Авторы:

Кузьмин Никита Игоревич

студент

Панкова Наталья Николаевна

студентка

Научный руководитель:

Додонов Михаил Витальевич

канд. пед. наук, доцент, преподаватель

ФГАОУ ВО «Самарский государственный аэрокосмический университет им. академика С.П. Королёва (НИУ)»

г. Самара, Самарская область

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП С ПОМОЩЬЮ ПРЯМОГО ПЕРЕБОРА ПАРОЛЯ – BRUTFORCE

Аннотация*: в представленной работе исследователями рассматриваются способы и методы перебора паролей посредством брутфорса. Отмечено, что одним из необходимых условий получения доступа к данным системы является идентификация и аутентификация любого пользователя данной системы или процесса.*

Ключевые слова*: брутфорс, хэширование, аутентификация.*

Основные понятия

Определение 1. Брутфорс (BrutForce, метод «грубой силы») – метод поиска решений задач математики путем перебора всех возможных вариаций ответов.

Определение 2. Хэширование (Хэш функция, hash) – преобразование последовательности данных, состоящей из любого количества символов, в битовую строку определенной длины. Выполняется определенным алгоритмом.

Определение 3. Аутентификация – процесс проверки подлинности посредством сравнения предоставленного пароля и пароля сохраненного в БД пользователя или операционной системы.

Введение

Одним из необходимых условий получения доступа к данным системы является идентификация и аутентификация любого пользователя данной системы или процесса. Использование паролей – это один из самых распространенных способов аутентификации. Но, к сожалению, подбор паролей в наше время также достаточно легко осуществить.

Самым распространенным способом взлома паролей является брутфорс. Он заключается в том, что злоумышленник получает доступ к программе, системе или профилю с помощью перебора паролей на основе критериев, которые задаются владельцем. Этот метод может занимать достаточно много времени, но очень действенен, поэтому им пользуются и по сей день. Особенность данного способа в том, что пароль рано или поздно всё равно будет взломан, но иногда на это могут уйти столетия. Поэтому он будет неэффективен для длинных паролей, в которых используются и цифры, и строчные буквы, и заглавные, и разрешенные специальные символы. Но для того, чтобы защитить пароль от взлома, недостаточно просто сделать его длинным и сложным, нужно также продумать гармоничную и при этом действенную концепцию шифрования, иначе утечки информации Вам не избежать.

В последнее время часто начали появляться новости об утечках паролей с различных крупных ресурсов. Одной из наиболее крупных была утечка 6,5 миллионов хэшей паролей крупной социальной сети Linkedln. До сих пор этот случай исследуют сотрудники ФБР. Также были опубликованы хэши таких популярных сервисов, как Last.fm, YahooVoice, eHarmony, NVIDIA. Компания Rapid 7 тщательно изучила и проанализировала все 165 тысяч хэшей, которые были украдены с Linkedln, и опубликовала следующую инфографику самых часто используемых. На первом месте – пароль link, на втором – 1234, на третьем – work, далее идут god, job, 12345, connect, jesus, sex, ilove, the, angel, 123456 и т. д.

Ниже перечислены возможные способы перебора паролей.

1. Глобальный перебор.

Данный способ заключается в том, что взломщик перебирает все варианты паролей, которые возможны. Но если пароль состоит более чем из шести символов, то данный метод будет уже неэффективным.

2. Тотальный перебор, который оптимизирован по статистике встречаемости символов.

Все символы можно встретить в паролях пользователей с разной вероятностью. Допустим, вероятность того, что в пароле используется буква «а» больше, чем вероятность, что в пароле есть буква «т». Были проведены исследования, в результате которых доказали, что статистика встречаемости символов и знаков в естественном языке практически такая же, как статистика встречаемости в алфавите паролей. Время на перебор затрачивается намного меньше, когда взломщик сначала перебирает пароли, которые состоят из часто встречающихся символов.

Также при подборе пароля можно использовать статистику встречаемости биграмм и триграмм. Биграмма – это последовательность из двух последовательных элементов, триграмма – из трех. Чтобы взламывать пароли подобным методом, было написано большое количество программ, которые в основном были ориентированы на взлом операционных систем.

Существуют две основные технологии подбора паролей:

– подача паролей, которые последовательно генерируются, на вход самой системы, а после их явное опробование;

– вычисление хэшей пароля и ее сравнение с известным образом пароля.

3. Тотальный перебор, приспособленный для работы с базами. Чаще всего пользователи используют какие-то осмысленные слова своего родного или зарубежного языка. Так как человеку просто запомнить близкое для себя слово, то он использует имена, названия улиц, дату рождения, вместо случайных последовательностей. Из-за этого уменьшается число вариаций пароля.

В таком случае взломщик сначала толковый словарь Ожегова. В интернете содержится множество сформированных словарей для перебора паролей для различных пользователей разных возрастов и проживающий в различных странах.

4. Подбор пароля с использованием знаний о пользователе. Пользователи любят использовать запоминающиеся пароли. Многие, чтобы не забыть пароль, используют имена, животных, номера машин, телефона и так далее.

Помимо перебора паролей существуют и другие способы его взлома. Перечислим некоторые из них.

1. Взлом при помощи радужной таблицы.

Радужная таблица – это перечень хэш-функций паролей. Эта таблица очень большая, и для ее использования нужны компьютеры с высокой вычислительной мощностью.

2. Фишинг.

Фишинг является самым простым способом взлома, он заключается в том, чтобы просто узнать пароль у самого пользователя. Пользователю приходит сообщение с просьбой ввести пароль или какие-то другие личные данные, чтобы избежать, например, блокировки денежных средств или данных, и он добровольно это делает.

3. Социальная инженерия.

Этот способ аналогичен фишингу, но заключается в том, что пароль узнается у пользователя вживую, а не через онлайн-сервисы.

4. Вредоносные программы.

С их помощью перехватывается информация, которую вы вводите в компьютер или создают скриншоты, которые позже направляются к злоумышленникам. Также с помощью специальных программ можно получить доступ к файлу с сохраненными паролями из истории браузера.

Список литературы

1. Смирнов С.М. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007 – 349 с.