УДК 004.056.53
М. Шмигельський, В. Ліщинський
(Тернопільський національний технічний університет імені Івана Пулюя)

ОСНОВНІ МЕТОДИ І ПРИЙОМИ ПОРУШЕННЯ БЕЗПЕКИ СУЧАСНИХ БЕЗДРОТОВИХ МЕРЕЖ

UDC 004.056.53
M. Shmyhelskyi, V. Lishchynskyi
(Ternopil Ivan Puluj National Technical University, Ukraine)

BASIC METHODS AND TECHNIQUES OF SECURITY BREACH IN MODERN WIRELESS NETWORKS

З кожним днем цифровий документообіг витісняє паперові форми передачі документів, але породжує і нові загрози порушення конфіденційності, цілісності та доступності інформації. Особливою актуальністю відзначається питання безпеки передачі даних по бездротових каналах зв'язку, які, на даний момент, вважаються перспективними засобами отримання та передачі інформації, у зв'язку з гнучкістю організації мережі, особливо в місцях де провідні мережі не можуть бути організовані в принципі, а завдяки мінімальним витратам часу, що на даний момент є основними вимогами до систем передачі інформації.

Бездротові мережі використовують радіохвилі, які поширюються за законами фізики і принципом дії передавальних антен в зоні радіусу мережі. На сьогоднішній день системи радіодоступу будуються у відповідності з наступними стандартами: HiperLAN2; MMDS; WLL; IEEE 802. 16; EEE 802.11 / b / g / n.

Отже, перейдемо безпосередньо до методів і засобів забезпечення безпеки бездротових з'єднань. Кожна бездротова мережа має, як мінімум, 2 ключові компоненти: базову станцію та точку доступу. Бездротові мережі можуть функціонувати в двох режимах: Ad-hoc (peer-to-peer) та Infrastructure.

Атаки на бездротові мережі умовно діляться на 3 основні категорії:

- Пасивні атаки. Основною метою таких атак є перехоплення даних, що проходять через стільникову мережі. Для здійснення цього зловмисникові необхідний комп'ютер з бездротовим мережевим адаптером і спеціальним програмним забезпеченням для перехоплення трафіку.

- Активні атаки. Однією з найбільш результативних атак є атака «Man-in-the-Middle», яка полягає в перехопленні сеансу 2 клієнтів. Атакуючий має 2 мережевих адаптера і організовує фальшиву точку доступу. Він змушує інших клієнтів використовувати його точку доступу, а сам перенаправляє трафік на реальну точку доступу, тим самим, отримуючи доступ до всіх сеансів зв'язку

- Атаки перешкодами. Мета атаки - глушіння сигналу, тобто це атака на відмову в обслуговуванні, специфічна для бездротових мереж. Суть атаки полягає в генерації радіошуму на частоті роботи бездротової мережі. Це не означає, що глушіння сигналу є ознакою атаки, так як перешкоди можуть виходити від сторонніх радіопристроїв.

Основні ризики безпеки бездротових мереж пов’язані з авторизованим доступом, з нефіксованою природою зв'язку, з вразливостями мереж і вимушеними простоями, з витіканням інформації з провідної мережі, з особливостями функціонування бездротових мереж. Єдиний вірний підхід з бездротовими рішеннями, як і з дротовими, – це будувати багаторівневу систему захисту мережі з використанням:

- контролю доступу;
- аутентифікації користувачів;
- шифрування трафіку;
- системи запобігання вторгнень в бездротову мережу;
- системи виявлення чужих пристроїв і можливості їх активного придушення;
- моніторингу спотворення сигналів і DoS-атак;
- моніторингу вразливостей в бездротової мережі і можливості аудиту вразливостей;
- функцій підвищення рівня безпеки інфраструктури бездротової мережі, наприклад, аутентифікація пристроїв (X.509 тощо), захист даних управління – MFP / Management Frame Protection.