УДК 621.391

Анализ уязвимости сети SIP фрод-угрозам по результатам тестирования оборудования действующей сети

А.М. Морозов [1]

[1] МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Проведен анализ риска информационной безопасности при реализации некоторых из фрод-угроз. Разработаны соответствующие алгоритмы атак злоумышленника и предложены способы защиты от них. Результаты получены с помощью тестирования, проведенного на стенде оборудования одного из российских операторов связи.

Email: a.m.morozov@gmail.com

Ключевые слова: *информационная безопасность, сеть SIP, оператор связи; фрод-угрозы, fraud, MIDM, man-in-the-middle, INVITE, SIP-access, SIP-trunk.*

IP-телефония или передача голосовых данных по сетям IP (Voice over IP — VoIP) — это технология с использованием IP-сети в качестве основного средства передачи данных. В сети VoIP принята выделенная от транспортного потока сеть сигнализации. Из нескольких созданных систем сигнализации для VoIP по выполнению функций установления, управления и разъединения соединения наиболее перспективным является протокол инициирования сеанса связи SIP (Session Initiation Protocol), разработанный инженерной группой Интернет IETF. Для транспортировки мультимедийных данных медиапотока (аудио, видео, текст, факс) в реальном масштабе времени между участвующими в сеансе связи пользователями VoIP используется транспортный протокол реального масштаба времени RTP (Real-Time Transport Protocol). Далее такие сети VoIP будем называть по протоколу сигнализации сетями SIP. Благодаря мобильности пользователя эти сети стали составлять конкуренцию сетям мобильной связи.

Как отмечается в работе [1] со ссылкой на данные Ассоциации CFCA (Communication Fraud Control Association) по контролю за угрозой fraud (фрод — использование услуг связи без их оплаты), потери операторов связи во всем мире составляют бóльшую долю от их общих доходов. Это относится ко многим типам сетей связи, причем такие потери операторов от фрод-угроз в сетях передачи данных по сетям IP выше, чем во многих сетях связи других типов. По данным CFCA за 2011 г., общие потери операторов связи России от фрода значительно ниже в сравнении с потерями операторов связи других регионов мира. В то же время, согласно данным этой Ассоциации за 2011 г., российские операторы связи в международном исследовании по проблемам мошенничества в телекоммуникационной индустрии

принимали участие меньше всех — 1,7 % (для сравнения операторы связи стран Западной и Восточной Европы — соответственно 25,9 и 6,9 %, стран Африки — 5,2 %). Поэтому актуальным является проведение испытаний на оборудовании действующей российской сети SIP в целях обнаружения уязвимостей в системе, подвергающейся фрод-угрозам.

Данная работа посвящена анализу риска информационной безопасности (ИБ) некоторых из фрод-угроз по результатам такого тестирования, проведенного на стенде оборудования одного из российских операторов. Под риском ИБ рассматривается характеристика последствий реализации фрод-угроз в сети SIP [2]. При этом учитывалось, что одним из наиболее чувствительных к угрозам фрода является участок взаимодействия разных операторов связи и в первую очередь операторами разных стран. Широкое применение на сетях операторов связи получили так называемые пограничные контроллеры сессий (Session Border Controller — SBC). SBC размещается на границе сети оператора связи, транслирует сигнальный поток и медиа-поток, обеспечивая единую точку входа-выхода операторской сети, и реализует широкий спектр функций контроля безопасности связи (сокрытие топологии сети оператора связи, защиту от угрозы «анализ трафика», контроль обмена сигнальными сообщениями, фильтрацию трафика на разных уровнях и др.).

Схемы моделирования каналов и имитация атак злоумышленника. В современных сетях связи протокол SIP применяется в двух вариантах взаимодействия: взаимодействие программного коммутатора софтсвич (softswitch) и абонентского терминала (на участке от абонентского устройства до программного коммутатора); взаимодействие между двумя программными коммутаторами softswitch для обеспечения межстанционного взаимодействия (на участке программный коммутатор — программный коммутатор), где они реализуют функцию маршрутизации вызовов в сети. Схема взаимодействия программного коммутатора софтсвич (softswitch) и абонентского терминала получила название SIP-access. Схемы межстанционного взаимодействия с использованием протокола SIP получили название SIP-trunk. Особенностью схемы SIP-trunk является невозможность применения механизма авторизации (authorization), предусмотренной протоколом SIP, при организации SIP-соединения между двумя программными коммутаторами, что создает предпосылки для реализации атак злоумышленника.

Тестирование проводилось на следующих двух схемах.

1. Схема, моделирующая взаимодействие двух операторов сетей связи по протоколу SIP. Между софтсвичами (ssw1 и ssw2) операторов 1 и 2 организован SIP-trunk. Стык сетей двух операторов защищен с помощью SBC (рис. 1). Участок сети между SBC операторов (на схеме обозначен как Internet) является незащищенным. На рисунке также указаны вариант сигнального обмена между софтсвичами и

направление медиа-потоков при установлении сессии (dialog 1) между абонентами A и B (абонент A оператора 2 вызывает абонента B оператора 1).

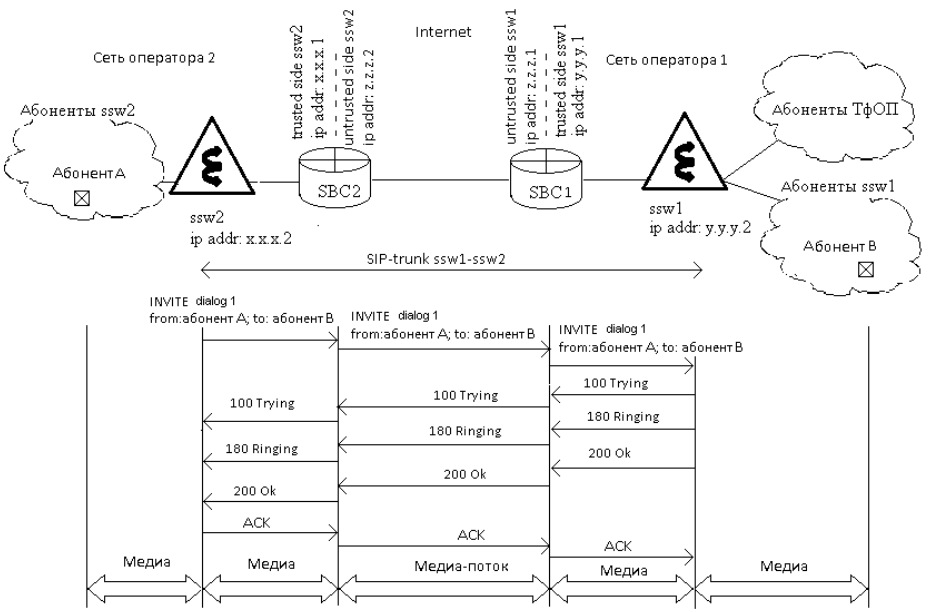

Рис 1. Схема моделирования канала взаимодействия между двумя операторами связи (SIP-trunk)

2. Схема, моделирующая организацию абонентского SIP-доступа (SIP-access) к софтсвичу оператора через незащищенные сети (рис. 2). Стык сети оператора с внешними сетями (на схеме Internet) защищен с помощью SBC. На схеме указаны сигнальный обмен SIP-абонент — софтсвич оператора и направления медиа-потоков при установленном соединении. В данной схеме используется механизм авторизации (authorization — определение полномочий) сообщений запроса на установление соединения сессии (INVITE).

В процессе тестирования на схемах моделирования проводилась имитация атак злоумышленника «человек посередине» MIDM (man-in-the-middle). Такой вид атак в сети SIP описан во многих публикациях зарубежных авторов (например, [3]).

На всех иллюстрациях данной работы trusted side и untrusted side означают соответственно участки сети, контролируемые и неконтролируемые оператором (подверженные атаке участки сети). Далее рассмотрены три разработанных алгоритма таких атак, для некоторых из них приведены меры защиты.

Перехват и модификация сообщения INVITE от легитимного пользователя. При атаке данного вида используется возможность терминала SIP одновременно поддерживать более одной активной сессии.

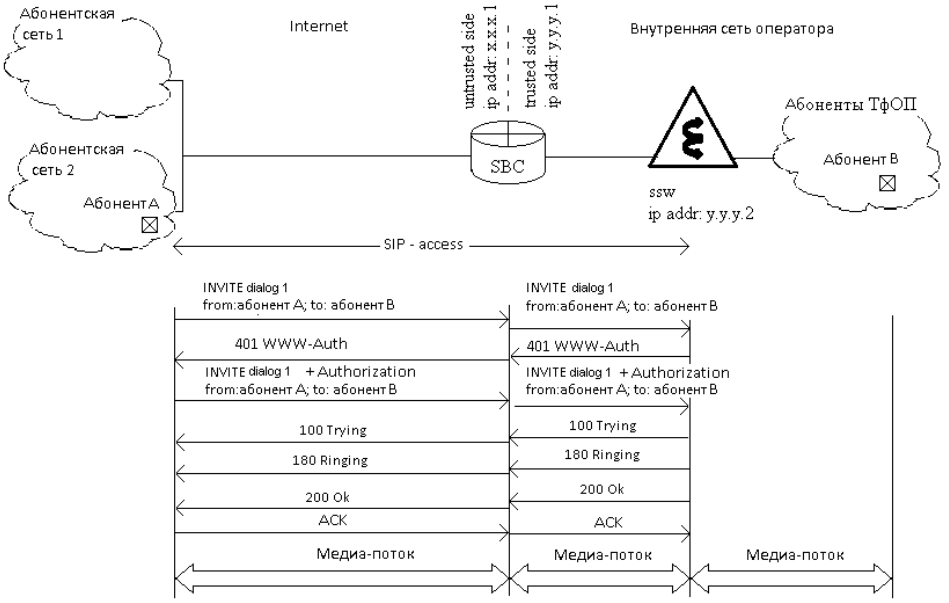

Рис. 2. Схема моделирования канала абонентского доступа SIP-access

Согласно алгоритму такой атаки, при установлении исходящего соединения легитимным пользователем генерируется запрос INVITE, который содержит параметры, необходимые для маршрутизации вызова и тарификации (адрес вызывающего и вызываемого абонента), для установления медиа-сессии (IP-адрес сетевого терминала вызывающего абонента, протокол передачи медиа-потока, порт, набор кодеков и прочие атрибуты медиа-потока) и для однозначной идентификации организуемого диалога. Злоумышленник перехватывает запрос INVITE, модифицирует в нем параметры вызываемого абонента, медиа-сессии (указывает параметры своего сетевого устройства) и идентификации диалога. Злоумышленник отслеживает и перехватывает все дальнейшие сообщения протокола в рамках открытого модифицированным запросом INVITE диалога и отвечает на них от имени легитимного пользователя, что приводит к установлению медиа-сессии между сетевым устройством злоумышленника и вызываемым им абонентом.

Имитация механизма переадресации вызова легитимным пользователем с помощью сообщения ответ 302 (moved temporarily — перемещается временно) на поступающий запрос INVITE. Алгоритм атаки данного вида основан на использовании возможностей протокола SIP по управлению сессией, а именно: функцию реализации услуги мобильности пользователя с помощью функции переадресации входящего вызова (RFC 5806 [4]).

Атака реализуется следующим образом. Злоумышленник звонит на номер телефона пользователя-жертвы. Далее злоумышленник перехватывает поступающий пользователю-жертве запрос INVITE и

возвращает софтсвичу ответ 302, содержащий параметры, обработав которые софтсвич в соответствии с RFC 5806 [4] выполняет переадресацию вызова (устанавливает соединение между телефоном злоумышленника и требуемым злоумышленником абонентом).

Имитация механизма переадресации вызова легитимным пользователем с помощью запроса INVITE. Данная атака во многом аналогична предыдущей атаке. Однако в этом случае злоумышленник модифицирует перехваченный запрос INVITE для инициации процедуры переадресации вызова.

Реализация алгоритмов атаки. Рассмотрим схемы и разработанные автором алгоритмы реализации следующих атак злоумышленника:

– модификация запроса INVITE на SIP-trunk;

– имитация «переадресации вызова» с помощью ответа 302 на SIP-access и SIP-trunk;

– имитация «переадресации вызова» с помощью запроса INVITE на SIP-trunk.

Результаты реализации этих алгоритмов на оборудовании действующей сети показали высокую вероятность риска ИБ, возникающей от фрод-угрозы, в сети SIP одного из российских операторов.

Модификация запроса INVITE на SIP-trunk. На рис. 3 представлена схема реализации атаки модификации запроса INVITE на SIP-trunk.

Злоумышленник перехватывает и модифицирует INVITE от ssw2 к ssw1, далее он перехватывает все сообщения в рамках диалога. В результате устанавливается соединение между терминалом злоумышленника и вызываемым им абонентом.

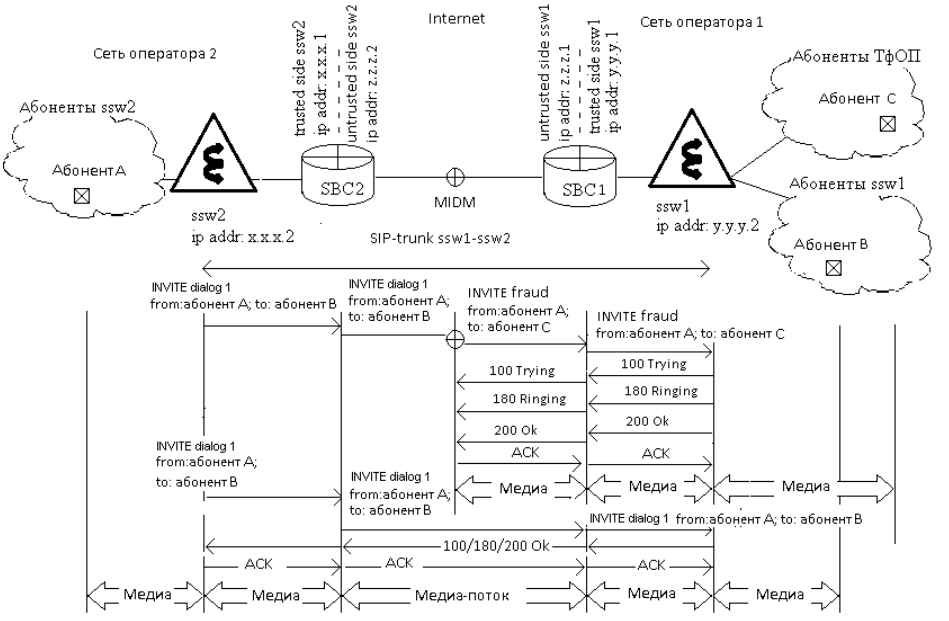

Рис. 3. Схема реализации атаки модификации запроса INVITE на SIP-trunk

Софтсвич ssw2, не получив ответ на отправленный им запрос, повторно направляет INVITE через промежуток времени, определенный соответствующим таймером. В результате устанавливается активная сессия между легитимным пользователем и вызываемым им абонентом. Таким образом, для легитимного пользователя факт проведения атаки остается незамеченным. Системы тарификации софтсвича ssw1 фиксируют установление двух активных сессий абонентом А и относят стоимость обоих вызовов на его счет. Обнаружить факт фрода возможно при сравнении биллинговых данных софтсвичей ssw1 и ssw2. Значительно усложняет реализацию атаки данного вида настройка на SBC строгих правил фильтрации по адресам сетевого уровня: например, в приведенной схеме разрешение обмена сигнальным и медиа-потоком только между IP-адресами SBC1 и SBC2.

Имитация «переадресации вызова» с помощью ответа 302 на SIP-access и SIP-trunk. Механизм авторизации не применяется к ответам на запросы, что создает уязвимость протокола SIP и потенциальную угрозу реализации атаки типа «имитация переадресации вызова» имитации механизма переадресации. На рис. 4 показана схема проведения такой атаки на SIP-access с помощью ответа 302.

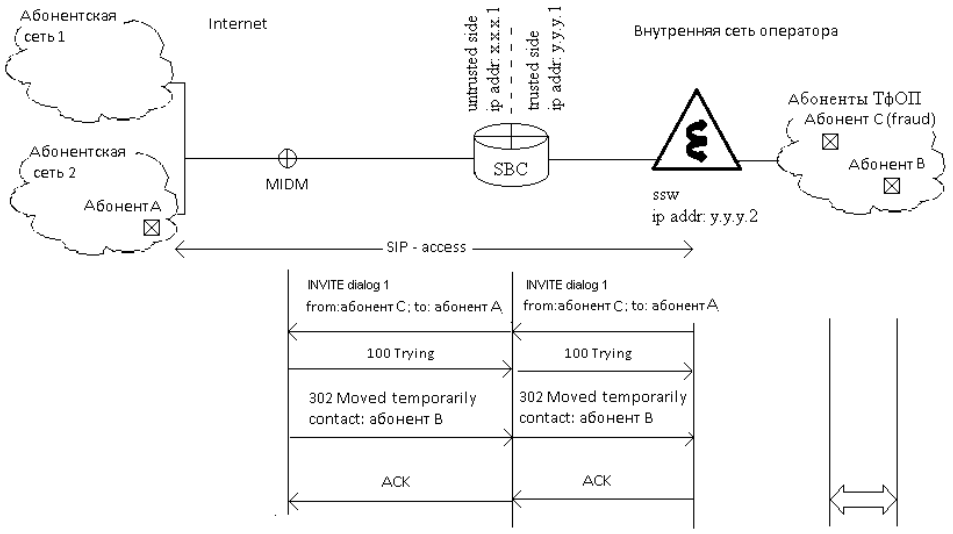

Рис. 4. Атака «имитация переадресации вызова» с помощью ответа 302 на SIP-access

Злоумышленник (на схеме абонент С) выполняет вызов пользователя-жертвы (абонент А), перехватывает поступающий от софтсвича запрос INVITE на это соединение и возвращает софтсвичу ответ 302 (moved temporarily), содержащий в поле Contact адрес абонента, с которым злоумышленник желает установить соединение (на схеме с абонентом В). Получив данный ответ, софтсвич выполняет переадреса-

цию вызова и устанавливает соединение между злоумышленником и требуемым абонентом (на схеме между абонентом С и абонентом В).

Системы тарификации софтсвича (ssw) фиксируют использование абонентом А услуги переадресации вызова и тарифицируют выполненное соединение как вызов абонентом А абонента В. На основании этих систем тарификации невозможно отличить данную атаку от реализации услуги переадресации легитимным пользователем. Защитой от такой атаки может быть фильтрация всех сообщений ответа 302 (moved temporarily) на SBC и реализация услуги переадресации средствами софтсвича. Однако данный метод ограничивает функциональность терминала пользователя и не всегда возможен.

Атака «имитация переадресации вызова» с помощью сообщения ответа 302 может быть реализована и на топологии SIP-trunk. Схема проведения атаки аналогична схеме, показанной на рис. 4.

Имитация «переадресации вызова» с помощью запроса INVITE на SIP-trunk. На рис. 5 приведена схема проведения атаки «имитация переадресации вызова» с помощью запроса INVITE на участке SIP-trunk. Примером такой атаки является использование запроса INVITE с заголовком diversion.

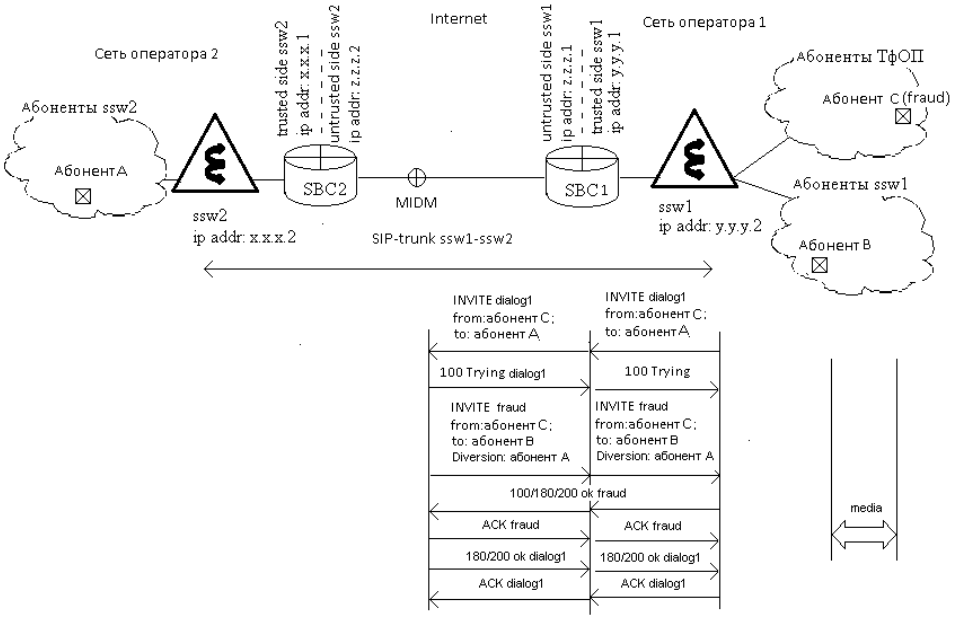

Рис. 5. Атака «имитация переадресации вызова» с помощью запроса INVITE

Атака начинается с направления вызова от злоумышленника (на схеме абонент С) абоненту-жертве (абонент А). Обрабатывая данный вызов, софтсвич ssw1 инициирует сессию (направляет запрос INVITE на софтсвич ssw2). Злоумышленник MIDM перехватывает этот запрос

и модифицирует его, подменяя параметры вызываемого абонента на нужный злоумышленнику адрес, изменяя параметры идентификации диалога и добавляя заголовок diversion содержащий идентификатор абонента-жертвы. Модифицированный запрос INVITE возвращается софтсвичу ssw1. Приняв модифицированный запрос и обнаружив в нем заголовок diversion, софтсвич ssw1 в соответствии с RFC 5806 [4] реализует процедуру переадресации вызова от абонента А абоненту В. В результате устанавливается соединение между злоумышленником (абонент С) и абонентом В.

Системы тарификации софтсвича ssw1 фиксируют реализацию абонентом А услуги переадресации и начисляют стоимость вызова абонентом А абонента В на счет абонента А. Выявить факт мошенничества можно при анализе биллинговых данных софтсвичей ssw1 и ssw2, обнаруживая несовпадения и аномалии. Предотвратить данную атаку средствами SBC не представляется возможным.

Реализация атаки данного вида на топологии SIP-access при использовании механизма авторизации запросов INVITE маловероятна.

В заключение отметим, что результаты проведенного тестирования уязвимости сети SIP от фрод-угрозы дают основание сделать вывод об актуальности проведения дальнейших работ по изучению фрод-угроз и поиску мер противодействия данным угрозам. Причем при поиске мер противодействия фрод-угрозам необходимо учитывать такие аспекты, как правовой, научно-технический, экономический, международный, социальный и др. В частности, следует:

– принять соответствующие нормативные документы и правовые акты, регламентирующие права и ответственность провайдеров услуг связи в вопросах противодействия мошенничеству, определяющие порядок сбора и предоставления доказательной базы для защиты прав операторов и пользователей в суде;

– провести научные исследования проблемы, поиск и исследование эффективных методов противодействия, поиск надежных алгоритмов обнаружения мошеннических действий;

– создать и внедрить отечественную систему противодействия мошенничеству;

– обеспечить защиту бизнеса, сохранение прибыли предприятий связи, возврат денег из теневого оборота в экономику;

– наладить тесное международное научное сотрудничество (в первую очередь в отношении участков взаимодействия сетей связи операторов разных стран), поскольку проблема носит глобальный характер;

– организовать защиту граждан от действий злоумышленников.

СПИСОК ЛИТЕРАТУРЫ

1. Communications Fraud Control Association (CFCA). 2011 Global Fraud Loss Survey. URL: www.cfca.org
2. Бельфер Р.А., Морозов А.М. Информационная безопасность сети связи для соединения абонентов ТфОП/ISDN через SIP-T // Электросвязь. 2012. № 3. С. 22–25.
3. Billing Attacks on SIP-Based VoIP Systems / Zhang R., et al. // Proc. WOOD '07 Proceedings of the first USENIX workshop on Offensive Technologies, USENIX Association Berkley, CA, USA, 2007.
4. RFC 5806. S. Levy, M. Mohali. Diversion Indication in SIP. 2010. URL: http://tools.ietf.org/html/rf5806

Статья поступила в редакцию 25.10.2012.