УДК 004.77
Гринюк А. – ст. гр. СНмп-51, Олійник І. – ст. гр. СН-41
Тернопільський національний технічний університет імені Івана Пулюя

ЗАГРОЗИ І РИЗИКИ БЕЗПЕКИ БЕЗПРОВІДНИХ МЕРЕЖ

Науковий керівник: асистент Маєвський О.В.

Головна відмінність між дротовими і безпровідними мережами пов’язана з абсолютно неконтрольованою областю між кінцевими точками мережі. В досить широкому просторі мереж безпровідне середовище ніяк не контролюється. Сучасні безпровідні технології пропонують обмежений набір засобів керування всією областю розгортання мережі. Це дозволяє атакуючим знаходитися в безпосередній близькості від безпровідних структур, виробляти цілий ряд нападів, які були неможливі на дротовому сегменті.

Найбільш поширена проблема в безпровідних мережах, – можливість анонімних атак. Анонімні шкідники можуть перехоплювати радіосигнал і розшифровувати передавані дані. Обладнання, використовуване для підслуховування в мережі, може бути не складніше того, яке використовується для звичайного доступу до цієї мережі. Перехоплення такого типу практично неможливо зареєструвати, і ще важче йому перешкодити. Використання антен і підсилювачів дає зловмисникові можливість знаходитися на значній відстані в процесі перехоплення. Підслуховування ведуть для збору інформації в мережі, яку згодом передбачається атакувати.

Інший спосіб підслуховування – підключитися до безпровідної мережі. Активне підслуховування в локальній безпровідній мережі зазвичай засноване на неправильному використанні протоколу Address Resolution Protocol (ARP). Насправді ми маємо справу з атакою типу MITM (man in the middle, «людина посередині») на рівні зв'язку даних. Вони можуть приймати різні форми і використовуються для руйнування конфіденційності і цілісності сеансу зв'язку. Атаки MITM складніші, ніж більшість інших атак.

Повну паралізацію мережі може викликати атака типу DOS. У всій мережі, включаючи базові станції і клієнтські термінали, виникає така сильна інтерференція, що станції не можуть зв'язуватися одна з одною. Ця атака вимикає всі комунікації в певному районі. Атакам DOS на безпровідні мережі важко запобігти або зупинити.

Глушіння в мережах відбувається тоді, коли навмисна або ненавмисна інтерференція перевищує можливості відправника або одержувача в каналі зв'язку. Атакуючий може використовувати різні способи глушіння. Глушіння клієнтської станції дає можливість шахраєві підставити себе на місце заглушеного клієнта. Також глушіння можуть використовувати для відмови в обслуговуванні клієнта, аби йому не вдавалося реалізувати з'єднання. Глушіння базової станції надає можливість підмінити її атакуючою станцією. Таке глушіння позбавляє користувачів доступу до послуг.

В безпровідних мережах застосовуються криптографічні засоби для забезпечення цілісності і конфіденційності інформації. Проте помилки приводять до порушення комунікацій і зловмисного використання інформації. Використовувати криптографічні механізми краще, ніж не використовувати їх зовсім, але завдяки відомій уразливості потрібні інші методи захисту від перерахованих вище атак. Безпровідний доступ забезпечує повну анонімність атаки. Без відповідного обладнання в мережі, що дозволяє визначати місце розташування, атакуючий може легко зберігати анонімність і ховатися де завгодно на території дії безпровідної мережі. В такому разі зловмисника важко зловити.