УДК 004.7:004.056.5

АНАЛІЗ МЕХАНІЗМІВ ЗАХИСТУ ТА ВРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ WI-FI МЕРЕЖ

Автор: Шовкута Володимир Андрійович
Керівник – співавтор: Флоров Сергій Володимирович
ДВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, E-mail: v.shovkuta@gmail.com

Сьогодні все більше користувачів надають перевагу бездротовим мережам Wi-Fi, що міцно посіли важливе місце в нашому житті. Вони дозволяють отримати широкосмуговий доступ до мережі Інтернет, дають можливість обміну файлами у локальній мережі, не застосовуючи кабелі передачі даних. Перебуваючи в громадському місці чи в колі друзів, багато хто починає шукати найближчу точку доступу Wi-Fi, ні на хвилину не замислюючись про питання безпеки при користуванні бездротовими мережами. Слабке уявлення користувачів про загрози в бездротових мережах дозволяють зловмиснику отримати доступ до інформації користувачів, адже завдяки особливостям середовища передачі бездротові мережі не можуть забезпечити розмежування доступу до даних, тому пакети, що передаються клієнтом або точкою доступу, можуть бути отримані будь-яким пристроєм в зоні дії мережі.

Ключові слова – Wi-Fi; бездротові мережі; шифрування, автентифікація, точка доступу, мережеве обладнання, WEP, WPA, WPA2, WPS, WDS.

ВСТУП

За прогнозом компанії Cisco, наведеним у звіті «Наочний індекс розвитку мережевих технологій: повний прогноз на період 2015-2020 рр.» (Cisco Visual Networking Index™ (VNI) Complete Forecast for 2015 to 2020), число точок доступу Wi-Fi в світі (включаючи домашні) виросте семикратно і до 2020 року досягне 432 млн (так, наприклад, показник 2015 року – 64 млн), а на Wi-Fi та мобільні пристрої буде припадати близько двох третин IP-трафіку [1].

А, наприклад, за даними, наведеними в інфографіці для сайту BotRevolt.com, 49 відсотків всіх мереж Wi-Fi є незахищеними, з яких 89 відсотків є мережами, розташованими у громадських місцях, а на маршрутизаторах 80 відсотків сімей у світі досі встановлені паролі за замовчанням [2].

Все це, з огляду на неминуче розповсюдження бездротових мереж та зростаючий трафік у цих мережах, може призвести до безлічі інцидентів інформаційної безпеки, наприклад:

- розголошення конфіденційної або внутрішньої інформації;
- несанкціонований доступ до інформації;
- вірусна атака;
- компрометація облікових записів;
- перевищення повноважень;
- моніторинг інформаційної системи;
- атаки на мережеве обладнання та інше.

ОРГАНІЗАЦІЯ WI-FI МЕРЕЖ

Організацію бездротових мереж Wi-Fi можна поділити на 2 групи:

1. Ad-hoc (бездротові самоорганізовані мережі);
2. Hot-spot (бездротові керовані мережі).

У бездротової локальної мережі типу Ad-hoc зв'язок встановлюється безпосередньо між пристроями, обладнаними Wi-Fi-адаптерами, і в цьому випадку точка доступу взагалі не використовується.

У бездротової локальної мережі, що функціонує в режимі Hot-spot, бездротові пристрої спілкуються між собою через точку доступу, за допомогою якої відбувається не тільки взаємодія всередині мережі, але й доступ до зовнішніх мереж. Точка доступу передає ідентифікатор мережі SSID (Service Set ID) за допомогою спеціальних сигнальних пакетів. Бездротові пристрої підключаються до точки доступу, використовуючи її ідентифікатор мережі SSID, і обмінюються інформацією один з одним. У цьому випадку точка доступу використовується в якості центральної точки підключення бездротових пристроїв.

З точки зору захисту інформації Hot-spot має більше значення, оскільки, отримавши доступ до точки доступу, зловмисник може мати змогу отримати інформацію не тільки зі станцій, розміщених у цій бездротовій мережі, а й зі станцій розміщених у дротовій мережі, до якої підключена ця точка доступу [3].

МЕХАНІЗМИ ЗАХИСТУ WI-FI МЕРЕЖ

Механізми захисту Wi-Fi мереж передбачають автентифікацію (клієнт та точка доступу представляються один одному і підтверджують права на обмін даними) та шифрування (обрання алгоритму шифрування інформації та даних, що передаються по бездротовій мережі, генерація та зміна ключів).

Методи автентифікації клієнтів.

1. Відкрита автентифікація (Open Authentication).

Відкрита автентифікація передбачає захист бездротової мережі на основі MAC-фільтрації. Клієнт робить запит автентифікації, надсилаючи точці доступу свою MAC-адресу, точка доступу відповідає або підтвердженням (у разі знаходження MAC-адреси клієнта у таблиці дозволених адрес) або відмовою у автентифікації.

Порівняння MAC-адреси клієнта з таблицею дозволених MAC-адрес підтримується більшістю виробників мережевого обладнання та може

застосовуватися як додатковий захід захисту разом з наступними методами.

2. Автентифікація із загальним ключем (Shared Key Authentication).

Клієнт надсилає запит на автентифікацію точці доступу, отримуючи у відповідь підтвердження, що містить випадкову інформацію довжиною 128 біт. Клієнт шифрує отримані дані за допомогою алгоритму WEP (Wired Equivalent Privacy) за допомогою побітового додавання за модулем 2 (операція XOR) отриманої випадкової послідовності та послідовності ключа й відправляє зашифрований текст разом із запитом на асоціацію. Впевнившись у відповідності, точка доступу надсилає клієнту підтвердження асоціації. Після цього клієнт вважається підключеним до мережі.

Для використання автентифікації із загальним ключем необхідно попередньо налаштувати статичний ключ шифрування алгоритму WEP [4].

3. WPA (Wi-Fi Protected Access).

Внаслідок перших успішних атак на метод WEP було випущено проміжний стандарт WPA, що включає у собі нову систему автентифікації на базі 801.1x та новий метод шифрування TKIP (Temporal Key Integrity Protocol) – протокол перевірки цілісності ключа, який використовує вдосконалений спосіб керування ключами і покадрову зміну ключа.

Існують два варіанти автентифікації: за допомогою зовнішнього серверу, якому користувачі надають свої дані для автентифікації (WPA-Enterprise), та з використанням завчасно наданого ключа, що встановлюється на точці доступу (WPA-Pre-Shared Key) [5].

4. WPA2 (Wi-Fi Protected Access2, IEEE 802.11i).

WPA2 або IEEE 802.11i є варіант стандарту безпеки бездротових мереж, у якому в якості основного алгоритму шифрування було обрано стійкий блоковий шифр AES, а для зберігання зворотної сумісності з WPA може використовуватися TKIP. Алгоритм автентифікації у порівнянні з WPA зазнав незначних змін, але зберіг два варіанти автентифікації: WPA-Enterprise та WPA-Pre-Shared Key [5].

Методи шифрування даних.

1. WEP-шифрування.

WEP – один з перших алгоритмів, що забезпечує захист інформації, яка циркулює у бездротовій мережі. У якості основи для WEP було обрано потоковий шифр RC4 з ефективними довжинами ключів 40 чи 104 біт. На практиці використовують ключі довжиною 64 чи 128 біт, 24 біта з яких використовуються у якості вектору ініціалізації (Initialization Vector, IV), що містить дані для розшифрування повідомлення.

WEP-шифрування полягає у наступному: в першу чергу передані в пакеті дані перевіряються на цілісність за допомогою алгоритму CRC-32, після чого отримана контрольна сума додається в службове поле заготовки пакету даних. Далі генерується вектору ініціалізації довжиною 24 біти, до якого додається статичний 40 чи 104 бітний секретний ключ. Отриманий таким чином ключ довжиною 64 чи 128 біти є ключем для генерації псевдовипадкового числа, що використовується для шифрування даних. Наступним кроком алгоритму є виконання операції XOR між даними, що передаються, та отриманою псевдовипадковою послідовністю. Використаний вектор ініціалізації додається у службове поле кадру [4].

2. WPA-шифрування.

Головною особливістю наступного стандарту безпеки – WPA – стала технологія динамічної генерації ключів, побудована на протоколі TKIP, що використовує вектор ініціалізації довжиною 48 біт, замість 24 біт у WEP, та реалізація правила зміни його бітової послідовності для виключення повторного застосування ключа. Використання протоколу TKIP передбачає те, що для кожного пакету даних відбувається генерація нового ключа довжиною 128 біт. Крім цього контрольні криптографічні суми розраховуються за методом MIC (Message Integrity Code): у кожний кадр вкладається спеціальний код цілісності повідомлення довжиною 8 байт, перевірка якого дозволяє попередити атаки з використанням підміни пакетів. Якщо протягом хвилини буде відправлено більше двох пакетів, що не пройшли перевірку, то клієнта буде заблоковано на одну хвилину [5].

3. WPA2-шифрування.

Впровадження WPA2 істотно підвищило захищеність бездротових Wi-Fi мереж у порівнянні з попередніми технологіями. Новий стандарт передбачає обов'язкове використання стійкого блочного шифру AES – CCMP (Advanced Encryption Standard – Counter CBC-MAC Protocol). У режимі WPA-Pre-Shared Key з уведеного у вигляді відкритого тексту паролю генерується ключ PSK (PreShared Key) довжиною 256 біт. Цей ключ сумісно з SSID та ще чотирма параметрами використовується для генерації тимчасових сеансових ключів PTK (Pairwise Transient Key) для взаємодії бездротових пристроїв. Режим WPA2-Enterprise дозволяє більш гнучко організувати роботу мережі за допомогою інтеграції із зовнішнім сервером, що здійснює керування доступом. Робота в цьому режимі потребує реєстраційних даних, таких як ім'я та пароль користувача, сертифікат безпеки чи одноразовий пароль, а автентифікація виконується між клієнтом і центральним сервером автентифікації [5].

Також, окремо варто згадати протокол WPS (Wi-Fi Protected Setup), що використовується для напівавтоматичного налаштування бездротової мережі для користувачів, які мають складнощі з самостійним налаштуванням точки доступу. При першому підключені користувачу буде запропоновано ввести 8 цифр з етикетки точки доступу; за умови правильного набору цього паролю, користувач створює SSID мережі, обирає ключ, протокол безпеки (WPA чи WPA2) та необхідний тип шифрування (TKIP чи AES) у діалоговому вікні операційної системи. При наступних підключеннях за допомогою WPS користувачу буде запропоновано або ввести пароль з етикетки пристрою, або натиснути на відповідну клавішу на точці доступу, після чого клієнт підключиться до точки доступу.

ВРАЗЛИВОСТІ ПРОТОКОЛІВ БЕЗПЕКИ WI-FI МЕРЕЖ

Варто розуміти, що до мережі з відкритою автентифікацією може підключитись будь-хто в зоні покриття, адже точка доступу не обов'язково має налаштований MAC-фільтр. Та навіть у разі налаштованого MAC-фільтру ніщо не заважає підібрати MAC-адресу авторизованого клієнта.

Використання режиму прихованого ідентифікатора мережі дозволяє приховати SSID мережі в списку доступних мереж, а підключення до неї стає можливим за умови, що клієнт знає її ідентифікатор та заздалегідь створив профіль підключення. У разі використання режиму приховання SSID точка доступу, так само, як і в звичайному режимі, надсилає службові кадри-маячки (beacon frames) з інформацією для підключення, але залишає пустим поле з SSID. Але це не захистить від можливості дізнатися SSID мережі за допомогою утиліт сканування ефіру, бо всі клієнти в мережі, що підключені до дочки доступу, знають SSID цієї мережі та при підключені надсилають кадри типу Probe Request, вказуючи ідентифікатор мережі з профілю підключення. Це дає хибні сподівання на захист мережі від зловмисника.

Через відсутність шифрування в таких мережах весь трафік може бути проаналізовано зловмисником на наявність конфіденційних даних. При користуванні такими мережами слід використовувати допоміжні технології, такі як, наприклад, HTTPS та VPN, для забезпечення певного рівня захищеності.

Протокол WEP фактично передає кілька байт свого тимчасового ключа разом з кожним пакетом даних. Відповідно, не залежно від складності паролю, проводячи перехоплення пакетів у бездротовій мережі з WEP-шифруванням, можна отримати ключ від цієї мережі. Так, наприклад, кількість пакетів, які треба перехопити для успішного злому мережі з WEP-ключем довжиною 64 біти, – близько півмільйона пакетів, а в багатьох випадках і менше, для злому мережі з ключем довжиною 128 біт вже буде потрібно близько двох мільйонів пакетів. Швидкість зламу прямо пропорційна інтенсивності трафіку між клієнтом та точкою доступу [4].

Незважаючи на застарілість та відносно легкі способи зламу, WEP шифрування й досі використовується при побудові розподілених бездротових мереж WDS (Wireless Distribution System), що дозволяють використовувати другу точку доступу як бездротовий міст для поєднання двох дротових мереж або як повторювач для розширення зони покриття першої точки доступу.

Протоколи WPA та WPA2, на відміну від WEP, шифрують дані кожного клієнта окремо за допомогою тимчасового PTK-ключа, що генерується після підключення клієнта до точки доступу. Для отримання PTK-ключа необхідно знати п'ять параметрів мережі, які можна вільно перехопити при прослуховуванні пакетів мережі, а головною перепоною на шляху зловмисника стає отримання Pre-Shared Key за допомогою перебору всіх можливих комбінацій паролю чи з використанням словника.

Для спроби підбору паролю зловмиснику потрібно перехопити «рукостискання» (handshake) між клієнтом і точкою доступу. Швидкість підбору залежить від швидкодії комп'ютера зловмисника та ємності словника паролів [5].

Протокол WPS дозволяє клієнту підключитись до точки доступу за допомогою PIN-коду, що складається лише з восьми цифр, остання з яких є контрольною сумою. Через реалізацію у алгоритмі двоетапної перевірки PIN-коду спочатку перевіряються перші чотири цифри; якщо вони підібрані невірно, точка доступу відправить пакет M4, якщо ж перші чотири цифри підібрані вірно, а цифри на позиціях 5-7 – ні, то точка доступу відправить пакет M6. Для отримання доступу до мережі потрібно перебрати перші чотири цифри, що дорівнює 10000 комбінацій та цифри на 5-7 позиціях, що дорівнює 1000 комбінаціям. Отже для підбору PIN-коду достатньо перебрати 11000 комбінацій.

ВИСНОВОК

Розглянуті методи захисту та вразливості протоколів бездротових Wi-Fi мереж наочно демонструють їх вразливість.

Такі заходи, як MAC-фільтрація і приховання ідентифікатора мережі, не є перепоною на шляху зловмисника, тому їх доцільно використовувати лише у комплексі з іншими заходами.

Протоколи WEP і WPS, маючи відповідні програмні засоби, можна зламати за короткий проміжок часу, тому за можливістю потрібно відмовитись від їх використання.

Успіх атаки на WPA/WPA2 у кінцевому результаті залежить від наявності паролю в словнику, оскільки повний перебір паролю довжиною від 8 до 63 символів займає значний час.

Для забезпечення безпеки бездротових мереж розроблено відносно багато методів. Так, наприклад, можна використовувати віртуальні приватні мережі VPN (Virtual Private Network) чи протокол SSL (Secure Sockets Layer).

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. White paper: Cisco VNI Forecast and Methodology, 2015-2020 [Електронний ресурс]. – Режим доступу: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html#wp9001447 (дата звернення 10.11.2016), вільний.
2. Wifi Network Security Statistics/Graph [Електронний ресурс]. – Режим доступу: http://graphs.net/wifi-stats.html (дата звернення 10.11.2016), вільний.
3. Владимир Антонович Ткаченко. Технологии стандарта 802.11x [Електронний ресурс]. – Режим доступу: http://www.lessons-tva.info/articles/net/003.html (дата звернення 10.11.2016), вільний;
4. Дмитрий Бугрименко. Проблемы безопасности в беспроводных ЛВС IEEE 802.11 и решения Cisco Wireless Security Suite [Електронний ресурс]. – Режим доступу: https://www.cisco.com/web/RU/downloads/WLANSecurity-1.2a.pdf (дата звернення 10.11.2016), вільний;
5. Василий Леонов. Как ломаются беспроводные сети [Електронний ресурс]. – Режим доступу: http://citforum.ru/nets/wireless/crack/ (дата звернення 10.11.2016), вільний;