ВРАЗЛИВОСТІ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ НА ОСНОВІ ПРОТОКОЛУ SS7

Барсук А.Т.
Науковий керівник – проф. Олейніков А.М.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. КРіСТЗІ, тел. (057) 702-14-30)
e-mail: andrii.barsuk@nure.ua

SS7 hack is the process of getting calls or sms for a subscriber, getting on another mobile number or in an application. These days many applications uses confirmation of a user identity from sms or voice call. . If some how call and sms routed to another number then its possible to hack. In this ss7 hack tutorial, the ss7 protocol and call flows will be explained.

SS-7 (система сигналізації №7) – система, заснована на використанні загального каналу сигналізації і придатна для застосування в мережах різної конфігурації. В телефонії сигналізацією називають передачу керуючої інформації для встановлення/роз'єднання з'єднань «точка-точка». Зараз є обов'язковою до застосування в телефонних мережах загального користування, ISDN, мережах стільникового зв'язку, інтелектуальних мережах та ін. Система SS7 має модульну структуру і складається з двох основних частин: підсистеми передачі повідомлень (МРТ) і різних підсистем користувачів, структура і характеристики яких залежать від виду переданої інформації (мова, дані та ін.).

Для того щоб здійснити атаку на абонента потрібно підключиться до сигнальної мережі SS7 і відправити службову команду Send Routing Info для SM (SRI4SM) в мережевий канал, вказуючи номер телефону абонента що атакується в якості параметра. Домашня абонентська мережа відправляє у відповідь таку технічну інформацію: IMSI (International Mobile Subscriber Identity) і адреса MSC – унікального коду комутатору стільникового оператору, за яким в даний час надаються послуги передплатнику.

Після цього змінюється адреса білінгової системи в профілі абонента на адресу своєї власної псевдобіллінговой системи (наприклад, повідомляє, що абонент прилетів на відпочинок і в роумінгу зареєструвався на новій білінговій системі). Як відомо, ніяку перевірку така процедура не проходить. Далі атакуючий вводить оновлений профіль в базу даних VLR через повідомлення «Insert Subscriber Data» (ISD).

Коли абонент здійснює вихідний дзвінок, його комутатор звертається до системи зловмисника замість фактичної білінгової системи. Система зловмисника відправляє комутатора команду, що дозволяє перенаправити виклик третій стороні, яку контролює зловмисник.

У сторонньому місці встановлюється конференц-зв'язок з трьома передплатниками, два з них є реальними (абонент А і абонент В), а третій

вводиться зловмисником незаконно і здатний прослуховувати і записувати розмову.

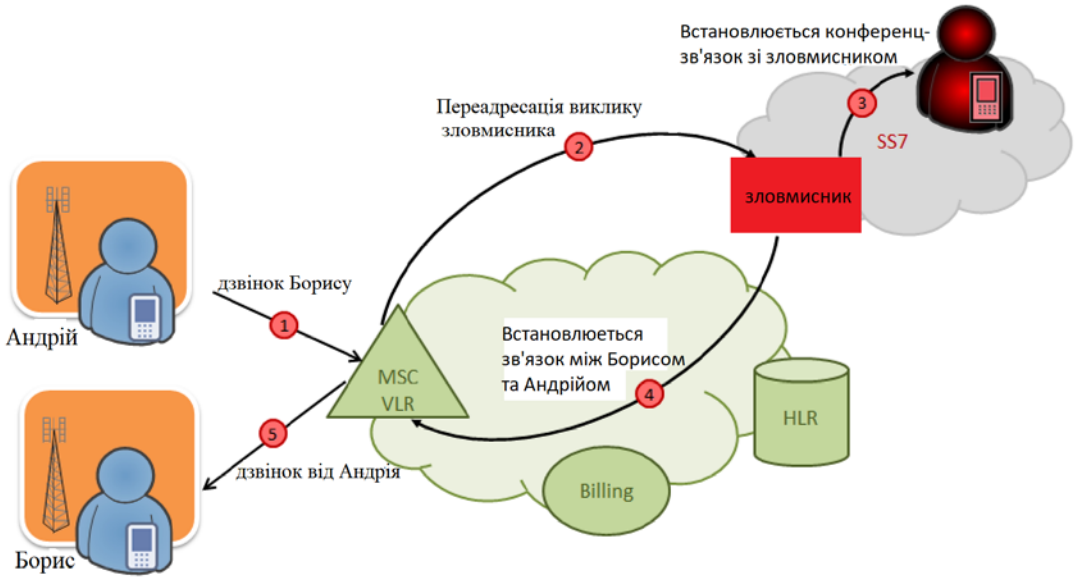

Рисунок 1 – Схема перехоплення голосових і SMS-повідомлень.

Відповідним чином можливо отримати і SMS абонента що атакується. Маючи доступ до псевдобіллінговой системи, на яку вже зареєструвався наш абонент, можна отримати будь-яку інформацію, яка приходить або йде з його телефону.

Доступ продають в даркнеті, а при бажанні можна знайти і безкоштовно. Така доступність обумовлена тим, що в мало розвинутих державах отримати статус оператора дуже просто, відповідно і отримати доступ до SS7 хабам. Так само присутні недобросовісні працівники у операторів.

Перелік посилань:

1. Атака на протокол SS7: как перехватить чужие звонки и SMS [Электронный ресурс] – Режим доступа: https://networkguru.ru/ataka-na-protokol-ss7/.

2. Система сигнализации 7 в телефонии [Электронный ресурс] – Режим доступа: https://translate.academic.ru/SS7/en/ru/

3. Взлом мобильной связи через SS7: перехват SMS, слежка и прочее [Электронный ресурс] – Режим доступа: https://tgraph.io/Vzlom-mobilnoj-svyazi-cherez-SS7-perehvat-SMS-slezhka-i-prochee-08-19