УДК 004.415.056:658.115

А. О. Азарова
В. О. Гудзь
В. О. Блонський

АНАЛІЗ МЕТОДІВ ЗАХИСТУ GSM МЕРЕЖ ТА ШЛЯХІВ ЙОГО ПІДВИЩЕННЯ

Вінницький національний технічний університет

Анотація

У статті проаналізовано різні шляхи прослуховування GSM мереж, як активні, так і пасивні, а також засоби її захисту. Обґрунтовано вибір програми GSM SpyFinder із метою захисту смартфона від різного типу шпигунського устаткування у процесі мобільного зв'язку.

Ключові слова: мобільний зв'язок, GSM.

Abstract

The article analyzes different ways of GSM networks listening, both active and passive, as well as its means of protection. The choice of GSM SpyFinder is justified in order to protect the smartphone from various types of spyware during the mobile communication process.

Keywords: Mobile Communication, GSM.

Мобільний зв'язок є невід'ємною частиною комунікацій у суспільстві. Проте із розвитком технологій мобільного зв'язку одночасно збільшується кількість шпигунського програмного забезпечення, яке дозволяє прослуховувати розмови користувачів по мобільному телефону. Наявне програмне та апаратне забезпечення не дозволяє в повній мірі захистити конфіденційність процесу обміну інформацією засобами мобільних пристроїв. Тому проблема захисту мобільного зв'язку є дуже актуальною [1].

Мобільний зв'язок – це зв'язок із застосуванням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно пересуватися в межах телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції [2].

Абревіатурою GSM позначається глобальний стандарт стільникового цифрового зв'язку, в якому передбачено поділ каналів як за частотою (FDMA), так і за часом (TDMA). Технологія GSM (Global System for Mobile Communications) із самого моменту її розроблення була створена з урахуванням усіх вимог безпеки [5]. Мережа була створена з можливістю аутентифікації передплатників з використанням попередньо відкритого ключа та методології відповіді на запит. У GSM зв'язок між мобільною трубкою та базовою станцією також може бути зашифрованим. Із розвитком UMTS (Universal Mobile Telecommunications System) існує також додатковий USIM (Universal Subscriber Identity Module), який забезпечує більш тривалий ключ аутентифікації, що у свою чергу дозволяє підвищити безпеку, а також аутентифікацію базової станції для захисту користувача від підміни [3-4]. Водночас, самі мобільні оператори реалізовують захист мережі шляхом шифрування сигналу використовуючи досить складні алгоритми.

Проаналізуємо переваги і недоліки основних методів прослуховування користувачів мобільного зв'язку. Існує кілька основних методів прослуховування користувачів – активний та пасивний. Під активним методом розуміється пряме втручання в ефір [1,5]. Для цього необхідний спеціалізований технічний комплекс а також працівники, які мають достатній рівень знань у сфері зв'язку, для того щоб із ним працювати. Прослуховування такого типу вимагає близького розташування до об'єкта прослуховування (близько 500 м). Система активного прослуховування активно втручається в мережу GSM між стільниковим телефоном і базовою станцією. Таке обладнання, відоме під назвою IMSI-пастка, складається з передавача та приймача і симулює роботу базової станції GSM. По суті, це невелика базова станція GSM, яка примушує стільниковий телефон користуватися її послугами, а не справжньою базовою станцією. Вона може встановити номер телефону IMEI і номер SIM картки, вмикати і вимикати у телефоні різні послуги мережі GSM, вимикати шифрування GSM A5/1 в телефоні користувача, перехопити або сфальсифікувати вхідне/вихідне SMS повідомлення, і, навіть, «зламати» сам телефон, скопіювати наявну інформацію і впровадити в нього шкідливі програми та віруси.

Пасивний метод прослуховування вимагає спеціального обладнання та висококваліфікованих працівників. Сьогодні на різноманітних Інтернет-ресурсах можна придбати все необхідне для прослуховування абонентів на невеликій відстані. Принцип атаки такий: недалеко від об'єкта

розміщується пасивна система перехоплення GSM ефіру [3-4]. У момент виклику або підключення до мережі, сигнал, перехоплюється, розкодовується, а потім перенаправляється на базову станцію. У результаті такого втручання можна не тільки прослухати телефонну розмову, а також дізнатися IMEI, IMSI, TMSI ідентифікатори, номер вашої SIM-карти. Згодом цю інформацію можна використовувати для телефонних дзвінків від вашого імені, підробки сім-карти, отримання доступу до платіжних систем та ін.

Іншим способом прослуховувати є прослуховування із затримкою. Час затримки залежить від використовуваного оператором рівня шифрування [1].

Ще одним засобом прослуховування абонентів є встановлення на смартфон спеціального ПЗ. Проте, існує велика кількість програм, які дозволяють повідомляти конфігурацію поточного сеансу зв'язку, зокрема те, передається розмова у відкритому доступі чи із використанням алгоритму шифрування [6]. Однією із таких програм є GSM SpyFinder. Вона здатна захистити смартфон від різного типу шпигунського устаткування, зокрема від активного GSM перехоплювача з дешифратором A5, який може перехоплювати вхідні та вихідні GSM дзвінки і SMS з будь-яким типом шифрування в реальному часі [7-8]. Також додаток може захистити від 3G IMSI/IMEI/TMSI кетчера, який призначений для впливу на обраний телефон, щоб змусити його переключитися в режим GSM з метою перехоплення даних з такого телефону пасивним перехоплювачем. GSM Spy Finder дозволяє уникнути загроз, які спричиняють блокувальники стільникових телефонів (стільниковий брандмауер), для вибіркового або масового придушення GSM/UMTS цілей [1,5].

Як і будь-які технології, технологія GSM не є ідеальною та має певні недоліки, які можуть порушити конфіденційність інформації, яка передається засобами мобільного зв'язку, проте, використання наявного ПЗ дозволяє суттєво зменшити кількість таких порушень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Види прослуховування мобільних телефонів. URL: https://ssbb.com.ua/uk/news/vidi-prosluhovuvannya-mobilnogo-telefonu. (дата доступу: 5.03.2020 р.).
2. Зайцев А.П., Шелупанов А.А, Мещеряков Р.В., Скрыль С.В., Голубятников И.В. Технические средства и методы защити информации. Москва: «Машиностроение». 2009. 508 с
3. Хорев А. А. Защита информации от утечки по техническим каналам. М.: НПЦ «Аналитика», 2008 р. С. 436-440.
4. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Захист інформації від несанкціонованого копіювання шляхом прив'язки до унікальних параметрів вінчестера і використання ключа активації" / Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Заявка від 05.06.2018 р. №80958. Дата реєстрації 11.06.2018 р.
5. Хома В.В. Загрози інформаційній безпеці абонентів стаціонарних телефонних мереж – Вісник Національного університету "Львівська політехніка". – 2008.
6. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Програмний модуль ідентифікації користувача за відбитками пальців через смартфон з подальшою авторизацією" / Азарова А. О., Азарова Л. Є., Мисько Ю. О., Колган В. А. Заявка від 05.06.2018 р. №80951. Дата реєстрації 11.06.2018 р.
7. Свідоцтво про реєстрацію авторського права на твір №80464. Комп'ютерна програма „Мобільний додаток для захищеного передавання конфіденційних даних у смартфонах" / Азарова А. О., Азарова Л. Є., Бадя Ю. В. Заявка від 12.06.2018 р. №81238. Дата реєстрації 24.07.2018 р.
8. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Програмний модуль ідентифікації користувача за відбитками пальців через смартфон з подальшою авторизацією" / Азарова А. О., Азарова Л. Є., Мисько Ю. О., Колган В. А. Заявка від 05.06.2018 р. №80951. Дата реєстрації 11.06.2018 р.

Азарова Анжеліка Олексіївна, кандидат технічних наук, професор, заступник декана Факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва.

Блонський Владислав Олександрович, Вінницький національний технічний університет**,** м. Вінниця, факультет менеджменту та інформаційної безпеки, УБ-15б, vlados,blonskiy@gmail.com.

Гудзь Віталій Олександрович, Вінницький національний технічний університет**,** м. Вінниця, факультет менеджменту та інформаційної безпеки, УБ-15б, vitalik1211@ukr.net.

Anzhelika Azarova, PhD in technique, Professor, Deputy dean of the Faculty of management and information security by scientific work and international cooperation Vinnytsia National Technical University, Vinnytsia.

Vladyslav Blonskyi, Vinnytsia National Technical University, Vinnytsia, Department of Management and Security of Information Systems, vlados.blonskiy@gmail.com.

Vitalii Hudz, Vinnytsia National Technical University, Vinnytsia, Department of Management and Security of Information Systems, vitalik1211@ukr.net.