УДК 004.056.52, 004.056.53
О.Маєвський
(Тернопільський національний технічний університет імені Івана Пулюя)

СЛАБКІСТЬ АЛГОРИТМУ ШИФРУВАННЯ WEP

Стандарт IEEE 802.11 вводить додаткові вразливості, дозволяючі обійти ідентифікацію WEP-ключа. Стандарт визначає IV (вектор ініціалізації) як 24-бітове поле, яке викличе багатократне використання вектору ініціалізації і деградацію шифру RC4, використовуваного в WEP до такого рівня, коли він стає схильний до атак.

Стандарт визначає, що WEP-алгоритм – це форма електронної книги кодів, в якій блок звичайного тексту за допомогою логічного “або” шифрується за допомогою псевдовипадкової послідовності певної довжини. Послідовність ключа генерується WEP-алгоритмом.

Секретний ключ з'єднується з вектором ініціалізації, і результуюча послідовність служить вхідною інформацією для PRNG (псевдовипадкового генератора чисел). PRNG використовує потоковий шифр RC4 для отримання ключової послідовності псевдовипадкових октетів, рівних по довжині числу октетів даних, які мають бути передані. В цілях захисту даних від неавторизованої модифікації застосовуються алгоритми перевірки цілісності, які створюють перевірочні суми на базі тексту повідомлення і приєднуються до нього, створюючи таким чином IVC (величину перевірки цілісності). Після цього проводиться шифрування за допомогою математичного поєднання виходів IVC і PRNG через побітне логічне “або”, що і породжує зашифрований текст.

В потокового шифрування є проблема: якщо всі повідомлення шифруються з одним і тим же IV, то атакуючий може розпізнати його і розшифрувати повідомлення. Одна така атака полягає в тому, що два зашифрованих повідомлення побітно об'єднуються логічним “або”. Якщо різні зашифровані повідомлення використовують однаковий IV, процес логічного “або” для цих повідомлень ефективно скорочує дію ключа і призводить до логічного “або” для первинного тексту повідомлень. Якщо відоме одне з повідомлень, то в результаті “або” легко видобути інше повідомлення.

Якщо дані, зашифровані за допомогою потокового шифру, достатньо довгі і зашифровані за допомогою одного IV, проблема знаходження секретного ключа стає ще простішою. Повторне використання одного і того ж ключа призводить до того, що називається глибиною аналізу. Частотний аналіз, пастки і інші класичні технології дають способи обчислення оригінального тексту із зашифрованого повідомлення.

Потокові шифри також схильні до атак текстів і обраних зашифрованих текстів. Атакуючий повинен тільки послати електронне повідомлення “мішені”, яку він хоче атакувати, або простежити за тим, як “мішень” відвідує відомий веб-сайт. Хоча ці дії і виглядають зовсім нешкідливими, якщо атакуючий прослуховує безпровідний трафік своєї “мішені”, тоді він знає і IV, і передаваний текст. Прості обчислення, виконані з цією інформацією, дадуть йому секретний ключ, який може бути використаний не лише для доступу до безпровідної мережі, але також для розшифровки усіх майбутніх пакетів, що передаються через безпровідну мережу.

Серед експертів в області безпеки немало питань викликає і процес генерації приманки для PRNG. Генерація цієї приманки збільшує шанси і ймовірність того, що атакуючий зможе визначити секретний ключ з шифрованої атаки. Якщо атакуючий може атакувати зашифровані дані, зрозуміти схему генерації IV і отримати інформацію про достатнє число IP-діаграм, він зможе вичислити первинне значення секретного ключа на основі цієї інформації.