УДК 621.391

В.С. Бєлов [1]
С.О. Кирилюк [1]

Аналіз вразливостей стандарту GSM

[1]Вінницький національний технічний університет

Анотація.
Розглянуто та проведено аналіз вразливостей мережі мобільного зв'язку стандарту GSM на основі SS7.
Ключові слова: GSM, вразливість, відслідковування абонента, визначення місцезнаходження, безпека.

Abstract.
The vulnerability analysis of the GSM mobile communication network based on SS7 is considered and conducted.
Keywords: *GSM, vulnerability, tracking subscriber, location determination, security.*

Вступ

На сучасному етапі розвитку мережі мобільного зв'язку є найбільш активною частиною дуже важливої інформаційної інфраструктури і ключовим інструментом в багатьох сферах життя суспільства, від управління персональними банківськими рахунками до переговорів на рівні лідерів світових держав. Але не зважаючи на завірення в захищеності мобільного зв'язку, можна знайти не мало прикладів зворотного: в Інтернеті не один раз з'являлись записи приватних телефонних розмов міністрів, послів, військових, бізнесменів і інших людей, чий статус зазвичай асоціюється з підвищеними мірами безпеки.

Рівень безпеки всієї системи визначається рівнем найслабшої ланки. Зокрема, процес встановлення виклику в сучасних мобільних мережах заснований на технології SS7, в якій безпека протоколів зводилась до фізичного захисту вузлів і каналів зв'язку, а отримання доступу в мережу за допомогою несанкціонованого вузла було неможливо. Але пізніше було розроблено специфікацію SIGTRAN, яка дозволяє передавати повідомлення SS7 по IP-мережам. В результаті зловмисник має можливість безконтрольно посилати, перехвачувати і змінювати повідомлення протоколів SS7, здійснювати різні атаки на мобільні мережі та їх абонентів.

Основна частина

Перш ніж перейти до опису самих атак, нагадаємо про те, як влаштовані мережі мобільного зв'язку. Наприклад, у вас є номер типу +380972583658, це MSISDN (Mobile Subscriber Integrated Services Digital Number). Він не зберігається в SIM-карті, як багато хто думає. В SIM-картка зберігає інший ідентифікатор - IMSI (International Mobile Subscriber Identity), який передається в мережу тільки під час реєстрації абонента. Це 15-значне число виду 250115556667778, в якому 250 - код країни, 11 - код оператора, а інші 10 цифр - внутрішній унікальний номер даної SIM-карти (MSIN, Mobile Subscriber Identification Number). Саме IMSI використовується для ідентифікації абонента всередині мережі, тобто для здійснення будь-яких операцій з номером.

Інформація про відповідність IMSI і MSISDN зберігається в базі даних, що іменується HLR (Home Location Register). При цьому для кожного з сегментів мережі (комутаторів) використовується аналогічна база даних VLR (Visitor Location Register) - її відмінність полягає в тому, що дані в ній зберігаються тимчасово, копіюючи з HLR при появі абонента саме в цій частині мережі. В VLR також зберігаються дані про поточне місцезнаходження абонента,

настройки переадресації тощо. Всіма цими даними користується для своєї роботи комутатор, він же MSC (Mobile Switching Center).

Для проведення атак зловмиснику недостатньо встановити потрібне ПЗ, що моделює обладнання оператора. Потрібно ще й підключення в якості оператора, яке легко купити на чорному ринку: в ряді країн, де операторську ліцензію видають кому завгодно, подібний «бізнес» процвітає, а для успішної атаки не важливо, з якої країни ваш «оператор»: зловмисник заплативши за доступ до шлюзу може атакувати абонента в будь-якій точці світу.

Спочатку у зловмисника є тільки номер телефону (MSISDN). Щоб виконати будь-які дії з ним, потрібно отримати IMSI. Це можна зробити шляхом формування запиту на доставку SMS-повідомлення з зовнішньої «мережі», яка моделюється на комп'ютері. В цьому випадку домашня мережа повідомляє у відповідь на запит адресу MSC/VLR, якими в даний момент обслуговується абонент. При цьому відбувається і передача IMSI, оскільки він також необхідний для маршрутизації. Після цієї нехитрої процедури зловмисник вже має IMSI для управління параметрами «облікового запису» абонента, адреса HLR, в якому ці параметри зберігаються, а також в якій країні жертва зараз знаходиться.

Тепер зловмисник може отримати запит точного місця розташування абонента: атакуючий, знаючи поточний MSC/VLR, відправляє туди запит про те, якою базовою станцією (БС) обслуговується абонент з даним IMSI. У відповідь приходить унікальний ідентифікатор БС, за яким через відкриті бази даних можна дізнатися, де вона знаходиться, і з точністю до пари сотень метрів знайти абонента.

Також зловмисником може бути порушено доступність абонента. У HLR надсилається повідомлення про те, що абонент зареєструвався в роумінговій мережі. Передається IMSI і адреса нового MSC/VLR. Тепер жертві ніхто не зможе ні зателефонувати, ні відправити SMS тому, що домашня мережа переадресує запити де насправді абонента немає, при цьому абонент буде як і раніше зареєстрований в мережі і нічого не запідозрить. Крім того зловмисник може перенаправити всі дзвінки і повідомлення собі вказавши свій MSC/VLR - і весь трафік буде направлений йому. Наприклад, таким чином може бути зібрано одноразові SMS-паролі для двох факторної авторизації в різних сервісах, а це створює майже необмежені можливості для крадіжки грошових коштів та облікових записів. А також може бути просто прочитано все SMS-листування, причому жертва навіть не запідозрить, що за нею стежать. Справа в тому, що SMS вимагає від MSC/VLR підтвердження його доставки, і якщо його не відправляти, а замість цього перереєструвати абонента на його «справжній» MSC, то через кілька хвилин буде зроблена ще одна спроба доставки повідомлення і воно надійде адресату. Тобто один і той же SMS буде відправлено два рази: спочатку зловмиснику, потім жертві.

Як відомо, USSD-запити завжди працюють і в роумінгу, дозволяючи перевіряти баланс, підключати різні послуги і тарифні опції. Змоделювавши USSD-запит від VLR до HLR, можна, наприклад, ініціювати переказ коштів з одного рахунку на інший. У деяких операторів для підтвердження цієї операції використовується SMS-авторизація, але SMS зловмисник може перехопити, як описано вище.

Також за допомогою SS7 можна влаштувати справжню DoS-атаку на комутатор, яка призведе до неможливості приймати вхідні дзвінки у всіх абонентів, що знаходяться в зоні його обслуговування. Для цього потрібно знати, що при реєстрації в VLR виділяється тимчасовий роумінговий номер, який потрібен, щоб MSC знав, куди саме направляти виклик. Так ось, якщо масово відправляти запити на виділення роумінгових номерів, то їх кількість закінчиться, і «справжнім» абонентам ніхто не зможе додзвонитися через перевантаження комутатора.

Висновки

Рішення для захисту в основному зводяться до моніторингу атак для виявлення підозрілої активності по вищеописаним сценаріями - це дозволяє вибірково блокувати певні запити. Тим часом оператори намагаються не афішувати наявність вразливостей: на їх бізнес можливості злому практично не впливають, а абонентам можна порадити все-таки не вести по телефону конфіденційних переговорів і не покладатися на SMS для авторизації. Крім того, для подібних

цілей краще придбати окрему SIM-карту, номер якої не знатиме ніхто з вашого кола спілкування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Signaling Transport – The Internet Society [Електронний ресурс]. – 2007. – Режим доступу до ресурсу: http://datatrecker.ietf.org/wg/sigtran/documents/
2. SMS SS7 Fraud 3.1– GSM Association [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: http://www.gsma.com/newsroom/wp-counter/uploads/2012/12/IR7031.pdf
3. Как раскрыть местоположение мобильного абонента. [Електронний ресурс]. – Пузанков С., Positive Tehnologies, 2013 – Режим доступу до ресурсу: http://habrahabr.ru/company/pt/
4. Аналіз сайтів рухомої мережі GSM–1800 – О.В. Колісник, В.С. Бєлов – Матеріали міжнародної науково-практичної Інтернет-конференції Молодь в технічних науках: дослідження, проблеми, перспективи (МТН-2015). Україна, Вінниця, ВНТУ. [Електронний ресурс]. – 2015. – Режим доступу – http://inmad.vntu.edu.ua/portal/static/1AC7978B-3949-40AB-8C3E-A0C539CAFD50.pdf

Бєлов Володимир Сергійович – асистент кафедри телекомунікаційних систем і телебачення, Вінницький національний технічний університет, м. Вінниця, e-mail: belov@vntu.edu.ua

Кирилюк Сергій Олександрович – студент групи ТКТ-16мс, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, м. Вінниця, e-mail: kso1996.08@gmail.com.

Belov Vladimir – assistant of the Chair of Telecommunication Systems and Television, Vinnytsia National Technical University. Vinnitsa, e-mail: belov@vntu.edu.ua

Kyrylyuk Serhii - group TKT-16ms, The Faculty of Infocommunications, Radioelectronics and Nanosystems, Vinnytsia National Technical University, Vinnitsia, e-mail: kso1996.08@gmail.com.