электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 621.382

Метрики стойкости парольной защиты

Марков Г.А.

Студент, кафедра «Информационная безопасность» МГТУ им. Н.Э. Баумана, г. Москва, Россия

Научный руководитель: Цирлов В.Л., кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, г. Москва, Россия

МГТУ им. Н.Э. Баумана
gm@cnpo.ru

Подсистема аутентификации является первым рубежом в системе защиты информации компьютерной системы. Традиционными системами аутентификации являются основанные на секретных идентификаторах - паролях. К сожалению, парольные системы уязвимы по объективным и субъективным причинам, например, по причине выбора нестойкого пароля, наличия уязвимостей в системах и протоколах аутентификации, распространенности систем подбора паролей и систем перехвата и др. Например, согласно статистике, 80% инцидентов в области информационной безопасности связаны с компрометацией парольной защиты [1,7]. Известен ряд мероприятий, направленный на повышение безопасности парольной защиты, например, генерация стойких паролей и внедрение соответствующей парольной политики безопасности. К недостаткам последнего подхода можно отнести то, что требования к паролям, как правило, определяются вербально, например, формулируется требование, согласно которому длина пароля должна быть больше шести или восьми символов. В работе рассмотрены метрики (показатели стойкости паролей), позволяющие сформулировать формальные требования к стойкости паролей, исходя из возможности их компрометации, а также проведено исследование парольной защиты на примере социальных сетей.

Требования к парольным системам

В общем плане пароль представляет собой последовательность символов, позволяющих пользователю получать доступ к ресурсам и процессам компьютерной системы. Известно, что вероятность подбора паролей рассчитывается по следующей формуле:

$$P = \frac{V \cdot T}{|A|^n},$$

где: V – скорость подбора пароля злоумышленником, T - срок действия пароля, A - алфавит паролей, $|A|^n$ - мощность пространства паролей, n - длина пароля.

В настоящее время в российских стандартах имеются требования к повышению стойкости парольной защиты, касающиеся, главным образом, минимальной длины пароля. Например, в руководящих документах Гостехкомиссии России определено, что «в автоматизированной системе должны выполняться идентификация и проверка подлинности субъектов доступа при входе в нее по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов» [6].

Подобные требования можно встретить в зарубежных стандартах [11, 12].

Ориентируясь на указанные стандарты и общепринятую практику можно сформулировать определение слабого («ненадежного») пароля, который может быть относительно легко подобран. Пусть слабый пароль - это пароль, который: короткий (меньше 8 символов), набран в одном регистре, набран в простом алфавите (только символы или только цифры), найдется в общедоступных словарях, как-либо связан с владельцем, так что может быть отгадан. С точки зрения автоматизации оценки стойкости парольной защиты представляет интерес получить формальные показатели стойкости паролей.

Метрики стойкости паролей

Существуют различные показатели стойкости парольной защиты, называемые парольными метриками, а именно:

- численные метрики;
- вероятностные метрики;
- информационная энтропия по Шеннону;
- эвристические модификации энтропии;
- вероятностные модификации энтропии.

Численные метрики, как правило, представляют нормированные значения времени получения пароля методом прямого перебора [3]. Такой подход, к сожалению, не учитывает современные методы целенаправленного перебора и угадывания, а также должен учитывать особенности интерфейса и имеющиеся вычислительные мощности.

Вероятностные метрики и вероятностные модификации получают, исходя из анализа имеющейся статистики парольных баз для конкретных систем [2, 8]. К недостаткам метрик относят необходимость наличия базы паролей по системе или выполнение аппроксимации имеющейся статистики к реальной системе. С точки зрения результативности атаки на парольную систему, использование вероятностей может быть не всегда оправдано, т.к. факт самого нахождения пароля в словаре (в условиях современной вычислительной базы) сводит его энтропию к нулю.

По указанным причинам в работе рассмотрены информационная энтропия по Клоду Шеннону [6] и «эвристическая» энтропия, рекомендованная стандартом NIST [10]. Отличие идеологий метрик состоит в предположениях, используемых при их обосновании: Шеннон предположил, что пароли генерируются случайным датчиком, в документе NIST полагается, что пароль выбирается человеком.

Итак, в качестве основной метрики мы используем понятие информационной энтропии по Шеннону:

$$H(A^*) = log_2|A^*| = log_2|A|^n = n \cdot log_2|A| = n\frac{ln|A|}{ln2},$$

где: $|A|$ - мощность алфавита, *n* - длина пароля.

Метрика показывает, чем случайнее набор символов, тем надежнее пароль и тем сложнее его запомнить. Любые попытки сделать пароль запоминающимся приводит к снижению энтропии и предсказуемости пароля.

Согласно метрике можно показать, что пароль, например, состоящий из 7 цифр, практически эквивалентен паролю, состоящему из 5 латинских символов одного регистра (см.табл.1).

Таблица 1

Примеры энтропий паролей, бит

Алфавит\Длина	5	6	7	8
ab..z	**23.5**	28.2	32.9	37.6
1234567890	16.6	19.9	**23.2**	26.5
ab..zAB..Z123467890	29.7	35.7	41.6	47.6
ab..zAB..Z1аб..яАБ..Я123467890	35	41.9	48.9	55.9

Рекомендациям NIST можно сопоставить следующую формулу энтропии пароля, созданного человеком (а не генератором паролей):

$$S(A,n) = 4 + \sum_{\substack{i=2 \\ i\le n}}^{8} 2_i + \sum_{\substack{i=9 \\ i\le n}}^{20} 1.5 + \sum_{\substack{i=21 \\ i\le n}}^{n} 1 + 6\chi_A,$$

где: n - длина пароля, n>1; χ_A – характеристическая функция наличия в пароле неалфавитных символов или символов в верхнем регистре.

Указанная формула, проще говоря, означает, что энтропия первого символа равна 4 битам, энтропия следующих семи символов - по 2 бита на каждый, от 9-го до 20-ый символ по 1.5 бита энтропии на символ, 21-ый символ и дальше несет в себе 1 бит энтропии. Однако, если используется также верхний регистр букв или неалфавитные символы, то добавляется ещё 6 битов. К примеру, сложный пароль из 8 символов будет иметь энтропию 24 бит.

Таким образом, слабый пароль формально может быть определён двумя метриками: энтропией в 56 бит по Шеннону и энтропией в 24 бит согласно стандарту NIST.

Исследование стойкости парольной защиты в социальных сетях

За последние годы в результате хакерских атак были неоднократно скомпрометированы базы паролей социальных сетей [8]. Например, в Интернет в то или иное время были доступны базы: black list twitter-2010, twitter-2011, vk-2009 и др. Также известны базы паролей вирусных программ (например: conficker, morris-worm и др.), тестовая база rockyou, база скомпрометированных паролей hotmail и др.

Для исследования была представлена скомпрометированная база парольной защиты одной отечественной социальной сети, содержащая имя почты и пароль. В результате обработки базы с помощью исследовательской программы [5] была получена статистика, представленная в табл.2-4.

Таблица 2

Результаты исследования парольной базы

Всего исследуемых паролей	83524
Число паролей состоящих только из цифр	17382 (20.8%)
Число паролей состоящих только из букв	38684 (46.3%)
Число паролей состоящих только из букв и цифр	27458 (32.9%)
Число паролей состоящих только из русских букв	15562 (18.6%)
Число паролей состоящих из английских букв	17632 (21.1%)
Число паролей состоящих из русских и английских букв	05490 (6.6%)

Таблица 3

Проверка наличия слабого пароля

Меньше 8 символов	30798 (37%)
Символы одного регистра	58514 (70%)
Совпадает с именем почты	00776 (1%)
Совпадает со словарем	03675 (4.4%)
Содержит телефон	07700 (9.2%)
Слабые пароли (энтропия меньше 56 бит)	67451 (80.7%)

Таблица 4

Топ-5 распространённых паролей в России

Пароли	Энтропия по Шеннону	Энтропия по NIST	Энтропия с учетом словарей
123456	20	20	0
123456789	30	26	0
qwerty	28	14	0
111111	20	20	0
1234567890	33	27	0

Выводы

1. Исследование показало, что при определении требований к стойкости парольной защиты целесообразно использовать не вербальные описания, а энтропийные метрики. Такие парольные метрики больше учитывают стойкость систем аутентификации к атакам на подбор паролей и их удобнее использовать при верификации безопасности систем.

2. Если сравнить результаты исследования с общедоступной ретроспективной статистикой [4, 9], то можно сделать выводы, что простые пароли практически не изменились, модными паролями сейчас являются сотовые телефоны, наблюдается незначительная тенденция к усилению парольной защиты благодаря новым парольным политикам интерфейсов социальных сетей.

Список литературы

1. Беленко А. Пароли: стойкость, политика назначения и аудит // Защита информации. Инсайд. 2009. № 1. С. 61-64.

2. Гуфан К.Ю., Новосядлый В.А., Эдель Д.А. Оценка стойкости парольных фраз к методам подбора // Открытое образование. 2011. №2. 127-130 с.

3. Заркумова Р.Н. Исследование количественных характеристик системы парольной защиты информации // Сборник научных трудов НГТУ. 2010. № 2(60). С.83-88.

4. Евтеев Д. Анализ проблем парольной защиты в российских компаниях // ЗАО «Позитив Текнолоджиз». 2009. 33 с.

5. Марков Г.А. К вопросу об определении стойкости парольных систем // Сборник трудов Третьей всероссийской НТК «Безопасные информационные технологии» / под. Ред. В.А.Матвеева. М: НИИ РЛ МГТУ им.Н.Э.Баумана. 2012. С.21-23.

6. Методы оценки несоответствия средств защиты информации / А.С. Марков, В.Л.Цирлов, А.В.Барабанов. М.: Радио и связь, 2012. 192 с.

7. Основы информационной безопасности: Учебное пособие / О.А.Акулов, Д.Н.Баданин, Е.И.Жук, Н.В.Медведев, П.М.Квасов, И.И.Троицкий. М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. 161 с.

8. Bonneau J. Guessing human-chosen secrets // Technical Report UCAM-CL-TR-819. 2012. 161 p.

9. Burnett M. Perfect Password: Selection, Protection, Authentication. Syngress Publishing, 2006.194 p.

10. Burr W.E. and etc. Electronic Authentication Guideline // NIST Special Publication 800-63-1. 2011. 110 p.

11. Information Assurance Implementation // Department of Defense Instruction 8500.2. 2003. 102 p.

12. PCI DSS Requirements and Security Assessment Procedures. Version 2.0. PCI Security Standards Council LLC. 2010. 75 p.