УДК 004.716

Ю.Р. Гарасим, П.А. Пуля

Національний університет «Львівська політехніка», Львів

ДОСЛІДЖЕННЯ ТА АНАЛІЗ ЗАХИЩЕНОСТІ БЕЗПРОВІДНИХ ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖ ЗВ'ЯЗКУ. ВДОСКОНАЛЕННЯ ПРОТОКОЛУ WEP

Робота присвячена дослідженню та аналізу захищеності безпровідних корпоративних мереж зв'язку. Розглянуто принцип функціонування та структуру основних видів безпровідних мереж. Проведено аналіз існуючих протоколів, визначено їхні недоліки та переваги. Запропоновано модифікацію протоколу WEP, яка полягає в постійному оновленні спільного таємного ключа між точкою доступу та безпровідним терміналом. Таке рішення ефективно працює на існуючому обладнанні та надає значні переваги в порівнянні із стандартним.

Ключові слова: *захищена безпровідна мережа зв'язку, протоколи шифрування даних, пакети даних, автентифікація користувачів.*

Вступ

Спроби проникнення в закриту корпоративну мережу можуть відбуватися з кількох причин. По-перше, цілеспрямований злам з метою викрадення конфіденційної інформації. Найчастіше саме через це необхідно подбати про безпеку безпровідного сегменту мережі. По-друге, набагато більшою популярністю користуються спроби проникнути в мережу, щоб скористатися чужим інтернет-з'єднанням. Якщо локальна мережа організації використовується як плацдарм для розсилки спаму або наступної масштабної інтернет-атаки – наслідки можуть бути вкрай неприємними як зі сторони інтернет-провайдера, так і з сторони контролюючих органів.

Основний матеріал

Безпека аналогічна захисту провідних мереж (протокол WEP). Всі сучасні безпровідні пристрої підтримують протокол безпеки WEP, що був закладений в специфікацію безпровідних мереж стандарту IEEE 802.11 [1].

Спочатку передаються в пакеті дані, які перевіряються на цілісність (алгоритм CRC-32), після чого контрольна сума (Integrity Check Value, ICV) додається в службове поле заголовка пакета. Далі генерується 24-бітний вектор ініціалізації (IV), до якого додається статичний (40-або 104-бітовий) секретний ключ. Отриманий таким чином 64- або 128-бітовий ключ є вихідним ключем для генерування псевдовипадкового числа, що використовується для шифрування даних. Далі дані шифруються за допомогою логічної операції XOR з псевдовипадковою ключовою послідовністю, а ектор ініціалізації додається у службове поле кадру (рис. 1).

На приймальній стороні дані можуть бути розшифровані, оскільки разом з ними передається інформація про вектор ініціалізації, а статична частина ключа зберігається у користувача, якому передаються дані. Протокол WEP передбачає два способи автентифікації користувачів: Open System (відкрита) і Shared Key (загальна) [2]. Однак навіть у разі відкритої системи допускається застосування WEP-шифрування даних.

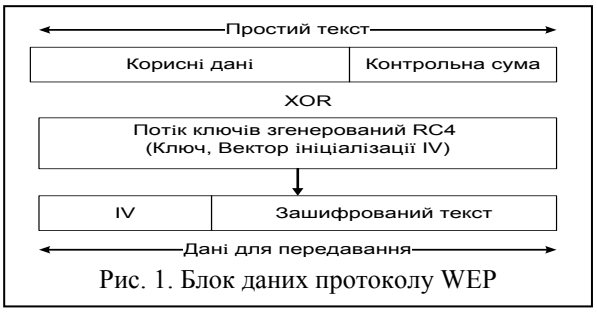

Рис. 1. Блок даних протоколу WEP

Механізм безпеки в протоколі WPA. WPA (Wi-Fi Protected Access)-являє собою новітню програму сертифікації пристроїв безпровідного зв'язку. Перевагами WPA є посилена безпека даних та посилений контроль доступу до безпровідних мереж. У WPA забезпечена підтримка стандартів 802.1X, а також протоколу EAP (Extensible Authentication Protocol). WPA підтримується шифрування згідно зі стандартом AES (Advanced Encryption Standard), який має ряд переваг над використовуваним в WEP RC4, наприклад, стійкіший криптоалгоритм.

Великою перевагою при впровадженні WPA є можливість роботи технології на існуючому апаратному забезпеченні Wi-Fi [3].

Автентифікація користувачів. Wi-Fi Alliance впроваджує таку формулу для визначення структури WPA:

$$WPA = 802.1X + EAP + TKIP + MIC.$$

Неодмінною умовою автентифікації є пред'явлення користувачем свідоцтва, що підтверджує його право на доступ в мережу. Без автентифікації робота в мережі для користувача буде заборонена [1].

WPA має спрощений режим. Цей режим отримав назву Pre-Shared Key (WPA-PSK). При застосуванні режиму PSK необхідно ввести один пароль для кожного окремого вузла безпровідної мережі. Якщо паролі співпадають з записами в базі даних, користувач отримає дозвіл на доступ в мережу.

Часовий протокол цілісності ключа (протокол TKIP). TKIP (Temporal Key Integrity Protocol) [4] протокол динамічних ключів мережі, які змінюються досить часто. При цьому кожному пристрою також привласнюється ключ, що теж змінюється. TKIP відповідає за збільшення розміру ключа з 40 до 128 біт, а також за заміну одного статичного ключа WEP ключами, які автоматично генеруються і розсилаються сервером автентифікації. Крім того в TKIP використовується спеціальна ієрархія ключів та методологія управління ключами, що унеможливлює зайву передбачуваність, яка використовувалася для несанкціонованого зняття (компрометації) захисту WEP ключів. Ієрархія ключів TKIP замінює один ключ WEP (статичний) на 500 мільярдів можливих ключів, які будуть використані для шифрування даного пакету даних.802.11i. [5]

Перевірка цілісності повідомлення (протокол MIC). Протокол перевірки цілісності пакетів, що захищає їх від перехоплення також бере участь у захисті інформації при зміні напрямку пакетів, зміст яких може бути змінено, а модифікований пакет знову передається через мережу.

Протокол WPA2. WPA2-вдосконалення протоколу WPA, в якому використовується більш стійкий AES алгоритм шифрування. Аналогічно з WPA, WPA2 також поділяється на два типи: WPA 2-PSK і WPA 2-802.1x [4].

Віртуальні приватні мережі – VPN. Протокол, який використовують в будь-якому типі мереж для безпечного підключення клієнтів до мережі через загальнодоступні Інтернет-канали. Для шифрування трафіку в VPN найчастіше використовується протокол IPSec, створюються безпечні «тунелі» [6] від користувача до вузла доступу або сервера. Він забезпечує практично стовідсоткову безпеку каналу зв'язку.

Переваги Wi-Fi. Дозволяє розгорнути мережу без прокладання кабелю, може зменшити вартість розгортання і розширення мережі. Місця, де не можна прокласти кабель. Пристрої різних виробників можуть взаємодіяти на базовому рівні послуг.

Wi-Fi мережі підтримують роумінг, тому клієнтська станція може переміщуватися в просторі, переходячи від одного пункту доступу до іншого.

Wi-Fi-це набір глобальних стандартів. На відміну від стільникових телефонів, Wi-Fi обладнання може працювати в різних країнах у всьому світі.

Недоліки Wi-Fi. Частотний діапазон та експлуатаційні обмеження в різних країнах неоднакові. Досить високе в порівнянні з іншими стандартами споживання енергії. Найбільш розповсюджений стандарт шифрування WEP може бути відносно легко скомпрометований навіть при правильному налаштуванні. Незважаючи на те, що нові пристрої підтримують більш сучасний протокол WPA старіші пункти доступу не підтримують його і потребують заміни. Багато організацій використовують додаткове шифрування (наприклад VPN) для захисту від несанкціонованих вторгнень.

Модифікація протоколу WEP. Ідея модифікації полягає в постійному оновленні спільного таємного ключа між точкою доступу та безпровідним терміналом. Відомою є небезпека ризику повторення вектору ініціалізації після кожних 5000 кадрів відповідно до парадоксу «дня народження». Наприклад, існує WEP система, в якій після кожних 5000 кадрів спільний таємний ключ змінюється. Мережевий потік даних визначає кількість переданих кадрів WEP, тому ці два параметри є важливими для встановлення часу зміни спільного таємного ключа. Метою є мінімізація інформації, яку може отримати зловмисник із кадрів, що передаються та максимально зменшити час, який відведений йому для здійснення атаки. Структура модифікованого WEP кадру наведена на рис. 2.

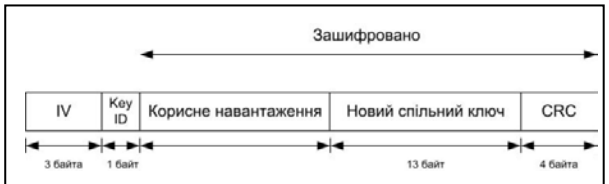

Рис. 2. Структура модифікованого WEP кадру

В звичайному WEP кадрі поле ідентифікатора ключа (Key ID) встановлює, який ключ із чотирьох можливих використовуватиметься для дешифрування поточного кадру. Значення поля Key ID може бути від 0 до 3. Коли ж поле Key ID отримає значення, що перевищує 3 необхідно вирахувати 4 від значення Key ID, отримавши при цьому коректний ключ дешифрування поточного кадру. Кожен раз, коли значення поля Key ID перевищує 3 – це говорить про те, що корисне навантаження кадру містить новий спільний таємний ключ для наступного шифрування. В певний момент часу існує 4 спільні ключі та новий спільний таємний ключ надходить в однакові інтервали часу, замінюючи старший з них. Корисне навантаження кадру постійно жертвує 104 бітами свого вмісту при передаванні нового спільного таємного ключа. В той час як приймач дешифровує кадр він отримує 104 біти з корисного навантаження кадру та використовує їх в якості спільного таємного ключа для наступного шифрування.

Відомими є два різних підходи використання ключів в протоколі WEP, існують як ключі за замовчуванням, так і таблиці ключів [7]

Стандартні ключі. Якщо система використовує стандартні ключі, тоді точка доступу буде пере-

давати новий спільний таємний ключ для наступного шифрування в корисному навантаженні кадру. У випадку використання стандартних ключів, усі безпровідні термінали використовуватимуть однаковий набір спільних ключів та виникатиме потреба частішого оновлення спільних таємних ключів. Використання таких параметрів як мережевий потік або кількість переданих кадрів для зміни спільних таємних ключів виключає можливість повторного використання вектору ініціалізації для однакових спільних ключів. Якщо режим не використовується він отримає оновлені спільні таємні ключі від точки доступу в звичайному кадрі WEP без передавання жодної іншої інформації в ньому. Поле Key ID може використовуватися для встановлення того факту, що кадр містить новий спільний таємний ключ для наступного шифрування.

Таблиці ключів. В цьому типі системи точка доступу буде передавати новий спільний таємний ключ лише окремому безпровідному терміналу. Маючи більше спільних таємних ключів, система буде оперувати спільними ключами довший час, оскільки вимагається більше часу для використання векторів ініціалізації. Постійне оновлення спільних ключів забезпечує те, що вектор ініціалізації не буде повторюватися із тим самим спільним ключем. Тому цей метод приділяє достатню увагу атакам на повторне використання вектору ініціалізації.

Висновки

Сучасний протокол WEP є вразливим до більшості атак криптоаналізу. Це є причиною не відповідного використання криптографії, а не розміру ключа.

Можливим недоліком нового методу є обчислювана надлишковість, що пов'язана із генеруванням, передаванням сеансових ключів в точці доступу. В цій статті було показано як запропонований модифікований метод протоколу WEP робить його більш захищеним та стійкішим стосовно конфіденційності повідомлень. Спільні ключі оновлюються з певною частотою, що робить більшість атак криптоаналізу неможливими або більш ресурсоємними.

В стандарті IEEE 802.11i повинен бути механізм управління ключами, що забезпечує його безпеку, але це зумовлене значним оновленням апаратного забезпечення. Запропоноване рішення є ефективною альтернативою поки використовується обладнання стандарту 802.11 та розгортаються мережі стандарту 802.11i. Таке рішення ефективно працює на існуючому обладнанні та надає значні переваги в порівнянні із стандартним протоколом WEP.

Список літератури

1. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – Видавнича група BHV, 2009. – 608 с.

2. Поллино Д.Л. Безопасность беспроводных сетей / Д.Л. Полино, М.Ю. Максим. – М.: ДМК-Пресс, 2004. – 320 с.

3. Пахомов С. Подробнее о Wi-Fi защита данных [Електронний ресурс] / С. Пахомов, М. Афанасьєв. – Режим доступу: http://www.ferra.ru/online/networks/s26260/

4. Borisov N. Intercepting mobile communications : The insecurity of 802.11 / N. Borisov, I. Goldberg, D.Wagner. – Rome, Italy, 2001. – 460 p.

5. Ertaul L. IEEE 802.11 WLAN Security / L. Ertaul, O. Catambay. – California State University, 2005. – 660 p.

6. Horton Mike. Network Security – Portable Reference / Mike Horton, Clinton Mugge. – McGraw-Hill/Osborne, 2003. – 760 p.

7. Edney J. Real 802.11 Security Wi-Fi Protected Access and 802.11i / J. Edney, W.A. Arabaugh. – Pearsons Education Inc. , 2004. – 440 p.

Надійшла до редколегії 29.01.2010

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

ИССЛЕДОВАНИЯ И АНАЛИЗ ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ ЗАЩИЩЕННЫХ КОРПОРАТИВНЫХ СЕТЕЙ СВЯЗИ. УСОВЕРШЕНСТВОВАНИЕ ПРОТОКОЛА WEP

Ю.Р. Гарасим, П.А. Пуля

Работа посвящена исследованию и анализу защищенности беспроводных корпоративных сетей связи. Рассмотрен принцип функционирования и структура основных видов беспроводных сетей. Проведен анализ существующих протоколов, определены их недостатки и преимущества. Предложена модификация протокола WEP, которая заключается в постоянном обновлении общего секретного ключа между точкой доступа и беспроводным терминалом. Такое решение эффективно работает на существующем оборудовании и предоставляет значительные преимущества в сравнении со стандартным.

Ключевые слова: *защищена беспроводная сеть связи, протоколы шифровки данных, пакеты данных, аутентификация пользователей.*

SECURE CORPORATE WIRELESS NETWORKS RESEARCH AND ANALYSIS. WEP PROTOCOL IMPROVEMENT

I.R. Garasym, P.A. Pulya

Work is devoted research and analysis of protected of wireless corporate communication networks. Principle of functioning and structure of basic types of wireless networks is considered. The analysis of existent protocols is conducted, their failings and advantages are certain. Modification of protocol of WEP is offered, which consists in the permanent update of the general secret key between the point of access and wireless terminal. Such decision effectively works on an existent equipment and gives considerable advantages by comparison to standard.

Keywords: *a wireless communication network is protected, protocols of enciphering of information, packages of information, authentication users.*