УДК 378:147.157+004:37

АЛГОРИТМ ПРОГРАММНОЙ ГЕНЕРАЦИИ ПАРОЛЬНОГО ДОСТУПА К ДАННЫМ

Г.К. Кожевников, доцент, к.т.н., Т.С. Бондаренко, ассистент,
Украинская инженерно-педагогическая академия

Аннотация. *Проведена разработка алгоритма парольного доступа к данным с использованием метода программной генерации парольного доступа. Проанализированы недостатки существующих методов формирования парольного доступа. Для программной реализации использовали язык программирования ASP.net с использованием максимально сложной символьной комбинации пароля.*

Ключевые слова: *парольный доступ, программная генерация, буфер обмена, алгоритм, защита данных, макрос, дилемма.*

Введение

Одним из наиболее распространенных методов защиты информации является парольный доступ к данным [1]. Однако, наряду с несомненными достоинствами, этот метод защиты данных обладает и определенными недостатками: пароль можно забыть, его могут «взломать», если он недостаточно сложный.

Таким образом, при использовании парольного доступа возникает дилемма: простой пароль никому не нужен, т.к. его легко взломать; сложный пароль никому не нужен, т.к. его легко забыть или потерять или обнаружить, записанным где-либо.

Специалисты рекомендуют в качестве пароля использовать фразы. Но и эти пароли не лишены недостатков. Известно, что словари всех языков давно составлены вместе со всеми возможными формами слов и распространённые системы подбора паролей начинают перебор, используя словарь, в котором слова расставлены по частоте их употребления.

Цель и постановка задачи

В связи с выше изложенным возникает задача разработать алгоритм парольного доступа, который, с одной стороны, обладает достаточной степенью стойкости к попыткам «взлома» пароля, а, с другой стороны, не требует больших усилий для запоминания пароля и его хранения.

Методы исследований

Указанные выше недостатки могут быть устранены, если вместо обычной схемы парольного доступа использовать алгоритм, использующий метод программной генерации парольного доступа к данным, приведенный на рис. 1.

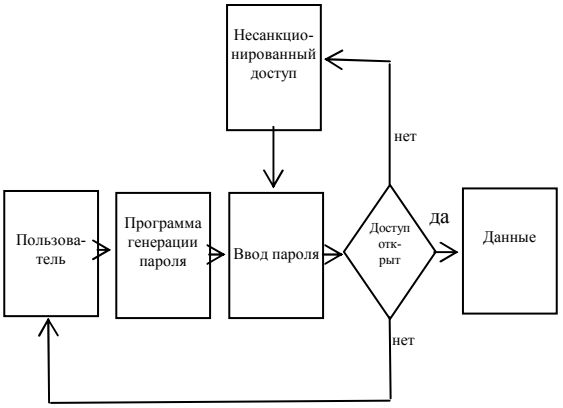

Рис. 1. Алгоритм программной генерации парольного доступа к данным

Как и в обычном алгоритме, доступ к данным будет открыт при условии правильного ввода пароля. Но, если несанкционированный доступ осуществляется с обычной точки ввода пароля, то пользователь для формирования пароля использует специальную программу генерации.

В качестве программы генерации пароля можно использовать известные программы, например, Advanced Password Generator. Однако делать это не рекомендуется, поскольку для опытного пользователя не составит труда включить данную программу в приведенный выше алгоритм программной генерации паролей. Разработка собственной программы не займет много времени, а секретность алгоритма генерации пароля будет служить

дополнительной степенью защиты для системы хранения данных.

В качестве параметров генерации пароля можно использовать набор символов, которые могут быть использованы для записи пароля, длину пароля и ключ генерации пароля (любое число или сочетание символов). Последний параметр используется для инициализации генератора случайных чисел. Таким образом, длина пароля не зависит от длины ключа, то есть, вводя всего один символ, вы можете получить максимально возможную последовательность символов пароля. Чтобы исключить возможность несанкционированной генерации пароля, целесообразно в программе генерации пароля, кроме генератора случайных чисел, использовать дополнительные функции (тригонометрические, экспоненциальные и т.п.), обеспечивающие искажение результатов работы датчика случайных чисел.

Если в качестве пароля выбрано случайное сочетание символов клавиатуры разных регистров, то возможных вариантов пароля при его длине 12 символов будет примерно $142^{12} \approx 7 \cdot 10^{25}$. Тогда, если кто-либо попытается взламывать вашу защиту, перебирая пароль со скоростью 10 000 вариантов в секунду (средний компьютер), то перебор вариантов займёт

$$\frac{142^{12}\,\text{вариантов}}{10000\ \text{вар/сек}} = 7 \times 10^{21}\,\text{сек} = 2 \times 10^{14}\,\text{год}.$$

Однако, маловероятно, чтобы кто-либо использовал для формирования пароля все возможные символы клавиатуры. Вместе с тем, при использовании алгоритма парольной генерации, если ввод сгенерированного пароля осуществляется не через клавиатуру, а через буфер обмена, число возможных символов пароля равно не 142, как на клавиатуре, а 256 (полный набор символов ASCII). При этом число возможных вариантов пароля при его длине 12 символов будет равно $256^{12} \approx 8 \cdot 10^{28}$. Таким образом, использование алгоритма парольной генерации позволяет повысить стойкость парольной защиты данных.

Еще одна проблема парольного доступа к дан ным – необходимость использования нескольких паролей для различных целей. Специалисты настоятельно рекомендуют не использовать один пароль для нескольких целей. Предположим, что вы придумали и ухитрились запомнить один хороший пароль. Но что делать, если вам необходимо запомнить 3 – 4, а может и больше, паролей. В данном случае использование алгоритма программной генерации парольного доступа существенно облегчает решение данной проблемы. Используя алгоритм программной генерации, можна использовать в качестве пароля номер телефона, имя любимой собаки, дату рождения и все возможные варианты, которые существенно облегчают запоминание, но не рекомендуют использовать специалисты.

Известно, что при наборе пароля, хотя он, как правило, на экране не отображается, следует всё же избегать чужих глаз. Предлагаемый алгоритм программной генерации пароля предоставляет возможность легко справиться с данной задачей. Для этого необходимо программу генерации пароля оформить в виде макроса MS Word или MS Excel. Тогда порядок ввода пароля может быть следующим:
– вызвать, например, текстовый документ, содержащий встроенный макрос генерации паролей;
– при загрузке документа либо при выполнении определенных действий с текстом макрос запускается на выполнение и генерирует пароль, который записывает в буфер обмена Office;
– вставить сгенерированный макросом пароль из буфера обмена в поле ввода пароля и очистить буфер обмена.

Еще одно достоинство предлагаемого алгоритма заключается в том, что сгенерированный пароль можно передавать в поле ввода через буфер обмена. При этом не используется клавиатура, что является дополнительной степенью защиты пароля пользователя от так называемых программ «клавиатурных шпионов».

Результаты

Авторами разработан на языке ASP.net ряд простых, но эффективных программ генерации паролей. Опыт использования предложенного алгоритма показал, что его применение не только не усложняет задачу парольного доступа к данным, но и в отдельных случаях облегчает процедуру ввода пароля.

Выводы

Описанный алгоритм с одной стороны облегчает пользователю решение проблемы запоминания и хранения стойких паролей, а с другой стороны повышает стойкость системы хранения данных к несанкционированному доступу за счет использования максимально сложной символьной комбинации пароля.

Литература

1. Бэнкс М.А. Информационная защита ПК / Пер. с англ. – К.: ВЕК+, 2001. – 272 с.

Рецензент: О.П. Алексеев, профессор, д.т.н., ХНАДУ.

Статья поступила в редакцию 28 июня 2006 г.