SecurEnvoy

Официальный документ

Варианты двухфакторной аутентификации

Авторы: Эндрю Кемшелл
Фил Андервуд

Дата: июль 2011 г.

Оглавление

1. Проблемы с паролями

Надежность пароля

Общий принцип – следующий: чем длиннее пароль, тем он надежнее; это напрямую относится к математике.

Пароли могут быть связаны с криптографическими значениями, которые зависят от числа переменных. С помощью дополнительных переменных, таких как верхний регистр, нижний регистр и числа, можно создать более надежные пароли.

Длинные пароли хорошо выполняют свою функцию, но следует учитывать следующее, например:

Пароль пользователя 1 = redcheese6
Пароль пользователя 2 = zglihalq

Пароль пользователя 1 состоит из 2 слов и одной цифры; если предположить, что в английском языке можно легко запомнить 20 000 слов, то надежность пароля составляет 20К * 20К * 10 = 4 миллиарда комбинаций или (в терминах криптографической надежности) 32-битовый ключ.

Пароль пользователя 2 представляет собой 8 произвольно заданных символов, поэтому, надежность составляет 26 в степени 8 = 208 миллиардов комбинаций или (в терминах криптографической надежности) 38-битовый ключ.

Пароль пользователя 2 надежнее и превосходит надежность пользователя 1. Однако для получения такой надежности от пользователя обычно требуется фотографическая память, либо данный пароль следует записать.

Взломы паролей

Теперь, когда нам известно понятие надежности пароля, как его защитить от взлома? К сожалению, универсального средства не существует. Надежные пароли трудно запомнить, и часто на мониторе компьютера можно увидеть стикер с написанным на нем паролем.

Практически половина всех взломов паролей выполняется физическими методами с использованием навыков и знаний в сфере прикладной социологии.

Самый простой способ – прочесть надпись на стикере, прикрепленном к компьютеру коллеги, либо «подсмотреть» пароль по клавишам, нажимаемым во время входа в систему.

Более изощренные взломы – использование программных средств для отслеживания нажатий клавиш при регистрации в системе, которые потом передаются злоумышленнику для последующего использования. Шпионское ПО может установиться при заражении компьютера вирусом, троянской или шпионской программой, которые иногда автоматически загружаются с веб-сайтов (все это происходит без ведома пользователя). Такие атаки наиболее неприятны, потому что пользователь не знает, что его пароль взломан, и не может ничего сделать до тех пор, пока не будет слишком поздно.

Сетевое слежение – еще один распространенный тип атак, когда такие программы, как Cain, Able, Dsniff «снимают» пароли во время их прохождения по сети. Такие программы захватывают регистрационную информацию в веб-сети, на FTP и в телекоммуникационных сетевых протоколах (telnet используется с сетевым коммуникационным оборудованием или в системах Unix). Такие программы срабатывают очень эффективно и с минимальными настройками или вмешательством пользователя.

Пароли проходят по сети одним из двух способов.

При первом методе пароль передается в форме простого текста, поэтому любое использование дешифратора протокола сделает возможным получение пароля в виде простого текста.

Второй способ обеспечивает некоторую защиту хешированием пароля. Алгоритм хеширования – односторонняя функция, при которой пароль в виде простого текста трансформируется в хэш (случайные данные) фиксированной длины. Типичные программы хеширования – MD5 и SHA-1, дающие на выходе 128- и 160-битовые хэши.

Однако взломщикам достаточно легко уничтожить хэш с помощью программных средств для генерирования файла словаря разных паролей и их прогона через тот же алгоритм хеширования. Если выход из этого алгоритма – тот же, что и хэш, то пароль известен. Данный метод называется «грубой атакой». В настоящее время на рынке имеются коммерческие программы, например, LOphtCrack.

Мощность современных технологий позволяет взломать даже самые надежные пароли. Современный компьютер на базе Pentium с программой LOphtCrack может поддерживать взломы паролей со скоростью 3 миллиона в секунду. Если бы эта программа использовалась в нашем примере, то все пароли были бы взломаны спустя следующие значения времени.

Пользователь 1	менее чем через 23 минуты!
Пользователь 2	менее чем через 20 часов

Наконец, паролями сложно управлять, поскольку пользователи обычно сами придумывают свои пароли.
Ниже представлен фрагмент проверки, проведенной для крупного клиента. Были проверены 342 пароля учетных записей.

29 пользователей имели пароль **«password»**.
1 пользователь имел пароль **«password 1».**
4 пользователя имели только цифры, из которых, два пароля выглядели как дата рождения.
3 пользователя имели пароли из 5 символов.

Ключом к предотвращению всех рассмотренных атак на пароли является одноразовый динамический пароль, который можно использовать при его первой отправке. Любая попытка записать и воспроизвести пароль делает его недействительным, поскольку первоначальный пароль уже заблокирован. Данный метод также называется надежной двухфакторной аутентификацией.

2. Проблемы с сертификатами (без смарт-карт)

Использование цифровых сертификатов на пользовательском ПК снимет необходимость применения токенов или смарт-карт и решает все рассмотренные проблемы со взломами паролей; однако у них имеются собственные проблемы, связанные с управлением, поддержкой и безопасностью.

От пользователей роуминга потребуется носить свои сертификаты с собой для получения доступа, например, в гостинице, Интернет-кафе, со смартфона или с домашнего компьютера. Пользователи, импортирующие свои сертификаты в компьютер общего доступа, подвергают собственную безопасность серьезной угрозе, если забывают удалить сертификат по окончании работы.

Цифровые сертификаты хранятся на компьютере, который они используют. Это приводит к возникновению ряда проблем обеспечения безопасности, если несколько пользователей имеют доступ к одному компьютеру. Данный подход особенно проблематичен там, где компьютеры установлены в общественных местах: в школах, библиотеках или гостиницах.

Надежные принципы аутентификации требуют, чтобы физическое устройство было закреплено за человеком, который аутентифицируется. Данный принцип нарушается, когда компьютер используется несколькими лицами. Большинством домашних компьютеров пользуются все члены семьи!

Как правило, пользователи не делают резервных копий личных ключей в своих браузерах, и, следовательно, они будут утеряны, если диск переформатировать, или произойдет сбой в его работе. С появлением агрессивного рекламного программного обеспечения, снижающего производительность компьютеров, можно ожидать, что для незащищенных компьютеров потребуется полная смена системы минимум раз в год.

3. Принципы надежной двухфакторной аутентификации

Для идентификации личности существуют три области, которые можно использовать для аутентификации.

Первая область: пользователь должен запомнить секретный код, пароль или пин-код – то, что известно только ему.

Вторая область аутентификации – использование физических устройств, как то: ключей, кредитных карт или сотового телефона – то, что принадлежит только их владельцу.

Последняя область аутентификации – биометрическая, например, отпечаток пальца.

Принцип двухфакторной аутентификации – использование двух из указанных областей для обеспечения более высокого уровня аутентификации.

Хороший пример двухфакторной аутентификации применяется в повседневной жизни в банкоматах. Для снятия наличных с банкомата в него сначала нужно вставить кредитную карту (принадлежащую владельцу), после чего ввести пин-код (известный владельцу). При утере кредитной карты остается второй фактор (пин-код) для защиты кредитной карты до тех пор, пока банк не будет извещен о том, что карта утеряна.

Двухфакторная аутентификация компании SecurEnvoy работает по тому же принципу, что и банкоматы, за исключением того, что используемое устройство – это сотовый телефон, а не кредитная карта.

Наконец, важно, чтобы устройство владельца было аутентифицировано способом, предотвращающим все атаки, описанные в разделе 1. Это делается с помощью одноразового кода-пароля, который после аутентификации блокируется для предотвращения любых атак злоумышленников, пытающихся «подсмотреть через плечо», определить регистрационную информацию по нажатию клавиш, отследить протоколы связи или организовать грубую атаку.

4. Принадлежащие владельцу устройства (типы аутентификации)

4.1 Смарт-карты

Основной проблемой успешного применения смарт-карт является их зависимость от считывающих устройств. Стратегия аутентификации, основанная на данном методе, может быть целесообразной в среде с управляемыми считывающими устройствами, например, банкоматами или в киосках, активируемых смарт-картами. Однако применение данного подхода в Интернет-сообществе имеет следующие серьезные ограничения:

Доступ с домашнего ПК
Применение встроенных считывающих устройств для смарт-карт на рынке домашних ПК практически не распространено. Пользователям потребуется приобрести необходимое считывающее устройство и установить требуемое ПО. Для ПК более ранних моделей с установленными операционными системами Windows 9* или Windows 2000 потребуется дополнительный этап установки программного обеспечения Microsoft Smartcard Base. Поэтому, вполне вероятно, что в этом случае количество обращений в службу технической поддержки будет довольно большим.

Доступ с ПК другой компании
Корпоративные ПК обычно выпускаются без считывающих устройств для смарт-карт и заблокированы во избежание установки неавторизованного программного обеспечения. Даже если конечный пользователь приобрел считывающее устройство для смарт-карт, то установка нужного ПО вряд ли окажется возможной. Использование смарт-карт, выпущенных другими компаниями, неприемлемо.

Доступ из гостиниц, Интернет-кафе или Интернет-киосков
Здесь смарт-карты также практически не распространены, поскольку эти среды заблокированы; даже если у пользователя имеется считывающее устройство, потребуется установка программного обеспечения, что невозможно. Использование смарт-карт в этих средах также нецелесообразно.

Доступ со смартфонов, Blackberry, PocketPC и т.д.
За последние 5 лет наблюдался экспоненциальный рост спроса на смартфоны, включающие в себя Интернет-браузеры. Из-за компактных размеров этих устройств установить на них считывающее устройство не возможно, поэтому, использование смарт-карт в этих средах – так же не целесообразно.

4.2 Токены

Устройства с токенами предлагают пользователям явные преимущества в том, что их можно использовать в любой среде, и они не требуют дополнительных аппаратных или программных средств на пользовательских ПК или на смартфонах. Однако здесь необходимо учитывать следующее:

Развертывание
Каждый токен должен быть присвоен и развернут для пользователя, который подлежит аутентификации. Это дорогостоящее мероприятие, включающее рассылку токенов надлежащим пользователям, после чего перед активацией необходимо убедиться, что каждый пользователь получил соответствующий токен.

Утерянные или вышедшие из строя токены
При опросе в 5 компаниях, применяющих технологию использования токенов, в среднем 10% развернутых токенов вышли из строя или были утеряны и требовали замены! По этой причине следует закладывать дополнительные 10%-е расходы на дополнительные токены. Более того, для таких пользователей следует предусмотреть аварийный доступ, пока они ждут получения новых токенов, но по-прежнему нуждаются в доступе.

Краткосрочные подрядчики или бизнес партнеры

Данный тип пользователей связан с дополнительными затратами на развертывание, и они не всегда возвращают свои токены по окончании действия контракта. Это приводит к дополнительным затратам на поставку, администрирование и развертывание новых токенов.

B2B электронная коммерция и торговля
Когда двухфакторная аутентификация необходима для проведения операций между компаниями, то использование токенов выглядит нецелесообразным. Представьте себе покупателя, который хочет вести бизнес с 20 компаниями, и всем им нужны токены. Покупателю потребуется обслуживать 20 идентичных токенов и находить способ соотнесения корректного токена к соответствующей компании. Данный подход не только неудобен, но и затратен как по самим токенам, так и по их развертыванию в компаниях, которые его предпочли.

Повторное развертывание каждые 3-4 года
Некоторые токены, например, RSA Security, имеют фиксированный срок службы 3-4 года и требуют замены и повторного развертывания во всей существующей пользовательской базе. Другие типы токенов могут служить дольше, однако, вследствие их частого использования и постепенного износа их замена неизбежна.

Безопасность
Токен нужен лишь тогда, когда владельцу требуется аутентификация с его помощью, поэтому обнаружение пропажи токена или заявление о том, что токен украден, вряд ли будут сделаны до очередной регистрации пользователя. К тому времени, когда будет обнаружена пропажа, может быть уже поздно!

Что касается мобильных телефонов, то они являются средством связи пользователя с внешним миром, и пропажа телефона будет обнаружена сразу же, когда потребуется сделать звонок. Поэтому заявление об утрате мобильного телефона будет сделано намного раньше.

Удобство для конечного пользователя
Что удобнее: носить с собой мобильный телефон и токен или только мобильный телефон? Ответ очевиден. Пользователю бывает очень досадно обнаружить, что он забыл токен и не может войти в систему.

4.3 Аутентификация на базе телефона

Согласно текущим оценкам, в настоящее время в Россиии используется более 130 миллионов мобильных телефонов; ежегодно отправляется и принимается более миллиарда SMS-сообщений. Также, по оценкам, на каждый продаваемый в мире ПК приходится 3,5 проданных сотовых телефона. Столь крупный масштаб развертывания сотовой связи делает целесообразным использование данного способа связи для надежной аутентификации.

В целом производители используют два подхода:

1. Программное обеспечение, установленное на телефоне, которое генерирует одноразовый код-пароль
Основной проблемой использования ПО, установленного в телефоне, является процедура его запуска! Большое разнообразие пользовательских интерфейсов на разных моделях телефонов чрезвычайно затрудняет работу персонала технической поддержки. Ему приходится полностью обучаться обращению со всеми поддерживаемыми моделями телефонов, чтобы научить пользователей навигации по нужным меню и подменю для перехода в раздел Java с последующим запуском соответствующей программы аутентификации. Кроме того, для установки дополнительных программных средств некоторые модели телефонов должны быть подключены к компьютеру; в других моделях для загрузки ПО можно пользоваться телефонным браузером. Оба способа требуют от пользователя понимания программного обеспечения и умения его устанавливать.
Общепризнано, что поддержка более чем одной операционной системы приводит к значительным техническим сложностям. Подход, требующий установки программного обеспечения на сотовый телефон, можно считать приемлемым для развертывания на одной или нескольких моделях сотовых телефонов.

Наконец, следует помнить, что пользователей, не имеющих корпоративного сотового телефона, приходится «заставлять» использовать личный телефон. Добавление новой программы на личный телефон не только не приветствуется, но и является вторжением в частную собственность, в данном случае в личный телефон сотрудника. Для сравнения: отправка одноразового SMS-сообщения не более навязчиво, чем общение пользователя с другим человеком, особенно, если его номер будет храниться в тайне и использоваться только для отправки SMS-сообщений аутентификации.

2. Аутентификационная информация, отправляемая по SMS в реальном времени.
Все сотовые телефоны стандарта GSM можно поддерживают использование SMS- сообщений без необходимости дополнительного программного обеспечения на телефоне. Однако, отправка данных для аутентификации на телефон пользователя в режиме времени, близком к реальному, является неверным подходом. Неразумно ожидать, что данный текст придет сразу после того, как пользователь введет имя и пин-код, поскольку текстовые SMS-сообщения могут задерживаться в периоды пиковых перегрузок. Кроме того, если пользователь расположен в зоне, где сотовый сигнал не принимается, особенно в зданиях с толстыми каменными стенами, то входящее SMS-сообщение получить невозможно!

4.4 Простота использования

На рынке аутентификации с помощью токенов принято использовать шестизначный номер, поскольку он легко читается, и в комбинации с пин-кодом позволяет получить коды аутентификации, состоящие от 10 цифр (пин-код из 4 цифр) до 14 цифр (пин-код из 8 цифр).

В некоторых подходах используется сложное шифрование, выполняемое человеком, где SMS-сообщения содержат 20 цифр. В этом случае пользователь, которому нужно аутентифицироваться, получает код аутентификации из первых 10 цифр, преобразуя их с использованием следующих 10 цифр для формирования новой зашифрованной версии пин-кода. Данный подход – сложный и трудоемкий для пользователей и, скорее всего, они его не воспримут.

5.0 Решение SecurEnvoy

Одноразовый код-пароль
Одноразовый динамический код предотвращает все атаки на пароль, рассмотренные в **разделе 1.**

Простота использования
Принцип SecurEnvoy – использовать простые 6-значные коды в текстовом SMS-сообщении, поскольку они легко читаются и просты в обращении. В комбинации с пин-кодом SMS-сообщение позволяет получить коды аутентификации, состоящие из 10 цифр (пин-код из 4 цифр) или 14 цифр (пин-код из 8 цифр).

Не требуется устанавливать дополнительное программное обеспечение на мобильный телефон пользователя
Этим обеспечивается поддержка всех мобильных телефонов, и снимаются проблемы обслуживания, связанные с управлением таким ПО на разных моделях телефонов.

При регистрации пользователя не требуется SMS-сообщение в режиме реального времени
При первой регистрации пользователя ему направляется первый одноразовый код-пароль. Предварительная отправка первого нужного кода-пароля дает пользователю достаточно времени для получения 6-значного кода-пароля. Если мобильный телефон пользователя временно находится вне зоны действия, выключен или провайдер занят, то SMS-сообщение сохраняется, и его отправка регулярно повторяется (обычно это происходит в течение 4 дней, пока сообщение не будет успешно передано пользователю).

В маловероятном случае, когда у пользователя нет доступа к сотовому телефону, 6-значный код-пароль может быть передан по обычной телефонной линии в форме голосового сообщения через операторов мобильной связи.

После этого конечный пользователь подключается к своему защищенному корпоративному ресурсу, где он должен ввести логин, пин-код и код-пароль.

Логин:	Тот же, что используется в Microsoft или в другом каталоге LDAP.
Пин-код:	Число из 4-8 цифр или пароль Microsoft.
Код-пароль:	6-значный код, отправленный ранее пользователю по SMS.

Примечание: Пин-код может быть сконфигурирован как пароль Microsoft для текущих пользователей или как код, состоящий из 4-8 цифр

Если введен неправильный пин-код или пароль, то на мобильный телефон пользователя отправляется новый пароль. И даже если этот пароль будет удален, то еще один новый пароль будет по-прежнему доступен.

Если неправильные пин-коды или коды-пароли введены больше 10 раз, то пользователь деактивируется, и новые коды-пароли высылаться не будут. Данная мера безопасности направлена на предотвращение грубых хакерских атак.

Коды-пароли отправляются на телефоны пользователей так, что новый код стирает старое сообщение, поэтому удалять сообщения со старыми кодами не требуется. В мобильном телефоне пользователя всегда будет только одно SMS-сообщение с паролем, полученное с сервера безопасности, который динамично обновляется.

Security Server интегрируется непосредственно в самые распространенные серверы каталогов, поддерживающие LDAP, благодаря чему не нужно создавать новую базу данных пользователей или синхронизировать ее с другими базами данных.

6.0 Расходы на SMS

Обычному пользователю с удаленным доступом потребуется аутентификация только один раз в день, после чего в оставшееся время сеанса (как правило, 8-часового) будет использоваться VPN или cookie в браузере. В худшем случае пользователь всегда работает удаленно, и ему приходится аутентифицироваться каждый рабочий день. В году 270 рабочих дней; с учетом праздников получается порядка 250 аутентификаций в год.

Наиболее распространенные однопользовательские тарифы провайдеров включают в себя SMS-сообщения по цене до 2 рублей за одно SMS. Корпоративным масштабным клиентам одно сообщение мобильного оператора МТС обходится 34 копейки. Таким образом, в худшем случае стоимость SMS-аутентификации при цене 0,34 рубля за сообщение составляет 250 * 0,34 = 85 рублей на одного пользователя в год.

Некоторые коммерческие корпоративные тарифы для мобильных телефонов предусматривают бесплатные телефонные звонки или сообщения внутри корпоративной сети. Эти бесплатные SMS-сообщения могут передаваться через модем Wavecom или Siemens, которые поддерживают SIM-карту GSM.