

ЛАБОРАТОРНАЯ РАБОТА № 3

Защита информации с помощью пароля

1 ЦЕЛЬ РАБОТЫ

Целью работы является исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль.

2 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

2.1 Атаки на пароль

На сегодняшний день пароль является наиболее приемлемым и потому наиболее часто используемым средством установления подлинности, основанным на знаниях субъектов доступа.

В любой критической системе ошибки человека-оператора являются чуть ли не самыми дорогостоящими и распространенными. В случае криптосистем, непрофессиональные действия пользователя сводят на нет самый стойкий криптоалгоритм и самую корректную его реализацию и применение.

В первую очередь это связано с выбором паролей. Очевидно, что короткие или осмысленные пароли легко запоминаются человеком, но они гораздо проще для вскрытия. Использование длинных и бессмысленных паролей безусловно лучше с точки зрения криптостойкости, но человек обычно не может их запомнить и записывает на бумажке, которая потом либо теряется, либо попадает в руки злоумышленнику. Именно из того, что неискушенные пользователи обычно выбирают либо короткие, либо осмысленные пароли, существуют два метода их вскрытия: атака полным перебором и атака по словарю.

Защищенность пароля при его подборе зависит, в общем случае, от скорости проверки паролей и от размера полного множества возможных паролей, которое, в свою очередь, зависит от длины пароля и размера применяемого алфавита символов. Кроме того, на защищенность сильно влияет реализация парольной защиты.

В связи с резким ростом вычислительных мощностей атаки полным перебором имеют гораздо больше шансов на успех, чем раньше. Кроме того, активно используются распределенные вычисления, т.е. равномерное распределение задачи на большое количество машин, работающих параллельно. Это позволяет многократно сократить время взлома.

Однако вернемся на несколько лет назад, когда вычислительной мощности для полного перебора всех паролей не хватало. Тем не менее, хакерами был придуман остроумный метод, основанный на том, что в качестве пароля человеком выбирается существующее слово или какая-либо информация о себе или своих знакомых (имя, дата рождения и т.п.). Ну, а поскольку в любом языке не более 100000 слов, то их перебор займет весьма небольшое время, и от 40 до 80% существующих паролей может быть угадано с помощью простой схемы, называемой “атакой по словарю”. Кстати, до 80% этих паролей может быть угадано с использованием словаря размером всего 1000 слов!

Пусть сегодня пользователи уже понимают, что выбирать такие пароли нельзя, но, видимо, никогда эксперты по компьютерной безопасности не дождутся использования таких простых и радующих душу паролей, как 34jXs5U@bTa!6;). Поэтому даже искушенный пользователь хитрит и выбирает такие пароли, как hope1, user1997, pAsSwOrD, toor, roottoor, paqo1, gfhjkm, asxz. Видно, что все они, как правило, базируются на осмысленном слове и некотором простом правиле его преобразования: прибавить цифру, прибавить год, перевести через букву в другой регистр, записать слово наоборот, прибавить записанное наоборот слово, записать русское слово латинскими буквами, набрать русское слово на клавиатуре с латинской раскладкой, составить пароль из рядом расположенных на клавиатуре клавиш и т.п.

Поэтому не надо удивляться, если такой “хитрый” пароль будет вскрыт хакерами — они не глупее самих пользователей, и уже вставили в свои программы те правила, по которым может идти преобразование слов. В самых “продвинутых” программах (John The Ripper, Password Cracking library) эти правила могут быть программируемыми и задаваться с помощью специального языка самим хакером.

Приведем пример эффективности такой стратегии перебора. Во многих книгах по безопасности предлагается выбирать в качестве надежного пароля два осмысленных слова, разделенных некоторым знаком (например, good!password). Подсчитаем, за сколько времени в среднем будут сломаны такие пароли, если такое правило включено в набор программы-взломщика (пусть словарь 10000 слов, разделительными знаками могут быть 10 цифр и 32 знака препинания и специальных символа, машина класса Pentium со скоростью 15000 паролей/сек): $10000 \cdot (32 + 10) \cdot 10000 / 15000 \cdot 2 = 140000$ секунд или менее 1.5 дня!

Чем больше длина пароля, тем большую безопасность будет обеспечивать система, так как потребуются большие усилия для его отгадывания. Это обстоятельство можно представить в терминах ожидаемого времени раскрытия пароля или ожидаемого безопасного времени. Ожидаемое безопасное время (T_6) — половина произведения числа возможных паролей и времени, требуемого для того, чтобы попробовать каждый пароль из последовательности запросов. Представим это в виде формулы:

$$T_6 = \frac{A^S \cdot t}{2}, \quad (1)$$

где t — время, требуемое на попытку введения пароля, равно E/R ; E — число символов в передаваемом сообщении при попытке получить доступ (включая пароль и служебные символы); R — скорость передачи (символы/мин) в линии связи; S — длина пароля; A — число символов в алфавите, из которых составляется пароль. Если после каждой неудачной попытки подбора автоматически предусматривается десятисекундная задержка, то безопасное время резко увеличивается.

Поэтому при использовании аутентификации на основе паролей защищенной системой должны соблюдаться следующие правила:

- а) не позволяют пароли меньше 6–8 символов;
- б) пароли должны проверяться соответствующими контроллерами;
- в) символы пароля при их вводе не должны появляться в явном виде;
- г) после ввода правильного пароля выдается информация о последнем входе в систему;
- д) ограничивается количество попыток ввода пароля;
- е) вводится задержка времени при неправильном пароле;
- ж) при передаче по каналам связи пароли должны шифроваться;
- з) пароли должны храниться в памяти только в зашифрованном виде в файлах, недоступных пользователям;
- и) пользователь должен иметь возможность самому менять пароль;
- к) администратор не должен знать пароли пользователей, хотя может их менять;
- л) пароли должны периодически меняться;
- м) устанавливаются сроки действия паролей, по истечении которых надо связаться с администратором.

2.2 Проблема выбора пароля

Выбор длины пароля в значительной степени определяется развитием технических средств, их элементной базы и ее быстродействием. В настоящее время широко применяются многосимвольные пароли, где $S > 10$. В связи с этим возникают вопросы: как и где его хранить и как связать его с аутентификацией личности пользователя? На эти вопросы отвечает комбинированная система паролей, в которой код пароля состоит из двух частей. Первая часть состоит из 3–4-х десятичных знаков, если код цифровой, и более 3–4-х, если код буквенный, которые легко запомнить человеку. Вторая часть содержит количество знаков, определяемое требованиями к защите и возможностями технической реализации системы, она помещается на физическом носителе и определяет ключ-пароль, расчет длины кода которого ведется по указанной выше методике. В этом случае часть пароля будет недоступна для нарушителя.

Однако при расчете длины кода пароля не следует забывать о том, что при увеличении длины пароля нельзя увеличивать периодичность его смены. Коды паролей необходимо менять обязательно, так как за большой период времени увеличивается вероятность их перехвата путем прямого хищения носителя, снятия его копии, принуждения человека. Выбор периодичности необходимо определять из конкретных условий работы системы, но не реже одного раза в год. Причем желательно, чтобы дата замены и периодичность должны носить случайный характер.

Для проверки уязвимости паролей используются специальные контроллеры паролей. Например, известный контроллер Кляйна, осуществляет попытки взлома пароля путем проверки использования в качестве пароля входного имени пользователя, его инициалов и их комбинаций, проверки использования в качестве пароля слов из различных словарей, начиная от наиболее употребительных в качестве пароля, проверки различных перестановок

слов, а также проверки слов на языке пользователя–иностранца. Проверка паролей в вычислительных сетях с помощью контроллера Кляйна показала довольно высокие результаты — большинство пользователей используют простые пароли. Показателен пример, когда контроллер Кляйна позволил определить 100 паролей из 5 символов, 350 паролей из 6 символов, 250 паролей из 7 символов и 230 паролей из 8 символов.

Приведенный анализ позволяет сформулировать следующие правила снижения уязвимости паролей и направленные на противодействие известным атакам на них:

- расширяйте применяемый в пароле алфавит — используйте прописные и строчные буквы латинского и русского алфавитов, цифры и знаки;
- не используйте в пароле осмысленные слова;
- не используйте повторяющиеся группы символов;
- не применяйте пароли длиной менее 6–8 символов, так как запомнить их не представляет большого труда, а пароль именно нужно запоминать, а не записывать. По той же причине не имеет смысла требовать длину неосмысленного пароля более 15 символов, так как запомнить его нормальному человеку практически невозможно;
- не используйте один и тот же пароль в различных системах, так как при компрометации одного пароля пострадают все системы;
- проверяйте пароли перед их использованием контроллерами паролей.

Для составления пароля можно дать рекомендации, которыми пользоваться надо очень осторожно:

- выберите несколько строк из песни или поэмы (только не те, которые Вы повторяете первому встречному) и используйте первую (или вторую) букву каждого слова — при этом пароль должен иметь большую длину (более 15 символов), иначе нужно менять регистры букв, применять латинские буквы вместо русских или наоборот, можно вставлять цифры и знаки;
- замените в слове из семи–восьми букв одну согласную и одну или две гласных на знаки или цифры. Это даст вам слово-абракадабру, которое обычно произносимо и поэтому легко запоминается. Подведем итог:

Что такое плохой пароль:

- Собственное имя;
- Слово, которое есть в словаре;
- Идентификатор, присвоенный Вам какой-нибудь системой, или любые его вариации;
- Дата рождения;
- Повторенный символ (например: ААА);
- Пароль меньше 6 символов;
- Пароль, установленный Вам чужим человеком;
- Пароль, состоящий из символов соседствующих на клавиатуре (например: QWERTY или ЙЦУКЕ);

- Пароль состоящий из паспортных данных: персональный номер, номер водительских прав и т.д.

Что такое хороший пароль:

- Бессмысленная фраза;
- Случайный набор символов вперемешку с буквами.

2.3 Порядок работы с программами вскрытия паролей.

В данной лабораторной работе используется программный продукт для вскрытия закрытых паролем архивов: Advanced ZIP Password Recovery

2.4 Работа с программами взлома на примере AZPR

Программа AZPR используется для восстановления забытых паролей ZIP-архивов. На сегодняшний день существует два способа вскрытия паролей: перебор (brute force) и атака по словарю (dictionary-based attack).

Панель управления:

- кнопки Открыть и Сохранить позволяют работать с проектом, в котором указан вскрываемый файл, набор символов, последний протестированный пароль. Это позволяет приостанавливать и возобновлять вскрытие.
- кнопки Старт и Стоп позволяют соответственно начинать и заканчивать подбор пароля.
- кнопка Набор позволяет задать свое множество символов, если известны символы, из которых состоит пароль.
- кнопка Справка выводит помощь по программе.
- кнопка О AZPR выводит информацию о программе.
- кнопка Выход позволяет выйти из программы



Рассмотрим возможности программы:

Выбирается архив для вскрытия и тип атаки (см. рис).

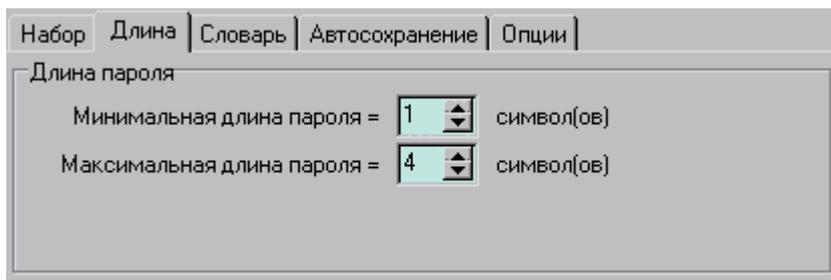


Выбираются параметры работы:

- Закладка Набор

Программа позволяет выбрать область перебора (набор символов). Это значительно сокращает время перебора. Можно использовать набор пользователя, заданный с помощью кнопки Набор. Можно ограничить количество тестируемых паролей, задав начальный пароль. В случае если известна часть пароля, очень эффективна атака по маске. Нужно выбрать соответствующий тип атаки, после этого станет доступным поле маска. В нем нужно ввести известную часть пароля в виде P?s?W?r? , где на месте неизвестных символов нужно поставить знак вопроса. Можно использовать любой другой символ, введя его в поле символ маски.

- Закладка Длина



Позволяет выбрать длину пароля.

- Закладка Словарь

Позволяет выбрать файл-словарь. Выбирайте файл English.dic, он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

- Закладка Автосохранение

Можно выбрать имя файла для сохранения результатов работы и интервал автосохранения.

- Закладка Опции

Выбирается приоритет работы (фоновый или высокий), интервал обновления информации о тестируемом в данный момент пароле. Увеличение интервала повышает быстродействие, но снижает информативность. Также можно установить режим ведения протокола работы и возможность минимизации программы в tray (маленькая иконка рядом с часами).

3 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТ

3.1. Проведение атаки перебором (bruteforce attack)

1. Создайте запароленный архив, используя программу WinRar, при этом длина пароля должна составлять от 1 до 8 символов для различных алфавитов:

- А) только английские малые буквы;
- Б) только английские малые буквы и цифры;
- В) английские буквы большого и малого регистра и цифры.

Используя программу для вскрытия паролей произвести атаку на зашифрованный файл. Область перебора – английские буквы большого и малого регистра и цифры, длина пароля от 1 до 8 символов. Проверить правильность определенного пароля, распаковав файл и ознакомившись с его содержимым.

2. Выполнив пункт 1, сократить область перебора до фактически используемого (например, если пароль 6D1A – то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время.

3. Провести анализ затраченного времени на взлом в зависимости от длины пароля и алфавита.

3.2.Проведение атаки по словарю (dictionary attack)

1. Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто используемые в качестве паролей.

2. Попытайтесь определить пароль методом прямого перебора. Сравнить затраченное время.

4.СОДЕРЖАНИЕ ОТЧЕТА

- 1) титульный лист;
- 2) формулировку цели работы;
- 3) описание результатов выполнения;
- 4) выводы, согласованные с целью работы.

5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие виды атак на пароль Вы знаете?
2. Что такое плохой пароль?
4. Как можно противостоять атаке полным перебором?
4. Как длина пароля влияет на вероятность раскрытия пароля?
5. Какие рекомендации по составлению паролей Вы можете дать?