УДК 004

Визуальная безопасность графических паролей

А. А. Красавин
Московский физико-технический институт (государственный университет),
ЗАО «ОКБ САПР», Москва, Россия

Рассмотрено понятие графического пароля, проведено его сравнение с символьными паролями, рассмотрены факторы, влияющие на безопасность графических паролей, и приведены возможные способы их модификации с целью повышения безопасности.

Ключевые слова: аутентификация, графический пароль.

Зачем нужны графические пароли?

Пункт 1. Выполнение входа в систему на ПК посредством сенсорного ввода традиционно было довольно громоздким процессом. Требования, предъявляемые к надежности паролей, растут: приходится вводить цифры и символы в разных регистрах, поэтому ввод длинного сложного пароля на экранной клавиатуре может занять до 30 секунд. Одним из главных условий, приведших к созданию графических паролей, стало требование ускорить ввод пароля.

Пункт 2. Стандартные пароли, содержащие в себе цифры, буквы в разных регистрах и особые символы, сложны для запоминания. Типичные же последовательности цифр, такие как 1111 или 1234, или пароли, составленные на основе персональных данных человека (большинство из которых не так уж и сложно получить), очевидно, ненадежны. Отсюда пришло второе условие: пароль должен быть как достаточно надежным, так и легким для запоминания. Таким решением стали графические пароли.

Что такое графические пароли?

Многочисленные исследования показали, что человеку, как правило, гораздо проще запоминать рисунки и жесты, чем наборы цифр и букв.

Графический пароль — это совокупность некоторого рисунка, выбираемого пользователем, и неких жестов, которые на этот рисунок накладываются. При попытке войти при помощи графического пароля в операционную систему (ОС), происходит оценка нарисованных графических знаков и сравнение их с графическими знаками, которые были использованы при создании пароля. Затем происходит оценка разницы между каждым графическим знаком, и принимается решение об авторизации на основании количества ошибок в комплексе.

Графические пароли уже используются наряду со стандартным способом аутентификации. Так, в Windows 8 при создании и вводе графического пароля используются комбинации кругов, прямых линий или прикосновений нанесенных на сетку размером 100×100, а в ОС Android используется сетка с 9 точками, которые пользователю предлагается соединить в некотором порядке.

Сложность графического пароля можно определить количеством различных паролей с одной длиной (для графического пароля под длиной следует понимать количество использованных жестов). Это количество напрямую влияет на то, сколько времени нужно потратить злоумышленнику для взлома пароля для любого из используемых им методов (прямого перебора, перебора с использованием словаря и т. д.).

Если сравнить таким образом безопасность различных типов паролей, используемых в Windows 8, то результаты будут следующими (табл. 1)

Из таблицы видно, что графический пароль удовлетворяет, теоретически требованиям, выдвинутым в *пункте 1*. Но что же может повлиять на его безопасность?

Факторы, влияющие на безопасность графических паролей

Следы на поверхности экрана

При использовании планшетов и коммуникаторов на поверхности экрана остаются следы от прикосновений. Эти следы могут очень точно обозначать те места, где пользователь провел линию,

Красавин Александр Алексеевич, студент, программист.
E-mail: akrasav@mail.ru

Статья поступила в редакцию 14 июня 2014 г.

Таблица 1

Результаты сравнения безопасности различных видов паролей в Windows 8

Длина	10-разрядный ПИН-код	Простой пароль из набора знаков a—z	Пароль из более сложного набора знаков	Графический пароль из нескольких жестов
1	10	26	нет	2554
2	100	676	нет	1581773
3	1 000	17 576	81 120	1155509 083
4	10 000	456976	4 218 240	612157353732
5	100 000	11 881376	182 790 400	398046621309 172
6	1 000 000	308915776	7 128 825 600	
7	10 000 000	8031810176	259 489 251 840	
8	100 000 000	208827064576	8 995 627 397 120	

а где нарисовал круг, причем зачастую можно даже угадать их направление. Это существенно понижает безопасность графического пароля: количество различных паролей с одной длиной, которые мы можем теперь получить, уменьшается в разы:

Таблица 2

Безопасность графического пароля

Длина	ПИН-код	Пароль	Пароль с Shift	Только жесты-касания	Жесты из линий и кругов
1	1	1	1	1	2
2	2	2	4	2	8
3	6	6	18	6	48
4	24	24	96	24	384

"Точки интереса"

При выборе графического пароля пользователь выбирает не произвольные точки, а какие-то особые точки (например, нос человека, его лицо, колесо машины и т. д.), на которые ему проще обратить внимание, а значит, легче запомнить и воспроизвести жесты, с ними связанные (*пункт 1*, первое требование). Эти точки можно назвать, как "точки интереса".

Их количество на изображении ограничено, что также, как и следы на экране, в несколько раз уменьшает количество различных паролей с одной длиной, которые мы можем получить, используя рисунок (табл. 3):

Таблица 3

Точки интереса

Длина	**5**	**10**	**15**	**20**
1	75	200	375	600
2	5 625	40 000	140 625	360 000
3	421 875	8 000 000	52 734 375	216 000 000
4	31 640 625	1 600 000 000	19 775 390 625	129 600 000 000

Пароль легче "подглядеть"

Пароль стал проще для запоминания (см. п.1). А значит, проще стало и злоумышленнику запомнить его. Этот вывод может существенно понизить удобство использования графических паролей.

Повышение безопасности графических паролей

Единственный способ повысить безопасность графического пароля в том виде, в котором он используется сейчас, — увеличить количество точек внимания на изображении или количество используемых при создании пароля жестов. А это отобразится на сложности его запоминания и скорости его ввода и, как следствие, негативно повлияет на его удобство в использовании.

Вариантом повышения безопасности графического пароля может стать использование динамического пароля. Для этого типа паролей не используются рисунок и жесты на нем. В данном случае пользователь запоминает некоторые пиктограммы из какого-то списка, задает их порядок, а затем для каждой выбирает некоторые жесты для них. При входе в систему некоторое количество пиктограмм отображается на экране, а пользователь должен просто соединить выбранные им пиктограммы в нужном порядке (или обвести их правильно). Если порядок пиктограмм и жестов задан правильно, то он получает доступ.

В другой вариации динамического пароля пользователю даже не нужно придумывать жесты для каждой из выбранной им пиктограмм. При входе в систему на экране гарантированно отображается три или четыре из них. Пользователю нужно просто найти среди всех пиктограмм на эк-

ране "свои", соединить их в уме линиями и поставить точку внутри получившейся геометрической фигуры (треугольника или четырехугольника). Для большей безопасности, чтобы такой пароль сложнее было угадать, можно повторить эту процедуру неоднократно, каждый раз изменяя набор отображаемых на экране пиктограмм.

Таким образом, для динамических паролей сохраняются такие плюсы использования графических паролей, как простота их запоминания и сложность взлома: также используется визуальная информация для запоминания и система "точка интереса" — жест, обеспечивающая их безопасность. При этом, однако, решаются две проблемы "простых" графических паролей: наличие следов на поверхности экрана и возможность подглядеть пароль, так как при вводе пароля все пиктограммы располагаются случайным образом на экране, так что понять, что за пиктограммы использует пользователь при вводе пароля из движений по экрану злоумышленнику становится значительно сложнее.

Однако большим минусом для таких паролей может стать время их ввода: если на экране отображается большое количество пиктограмм, то поиск среди них нужной может занять продолжительное время.

Visual security of graphical passwords

A. A. Krasavin
Moscow Institute of Physics and Technology (State University),
OKB SAPR JSC, Moscow, Russia

This article deals with the concept of a graphical password, its comparison with character passwords, the factors affecting the security of graphical passwords, and shows how they can be modified to improve their security.

Keywords: authentication, graphical password.

Received June 14, 2014