Я угадаю Ваш пароль

> Тарас Злонов, CIO-World, 24 февраля 2009 года

Сегодня, когда на рынке средства для аутентификации пользователей постоянно появляются новые решения, всё чаще можно слышать утверждение, что парольная аутентификация отжила свой век.

Обычно такие размышления предшествуют рекламе очередного аппаратного, программного или, что, конечно же, ещё лучше, аппаратно-программного решения для безопасной, надёжной, гарантированной аутентификации пользователей, лишённого общеизвестных недостатков паролей. На самом деле всё не так просто. Да, действительно, пароли взламывают, подсматривают, подбирают, перехватывают и просто угадывают, но стоит ли от них отказываться?

Пароли обеспечивают вполне приемлемый уровень безопасности во многих случаях, но это должны быть не те пароли из 5–6 символов, к которым мы все привыкли, а действительно надёжные пароли. В сущности, конфиденциальность информации в современных алгоритмах шифрования обеспечивается ключом, т.е. тем же паролем. Вот только ключ имеет длину 256 и более бит, что примерно равносильно случайному 40-символьному паролю из строчных и заглавных латинских букв, цифр и спецсимволов [Учитывался знак “пробел” и следующие 32 символа: `~!<>;%:?*()_+`@#$^&–=/\|.,[]{}'"`]. Такой пароль подобрать за разумное время не получится, вот только вряд ли кто-либо будет его использовать.

Таким образом, пароли, безусловно, имеют определённые слабости, но главная уязвимость заключается всё же в способе, которым пользователи их выбирают. Принято считать, что надёжность пароля тем выше, чем больше времени потребуется для его подбора. Соответствующие утилиты по перебору паролей популярны среди хакеров и рядовых пользователей. Отдельные компании даже зарабатывают, продавая такие утилиты.

Попробуем разобраться с тем, как работают данные программы. Ведь злоумышленник, который захочет получить доступ к Вашим данным, будет, скорее всего, использовать их же.

По мере роста производительности персональных компьютеров утилиты подбора паролей также увеличивали скорость перебора - для некоторых приложений скорость проверки может достигать нескольких сотен тысяч паролей в секунду. В отдельных случаях производительности одного компьютера всё же оказывается недостаточно и, чтобы не тратить на взлом месяцы, злоумышленники используют распределённые вычисления. В частности, заражённые вирусом компьютеры, объединённые в бот-сеть, могут ускорить процесс подбора пароля в тысячи раз.

Рост мощности и распределённые атаки были доступны взломщикам не всегда, поэтому им, особенно раньше, нужны были более простые способы повышения эффективности перебора. И такие способы были найдены. В их основе лежит так называемый “человеческий фактор”. Несмотря на то, что, например, 6-символьных паролей на обозначенном выше множестве символов может быть около 700 миллиардов, на практике большая их часть никогда не будет использоваться пользователями в качестве паролей, а значит, нет необходимости делать полный перебор всех вариантов.

Типичный пароль, как правило, состоит из корня и дополнения, которое в 90% случаях “дописывается” в конец пароля, а в 10% - в начало. Пароли, в которых одновременно есть добавления и в начале и в конце, - большая редкость. В качестве корня не обязательно используется слово из словаря, но чаще всего это всё же что-то осмысленное.

Утилиты для подбора паролей идут методом последовательного приближения. Суть его состоит в том, чтобы попытаться сэкономить время, перебирая сначала наиболее простые варианты. Так, в первую очередь проверяются слова из словарей. Словари могут использоваться, конечно, и энциклопедические, но обычно взломщики ограничиваются специальными парольными словарями, в которых всего несколько тысяч слов (обычно не более 5 000), таких как: `password`, `12345`, `qwerty` и т.д. Основой для составления таких словарей чаще всего служат взломанные базы данных учётных записей публичных сайтов. Именно по результатам анализа таких баз и выбираются наиболее популярные слова, которые пользователи применяют в качестве паролей.

Дополнения к корню пароля так же весьма специфичны и на практике используются такие, как: `1`, `+`, `!` и т.д.(всего около 100 различных вариантов). Вторым этапом при взломе пароля проверяются все возможные комбинации слов из словаря с разными дополнениями. По статистике 24% паролей попадают в эти 500 000 вариантов, на проверку которых уйдет буквально несколько минут.

Для взлома остальных паролей используется более широкий спектр словарей - английские слова, русские слова, набранные в транслите, имена собственные, русские слова, набранные при включенной английской раскладке и т.д. В качестве дополнений помимо уже упомянутых пробуются сочетания двух цифр (`12`, `90`...),года (`1980`, `2009`...), одиночные символы и т.д.

В качестве ещё одного приёма по повышению надёжности паролей пользователи применяют хитрые замены, например, “`@`”вместо “`a`”, “`$`” вместо “`S`” и т.д. Злоумышленники учитывают и это. Также практически всегда проверяются цифровые пароли, т.е. пароли состоящие из одних только цифр: их не так много, но пользователей, выбирающих для паролей номера телефонов или другие числовые последовательности достаточно много.

Затратив от нескольких часов до нескольких дней с применением описанных выше методик можно подобрать около 2/3 всех паролей.

Важно, что в рассматриваемых подходах никак не учитывается личность пользователя. На практике любая информация о пользователе может существенно ускорить процесс подбора его пароля. Почтовые индексы, имена людей из адресной книги, важные даты и т.д. - всё идёт в ход. При наличии возможности злоумышленник составляет словарь пользователя, сканируя все файлы на его жёстком диске, собирая слова, в том числе и из удалённых файлов. Если пароль хотя бы раз оказался в исходящем или входящем письме, был когда-то записан в какой-либо файл или оказался в сохранённых данных какой-либо программы, злоумышленник его постарается найти.

Между тем, создать сложный пароль, неподдающийся описанным выше атакам совсем не сложно и под силу любому пользователю. Например, можно набрать в английской раскладке первые буквы стихотворения “`У лукоморья дуб зелёный, златая цепь на дубе том`”, причём слово “`дуб`” - заглавными буквами и полностью: `ekLE<ppwyln`. Полученный 11-символьный пароль запомнить элементарно, а подобрать крайне сложно.

Или ещё пример: пароль из 27 символов `69728ooh3f34t73wwj60qww294e` - всего лишь фраза “`you will never guess my password`”, набранная с помощью клавиш, расположенных на один ряд выше (`y -> 6`, `o -> 9`, `u -> 7` и т.д.).

Все хорошо понимают, но почему-то пренебрегают тем фактом, что даже самый надёжный пароль может оказаться бесполезным, если записать его в легкодоступном месте, или если один и тот же пароль использовать сразу в нескольких приложениях. Не стоит для почтового ящика на публичном сервере использовать тот же пароль, что и для доступа к системе теле-банк. Ведь пароль, передаваемый в открытом виде на почтовый веб-сайт или вводимый с клавиатуры на случайном рабочем месте, может легко попасть в руки злоумышленнику. К тому же не редко отдельные сайты после ответа на элементарный “секретный” вопрос просто высылают пароль в открытом виде по почте.

Придуманный сложный пароль в самом крайнем случае можно записать, но тогда записку надо хранить в надёжном месте, а записать лучше не сам пароль, а например, предложение с его использованием, а ещё лучше - подсказку, которая позволит вспомнить пароль. Скажем, в приведённом выше примере можно было бы записать “`A.C. Пушкин, начало, ДУБ`”. С такой очевидной для Вас подсказкой вряд ли хоть кто-то догадается, о чём идёт речь.

Другой вариант хранения паролей - использование специальных программ-сейфов. Такие приложения хранят пароли от других программ и веб-сайтов в шифрованном виде, защищённом с использованием мастер-пароля, который, естественно, должен быть максимально сложным.

Подводя итоги, заметим, что сегодняшнему многообразию способов и методов аутентификации способствует вовсе не “архитектурная” слабость паролей, а лишь неправильное их использование. Хотя, вне всякого сомнения, для отдельных задач, особенно когда речь идёт об удалённом доступе, обыкновенная парольная аутентификация совершенно не приемлема. Как минимум, она должна быть дополнена протоколом установления защищённого соединения.