнти. В таких випадках зловмисник буде змушений очікувати на появу клієнта або ж розпочати атаку грубої сили задля отримання імені точки доступу, або ж MAC адреси. У випадку з MAC адресами, їх імовірніше отримати в процесі перебору аніж SSID, оскільки кількість MAC адресів є скінченною комбінацією і дорівнює $A^{6}_{A^{2}_{16}}$, то у випадку SSID їх кількість прямує до безкінечності.

Для конфігурації системи-приманки з використанням методу автентифікації WPA/WPA2 повинен бути встановлений ключ, який може бути віднайдений під час перебору за загальнодоступними словниками. Виробники сучасних точок доступу навчились протидіяти атаці грубої сили на механізм WPS, запроваджуючи час очікування після певної кількості невдалих спроб. Такий функціонал може унеможливити доступ зловмисника до системи-приманки [6–7].

На основі викладених вище даних сформулюємо таблицю істинності комбінацій механізмів захисту бездротових мереж стандарту IEEE 802.11 (табл. 1) та побудуємо блок-схему алгоритму дослідження системи приманки на можливість бути атакованою (рис. 1).

Таблиця 1

Можливі комбінації механізмів захисту бездротових мереж стандарту IEEE 802.11

№	Open	WEP	WPA	MAC Filter	Hidden SSID	WPS	Присутність клієнтського пристрою
1	+	-	-	-	-	-	Не є необхідністю
2	+	-	-	+	-	-	Необхідна
3	+	-	-	-	+	-	Необхідна
4	+	-	-	+	+	-	Необхідна
5	-	+	-	-	-	-	Не є необхідністю
6	-	+	-	+	-	-	Необхідна
7	-	+	-	-	+	-	Необхідна
8	-	+	-	+	+	-	Необхідна
9	-	-	+	-	-	-	Необхідна
10	-	-	+	+	-	-	Необхідна
11	-	-	+	-	+	-	Необхідна
12	-	-	+	+	+	-	Необхідна
13	-	-	+	-	-	+	Не є необхідністю
14	-	-	+	+	-	+	Необхідна
15	-	-	+	-	+	+	Необхідна
16	-	-	+	+	+	+	Необхідна

Задля оцінки складності подолання умовного захисту системи-приманки зробимо їх оцінку за рахунок коефіцієнтів методу аналізу ієрархій, на основі таких критеріїв, як час подолання захисту, наявність відповідного апаратного забезпечення яке доведеться використати зловмиснику (табл. 2).

Даний метод дозволяє отримати співвідношення шкал від парних порівнянь із не великим відхиленням [8–10]. В якості коефіцієнтів використовується фактичне вимірювання або суб'єктивна думка. На виході отримується співвідношення ваг та індекс узгодженості.

У стандартному виконанні методу аналізу ієрархій здійснюється оцінка будь-якої групи характеристик за допомогою шкали коефіцієнтів від 1 до 9 (табл. 3). За допомогою даної таблиці виводиться матриця ваги кожного з елементів по відношенню одне до одного (1).

$$N = \begin{vmatrix} 1 & a_{12} & \cdots & a_{1n} \\ a_{12}^{-1} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n}^{-1} & a_{2n}^{-1} & \cdots & 1 \end{vmatrix}. \qquad (1)$$

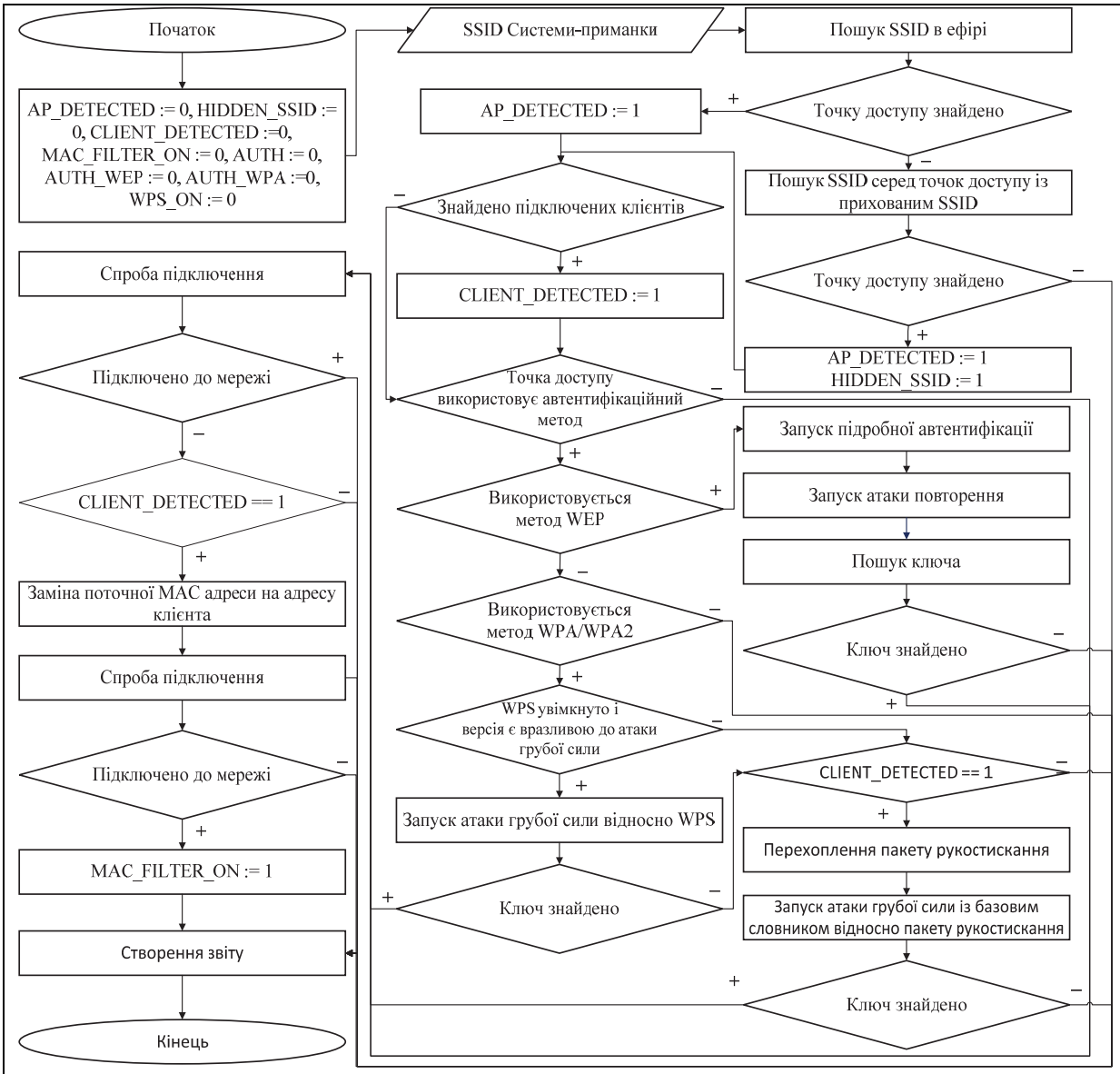

Рис. 1. Алгоритм діагностичної моделі системи приманки бездротової мережі IEEE 802.11

Таблиця 2

Оцінка складності подолання умовного захисту системи-приманки

Оцінковий Критерій / Метод захисту	Час подолання	Наявність відповідного АЗ	Складності під час проведення атаки
WEP	t ~ 30 хв.	Для реалізації даної атаки достатньо мати базову мережеву картку Wi-Fi	Якщо клієнт не підключений до точки доступу, зловмиснику потрібно провести атаку підробної автентифікації
WAP/WPA2	5 хв > t > ∞	Для реалізації даної атаки необхідно мати мережеву картку за допомогої якої можна відправити пакет деавтентифікації.	Якщо клієнт не підключений до мережі, то атака не може бути здійснена, оскільки перехоплення пакету рукостискання є не можливим.
			Атака набуває складності із збільшенням кількості символів у ключі і кількості
MAC Filter	1 хв > t > ∞	Для реалізації даної атаки достатньо мати базову мережеву картку Wi-Fi	Проведення атаки ускладнюється якщо до мережі не підключені клієнти, в такому випадку потрібно провести атаку грубої сили
Hidden SSID	1 хв > t > ∞	Для реалізації даної атаки достатньо мати базову мережеву картку Wi-Fi	Проведення атаки ускладнюється якщо до мережі не підключені клієнти
WPS	1 хв > t > ∞	Для реалізації даної атаки достатньо мати базову мережеву картку Wi-Fi	Проведення атаки ускладнюється або є не можливим у випадку якщо версія WPS > 1

Таблиця 3

Шкала оцінки коефіцієнтів у методі аналізу ієрархій

Цифрове значення	Визначення
1	Рівне значення
3	Не значна перевага одного значення над іншим
5	Істотна перевага одного значення над іншим
7	Видима перевага одного значення над іншим
9	Абсолютна перевага одного значення над іншим
2,4,6,8	Середнє судження поміж двох суміжних суджень

На основі табл. 2, 3 зробимо оцінку складності обходу механізмів захисту по відношенню одне до одного.

Таблиця 4

Порівняння складності обходу механізмів захисту точки доступу стандарту IEEE 802.11

MAC Filter	½	Hidden SSID
	5	WEP
	8	WPA/WPA2
	7	WPS
Hidden SSID	2	MAC Filter
	5	WEP
	8	WPA/WPA2
	7	WPS
WEP	1/6	Hidden SSID
	1/6	MAC Filter
	5	WPA/WPA2
	5	WPS
WPA	1/8	Hidden SSID
	1/8	MAC Filter
	1/6	WEP
	1/4	WPS
WPS	1/7	Hidden SSID
	1/7	MAC Filter
	1/6	WEP
	4	WPA/WPA2

На основі (1) та табл. 4 знайдемо матрицю ваг кожного з елементів по відношенню одне до одного

$$N = \begin{vmatrix} 1 & 2 & 1/5 & 1/8 & 1/7 \\ 1/2 & 1 & 1/5 & 1/8 & 1/7 \\ 5 & 5 & 1 & 1/6 & 1/6 \\ 8 & 8 & 6 & 1 & 4 \\ 7 & 7 & 6 & 1/4 & 1 \end{vmatrix}.$$

Знайдемо суми коефіцієнтів для кожного зі стовпців для подальшої нормалізації матриці N (3).

$$S_i = \sum_{i=1}^{n} a_i = a_{i1} + a_{i2} + ... + a_{in}\ , \qquad (2)$$

$$|N| = \begin{vmatrix} \frac{1}{S_1} & \frac{a_{12}}{S_2} & \dots & \frac{a_{1n}}{S_n} \\ \frac{a_{12}^{-1}}{S_1} & \frac{1}{S_2} & \dots & \frac{a_{2n}}{S_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{a_{1n}^{-1}}{S_1} & \frac{a_{2n}^{-1}}{S_2} & \dots & \frac{1}{S_n} \end{vmatrix}. \qquad (3)$$

Відповідно до (2), суми стовпців будуть наступними – $S_1 = 21,5$; $S_2 = 23$; $S_3 = 12,41$; $S_4 = 1,67$; $S_5 = 5,45$. Відповідно до (3) знайдемо нормалізовану матрицю |N|:

$$|N| = \begin{vmatrix} \frac{1}{21,5} & \frac{2}{23} & \frac{1/5}{12,41} & \frac{1/8}{1,67} & \frac{1/7}{5,54} \\ \frac{1/2}{21,5} & \frac{1}{23} & \frac{1/5}{12,41} & \frac{1/8}{1,67} & \frac{1/7}{5,54} \\ \frac{5}{21,5} & \frac{5}{23} & \frac{1}{12,41} & \frac{1/6}{1,67} & \frac{1/6}{5,54} \\ \frac{8}{21,5} & \frac{8}{23} & \frac{6}{12,41} & \frac{1}{1,67} & \frac{4}{5,54} \\ \frac{7}{21,5} & \frac{7}{23} & \frac{6}{12,41} & \frac{1/4}{1,67} & \frac{1}{5,54} \end{vmatrix} =$$

$$= \begin{vmatrix} 0,047 & 0,087 & 0,016 & 0,075 & 0,026 \\ 0,023 & 0,043 & 0,016 & 0,075 & 0,026 \\ 0,232 & 0,218 & 0,08 & 0,1 & 0,03 \\ 0,372 & 0,348 & 0,483 & 0,6 & 0,733 \\ 0,326 & 0,304 & 0,483 & 0,15 & 0,183 \end{vmatrix}.$$

Просумувавши коефіцієнти кожного рядка нормалізованої матриці і розділивши суму на кількість коефіцієнтів рядка за допомогою (4), можна отримати вагу кожного з механізмів захисту.

$$x = \begin{bmatrix} \sum \frac{row_1}{n} \\ \sum \frac{row_k}{n} \\ \dots \\ \sum \frac{row_k}{n} \end{bmatrix}. \qquad (4)$$

Отже, в даному випадку отримаємо наступну матрицю

$$x = \begin{bmatrix} \frac{0,047+0,087+0,016+0,075+0,026}{5} \\ \frac{0,023+0,043+0,016+0,075+0,025}{5} \\ \frac{0,232+0,218+0,08+0,1+0,03}{5} \\ \frac{0,372+0,348+0,483+0,6+0,733}{5} \\ \frac{0,326+0,304+0,483+0,15+0,183}{5} \end{bmatrix} =$$

$$x = \begin{bmatrix} 0,0502 \\ 0,0366 \\ 0,132 \\ 0,5072 \\ 0,2892 \end{bmatrix}.$$

Відповідно до матриці *x* отримуємо коефіцієнти для кожного із механізмів захисту.

Фільтрування за MAC адресою дорівнює 0,0502; приховування імені точки доступу (SSID) за рахунок вимкнення функції розсилання маячків у відкритий ефір рівне 0,0366; метод автентифікації WEP рівний 0,132; методи автентифікації WPA/WPA2 дорівнює 0,5072; WPS дорівнює 0,2892.

Висновки

На основі отриманих коефіцієнтів в результаті проведеного обчислення за методом оцінки ієрархій можемо оцінити складності обходу кожної із комбінацій механізмів захисту точки доступу стандарту IEEE 802.11 за рахунок додавання коефіцієнтів, на відрізку від 0 до 1. Оскільки увімкнений механізм WPS лише погіршує захищеність точки доступу то комбінація даного механізму з методом автентифікації WPA/WPA2 представлятиме собою різницю коефіцієнтів, а саме:

$$\text{WPA} - \text{WPS} = 0,5072 - 0,2892 = 0,218.$$

Для того щоб зацікавити зловмисників – захист на точці доступу однозначно повинен бути присутнім, але таким чином, щоб його можна було з відносно не великими зусиллями подолати. Авторами пропонуються наступні варіанти конфігурацій з табл. 1, це варіанти 4–8, як імовірність наявності у мережі застарілого обладнання. Варіант 9, з ключем який можна знайти у базових словниках для перебору, атакою грубої сили. Варіант 13, як імовірно не вірна конфігурація або не можливість відключити вразливий протокол WPS на точці доступу.

Наведені вище шаблони конфігурацій дозволять збільшити імовірність взаємодії зловмисника із системою-приманкою.

В даній роботі коефіцієнт для методу автентифікації WPA представлений як найстійкіший механізм захисту бездротових мереж. Та даний метод потребує окремої детальної оцінки. Подальшими кроками у даному дослідженні буде дослідження методу автентифікації WPA/WPA2, визначення довжини ключа для взаємодії зі зловмисником певного рівня кваліфікації.

Список літератури

1. *Goel R. Wireless Honeypot: Framework, Architectures and Tools / R. Goel, A. Sardana, R. C. Joshi // International Journal of Network Security, Vol.15, No.5, PP.373-383, Sept. 2013. – 373 – 383 p.*
2. *Zhang L. A Network Security Evaluation Method based on FUZZY and RST / Lijuan Z., Qingxian W. // 2010 2nd International Conference on Education Technology and Computer (ICETC). – P. 40-44.*
3. *Методи та засоби аналізу систем приманок в процесі зламу / Дудикевич В.Б., Піскозуб А.З., Тимошик Н.П., Тимошик Р.П., Дуткевич Т.В. // Науково-технічний журнал «захист інформації» № 1, 2009. – С. 27-31.*
4. *Оцінка ефективності систем захисту інформації / Гарасимчук О.І., Костів Ю.М. // Інформатика, математичне моделювання та інформаційні технології. Вісник КНУ імені Михайла Остроградського. Випуск 1/2011 (66). Частина 1. – 2011. – С. 16-20.*
5. *Сучасні системи віртуальних приманок на основі технології honeypot / Гнатюк С.О., Волянська В.В., Карпенко С.В. // Науково-практичний журнал «захист інформації» № 3. – 2012. – С. 107-115.*
6. *Інформаційна модель безпеки технологій зв'язку / Дудикевич В.Б., Хорошко В.О., Микитин Г.В., Банах Р.І., Ребець А.І. // Інформатика та математичні методи в моделюванні. – 2014 Том 4. – №2. – С. 137-148.*
7. *Комплексний підхід до захисту мовної інформації в технологіях безпровідного зв'язку / В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець, Р.І. Банах // Інформаційна безпека. – Східноукраїнський Національний університет імені Володимира Даля.) – 2013. – № 4(12). – С. 16-22.*
8. *Zhang R. Security for Wireless Network Based on Fuzzy-AHP with Variable Weight / R. Zhang, L. Huang, M. Xiao // 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing. – P. 490-493.*
9. *Ajah I. A. Evaluation of Enhanced Security Solutions in 802.11-Based Networks / Ajah I. A. // International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014. – P. 29-42.*
10. *Zhang L. Network Security Evaluation through Attack Graph Generation / Zhang L., Tang H., Cui Y.M., Zhang J. // World Academy of Science, Engineering and Technology 30 2009. – P. 407-410.*

Надійшла до редколегії 14.03.2017

Рецензент: д-р техн. наук, проф. Г.В. Микитин, Національний університет «Львівська політехніка», Львів.

ДИАГНОСТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ-ПРИМАНКИ БЕЗПРОВОДНОЙ СЕТИ СТАНДАРТА IEEE 802.11

Р.И. Банах, А.З. Пискозуб

Проведен детальный анализ существующих методов и механизмов защиты точек беспроводного доступа стандарта IEEE 802.11 (Wi-Fi) и имеющихся в них уязвимостей для оборудования сигмента SOHO. Разработан алгоритм оценки условной защищенности системы-приманки для создания условий для дальнейшего взаимодействия с злоумышленником с надлежащим уровнем квалификации и наличием надлежащего апаратного обеспечения у последнего.

Ключевые слова: *система-приманка, диагностика, оценка выбору конфигураций, метод анализа иерархий.*

A DIAGNOSTICAL MODEL OF HONEYPOT FOR IEEE 802.11 WIRELESS NETWORK

R.I. Banakh, A.Z. Piskozub

Detailed analysis of existed defense methods mechanisms and their vulnerabilities of IEEE 802.11 wireless access points for SOHO segment is provided. An evaluation algorithm of conditional security for IEEE 802.11 wireless networks is designed. Requirements for honeypot settings in order to provide conditions for further interaction with attacker who has appropriate level of qualification and needed computing availability owning are formulated.

Keywords: *honeypot, diagnostic, evaluation of configuration, analytic hierarchy process.*