УДК 681.3.07
Фурко Ю. – ст. гр. РІ-41
Тернопільський державний технічний університет імені Івана Пулюя

ШЛЯХИ ЗЛОМУ ТА МЕТОДИ ЗАХИСТУ МЕРЕЖ 802.11G

Науковий керівник: Луцків А.М

Захисту бездротових мереж варто приділяти особливу увагу. Адже Wi-Fi це бездротова мережа з великим радіусом дії. Відповідно, зловмисник може перехоплювати інформацію або ж атакувати мережу, знаходячись на безпечній для себе відстані.

Наведемо основні способи захисту:

- Використання WEP-протоколу 64-, 128-, 256- і 512-бітних протоколів шифрування.
- Використання TKIP-протоколу динамічних ключів мережі.
- Використання MIC - протоколу перевірки цілісності пакетів, що захищає їх від перехоплення, а також бере участь у захисті інформації при зміні напрямку руху пакетів.
- Використання WPA2 – протоколу (вдосконаленого WPA-протоколу, де використовується більш стійкий AES алгоритм шифрування).
- Розробка мереж, що відповідають стандарту 802.1X безпеки, у який, в свою чергу, входять кілька спеціалізованих протоколів захисту.
- Створення VPN – мереж між вузлами мережі для безпечного підключення клієнтів до мережі через загальнодоступні Інтернет-канали.

До основних методів атаки відносяться:

1. Access Point Spoofing & MAC Sniffing. Access Control List – полягає у відносно простому перехопленні MAC – адреси, яка навіть з WEP-шифруванням передається у відкритому вигляді.
2. WEP Attacks – атаки на протокол WEP.
3. Plaintext атака – зловмисник на основі первинного повідомлення і отриманої зашифрованої відповіді, може підібрати ключ шифрування.
4. Атака Fluhrer-mantin-shamir.
5. Low-hanging Fruit – найпростіша атака, яка базується на тому факті, що більшість бездротових мереж не захищені, в них не вимагається авторизація і навіть не використовується WEP, так що людина з бездротовою мережевою карткою і сканером може легко підключитися до Access Point'у і використовувати всі ресурси, що надаються власником мережі.

Якщо організації захисту бездротових мереж не приділяти належної уваги зловмисник може: отримати доступ до ресурсів WI - FI-мережі, а через неї і до ресурсів об'єднаних з нею локальних мереж; прослуховувати трафік, перехоплюючи з нього певну, цікавлячу зловмисника конфіденційну інформацію; спотворювати інформацію, що передається мережею; використовувати інтернет-трафік; атакувати ПК користувачів і сервери бездротової мережі; впроваджувати підроблені точки доступу; розсилати спам, і здійснювати інші протиправні дії від імені скомпрометованої мережі.