Противодействие «атакам на округление» в онлайн-банкинге

АЛЕКСАНДР САМАРИН,
аудитор информационных систем

В последнее время в прессе появляются сообщения о том, что клиенты научились делать деньги в онлайн-банках с помощью операций «округления». В чем же состоит способ заработка при конвертации средств на счетах интернет-банка? В этой статье рассмотрим практический опыт реализации методик противодействия «атакам на округление» в онлайн-банкинге для физических лиц.

При использовании компьютера пользователь — сам себе кассир

Принцип «атаки на округление»

При реальном обмене денежных средств в банковской кассе (без использования компьютера) коллизии округления не возникают: клиент пришел, выложил некоторое количество рублей и получил эквивалент в долларах/евро или наоборот. Кроме удостоверения личности и подписи на квитанции, никаких вопросов.

Все меняется, когда клиент регистрируется в интернет-банке. При использовании компьютера пользователь — сам себе кассир. Однако это не значит, что интернет-банк бесконтрольно доверяет своему клиенту обменные операции. Но, как известно, любой контроль несовершенен, даже компьютерный.

Проведем эксперимент. Внесем 100 рублей и получим взамен, по курсу 60 рублей за доллар, 1,67 доллара. Программа обмена валют (по правилам банка) автоматически округляет число 1,66 (6) до результата 1,67. Сделаем следующий шаг. Внесем 0,3 рубля (30 копеек) и, согласно тем же правилам, получим от банка 0,01 доллара (1 цент), который по обменному курсу стоит 60 копеек. Программа обмена округлила число 0,005 в бóльшую сторону до значения 0,01 доллара. Теперь мы понимаем, что каждый раз при обмене 30 копеек мы будем получать 1 цент. Таким образом, пользователь интернет-банка за 100 таких операций выручит 1 доллар за 30 рублей.

Ввиду того что такие операции пользователь выполняет на компьютере, возникает естественное желание автоматизировать этот нудный, но доходный процесс. Необходимо, чтобы компьютер пользователя сам целенаправленно общался с банковским онлайн-обменником. Применив элементарные навыки программирования, можно написать простой php-скрипт, который, извлекая данные (курс валют) из страницы браузера, будет подставлять значение «30 копеек» в ячейку для обмена и выполнять запрограммированную рутинную операцию. Такое автоматизированное общение программного «робота» значительно ускорит рост поступления денег на счет клиента при, казалось бы, копеечном обмене. Беда в том, что с такой же скоростью пропорционально будут уменьшаться деньги на счете банка. Банковские системы автоматизированного контроля обязательно запишут действия пользователя в специальный электронный журнал (лог) для анализа произошедшего, и затем последует внутреннее расследование — ведь банк потеряет деньги.

Изложенная схема у специалистов называется «атакой на округление». С появлением онлайн-обменников пользователи, изучавшие округление дробей в начальной школе, стали применять полученные знания на практике, используя уязвимость некоторых банковских систем дистанционного обслуживания, спроектированных без учета школьных знаний.

По оценкам Positive Technologies, около 25% банковских дистанционных систем обслуживания имеют реальную уязвимость, связанную с «атакой на округление». На практике процент уязвимости выше.

Алгоритмы нейтрализации и противодействия

Перейдем на сторону банка и посмотрим, какие методы защиты от клиентов-менял можно применить, ведь в банке было проведено служебное расследование. Недопустимо, чтобы банк нес ежедневные убытки, необходимо принимать меры.

Алгоритм первый, самый простой. Достаточно ограничить количество обменных операций в сутки, например не более 15. Клиент, который не занимается валютными «округлениями», не постра-

По оценкам Positive Technologies, около 25% банковских дистанционных систем обслуживания имеют реальную уязвимость, связанную с «атакой на округление»

дает, а банк строго ограничивает размер своих реальных, но уже копеечных убытков.

Алгоритм второй, чуть посложнее. При онлайн-обмене можно увеличить интервал времени между последующими операциями до 2–3 минут. Если сеанс дистанционного обслуживания ограничен банком 15–30 минутами, то за время сеанса при интервале между операциями 2–3 минуты можно выполнить максимум 15 обменов за полчаса. Такой прием сразу рушит все перспективы быстрого обогащения, причем не ущемляет права порядочных клиентов, которые нуждаются в разовых операциях валютного обмена. В этом случае банк также несет несущественные убытки.

Алгоритм третий, более сложный, чем два предыдущих. Заключается в том, чтобы блокировать обменные операции «копеечного» масштаба, то есть допускать к обмену суммы не менее 10 долларов или 1000 рублей. Особенность такого ограничения в том, что «атака на округление» не приносит клиенту-меняле желаемого дохода в двести процентов. Например, если обменять 1000,30 рублей на доллары по курсу 60 рублей, то можно получить 16,67 доллара. При обмене 1000,60 рубля (курс тот же) вы получите 16,68 доллара. Таким образом, на 1000 рублей можно заработать всего лишь 1 цент, потому что каждая операция будет начинаться с 1000 рублей. Доходность примерно 0,03% в сравнении с 200% при «атаке на округление» не впечатляет. При этом добросовестные клиенты, которые разово обменивают суммы более 1000 рублей, также не испытывают затруднений при операциях по валютному обмену. Исходя из практики, убытки банка минимальны.

Алгоритм четвертый, довольно спорный, а потому отнесем его в категорию самых сложных. Когда у банковской системы дистанционного обслуживания клиент просит обменять рубли, то система «за кулисами» пересчитывает вводимую обменную сумму пользователя, всегда вычитая эквивалент полцента в рублях. Хотите обменять 0,6 рубля (60 копеек)? Система по алгоритму рассчитает стоимость полуцента (по курсу 60 руб./долл. — это 30 копеек) и вычтет ее «негласно» из ваших 60 копеек. Затем посчитает полученную сумму по курсу, округлит результат и выдаст вам 1 цент. Хотите обменять 0,59 рубля (59 копеек)? Система опять вычтет 30 копеек, округлит результат и выдаст вам 0 центов, любезно уведомив при этом о недостаточности средств. Банк при таком механизме не теряет ни копейки, перекладывая потери на клиента, в том числе лояльного банку.

Другие методики пока нам неизвестны. Однако и четыре вышеизложенные убеждают, что против «атак на округление», инициируемых клиентами-менялами, есть действенные меры нейтрализации и защиты. Хакеры, люди сведущие в программировании, «атаками на округление» не интересуются. Эксплуатировать подобные недостатки неграмотно спроектированного обменного алгоритма дистанционной банковской системы — дело нудное и неблагодарное.

В истории существования цифровых компьютеров «атаки на округление» известны давно, однако все случаи выявлялись специалистами благодаря тому, что любая компьютерная система ведет электронные журналы регистрации событий — логи, хотя пользователей об этом не уведомляют, так как это служебная тайна.