Использование графической информации для защиты программного и информационного обеспечения

С.А. Панкратов

ГОУВПО «Московский государственный текстильный университетимени А.Н. Косыгина»

Как известно, столь привычные для нас буквенно-цифровые пароли совсем небезопасны. Специалисты онлайнового банка «Egg» недавно провели исследование, которое показало, что пользователи, как правило, применяют в качестве паролей хорошо известные им имена детей, партнеров, спортсменов-чемпионов, кинозвезд и т.п. Более того, люди меняют пароли только тогда, когда система заставляет их это сделать. Что бы ни защищали эти пароли, люди упорно используют примитивные слова вместо цифро-буквенных сочетаний. Подобный подход отчасти объясняется неосведомленностью, отчасти ленью, а отчасти свойствами нашей памяти, неспособной запомнить стойкий к перебору код типа «58hGj1%p3» [2].

В данной работе предлагается способ графической аутентификации, который учитывает психологию людей, существенно повышающий защищенность систем, но не усложняющий саму процедуру. Пользователю предоставляется несколько коллекций изображений разбитых по темам (рис.1).

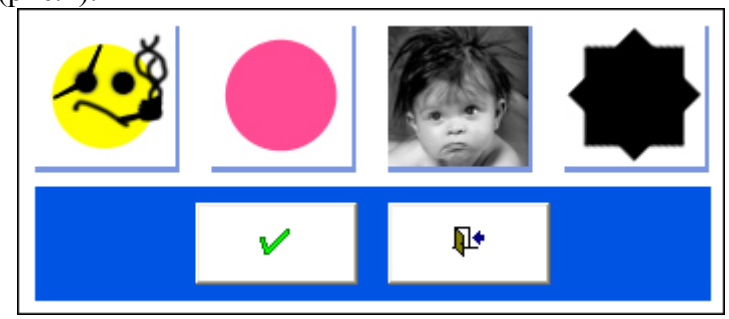

Рис.1. Коллекции изображений

При выборе коллекции появляется поле с девятью изображениями, под которыми располагаются поле для ввода дополнительного текстового пароля и кнопки управления (рис.2).

Рис.2. Интерфейс системы графической аутентификации

Пользователь должен выбрать набор изображений и ввести текстовый пароль (есть функция отображения вводимого пароля в виде символа «*»). При ошибочном вводе пароля изображения перемешиваются, выстраиваясь в определенную комбинацию, и текстовое поле очищается. Таких комбинаций девять. Свойство перемешивания изображений позволяет избавиться от «подглядывания» и легкого визуального запоминания пароля. Что касается внутреннего алгоритма, то вводимые графический и текстовый пароли преобразуются алгоритмом хеширования MD5 в хэш-коды, которые представляют собой строки длинной в 32 символа (например, «13A5777F1C2927F2C641020ACF086983»). Эти коды хранятся в базе данных и сложны для понимания истинного значения пароля и его взлома. Программа-шпион не сможет отследить ввод графического пароля с клавиатуры, так как помимо текстового (второстепенного) пароля существует еще графический. Выявить четкий алгоритм ввода координат мыши при нажатии на изображения также невозможно, так как изображения перемешиваются, и последовательность координат кликов меняется. Кроме того, можно установить промежуток времени, через который пользователь должен поменять пароль, например, пользователь должен. Запомнить пароль в виде набора картинок легче (например, вообразив себе некую историю или сценку), в чем и отражается неоспоримое преимущество графических паролей [1].

Если рассмотреть ситуацию подбора пароля относительно записей в базе данных, то она выглядит следующим образом: как текстовый, так и графический пароль хранится в БД в виде хеш-кода. Его алфавит содержит большие латинские буквы и цифры. Следовательно, если взять графический пароль за «логин», а текстовый – за «пароль», то по формуле Андерсона (1) можно подсчитать время, за которое пароль заданной длины будет гарантированно подобран методом «Грубой силы»:

$$T <= \frac{A^L}{V} \qquad (1)$$

T – Время;
A – Алфавит;
L – Длина;
V – Скорость перебора.

$$T <= \frac{36^{32}}{10^{7}} = 6{,}33*10^{42}$$ лет

Но данным методом подбора пароля никто пользоваться не будет, так как текущему пользователю доступна таблица (а точнее, представление), которая предоставляет данные по текущему пользователю. И если злоумышленник разработает систему-сниффер (перехватчик), которая будет перехватывать сигнал с паролем, передающий из программы в базу данных, то у него есть шанс заменить пароль в виде хеш-кода на тот, который хранится в БД.

Количество возможных комбинаций пароля, если пользователь использует только блок графического пароля, можно вычислить по формуле расчета максимального числа комбинаций пароля (2).

$$A_n^m = \frac{n!}{(n-m)!} \qquad (2)$$

n – Алфавит текстового пароля или количество элементов графического пароля;
m – Количество элементов в водимом пароле.

$$A_9^1 + A_9^2 + A_9^3 + A_9^4 + ... + A_9^9 + 1 = 986410,$$

т.е. пользователь может выбрать себе пароль из 986 410 комбинаций – без учета функции перемешивания элементов; из 8 877 681 – с учетом этой функции.

Ситуация, когда пользователь использует только текстовый пароль. В данной системе текстовый пароль может содержать в себе латинский алфавит разного регистра – 52 символа; кириллицу разного регистра – 66 символов; цифры от 0 до 9 – 10 символов; различные символы, такие как: знаки препинания (.,;:!?), пробел, скобки, кавычки – 29 символов. Итого получаем, что в текстовый блок можно включить 157 символов.

Предположим, что пользователь может ввести 12 символов (хотя на самом деле система прошла тест на ввод 100 символов), тогда по той же формуле получаем:

$$A_{157}^1 + A_{157}^2 + A_{157}^3 + A_{157}^4 + ... + A_{157}^{12} + 1 = 1.46752*10^{26}$$

Всего возможных паролей:

$$986410*1.46752*10^{26} \approx 1{,}5*10^{32}$$

Выводы:

- В статье рассмотрен способ графической аутентификации для дополнительной защиты программного и информационного обеспечения, которая учитывает психологию людей.
- Исследования способа графической аутентификации показали, что при существенном увеличении степени защиты не усложняется сама процедура получения доступа.

Литература

1. Панкратов С.А., «Проблемы экономики и прогрессивные технологии в текстильной, легкой и полиграфической отраслях промышленности», Всероссийская науч.-техн. конф. (2009, Санкт-Петербург) «Система графической аутентификации»: тез.докл. – СПб.: СПГУТД, 2009. – 301 с.
2. Панкратов С.А., Фирсов А.В., «Комплексная защита корпоративной информации на текстильном предприятии», «Современные технологии и

оборудование текстильной промышленности» (ТЕКСТИЛЬ – 2011). - М.: ФГБОУ ВПО «МГТУ им. А.Н. Косыгина», 2011. – 40 с.