УДК 004.415.5
Комарніцький М. – ст. гр. СІ-41
Тернопільський національний технічний університет імені Івана Пулюя

ОРГАНІЗАЦІЯ ЗАХИСТУ РЕСУРСІВ БЕЗДРОТОВИХ МЕРЕЖ IEEE 802.11 З ВИКОРИСТАННЯМ ПРОТОКОЛУ WPA2

Науковий керівник: асистент кафедри КС, Жаровський Р.О.

Стандарт IEEE 802.11 на локальні бездротові мережі WLAN розроблено Інститутом інженерів з електротехніки й електроніки (Institute of Electrical and Electronics Engineers).

Низький рівень безпеки є одним із головних недоліків безпровідних мереж Wi-Fi. Застосування WPA2 (Wi-Fi Protected Access 2) та заснованого на портах протоколу аутентифікації IEEE 802.1X. не захистить вас від "нелегальних" пристроїв, атак типу "відмова в обслуговуванні" (denial-of-service) або іншого втручання ззовні, але забезпечить безпеку бездротових комунікацій.

Протокол WPA2 використовує новий метод шифрування – CCMP(Counter-Mode with CBC-MAC Protocol), заснований на алгоритмі шифрування AES (Advanced Encryption Standard).

WPA2 працює у двох режимах аутентифікації: персональному (Personal) і корпоративному (Enterprise). У режимі WPA2-Personal з введеної відкритим текстом парольної фрази генерується 256-розрядний ключ, що іноді називають попередньо розподіленим ключем (PreShared Key - PSK). Ключ PSK, а також ідентифікатор SSID (Service Set Identifier) і довжина SSID разом утворюють математичний базис для формування головного парного ключа Pairwise Master Key - PMK, який використовується для ініціалізації чотиристороннього зв'язку та генерації тимчасового парного або сеансового ключа Pairwise Transient Key - PTK, для взаємодії бездротового користувацького пристрою з точкою доступу.

Виконавши процедуру аутентифікації 802.1X, клієнт отримує від сервера аутентифікації головний ключ Master Key - MK, який "прив'язується" до даного сеансу аутентифікації. На основі цього ключа на клієнті і на сервері аутентифікації генерується один і той же парний головний ключ PMK. Аутентифікатор отримує ключ PMK від сервера аутентифікації за допомогою попередньо визначеного атрибута RADIUS. Володіючи ключем PMK, клієнт і пункт доступу генерують парний тимчасовий ключ PTK, практично не обмінюючись ними.

У WPA2 є три типи ключів PTK: ключ підтвердження ключа Key Confirmation Key - KCK, що застосовується для перевірки цілісності кадру; EAPOL-Key (використовується в контрольній сумі MIC); ключ шифрування ключа Key Encryption Key - KEK, використовується для шифрування групового тимчасового ключа Group Transient Key - GTK і тимчасові ключі Temporal Keys - TK - для шифрування трафіку.

Для аутентифікації і забезпечення цілісності даних WPA2 використовує протокол CBC-MAC (Cipher Block Chaining Message Authentication Code), а для шифрування даних та контрольної суми MIC - режим лічильника Counter Mode - CTR.

З точки зору корпоративної безпеки технологія Wi-Fi готова до широкого впровадження. Протокол WPA2 забезпечує шифрування і цілісність даних, а використання його з механізмами аутентифікації 802.1X, гарантуватиме повну безпеку передачі даних по бездротових каналах зв'язку.