
БУДЬ НА ЧЕКУ.
В ТАКИЕ ДНИ
ПОДСЛУШИВАЮТ СТЕНЫ.
НЕДАЛЕКО ОТ БОЛТОВНИ
И СПЛЕТНИ
ДО ИЗМЕНЫ.
НЕ БОЛТАЙ!

Парольная защита информации

План занятия

1. Актуальность проблемы парольной защиты.
2. Взлом парольной защиты.
3. Правила парольной защиты.
4. Практическая работа : создание надежного легко запоминающегося пароля.

Актуальность проблемы парольной защиты

Аутентификация пользователей, т.е. подтверждение их подлинности, обеспечивается в первую очередь путем использования парольной защиты.

Слабая парольная защита является одной из основных причин уязвимости компьютерных систем к попыткам несанкционированного доступа.

В 2008 году 84 % компьютерных взломов были осуществлены вследствие несовершенства парольной защиты.

По данным опросов, проведенных по заказу устроителей международной выставки Infosecurity Europe более 70 % британцев признались, что отдали бы постороннему пароль от своего компьютера в обмен на плитку шоколада, а некоторые и без какой бы то ни было материальной компенсации. Кроме того, по результатам другого опроса 79 % жителей Великобритании хоть раз отдавали посторонним лицам информацию, которая могла бы быть использована для кражи персональных данных, необходимых для незаконных операций с кредитными карточками и другими финансовыми инструментами.

По результатам опроса, проведенного компанией Sophos, 41 % респондентов используют один и тот же пароль во всех случаях, из них 75 % используют не только один и тот же пароль во всех случаях, но он является простым, легко угадываемым. Следовательно, 31 % пользователей (75 % от 41 %) не обладают учетными записями с надежно защищенными паролями доступа.

Другое исследование, проведенное в Великобритании, показало, что почти две трети коммерческих пользователей не применяют пароль при входе в системы своих ноутбуков, а из тех, кто пользуется паролем, 15 % употребляют в качестве пароля собственное имя, а 10 % сообщают свой пароль коллегам. Одна треть опрошенных ни разу не меняла пароль на протяжении прошедшего года .

По данным 2009 г. самым популярным паролем по-прежнему остается «1234». На втором месте «12345678», на которые приходится 14 % взломов. Благодаря подбору только этих двух паролей, в прошлом году хакеры похитили с банковских счетов несколько миллионов долларов. К числу самых популярных паролей относятся «QWERTY» и «AZERTY» (соответствующие клавиши расположены подряд в левой верхней части клавиатуры для англо- и франкоговорящих стран), а также имена детей и их даты рождения.

Пароли «Покемон» и «Матрица» позволили осуществить взлом в 5 % случаев, а пароли «password» и «password1» – еще в 4 %.

Председатель правления Microsoft Билл Гейтс в одном из своих выступлений еще в 2006 г. предсказал гибель традиционным паролям, так как они не в состоянии с должной надежностью обеспечить информационную безопасность.

Для замены традиционного пароля перспективными являются биометрические системы контроля доступа.

Взлом парольной защиты

Для взлома парольной защиты используются следующие методы:

1. Узнавание пароля.
2. Угадывание пароля.
3. Словарная атака.
4. Метод прямого перебора.
5. Использование программных закладок.
6. Удаленный доступ к компьютеру.
7. Непосредственный доступ к компьютеру.
8. Перехват паролей с использованием технических средств.

Узнавание пароля

- доступность записанных паролей
- выведывание информации
- контрольные вопросы при регистрации

Угадывание пароля

- имена
- фамилии
- год рождения
- номер телефона
- совпадение с логином

Словарная атака

- обычное использование словаря;
- записанные дважды слова;
- обратный порядок символов слов;
- усеченные до заданного количества символов слова;
- слова без гласных, за исключением заглавной;
- транслитерация русских букв латинскими по заданной таблице транслитерации;
- замена раскладки локализации латинской раскладкой клавиатуры;
- замена латинской раскладки клавиатуры раскладкой локализации.

Метод прямого перебора

- время взлома пароля, состоящего из слов английского (русского) языка составляет до 2 минут;
- время взлома пароля длиной 8 символов, состоящего из цифр составляет 18 секунд;
- время взлома пароля длиной 8 символов, состоящего из цифр и букв английского алфавита составляет до 6 суток;
- время взлома пароля длиной 8 символов, состоящего из цифр, букв и символов достигает 61 суток.

Использование программных закладок

Программная закладка – это программа или фрагмент программы, скрытно внедряемый в защищенную систему и позволяющий злоумышленнику, внедрившему его, осуществлять несанкционированный доступ к тем или иным ресурсам защищенной системы .

Удаленный доступ к компьютеру

Получение парольной информации злоумышленником возможно при успешном проведении сетевых атак и получении возможности удаленного управления компьютером.

Очевидно, что в этом случае обеспечивается возможность получения любой, в том числе, парольной информации, хранящейся в компьютере.

Непосредственный доступ к компьютеру

- не перекрыта возможность загрузки операционной системы с внешних носителей (дискет, CD, DVD)
- вскрытие корпус компьютера и

а) подключения жесткого диска атакуемого компьютера к другому компьютеру

б) загрузка с другого жесткого диска

Перехват паролей с использованием технических средств

В подавляющем большинстве случаев используются электромагнитный и электрический каналы утечки, реже – оптический канал, предполагающий возможность визуального наблюдения за процессом ввода информации. Такое наблюдение может осуществляться с использованием оптических приборов или видеокамер.

Правила парольной защиты

Требования к надежному паролю:

1. Пароль должен быть секретным
2. Пароль должен быть длинным
3. Пароль должен быть трудно угадываемым
4. Пароль не должен представлять собой распространенные слова, имена, названия
5. Пароль должен быть сложным
6. Пароль должен регулярно меняться

Требования к надежному паролю (продолжение):

7. Пароль должен значительно отличаться от паролей, использовавшихся ранее
8. Каждый пароль должен использоваться уникально
9. Подсказки к паролям не должны использоваться
10. Пароль не должен передаваться по недостаточно надежно защищенным каналам связи
11. Пароль должен немедленно заменяться, если есть подозрения, что он мог быть раскрыт.

Пароль должен быть секретным:

- недопустимо отображение пароля на экране;
- записанный пароль нельзя хранить в местах, доступных неавторизованным лицам, например, на листочках, приклеиваемых к монитору;
- файл паролей должен иметь надежную криптографическую защиту; – пароль не рекомендуется сохранять в компьютере даже в специальных защищенных файлах – для большей безопасности пароль следует хранить записанным на внешний носитель, который должен быть надежно защищен от несанкционированного доступа;
- возможности операционной системы и других программ по сохранению пароля должны игнорироваться, на предложение программ запомнить пароль нужно всегда отвечать отказом.

Пароль должен быть длинным:

пароль должен состоять не менее чем из 8 символов, иначе он легко может быть взломан программами прямого перебора

Пароль должен быть трудно угадываемым:

недопустимо совпадение пароля с логином, использование в качестве пароля имени, фамилии, даты рождения, номеров телефонов пользователя или его родственников, кличек любимых домашних животных, названий спортивных клубов, географических названий, например, любимых мест отдыха и т.п.

Пароль не должен представлять собой распространенные слова, имена, названия

для защиты от атаки со словарем.

Пароль должен быть сложным

Пароль должен представлять собой случайную комбинацию различных символов для защиты от атаки методом прямого перебора: пароль должен содержать не только буквы, как прописные, так и строчные, цифры, а также различные не буквенно-цифровые символы

(` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /), которые могут быть введены с клавиатуры, т.е. при вводе пароля должно выполняться переключение верхнего и нижнего регистров клавиатуры, а, если возможно, то и переключение раскладки клавиатуры (т. е. переключение языка – английский-русский); лучшими паролями являются пароли, сгенерированные как случайные последовательности.

Пароль должен регулярно меняться

Желательно, чтобы изменения пароля осуществлялись не реже одного раза в 60-90 дней и не по графику, а случайным образом.

Пароль должен значительно отличаться от паролей, использовавшихся ранее

В противном случае, обладая информацией о предыдущих паролях, возможно подобрать текущий пароль.

Каждый пароль должен использоваться уникально

Каждый пароль должен использоваться только одним пользователем и для получения доступа только к одной из систем или программ, т. е. нельзя использовать один и тот же пароль для доступа, например, к сеансу работы с компьютером и для доступа к электронному почтовому ящику.

Подсказки к паролям не должны использоваться

Следует всегда игнорировать предусмотренные на случай, если пароль будет забыт, предложения операционной системы или других программ ввести при задании пароля подсказку, указать дополнительные сведения или ответ на контрольный вопрос (например, о вашем росте, любимом блюде, девичьей фамилии матери, номере паспорта и т.п.), – злоумышленнику может оказаться значительно легче узнать (подобрать) ответ на подсказку, чем узнать пароль.

Пароль не должен передаваться по недостаточно надежно защищенным каналам связи, например, пересылаться по электронной почте, передаваться по телефону, факсу и т.п..

Пароль должен немедленно заменяться,
если есть подозрения,
что он мог быть раскрыт.

Практическая работа

Создание надежного легко запоминающегося пароля

Пример

1. Возьмем слова известной песни

«Три танкиста, три веселых друга – экипаж машины боевой»

2. Используем первые буквы слов, заменив числительные цифрами и сохранив знаки препинания:

«3Т,3вд-ЭМБ»

3.Наберем полученный текст латинскими буквами:

@3N?3dl-“V<@


Функциональные клавиши
Клавиши управления питанием компьютера
Световые индикаторы
Esc
F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12
Power Sleep Wake Up
Num Lock Caps Lock Scroll Lock
Fn
Backspace
Tab
Caps Lock
Enter
Shift
Ctrl
Alt
Space Bar
(Пробел)
Print Scrn SysRq
Scroll Lock
Pause
Insert Home Page Up
Delete End Page Down
Num Lock
Специальные клавиши
Алфавитно-цифровая клавиатура
Специальные клавиши
Клавиши управления курсором
Цифровая клавиатура