УДК 681.518

Панська А.В., Резніченко В.А.
Кіровоградський національний технічний університет

Загрози та вразливості бездротових мереж

При побудові бездротових мереж однією з найбільш гострих проблем є забезпечення їх безпеки. Якщо в звичайних мережах інформація передається по дротах, то радіохвилі, які використовуються для бездротових рішень, досить легко перехопити при наявності відповідного обладнання. Принцип дії бездротової мережі призводить до виникнення великої кількості можливих вразливостей для атак і проникнень.

Обладнання бездротових локальних мереж WLAN (Wireless Local Area Network) включає в себе точки бездротового доступу і робочі станції для кожного абонента.

Точки доступу AP (Access Point) виконують роль концентраторів, які забезпечують зв'язок між абонентами і між собою, а також функцію мостів, які здійснюють зв'язок з кабельної локальної мережею і з Інтернетом. Кожна точка доступу може обслуговувати кілька абонентів. Кілька близько розташованих точок доступу утворюють зону доступу Wi-Fi, в межах якої всі абоненти, забезпечені бездротовими адаптерами, отримують доступ до мережі. Такі зони доступу створюються в місцях масового скупчення людей: в аеропортах, студентських містечках, бібліотеках, магазинах, бізнес-центрах і т. Д.

У точки доступу є ідентифікатор набору сервісів SSID (Service Network Idetnifier). SSID - це 32-бітна рядок, що використовується в якості імені бездротової мережі, з якої асоціюються всі вузли. Ідентифікатор SSID необхідний для підключення робочої станції до мережі. Щоб зв'язати робочу станцію з точкою доступу, обидві системи повинні мати один і той же SSID. Якщо робоча станція не має потрібного SSID, то вона не зможе зв'язатися з точкою доступу і з'єднався з мережею.

Головна відмінність між провідними і бездротовими мережами пов'язано з наявністю неконтрольованої області між кінцевими точками бездротової мережі. Це дозволяє атакуючим, що знаходяться в безпосередній близькості від бездротовий структур, виробляти цілий ряд нападів, які неможливі в дротовому світі.

При використанні бездротового доступу до локальної мережі загрози безпеки істотно зростають. Перелічимо основні вразливості і загрози бездротових мереж.

Мовлення радіомаяка. Точка доступу включає з певною частотою широкомовний "радіомаяк", щоб оповіщати навколишні бездротові вузли про свою присутність. Ці широкомовні сигнали містять основну інформацію про точку бездротового доступу, включаючи, як правило, SSID, і запрошують зареєструватися бездротові вузли в даній області. Будь-яка робоча станція, що знаходиться в режимі очікування, може отримати SSID і додати себе в відповідну мережу. Мовлення радіомаяка є вродженою патологією бездротових мереж. Багато моделей дозволяють відключати містить SSID частина цього мовлення, щоб кілька утруднити бездротове підслуховування, але SSID проте посилається при підключенні, тому все одно існує невелике вікно уразливості.

Виявлення WLAN. Для виявлення бездротових мереж WLAN використовується, наприклад, утиліта NetStumber спільно з супутниковим навігатором глобальної системи позиціонування GPS. Дана утиліта ідентифікує SSID мережі WLAN, а також визначає, чи використовується в ній система шифрування WEP. Застосування зовнішньої антени на портативному комп'ютері уможливлює виявлення мереж WLAN під час

обходу потрібного району або поїздки по місту. Надійним методом виявлення WLAN є обстеження офісної будівлі з переносним комп'ютером в руках.

Підслуховування. Підслуховування ведуть для збору інформації про мережу, яку передбачається атакувати згодом. Перехоплювач може використовувати здобуті дані для того, щоб отримати доступ до мережевих ресурсів. Обладнання, що використовується для підслуховування в мережі, може бути не складніше того, яке застосовується для звичайного доступу до цієї мережі. Бездротові мережі за своєю природою дозволяють з'єднувати з фізичної мережею комп'ютери знаходилися безпосередньо в мережі. Це дозволяє підключиться до бездротової мережі, розташований в будівлі, людині, що сидить в машині на стоянці поруч з ним. Атаку за допомогою пасивного прослуховування практично неможливо виявити.

Помилкові точки доступу в мережу. Досвідчений атакуючий може організувати неправдиву точку доступу з імітацією мережевих ресурсів. Абоненти, нічого не підозрюючи, звертаються до цієї помилкової точки доступу і повідомляють їй свої важливі реквізити, наприклад аутентифікаційну інформацію. Цей тип атак іноді застосовують в поєднанні з прямим глушінням, щоб заглушити справжню точку доступу в мережу.

Відмова в обслуговуванні. Повну паралізації мережі може викликати атака типу "відмова в обслуговуванні" (Dos). Мета будь-якої DoS-атаки полягає в створенні перешкоди при доступі користувача до мережевих ресурсів. Бездротові системи особливо сприйнятливі до таких атак. Фізичний рівень в бездротової мережі - абстрактне простір навколо точки доступу. Зловмисник може включити пристрій, що заповнює весь спектр на робочій частоті перешкодами і нелегальним трафіком, - таке завдання не викликає особливих труднощів. Сам факт проведення DoS-атаки на фізичному рівні в бездротової мережі важко довести.

Атаки типу "людина-в-середині". Атаки типу "людина-в-середині" виконуються на бездротових мережах набагато простіше, ніж на провідних, так як до провідної мережі потрібно реалізувати певний вид доступу. Зазвичай атаки "людина-в-середині" використовуються для порушення конфіденційності і цілосності сеансу зв'язку. Атаки "людина-в-середині" більш складні, ніж більшість інших атак: для їх проведення потрібно детальна інформація про мережу. Зловмисник зазвичай підміняє ідентифікацію одного з мережевих ресурсів. Зловмисник використовує можливість прослуховування і нелегального захоплення потоку даних з метою зміни його вмісту, необхідного для задоволення деяких своїх цілей, наприклад спуфінгу IP-адрес, зміни MAC-адреси для імітування іншого хоста і т.д.

Анонімний доступ в Інтернет. Незахищені бездротові ЛОМ (локальні обчислювальні мережі) забезпечують хакерам найкращий анонімний доступ для атак через Інтернет. Хакери можуть використовувати незахищену мережу WLAN організації для виходу через неї в Інтернет, де вони будуть здійснювати протиправні дії, не залишаючи при цьому своїх слідів. Організація з незахищеною ЛОМ формально стає джерелом атакуючого трафіку, націленого на іншу комп'ютерну систему, що пов'язано з потенційним ризиком правової відповідальності за заподіяну шкоду жертві атаки хакерів.

Атаки, які використовуються хакерами для злому бездротових мереж, не обмежуються описаними вище.

Список використаних джерел

1. *Шаньгін В.Ф. «Захист інформації в комп'ютерних системах і мережах» - М.: ДМК Прес, 2012. – 592 с.*