www.volsu.ru

ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.4.1

УДК 004.942
ББК 32.973.5

ПРОТОКОЛ SS7 И БЕЗОПАСНОСТЬ МОБИЛЬНОЙ СЕТИ

Кристина Петровна Гужаковская

Кандидат физико-математических наук,
доцент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Юрий Петрович Умницын

Доцент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Статья посвящена рассмотрению GSM сетей сотовой связи, которые играют важную роль в современном обществе, внося новые формы диалога и общения в современном мире. Показано, что эти сети играют двоякую роль в обществе: могут предоставлять средство для коммуникации с человеком, находящимся в любой точке земного шара, и могут являться средством для похищения конфиденциальных данных злоумышленником из-за устаревшей технологии для настройки телефонных станций, созданной еще в 1970-х годах.

Ключевые слова: уязвимости протокола SS7, GSM-связь, IMSI, MSISDN, MSC/VLR.

В настоящее время смартфоны находятся во владении практически у каждого человека. Чаще всего они используются как источник развлечений в социальных сетях или как устройство для работы. По своему функционалу смартфон стал близок к персональному компьютеру. И мы, работая с этим устройством изо дня в день, стали задумываться, насколько наш гаджет защищен от различных нападений со стороны злоумышлен-

ника. Ведь мы живем во времена весьма серьезного роста технологических возможностей, когда взломать телефон не составляет особого труда. В этой статье изложена технология взлома смартфона через уязвимость SS7 (системы сигнализации по общему каналу № 7).

Многие задаются вопросом, каким же образом злоумышленник сможет получить конфиденциальные данные, если телефон будет надежно защищен всеми известными средствами защиты? Для злоумышленника это не окажется проблемой, если он не будет проходить системы защиты на телефоне, а пойдет через уязвимость в телекоммуникационной системе, которая позволяет взломать телефон из-за уязвимости протокола SS7 (Signaling System №7 – Система Сигнализации по Общему Каналу № 7).

Как известно, протокол SS7 – это средство, состоящее из набора сигнальных телефонных протоколов (рис. 1), используемых для обмена информацией между элементами мобильной сети [10].

Как видно из рисунка, стек протокола SS7 разделен на уровни, которые можно сопоставить с моделью OSI. MTP Layer 1 сопоставляется с первым уровнем, MTP Layer 2 – со вторым, MTP Layer 3 – с третьим, и так далее.

MTP (Message Transfer Part – Перенос Части Сообщения) – это система, включающая в себя все уровни MTP стека SS7. Она отвечает за гарантированную доставку сообщения сетевой сигнализации между цифровыми станциями. MTP передает сообщения без потерь, дублирований, искажений и нарушений последовательности.

MTP Layer 1 – это звено, используемое для передачи информации путем преобразования ее в поток битов между двумя пунктами сигнализации.

MTP Layer 2 – это звено, используемое для проверки ошибок и правильности последовательностей сообщения в случае конфликтов на этом уровне сообщение отправляется повторно.

MTP Layer 3 – это звено, используемое для маршрутизации сообщения и переадресации трафика от неисправных звеньев.

Протокол ISUP (ISDN User Part) служит для управления вызовами между устройствами телефонной сети.

Протокол SCCP служит для взаимодействия сервисных узлов. Он дает сведения о состоянии подсистем и опирается на протокол MTP Layer 3 для маршрутизации и поиска ошибок.

В TCAP размещается информация о маршрутах, используется протоколом ISUP для адресации вызовов; также этот протокол применяется для указания того, кто будет оплачивать счет за разговор.

Протокол SS7 был реализован в 1970-х гг. для определения и соединения стационарных

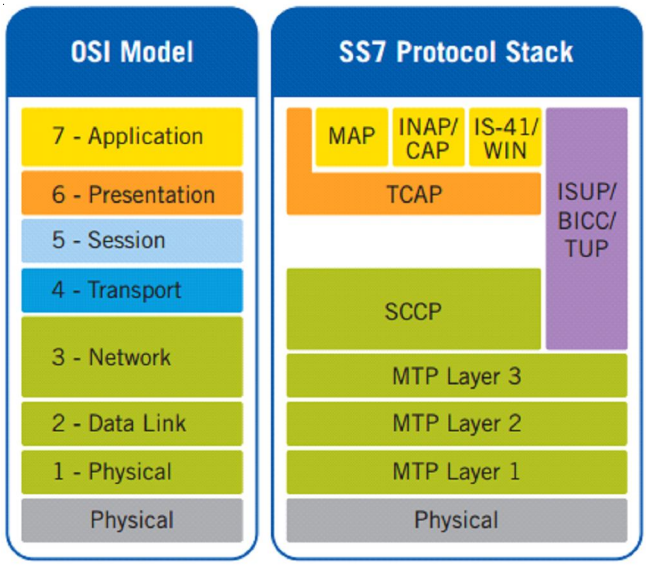

Рис. 1. Уровни протокола сигнализации по общему каналу № 7 [3]

телефонов между сетями, сейчас он используется для определения стоимости за звонок и SMS. В протоколе использовался физически недоступный пользователям канал, по которому передавались команды, устанавливающие телефонные соединения. В то время разработчики полагали, что протокол надежно защищен и никто, кроме персонала, доступ иметь к нему не будет, так как физический канал отделен от голосового канала. Поэтому для сигнального трафика не применялось шифрование и прочие меры защиты. Но время идет, технологии развиваются, и в 2000-х гг. был разработан SIGTRAN-протокол (Signaling Transport – Передача сигнала) [9]. Он поддерживает те же функции управления вызовами, что и SS7, но еще имеет возможность адресации через интернет-протокол (IP) и передачу данных по протоколу SCTP, который принадлежит транспортному уровню в компьютерной сети и обеспечивает гарантированную доставку данных приложений по IP-сетям. Это позволило получить доступ к физическому каналу. Так как шифрование не применялось, отличить настоящие команды от команд злоумышленника очень сложно, ведь оборудование будет исправно выполнять все получаемые команды, и оно не проверяет источники пакета, потому что системы проверки не были реализованы ввиду невозможности проникнуть в физический канал. Теперь для взлома достаточно наличия компьютера с интернет-соединением и установленным программным обеспечением для формирования и отправки SS7 пакетов и SS7-шлюза [5]. Доступ к шлюзу обеспечить несложно, так как во многих странах его может получить любой желающий на черном рынке у действующего оператора или через взломанное операторское оборудование. Когда все вышеперечисленное сделано, можно реализовать атаку «человек посередине» [6].

Реализация атаки через уязвимость SS7-протокола

Чтобы успешно реализовать данную атаку, необходимо получить IMSI (International Mobile Subscriber Identity – Международная идентификация мобильного абонента) – пятнадцатизначное число, которое присваивается индивидуально каждой SIM-карте и хранится на ней. Первые три цифры выделены для кода стран, следующие две определяют коды мобильной сети, а оставшиеся – это идентификатор пользователя. Получить его можно, если известен номер мобильного телефона MSISDN (Mobile Subscriber Integrated Services Digital Number – Цифровой номер с интегрированными услугами мобильного абонента), он связан с IMSI и находится в абонентской базе данных сотового оператора HLR (Home Location Register – Главная регистрация местоположения). MSISDN необходим для получения звонков и идентификации абонента при получении услуг. Для получения IMSI необходимо сделать фальшивую сеть при помощи компьютера с соответствующим программным обеспечением и отправить SMS на номер абонента (MSISDN). Обычно чтобы SMS добралось до получателя, ему необходимо построить маршрут до места нахождения абонента. Поэтому база данных HLR, в которой на данный MSISDN сопоставляется соответствующий IMSI, отправит нам адрес коммутатора MSC/VLR, на котором сейчас обслуживается абонент, и IMSI его SIM-карты. MSC (Mobile Switching Center – Центр мобильной коммутации) – это телефонная станция, в задачи которой входит коммутация каналов, отслеживание местоположения абонента для направления к нему звонков, SMS и предоставления сервисов GSM. На практике данный узел часто совмещают с VLR (Visitors Location Register – Регистр местонахождения посетителей) – базой данных, хранящей всю информацию о пользователях, временно зарегистрированных в зоне действия данного коммутатора [8].

Определение местоположения абонента

Как известно, вся сотовая сеть разделена на так называемые соты – зоны действия базовых станций, объединенные между собой центрами коммутации (см. рис. 2).

Так как сотовая связь охватывает практически все уголки нашей планеты и каждый человек обслуживается той или иной базовой станцией, в пределах которой сейчас находится, то если узнать расположение этой станции,

можно приблизительно узнать местонахождение человека. Необходимо на найденный нами адрес коммутатора MSC/VLR отправить запрос на определение текущей базовой станцией, обслуживающей IMSI, нашей цели. В ответ мы получим идентификатор базовой станции, по которому определим ее местонахождение, а следовательно, и абонента.

Перехват сообщений абонента

Для этого необходимо передать IMSI жертвы и адрес злоумышленника MSC/VLR в HLR [2]. В этом случае все сообщения, поступающие абоненту, будут приходить к злоумышленнику. Чтобы абонент не смог заподозрить, что за ним следят, когда он будет отправлять сообщение другому абоненту, необходимо сделать переопределение на реальный коммутатор MSC, и сообщение придет к злоумышленнику, а после к абоненту, которому посылалось SMS.

Также злоумышленник сможет взломать различные мессенджеры, такие как Telegram, WhatsApp, ВКонтакте, перехватив пароли авторизации через SMS.

Перехват разговора абонента

Для этого злоумышленнику необходимо во временно зарегистрированной базе VLR изменить адрес биллинга абонента и перехватить запрос на тарификацию исходящего вызова (биллинговая система (от англ. billing – выписывание счета) – система, для вычисления стоимости услуг [7]). Так можно узнать номер, к которому обращается абонент. Потом нужно сделать переадресацию вызова на MSISDN злоумышленника и сделать конференцсвязь с настоящим абонентом. Теперь можно незаметно прослушивать беседу, так как все эти операции проходят очень быстро.

Атаки через SS7 перспективны для осуществления злоумышленниками [1]. Ведь атакующему не обязательно находиться поблизости от абонента, и атака может производиться из любой точки на планете. Поэтому вычислить злоумышленника практически невозможно, через данную уязвимость может быть взломан практически любой телефон в мире. Подслушать разговоры, перехватить SMS, получить доступ к мобильному банку, социальным сетям не составит особого труда из-за уязвимости в телефонной инфраструктуре SS7, по которой передаются служебные команды сотовых сетей. Из-за того, что уязвимость с протоколом SS7 находится в ведении оператора, от такой атаки защититься самостоятельно не получится. Пока сотовые операторы не смогут отказаться от этой технологии, данная угроза в области информационной безопасности будет оставаться актуальной.

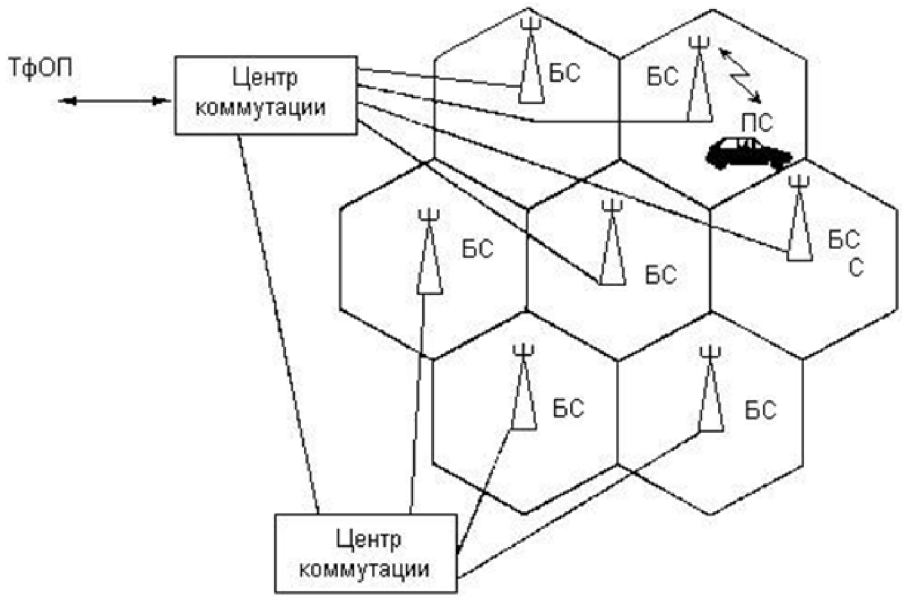

Рис. 2. Строение сотовой сети [4]

СПИСОК ЛИТЕРАТУРЫ

1. Атакуем SS7: анализ защищенности сотовых операторов в 2015 году. – Электрон. дан. – Режим доступа: http://www.securitylab.ru/analytics/483082.php (дата обращения: 28.02.2017). – Загл. с экрана.

2. Объединение мобильной и фиксированной связи: как это работает изнутри. – Электрон. дан. – Режим доступа: https://habrahabr.ru/company/beeline/blog/138620/ (дата обращения: 28.02.2017). – Загл. с экрана.

3. Рисунок стека протокола SS7. – Электрон. дан. – Режим доступа: https://im0tubru.yandex.net/i?id=ee466ce24c456ea61bd7602f304995fd&n=33&h=215&w=232 (дата обращения: 28.02.2017).

4. Рисунок строения сотовой связи. – Электрон. дан. – Режим доступа: https://yandex.ru/images/search?p=3&text=стек%20протокола%20ss7&img_url=http%3A%2F%2Fwww.gl.com%2Fimages%2Fmtp2-simulator-web-protocolstack.gif&pos=108&rpt=simage (дата обращения: 28.02.2017).

5. Сотовые сети: взлом проще простого. – Электрон. дан. – Режим доступа: https://blog.kaspersky.ru/hacking–cellular–networks/9862/ (дата обращения: 28.02.2017).

6. Фишер, Д. Что такое «человек посередине»? / Д. Фишер. – Электрон. дан. – Режим доступа: https://blog.kaspersky.ru/chto–takoe–chelovek–poseredine/740/ (дата обращения: 28.02.2017).

7. Характеристика и назначение биллинговых систем. – Электрон. дан. – Режим доступа: https://studopedia.su/2_28017_harakteristika-i-naznachenie-billingovih-sistem.html (дата обращения: 29.02.2017).

8. Центр мобильной коммутации. – Электрон. дан. – Режим доступа: https://ru.wikipedia.org/wiki/Базовая_сеть_GSM#.D0.A6.D0.B5.D0.BD.D1.82.D1.80_.D0.BC.D0.BE.D0.B1.D0.B8.D0.BB.D1.8C.D0.BD.D0.BE.D0.B9_.D0.BA.D0.BE.D0.BC.D0.BC.D1.83.D1.82.D0.B0.D1.86.D0.B8.D0.B8 (дата обращения: 28.02.2017). – Загл. сэкрана.

9. SI3000 CS. Описание системы. – Электрон. дан. – Режим доступа: http://ftp.ufanet.ru/pub/boco/private/SI3000/B_SYSTEM_DESCRIPTION.PDF (дата обращения: 28.02.2017). – Загл. с экрана.

10. Siemens. Информация. Сигнализация. Система Сигнализации по Общему Каналу № 7 : A30808-X2798-X8-1-5618. С. 10. – Электрон. текстовые дан. – Режим доступа: http://mtusii.narod.ru/files/lecture/A0021510_CC7_R.PDF (дата обращения: 27.02.2017). – Загл. с экрана.

REFERENCES

1. *Atakuem SS7: analiz zashchishchennosti sotovykh operatorov v 2015 godu* [We Attack SS7: Analysis of Cellular Operators Security in 2015]. URL: http://www.securitylab.ru/analytics/483082.php (accessed 28 February 2017).

2. *Obyedinenie mobilnoy i fiksirovannoy svyazi: kak eto rabotaet iznutri* [Combining Mobile and Fixed Communications: How It Works from the Inside]. URL: https://habrahabr.ru/company/beeline/blog/138620/ (accessed 28 February 2017).

3. *Risunok steka protokola SS7* [Picture of the SS7 Protocol Stack]. URL: https://im0tubru.yandex.net/i?id=ee466ce24c456ea61bd7602f304995fd&n=33&h=215&w=232 (accessed 28 February 2017).

4. *Risunok stroeniya sotovoy svyazi* [Drawing of the Structure of Cellular Communication]. URL: https://yandex.ru/images/search?p=3&text=stek%20protokola%20ss7&img_url=http%3A%2F% 2Fwww.gl.com%2Fimages%2Fmtp2-simulator-web-protocolstack.gif&pos=108&rpt=simage (accessed 28 February 2017).

5. *Sotovye seti: vzlom proshche prostogo* [Cellular Networks: Hacking is Easy]. URL: https://blog.kaspersky.ru/hacking–cellular–networks/9862/ (data obrashcheniya: 28.02.2017).

6. Fisher D. *Chto takoe «chelovek poseredine»?* [What Is a “Man in the Middle”?]. URL: https://blog.kaspersky.ru/chto–takoe–chelovek–poseredine/740/ (accessed 28 February 2017).

7. *Kharakteristika i naznachenie billingovykh sistem* [Characteristics and Purpose of Billing Systems]. URL: https://studopedia.su/2_28017_harakteristika-i-naznachenie-billingovih-sistem.html (accessed 29 February 2017).

8. *Tsentr mobilnoy kommutatsii* [Mobile Switching Center]. URL: https://ru.wikipedia.org/wiki/Bazovaya_set’_GSM#.D0.A6.D0.B5.D0.BD.D1.82.D1.80_.D0.BC.D0.BE.D0.B1.D0.B8.D0.BB.D1.8C.D0.BD.D0.BE.D0.B9_.D0.BA.D0.BE.D0.BC.D0.BC.D1.83.D1.82.D0.B0.D1.86.D0.B8.D0.B8 (accessed 28 February 2017).

9. *SI3000 CS. Opisanie sistemy* [SI3000 CS. Description of the System]. URL: http://ftp.ufanet.ru/pub/boco/private/SI3000/B_SYSTEM_DESCRIPTION.PDF (accessed 28 February 2017).

10. *Siemens. Informatsiya. Signalizatsiya. Sistema Signalizatsii po Obshchemu Kanalu № 7: A30808-X2798-X8-1-5618* [Siemens. Information. Signaling. Signaling System on Common Channel No. 7: A30808-X2798-X8-1-5618]. URL: http://mtusii.narod.ru/files/lecture/A0021510_CC7_R.PDF (accessed 27 February 2017).

PROTOCOL SS7 AND THE SECURITY OF MOBILE NETWORKS

Kristina P. Guzhakovskaya

Candidate of Sciences (Physics and Mathematics),
Associate Professor of Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Yuriy P. Umnitsyn

Associate Professor of Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The paper considers Global System for Mobile Communications, which plays the important role in contemporary society and carries new forms of dialog in the modern world. It is shown, that GSM-nets play two roles: firstly, they serve as communication tools for people who are in any point of world, and secondly, they can be used as tools for confidential data theft due to the old technology for telephone exchange setting, created as early as in the 1970s.

Attacks using SS7 are often executed by hackers. After all, the attacker does not have to be close to the subscriber, and the attack can be made from anywhere on the planet. Therefore, to calculate the attacker is almost impossible, through this vulnerability can be hacked through almost any phone in the world. It will not be difficult to eavesdrop on conversations, intercept SMS, get access to the mobile Bank, social networks because of the vulnerability in the SS7 telephone infrastructure, through which service commands of cellular networks are transmitted. Due to the fact that the vulnerability with the Protocol SS7 is on the side of the operator, protection from such an attack is impossible. Until mobile operators are able to abandon this technology, this threat in the field of information security will remain relevant.

Key words: vulnerabilities of SS7 protocol, GSM communication, IMSI, MSISDN, MSC/VLR.