Protect information from unauthorized access in wireless networks

Maria Mandrona

Security of Information Technologies Department,
Lviv Polytechnic National University, UKRAINE,
Lviv, S. Bandery street 12,
E-mail: mandrona@yandex.ua

In today's world of information technology long used wireless technology to transfer information. Today, wireless networks used in offices and at home. But a question of security remains weak and the vulnerable side of wireless technologies. Unlike wired networks, wireless networks are physically impossible to limit and, therefore, very difficult to organize their protection, because a wireless network has a great radius of action.

Accordingly, an attacker can intercept information, or to attack the network, and thus located at a safe distance.

Security – one of the key factors for designing any system. Modern wireless technologies offer not very effective methods to protect information. Traditionally distinguish several kinds of attacks on wireless networks that are different methods, and to the degree of threat:

- hacking networks (interception management, joining the network);
- cloning (eavesdropping, theft of money and traffic).

In wireless networks to reduce the likelihood of unauthorized access envisaged access control by MAC-addresses of devices and WEP.

Since access control is implemented using the access point, it is possible only with the infrastructure network topology. The control mechanism involves advance tabulations of MAC-addresses allowed users to access point and provides transfer only between registered wireless adapters.

Since the emergence of standard 802.11i can be said about the absolute chain of protection: registration, exchange of credentials, authentication and encryption are more reliable, proven, effective and productive as against sudden attacks, and against those who planned in advance.

Захист інформації від несанкціонованого доступу в бездротових мережах

Марія Мандрона

Кафедра безпеки інформаційних технологій,
Національний університет "Львівська політехніка",
УКРАЇНА, м.Львів, вул.С.Бандери, 12,
E-mail: mandrona@yandex.ua

Захисту конфіденційної інформації в бездротових мережах варто надавати особливу увагу. Адже бездротова мережа має великий радіус дії, і тому зловмисник може перехоплювати інформацію або ж атакувати мережу, знаходячись на безпечній відстані. В роботі наведені класифікація бездротових мереж, класифікації атак, та види захисту конфіденційної інформації від несанкціонованого доступу.

Ключові слова – бездротові мережі, точки доступу, атаки, хакер, несанкціонований доступ, захист бездротових мереж.

I. Вступ

На сьогоднішній день бездротові мережі отримали величезне розповсюдження. Вони використовуються, як у офісах, так і в домашніх умовах. Ці мережі дуже зручні в користуванні і дозволяють незалежно від місця знаходження бути он-лайн: обмінюватися даними, відправляти і приймати пошту, знаходити потрібну інформацію в Інтернет.

II. Бездротова мережа

Бездротова мережа – це гнучка інфраструктура, що представляє собою комплекс апаратно-програмних засобів для передачі інформації. Бездротові мережі можуть виступати як альтернатива провідним мережам та успішно доповнювати їх, надаючи додаткові функції. У бездротових мережах для передачі даних використовуються радіохвилі.

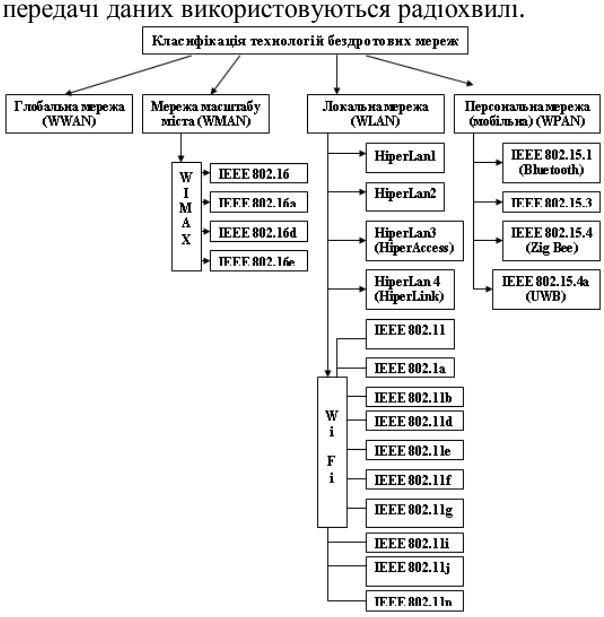

Рис.1 Класифікація бездротових мереж за територіальною ознакою

III. Атаки на бездротові мережі

Атака – це запуск людьми спеціальних програм для отримання неавторизованого доступу до мережі [3]. Загальну класифікацію атак на бездротові мережі можна подати у наступному вигляді.

Рис.2 Загальна класифікація атак

Існують різні способи несанкціонованого доступу на бездротові мережі на рис.3 представлена класифікація видів атак на бездротові мережі.

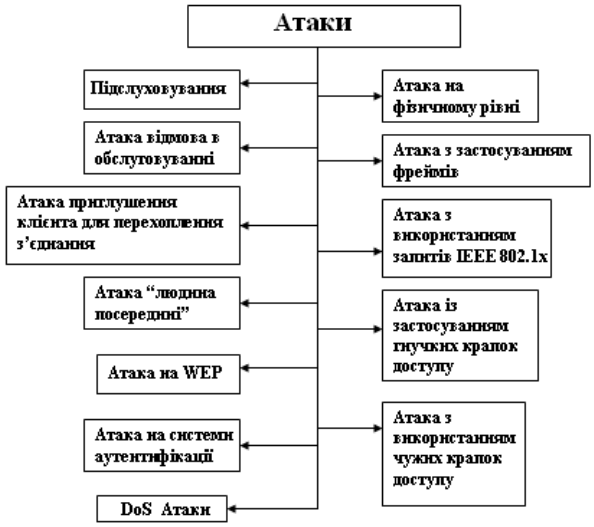

Рис.3 Класифікація видів атак

Існують різні причини, що спонукають хакерів займатися атаками [1]. Одна з причин: заради цікавості. Такі люди займаються зламуванням задля розваги та самоствердження. Вони можуть навіть зробити послугу суспільству, публічно сповістити про виявленні небезпечні місця мереж, що примусить звернути увагу на існуючі проблеми.

Інша причина атак криється в застосуванні чужої мережі, тобто в крадіжці інтернет-трафіку.

Третя, найважливіша причина – це викрадення конфіденційної інформації. Ці зловмисники є найне-безпечнішими. Стандартні заходи безпеки можуть лише затримати такого супротивника на декілька годин. Якщо безпеці мережі не приділити належної уваги, то атака неминуче виявиться успішною.

IV. Захист бездротових мереж

Система захисту - це один з найважливіших і складних елементів бездротових мереж.

Здатність хакерів відстежувати трафік, отримувати неавторизований доступ до ресурсів і викликати відмову в обслуговуванні бездротовою мережею її користувачів - ось ті проблеми, які доведеться вирішувати. Використовуючи ефективні механізми аутентифікації і шифрування, можна істотно знизити небезпеку. Проте слід мати на увазі, що необхідний рівень безпеки залежить від пропонованих до мережі вимог.

Нижче наведена класифікація різних методів захисту бездротових мереж.

Рис.4 Класифікація методів захисту бездротових мереж

Розглянувши усі доступні на сьогоднішній день методи захисту, можна виділити головні: WEP, WPA, WPA2, 802.1X. Який саме метод слід вибрати залежить від мети, яку переслідує користувач, та від існуючого обладнання. WPA2 та 802.1X – більш нові методи захисту, вони потребують потужного обладнання для криптографічних обчислень. Якщо пристрої спроможні підтримувати ці методи, то краще вибрати саме їх. Якщо ні, то можна зупинити свій вибір на WPA, якщо і цей стандарт обладнанням не підтримується, то хоча б на WEP. Також не треба зневажати допоміжними засобами [2]. Але необхідно розуміти, що будь-який захист можна обійти, це просто питання часу.

Висновок

У цій статті розглянуто бездротові мережі, розроблено загальну структурну класифікацію за територіальною ознакою, розглянуто основні атаки та розроблено загальну класифікація атак на бездротові мережі. Розглянуто усі доступні на сьогоднішній день методи захисту.

Література

[1] Владимиров А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей. – М.: НТ Пресс, 2005. – 463 с.

[2] Рошан Педжман, Лиэри Джонатан. Основы построение беспроводных локальных сетей стандарта 802.11. – М.: Издательский дом "Вильямс", 2004. – 304 с.

[3] Мерит Максим, Дэвид Полино. Безопасность безпроводних сетей» пер. с англ. Семенова А.В. – М.: Компания АйТи; ДМК Пресс, 2004.- 288с.