УДК 004.056.53

студентка А.А. Свиридова
ГВУЗ «Национальный горный университет»

РЕКОМЕНДАЦИИ ПО СОЗДАНИЮ ПАРОЛЕЙ

В данной работе рассмотрена проблема создания паролей устойчивых к парольным атакам. Описаны основные требования к современным паролям, а так же приведены некоторые рекомендации и методики по их созданию.

Одной из наиболее актуальных проблем современности, в сфере защиты персональной информации, является создание пароля устойчивого к парольным атакам, так как пароль представляет собой ключ доступа к информации, которую пользователь хранит на своем компьютере и в online-аккаунтах.

Пароль – это секретное слово или набор символов, предназначенный для подтверждения личности или полномочий. Если преступники или другие пользователи овладеют этой информацией, они смогут использовать имя владельца пароля для открытия новых карточных счетов, использовать для мошенничества или от его имени выполнять операции в online. Во многих случаях пользователь не получит предупреждения о таких атаках, а вовремя не обнаружив их, понесет моральный или материальный ущерб.

Основные требования, выставляемые к паролям:

– устойчивость к парольным атакам;

– легкая запоминаемость.

Создавая устойчивый к атакам пароль, следуйте приведённым ниже рекомендациям [1]:

Не делайте:

1. Не используйте только слова или числа.
2. Не используйте известных слов.
3. Не используйте слов из других языков.
4. Не используйте сленг хакеров.
5. Не используйте личные сведения.
6. Не переворачивайте известных слов.
7. Не записывайте свой пароль.
8. Не используйте один пароль на всех компьютерах (сервисах).

Делайте:

1. Придумывайте пароль длиной не меньше восьми символов.
2. Смешивайте буквы верхнего и нижнего регистра.
3. Смешивайте буквы и цифры.
4. Включайте не алфавитно-цифровые символы.
5. Придумайте пароль, который вы можете запомнить.
6. Изменяйте пароли не реже, чем один раз в 6 месяцев.

Есть множество методик создания безопасных паролей. Вот один из предложенных алгоритмов [2]:

Шаг 1. Случайным образом берем любое прилагательное. Например, "веселый".

Шаг 2. Случайным образом берем любое существительное. Главное, чтобы это существительное «плохо сочеталось» с прилагательным, которое мы взяли в шаге 1. Например, "слон".

Шаг 3. Берем цифру, которую легко запомнить (любимую цифру, дату рождения, последние 4 номера мобильного телефона, и т.д.). Например, "2511".

Шаг 4. Берем любой знак препинания. Например, "?".

Шаг 5. Запишем строки, которые мы получили в 1 — 4 шагах в одну большую строку: "веселыйслон2511?".

Шаг 6. Поменяем в этой строке строчную букву на прописную: "ВеСелыйслон2511?".

Шаг 7. Наберем на клавиатуре эту строку в английской раскладке: "DtCtksqckjy2511&".

Преимущества этого алгоритма очевидны, ведь на выходе мы получаем пароль, который:

1. Непросто взломать методом перебора (пароль включает в себя строчные буквы, прописные буквы, цифры и знаки препинания).

2. Легко запомнить (большинство людей с легкостью смогут запомнить пароль, включающий в себя «парадоксальное» словосочетание, цифру и знак препинания).

Ещё одним важным моментом представляется хранение самого пароля. Его защите нужно уделять не меньше внимания, чем защите самой информации.

Рекомендации по безопасности хранения пароля [3]:

1. Не показывайте пароль никому.
2. Защищайте записанные пароли.
3. Никогда не отправляйте пароль по e-mail или в ответ на e-mail запрос.
4. Регулярно меняйте пароль.
5. Не вводите паролей на компьютерах, которые вы не контролируете.

Применение парольной защиты информации является одним из наиболее популярных методов. Но проведя анализ требований к современным паролям, становится понятно, что создание эффективного устойчивого пароля составляет проблему. Поэтому актуальным вопросом современности слала разработка «адекватной» альтернативы этому методу.

Перечень литературы:

1. http://rhd.ru/docs/manuals/enterprise/RHEL-4-Manual/security-guide/s1-wstation-pass.html – Рекомендации по созданию пароля.
2. http://habrahabr.ru/blogs/infosecurity/65893/ – Методика создания пароля.
3. http://sb-money.ru/article.php?a=68 – Безопасность хранения пароля.