УДК 681.3
Сівіцький О. В. - ст.гр. СІ-42
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ПЕРЕДАЧІ ДАНИХ НА БАЗІ СТАНДАРТУ 802.15

Науковий керівник: к.т.н., доцент, Луцків А.М.

Bluetooth – це технологія бездротового зв'язку короткого діапазону, яка використовується для підключення двох і більше пристроїв на відстані до 8 метрів. Ця технологія базується на стандарті IEEE 802.15. Основним призначенням Bluetooth є забезпечення економного і дешевого радіозв'язку між різними типами електронних пристроїв, таких як: мобільні телефони, смартфони, планшети, КПК, ігрові приставки, периферійні пристрої, гарнітура для IP-телефонії, а також на основі даної технології можна створювати локальні комп'ютерні мережі. Також дослідниками доведено те, що інформацію яка передається по протоколу 802.15 можна перехоплювати на відстані до 2 кілометрів за допомогою доступного радіотехнічного обладнання.

Як стверджують виробники, захисні функції bluetooth гарантують безпечну комунікацію на всіх взаємодіючих рівнях. Однак, з точки зору безпеки, в цій технології є ряд недоліків: технологія робить сильний акцент на ропізнання пристроїв, але водночас bluetooth-технологія не пропонує жодного способу розпізнавання користувачів, що робить bluetooth-пристрої особливо уразливими до так званих spoofing-нападів та низки інших.

Для перевірки захищеності інформаційних систем на базі даної технології використовуються наступні програмні засоби [1]:

1. Bluesnarfing –це програмна утиліта, яка надає несанкціонований доступ до інформації, за допомогою OBEX-атак.
2. BlueBug – технологія яка дозволяє завантажувати з телефонної книги контакти, виклики та SMS повідомлення. Принцип роботи базується на надсиланні AT-запитів через приховані канали для вразливих телефонів без надсилання повідомлення власнику.
3. BlueSmack – програмна утиліта, яка дозволяє зламати декілька пристроїв одразу, за допомогою атаки "відмова в обслуговуванні" й може бути проведена з використанням стандартних інструментів, які поставляються з офіційним Linux-пакетами утиліти Bluez.
4. Blueprinting це технологія , яка дозволяє віддалено дізнаватися подробиці про Bluetooth-пристрої. Blueprinting може бути використана для отримання інформації про виробників і моделі пристроїв, й з'ясувати, чи є в робочому радіусі зв'язку пристрої, які мають проблеми з Bluetooth безпекою

А також є цілка низка інших утиліт, які можуть бути використані для аудиту інформаційної безпеки системи передачі даних стандарту: BlueSnarf++, Bluestab, BlueBump, BlueSpooof, BlueDump, Blooover, Blooover II, Blooonix, HeloMoto та інші.

Література:

- Bluetooth Security Vulnerabilities and Bluetooth Projects [Електронний ресурс]. - Режим доступу: URL: http://trifinite.org/trifinite_org.html/