У статті наведено аналіз сучасних методів злому механізмів парольного захисту операційних систем. Пропонується підхід до вибору пароля відповідно до критерію «зручність - захищеність». Розглядаються подальші напрямки розвитку технологій по захисту пароля в ОС

Ключові слова: пароль, геш, операційна система, злом

В статье приведен анализ современных методов взлома механизмов парольной защиты операционных систем. Предлагается подход к выбору пароля в соответствии с критерием «удобство – защищенность». Рассматриваются дальнейшие направления развития технологий по защите пароля в ОС

Ключевые слова: пароль, хеш, операционная система, взлом

The report presents the analysis of modern methods of hacking the security mechanisms of passwords in operation systems. It's suggested a new approach of choosing the passwords according the principle «comfort – security». The new directions of further development of technologies for securing passwords in operation systems are considered

Key words: password, hash, operations system, hack

УДК 0004.056.5

АНАЛИЗ УСТОЙЧИВОСТИ К ВЗЛОМУ СОВРЕМЕННЫХ МЕХАНИЗМОВ ПАРОЛЬНОЙ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ

А.В. Снегуров
Кандидат технических наук, доцент*
Контактные тел.: (057) 702-10-67
E-mail: arksn@rambler.ru
В.Х. Чакрян*
Контактный тел.: 093-866-35-89
E-mail: Vadim-Romeo@mail.ru
*Кафедра телекоммуникационных систем
Харьковский национальный университет радиоэлектроники
пр. Ленина, 14, г. Харьков, 61166

Постановка проблемы

Одним из основных механизмов обеспечения информационной безопасности в организации (на предприятии) является использование парольной защиты операционных систем (ОС). Согласно международному стандарту ISO/IEC 27001-2005 (приложение А, пункт А.11.5) должна существовать процедура безопасного входа в операционную систему, все пользователи должны иметь уникальный идентификатор для их индивидуального опознавания, система управления паролями должна гарантировать качественные пароли.

Однако анализ ситуации в этой области информационной безопасности показывает ряд проблем с использованием данного механизма защиты. Так, по информации securitylab [1] в 2008 году 84% случаев взломов систем безопасности компаний и персональных страниц причиной была именно слабая парольная защита. Это обусловлено низкой компьютерной грамотностью пользователей, а также их нежеланием использовать сложные пароли. Тяга пользователей к простым и незамысловатым паролям объясняется просто. По данным компании Protocom Development Systems, 35% пользователей приходится запоминать от одного до пяти паролей, а 38% - от шести до десяти. При этом четверть пользователей регулярно забывает свои пароли, поэтому большинство людей пренебрегают советами специалистов, пользуясь самыми простыми паролями [2]. По данным компании Positive Technologies [3] наиболее распространенными паролями у российских пользователей являются пароли, состоящие только из цифр (53% от числа всех проанализированных паролей), используемые пароли в большинстве случаев не превышают 8-ми символов и лишь единицы пользователей используют пароли длиннее 12-ти символов. Администраторами информационных систем зачастую используются незамысловатые пароли низкой стойкости, которые могут содержаться в публично распространяемых словарях (15%), полностью совпадать с логином (10%) или вовсе отсутствовать (2%). Поэтому актуальным вопросом является внедрение такой системы управления парольной защиты, которая бы обеспечивала необходимый уровень защиты, а также была доступна для пользователя простыми пользователями.

Вопросам парольной защиты посвящено большое количество публикаций и исследований. Так в своей книге [4] Марк Барнетт рассматривает проблемы парольной защиты. В данном источнике описаны современные методы взлома паролей, рассматриваются проблемы человеческого фактора, а так же предлагаются методы повышения защищенности пароля. Исследование проблем парольной защиты в российских компаниях приведено в [3]. Однако проблемы внедрения парольной защиты в современных организациях (предприятиях), а также свободное распространение программ взлома паролей в сети Интернет, делает необходимым дальнейшее проведение исследований в этой сфере.

Цель исследования

В статье рассмотрены современные угрозы и уязвимости парольной защиты операционных систем. Приведены исследования скоростных характеристик различных методов взлома парольной защиты ОС. Предложен способ оценки качества парольной защиты с учетом как стойкости пароля к взлому, так и удобства его использования пользователями ПК. На основании анализируемой информации и предлагаемых решений рассматривается метод выбора пароля, соблюдая принцип «удобство - защищенность».

Основной материал исследования

Существуют следующие механизмы подбора пароля [4]:

Метод прямого перебора (англ. Brute-Force). Требует очень много времени для подбора, тем не менее, приносит 100% результат.

Подбор по словарю (англ. Dictionary attack). Данный метод позволяет быстро подобрать простые «словарные» пароли.

Радужная таблица (англ. rainbow table). Данный метод был предложен Филиппом Окслином в 2003 году и стал первой существенной ступенью в увеличении скорости подбора паролей. Данный метод это специальный вариант таблиц поиска, использующий механизм разумного компромисса между временем поиска по таблице и занимаемой памяти (time-memory tradeoff). Радужная таблица создается построением цепочек возможных паролей. Каждая цепочка начинается со случайного возможного пароля, затем подвергается действию хеш-функции и функции редукции. Функция редукции преобразует результат хеш-функции в некоторый возможный пароль. Затем к этому пароля снова применяется хеш-функция и цепочка повторяется вновь. В цепочку записываются лишь начальное и конечное значения. Все остальные значения порождаются в процессе обработки цепочки. Единственный недостаток радужных таблиц состоит во времени генерации самих таблиц.

В начале 2010 года компания Objectif Securite создала специальную радужную таблицу для подбора паролей на Windows XP. Данная радужная таблица, весом в 90 Гб, была помещена на новый SSD диск (англ. SSD, solid-state drive). За счет большой скорости диска (до 3 Гбит/с) и усовершенствованной таблицы любой пароль на Windows XP может быть взломан всего за 5,3 секунды, что в 174000 раз быстрее, чем взлом такого пароля методом прямого перебора на компьютере с процессором Pentium Dual Core T4500 (2,3 ГГц.) и 2 Гб ОЗУ [5].

Еще одним весомым шагом на пути ускорения анализаторов паролей стало использование графических процессоров. CUDA (англ. Compute Unified Device Architecture) – программно-аппаратная архитектура, позволяющая производить вычисления с использованием графических процессоров NVIDIA, поддерживающих технологию GPGPU (произвольных вычислений на видеокартах). Первоначальная версия CUDA SDK была представлена 15 февраля 2007 года. Уже в 2008 году Elcomsoft использовала данную разработку для ускорения своих продуктов по восстановлению паролей. Данная технология позволяет производить параллельные вычисления, что ускоряет работу в 20-50 раз, по сравнению с методом прямого перебора [6].

Существуют также другие методы взлома парольной защиты, основанные на социальной инженерии, использовании вредоносного программного обеспечения и другие.

Безопасная длина пароля

Опытным путем было вычислено, что грамотно-подобранный пароль (должен содержать: буквы малого и большого регистра, цифры, дополнительные символы) не менее чем из 9 знаков, что на данный момент, является достаточно стойким. Описание методов взлома 9-тизначного пароля:

1. С применением радужных таблиц.
2. Метод полного перебора (Brute Force).

В табл. 1 представлены результаты оценки времени (в годах), требуемого для взлома 9-тизначного пароля методом прямого перебора. Оценка происходила на компьютере с маркой процессора Pentium Dual Core T4500 (2.3 ГГц) и 2 Гб ОЗУ. В качестве программы восстановления пароля использовалась программа Cain-&Abel v.4.9.38.

Таблица №1

Время, требуемое на взлом 9-тизначного пароля методом прямого перебора [лет]

	полный алфавит	полный алфавит и цифры	полный алфавит, цифры и доп. символы	Всевозможные символы
NT	5,95	28,95	181,05	1345
MD5	7,05	34,25	214	1595

Исходя из вышеприведенных данных видно, что метод прямого перебора является неэффективным для взлома сложных паролей.

3. Метод с использование графических ускорителей.

С использованием графического ускорителя скорость перебора можно увеличить в 50 раз по сравнению с методом полного перебора. Даже с использование данных технологий время взлома будет составлять порядка 30 лет для паролей на Win Vista/Win7/Win Server 2008, и 40 лет для Unix систем.

Этот метод так же окажется затратным, так как стоимость качественного графического ускорителя CUDA составляет 4500 грн. А для приемлемого время подбора пароля их потребуется около 40 штук.

Методы повышения стойкости пароля в ОС

Самая главная проблема связана с человеческим фактором. Требования к паролю все больше ужесточаются, а соответственно растет его длина и сложность. Это приводит к трудности или нежеланию простых пользователей запоминать данный пароль. Зачастую это приводит к тому, что пользователь либо вовсе отказывается от использования пароля либо записывает его на листике и кладет на видном месте. Потому для

создания грамотного и удобного пароля необходимо учитывать 3 момента: длина пароля, сложность пароля и возможность его запоминания.

Марк Барнетт в своей книге «Идеальные пароли» предлагает следующие методы повышения стойкости паролей [4].

Методы увеличения длины пароля: слияние слов, использование скобок, числовые шаблоны, смешные слова, повторение, метод префиксов и суффиксов, метод предложений.

Методы увеличение сложности пароля: применение различных диалектов, разбиение на фрагменты, повторение, замена, бормотания и заикания, опечатки, неграмотность, применение сленга и иностранных языков.

Методы запоминания пароля: рифма, повторение, визуализация, ассоциации, юмор и ирония, преувеличение, преуменьшение, грубость и оскорбления, метод разделения на фрагменты.

На наш взгляд, одной из наиболее удобных механизмов запоминания пароля является метод ассоциаций. Используя данный метод можно взять любое слово, создать для него смешную ассоциацию и записать созданный ассоциативный образ одним словом. В качестве ассоциативного образа пользовать может использовать запомнившееся событие из своей жизни, которое неизвестно другим. Затем из записанного слова создается пароль, преобразуя его таким образом, чтобы в него входили буквы большого и малого регистров, цифры и знаки. Для полной уверенности можно создать подсказку, в которой должно быть записано слово или событие, от которого была создана ассоциация.

Еще одной из актуальных угроз являются радужные таблицы. Единственный метод борьбы с ними – использование хешей с «солью» для хранения системных паролей. В данном случае «соль» является модификатором пароля, проводя над ним псевдослучайные изменения. В результате изменяется и получаемый хеш. Такой метод хеширования используется в большинстве Unix подобных систем. В Windows подобных системах хеширование с «солью», пока что, не используется.

Снизить уровень угрозы, представляемый программами подбора пароля с использованием графических ускорителей можно заменив алгоритм хеширования на более стойкий. Весной 2012 NIST (National Institute of Standards and Technology) планирует провести конференцию, в ходе которой будет выбран алгоритм хеширования для нового стандарта SHA-3. Данный стандарт сможет стать новой точкой опоры для будущих поколений операционных систем.

Так же следует придерживаться общих рекомендаций по использованию пароля:

- пароль должен состоять из букв нижнего и верхнего регистров, цифр и знаков;
- пароль должен быть не менее 9 символов в длину;
- пароль к важному объекту должен быть уникален;
- нельзя вводить пароль в присутствии несанкционированных лиц, стоящих рядом с вами, которые имеют возможность подсмотреть его;
- не разглашать пароль и не оставлять информацию, которая может помочь в подборе пароля несанкционированным лицом;
- при нарушении безопасности пароля должна быть осуществлена его смена, необходимо менять пароль через определенный период времени (в зависимости от его сложности);
- не рекомендуется при выборе пароля использовать даты рождения, имена, свою фамилию, фамилию матери, номера паспорта, автомобиля и т.д., при смене пароля не рекомендуется использовать старые пароли.
- использовать антивирус и файервол для защиты компьютера от вторжений и вирусных атак, направленных на компрометацию данных;
- своевременно устанавливать заплатки и патчи для защиты операционных систем и программного обеспечения.

Выводы

Современные технологии и вычислительная мощность дают злоумышленнику большие возможности по преодолению парольной защиты операционных систем. В статье проведен анализ существующих механизмов взлома паролей с оценкой их временных параметров. К сожалению, разработанные специалистами по информационной безопасности требования к парольной защиты не выполняются простыми пользователями ввиду сложности их использования. В статье рассмотрены пути решения данной проблемы.

Литература

1. Слабая парольная защита - причина 84% компьютерных взломов [Электронный ресурс] / securitylab.ru. Режим доступа: – http://www.securitylab.ru/news/368799.php/ - 25.02.2009г. - Загл. с экрана.
2. Названы самые популярные пароли интернета [Электронный ресурс] / securitylab.ru. Режим доступа: – http://www.securitylab.ru/news/367212.php - 30 января, 2009 - Загл. с экрана.
3. Анализ проблем парольной защиты в российских компаниях [Электронный ресурс] / Positive Technologies Режим доступа – http://www.ptsecurity.ru/download/PT-Metrics-Passwords-2009.pdf - Загл. с экрана.
4. Mark Burnett, Perfect passwords / M.Burnett. - Canada: Syngress Publishing, Inc., 2006. - 177 с.
5. Positive Technologies: ошибки парольной защиты [Электронный ресурс] / itsec.ru. Режим доступа: – http://www.itsec.ru/newstext.php?news_id=59094 - 29.06.2009 - Загл. с экрана.
6. Новости компании Objectif Securite [Электронный ресурс] / objectif-securite.ch. Режим доступа – https://www.objectif-securite.ch/en/news.php - февраль 2010 - Загл. с экрана.
7. Технология CUDA используется для взлома паролей [Электронный ресурс] / elcomsoft.ru. Режим доступа – http://www.elcomsoft.ru/lhc.html - Загл. с экран.