Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.421

Гончарик
Мария Сергеевна

Методы и средства генерирования и проверки паролей пользователей

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

по специальности 1-40 80 05 Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Научный руководитель
Ярмолик В. Н.
д.т.к., профессор

Минск 2015

ВВЕДЕНИЕ

Сегодня система паролей широко применяется в среде Интернет технологий. Большинство современных порталов и сайтов используют личную информацию пользователей и обязуются защищать эти данные от несанкционированного доступа. Обычно, управление доступом к таким данным осуществляется через профили пользователей. Для аутентификации пользователя используется система паролей, что выводит на первый план проблему выбора надежного пароля.

В большинстве случаев вопрос выбора пароля ложится на пользователя системы. Именно пользователь выбирает себе пароль и отвечает за его надежность и сохранность. Если сайт при создании профиля пользователя сам генерирует для него пароль, то обычно этот же сайт предоставляет возможность пользователю сменить пароль. Многие пользователи часто игнорируют проблемы безопасности своего профиля, создавая легко угадываемые пароли, храня их в общедоступных местах, таким образом, подвергая опасности свои данные.

Система паролей среднестатистического сайта обычно осуществляет контроль пароля лишь по его длине и набору поддерживаемых символов. Анализ пароля на надежность обычно не проводится. Однако, с точки зрения как владельца сайта, так и его пользователей было бы полезно предупреждать пользователя в случае, если его пароль является ненадежным. Владелец сайта снимает с себя ответственность за сохранность данных пользователя при ненадежном пароле. Внимание пользователя будет обращено на слабость пароля, даст ему возможность выбрать другой, более надежный, пароль.

Большой вклад в анализ возможных проблем выбора надежного пароля сделал Вильям Столлингс (William Stallings). Он изучал и систематизировал основные методы и средства, используемые в системах защиты компьютерных сетей, в том числе и в системах генерации и проверки паролей, а также предложил концепции для решения этих проблем.

В рамках данной диссертации были проанализированы методы и средства генерации и проверки паролей пользователя. Некоторые из них были оптимизированы и реализованы в программном средстве для генерации и проверки надежности пароля пользователя.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью работы является анализ методов и разработка программного средства генерирования и проверки паролей пользователей.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ существующих угроз и методов защиты паролей пользователей;
2. Разработать методы генерирования и проверки паролей, пригодные для программной реализации;
3. Разработать программное средство генерирования и проверки паролей.

Объектом исследования является система генерирования паролей.

Предметом исследования являются средства и методы генерирования и проверки паролей.

Систему паролей можно отнести к первой линии защиты информации пользователей от нарушителей. Многие пользователи по собственному выбору создают слишком короткие, либо легко угадываемые пароли, что делает систему уязвимой. Нарушители могут с легкостью подобрать пароль, используя простой перебор слов или наиболее часто используемых паролей. Таким образом, существует потребность в средствах генерации пользовательских паролей, которые было бы сложно угадать, а также в средствах проверки паролей, выбранных пользователями. Множество систем из сферы интернет услуг, программных приложений используют для аутентификации пользователя систему паролей. Её широкое применение делает разработку средств генерации и проверки паролей актуальной.

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Работа выполнялась в соответствии научно-техническими заданиями и планами работ кафедры «Программное обеспечение информационных технологий», и хозяйственными договорами с предприятиями Республики Беларусь:

1. «Разработать модели, методы, алгоритмы для оценки качества и диагностируемости аппаратно-программных средств сложных систем и

внедрения в современные обучающие комплексы» (ГБ № 11-2004, № ГР 20111065, научный руководитель НИР – В. В. Бахтизин).

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя В. Н. Ярмолика заключается в формулировке целей и задач исследования.

Апробация результатов диссертации

Основные положения диссертационной работы обсуждались в рамках Международной заочной научно-практической конференции «Наука, образование, общество: тенденции и перспективы» (г. Москва, 28 ноября 2014 г.), XXIX Международной заочной научно-практической конференции «Научная дискуссия: вопросы технических наук» (г. Москва, 11 декабря 2014 г.).

Опубликованность результатов диссертации

По теме диссертации опубликовано 2 работы в сборниках трудов и материалов международных конференций.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованных источников, списка публикаций автора и приложений. В первой главе представлен анализ предметной области, выявлены основные существующие проблемы в рамках тематики исследования, показаны направления их решения. Вторая глава посвящена разработке алгоритмов генерирования и проверки пароля пользователя, оптимизации алгоритма проверки пароля. В третьей главе предложена реализация методов генерирования и проверки паролей в виде программного средства. В четвертой главе описанного программного средства процесс тестирования и приведены результаты экспериментальных исследований полученных алгоритмов.

Общий объем работы составляет 77 страниц, из которых основного текста – 38 страниц, 23 рисунка на 8 страницах, 7 таблиц на 2 страницах, библиографический список (список использованных источников и списка публикаций автора) 33 наименований на 3 страницах и 6 приложений на 26 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** определена область и указаны основные направления исследования, показана актуальность темы диссертационной работы, дана краткая характеристика исследуемых вопросов, обозначена практическая ценность работы.

Глава 1 магистерской диссертации посвящена анализу проблемы использования паролей пользователей. В ней отражены общие сведения о системе пароля, сделан обзор существующих угроз, рассмотрены различные стратегии выбора пароля методы генерирования пароля.

Практически все современные многопользовательские системы требуют, чтобы пользователь предоставлял имя или идентификатор (ID) и пароль. Пароль служит для аутентификации пользователя при входе в систему. Аутентификация – действие по проверке заявленной подлинности объекта или субъекта (логической сущности). Пароль (фр. Parole – слово) – это условное слово или набор знаков, предназначенный для подтверждения личности или полномочий. Пароли часто используются для защиты информации от несанкционированного доступа. В большинстве вычислительных систем комбинация «имя пользователя– пароль» используется для удостоверения пользователя.

Специалисты по компьютерной безопасности установили, что сотни тысяч людей используют одинаковые пароли доступа к своей конфиденциальной информации в сети. При этом большинство пользователей регулярно забывает свои пароли, поэтому пренебрегают советами специалистов, пользуясь самыми простыми паролями. Простые, легко угадываемые пароли считаются слабыми и уязвимыми. Пароли, которые очень трудно или невозможно угадать, считаются более стойкими. Однако такие пароли сложны для запоминания. В связи с тем, что многие пользователи используют простые, легко угадываемые пароли, существует ряд угроз для системы паролей.

Одной из двух самых распространенных угроз безопасности являются нарушители (второй угрозой являются вирусы), обычно называемые хакерами или взломщиками. Целью нарушителя является получение доступа к системе или расширение прав, предоставленных ему системой на законном основании. Для этого нарушителю, как правило, требуется раздобыть информацию, которая должна быть защищенной. В большинстве случаев эта информация представлена в форме пароля пользователя. Зная пароль некоторого другого пользователя, нарушитель может войти в систему под его именем и получить все привилегии, которыми обладает этот пользователь.

Нарушители владеют различные способы подбора пароля. Эти способы более подробно описаны в магистерской диссертации. В большинстве случаев защитой от подбора пароля является использование сложных паролей. Система должна уметь проверять пароль на надежность.

Вильям Столлингс предлагает 4 стратегии выбора паролей:

1. Обучение пользователя;
2. Компьютерная генерация паролей;
3. Реактивная проверка паролей;
4. Упреждающая проверка паролей.

Из этих четырех стратегий Вильям Столлингс отдает предпочтение упреждающей проверке паролей. В этой схеме, пользователь может выбрать свой собственный пароль. Тем не менее, во время выбора, система проверяет, является ли пароль допустимым, и, если нет, отклоняет его. Данная стратегия позволяет пользователю как придумывать пароль самостоятельно, так и пользоваться генератором паролей, главное, чтобы предлагаемый пароль прошел затем проверку.

Автоматический генератор паролей представляет собой программу, которая вырабатывает случайные пароли. В своей простейшей форме она может просто генерировать случайное цифровое значение и кодировать его в виде последовательности печатных символов. Если программа использует хороший генератор случайных чисел, она может давать пароли, которые будут и относительно короткими и трудными для угадывания. Существенным недостатком является то, что такие пароли чрезвычайно трудно запомнить.

Чтобы сделать пароль более запоминаемым, большинство генераторов паролей вырабатывают «произносимые» пароли. Часто подобные генераторы создают пароли, просто чередуя гласные и согласные. Более сложные генераторы способны производить легко запоминаемые пароли. Например, генератор, описанный в стандарте FIPS PUB 181. Алгоритм генерирует слова, формируя произносимые слоги и составляя из них слова. Генератор случайных чисел создает поток случайных символов, используемых для создания слогов и слов.

Глава 2 магистерской диссертации посвящена разработке методов генерирования и проверки паролей. В ней приводятся алгоритмы генерирования и проверки паролей, затем описан подход к оптимизации алгоритма проверки пароля и реализован вывод оптимизированной формулы проверки пароля на надежность.

Простейший алгоритм генерации пароля выглядит следующим образом:

1. Задать длину, область выборки символов генерируемого пароля.
2. Инициализировать ГПСЧ (генератор псевдослучайных чисел).
3. Для каждого символа получить значение из ГПСЧ.

4. Для каждого числа получить символ пароля из области выборки согласно правилам соотнесения символов.

Из различных подходов к реализации стратегии упреждающей проверки пароля был выбран один. Этот подход заключается в том, чтобы просто составить большой словарь возможных «плохих» паролей. Когда пользователь выбирает пароль, система проверяет, чтобы убедиться, что этот пароль не находится в списке «плохих». При этом подходе существуют две проблемы:

1. Объем словаря: чтобы быть эффективным, словарь должен быть очень большим, порядка десятков мегабайтов.

2. Время: время, необходимое для поиска в большом словаре, само по себе может быть долгим.

В работе для реализации данного подхода был выбран метод, использующий модель Маркова. Данный метод позволяет сократить время, необходимое для поиска в большом словаре. Однако его недостатком является то, что много времени требуется для построения модели. В ходе исследований был найден способ сократить объем словаря «плохих» паролей и ускорить построение модели Маркова. В рамках магистерской диссертации была выведена формула (1) для проверки паролей с применением модели Маркова:

$$P = \sqrt{\frac{a_1(1-\frac{\sum t_i}{k})^2+a_2(\frac{m}{n})^2+a_3(\frac{l}{L})^2}{a_1+a_2+a_3}}, \quad (1)$$

где

a_j – весовые коэффициенты,

t_i – количество найденных элементов матрицы T модели Маркова, соответствующих триграммам анализируемого пароля;

k – количество триграмм в анализируемом пароле;

m – количество типов символов в анализируемом пароле;

n – количество типов символов, допустимых для паролей данной системы;

l – длина пароля;

L – допустимая максимальная длина пароля.

Глава 3 магистерской диссертации посвящена реализации рассмотренных методов генерирования и проверки паролей в виде программного средства. В ней описаны процессы проектирования и разработки программы, в основе которой лежит формула (1). Также в главе 3 приведены рисунки, отражающие пользовательский интерфейс разработанного программного средства.

В **главе 4** приведены результаты тестирования разработанного программного средства. В ней описаны условия тестирования, также

результаты тестирования построения модели Маркова до и после оптимизации, а также процесс поиска порога вероятности и весовых коэффициентов.

Оптимизация алгоритма позволила сократить временные затраты более чем в 3 раза, а затраты на память – почти в 2 раза, при уменьшении объема словаря слабых паролей почти в 1.94 раза.

Для подбора весовых коэффициентов и определения порога вероятности для классификации потенциальных паролей требовалось провести тестирование системы на большом числе паролей согласно следующему алгоритму:

1. установить значения весовых коэффициентов;
2. посчитать вероятности для заведомо надежных паролей;
3. посчитать вероятности для заведомо ненадежных паролей;
4. найти минимальное значение вероятности для заведомо надежных паролей;
5. найти максимальное значение вероятности для заведомо ненадежных паролей;
6. если минимальное значение вероятности для заведомо надежных паролей больше или равно максимальному значению вероятности для заведомо ненадежных паролей, то выбранные весовые коэффициенты являются оптимальными. Переходим к шагу 9.
7. если минимальное значение вероятности для заведомо надежных паролей меньше максимального значения вероятности для заведомо ненадежных паролей, то переходим к шагу 8.
8. Смотрим, сколько заведомо надежных паролей попадают в интервал между найденными экстремумами. Если их количеством можно пренебречь, переходим к шагу 9, иначе меняем какой-либо весовой коэффициент и возвращаемся к шагу 2.
9. Порог вероятности для классификации потенциальных паролей будет равен максимальному значению вероятности для заведомо ненадежных паролей.

Для тестирования программы, подбора весовых коэффициентов и определения порога вероятности классификации был создан список из 200 паролей.

Тестирование разработанного программного средства, а также способа оптимизации построения модели Маркова показало следующие результаты:

1. Самый большой расход временных ресурсов отводится на построение модели Маркова, однако при внедрении формулы (1) данные потери существенно сокращаются.
2. Формула (1) также позволяет экономить ресурсы памяти.

3. Весовые коэффициенты делают формулу (1) более гибкой и позволяют настраивать систему под различные словари паролей для уменьшения ошибок отказа надежным паролям.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Среди стратегий выбора пароля наиболее перспективной является упреждающая проверка пароля.
2. В системах с упреждающей проверкой паролей пользователей можно использовать простейший генератор пароля, так как пользователь в любом случае имеет возможность задать собственный пароль.
3. Проверка пароля на основе словаря языка может потребовать большие ресурсы времени и памяти (места хранения).
4. В рамках диссертации было выполнено проектирование и реализация программного средства Passwords_Management для генерации и проверки пароля пользователя.
5. Для оптимизации и экономии ресурсов была разработана формула (2.10), применение которой существенно сократило расходы времени и памяти.
6. Весовые коэффициенты добавили гибкость и позволили проводить настройку программного средства под различные словари паролей для уменьшения ошибок отказа надежным паролям.
7. Разработанная формула показала свою эффективность.

Рекомендации по практическому использованию результатов

Разработанное программное средство может применяться в качестве независимого модуля и быть использовано на стороне клиента. В качестве рекомендации к применению можно посоветовать проводить инициализацию модели Маркова лишь один раз при загрузке клиента или при обновлении списка ненадежных паролей, а в процессе использования модель можно обновлять данными с клиентской формы, что не займет большое количество времени.

Также следует обратить внимание на словарь языка для построения модели Маркова. В данной работе использовался словарь объемом в 1422 слова. В реальных условиях данный словарь будет слишком маленьким. Для использования разработанного программного средства следует создать большой словарь паролей исходя из параметров портала или сайта.

В дальнейшем разработанное программное средство и формула могут быть усовершенствованы.

СПИСОК ОПУБЛИКРВАННЫХРАБОТ

1-А. Гончарик, М. С. Упреждающая проверка паролей пользователей / М. С. Гончарик // Наука, образование, общество: тенденции и перспективы: Сборник научных трудов Международной заочной научно-практической конференции 28 ноября 2014 г.: в 5 частях. Часть III. М.: «АР-Консалт», 2014 г. – с. 21 – 22.

2-А. Гончарик, М. С. Применение на практике стратегии упреждающей проверки пароля / М. С. Гончарик // Научная дискуссия: вопросы технических наук. № 11-12 (22): сборник статей по материалам XXVIII – XXIX международной заочной научно-практической конференции. М.: «Международный центр науки и образования», 2014. – с. 170 – 174.