УДК 681.3.06 СТАНДАРТИ ТА БЕЗПЕКА БЕЗДРОТОВОГО ЗВ'ЯЗКУ

Запека М.,
студентка гр. 126ІСТ_бд_3.1
Дегтярьова Л.М., доцент кафедри
інформаційних систем та технологій, к.т.н., доцент

Бездротові технології передачі даних тривалий час використовуються в сучасному світі інформаційних технологій. Використання ліцензійних частот, висока вартість обладнання, невелика швидкість передачі даних були негативними факторами, які перешкоджали широкому поширенню даних мереж, але поява та ратифікація стандарту IEEE 802.11b [1] (а потім версій "a" и "g" стандарту IEEE 802.11 [2]) дозволило істотно збільшити швидкість передачі даних, забезпечивши швидкодія, яка досягається за рахунок одночасної роботи з двома частотним каналам. На сьогоднішній день бездротові мережі набули широкого поширення не тільки в офісах, але і в мережах домашнього користування.

IEEE 802.11 – базовий набір стандартів зв'язку для комунікації в бездротовій локальній мережевій зоні частотних діапазонів 0,9; 2,4; 3,6; 5 і 60 ГГц. Ця технологія розвиває ціле сімейство стандартів передачі цифрових потоків даних по радіоканалах – 4 основні режими роботи бездротової мережі Wi-Fi (802.11a, 802.11b, 802.11g, 802.11n), які відрізняються максимальною швидкістю передачі даних:

- IEEE 802.11a – описує значно вищі швидкості передачі ніж 802.11b. Використовуються частотні канали в частотному спектрі 5 ГГц. Протокол не сумісний з 802.11b. Ратифікований в 1999 році. Використовувана радіочастотна технологія: OFDM. Кодування: Convoltion Coding. Модуляції: BPSK, QPSK, 16-QAM, 64-QAM. Максимальні швидкості передачі даних в каналі: 6, 9, 12, 18, 24, 36, 48, 54 Мбіт/с.
- IEEE 802.11b – описує великі швидкості передачі і вводить більше технологічних обмежень. Цей стандарт широко просувався з боку WECA і спочатку називався Wi-Fi. Використовуються частотні канали в діапазоні 2.4 ГГц. Ратифікований в 1999 році. Використовувана радіочастотна технологія: DSSS. Кодування: Barker 11 і CCK. Модуляції: DBPSK і DQPSK. Максимальні швидкості передачі даних в каналі: 1, 2, 5.5, 11 Мбіт/с.
- IEEE 802.11g – описує швидкості передачі даних еквівалентні 802.11a. Використовуються частотні канали в діапазоні 2.4 ГГц. Протокол сумісний з 802.11b. Ратифікований в 2003 році. Використовувані радіочастотні технології: DSSS і OFDM. Кодування: Barker 11 і CCK. Модуляції: DBPSK і DQPSK. Максимальні швидкості передачі даних в каналі: 1, 2, 5.5, 11 Мбіт/с на DSSS і 6, 9, 12, 18, 24, 36, 48, 54 Мбіт/с на OFDM.
- IEEE 802.11n – найпередовіший комерційний WiFi-стандарт. Використовуються частотні канали в частотних діапазонах 2.4 ГГц і 5

ГГц. Сумісний з 11b / 11a / 11g. Вийшов 11 вересня 2009 року. Підтримуються частотні канали WiFi шириною 20МГц і 40МГц (2x20MHz). Використовувана радіочастотна технологія: OFDM.

Повномірний перехід на бездротову мережу відбувся завдяки функціоналу Wi-Fi-мережі, який відповідав вимогам, що пред'являються до корпоративних, комерційним або промислових мереж.

В корпоративних мережах, які використовуються сучасними користувачами бездротових мереж, необхідні різні рівні доступу і якість сервісу для різних категорій користувачів і різного обладнання, з правом доступу до інформаційних ресурсів, необхідних для даної групи.

Мережі бездротового доступу більш доступні для хакерських атак, ніж кабельні мережі. Але цей факт безумовно не означає, що їх неможливо захистити. Існує чимало компаній, які вважають достатньою мірою захисту власних бездротових мереж використання способу шифрування даних WPA/WPA2, який представлено оновленою програмою сертифікації бездротового зв'язку, що забезпечує посилену безпеку даних і посилений контроль доступу до бездротових мереж. Однак це не гарантує того, що навіть при цьому корпоративні мережі цих компаній не зіткнуться з проблемами, що виникають в результаті DoS-атак зловмисників, і не понесуть фінансові втрати.

На сьогоднішній день стандартом 802.11b окреслено ряд заходів, які дозволяють захистити невеликі бездротові мережі, однак залишається невирішеним питання продуктивності цих заходів для великої кількості точок доступу і користувачів, оскільки зловмисники атакують найменш захищену частину мережевої інфраструктури - клієнтські робочі станції

В якості прикладів атак на клієнтів бездротових мереж можна назвати підключення ноутбука користувача до корпоративної мережі, який використовується і в домашній бездротовій мережі; організація каналу витоку інформації з мережі - при відправці по електронній пошті "дуже корисною програми".

Для посилення безпеки бездротових мереж на сьогоднішній день існують три засоби - стандарти бездротового безпеки IEEE 802.1x, 802.11i і протокол WPA [3].

Стандарт IEEE 802.1x застосовується для авторизації, автентифікації і акаунтинга користувачів, для перевірки можливості надання доступу до мережі. В даному стандарті бездротової безпеки використовуються динамічні ключі шифрування для збільшення захисту і стійкості до атак. Стандарт 802.1x дає змогу використовувати, наприклад, як засіб автентифікації, сервер RADIUS (Remote Access Dial-In User Server) в якості стандартного рішення, і протокол EAP (Extensible Authentication Protocol) в якості засобу транспортування повідомлень 802.1x.

Завдання RADIUS-сервера полягає в прийнятті незалежного рішення (позитивного або негативного) в процедуру надання доступу користувачу в мережу. Слід зазначити, що саме стандарт 802.1x надає можливість авторизації і аутентифікації користувача на сервері навіть для застарілих пристроїв, які працюють за процедурами та параметрами стандарту 802.11b.

В даний час існує декілька популярних реалізацій RADIUS-серверів: FreeRadius, GNU Radius, Cistron Radius, Radiator Radius, Microsoft IAS, Advanced Radius.

Серед найбільш використовуваних засобів захисту бездротових мереж [2] можна назвати: зміна пароля адміністратора, встановленого за замовчуванням; зменшення зони радіопокриття до мінімально прийнятного значення; заборона широкомовної розсилки ідентифікатора мережі (SSID); активізація фільтрації за MAC-адресами; зміна ідентифікатора мережі (SSID), встановленого за замовчуванням; встановлення та налаштування персональних міжмережевих екранів і антивірусних програм у абонентів бездротової мережі; для взаємної аутентифікації сервера і клієнта в технології 802.1X, що є складовою частиною стандарту, можна використовувати алгоритм RSA с довжиною ключа 1024 біт і більше; виконання необхідних налаштувань фільтрації трафіку на телекомунікаційному обладнанні і міжмережевих екранах; забезпечення резервного копіювання програмного забезпечення і конфігурацій обладнання; забезпечення резервування обладнання, що входить до складу бездротової мережі; здійснення періодичного моніторингу стану захищеності бездротової мережі за допомогою спеціалізованих засобів аналізу захищеності для бездротових мереж.

Оскільки на відміну від провідних мереж, бездротові неможливо обмежити фізично тому є досить проблематичним організація їх захисту у зв’язку з тим, що бездротова мережа має великий радіус дії, безпека залишається слабкою стороною бездротових технологій. Загальнодоступність даних послуг зв'язку дозволяє зловмиснику перехоплювати інформацію або ж атакувати мережу, перебуваючи на безпечній відстані. Для протидії цим негативним впливам і існують специфікації, опрацьовані робочими групами 802.11i, а також і Wi-Fi Alliance, які дозволяють підвищити захист бездротових мереж, створюючи умови для забезпечення повного ланцюга інформаційног захисту: реєстрація, обмін обліковими даними, аутентифікація і шифрування, роблячи ці процедури більш надійними, ефективними і результативними, як проти раптових атак, так і проти заздалегідь спланованих.

Список використаних джерел

1. Педжман Рошан, Джонатан Лиэри. Основы построения беспроводных локальных сетей стандарта 802.11. Руководство Cisco = 802.11 Wireless Local-Area Network Fundamentals. — М.: «Вильямс», 2004. — С. 304

2. Владимиров А. Взлом и защита беспроводных компьютерных сетей. — М.: НТ Пресс, 2005. — 464 стр.

3. В. Ф. Шаньгін. Захист інформації в комп’ютерних системах і мережах / В. Ф. Шаньгін – Київ : МК Прес, 2012. - 592 с.

4. Бурячок В. Л., Астапеня В. М., Соколов В. Ю. Способы повышения доступности информации в беспроводных системах стандарта IEEE 802.11 с MIMO // Сучасний захист інформації. 2016. №2. – С. 60–68.