**Практическое занятие – разбор задачи по теме**
**«Количественная оценка стойкости парольной защиты»**

Реализуются в открытых компьютерных системах. Являются наиболее распространенными. В качестве идентификации используется Login (имя пользователя), в качестве аутентификации – секретный пароль.
Преимущества: дешевизна, возможность использовать во всех компьютерных системах.
Недостаток: самые уязвимые ко взлому:

- перебор пароля в интерактивном режиме;
- подсмотр, кража из общедоступного места;
- возможность преднамеренной передачи пароля другому лицу;
- кража БД учетных записей из общедоступного места;
- перехват вводимого пароля путем внедрения в КС программных закладок;
- перехват паролей передаваемых по сети;
- возможность применения социального инжиниринга.

Большинство минусов, свойственных парольным системам, связано с наличием человеческого фактора, который проявляется в том, что пользователи склонны выбирать легкозапоминаемые пароли, а сложнозапоминаемые стараются где-то записать.

Для уменьшения влияния человеческого фактора требуется реализовать ряд требований к подсистеме парольной аутентификации.
Требования:

1. задавание минимальной длины пароля для затруднения перебора паролей в лоб;
2. использование для составления пароля различных групп символов для усложнения перебора;
3. проверка и отбраковка паролей по словарю;
4. установка максимальных и минимальных сроков действия паролей;
5. применения эвристических алгоритмов, бракующих нехорошие пароли;
6. определение попыток ввода паролей;
7. использование задержек при вводе неправильных паролей;
8. поддержка режима принудительной смены пароля;
9. запрет на выбор паролей самим пользователем и назначение паролей администратором, формирование паролей с помощью автоматических генераторов стойких паролей.

Вероятность подбора паролей злоумышленником, можно привести в следующем виде:

$$P(t < T) = \begin{cases} \dfrac{V \cdot T}{A^L}, V \cdot T < A^L; \\ 1, V \cdot T \geq A^L. \end{cases}$$

A – мощность алфавита символов, из которых состоит пароль;
L – длина пароля, символов;
V – скорость перебора паролей злоумышленником, паролей/секунду;
T – срок действия паролей, в секундах. Обычно задается в сутках, поэтому нужно умножить на количество секунд в сутках – 86400 с.;
P – вероятность подбора паролей злоумышленником за время t, меньшее срока действия паролей.

***Разберем пример:***

Парольная фраза длинной *L=10* состоит только из цифр, т.е. мощность используемого алфавита *A=10,* в соответствии с парольной политикой срок действия

одного пароля – 30 суток, тогда вероятность подбора пароля за $t<T$ (например, 29 суток) при скорости перебора паролей на ЭВМ (типа Intel(R) Core(TM)2 CPU 6300 @ 1.86GHz, 1867 МГц, ядер: 2, логических процессоров: 2, 2ГБ ОЗУ с ОС Windows 7) – 14,5 млн. паролей в секунду получаем $P=1$, т.к.:

$$V \cdot T > A^L;$$

$$14,5 \cdot 10^6 \cdot 30 \cdot 86400 > 10^{10};$$

$$3,7584 \cdot 10^{13} > 10^{10},$$

т.е. за срок менее 30 суток пароль из 10 цифр будет взломан.

Еще один вывод, который можно и нужно сделать по результату расчета: на сколько нужно увеличить длину пароля, что нужно сделать, чтобы соблюдалось следующее неравенство $V \cdot T < A^L$ . Т Для этого пароль нужно увеличить минимум на 4 символа, тогда получим $L=14$, т.е. $3,7584 \cdot 10^{13} > 10^{14}$ .

Все рассмотренное выше справедливо только для метода прямого перебора паролей («brute-force»). На данный момент существует множество более эффективных методик оценки защищенности парольных систем аутентификации и исключительно парольная аутентификация практически не применяется в системах хранящих, обрабатывающих и передающих конфиденциальную информацию.

См. статьи: Радужные таблицы, полный перебор, пароль и т.д.

http://ru.wikipedia.org/wiki/%D0%92%D0%B7%D0%BB%D0%BE%D0%BC_%D0%BF%D0%B0%D1%80%D0%BE%D0%BB%D1%8F

http://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D1%83%D0%B6%D0%BD%D0%B0%D1%8F_%D1%82%D0%B0%D0%B1%D0%BB%D0%B8%D1%86%D0%B0

http://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%B1%D0%BE%D1%80_%D0%BF%D0%BE_%D1%81%D0%BB%D0%BE%D0%B2%D0%B0%D1%80%D1%8E

http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%BD%D1%8B%D0%B9_%D0%BF%D0%B5%D1%80%D0%B5%D0%B1%D0%BE%D1%80