УДК 621.391

АНАЛІЗ РІВНЯ БЕЗПЕКИ МЕРЕЖ СИГНАЛІЗАЦІЇ SS7

Романов О.І., Осокін М.Г.
Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: a_i_romanov@ukr.net, nikitos397@gmail.com

Security level analysis of SS7 signaling networks

The publication examines the risks associated with the vulnerability of the SS7 system, which leads to the leakage of information when using mobile and Internet services. An analysis of attacks and the effectiveness of using two-factor authorization for information security has been carried out.

Сьогодні більшість людей користуються мобільними та інтернет-послугами, зокрема соціальними мережами і поштовими скриньками. Для кожного важлива конфіденційність його листувань і інформації, в чому допомагає двофакторна авторизація [1].

Принцип отримання інформації зловмисником наступний. Необхідно знайти SS7-шлюз і підключитись до нього. Для цього існують багато способів потрапити в мережу через зламане операторське обладнання, GGSN або фемтостільники [2].

Далі, маючи доступ до SS7 і знаючи номер телефону жертви, можна підслухати розмову, визначити місце розташування людини, перехопити SMS для доступу до мобільного банку, відправити USSD-команду на платний номер і здійснити інші атаки.

Вразливості сигнальних мереж дозволяють здійснювати найрізноманітніші атаки. За допомогою команд SS7 MAP можна віддалено розблокувати стільникові телефони. Незахищеність SS7 загрожує не тільки користувачам мобільних телефонів, але і зростаючій екосистемі промислових і IoT-пристроїв, від банкоматів до GSM-систем контролю за роботою газових станцій. У подібних умовах забезпечення безпеки мереж SS7 - одна з першочергових задач при побудові комплексного захисту мобільного зв'язку.

Розглянемо дані, які зібрані спеціалістами Positive Technologies про безпеку мереж різних операторів станом на 2015 рік [3].

Загрози з боку потенційного порушника щодо мереж SS7 і абонентів мобільних операторів можна розділили на три класи:

- Шахрайство;
- Витік чутливої інформації;
- Збої в роботі.

Серед загроз інформаційної безпеки, що відносяться до класу витоку даних, можна виділити основні п’ять:

- Прослуховування дзвінків;
- Перехват SMS-повідомлень;
- Визначення місцезнаходження абонента в реальному часі;
- Крадіжка інформації про абонента.

У всіх мережах SS7, що увійшли до вибірки, були можливі: крадіжка інформації про абонента, перехоплення SMS, визначення місця розташування абонента.

Розглянемо основні і найефективніші методи атаки:

- Send Routing Info;
- Send Routing Info For SM;
- Send Routing Info For LCS;
- Send IMSI.

Відсоток успіху атак представлений на рис.1

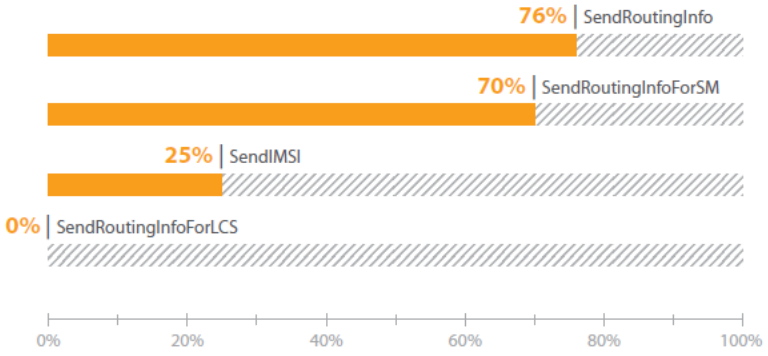

Рис. 1. Методи і доля успішних атак

Send RoutingInfo заснований на використанні вразливості, пов'язаної з відсутністю фільтрації невикористовуваних сигнальних повідомлень. Send Routing Info - повідомлення протоколу MAP, яке використовується про вхідний голосовий виклик і служить для запиту маршрутної інформації для локалізації абонента. Використовуючи даний метод, порушник може не тільки отримати інформацію про абонента, але і визначити його поточне місце розташування.

Send Routing Info For SM - повідомлення протоколу MAP, яке використовується при вхідному SMS-повідомленні і служить для запиту маршрутної інформації для локалізації абонента-отримувача. Це повідомлення повинно маршрутизироватися на обладнання SMS Home Routing, якщо воно встановлено в мережі оператора.

Send IMSI - повідомлення протоколу MAP, яке використовується для запиту ідентифікатора IMSI абонента за його телефонним номером. В даний час дане повідомлення практично не використовується операторами мобільного зв'язку, однак обладнання часто все ж обробляє його, відповідно до стандарту 3GPP.

Send Routung Info For LCS - повідомлення протоколу MAP, яке використовується в сервісах, що здійснюють розташування абонента, і служить для запиту маршрутної інформації. При нормальному режимі функціонування це повідомлення повинно передаватися тільки між елементами своєї мережі.

Розглянемо приклад атаки за допомогою Send Routing Info і фіктивного біллінгу. Атакуючий проникає в мережу сигналізації SS7, в каналах якої відправляє службове повідомлення Send Routing Info For SM (SRI4SM),

вказуючи в якості параметра, телефонний номер абонента А, що атакується. У відповідь домашня мережа абонента А посилає атакуючому деяку технічну інформацію: IMSI (міжнародний ідентифікатор абонента) і адреса комутатора MSC, який зараз обслуговує абонента.

Далі атакуючий за допомогою повідомлення Insert Subscriber Data (ISD) впроваджує в базу даних VLR оновлений профіль абонента, змінюючи в ньому адресу білінгової системи на адресу своєї, псевдобіллінговой системи.

Потім, коли атакований абонент здійснює вихідний дзвінок, його комутатор звертається замість реальної білінгової системи до системи атакуючого, яка дає комутатору директиву перенаправити виклик на третю сторону, знову ж підконтрольну зловмисникові.

На цій третій стороні збирається конференц-виклик з трьох абонентів, два з яких є реальними (викликає А і викликається В), а третій впроваджений зловмисником несанкціоноване і має можливість слухати і записувати розмову.

Рекомендовані заходи для захисту:

- настройки конфігурації,
- впровадження додаткових засобів захисту,
- комбінацію цих двох методів.

Більшість недоліків, що дозволяють визначити місце розташування абонента, а також реалізувати крадіжку даних, можуть бути усунені в результаті зміни конфігурації мережевого обладнання [4]. Наприклад, якщо встановити заборону на обробку повідомлень Any Time Interrogation і Send IMSI на HLR.

Архітектурні проблеми протоколів і систем, що дозволяють здійснювати відмову в обслуговуванні, перехоплення SMS-повідомлень, перенаправлення викликів і прослуховування дзвінків, а також зміна профілю абонента, можуть бути вирішені шляхом фільтрації небажаних повідомлень (таких як Send IMSI, Send Routung Info For LCS, Send Routing Info). Необхідно реалізувати фільтрацію таким чином, щоб відсікалися тільки небажані повідомлення, які використовуються в рамках атак.

Таким чином, для забезпечення надійності систем SS7 необхідно використовувати двофакторну авторизацію в сукупності з сучасними методами захисту, уважно слідкувати за станом обладнання і його програмним забезпеченням.

Література

1. Signal System Number 7 (SS7) [Електронний ресурс] – Режим доступу: http://4g5gworld.com/wiki/signaling-system-number-7-ss7
2. Kim Zetter, The critical hole at the heart of our cell phone networks [Електронний ресурс] – Режим доступу: https://www.wired.com/2016/04/the-critical-hole-at-the-heart-of-cell-phone-infrastructure/
3. Positive Technologies, Эксперты Positive Technologies комментируют скандал со взломом украинских операторов связи [Електронний ресурс] – Режим доступу: https://www.securitylab.ru/news/454289.php
4. Романов О.І., Гордашник Є.С. Аналіз і класифікація атак в мережах IP-телефонії на базі SOFTSWITCH CLASS V. Матеріали десятої МНТК «Проблеми телекомунікацій», 2016 р. С 170-173.