УДК 621.391

В.А. Матвеев, А.М. Морозов, Р.А. Бельфер

ФРОД И УГРОЗЫ В СЕТИ IP-ТЕЛЕФОНИИ ПО ПРОТОКОЛУ SIP

Рассмотрены формы фрода, которые являются основными для действующих технологий сетей связи с точки зрения наибольших потерь дохода провайдера. Показана актуальность угроз фрода на сети SIP Российской Федерации. Проведен анализ угроз фрода на сети SIP, установленной на сети связи общего пользования Российской Федерации, предусмотренных механизмов защиты от них, а также некоторые формы фрода и угрозы фрода, которые являются основными для действующей в нашей стране технологии сети VoIP по протоколу SIP.

E-mail: a.m.morozov@gmail.com

***Ключевые слова*:** *информационная безопасность (ИБ), сети связи, угрозы фрода, формы фрода, IP-телефония, VoIP, SIP.*

Введение. Согласно Рекомендации МСЭ-Т Е.408, одной из характеристик риска информационной безопасности (ИБ) в сетях связи является последствие реализации угроз [1]. Например, таким последствием может быть мошенничество, которое приводит к снижению финансовой прибыли провайдеров услуг сетей связи. В технической литературе по сетям связи мошенничество часто называют фродом (fraud), оно принимает различные формы, но все они сводятся к результату нечестной попытки убедить сторону в легитимности транзакции тогда, как на самом деле этого нет [2]. Далее в работе будем использовать предложенную терминологию. По мнению иностранных специалистов, в большинстве случаев фрод в сети связи преследует финансовую цель, но это может быть и плагиат, мошенничество в процессе выборов, при лжесвидетельстве и др. С появлением сетей связи следующего поколения (Next-Generation Network, NGN), электронной и мобильной коммерции увеличилось число случаев фрода.

Формы фрода в сетях связи. Рассмотрим примеры основных форм фрода в сетях связи. Основой выбора таких форм стали опубликованные отчеты Международной организации по контролю над фродом (Communications Fraud Control Association, CFCA), а также научно-технические работы в этой области. Приведем примеры угроз ИБ, приводящие к фроду (далее угрозы фрода) [3].

1. ***Мошенничество с подпиской*** (Subscription Fraud) заключается в том, что злоумышленник подписывается на услугу легальным способом (как правило, не от своего имени). При этом он может поступить следующим образом: а) использует сервис в личных целях, в основном с намерением минимизировать свои затраты или вовсе избежать оплаты; б) предпринимает действия, направленные на извлечение прибыли, например, перепродает услуги. В последнем случае

CFCA выделяет фрод в отдельную форму — фрод дилера (Dealer Fraud) [3]. В сетях IP-телефонии (передачи голосовых данных по сетям IP, VoIP) по протоколу SIP (Session Initiation Protocol) уделяется большое внимание защите с помощью механизмов аутентификации от мошенничества с подпиской [4, 5].

2. ***Перехват или кража подписки*** (Identity Take Over), с помощью чего мошенник получает возможность использовать услуги от имени легитимного пользователя. Например, компрометация аккаунта абонента, после чего злоумышленник начинает активное использование услуг за счет владельца скомпрометированного аккаунта (учетной записи пользователя на сервере доступа оператора связи, содержащей набор параметров, необходимых для оказания услуг связи пользователю-владельцу и для тарификации).

3. ***Мошеннический обход*** (Bypass Fraud). Выбор неавторизованных маршрутов прохождения сигнализации и (или) трафика. Например, операторы связи, стремясь сократить свои расходы по пропуску международного (междугородного) трафика через сети транзитных операторов, используют технологию VoIP для незаконной организации прямых IP-каналов к операторам-получателям этого трафика, в обход зоновых, междугородных или международных транзитных узлов связи. Возможен еще один вариант реализации этой формы мошенничества, основанный на том, что сеть SIP допускает установление сессий непосредственно между конечными терминалами без участия SIP-прокси (в архитектуре сети NGN функции SIP-прокси реализуются на софтсвиче) оператора. Такие вызовы не буду фиксироваться оператором, так как SIP-прокси (первоисточник для получения тарификационных данных) оператора не участвует в сигнальном обмене. Используя эту возможность, мошенник может организовать пропуск трафика по сети оператора связи в своих целях. Обнаружить реализацию данной формы мошенничества позволяет анализ данных с различных сетевых устройств, позволяющий выявить аномалии в прохождении трафика.

4. ***Манипуляция сигнальных сообщений.*** Пример этого фрода в сети сигнализации ОКС №7 (Manipulation SS7) — искажение адреса вызывающего абонента в сообщении IAM ТфОП/ISDN или в сообщении UDT сети GSM системы сигнализации ОКС №7 [6]. В сети сигнализации SIP данная форма фрода может быть реализована манипуляцией полей From и Contact в сигнальных сообщения протокола [4]. В результате реализации фрода система тарификации вызовов не сможет правильно тарифицировать соединение.

5. ***Мошенничество, основанное на уязвимостях в учрежденческих станциях и в системе голосовой почты*** (Private Branch Exchange, PBX, или Voice Mail). Например, системы голосовой почты могут быть сконфигурированы так, что будут инициировать вызов автору сообщения после того, как пользователь прослушал голосовое сообщение. Мошенник может воспользоваться этим функционалом, получив каким-либо способом доступ к голосовому почтовому ящику. Еще одним вариантом реализации такого мошенничества в сетях NGN может быть

получение злоумышленником доступа к SIP-прокси серверу оператора или к станциям корпоративных пользователей PBX [7].

6. ***Мошенничество, основанное на уязвимости при реализации дополнительных видов обслуживания (ДВО) в сетях NGN.*** Дополнительные виды обслуживания предоставляют широкие возможности абонентам, среди которых переадресация вызова, ожидание вызова, перенаправление вызова, участие в конференции, ограничение входящей и (или) исходящей связи и др. Как правило, в сетях NGN абонент, имеющий доступ к ДВО, активирует соответствующую услугу со своего терминала с помощью специального сервисного кода. Мошенник может использовать эту особенность. Например, активировать услугу переадресации абоненту-жертве, послав от его имени скомпрометированный сервисный код. В результате вызовы, поступающие на номер абонента-жертвы, будут переадресовываться на требуемый мошеннику номер. Оплата за переадресованные вызовы будет начислена на счет абонента-жертвы.

7. ***Фрод распределения дохода между операторами страны*** (Domestic Revenue Share Fraud, DRSF). Эта форма фрода подлежит контролю CFCA и предусматривает злонамеренные действия недобросовестного оператора, направленные на получение незаконной прибыли при взаимодействии со смежными операторами той же страны. Пример таких действий — генерация фиктивного большого объема трафика от сети оператора-жертвы на сеть оператора-мошенника.

8. ***Фрод распределения дохода между операторами разных стран*** (International Revenue Share Fraud, IRSF). Этот фрод аналогичен DRSF, но предусматривает злонамеренные действия недобросовестного оператора в отношении иностранного оператора-жертвы.

9. ***Фрод при использовании служб привилегированного тарифа*** (Premium Rate Service), т. е. платные службы, реализованные в соответствии с архитектурной концепцией интеллектуальной сети, оказывающие услуги развлекательного или информационного характера. В Российской Федерации такая услуга предоставляется интеллектуальной сетью, например оператором «Уралсвязьинформ». Осуществляя вызов на номера служб привилегированного тарифа, абонент оплачивает как услуги оператора связи (за организацию соединения), так и информационную услугу, оказываемую поставщиком информации [8]. Оплата распределяется между оператором сети связи и поставщиком услуги. Возможны различные варианты реализации такой формы фрода: инициация мошенником от скомпрометированного аккаунта легитимного абонента большого числа вызовов на службу привилегированного тарифа, владельцем которой является мошенник; оплата абонентами-жертвами услуг, предоставляемых другим абонентам. В работе [9] приведен еще один пример этой формы фрода, когда эту услугу нелегитимно запрашивает сам оператор. При этом оплата за оказание услуги переводится с поставщика-жертвы информации на счет оператора сети связи.

10. ***Использование техническим персоналом доступной ему служебной информации в целях совершения мошенничества.*** По данным, приведенным в работе [9], сотрудники телекоммуникационных компаний тем или иным способом сопричастны в 73 % случаев мошенничества. Согласно данным отчета CFCA за 2011 г., это значение превышено более чем в 10 раз.

11. ***Фрод при использовании кредитной карты*** (Credit Card Fraud). Примером такого фрода для получения услуг в сети IP-телефонии может быть использование мошенником украденной кредитной карты с найденным им PIN-кодом [5].

12. ***Клонирование*** (Clonning). Мошенник создает копии в целях получения бесплатных услуг сети связи. Примером в сети GSM может быть клонирование SIM-карт мобильной станции. Для этого мошеннику необходимо определить секретный ключ, позволяющий осуществить нелегитимную аутентификацию. В работе [9] показано, что для успешного проведения такой атаки потребовалось 8 ч.

В приведенные выше список включены формы фрода, которые наносят наибольший ущерб (по данным CFCA за 2011 г.). Так, мошенничество с подпиской составляет 10,8 %, а IRSF — 9,8 % от доли нанесения ущерба другими формами фрода. Согласно этому же отчету CFCA, потери в индустрии связи в 2011 г. составили 40,1 млрд долл., что соответствует 1,88 % от общей прибыли отрасли.

Перечисленные данные CFCA не являются достаточно точными по многим причинам. CFCA ограничивается ежегодным контролем чуть более 20 форм. Однако полагают, что число форм фрода в сетях связи может быть более 200 [10]. Сам факт мошенничества крайне трудно распознать и многие случаи остаются необнаруженными. Как правило, операторы стараются не обнародовать реальные значения потерь от мошенничества, опасаясь нанести ущерб своей репутации [11].

В некоторых источниках реальные суммарные потери новых операторов связи в результате мошенничества составляют до 20 % от их суммарного дохода [12].

Значительные потери от действий мошенников несут легитимные пользователи услуг связи. Многие методы мошенников направлены именно на пользователя, не только не имеющего ресурсов для организации противодействия подобного рода злонамеренным действиям, но даже и не подозревающего этого. Объем ущерба, нанесенного пользователям услуг связи в результате мошеннических действий, операторами связи не учитывается. Кроме того, нередко провайдеры услуг связи умышленно бездействуют, так как извлекают прибыль от действий мошенников направленных против абонентов — законопослушный абонент вынужден оплачивать услуги связи, даже если не вызывает сомнение тот факт, что этими услугами воспользовался мошенник. Отсутствие адекватной нормативной базы в вопросе борьбы с мошенничеством способствует этому.

Далеко не все основные операторы сетей связи охвачены при составлении ежегодных отчетов CFCA. Так, в 2011 г. 25,9 % операто-

ров сетей связи стран Западной Европы приняли участие в международном исследовании по проблемам мошенничества в телекоммуникационной индустрии. В России этот показатель составил 1,7 %. Потери от мошенничества около 12 % провайдеров услуг связи в странах Западной Европы достигают 1…2 % от годовой прибыли, в Российской Федерации — десятые доли процента [3]. Эти данные на фоне других стран, к сожалению, не свидетельствует о победе над проблемой мошенничества в России. Скорее это является признаком отсутствия постоянного представительства России в международных ассоциациях, занимающихся проблемами безопасности, слабой интеграцией России в международные проекты по борьбе с проблемами безопасности связи.

Во многих работах отмечено, что в сетях NGN возрастают потери дохода оператора сети связи от фрода. В качестве причин такого положения приводится расширение мобильной коммерции, спуффинг (получение доступа к банковским деталям в IP-сети) и др. В работе [5] указаны некоторые дополнительные причины потери дохода от фрода в отношении сети IP-телефонии — фрод дилера и фрод при использовании кредитной карты. В настоящее время такая сеть NGN на базе протокола сигнализации SIP устанавливается на сети оператора междугородной и международной связи ОАО «Ростелеком». Поэтому анализ различных форм фрода на такой сети актуален. Большинство рассмотренных форм фрода могут использоваться в сети SIP.

Примеры угроз фрода в сети SIP. Фродстером (Fraudster) будем называть мошенника, создающего угрозу ИБ в целях фрода. В кратком описании угроз фрода приведены примеры реализации их фродстером в сети SIP. Рассмотрим еще несколько примеров возможных угроз фрода более подробно.

1. ***Эмуляция легитимного пользователя.*** На рис. 1 приведена упрощенная схема для описания реализации такой угрозы фрода [5]. SIP-proxy voip.com проводит аутентификацию запроса, поступившего от абонента, и транслирует запрос на шлюз к сети ТфОП pstn.com. В целях идентификации легитимности своего запроса SIP-proxy voip.com добавляет к передаваемому запросу специальный параметр. На основании значения этого параметра шлюз pstn.com принимает решение об обработке или отклонении данного запроса. Возможность получения фродстером информации о значении этого параметра создает угрозу фрода эмуляции легитимного пользователя. Фродстер, включая ставший ему известным специальный параметр в свои запросы, получает возможность устанавливать SIP-сессии со шлюзом pstn.com от имени и за счет SIP-proxy voip.com.

Реальная реализация данного вида фрод-атаки в действующих сетях достаточно сложна, однако потенциально возможна. Для защиты от данного вида мошенничества необходимо на участке между SIP-proxy и ТфОП-шлюзом реализовать дополнительные меры безопасности: фильтрация сообщений по IP-адресу, использование технологий протоколов безопасности IPSec или TLS.

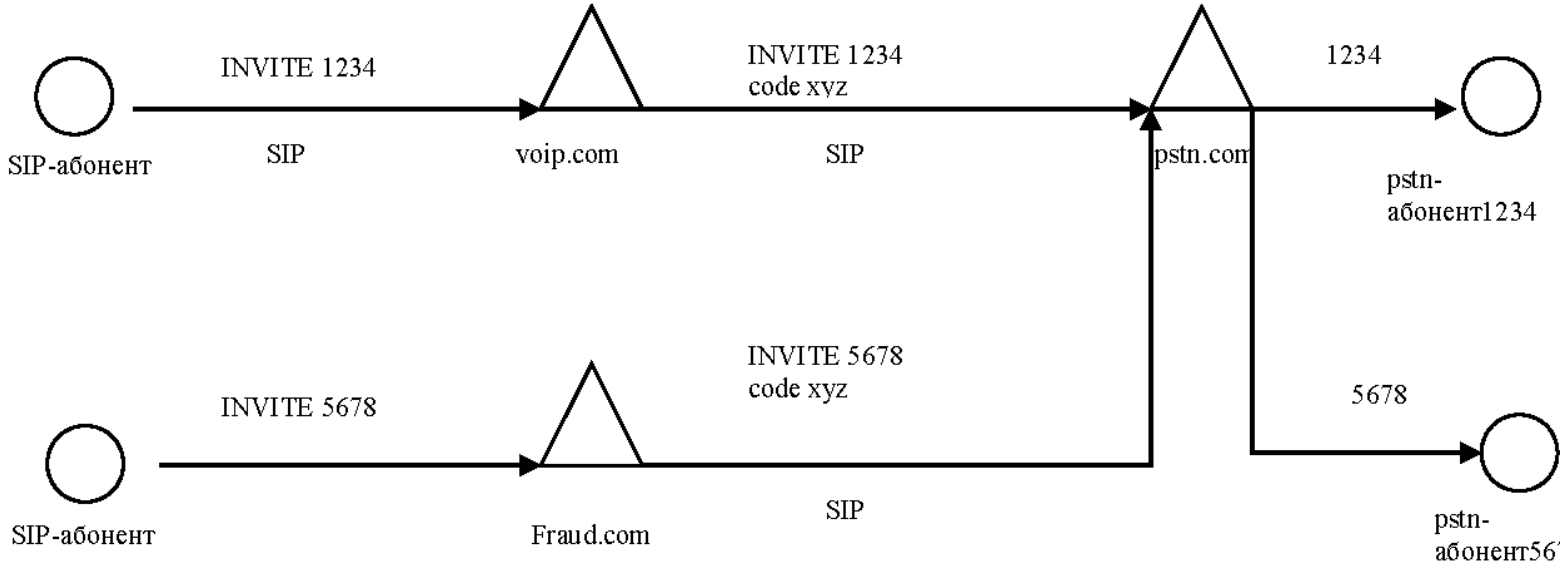

Рис. 1. Упрощенная схема для описания реализации угрозы эмуляции легитимного пользователя

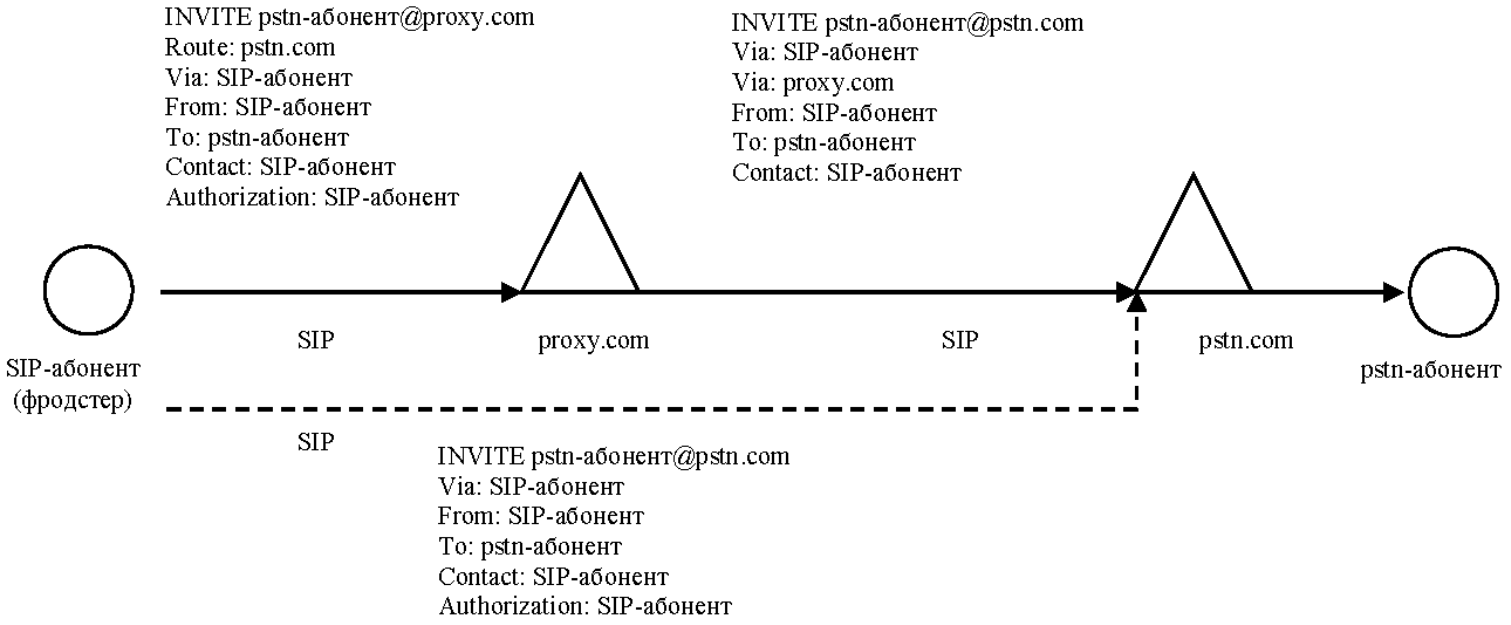

Рис. 2. Схема для описания реализации угрозы некорректного использования заголовка Route:

——→ — разрешенное направление; - - - - - - - - - → — запрещенное направление

2. ***Допуск переноса данных протоколом SIP, необходимых для организации медиа-сессии в любом запросе или ответе на запрос.*** В некоторых сценариях установления SIP-сессий двусторонняя передача полезного трафика (например, голоса) между конечными пользователями начинается до того, как SIP-терминал сообщит SIP-прокси об успешном установлении сессии (по сути до начала тарификации соединения). Эта особенность также создает угрозу мошенничества. Обнаружение угрозы основывается на анализе сигнального обмена и выявлении аномалий в нем (например, наличие непропорционально большого числа определенных сигнальных сообщений при установлении некоторых сессий).

3. ***Несанкционированный доступ фродстера к услугам связи при некорректном использовании SIP-заголовков в SIP-запросах.*** Согласно RFC3261, заголовок Route используется для передачи SIP-proxy информации об адресе, на который необходимо переслать запрос, содержащий заголовок Route. Получив запрос с заголовком Route SIP-proxy должен переслать имеющийся запрос на адрес, содержащийся в данном заголовке Route. Фродстером может быть осуществлена запрещенная для него передача SIP-запроса прямо на SIP-сервер. На рис. 2 приведена схема для описания реализации такой угрозы фрода [5]. Защитой от такой угрозы может служить административный запрет на обработку заголовков Route, а также создание классов ограничений выхода, позволяющих управлять доступом пользователей на определенные направления связи. Пример реализации подобных классов ограничений на оборудовании Cisco описан в работе [13].

4. ***Конфигурация сети VoIP с транзитом SIP-T, включающая систему сигнализации ОКС №7, которая вносит дополнительные возможности для фрода*** [7]. Атака DoS в ОКС № 7 создается мошенником в результате передачи им фиктивных сообщений обновления маршрутизации. Прием этих сообщений может приводить к таким изменениям таблиц маршрутизации в узле коммутации, которые фиктивно отражают неисправности, перегрузки узлов сети или каналов связи. В результате фрода нарушается правильная маршрутизация сообщений сигнализации, что отражается на возможности установления соединения. Защитой должна быть аутентификация в отношении подлинности источника и целостности сообщений обновления маршрутизации.

5. ***Компрометация учетной записи пользователя.*** При поступлении от SIP-пользователя запроса на установление сеанса связи SIP-прокси сверяет содержащиеся в запросе данные об инициаторе запроса со значениями из базы учетных записей пользователей. При нахождении совпадения запрос признается легитимным и обрабатывается, при отсутствии совпадений запрос отклоняется. Особенности протокола SIP дают возможность злоумышленнику получить список имеющихся на SIP-прокси пользовательских аккаунтов и далее ыполнять вызовы от имени легитимных пользователей [14].

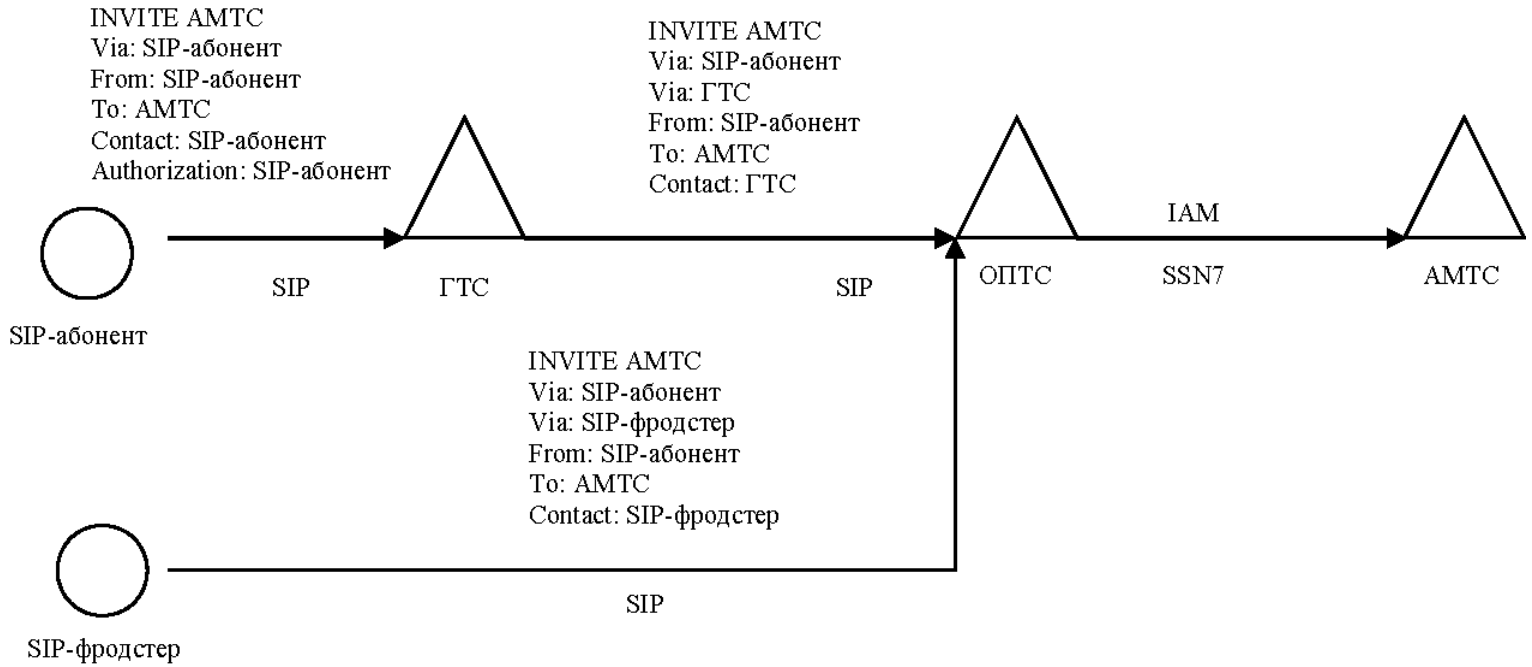

Рис. 3. Упрощенная схема маршрута междугородного или международного вызова от SIP-пользователя

Протоколом SIP предусмотрена процедура аутентификации, основанная на использовании пары идентификатор пользователя — пароль в целях аутентификации легитимного пользователя. Такая процедура может применяться для аутентификации любого запроса, поступающего от пользователя. Однако, во-первых, данный механизм согласно протоколу не является обязательным, а во-вторых, механизм содержит ряд уязвимостей. В частности механизм не защищен от подбора пары идентификатор пользователя — пароль по методу полного перебора (Brute Force Attack). В работе [14] описан вариант реализации атаки методом полного перебора на SIP-сервер, а в работе [15] — более сложный метод преодоления механизма аутентификации злоумышленником путем манипулирования SIP-запросами пользователя-жертвы.

Из приведенных примеров следует, что большинство основных форм фрода могут быть результатом угроз в сети SIP. Это показывает актуальность задачи защиты от этих угроз.

Формы фрода и примеры угроз фрода в сети SIP Российской Федерации. Приведем примеры возможных угроз фрода в сети SIP Российской Федерации, защита от которых с точки зрения потерь дохода провайдера является первостепенной задачей. Это относится как к угрозам, приведенным выше, так и к предлагаемым к рассмотрению вариантам угроз.

1. Наиболее распространенная схема организации связи с использованием протокола SIP в сетях операторов связи предполагает ***наличие нескольких софтсвичей***, являющихся оконечными транзитными станциями местной или зоновой связи и реализующих функции SIP-proxy с точки зрения протокола SIP. Такая схема обеспечивает обслуживание как местных вызовов SIP-абонентов, так и доступ SIP-абонентов к услугам междугородной или международной связи.

Упрощенная схема маршрута междугородного или международного вызова от SIP-пользователя приведена на рис. 3. Запрос на установление соединения от SIP-абонента поступает на софтсвич городской телефонной станции (ГТС), на котором реализованы функции аутентификации абонента. Проведя аутентификацию пользователя, софтсвич ГТС направляет SIP-запрос на организацию сеанса связи на софтсвич опорно-транзитной станции (ОПТС) или зонового транзитного узла. Софтсвич ОПТС транслирует поступивший вызов в направлении междугородной телефонной сети (МГТС).

По ряду объективных причин на софтсвиче ОПТС (зоновый транзитный узел) не может быть реализован, предусмотренный SIP-механизм аутентификации SIP-запросов (для реализации такого механизма на зоновом транзитном узле потребовалось бы хранить базу учетных записей всех SIP-абонентов, для которых выполняется транзит-вызовов через данный узел). Отсутствие аутентификации на участке ГТС — ОПТС создает угрозу фрода эмуляции легитимного пользователя, при которой фродстер направляет запрос на установление соединения непосредственно на софтсвич ОПТС.

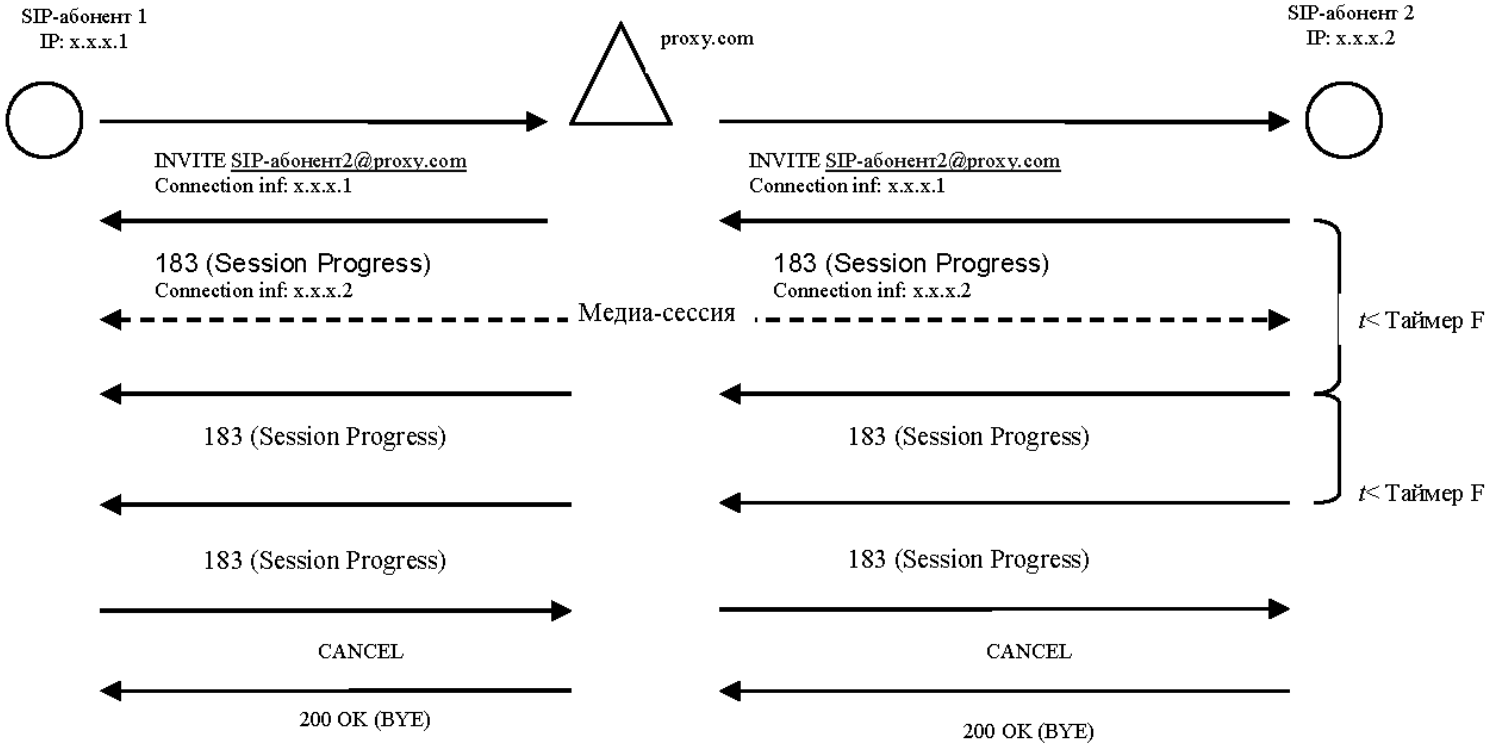

Рис. 4. Схема реализации угрозы фрода, в ходе которого злоумышленник манипулирует порядком следования сигнальных сообщений:

таймер F — таймер ожидания окончательного ответа; таймер F = 64 T1, где T1 = RTT (500 мс по умолчанию)

2. ***Манипуляции порядком следования сигнальных сообщений злоумышленником*** (рис. 4). При нормальной работе протокола последовательность сигнальных сообщений в ходе установления сессии может быть следующая:

— инициатор соединения отправляет запрос INVITE и запускает таймер ожидания ответа (по его истечении запрос INVITE будет передан повторно). В теле запроса INVITE, как правило, передаются параметры, необходимые для установления медиа-сессии (IP-адрес, UDP-порт, набор поддерживаемых кодеков и пр.);

— SIP-терминал вызываемого абонента, приняв запрос INVITE, отвечает на него предварительным ответом 1XX (могут быть ответы 100 Trying, 180 Ringing, 181 Call Is Being Forwarded, 182 Queued, 183 Session Progress) и приступает к обработке запроса. В ходе обработки запроса INVITE SIP-терминал вызываемого абонента может повторно передавать предварительные ответы;

— SIP-терминал инициатора соединения, получив предварительный ответ, запускает таймер ожидания окончательного ответа (таймер F). При повторном предварительном ответе таймер ожидания окончательного ответа перезапускается;

— когда вызываемый абонент принял вызов (например, снял трубку телефона), SIP-терминал вызываемого абонента сообщает об этом инициатору сессии при помощи окончательного ответа на запрос INVITE (ответ 200 OK);

— инициатор соединения, получив окончательный ответ, останавливает таймер ожидания окончательного ответа и подтверждает получение окончательного ответа сообщением ACK. Сообщения 200 и ACK сигнализируют об успешном установлении сессии и запускают процедуры тарификации;

— нормальное завершение сессии происходит, когда одна из сторон посылает запрос на завершение сессии BYE и вторая сторона подтверждает получение запроса (ответ 200 OK).

Параметры вызываемой стороны, необходимые для установления медиа-сессии, могут быть переданы SIP-терминалом вызываемого абонента в теле любого ответа — предварительного или окончательного. При этом следует отметить, что медиа-сессия организуется сразу после того, как SIP-терминалы сторон, участвующих в сессии, обменялись требуемыми данными, независимо от получения инициатором сессии окончательного ответа. Именно этой особенностью может воспользоваться мошенник (см. рис. 4), модифицировав порядок следования сигнальных сообщений так, что, во-первых, параметры медиа-сессии передаются в предварительном ответе, а во-вторых, предварительный ответ повторяется через время, меньшее времени таймера ожидания окончательно ответа, постоянно перезапуская его. В результате злоумышленник получает возможность использовать установившуюся медиа-сессию в обход системы тарификации. Обнаружение мошенничества основано на анализе данных по вызовам не завершившихся ответом, а также анализе сессий с аномально большим числом предварительных ответов.

3. ***Компрометация учетной записи пользователя.*** Возможные механизмы реализации приведены в работах [14, 15]. Обнаружение попыток компрометации учетных записей пользователей основано на анализе аномалий в сигнальном обмене (большое число запросов на аутентификацию и сообщений в отказе аутентификации, чрезмерно большого числа вызовов на несуществующие номера и пр.)

Заключение. Для снижения потерь от фрода в сети SIP Российской Федерации следует провести следующие научно-практические работы: проанализировать используемую зарубежными операторами сетей связи систему противодействия фроду (Fraud Detection System, FDS) в сети SIP; разработать экспертный метод оценки защищенности сети SIP, отражающий потери провайдера от каждой из угроз фрода; дать предложения по принятию мер дополнительной защиты от угроз фрода в сети SIP, реализация которых может вызвать наибольшие потери. Для угроз фрода, связанных с участками операторов сети других стран, провести согласование этих предложений.

СПИСОК ЛИТЕРАТУРЫ

1. ITU-T Recommendation E.408. Telecommunication Network Security Requirement, 2004.
2. Невдяев Л.М. Телекоммуникационные технологии. Англо-русский толковый словарь-справочник. — М.: МЦНТИ — Международный центр научной и технической информации, 2002.
3. Communications Fraud Control Association (CFCA). 2011. Global Fraud Loss Survey. www.cfca.org
4. Основы передачи голосовых данных по сетям IP / Д. Дэвидсон и др.; Пер. с англ. — М.: Вильямс, 2007.
5. SIP security / Dorgham Sisalem and ot. — John Wiley & Sons, Ltd., 2009.
6. Драйберг Ли, Хьюит В. Система сигнализации № 7 (SS7/OKC7), протоколы, структура и применение. — М.: Вильямс, 2006. — 752 с.
7. Бельфер Р.А., Морозов А.М. Информационная безопасность сети связи для соединения абонентов ТфОП/ISDN через SIP-T // Электросвязь. 2012. № 3. — С. 22—25.
8. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. — М.: Радио и связь, 2001. — 504 с.
9. http://www.isaac.cs.berkeley.edu/isaac/gsm.html
10. Bihina Bella MA., Olivier MS., Eloff JHP. A Fraud Detection Model for Next-Generation Networks / Southern African Telecommunication Networks and Applications Conference 2005 (SATNAC 2005): Proceedings. Champagne Castle, South Africa, September 2005. Vol. 1. — P. 321—326. http://mo.co.za/abstract/ngnfms.htm
11. Ченнинг И. Борьба с мошенничеством продолжается // Мобильные телекоммуникации. 2001. № 6. — С. 23—27.
12. Cahill M., Chen F., Lambert D., Pinheiro J., Sun Don X. Detecting Fraud in the Real World. Handbook of Massive Datasets. — Kluewer, 2002.
13. Park P. Voice over IP-security. — Cisco Systems, 2009.
14. Gauci S. Storming SIP Security // Hakin9. 2008. № 2. — P. 22—29. http://hakin9.org
15. SIP Digest Authentication Relay Attack / R. State and oth. http://tools.ietf.org/id/draft-state-sip-relay-attack-00.txt, 2009

Статья поступила в редакцию 4.07.2012