УДК 004

Л.А. Шувалова, А.О. Лавданський, В.В. Гурін

Черкаський державний технологічний університет, Черкаси

ВИКОРИСТАННЯ ПРОТОКОЛУ WPA2 ДЛЯ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

Розглянуто функціональні та деякі технічні аспекти роботи захисного протоколу Wi-Fi Protected Access 2 (WPA2) на основі стандарту IEEE 802.11i. Наведено переваги запровадження систем на основі даного механізму в порівнянні із застосуванням протоколів WEP та WPA для забезпечення практичного захисту бездротових локальних обчислювальних мереж підприємств та організацій, а також описана існуюча проблема зворотної сумісності зі старими пристроями, що апаратно не підтримують ключові технології зазначені в специфікації IEEE 802.11i, зокрема Advanced Encryption Standard (AES) в якості основного методу шифрування.

Ключові слова: *бездротова мережа, дані, протокол захисту, метод шифрування, ключ, аутентифікація.*

Вступ

Постановка проблеми. В наші часи бездротові локальні обчислювальні мережі (БЛОМ) набувають надзвичайної популярності в усіх сферах життя суспільства. З поширеністю доступності бездротових локальних мереж зростає необхідність забезпечення необхідного рівня їх захисту. Це пояснює постійне вдосконалення протоколів захисту, що затверджуються організаціями в якості стандартів для обов'язкового використання в апаратних засобах та програмному забезпеченні при побудові бездротових локальних мереж. Зокрема для популярного стандарту бездротового зв'язку передачі даних, що об'єднує декілька протоколів та ґрунтується на сімействі стандартів IEEE 802.11, більш відомого під торговою маркою Wi-Fi, існує декілька протоколів безпеки, затверджених у різні роки. В даній статті подано опис функціонування популярного сучасного захисного протоколу Wi-Fi Protected Access 2 (WPA2), описаного стандартом IEEE 802.11i.

Актуальність. Специфікація WPA2 організації Wi-Fi Alliance є значним удосконаленням механізму безпеки WEP (Wired Equivalent Privacy) вихідного стандарту 802.11. Використання протоколу WEP довело, що він виявився вразливим для атак і був неохоче прийнятий виробниками, що не забезпечило йому широкого застосування при побудові корпоративних мереж. Слабкі місця WEP стимулювали розробку стандарту 802.11i, який був затверджений і опублікований в 2004 р. В рамках проекту стандарту 802.11i організація Wi-Fi Alliance розробила протокол Wi-Fi Protected Access (WPA), а згодом – Wi-Fi Protected Access 2 (WPA2), що забезпечив більш високий рівень безпеки, ніж перша версія WPA. Невисокий рівень безпеки, довгий час залишався одним з головних недоліків мереж стандарту Wi-Fi. Перші спроби використання БЛОМ забезпечували безпеку даних за допомогою використання технології VPN лише на рівні 3, що крім додаткових витрат на інкапсулювання, проблем з роумінгом, гарантованою якістю обслуговування, підтримкою клієнтів та масштабованістю зберігало вразливість мережі IP для атак. Реалізований на рівні 2 протокол WPA2 захищає бездротову мережу більш надійно, забезпечуючи конфіденційність і цілісність даних. Проте лише він один не здатний забезпечити належну безпеку корпоративної мережі. Управління ж доступом з цього протоколу в поєднанні з заснованим на портах протоколом аутентифікації IEEE 802.1X дозволяє виключити виникнення більшості проблем безпеки. Застосування вищезазначеної пари протоколів не захищає мережу від "нелегальних" пристроїв, атак типу "відмова в обслуговуванні" (denial-of-service) або будь-якого іншого втручання ззовні, але забезпечує певний рівень безпеки бездротових комунікацій. Це пояснює прийняття у 2006 році рішення про обов'язковість підтримки протоколу WPA2 усіма пристроями, що є сертифікованими для використання в бездротових мережах стандарту Wi-Fi [2].

Основні відомості про WPA2 та його переваги перед WPA

Перша версія WPA використовувала метод шифрування RC4 та протокол TKIP (Temporal Key Integrity Protocol). Це мало можливість реалізовуватись програмно шляхом оновлення драйвера або вбудованого програмного забезпечення. Постійна ротація ключів та наявність лічильника пакетів запобігали атакам з відтворенням пакетів (packet replay) або їх повторним введенням (packet re-injection). Протокол WPA забезпечував контроль цілісності даних, використовуючи метод контрольної суми MIC (Message Integrity Code), іноді званий "Michael". Даний метод можна атакувати "грубою силою" (brute-force attack), але при цьому передача мережевого трафіку на хвилину автоматично припиняється і, якщо заснована на WPA точка доступу фіксує протягом 60 секунд більше однієї помилки MIC протоколу TKIP, сеансові ключі встановлюються заново, знижуючи, таким чином, ризик атак такого типу до мінімуму.

Протокол WPA2 запровадив новий метод шифрування, що отримав назву CCMP (Counter-Mode with CBC-MAC Protocol), заснований на більш по-

тужному, ніж RC4, алгоритмі шифрування AES (Advanced Encryption Standard).

WPA2, аналогічно до першого WPA, працює в двох режимах аутентифікації: персональному (Personal) і корпоративному (Enterprise). У режимі WPA2-Personal із введеної текстом парольної фрази генерується 256-розрядний ключ, що називають попередньо розподіленим ключем (PreShared Key, PSK). Ключ PSK, ідентифікатор SSID (Service Set Identifier) і його довжина разом утворюють математичний базис для формування головного парного ключа (Pairwise Master Key, PMK), який використовується для ініціалізації чотиристороннього квитування зв'язку та генерації тимчасового парного або сеансового ключа (Pairwise Transient Key, PTK), для взаємодії бездротового пристрою користувача з точкою доступу. Протоколу WPA2-Personal, як і протоколу WEP, властива наявність проблем розподілу та підтримки ключів, що робить його більш ефективним при застосуванні в домашніх умовах та у невеликих офісах, ніж на підприємствах з великою БЛОМ.

При використанні протоколу WPA2-Enterprise можна успішно вирішити проблеми, що стосуються розподілу статичних ключів та управління ними, а його інтеграція з більшістю корпоративних сервісів аутентифікації забезпечує контроль доступу на основі облікових записів. Для роботи в цьому режимі потрібні такі реєстраційні дані, як ім'я та пароль користувача, сертифікат безпеки або одноразовий пароль. Базою для режиму WPA2-Enterprise служить стандарт 802.1X, що підтримує засновану на контролі портів аутентифікацію, придатну як для дротових комутаторів, так і для бездротових точок доступу [2].

У WPA2 є три типи ключів PTK:

1. Ключ підтвердження ключа (Key Confirmation Key, KCK)., що застосовується для перевірки цілісності кадру (використовується в контрольній сумі MIC).

2. Ключ шифрування ключа (Key Encryption Key, KEK), який використовується для шифрування групового тимчасового ключа (Group Transient Key, GTK).

3. Тимчасові ключі (Temporal Keys, TK) – для шифрування трафіку [3].

Шифрування при застосуванні WPA2

В основі стандарту WPA2 лежить метод шифрування AES, що прийшов на зміну стандартам DES і 3DES в якості галузевого стандарту. Вимагаючи великого обсягу обчислень, стандарт AES потребує апаратної підтримки, яка не завжди є в старому обладнанні БЛОМ.

WPA2 використовує протокол CBC-MAC (Cipher Block Chaining Message Authentication Code) для аутентифікації і забезпечення цілісності даних, а для шифрування даних і контрольної суми MIC – режим лічильника (Counter Mode, CTR). WPA2 забезпечує цілісність даних для незмінних полів заголовку 802.11 за допомогою контрольної суми в якості коду цілісності повідомлення (MIC). Це відрізняє стандарт від WEP і WPA. Таким чином підтримується можливість розшифрування пакетів або компрометації криптографічної інформації за допомогою атак типу packet replay [2].

Використовується так званий вектор ініціалізації (Initialization Vector, IV), що складається з 128 розрядів і впливає на значення MIC. Для отримання даного вектору застосовується метод AES і тимчасовий ключ. На виході отримується 128-розрядний результат, що разом з наступними даними об'ємом 128 біт зазнають опрацювання операцією "виключне АБО". Її результат зашифровується за допомогою AES і тимчасового ключа TK. Далі над отриманим результатом і наступними 128 біт даних знову виконується операція "виключне АБО". Повторення процедури відбувається до того часу, доки не буде вичерпане усе корисне навантаження. Перші 64 розряди результату отриманого на останньому кроці використовуються для обчислення значення MIC [3].

При шифруванні даних і MIC використовується алгоритм заснований на режимі лічильника (CTR). Виконання цього алгоритму також починається з завантаження лічильника довжиною у 128 розрядів, де у полі лічильника замість значення, що відповідає довжині даних, береться значення лічильника, встановлене в одиницю. Тому для шифрування кожного окремого пакету фактично використовується свій лічильник. З застосуванням AES та TK шифруються перші 128 біт даних, над результатом цього шифрування виконується операція "виключне АБО". Перші 128 біт даних дають перший 128-розрядний зашифрований блок. Попередньо завантажене значення лічильника інкрементується і шифрується за допомогою AES і ключа шифрування даних. Потім над результатом цього шифрування і наступними 128 біт даних знову виконується операція "виключне АБО". Процедура повторюється до тих пір, доки усі 128-розрядні блоки даних не будуть зашифровані. Після цього в якості остаточного значення у полі лічильника записується нуль, лічильник шифрується з використанням алгоритму AES, а потім над результатом шифрування і MIC виконується операція "виключне АБО". Результат останньої операції додається до зашифрованого кадру [2].

Підрахувавши MIC, виконується його шифрування разом з даними. До отриманого результату додається заголовок стандарту 802.11 і поле номеру пакету CCMP. Також додається закінчення стандарту 802.11, після чого пакет є готовим до відправлення [3].

Розшифрування даних виконується в зворотному порядку. Для витягання лічильника застосовується той самий алгоритм, що і для його шифрування. При дешифруванні лічильника застосовуються алгоритм розшифровки заснований на режимі лічильника і ключ TK. На виході отримуються контрольна сума MIC та розшифровані дані. За допомогою алгоритму CBC-MAC, здійснюється перераху-

нок MIC для отриманих розшифрованих даних. При збіганні значень розшифровані дані вважаються достовірними, інакше пакет відкидається [2].

Проблеми зворотної сумісності

Хоча підтримка WPA2 і є загальнообов'язковою у сертифікаованих пристроях Wi-Fi, можлива проблема зворотної сумісності зі старими пристроями в зв'язку з потребами у апаратній підтримці алгоритму шифрування AES, що використовується в протоколі WPA2. Стандарт 802.11i використовує концепцію підвищеної безпеки (Robust Security Network, RSN), яка передбачає забезпечення бездротовими пристроями додаткових можливостей, що вимагають змін в апаратній частині та програмному забезпеченні. Отже мережа, повністю відповідна RSN, є несумісною з існуючим обладнанням WEP. Була визначена підтримка як обладнання RSN, так і WEP у перехідний період, однак зараз пристрої WEP вже поступаються місцем пристроям з повноцінною підтримкою виключно RSN. WPA2 в залежності від різних реалізацій може застосовувати TKIP, але за замовчуванням RSN використовує AES і CCMP [1].

Практичне застосування WPA2

Одним з найбільших недоліків використання протоколу WEP було управління таємними ключами. Багато адміністраторів великих БЛОМ вважали його вкрай незручним. В результаті цього ключі WEP не змінювалися тривалий час (або взагалі ніколи), полегшуючи завдання зловмисникам. RSN визначає ієрархію ключів з обмеженим терміном дії, подібну до TKIP. У AES / CCMP, щоб вмістити всі ключі, потрібно 512 біт – менше, ніж у TKIP. В обох випадках майстер-ключі використовуються не прямо, а для виводу інших ключів. Адміністратор повинен забезпечити єдиний майстер-ключ. Повідомлення складаються з 128-бітного блоку даних, зашифрованого таємним ключем такої ж довжини (128 біт). Хоча процес шифрування складний, адміністратор все ж не повинен вникати в нюанси обчислень. При цьому, кінцевим результатом є шифр, який набагато складніше, ніж навіть WPA. Продуктивність каналу зв'язку, як свідчать результати тестування обладнання різних виробників, падає на 5-20% при використанні як WEP, так і WPA. Однак дослідження обладнання, в якому застосовувалося шифрування AES замість TKIP, не виявили помітного падіння швидкості. Це надає гарантії того, що WPA2 надає надійній захист каналу без втрат в продуктивності в порівнянні з використанням першої версії протоколу WPA [1].

Висновки

Стандарт IEEE 802.11i (WPA2) розроблений на базі перевірених технологій, однак деякі механізми безпеки були спроектовані з нуля в тісній співпраці з кращими фахівцями з криптографії і вважаються одним з найефективніших рішень проблем захисту бездротових мереж. Хоча жодна система безпеки повністю не застрахована від можливості взлому, WPA2 – це рішення, на яке можна покладатися, воно уникло недоліків попередніх протоколів і вважається одним з найбільш стійких, розширюваних і безпечних рішень, що призначене в першу чергу для великих підприємств, де управління ключами і адміністрування створювали найбільше проблем.

Список літератури

1. Пролетарский А.В. Беспроводные сети Wi-Fi / А.В. Пролетарский, И.В. Баскаков, Д.Н. Чирков. – М.: БИНОМ. Лаборатория знаний, 2007. – 178 с.

2. Frank Bulk The ABCs Of WPA2 Wi-Fi Security – Network Computing, 2006, February 2. – P. 65-69.

3. 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) specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements. – IEEE 802.11i–2004.

Надійшла до редколегії 23.01 2012

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

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА WPA2 ДЛЯ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ

Л.А. Шувалова, А.А. Лавданский, В.В. Гурин

Рассмотрены функциональные и некоторые технические аспекты работы защитного протокола Wi-Fi Protected Access 2 (WPA2) на основе стандарта IEEE 802.11i. Приведены преимущества внедрения систем на основе данного механизма по сравнению с применением протоколов WEP и WPA для обеспечения практической защиты беспроводных локальных вычислительных сетей предприятий и организаций, а также описана существующая проблема обратной совместимости со старыми устройствами, которые аппаратно не поддерживают ключевые технологии, указанные в спецификации IEEE 802.11i, в частности, Advanced Encryption Standard (AES) в качестве основного метода шифрования.

Ключевые слова: *беспроводная сеть, данные, протокол защиты, метод шифрования, ключ, аутентификация.*

THE USAGE OF WPA2 PROTOCOL FOR WIRELESS NETWORKS SECURITY

L.A. Shuvalova, A.O. Lavdanskyi, V.V. Hurin

The functional and some technical aspects of Wi-Fi Protected Access 2 (WPA2) security protocol that is based on the IEEE 802.11i standard are reviewed. The advantages of introducing systems based on this technology in comparison with the usage of WEP and WPA for the practical protection of wireless local area networks of companies and organizations are presented. The current problem of backward compatibility with older devices with hardware that does not support key technologies specified in the IEEE 802.11i specification, in particular has no support for Advanced Encryption Standard (AES) as the primary encryption method is described.

Keywords: *wireless network, data, security protocol, encryption method, key, authentication.*