УДК 654.1

АНТИШПИГУНСЬКИЙ ЗАХИСТ GSM МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ

Косиєв О. А.

Гриник Р.О., ЛДУ БЖД, викладач КУІБ

ЛДУ БЖД

Мобільний зв'язок став невід'ємною частиною нашого життя, але розвиток мобільних технологій зумовлює розвиток шпигунського програмного забезпечення, в тому числі і для прослуховування розмов по мобільному телефону, тому захист мобільного телефону від прослуховування стає дедалі актуальнішим питанням.

Технологія глобальної системи мобільного зв'язку (Global System for Mobile Communications) спершу створювалась і впроваджувалась із врахуванням усіх державних вимог щодо рівня захищеності. Більшість держав світу для забезпечення підтримки цього рівня ввели заборону на використання і продаж потужних шифраторів, скремблерів, криптографічного обладнання, тощо. Самі ж оператори мобільного зв'язку захищають радіоканали шляхом шифрування сигналу з використанням достатньо складних алгоритмів.

Розрізняють кілька методів прослуховування абонентів - активний і пасивний. Для пасивного прослуховування абонента необхідне спеціальне устаткування та підготовлений персонал. На сьогодні на "чорному" ринку можна придбати цілі комплексні системи які дають можливість здійснювати прослуховування абонентів у радіусі 500 метрів. Опис таких систем і принцип їх роботи можна легко знайти в Інтернеті. За допомогою такого обладнання можна відстежувати GSM-розмови в реальному часі, ґрунтуючись на доступі до SIM-картки людини чи бази даних оператора мобільного зв'язку. Також розмови можна прослуховувати із затримкою, залежно від використовуваного оператором рівня шифрування у випадку, якщо доступ до бази даних відсутній. Така система також може бути і частиною мобільного комплексу відстеження й прослуховування рухомих об'єктів.

Другий метод прослуховування – це активне втручання в ефір. Для роботи з таким комплексом, який складається з кількох модифікованих телефонів та комп'ютера необхідний персонал, який володіє достатньою кваліфікацією в сфері зв'язку. Принцип дії такої атаки полягає в перехопленні мобільною системою сигналів для встановлення з'єднання і передачі даних за рахунок ближчого місцезнаходження до абонента (до 500 м), замінюючи найближчу базову станцію. Тобто комплекс стає "посередником" між абонентом і базовою станцією з усіма проблемами безпеки зв'язку, які виникають в такій ситуації. Такий мобільний комплекс після з'єднання здатен виконувати будь-яку функцію з керуванням зв'язком, в тому числі, з'єднати його з будь-яким необхідним номером чи, навіть, скасувати шифрування для довільного сеансу зв'язку.

Існує ще третій спосіб для прослуховування розмов і перехоплення трафіку мобільного абонента, для цього на смартфон «жертви» необхідно встановити шкідливе програмне забезпечення, при встановленні якого зловмисники можуть самі вибрати або й взагалі скасувати алгоритм шифрування, передати (або знищити) конфіденційну інформацію абонента і багато іншого.

Для сучасних смартфонів існують спеціальні програми, які можуть повідомляти користувача про конфігурацію налаштувань поточного сеансу зв'язку, у тому числі - чи передається його розмова відкрито, чи з використанням алгоритму шифрування.

EAGLE Security. Потужна програмний засіб для захисту мобільних телефонів від прослуховування, який шляхом перевірки сигнатур та ідентифікаторів базових станцій допомагає уникнути підключення до фальшивих базових станцій. Також, він здатний відзначати базові станції як підозрілі шляхом відстежування їх розташування, якщо вони переміщаються по місту або періодично зникають зі свого місця дислокації. Додаток дає можливість отримати перелік програмного забезпечення, встановленого на телефоні, яке має доступ до мікрофона та відеокамери, а також заборонити доступ небажаних програм до камери.

Android IMSI-Catcher Detector. Програмний комплекс, який дає змогу захистити смартфон від підключення до фальшивих базових станцій.

GSM SpyFinder. Дана програма здатна захистити смартфон від різного типу шпигунського устаткування, зокрема від активного GSM перехоплювача з дешифратором A5.x, який може перехоплювати вхідні та вихідні GSM дзвінки і SMS з будь-яким типом шифрування в реальному часі. Також додаток може захистити від 3G IMSI/IMEI/TMSI кетчера, який призначений для впливу на обраний телефон, щоб змусити його переключитися в режим GSM, для можливості перехоплення даних з такого телефону пасивним інтерцептором. GSM Spy Finder дає можливість оминути загрози, які виникають через блокувальними стільникових телефонів (стільниковий брандмауер), для вибіркового або масового придушення GSM/UMTS цілей.

Технологія GSM, яку використовують стільникові телефони володіє рядом вразливостей, які можуть порушити конфіденційність будь-якої інформації, яка передається мобільним зв’язком. Але завдяки створеним ресурсам та додаткам існує можливість зменшити кількість таких порушень або, навіть, звести імовірність таких порушень до мінімуму.

ЛІТЕРАТУРА

1. Прослуховування мобільних телефонів [Електронний ресурс] Режим доступу: http://it-tehnolog.com/statti/prosluhovuvannya-mobilnogo-telefonu/

2. Хома В. В., загрози інформаційній безпеці абонентів стаціонарних телефонних мереж, Вісник Національного університету "Львівська політехніка". - 2008. - № 608: Автоматика, вимірювання та керування. - С. 74-85.