Особливості забезпечення захисту безпровідних мереж стандарту 802.11

Полотай О.І.

Львівський державний університет безпеки життєдіяльності

Summary. Protective protocols of WEP and WAP wireless networks are considered and the peculiarities of their operation and data encryption are described..

Keywords: information security, protection protocols, encryption.

Всі сучасні бездротові пристрої (точки доступу, бездротові адаптери і маршрутизатори) підтримують протокол безпеки WEP (Wired Equivalent Privacy), який був спочатку закладений в специфікацію бездротових мереж IEEE 802.11. Даний протокол є свого роду аналогом провідної безпеки, проте реально ніякого, еквівалентного провідним мережам рівня безпеки, він, звичайно ж, не забезпечує.

Протокол WEP дозволяє шифрувати потік переданих даних на основі алгоритму RC4 з ключем розміром 64 або 128 біт – ці ключі мають так звану статичну складову довжиною від 40 до 104 біт і додаткову динамічну складову розміром 24 біта, звану вектором ініціалізації (Initialization Vector, IV).

Процедура WEP-шифрування виглядає наступним чином. Спочатку передані в пакеті дані перевіряються на цілісність (алгоритм CRC-32), після чого контрольна сума (integrity check value, ICV) додається в службове поле заголовка пакету. Далі генерується 24-бітний вектор ініціалізації (IV), а до нього додається статичний (40 або 104-бітний) секретний ключ. Отриманий таким чином 64 або 128-бітний ключ і є вихідним ключем для генерації псевдовипадкового числа, яке використовується для шифрування даних. Далі дані змішуються (шифруються) за допомогою логічної операції XOR з псевдовипадковою ключовою послідовністю, а вектор ініціалізації додається в службове поле кадру.

Протокол WEP є далеко не найкращим способом захисту бездротової мережі. Після публічної демонстрації численних вразливостей WEP, IEEE приступив до розробки стандарту 802.11i, покликаного усунути ці недоліки.

Однак процес його створення затягнувся, в зв'язку з чим один з наброс-ков (Draft 3) став використовуватися в якості проміжного рішення. Цей стандарт отримав назву Wi-Fi Protected Access (WPA). В WPA для аутен-тіфікаціі станції і мережі може використовуватися інфраструктура 802.1 X або загальний ключ [2].

На відміну від WEP ключі шифрування генеруються при встановленні з'єднання, а не розподіляються статично. Після успішної аутентифікації сервер RADIUS передає станції значення, яке використовується для ідентифікації даної сесії - кельмою (МК). Станція і сервер RADUIS на основі МК виводять Pairwise Master Key (PMK), який передається точки доступу сервером RADIUS. Для генерації PMK використовується псевдовипадкова функція (PRF), заснована на хеш-функції HMAC-SHA-1. Отримане значення ключа прив'язується до поточної сесії між точкою доступу і станцією.

Ключ PMK потім використовується точкою доступу і клієнтом для генерації ключа Pairwise Transient Key (PTK). Ключ PTK, довжина якого складає 512 біт, в подальшому розділяється на 4 ключа: Key Confirmation Key (КСК), Key Encryption Key (КЕК) і два ключа шифрування Temporal Key 1 і 2 (TK1 / TK2).

Ключ КСК застосовується в процесі виведення ключів шифрування для аутентифікації клієнта. Значення КЕК, використовується для захисту ключів шифрування широкомовного і групового трафіку Group Transient Key (GTK). Ключ GTK повинен бути однаковий для всіх станцій однієї мережі (BSS), тому він генерується точкою доступу і передається всім станціям. Ключі TK1 / TK2 застосовуються для захисту трафіку. Конкретні деталі їх застосування залежать від використовуваного криптоалгоритму [3].

Процес генерації ключа PMK заснований на обміні чотирма керуючими повідомленнями (4-way handshake, см IEEE802.11i):

- точка доступу відсилає станції випадкове число ANonce;

- станція генерує випадкове число SNonce і використовує функцію PRF-512 для виведення PTK на підставі PMK, ANonce, SNonce і MAC-адрес пристроїв. Значення SNonce

відсилається на точку доступу, причому це повідомлення захищається за допомогою функції контролю цілісності, що розраховується на основі ключа КСК;

- точка доступу отримує SNonce, виводить значення РТК і перевіряється цілісність повідомлення за допомогою отриманого значення КСК. Якщо дані коректні, станції відсилається інформація про підтримувані режимі безпеки і ключ GTK;

- станція перевіряє параметри безпеки на збіг із значеннями, отриманими під час сканування (в Beacon або Probe Response), і цілісність отриманого повідомлення. Якщо відхилень не виявлено – точці доступу відсилається підтверджуючий пакет.

В якості алгоритму шифрування в WPA використовується Temporary Key Integrity Protocol (TKIP), заснований на RC4, що дозволяє реалізувати сумісність з устаткуванням, що підтримує WEP. При використанні TKIP довжина вектора (TKIP Sequence Counter, TSK) ініціалізації збільшена до 48 байт, що знижує ймовірність його повторення.

Ключ шифрування перемішується з MAC-адресою і TSK, і отримане значення використовується в якості ключа RC4. Таким чином, при застосуванні TKIP для кожного пакета використовується свій унікальний ключ WEP.

Таким чином, WPA вирішує такі проблеми WEP [1]:

- статичний ключ шифрування;
- відсутність контролю цілісності повідомлень;
- недостатня довжина вектора ініціалізації.

Використання RC4 в якості основного алгоритму шифрування вже не задовольняє сучасним вимогам безпеки. У зв'язку з цим в стандарті 802.11i описується обов'язкове використання протоколу Counter Mode with CBC-MAC Protocol (Ccmp) для шифрування трафіку. У цьому протоколі, описаному в RFC 2610, використовується в якості криптографічного примітиву алгоритм AES-128, який є в даний час державним стандартом Сполучених Штатів Америки.

У таблиці 1 наведено відповідність між різними назвами протоколів захисту бездротових мереж і криптоалгоритмами, які ними використовуються.

Таблиця 1

Стандарти захисту безпровідних мереж

Назва	Стандарт	Функції безпеки	Інші назви
WPA	802.11i Draft 3	TKIP, RC4	Transition Security Network (TSN)
WPA2	802.11i	TKIP, RC4 CCMPЯК1P, AES/RC4	Robust Secure Network (RSN)

Як видно з таблиці, підтримка WPA2 або 802.11i означає, що для шифрування може використовуватися TKIP. В налаштуваннях підключення до бездротової мережі можна вибрати як WPA-TKIP, так і WPA2-TKIP.

Однак пристрої, які не підтримують WPA2 (наприклад, КПК на базі Windows Mobile), не можуть працювати з мережею, налаштовану на використання WPA2-TKIP, в зв'язку з деякими відмінностями в процесі встановлення з'єднання.

Література:

1. Гейер Дж. Беспроводные сети. Первый шаг: Пер. с англ. – М.: [Электронный ресурс] Издательский дом "Вильямс", 2005. – 192 с.: ил.
2. Мерритт М. Безопасность беспроводных сетей [Текст] / М. Мерритт. –М.: Книга по Требованию, 2015. – 282 с.
3. Радке Хорст-Дитер Все о беспроводных сетях / Хорст-Дитер Рад-ке , Йеремиас Радке. – М.[Электронный ресурс]: НТ Пресс, 2011. – 320 с.