УДК 004.056.55

Л.А. Шувалова

Черкаський державний технологічний університет, Черкаси

МЕТОДИ ЗАХИСТУ ДАНИХ У WI-FI МЕРЕЖАХ

Задача защиты беспроводных сетей является сейчас, как никогда актуальной. Поскольку среда передачи данных в беспроводных сетях открытая (для получения доступа к сети необходимо иметь только клиентский адаптер), очень важно организовать защиту такой сети от несанкционированного доступа. В статье рассмотрены методы защиты информации, используемые в беспроводных сетях, их преимущества и недостатки.

Ключові слова: *бездротова мережа, середовище передачі даних, технологія, авторизація, ідентифікатор, точка доступу.*

Вступ

Постановка проблеми. Поширення бездротових мереж у світі почалося з впровадження технології 802.11, яка в свою чергу трансформувалася у 802.11b, далі у 802.11g(a), і, нарешті, у 802.11n, яка є останньою розробкою. Оскільки середовище передачі у бездротових мережах відкрите (для отримання доступу до мережі потрібно мати лише клієнтський адаптер), дуже важливо організувати захист такої мережі від несанкціонованого доступу.

Постановка задачі. Головна мета статті – дослідження методів захисту бездротових мереж від несанкціонованого доступу, проаналізувати їхні переваги та недоліки.

Дослідження технологій

Середовище передачі у мереж стандарту 802.11 бездротове, але воно має межі для приймання клієнтським обладнанням, що зумовлено згасанням сигналу у вільному просторі [2]. Отже, очевидно, що для успішного доступу до мережі зловмисник повинен бути в радіусі поширення сигналу цієї мережі. Є декілька способів протистояти поширенню радіосигналу. Можна використати так звану "зону, що охороняється", тобто весь радіус покриття точки доступу охороняється, наприклад, територія огороджена парканом. Такий спосіб дає змогу запобігти випадковому виявленню мережі, але він не допоможе при цілеспрямованому скануванні території направленою антеною. Якщо сигнал не повинен виходити за межі певної будівлі, можна використати екранування стін металевою сіткою, що значно послабить рівень сигналу. Найпростішим методом для звичайного користувача точки доступу, який використовує ресурси бездротової мережі у власних цілях, є звичайне зменшення рівня вихідного сигналу [3]. Таку функцію на даний момент підтримують більшість точок доступу. При цьому користувач може впевнено користуватися ресурсами мережі лише у радіусі, який є меншим при меншому рівні сигналу. Ще одним способом називають приховування імені точки доступу (ESSID cloaking), але ця методика не допомагає у реальних умовах, оскільки точку можна визначити за активним спілкуванням з клієнтами. Сучасне програмне забезпечення ідентифікує таку точку доступу у режимі за замовчуванням.

Одним із способів авторизації користувачів у бездротовій мережі є фільтрація по MAC ідентифікатору [1]. Кожний бездротовий адаптер має свій унікальний фізичний ідентифікатор, який встановлюється на заводі. При первинному підключенні до точки доступу адміністратор повинен додати такий ідентифікатор клієнта у спеціальний список точки доступу. Такий список зберігається на точці доступу. При підключенні будь-якого клієнта точка доступу перевіряє його фізичний ідентифікатор шляхом пошуку його у спеціальному списку ідентифікаторів. Якщо ідентифікатор знайдено, то точка доступу починає обслуговувати клієнта, якщо ж ні – просто ігнорує його. Недоліком такого способу захисту є можливість зміни фізичного ідентифікатора на сучасних клієнтських адаптерах. Дізнатися фізичний ідентифікатор іншого користувача також не є проблемою – для цього існує спеціальне програмне забезпечення, яке дозволяє прослуховувати ефір та ідентифікувати окремих користувачів.

Важливо відзначити, що вказані методи не забезпечують конфіденційність даних, що передаються в мережі, вони просто обмежують доступ до мережі. Тобто, навіть якщо всі ці засоби включені на точці доступу, зловмисник зможе, включивши свій бездротової адаптер в режимі «monitor mode», слухати ефір і виловлювати всю передану інформацію.

Очевидно, що для захисту мережі потрібно активізувати механізм захисту, що вбудований у обладнання, яке надає сервіс бездротових мереж. На даний момент налаштування захисту обладнання бездротових мереж вимагає введення паролю. В деяких випадках (наприклад, недосвідчений користувач) пароль може бути найбільш вразливим місцем всієї системи. Все обладнання завжди має певні налаштування за замовчуванням. Інформація про ці налаштування повинна знаходитись у інструкції до цього обладнання. Іншими словами, така інформація є загальновідомою. Якщо користувач не змінить налаштування пароля для точки доступу, зловмисник зможе легко підібрати пароль і отримати доступ до всієї мережі. Також важливим фактором є складність паролю. Загальновідомо, що чим довший і складніший пароль, тим вищу він має криптостійкість, і для його підбору потрібно більше часу. Тому рекомендується використовувати випадково згенеровані паролі достатньої довжини. Рекомендується також змінювати пароль через певні проміжки часу.

Існує декілька алгоритмів захисту для бездротових мереж стандарту 802.11. Це WEP, WPA і WPA2. Кожен з них має декілька режимів роботи [2].

Технологія WEP (Wired Equivalent Privacy) була затверджена у 1997 році, при цьому у 2000 році було написано статтю про недоліки даної технології. У WEP використовується алгоритм RC4 на статичному ключі. Для підвищення захисту частина ключа є статичною, а інша частина – динамічною (вектор ініціалізації), що змінюється в процесі роботи мережі. Основним недоліком WEP є те, що вектор ініціалізації повторюється через деякі проміжки часу. Для того, щоб зламати це шифрування необхідно лише зібрати ці повтори і за секунди отримати іншу частину ключа. Весь процес взлому складає 5-10 хвилин. Саме через це не рекомендується застосовувати цей алгоритм захисту за будь-яких умов.

Технологія WPA (Wi-Fi Protected Access) була впроваджена замість застарілого протоколу WEP. WPA була перехідною технологією між WEP та відносно новим стандартом безпеки 802.11i. За шифрування даних в WPA відповідає протокол TKIP, який, хоча і використовує той же алгоритм шифрування – RC4 – що й у WEP, але на відміну від останнього, використовує динамічні ключі (тобто ключі часто змінюються). Він застосовує більш довгий вектор ініціалізації і використовує криптографічну контрольну суму (MIC) для підтвердження цілісності пакетів (остання є функцією від адреси джерела і призначення, а також поля даних). Можна виділити два основних режими роботи технології WPA: WPA-PSK і WPA-Enterprise [2]. Будь-яке сучасне бездротове обладнання стандарту 802.11 підтримує обидва ці режими. При використанні режиму WPA-PSK (так званий персональний режим) на точці доступу прописується ключ доступу, ввівши який користувач може почати користуватися ресурсами мережі. Такий спосіб захисту досить стійкий, але не досить зручний для адміністрування, оскільки для кожного користувача мережі потрібно ввести пароль точки доступу для його успішного підключення. При досить малих розмірах мережі це припустимо, але з ростом кількості клієнтів це перетворюється на досить важку задачу. Також, якщо є потреба відключити користувача від мережі, потрібно змінювати ключ точки доступу, причому після таких дій потрібно переналаштовувати всіх користувачів мережі.

При використанні технології WPA у режимі WPA-Enterprise для аутентифікації користувачів використовується зовнішній сервер (відносно точки доступу), наприклад RADIUS-сервер. У такому режимі користувачу необхідно ввести пару логін-пароль, по яким і відбувається підключення користувача до мережі. При цьому пара логін-пароль унікальна для кожного користувача.

На зміну протоколу шифрування TKIP, у якому теж знайдені недоліки, прийшов покращений алгоритм шифрування AES (Advanced Encryption Standard). AES також відомий під назвою Rijndael – симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт). Сучасне обладнання надає вільний вибір між цими двома

протоколами.

Рекомендується вибирати AES як більш надійний метод шифрування.

Технологія WPA2. На зміну протоколу WPA прийшов протокол WPA2, який входить до стандарту безпеки бездротових мереж 802.11i. Протоколи WPA2 працюють в двох режимах аутентифікації: персональному (Personal) та корпоративному (Enterprise). У режимі WPA2-Personal з введеної відкритим текстом парольної фрази генерується 256-розрядний ключ PSK (PreShared Key). Ключ спільно з ідентифікатором SSID (Service Set Identifier) використовуються для генерації тимчасових сеансових ключів PTK (Pairwise Transient Key), для взаємодії бездротових пристроїв. Як і протоколу WPA-PSK, протоколу WPA2-Personal притаманне певні проблеми, пов'язані з необхідністю розподілу та підтримки ключів на бездротових пристроях мережі, що робить його більш корисним для застосування в невеликих мережах з десятка пристроїв, у той час як для корпоративних мереж оптимальний WPA2 -Enterprise.

Технологія VPN. З додаткових методів захисту бездротових мереж можна виділити технологію VPN (Virtual Private Network). Дана технологія дозволяє створити у межах будь-якої мережі або декількох мереж віртуальну персональну мережу, яка надає широкі можливості щодо забезпечення конфіденційності клієнтів. Принцип дії VPN – створення так званих безпечних «тунелів» від користувача до вузла доступу або сервера. Для шифрування трафіку в VPN найчастіше застосовується протокол IPSec (близько 70% випадків), рідше – PPTP або L2TP. При цьому можуть використовуватися такі алгоритми, як DES, Triple DES, AES і MD5. VPN підтримується на багатьох платформах (Windows, Linux, Solaris) як програмними, так і апаратними засобами. Варто відзначити високу надійність технології. Зазвичай VPN рекомендується застосовувати у великих корпоративних мережах, для домашнього користувача встановлення та налаштування може здатися занадто громіздкою і трудомісткою. Технологію VPN можна використовувати як додатковий засіб захисту мережі у поєднанні з будь-якою технологією захисту бездротових мереж.

Висновки

Отже, можна зробити висновок, що WEP є далеко не ідеальним рішенням для забезпечення безпеки. WPA забезпечує набагато більш високий рівень безпеки, ніж WEP, але і WPA не може дати надійної захищеності мережі. Самим надійним та безпечним рішенням є WPA2. Використання цього протоколу у поєднання з VPN – оптимальне рішення для корпоративних користувачів.

Список літератури

1. Широкополосные беспроводные сети передачи информации / В.М. Вишневский, А.И. Ляхов, С.Л. Портной, И.Л. Шахнович. – М.: Техносфера, 2005. – 320 с.

2. Росс Д. Wi-Fi. Беспроводная сеть / Д.Росс. – М.: НТ Пресс, 2007. – 420 с.

3. Stewart S. Miller. Wi-fi Security / Stewart S. Miller. – 2003. – 460 p.

4. 802,11i-2004 – IEEE Standard for Local and Metropolitan Area Networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

Надійшла до редколегії 3.10.2011

Рецензент: д-р техн. наук проф. В.М. Рудницький, Черкаський державний технологічний університет, Черкаси.

МЕТОДЫ ЗАЩИТЫ ДАННЫХ В WI-FI СЕТЯХ

Л.А. Шувалова

Задача защиты беспроводных сетей является сейчас как никогда актуальной. Поскольку среда передачи данных в беспроводных сетях открытая (для получения доступа к сети необходимо иметь только клиентский адаптер), очень важно организовать защиту такой сети от несанкционированного доступа. В статье рассмотрены методы защиты информации, используемые в беспроводных сетях, их преимущества и недостатки.

Ключевые слова: *беспроводная сеть, среда передачи данных, технология, авторизация, идентификатор, точка доступа.*

METHODS OF DATA PROTECTING IN WI-FI NETWORKS

L.A. Shuvalova

The task of protecting wireless networks is now more relevant than ever. As the environment of data transmission in wireless networks is opened (it's necessary to have only the client adapter for getting access to the network), it's important to organize the protection of the network from unauthorized access. The article deals with methods of information security used in wireless networks, their advantages and disadvantages.

Keywords: *wireless network, environment of data transmission, technology, authorization, identifier, the access point.*