УДК 621.39
Шкрибайло І. – ст. гр. КА-11
Тернопільський національний технічний університет імені Івана Пулюя

СУЧАСНІ МЕТОДИ ЗАХИСТУ БЕЗПРОВІДНИХ МЕРЕЖ

Науковий керівник: к.т.н., доц. Савків В.Б.

Широке поширення бездротових пристроїв і їх невелика вартість призводять до того, що в периметрі мережевої безпеки виникають проломи. Активний адаптер бездротової мережі на підключеному до корпоративної мережі ноутбуці, принесена точка доступу - все це може стати зручними каналами для проникнення у внутрішню мережу.

Станції Wi-Fi можуть бути легко виявлені пасивними методами, що дозволяє з достатньо великою точністю визначати місце розташування бездротового пристрою. Наприклад, система Navizon може використовувати для визначення місця розташування мобільного пристрою систему GPS, базові станції GSM та точки бездротового доступу. Що стосується Bluetooth, то використанню цієї технології для визначення місця розташування власника мобільного телефону (наприклад) присвячено ряд серйозних робіт. Рівень ризику, пов'язаного з підключенням несанкціонованої точки доступу або клієнта бездротової мережі, можна знизити шляхом відключення невикористовуваних портів комутаторів, фільтрації по MAC-адресами (port-security), аутентифікації 802.1X, систем виявлення атак і сканерів безпеки, контролюючих поява нових мережевих об'єктів.

Контроль принесених на територію пристроїв дозволяє обмежити вірогідність підключення до мережі бездротових пристроїв. Обмеження доступу користувачів та відвідувачів до мережевих портів та слотів розширення комп'ютера знижує ймовірність підключення бездротового пристрою.

Необхідно визначити протоколи та алгоритми шифрування трафіку в бездротовій мережі. При використанні технології 802.1X визначаються вимоги до протоколів електронно-цифрового підпису і довжині ключа підпису сертифікатів, які використовуються для різних цілей. Стандарт 802.11i використовує концепцію підвищеної безпеки (Robust Security Network - RSN), яка передбачає, що бездротові пристрої повинні забезпечувати додаткові можливості. Це потребуватиме змін в апаратній частині та програмному забезпеченні, тобто RSN мережа стане несумісною з існуючим обладнанням WEP. У перехідний період буде підтримуватися як устаткування RSN, так і WEP, але надалі пристрої WEP почнуть відмирати. У концепції RSN в якості системи шифрування застосовується AES, подібно до того як алгоритм RC4 задіяний у WPA. Однак механізм шифрування куди більш складніший і не страждає від проблем, властивих WEP AES - блочний шифр, який оперує блоками даних по 128 біт. CCMP, у свою чергу, - протокол безпеки, який використовується AES. Він є еквівалентом TKIP в WPA. CCMP обчислює MIC, вдаючись до добре відомого і перевіреному методі Cipher Block Chaining Message Authentication Code (CBC-MAC). Зміна навіть одного біта в повідомленні призводить до зовсім іншого результату.

Правильно побудована політика безпеки є надійним фундаментом захищеної бездротової мережі. Внаслідок цього варто приділяти їй достатньо уваги, як на етапі впровадження мережі, так і в ході її експлуатації, відображаючи в нормативних документах зміни, що відбуваються в мережі.