

Как я перестал бояться токенов и полюбил одноразовые пароли

Д. Евтеев, эксперт по информационной безопасности отдела консалтинга и аудита MCSE:Security, MCTS

С. В. Гордейчик, руководитель отдела консалтинга и аудита, MCSE, MCT, MVP Enterprise Security, CISSP

Компания Positive Technologies

Одноразовые пароли являются популярным решением в системах, требующих строгой аутентификации. Они широко используются в «интернет-банкинге» и на сайтах электронной коммерции. Простое, надежное и понятное пользователю решение. Но так ли безупречна технология одноразовых паролей, как многие себе ее представляют?

One-Time-Password (OTP) – это ключевое слово, действенное для одного процесса аутентификации в течение ограниченного промежутка времени. Другими словами, использование технологии одноразовых паролей (в теории) позволяет защитить некий «секрет» для повторного его использования при аутентификации, кроме того, этот «секрет» меняется каждые 30–60 секунд.

В настоящее время одноразовые пароли преимущественно используются:

- в приложениях электронной коммерции;
- в банковских приложениях.

В большинстве случаев одноразовая аутентификация применяется в момент, когда пользователю необходимо осуществить вывод денежных средств или при оплате некоторых услуг. Однако встречаются ситуации, которые требуют ввода одноразового пароля в процессе входа в систему.

Широкое распространение технологии OTP в большей степени именно в банковских приложениях обусловлено тем, что в данном секторе требуется повышенный уровень без-

опасности, и при его обеспечении процессу аутентификации уделено большое внимание. Заставить своих клиентов использовать другие способы аутентификации, например цифровые сертификаты, данный сектор, в общем-то, может, но вряд ли такой банк будет пользоваться у них популярностью ввиду ряда неудобств, с которыми неизбежно столкнутся клиенты при выполнении подобных требований безопасности. Поэтому, безусловно, сектор электронной коммерции стремится предложить своим клиентам более универсальные способы работы с предоставляемыми услугами. Системы одноразовых паролей как раз удовлетворяют этим требованиям. Они не зависимы от платформы, операционной системы или браузера.

Основные варианты реализации одноразовых паролей – это заранее рассчитанные списки паролей, использование аппаратных генераторов OTP и SMS-сервис. Существуют и другие, более экзотические способы получения одноразовых паролей, но в большинстве случаев используются первые два из упомянутых выше вариантов.

Принцип работы автономных генераторов одноразовых паролей основан на алгоритме HMAC. Для расчета значения OTP принимаются два входных параметра – секретный ключ (начальное значение для генератора) и текущее значение времени (или внутренний счетчик). Секретный ключ хранится как в самом устройстве, так и на сервере аутентификации.

При нажатии на соответствующую кнопку на электронном брелоке сначала вычисляется значение HMAC-SHA-1, а затем выполняется операция усечения (выделения) из полученного 160-битового значения шести цифр, являющихся одноразовым паролем.

Помимо аппаратного генератора OTP, большую популярность в системах «интернет-банкинга» получили рассчитанные списки паролей. Подобный список одноразовых паролей представлен в виде карточки с нанесенными на нее индексами (рис. 1), где напротив каждого индекса находится поле, защищенное специальным слоем (аналогично защищенному слою в лотерейных билетах).

В случае использования карты «интернет-банкинг» обслуживающая система запрашивает у клиента ввод одноразового пароля, привязанного к определенному индексу. Клиент стирает защищенный слой рядом с этим индексом и производит требуемые действия (рис. 2). Если клиент не ошибся при вводе, система выполняет операцию клиента (в основном это операции с его счетом, оплата услуг и пр.).

Надо отметить, что использование карт «интернет-банкинг» подразумевает их замену в случае, когда все одноразовые пароли на ней были использованы. К сожалению, не везде это происходит именно так. Встречаются банки, которые позволяют клиенту использовать карты «интернет-банкинг» многократно, то есть после того, как все одноразовые пароли уже однажды были им использованы для проводки транзакций. Это удобно для клиента (не нужно ехать в банк), но фактически приводит к тому, что процесс применения одноразовых паролей не используется (и действительно, если систе-

1	13419981	13	59342786	25	19485750	37	68615053	49	78389008
2	18987702	14	12461355	26	37959114	38	58466294	50	60504783
3	24467881	15	17753770	27	52105176	39	76902907	51	52102652
4	13402165	16	38967125	28	82184792	40	21008694	52	99622998
5	64354207	17	34668726	29	50344587	41	58367243	53	08131695
6	26726278	18	57494568	30	37780701	42	86805296	54	92571806
7	89394613	19	59772229	31	91882177	43	00146086	55	47509335
8	46788622	20	98288250	32	82073170	44	88272097	56	15456362
9	19502368	21	58009028	33	22135835	45	67026008	57	35744683
10	18244397	22	77287170	34	60829625	46	65804704	58	98453040
11	02352005	23	56611149	35	14975916	47	80599530	59	56127481
12	36467540	24	87138641	36	87678227	48	41057364	60	56775104

Рис. 1. Карта «интернет-банкинг»

ма просит ввести уже использованный ранее одноразовый пароль, это противоречит самому определению одноразового пароля).

Совсем другое дело, если используется аппаратный генератор одноразовых паролей. В данном случае клиент банка становится обладателем неограниченного количества одноразовых паролей, которые меняются каждые 30–60 секунд. После получения одноразового пароля процесс аутентификации в целом идентичен процессу аутентификации при использовании заранее рассчитанных списков паролей, разве что система не запрашивает введения пароля по индексу: она просто просит ввести одноразовый пароль.

Можно выделить ряд проблем, возникающих при использовании одноразовых паролей.

Одноразовый пароль не позволяет использовать двухстороннее SSL-соединение

Если вы обратите внимание, то канал передачи на рис. 2 указан как защищенное SSL-соединение. Следует понимать, что это – одностороннее SSL-соединение, и оно уязвимо к атаке «человек посередине». Однако ограничение технологии одноразовых паролей не позволяет уста-

новить действительно защищенное двухстороннее SSL-соединение. И если мы рассматриваем использование одноразового пароля в качестве аутентификации на web-сервере при входе в систему и предполагаем последующий обмен с этим сервером важными данными, то нужно отдавать себе отчет в том, что эти данные могут быть скомпрометированы.

Невозможность проверки транзакции в системах, использующих одноразовые пароли

Существует мнение, что использование аппаратного генератора OTP не уступает использованию цифрового сертификата на смарт-карте. Как вы уже, видимо, поняли, оно ошибочно. Причем не только потому, что при использовании только технологии одноразовых паролей у нас нет возможности использовать двухсторонний SSL. Дело в том, что банковские системы разбиты на несколько компонентов, и в случае, когда мы не можем добавить электронную цифровую подпись к нашему запросу, все компоненты системы будут вынуждены доверять серверу аутентификации. Это снижает защищенность всей архитектуры в целом и позволяет воспользоваться уязвимостями, эксплуатация которых до этого момента была невозможна или крайне затруднена.

Кроме того, в случае использования одноразовых паролей, возможна компрометация всей системы в целом при компрометации сервера аутентификации OTP.

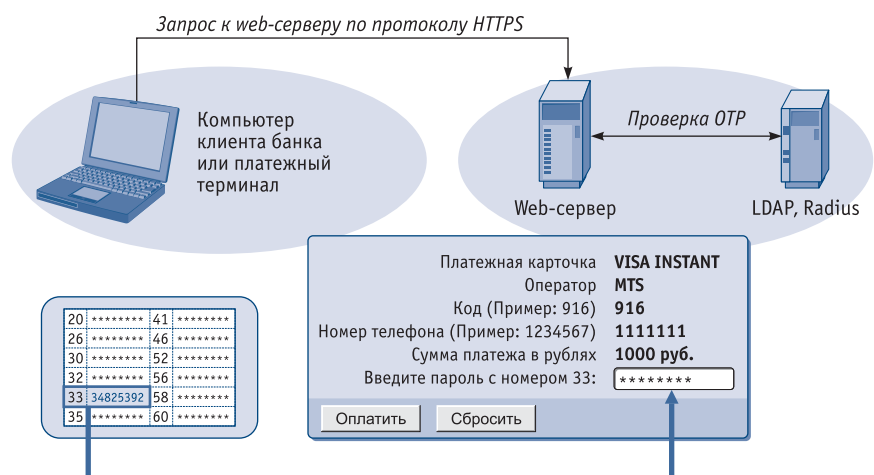


Рис. 2. Использование карточки «интернет-банкинг»

Уязвимости web-приложений в системах, использующих одноразовые пароли

Потенциальной уязвимостью при использовании одноразовых паролей могут стать ошибки web-приложения. И действительно, большинство систем, которые тем или иным образом используют одноразовые пароли, базируются на основе web-технологий. А из этого следует, что различные атаки на web-приложение могут способствовать обходу ввода одноразового пароля. Все зависит от того, на каком уровне и при каких условиях требуется ввод одноразового пароля, и, безусловно, наличие тех или иных уязвимостей в web-приложении.

Например, в случае наличия у нас уязвимости типа «внедрение операторов SQL» вероятнее всего мы сможем получать «правильные» одноразовые пароли, напрямую вытаскивая их из базы данных, тем самым, проходя успешную аутентификацию там, где она требуется.

Другой пример. Предположим, что одноразовый пароль требуется ввести при входе в защищаемую зону web-узла. Тогда уязвимости web-приложения типа «межсайтовое выполнение сценариев», «предсказуемое значение идентификатора сессии» и др. позволят злоумышленнику обойти процесс аутентификации и успешно осуществить несанкционированный доступ к приложению.

Ошибки при реализации системы, использующие одноразовые пароли

Надежность любой системы безопасности в значительной степени зависит от качества ее реализации. Другими словами, у практических решений есть свои недостатки, которые могут быть использованы злоумышленниками в своих целях. В полной мере это правило применимо и к системам аутентификации на базе одноразовых паролей.

Авторами данной статьи проверялась банковская система, использовавшая одноразовые пароли при осуществлении денежных транзакций. Одноразовые пароли генерировались с использованием электронного брелока известного производителя. Ранее банк использовал дру-

гую систему аутентификации при осуществлении транзакций. В процессе аудита выяснилось, что приложение осуществляет транзакцию при вводе пользователем в качестве пароля произвольной строки, чья длина отличается от стандартной. То есть, присутствовала уязвимость, приводившая к тому, что злоумышленник мог обойти процесс аутентификации с использованием одноразовых паролей.

Еще одна уязвимость, с которой авторы статьи встретились при обследовании другой банковской системы, заключалась в том, что, «время жизни» одноразового пароля было достаточным для возможного перебора его значений «в лоб». По заявлениям обслуживающего персонала данной системы, «время жизни» одноразового пароля должно было составлять не более 30 секунд, но проведенный анализ показал, что полученный одноразовый пароль в течение приблизительно 3 часов является действующим. Таким образом, подбор одноразовых паролей доказал высокую эффективность проведения данного вектора атаки при наличии подобной уязвимости: за незначительное время было подобрано несколько действующих одноразовых паролей.

Также к ошибкам реализации системы, использующей одноразовые пароли, можно отнести уже озвученный недостаток с карточками «интернет-банкинг». В случае если они используются многократно, в информационной системе существует, по крайней мере, несколько уязвимостей. Во-первых, защитный слой для OTP-пароля уже стерт, и потенциальный злоумышленник мог (может) видеть его (имея к карте физический доступ), а, во-вторых, получив один OTP-пароль (например, используя вектор атаки типа «фишинг»), он в состоянии осуществить транзакцию, дождавшись момента, когда информационная система попросит ввести ставший известным ему OTP-пароль. Вероятность наступления такого момента можно выразить математической формулой $1 - (59/60)^n$, где n – число экспериментов, n – степень. Данная формула будет работать при условии, что

эпизодичность запросов информационной системы к различным OTP-паролям равномерно распределена. При 100 запросах, вероятность того, что в одном из них встретится известный потенциальному злоумышленнику OTP-пароль, составляет 81,376 %, при 500 запросах – 99,9 %.

Недостатки системы, использующей одноразовые пароли

При утере карточки «интернет-банкинг» или электронного брелока, злоумышленник будет владеть необходимыми «одноразовыми» паролями для осуществления несанкционированных действий. Внимательный читатель может возразить: некоторые системы помимо одноразового пароля требуют для ввода еще и некий «секрет», известного только пользователю, поэтому в случае утери карты «интернет-банкинг» или электронного брелока, пользователь системы может быть спокоен за безопасность своего банковского счета. Оно конечно так, но только до момента, пока этот «секрет» не станет известен злоумышленнику (здесь действуют все методы по компрометации обычного статического пароля). Кроме того, это еще в большей степени усложняет архитектуру системы по обращению с одноразовыми паролями, а значит, возможно, породит новые уязвимости в реализации такой системы.

Уязвимости систем аутентификации на основе одноразовых паролей

В процессе обследования систем, базирующихся на использовании одноразовых паролей, была выявлена фундаментальная уязвимость, которая характерна для всех текущих реализаций при использовании аппаратных генераторов одноразовых паролей. Уязвимость заключается в том, что все системы, в которых используются OTP-токены, рассчитаны на аутентификацию по 6-символьной последовательности цифр. А это означает наличие одного миллиона комбинаций для перебора, который ограничен временем «жизни» одноразового пароля. Таким образом, если мы будем перебирать 150 000 одинаковых комбинаций каждый раз в период «жизни» одноразового па-

роля, то каждый раз с вероятностью в 85 % не сможем подобрать одноразовый пароль. Однако с увеличением числа попыток (экспериментов), вероятность того, что в следующий раз мы сумеем «наткнуться» на уже измененный одноразовый пароль, возрастает. В реализации, когда одноразовый пароль меняется каждые 30 секунд, мы с вероятностью 99 % сможем подобрать одноразовый пароль за 30 попыток, то есть за 15 минут. Этот факт подтверждает следующая математическая формула: $1 - (1 - 0,15)^{30} = 0,9924$, где 30 – число экспериментов, ^ – степень. Данная формула будет работать при условии, что генерация одноразовых паролей равномерно распределена.

Безусловно, чтобы осуществить такой брутфорс при смене одноразового пароля каждые 30 секунд, потребуется ежесекундно отправлять 5000 запросов к серверу, запрашивающему одноразовый пароль. И по большому счету такой брутфорс будет проходить на грани DoS-атаки. Но поскольку текущие технологии позволяют выдерживать подобную нагрузку, указанный вектор атаки реализуем. Следует также учитывать, что не во всех реализациях процесса аутентификации, основанного на использовании одноразовых паролей, время «жизни» такого пароля всегда составляет 30 секунд. Этот показатель может равняться 60 секундам и более (в случае, если есть уязвимость), что по большому счету увеличивает вероятность реализации описанного вектора атаки.

Кроме того, существует еще один небольшой нюанс. Дело в том, что OTP-токены и серверы аутентификации OTP зависимы от времени. И при их использовании существует «окно» рассинхронизации по времени. У каждого вендора, поставляющего OTP-токены, время рассинхронизации различно, но в большинстве случаев это «окно» приблизительно равно пяти минутам. А это означает, что в случае, когда одноразовый пароль меняется каждые 30 секунд, в одно и то же время существует 10 одноразовых паролей, которые сервер аутентификации воспримет как правильные. С учетом данного момента вероятность того, что мы

сможем подобрать одноразовый пароль по схеме, описанной выше, возрастает. Причем, атака может проходить с меньшим числом одновременных попыток аутентификации в секунду за счет увеличения числа проводимых экспериментов.

Атаки на клиентов

Концепция использования одноразовых паролей заключается в возможности прохождения процедуры аутентификации с недоверенного источника, не опасаясь при этом того, что вводимые данные могут быть перехвачены. Насколько действительность при использовании одноразовых паролей соответствует данной концепции?

Существует три основных метода реализации систем с одноразовыми паролями. Первая реализация построена на принципе синхронизации по времени с неким электронным устройством или на наличии внутреннего счетчика (то есть, в течение некоторого (обычно 30-секундного) промежутка времени действует один одноразовый пароль, в следующий аналогичный промежуток времени – другой и т. д.). Вторая реализация основана на принципе смены пароля после его правильного ввода, и последняя – когда система запрашивает некий индекс, а пользователь вводит пароль, привязанный к этому индексу (такой принцип используется в картах «интернет-банкинг»).

Все эти методы уязвимы к атаке на компьютере пользователя. Все дело в том, что злоумышленник может построить атаку следующим образом: после ввода данных для аутентификации никакого обращения на тот ресурс, на котором собственно и происходит аутентификация, со стороны компьютера пользователя происходить не будет. Вместо этого злоумышленник введет полученные данные со своего компьютера (или в скрытом режиме с компьютера «жертвы») и сможет выполнять несанкционированные действия. Для первого случая злоумышленнику нужно будет лишь попасть в диапазон «жизни» одноразового пароля. Второй случай вообще не вызывает затруднений. В третьем – может получиться так, что у злоумышлен-

ника система аутентификации на основе одноразовых паролей запросит отличный идентификатор к этому одноразовому паролю. Но, как уже было отмечено выше, при определенном количестве запросов система неизбежно затребует известный злоумышленнику одноразовый пароль.

Если же рассматривать атаку на компьютер пользователя со стороны специально подготовленных для этого «троянцев», то таковые существуют уже достаточно давно. И они отлично умеют собирать одноразовые пароли, вводимые пользователями с карточек «интернет-банкинг» и отправлять их своим хозяевам.

Таким образом, одноразовый пароль, так же как и статический, уязвим к его перехвату (атаки MITM, «фишинг» и пр.) и не дает никаких преимуществ пользователю при его вводе с недоверенного источника.

Далеко не всегда применение одноразовых паролей может повысить информационную безопасность системы. Следует понимать, что одноразовый пароль – это все та же «парольная фраза», вводимая пользователем. Только обращение с ней более сложное и перенесено с пользователя на систему, реализующую данный функционал. Поэтому совместно с использованием одноразовых паролей требуется дополнительный комплекс мероприятий, снижающий потенциальные риски информационной безопасности при использовании OTP.

В качестве меры противодействия описанным уязвимостям в системах, использующих одноразовые пароли, необходимы те же методы, которые применяются для противодействия злоумышленнику в системах, использующих статические пароли: различные временные задержки при вводе пароля, временное блокирование учетной записи при многократных ошибках аутентификации, использование CAPTCHA и т. д. ■

ЛИТЕРАТУРА

1. Давлетханов М. Концепция одноразовых паролей в системе аутентификации // ВУТЕ/Россия. №№ 7–8 (95).
2. <http://www.aladdin.ru>
3. <http://www.rsa.com>